



User Guide

AC2200 Home Wi-Fi System
HC2220-G1u

Contents

About This Guide	1
Chapter 1. Get to Know Your Devices.....	2
1. 1. Product Overview.....	3
1. 2. Appearance	3
1. 2. 1. LEDs	3
1. 2. 2. Buttons and Ports	4
Chapter 2. Connect the Hardware	6
2. 1. Position the Devices	7
2. 2. Connect Your Controller	7
2. 3. Connect Your Satellites	10
Chapter 3. Log In to Your Controller	11
Chapter 4. Set Up Internet Connection	13
4. 1. Use Quick Setup Wizard	14
4. 2. Set Up an IPv6 Internet Connection	15
4. 3. Configure the Controller in Access Point Mode.....	16
Chapter 5. Add Satellites to Your Network.....	17
5. 1. Sync Your Satellites.....	18
5. 2. Place Your Satellites	20
Chapter 6. USB Settings.....	22
6. 1. Access the USB Storage Device	23
6. 1. 1. Access the USB Device Locally	23
6. 1. 2. Access the USB Device Remotely.....	24
6. 1. 3. View USB Storage Device.....	26
6. 1. 4. Customize the Access Settings.....	27
6. 2. Media Sharing	30
6. 3. 3G/4G Settings	31
Chapter 7. Network Security	33
7. 1. Firewall & DoS Protection	34
7. 2. Service Filtering	35

7.3.	Access Control	36
7.4.	IP & MAC Binding	38

Chapter 8. NAT Forwarding..... 40

8.1.	Translate Address and Port by ALG.....	41
8.2.	Share Local Resources over the Internet by Virtual Server.....	42
8.3.	Open Ports Dynamically by Port Triggering.....	43
8.4.	Make Applications Free from Port Restriction by DMZ.....	45

Chapter 9. Customize Your Network..... 46

9.1.	Check Network Map and Manage Your Satellites	47
9.1.1.	Check Internet Status	47
9.1.2.	Manage Your Satellites.....	48
9.1.3.	View Online Devices Information.....	50
9.2.	Set Up Parental Controls.....	51
9.3.	Specify Wireless Settings.....	53
9.3.1.	Change Wireless Settings	53
9.3.2.	Use WPS for Wireless Connection	55
9.3.3.	Create Multi-SSID Networks	56
9.4.	Change LAN Settings.....	57
9.4.1.	Change the LAN IP Address	57
9.4.2.	Use the Router as a DHCP Server	58
9.4.3.	Reserve LAN IP Addresses.....	59
9.5.	Configure IPv6 LAN Settings.....	60
9.5.1.	Configure the RADVD Address Type	60
9.5.2.	Configure the DHCPv6 Server Address Type.....	61
9.6.	Set Up a Dynamic DNS Service Account	62

Chapter 10.Manage Your Controller..... 64

10.1.	Set System Time	65
10.2.	Test the Network Connectivity	65
10.3.	Update the Firmware.....	66
10.4.	Back Up and Restore Configuration Settings	67
10.5.	Change the Login Password	68
10.6.	Local Management	69
10.7.	Remote Management.....	69
10.8.	System Log.....	71
10.9.	CWMP Settings.....	72
10.10.	Monitor the Internet Traffic Statistics.....	73

Chapter 11.FAQ..... 75

About This Guide

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

When using this guide, please note that features of your device 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 and so on.
>	The menu structures to show the path to load the corresponding page. For example, Settings > Wireless > Wireless Settings means the Wireless Settings page is under the Wireless menu that is located in the Settings 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 are available from the [Download Center](http://www.tp-link.com/support) at www.tp-link.com/support.

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

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 www.tp-link.com/support.

Chapter 1

Get to Know Your Devices

This chapter introduces what your devices can do and shows its appearance.

It contains the following sections:

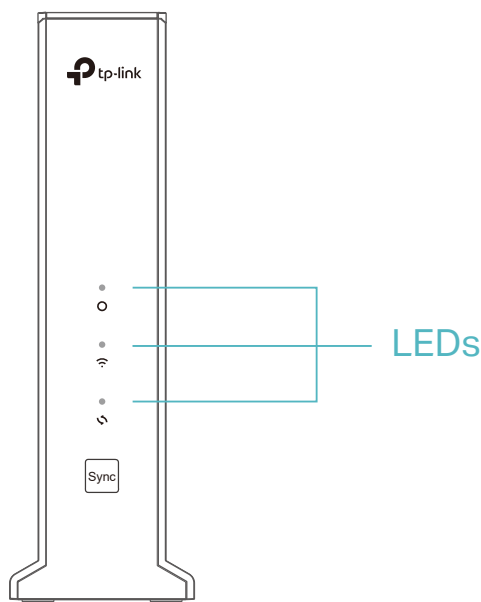
- [Product Overview](#)
- [Appearance](#)

1.1. Product Overview


TP-Link home Wi-Fi system uses multiple devices to provide a seamless, intelligent and easy-to-configure mesh network that covers the entire home. The system consists of three routers, one works as the Controller and the other two work as Satellite. The Controller connects to the modem or gateway, the Satellites extend the wireless coverage of your network.



1.2. Appearance

1.2.1. LEDs

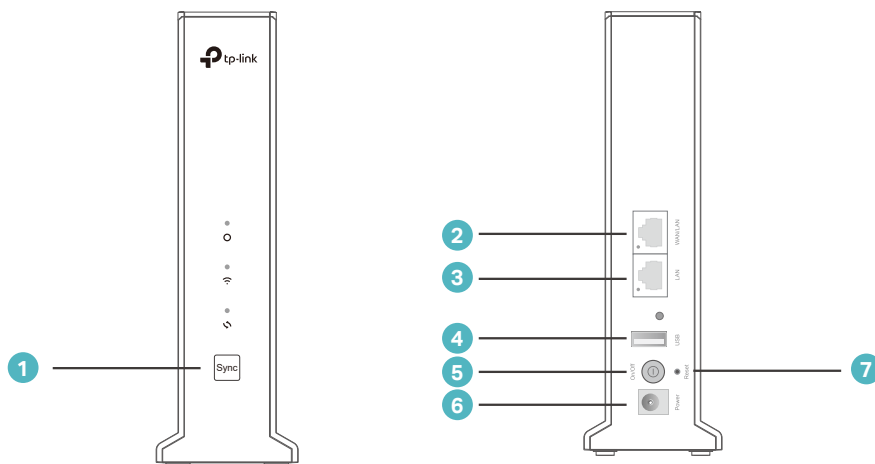



You can check the device's working status by following the LED Explanation table.

LED Explanation		
Name	Status	Indication
 (System Status)	Flashing Green	The device is starting or updating the firmware.
	Solid Green	The device is ready, and the internet is available.
	Solid Orange	The device is ready but the internet is unavailable.
	Off	Power is off.
	Solid Red	The firmware is corrupted.

LED Explanation		
Name	Status	Indication
 (Wireless)	Flashing Green	The wireless function is enabled, and the device is in the factory default state.
	Solid Green	For Controller, the wireless function is enabled. For Satellite, the wireless connection between Controller and Satellite is successful, and the signal is strong.
	Solid Orange	For Satellite, the wireless connection between Controller and Satellite is successful, but the signal is weak.
	Off	For Satellite, the wireless connection between Controller and Satellite failed.
 (Sync/WPS)	Flashing Green	A wireless device is trying to connect to the network via WPS. This process may take up to 2 minutes.
	Solid Green	A Satellite is trying to connect to the Controller via synchronization. This process may take up to 2 minutes. After successful connection, the LED will turn off. If the synchronization fails, the LED will flash for about 10 seconds and then turn off.
	Off	No WPS/Sync in process or WPS/Sync process has completed.

1.2.2. Buttons and Ports



Item	Description
1 Sync Button	For pairing the Controller and the Satellite and starting WPS process. Press the button to start a WPS process, press and hold the button for at least 5 seconds to start a synchronization process.
2 WAN/LAN Port	Combined with WAN/LAN interface capabilities, which can be used to connect the device to the internet or Ethernet network devices.
3 LAN Port	For connecting the your PC or other Ethernet network devices.
4 USB Port	For connecting to a USB storage device.
5 ON/OFF Button	The switch for the power. Press it to power on or off the device.  The diagram shows a power switch with two positions. The 'ON' position is indicated by a downward-pointing arrow above the switch, and the 'OFF' position is indicated by an upward-pointing arrow above the switch.
6 Power Port	For connecting the device to a power socket via the provided power adapter.
7 Reset Button	Press and hold the button for at least 5 seconds to reset the device into factory default settings.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- [Position the Devices](#)
- [Connect Your Controller](#)
- [Connect Your Satellites](#)

2.1. Position the Devices

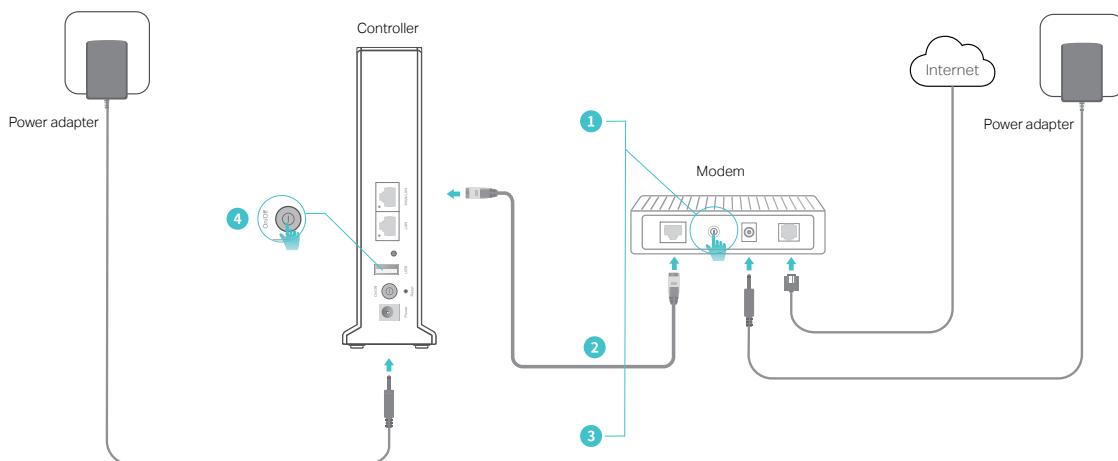
- The device should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the device in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create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

2.2. Connect Your Controller

You can set any one of the HC220-G1 routers as the Controller and the remaining two as Satellites.

Follow the steps below to connect your Controller.

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



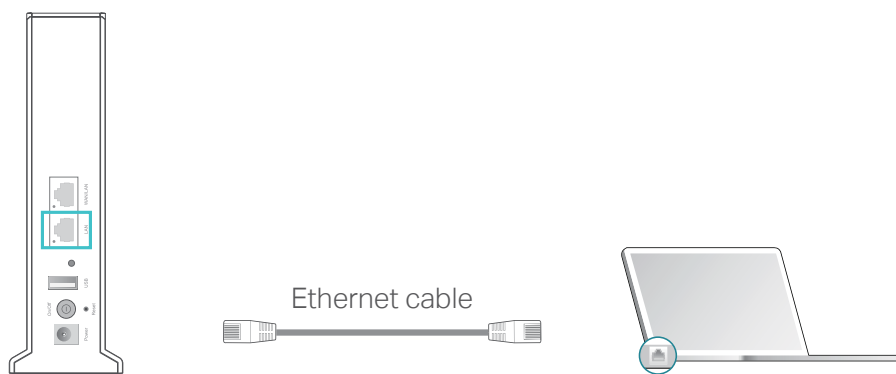
1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to the Controller's WAN/LAN port with an Ethernet cable.
3. Turn on the modem, and then wait about 2 minutes for it to restart.
4. Turn on the Controller.
5. Verify the System Status LED is solid green and the Wireless LED is flashing green.

- System Status LED is solid green and Wireless LED is flashing green.

6. Connect your computer to the Controller.

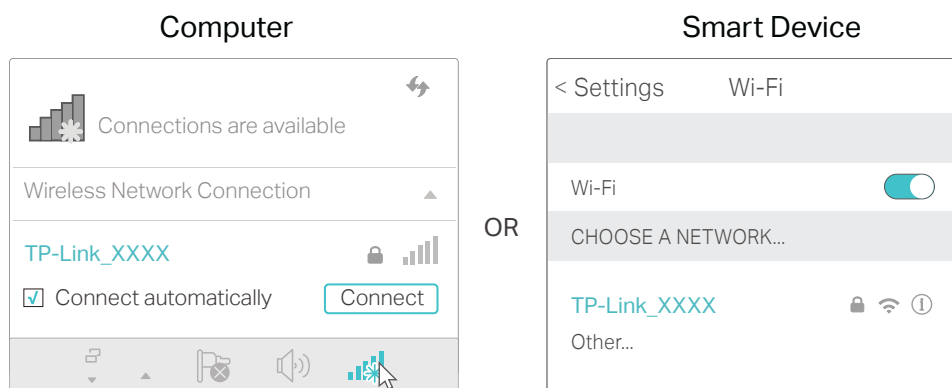
- **Method 1: Wired**

Turn off the Wi-Fi on your computer and connect the computer to the LAN port of the Controller using an Ethernet cable.



- **Method 2: Wireless**

- 1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the Controller.
- 2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.



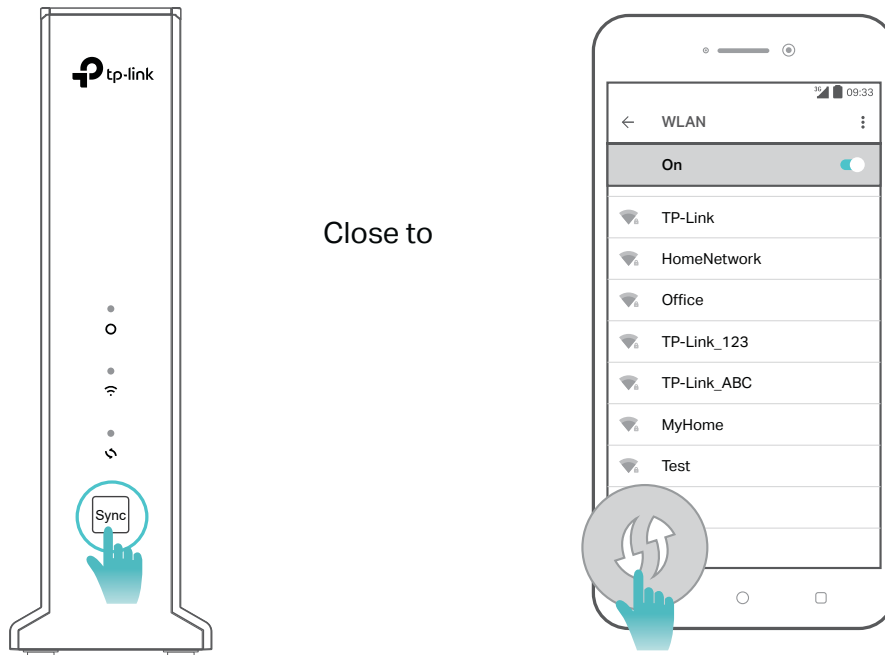
- **Method 3: Use the Sync button**

Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your Controller by this method.

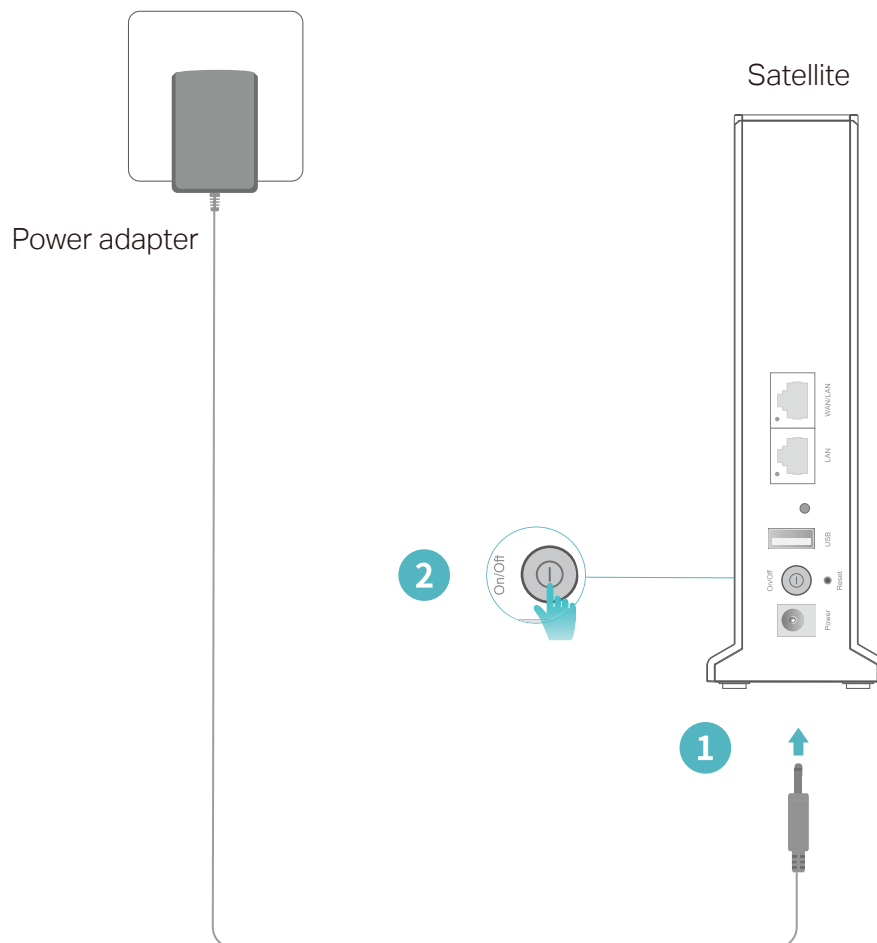
Note:

- WPS is not supported by iOS devices.
- The WPS function cannot be configured if the wireless function of the Controller 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) Tap the WPS icon on the device's screen. Here we take an Android phone as an example.
- 2) Immediately press the Sync button on your Controller.
- 3) The System Status LED will flash for about two minutes during the WPS process.



2.3. Connect Your Satellites



1. Connect your Satellites to the power sources with the provided power adapter.
2. Press the power ON/OFF button to turn on the satellite.
3. Verify that the System Status LED is solid green and the Wireless LED is flashing green.

● System Status LED is solid green and Wireless LED is flashing green.

Chapter 3

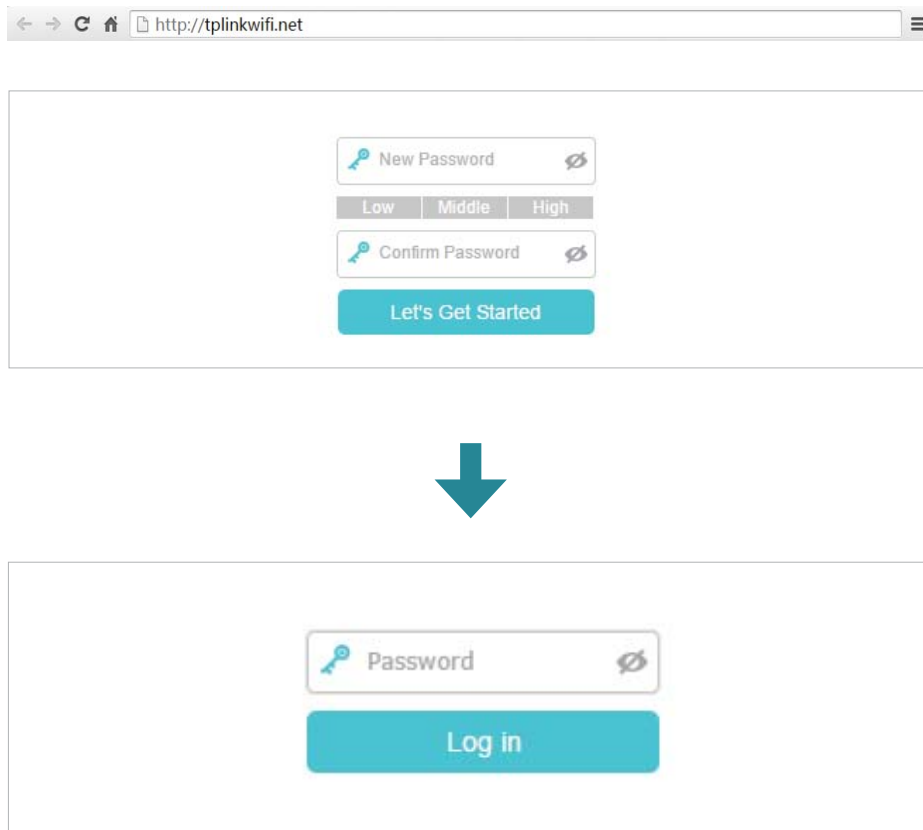
Log In to Your Controller

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

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

Follow the steps below to log in to your Controller.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Launch Enter <http://tplinkwifi.net> in the address bar of a web browser and create a login password for secure management and click [Save](#). Enter the password again on the login window and click [Log in](#) to log in to your Controller.



Note:

1. If the dialog boxes shown in the images above do not appear, it suggests that your IE Web-browser has been set to a proxy. You can go to [Tools > Internet Options > Connections > LAN Settings](#), and clear the [Using Proxy](#) checkbox, and click [OK](#).
2. If the login window does not appear, please refer to the [FAQ](#) section.

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your Controller to the internet. The Controller 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:

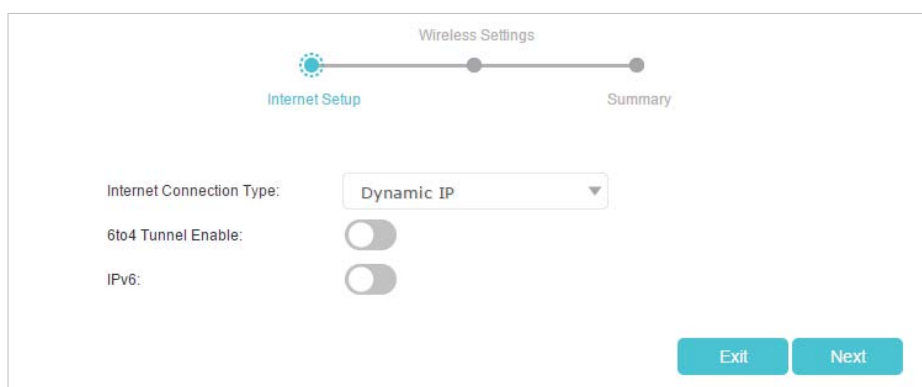
- [Use Quick Setup Wizard](#)
- [Set Up an IPv6 Internet Connection](#)
- [Configure the Controller in Access Point Mode](#)

4.1. Use Quick Setup Wizard

The Quick Setup wizard will guide you to set up your Controller.

You can refer to the instructions below to set up or modify the internet settings of your Controller.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Click **Quick Setup** on the top of the page and configure the basic internet connection, and then click **Next**.

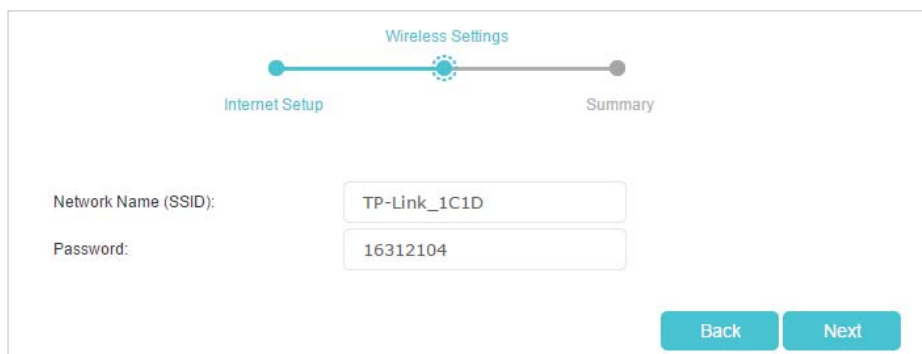


The screenshot shows the 'Internet Setup' step of the 'Wireless Settings' wizard. At the top, a progress bar indicates the current step. Below the progress bar, there are three configuration options: 'Internet Connection Type' with a dropdown menu set to 'Dynamic IP', '6to4 Tunnel Enable' with a disabled toggle switch, and 'IPv6' with a disabled toggle switch. At the bottom right, there are two buttons: 'Exit' and 'Next'.

- **Internet Connection Type:** Select your internet connection type and enter the corresponding information (if required) provided by your ISP. Three connection types are supported: **Dynamic IP**, **PPPoE** and **Static IP**.
- **6to4 Tunnel Enable:** Enable or disable the 6to4 tunnel function.
- **IPv6:** Enable IPv6 internet connection and set up the basic configuration, or disable the IPv6 connection. Refer to [Set Up an IPv6 Internet Connection](#) for advanced setup.

Note: 6to4 tunnel and IPv6 cannot be enabled at the same time.

3. Customize your wireless network name (SSID) and the password. You can keep the default settings or change them to a new one, both fields are case-sensitive, and then click **Next** to get a brief summary of your internet setup.



The screenshot shows the 'Wireless Settings' step of the 'Wireless Settings' wizard. At the top, a progress bar indicates the current step. Below the progress bar, there are two input fields: 'Network Name (SSID)' with the value 'TP-Link_1C1D' and 'Password' with the value '16312104'. At the bottom right, there are two buttons: 'Back' and 'Next'.

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 your network.

- Click **Finish** to complete the Quick Setup process. You can refer to [Test the Network Connectivity](#) to test your Internet connection

The screenshot shows the 'Wireless Settings' page with a progress bar at the top. The progress bar has three steps: 'Internet Setup' (current), 'Summary', and 'Summary'. Below the progress bar, the configuration is as follows:

Internet Connection Type:	Dynamic IP
6to4:	Disable
IPv6:	Disable
Network Name (SSID):	TP-Link_1C1D
Password:	16312104

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

4.2. 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, you can run the Quick Setup to enable [6to4 Tunnel](#) for permitting IPv6 connection.

Follow the steps below to set up an IPv6 connection:

- Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
- Go to [Settings](#) > [Advanced Settings](#) > [Internet](#).

The screenshot shows the 'Internet Setup' page with a table of WAN interfaces. The table has the following columns: WAN Interface Name, VLAN ID, Status, Operation, and Modify. The table is currently empty, showing dashes in all cells. Above the table, there are buttons for 'Refresh', '+ Add', and '- Delete All'.

WAN Interface Name	VLAN ID	Status	Operation	Modify
--	--	--	--	--

- Select your WAN Interface Name (**Status** should be **Connected**) and click the (Edit) icon.
- Scroll down the page to enable **IPv6**, and configure the IPv6 parameters.

IPv6:	<input checked="" type="checkbox"/> Enable
Addressing Type:	AUTO
IPv6 Gateway:	ewan_pppoe

- **Addressing Type:** Consult your ISP for the addressing type (HCPv6 or SLAAC). SLAAC is the most commonly used addressing type.
- **IPv6 Gateway:** Keep the default setting.

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.

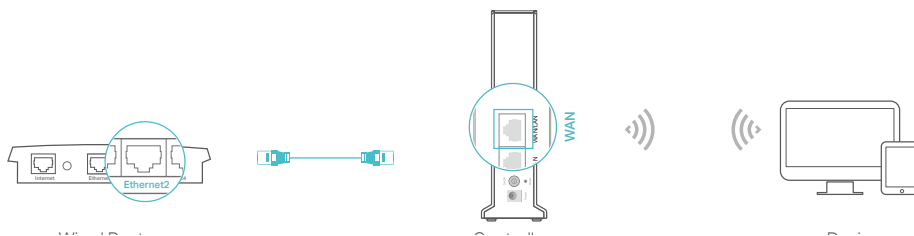
5. Click **OK** to make the settings effective. Now IPv6 service is available for your network

4.3. Configure the Controller in Access Point Mode

In Access Point mode, your Controller connects to a wired router via an Ethernet cable. Meanwhile the Controller and Satellites extend the wireless coverage of your existing network.

If you already have a wired router, you can use this mode.

To switch to Access Point Mode:



1. Connect the Controller's WAN/LAN port to your wired router's Ethernet port via an Ethernet cable as shown above.
2. Connect a computer to the Controller via an Ethernet cable or wirelessly by using the SSID (network name) and password printed on the label at the bottom of the Controller.
3. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
4. Go to **Settings > Operation Mode**, select Access Point and click Save. Log in to the router via <http://tplinkwifi.net> after the router reboots.
5. Go to **Quick Setup** or **Settings > Wireless > Wi-Fi Network** and set the SSID and password for the wireless network.

Now, you can connect to the SSID and enjoy your existing network.

Tips: In AP mode, functions like NAT, Parental Controls and QoS are not supported..

Chapter 5

Add Satellites to Your Network

This chapter describes how you can add the satellites to your network and extend the wireless coverage.

This chapter contains the following sections:

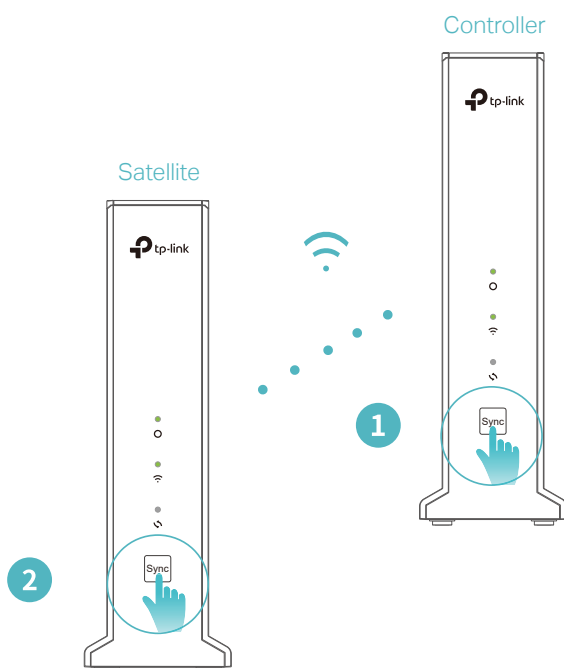
- [Sync Your Satellites](#)
- [Place Your Satellites](#)

5.1. Sync Your Satellites

The Wi-Fi System includes three routers, one works as the Controller and the others work as the Satellites. The Sync process is triggered by the Sync button, and the Satellites will automatically copy the settings of your Controller after successful sync.

Follow the steps below to sync the Satellites:

1. Place the Satellite close to the Controller.
2. Power on the Satellites and wait about two minutes for it to get ready.
 - System Status LED is solid green.
 - Wireless LED is flashing green.
3. Press and hold the Sync button on the Controller for about 5 seconds until its Sync LED turns solid green and within one minute, press and hold the Sync button on the Satellite for about 5 seconds until its Sync LED turns solid Green.



The Sync LEDs of the Controller and the Satellite light green and turn off about two minutes later. The Wireless LEDs of the Controller and the Satellite should be solid green after successful synchronization.

4. Repeat step 1-3 to sync another Satellite.

📌 Tips:

1. You can check the sync status on the web management page by visiting <http://tplinkwifi.net>, going to **Settings > Network Map** and clicking the **HC220-G1** icon.



2. For more information on the management of your Satellites, please refer to [Manage Your Satellites](#).

5.2. Place Your Satellites

After the Sync processes are complete, you may need to move your Satellites to appropriate places to extend the wireless signal coverage. The specific locations depend on the architectural style and layout of your house, please note that the Wi-Fi signal of one Satellite at least must be within the range of your Controller's Wi-Fi signal in order to sync with the Controller.

You can use the Satellites' wireless LEDs to help you to determine where to place them.

Examples of Typical Placement

- For multi-story house



- For ranch-style house



- For apartment



🔗 Tips:

- After the placement, if the Wireless status LED of Satellite is orange or red, please move it closer to the Controller, you can check the connection status and wireless signal status on the web management page by visiting <http://tplinkwifi.net>, going to **Settings > Network Map** and clicking the **HC220-G1** icon.

Chapter 6

USB Settings

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

You can also learn how to get wireless internet access through 3G/4G mobile network.

The router supports USB external flash drives and hard drives.

It contains the following sections:

- [Access the USB Storage Device](#)
- [Media Sharing](#)
- [3G/4G Settings](#)

6. 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:

1. If you use USB hubs, make sure no more than 4 devices are connected to the router.
2. If the USB storage device requires using bundled external power, make sure the external power has been connected.
3. If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
4. 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](#).

6. 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.

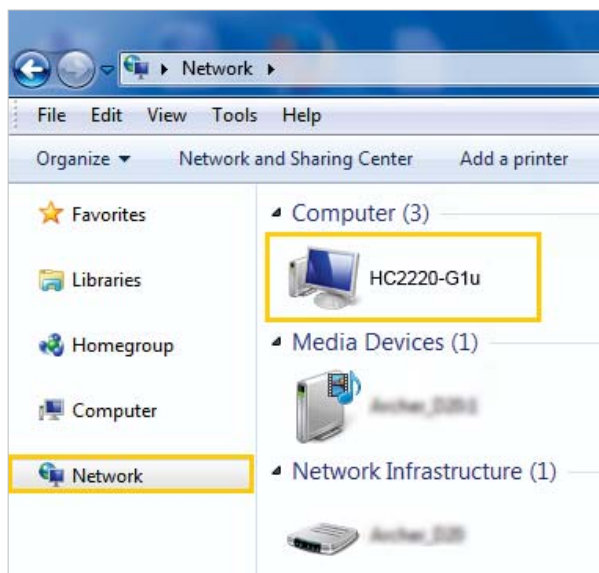
Windows Computer

➤ Method 1:

Go to [Computer > Network](#), then click the Network Server Name ([model number](#) by default) in the [Computer](#) section.

📌 Note:

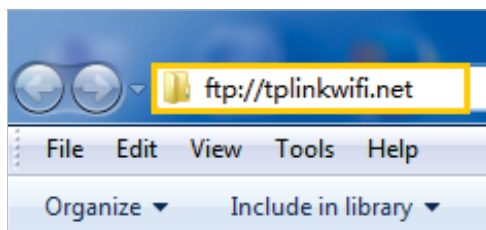
Operations in different systems are similar. Here we take Windows 7 as an example.



Windows
Computer

➤ Method 2:

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



Mac

- 1) Select [Go](#) > [Connect to Server](#).
- 2) Type the server address `smb://tplinkwifi.net`.
- 3) Click [Connect](#).



- 4) When prompted, select the [Guest](#) radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the [Registered User](#) radio box. To learn how to set up an account for the access, refer 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.

6.1.2. 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.

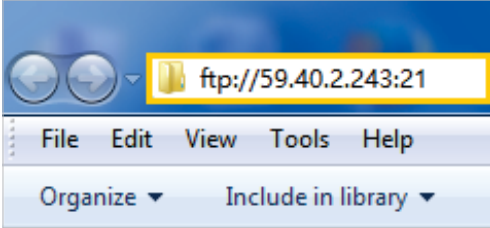
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > USB Sharing > USB Storage Device**, and locate the **Sharing Settings** section.
3. Select the **FTP (via Internet)** check box, and then click **Save**.

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Access Address	Port
<input checked="" type="checkbox"/>	Media Server	--	--
<input checked="" type="checkbox"/>	Network Neighborhood	\\Archer_C5	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.0.1:21	<input type="text" value="21"/>
<input checked="" type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21

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

Computer	<p>1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser.</p> <p>2) Type the server address in the address bar:</p> <p>Type in <code>ftp://<WAN IP address of the router>:<port number></code> (such as <code>ftp://59.40.2.243:21</code>). If you have specified the domain name of the router, you can also type in <code>ftp://<domain name>:<port number></code> (such as <code>ftp://MyDomainName:21</code>)</p> <div data-bbox="644 629 1136 855" style="text-align: center;">  </div> <p>3) Press Enter on the keyboard.</p> <p>4) Access with the username and password you set in To Set Up Authentication for Data Security.</p> <p>Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.</p>
	Smart Device

Tips:

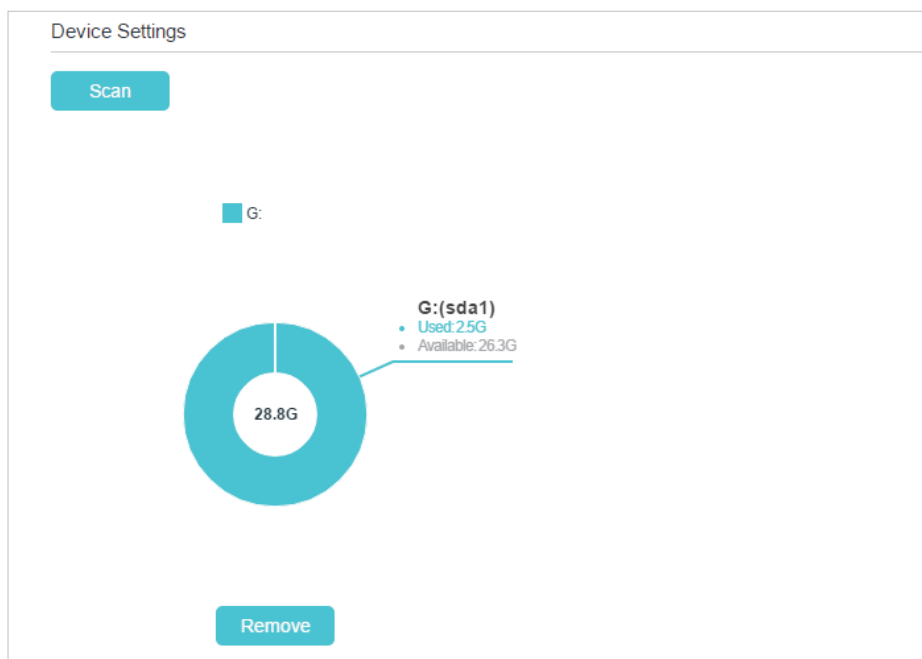
Refer to [Set Up a Dynamic DNS Service Account](#) to learn how to set up a domain name for you router.

6.1.3. View USB Storage Device

The router contains one USB port, you can use it to connect a USB storage device such as a flash drive or hard drive.

➤ **To view USB Storage Device Status**

1. Visit <http://tplinkwifi.net>, then log in with the password you set for the router.
2. Go to [Advanced > USB Sharing > USB Storage Device](#) or [Basic > USB Sharing > USB Storage Device](#) page.



- **Scan:** Usually, the router will automatically detect any newly inserted USB device. If you find that your USB device is not displayed in the **Device Settings** section, you can click **Scan** to refresh the web page with the updated information.
- **Remove:** Click this button to safely take the USB device offline before you remove the USB device physically.
- **Doughnut Chart:** Display the basic information of the USB storage device, including the total space and available space when the pointer is over the chart.
You can click the doughnut chart to hide the USB device from access, which will turn the chart into a gray one.

6.1.4. 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. In the **Sharing Settings** section, make sure **Network Neighborhood** is selected, and enter a Network/Media Server Name as you like, such as **MyShare**, then click **Save**.

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Access Address	Port
<input checked="" type="checkbox"/>	Media Server	--	--
<input checked="" type="checkbox"/>	Network Neighborhood	\\MyShare	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.0.1:21	<input type="text" value="21"/>
<input checked="" type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21

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

➤ **To Only Share Specific Content**

- Focus on the **Folder Sharing** section. Turn off **Share All**, then click **Add** to add a new sharing folder.

Folder Sharing

Share All:

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--	--

Volume Name:

Folder Path:

Folder Name:

Enable Authentication

Enable Write Access

Enable Media Sharing


- Select the **Volume Name** and **Folder Path**, then enter a **Folder Name** as you like.
- Decide the way you share the folder:
 - Enable Authentication:** By default, authentication is disabled for the folder sharing, if you select this check box, 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 select this check box, network clients can modify this folder.
- **Enable Media Sharing:** Select this check box 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. Refer to [3G/4G Settings](#) to learn more.

4. Click **Save** to make the settings effective.




 **Tips:**

The router can share 8 folders at most. You can click  on the page to detach the corresponding folder you do not want to share.

Folder Sharing

Share All:

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

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
<input type="checkbox"/>	1	HelloWorld	G:/Hello World	Off	sda1		 

➤ **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 the username and password when accessing the USB disk.

1. In the **Sharing Account** section, choose **Use Default Account** or **Use New Account**. The user name is **admin** and the password is the login password for the default account. If you choose **Use New Account**, you can create a new username and 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:

Password: (Same as Login Password)

Save

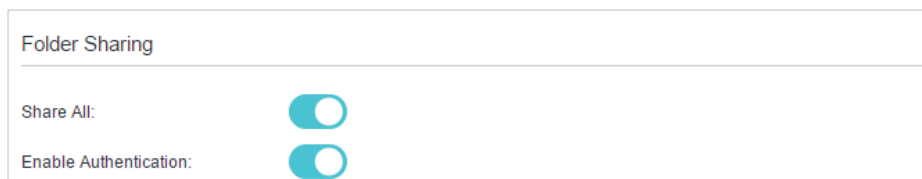
 **Note:**

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 system will automatically use its account information for USB access.
- If the sharing password is different from the Windows password, the Windows system 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, turning on **Enable Authentication** will enable authentication for all folders.

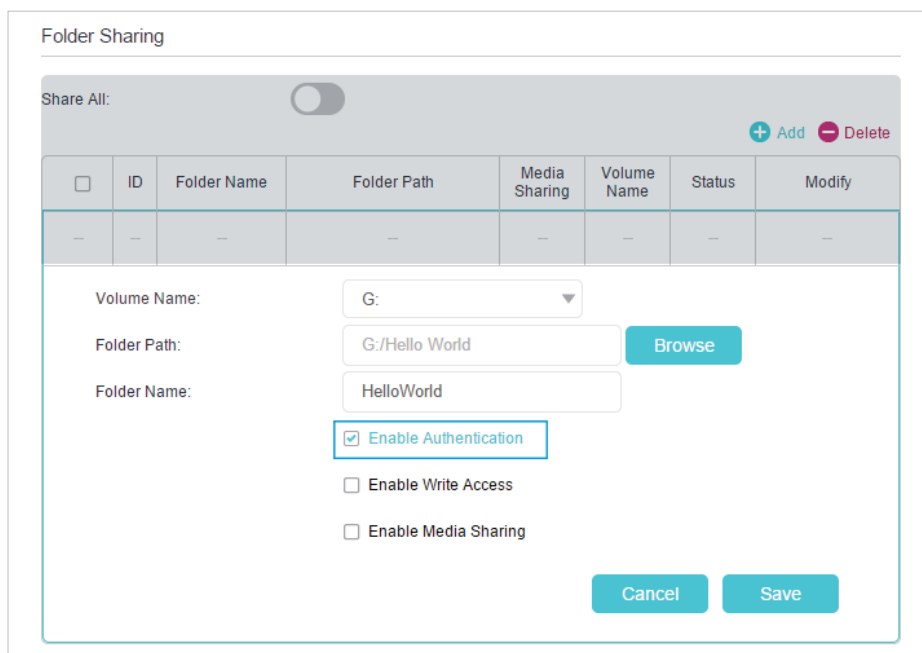


Folder Sharing

Share All:

Enable Authentication:

- If **Share All** is disabled, you can select **Enable Authentication** to apply authentication to specific folders.



Folder Sharing

Share All:

+ Add - Delete

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
-	-	-	-	-	-	-	-

Volume Name: G:

Folder Path: G:/Hello World

Folder Name: HelloWorld

Enable Authentication

Enable Write Access

Enable Media Sharing

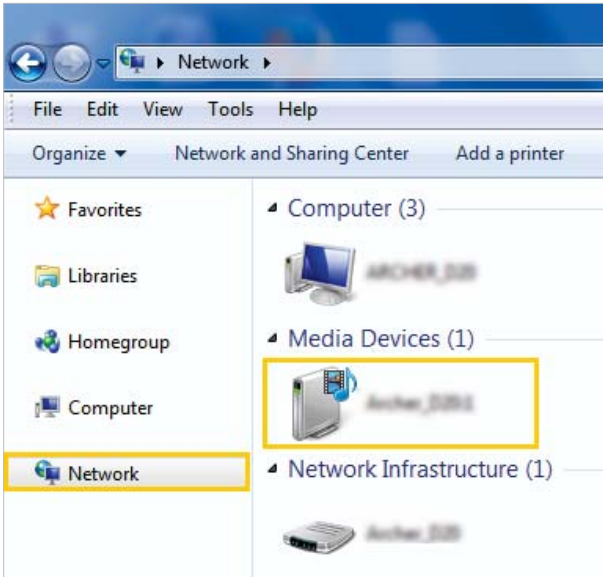
Note:

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](#).

6.2. 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 inserted into the router, your DLNA-supported 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	<ul style="list-style-type: none">• Go to Computer > Network, then click the Media Server Name (model number by default) in the Media Devices section. <p>Note: Here we take Windows 7 as an example.</p>  <p>The screenshot shows a Windows 7 Network folder window. The address bar shows 'Network'. The left sidebar has 'Network' selected. The main pane shows a tree view with 'Computer (3)', 'Media Devices (1)', and 'Network Infrastructure (1)'. Under 'Media Devices (1)', a device icon is highlighted with a yellow box.</p>
Smart Device	<ul style="list-style-type: none">• Use a third-party DLNA-supported player.

Chapter 7

Network Security

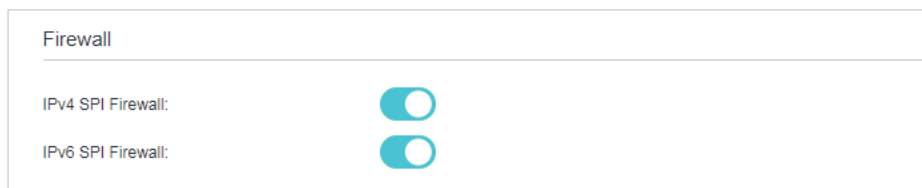
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent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

- [Firewall & DoS Protection](#)
- [Service Filtering](#)
- [Access Control](#)
- [IP & MAC Binding](#)

7. 1. Firewall & DoS Protection

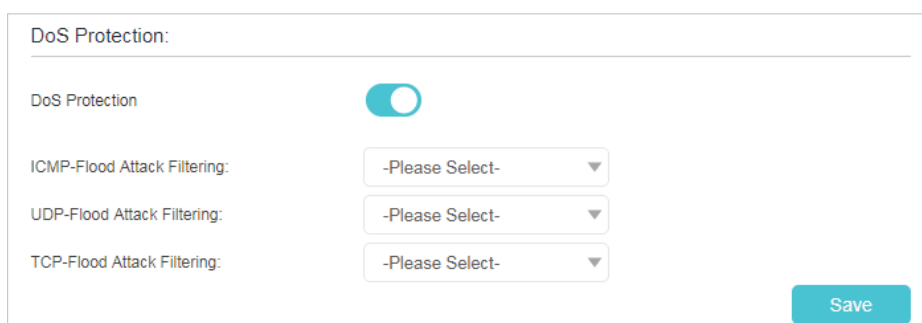
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

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 is 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 Controller.
2. Go to **Settings > Security > Firewall & DoS Protection**.



3. Enable **DoS Protection**.
4. Set the protection level (**Low**, **Middle** or **High**) for **ICMP-Flood Attack Filtering**, **UDP-Flood Attack Filtering** and **TCP-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-Flood Attack Filtering** - Enable to prevent the TCP (Transmission Control Protocol) flood attack.
5. Click **Save** to make the settings effective.

 **Tips:**

1. The level of protection is based on the number of traffic packets. You can specify the level under **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

Save

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 Refresh Delete

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

7.2. Service Filtering

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

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

Service Filtering

Service Filtering:

4. Click [Add](#).

Filtering List

<input type="checkbox"/>	ID	Service Type	Port	IP Address	Status	Modify
--	--	--	--	--	--	--

Service Type:
 Protocol:
 Starting Port:
 Ending Port:
 Service Type:
 Filter Service For: Single IP Address IP Address Range All IP Addresses

Cancel OK

5. Select a **Service Type** from the drop-down list and the following four boxes will be automatically filled in. 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 **OK** to make the settings effective.

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

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 Controller.
2. Go to **Settings > Security > Access Control** and enable **Access Control**.

Access Control

Access Control:

Access Mode

Access Mode: Blacklist Whitelist

[Save](#)

Devices in Blacklist

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

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

Online Devices

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

<input type="checkbox"/>	ID	Device Name	IP Address	MAC Address	Connection Type
<input type="checkbox"/>	1	DESKTOP-868P7E	192.168.23.103	8C 8C 4B 1D E8 A6	Wired
<input type="checkbox"/>	3	Unknown	192.168.23.102	34 E8 84 11 1C 8D	Wireless
<input type="checkbox"/>	4	Unknown	192.168.23.101	34 E8 84 11 1E 81	Wired

3. Select the access mode to either block (recommended) or allow the device(s) in the list.

To block specific device(s)

- 1) Select [Blacklist](#) and click [Save](#).
- 2) Select the device(s) to be blocked in the [Online Devices](#) table (or click the [Add](#) under the [Devices in Blacklist](#) and enter the [Device Name](#) and [MAC Address](#) manually).
- 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](#).

The screenshot shows a web interface titled "Devices in Whitelist". At the top right, there are buttons for "+ Add" and "- Delete". Below this is a table with the following structure:

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

Below the table, there are two input fields:

Device Name:

MAC Address:

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

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

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 a network device's IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with a matching IP address in the Binding list, but an 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 Controller.
2. Go to **Settings > Security > IP & MAC Binding** and enable **IP & MAC Binding**.

IP & MAC Binding

IP & MAC Binding:

Binding List + Add - Delete

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

ARP List Refresh Bind

<input type="checkbox"/>	ID	Device Name	MAC Address	IP Address	Bound	Modify
<input type="checkbox"/>	1	Unknown	34 E8 94 11 1C 8D	192.168.23.102	Unloaded	
<input type="checkbox"/>	2	Unknown	34 E8 94 11 1E 91	192.168.23.101	Unloaded	
<input type="checkbox"/>	3	DESKTOP-G0P7E1	8C EC 4E 1D E3 A8	192.168.23.103	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 + Add - Delete

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

MAC Address:

IP Address:

Enable This Entry

- 2) Enter the [MAC address](#) and [IP address](#) that you want to bind.
- 3) Select the [Enable This Entry](#) check box to enable the entry and click [Save](#).

Done!

Enjoy the internet without worrying about ARP spoofing and ARP attacks.

Chapter 8

NAT Forwarding

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

The router can use a forwarding feature to remove the isolation of NAT and allow external internet hosts to initiatively communicate with the devices in the local network, thus enabling some special features.

TP-Link router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPNP and DMZ.

This chapter contains the following sections:

- [Translate Address and Port by ALG](#)
- [Share Local Resources over the Internet by Virtual Server](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)

8. 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 etc. Enabling ALG is recommended.

Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller. Go to **Advanced > NAT Forwarding > ALG**.

ALG	
PPTP Pass-through:	<input checked="" type="checkbox"/> Enable
L2TP Pass-through:	<input checked="" type="checkbox"/> Enable
IPSec Pass-through:	<input checked="" type="checkbox"/> Enable
FTP ALG:	<input checked="" type="checkbox"/> Enable
TFTP ALG:	<input checked="" type="checkbox"/> Enable
H323 ALG:	<input checked="" type="checkbox"/> Enable
SIP ALG:	<input checked="" type="checkbox"/> Enable

Save

- **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.

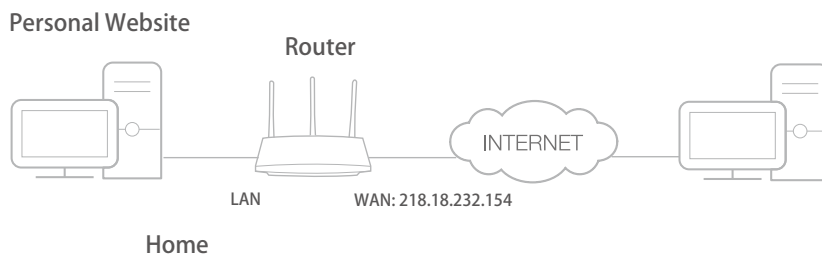
8.2. Share Local Resources over the Internet by Virtual Server

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

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

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

For example, the personal website has been built on my home PC (192.168.23.100). I hope that my friends can visit my website. 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 192.168.23.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
3. Go to **Settings > NAT Forwarding > Virtual Servers**, click **Add**.

Virtual Servers

+ Add - Delete

<input type="checkbox"/>	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:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP:

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

Protocol:

Enable This Entry

[Cancel](#) [OK](#)

4. Click [View Existing Applications](#), and choose HTTP. The external port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.23.100 in the [Internal IP](#) field.
5. Click [Save](#) to save the settings.

[Tips:](#)

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

Done!

Internet users can enter [http://WAN IP](#) (in this example: [http://218.18.232.154](#)) to visit your personal website.

[Tips:](#)

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

8.3. Open Ports Dynamically by Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP

address of the host. When the data from the internet returns to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs and video players. Common applications include MSN Gaming Zone, Dialpad, Quick Time 4 players, and so on.

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 [Settings > NAT Forwarding > Port Triggering](#) and click [Add](#).

Port Triggering

+ Add - Delete

<input type="checkbox"/>	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name: ewan_ipoe_d

Application: MSN Gaming Zone [View Existing Applications](#)

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

Cancel OK

3. Click [View Existing Applications](#), and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled in. Here we take [MSN Gaming Zone](#) as an example.
4. Click [Save](#) to save the settings.

Tips:

1. You can add multiple port triggering rules according to your network needs.
2. If the application you need is not listed in the existing applications list, you can 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 suggested.

8.4. Make Applications Free from Port Restriction by DMZ

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

Note:

DMZ is most applicable when you don't know which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

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

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.23.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
3. Go to **Settings > NAT Forwarding > DMZ** and select the **Enable** checkbox to enable DMZ.



4. Enter the IP address 192.168.23.100 in the **DMZ Host IP Address** field.
5. Click **Save** to save the settings.

Done!

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

Chapter 9

Customize Your Network

This chapter introduces how to view or change the settings of your network using the web management page.

It contains the following sections:

- [Check Network Map and Manage Your Satellites](#)
- [Set Up Parental Controls](#)
- [Specify Wireless Settings](#)
- [Change LAN Settings](#)
- [Configure IPv6 LAN Settings](#)
- [Set Up a Dynamic DNS Service Account](#)

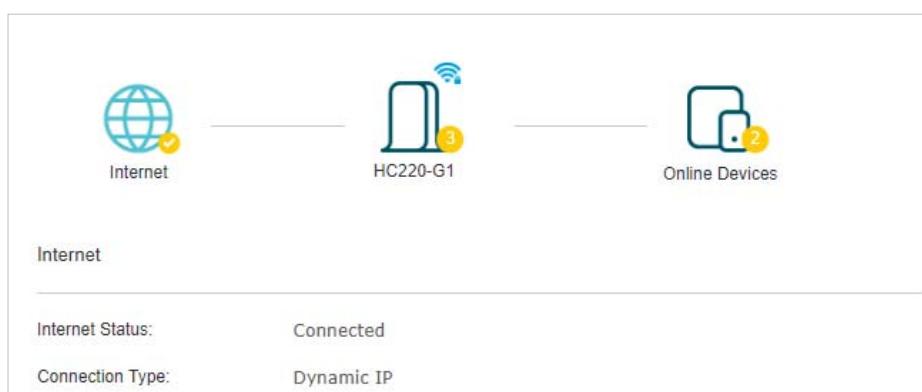
9. 1. Check Network Map and Manage Your Satellites

With the network map, you can check whether you have successfully set up your internet connection, manage your Satellites and view the information of connected devices.

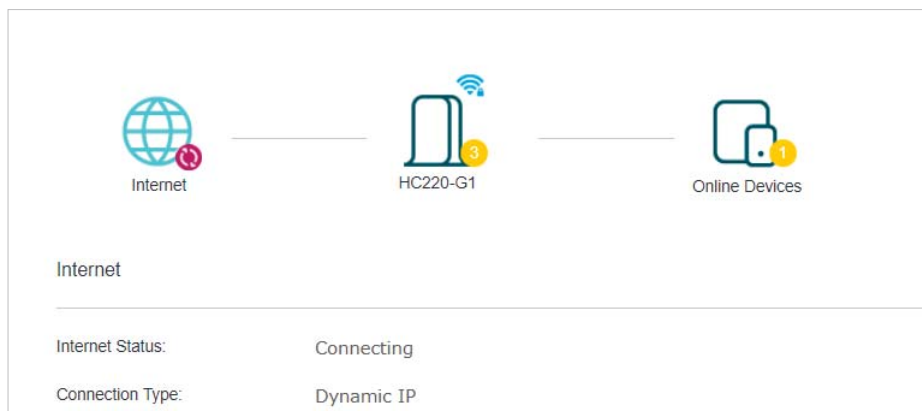
9. 1. 1. Check Internet Status

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Network Map**.

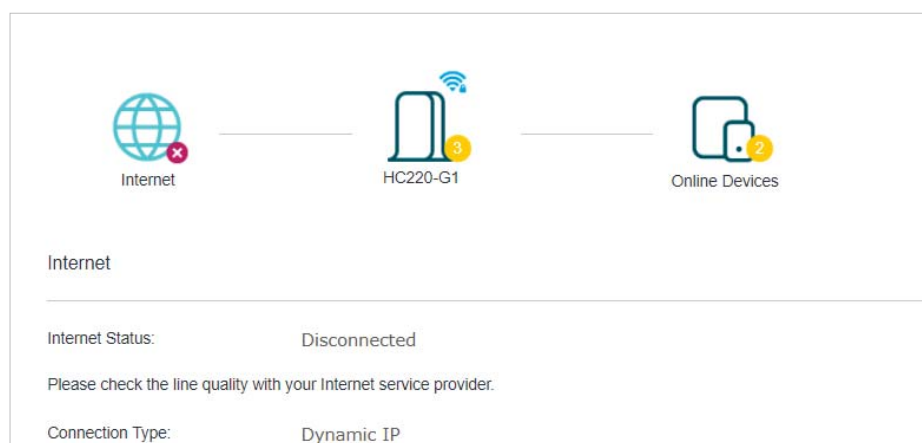
- Your Controller is connected to the internet.



- Your Controller is trying to connect to the internet, please wait a few seconds for the connection is complete.



- Your Controller has failed to connect to the internet. Please make sure internet connection type is set correctly, If the problem persists, please refer to [FAQ](#).



9.1.2. Manage Your Satellites

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Network Map** and click the **HC220-G1** icon.

You can view the connection status between your Controller and Satellites and the specific information, including device name (editable), assigned IP address, MAC address and status.

In the device table, the first row shows the information of Controller and the status of Controller shows the Internet connection status. The other rows show the information of Satellites, the status of Satellite shows the connection status between Controller and Satellite.

Device Number	Device Name	IP Address	MAC Address	Status	
1	HC220-G1	192.168.23.1	34:E8:94:11:1C:1D	Connected	
2	HC220-G1	192.168.23.103	34:E8:94:11:1C:6D	2.4G : Poor 5G : Poor	
3	HC220-G1	192.168.23.102	34:E8:94:11:1B:91	2.4G : Middle 5G : Good	

➤ **To change the name of the Controller or the Satellites.**

- 1) Locate the **Device Name** column and enter the new name(s).
- 2) Click **Save** to make the settings effective.

For example, you can change the device names according to their location.

Device Number	Device Name	IP Address	MAC Address	Status	
1	For Family Room	192.168.23.1	34:E8:94:11:1C:1D	Connected	
2	For Study	192.168.23.103	34:E8:94:11:1C:6D	2.4G : Poor 5G : Poor	
3	For Living Room	192.168.23.102	34:E8:94:11:1B:91	2.4G : Middle 5G : Good	

➤ **To remove a Satellite from your Wi-Fi System**

- 1) Click the Delete icon in the row of the Satellite you want to remove
- 2) Click **Yes** in the confirmation message box.




3) Reset the removed Satellite to its factory default settings in preparation for your intended use.

🔗 Tips: If you want to add the removed Satellite back to the Wi-Fi system, refer to [Add Satellites to Your Network](#).


9.1.3. View Online Devices Information

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to [Settings > Network Map](#) and click the [Online Devices](#) icon.


You can the detailed information of all clients connected to the Controller and the Satellites, including the device name, the connection types as well as the traffic statistics.



Internet




HC220-G1



Online Devices

For Family Room

ID	Name	IP Address	MAC Address	Connection Type	Signal Strength	Traffic Statistics
1	DESKTOP-G07F81	192.168.23.100	9C EC A6 1D 89 A8	Wired	--	--
2	HUAWEI_M000_10_P00-6-40132	192.168.24.100	84 CD 27 9E 1C C3	Wireless		TX: 585 Mbps RX: 585 Mbps

For Study

ID	Name	IP Address	MAC Address	Connection Type	Signal Strength	Traffic Statistics
--	--	--	--	--	--	--

For Living Room

ID	Name	IP Address	MAC Address	Connection Type	Signal Strength	Traffic Statistics
--	--	--	--	--	--	--

9.2. Set Up Parental Controls

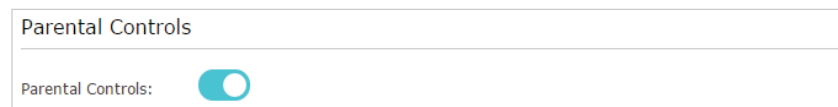
Parental controls allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

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

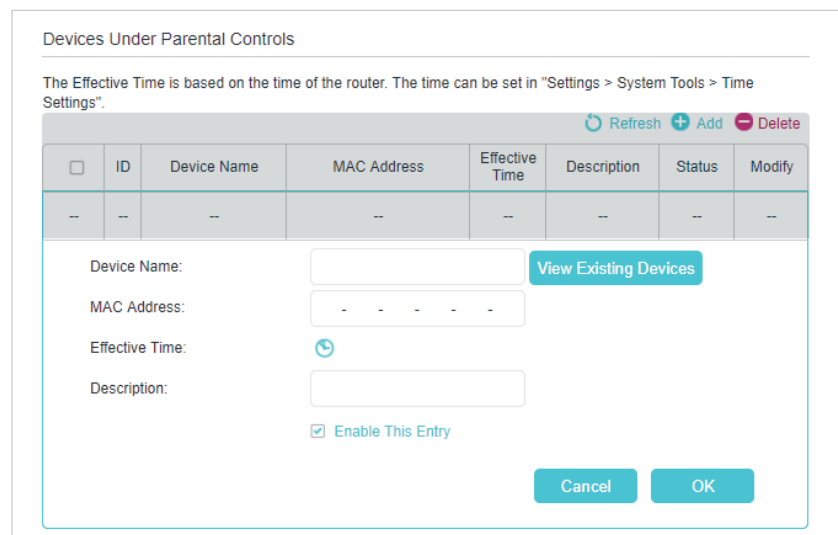
For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6 PM) to 22:00 (10 PM) on the weekdays and not other time.

How can I do that?

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



3. Click **Add**, and then click **View Existing Devices** and select the connected devices. Or, input the **Device Name** and **MAC Address** manually.



4. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click **OK**.

System Time: 01/01/2016 01:12:39

	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		Effective Time	Effective Time	Effective Time	Effective Time	Effective Time	
19:00		Effective Time	Effective Time	Effective Time	Effective Time	Effective Time	
20:00		Effective Time	Effective Time	Effective Time	Effective Time	Effective Time	
21:00		Effective Time	Effective Time	Effective Time	Effective Time	Effective Time	
22:00		Effective Time	Effective Time	Effective Time	Effective Time	Effective Time	
23:00							
24:00							

Effective Time

Reset OK

5. Enter a **Description** for the entry, select the **Enable This Entry** checkbox, and then click **OK**.
6. Enable **Content Restriction**, and select **Whitelist** as the restriction policy.

Content Restriction

Content Restriction:

Restriction Policy: Blacklist Whitelist

+ Add a New Keyword

Save

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** and enter "www.tp-link.com" and "Wikipedia.org" as the keywords and click **Save**.

Content Restriction

Content Restriction:

Restriction Policy: Blacklist Whitelist

+ Add a New Keyword

WWW.tp-link.com - wikipedia.org -

Save

8. You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries for your reference.

- **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.

Done!

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

9.3. Specify Wireless Settings

9.3.1. Change Wireless Settings

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Wireless > Wi-Fi Network**.

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

Turn on the **Wireless Radio** to enable the wireless network. If you don't want to use the wireless function, just turn off this option. And then click **Save** to make the settings effective.

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

Enter a new SSID (32 characters at most) and password and click **Save**. The SSID and password are 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 reference.

➤ **To change the security option:**

1. Go to [Settings](#) > [Wireless](#) > [Wi-Fi Network](#).
2. Select a security option and security version and encryption type. [WPA/WPA2 Personal](#) is recommended, WPA2 uses the newest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.

➤ **To change the mode or channel:**

1. Go to [Settings](#) > [Wireless](#) > [Wireless Settings](#).
2. Select the wireless network [2.4GHz](#) or [5GHz](#).
3. Select mode and channel and the related options.

Wireless Settings 2.4GHz | 5GHz

Mode:

Channel:

Channel Width:

Transmit Power: Low Middle High

[Save](#)

Mode: Select the desired transmission mode.

- **802.11n only:** Select only if all of your wireless clients are 802.11n devices.
- **802.11g/n mixed:** Select if you are using both 802.11g and 802.11n wireless clients.
- **802.11b/g/n 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 Controller. It is strongly recommended that you select 802.11b/g/n mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Controller.

- **802.11ac only (5GHz):** Select if all of your wireless clients are 802.11ac devices
- **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.

Transmit Power: Select **Low**, **Middle**, or **High** to specify the data transmit power. The default and recommended setting is **High**.

9.3.2. Use WPS for Wireless Connection

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

Method 1: Use the WPS button

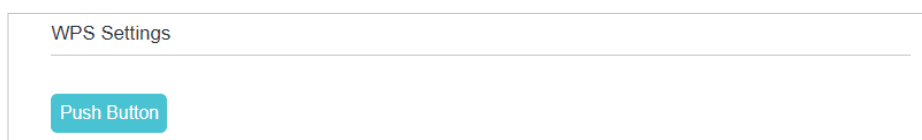
Use this method if your client device has a WPS button.

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

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 password you set for the Controller.
2. Go to **Settings > Wireless > WPS**.

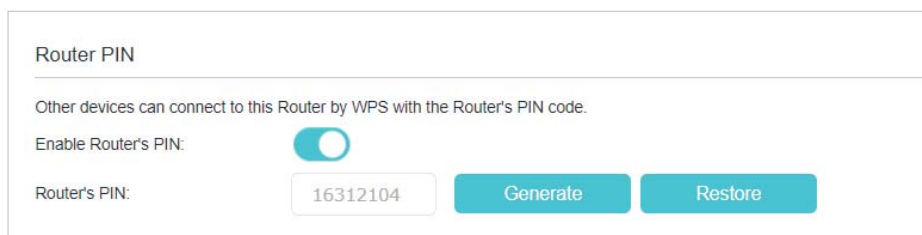


3. Click **Push Button**.
4. Press the WPS button of the client device directly.
5. The Sync LED of the Controller flashes for about 2 minutes during the WPS process.
6. When the Sync LED is on, the client device has successfully connected to the router.

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 password you set for the Controller.
2. Go to **Settings > Wireless > WPS**.



Router PIN

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

Enable Router's PIN:

Router's PIN: 16312104 Generate Restore

3. Take a note of the current **Router's PIN**. You can also click the **Generate** button to get a new PIN.
4. Enter the PIN on the client device. (The default PIN is also printed on the label of the Controller.)
5. The Sync LED flashes for about 2 minutes during the WPS process.
6. When the Sync 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 router is disabled. Please make sure the wireless function is enabled before configuring WPS.

9.3.3. Create Multi-SSID Networks

Your Controller supports additional up to three multi-SSID wireless networks for client access. You can specify the access and security options to ensure network security and privacy according to your situation.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Wireless > Multi-SSID**.
3. Select the **MSSID1 (2 or 3) Enable** check box to create the corresponding network.

Multi-SSID

MSSID1: Enable

Network Name (SSID): Hide SSID

Security: ▼

Version: Auto WPA2-PSK

Encryption: Auto AES

Password:

See each other: Allow guests to see each other

Access my local network: Allow guests to access to my local network

MSSID2: Enable

MSSID3: Enable

Save

4. Enter a new **Network Name (SSID)** or use the default name, this field is case sensitive. Don't select **Hide SSID** unless you want your guests to manually input the SSID for Wi-Fi access.
5. Select the **Security** option for the multi-SSID network, **WPA/WPA2 Personal (Recommended)** is recommended, and you can set a password for the network.
 - **See each other:** select the **Allow guests to see each other** check box if you want to allow the wireless clients on your multi-SSID network to communicate with each other via methods such as network neighbors and Ping.
 - **Access my local network:** select the **Allow guests to access my local network** check box if you want to allow the wireless clients on your multi-SSID network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.
6. Repeat Step 3 to 5 to set other two wireless networks if needed, and click **Save** to make the settings effective.

9.4. Change LAN Settings

9.4.1. Change the LAN IP Address

The Controller is preset with a default LAN IP 192.168.23.1, which you can use to log in to its web management page, and three guest LAN IP. 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 password you set for the Controller.
2. Go to [Settings > Advanced Settings > DHCP Server](#)
3. Select [IPv4](#) and click the edit icon in the [Modify](#) column.



The screenshot shows a configuration form for the DHCP Server. It includes the following fields and options:

- MAC Address: 34:E8:94:11:1C:1D
- IP Address: 192 . 168 . 23 . 1
- Subnet Mask: 255.255.255.0 (with a dropdown arrow)
- DHCP: Enable
- Radio buttons: DHCP Server and DHCP Relay

4. Enter a new [IP Address](#) appropriate to your needs.
5. Select the [Subnet Mask](#) from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
6. Keep the rest settings as default.
7. Click [OK](#) to make the settings effective.

9.4.2. Use the Router as a DHCP Server

You can configure your Controller to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the Controller, 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 password you set for the Controller.
2. Go to [Settings > Advanced Settings > DHCP Server](#).
3. Select [IPv4](#) and click the edit icon in the [Modify](#) column.

DHCP: Enable

DHCP Server DHCP Relay

IP Address Pool: 192 . 168 . 23 . 100 - 192 . 168 . 23 . 199

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

Default Gateway: 192 . 168 . 23 . 1 (Optional)

Default Domain: (Optional)

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

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

Cancel OK

4. Enable **DHCP** function and select **DHCP Server**.
5. 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 192.168.23.100 to 192.168.23.199 by default.
6. 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 Controller. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
7. Keep the rest settings as default and click **Save**.

Note:

1. The Controller 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 (192.168.23.50 to 192.168.23.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your situation on the **Settings > Advanced Settings > DHCP Server** page.

9.4.3. 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 Controller.

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Advanced Settings > DHCP Server** and select **IPv4**.

3. Scroll down to locate the **Address Reservation** table and click **Add** to add an address reservation entry for your device.

The screenshot displays the 'Address Reservation' configuration window. At the top, there are '+ Add' and '- Delete' buttons. Below is a table with the following structure:

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

Below the table, the configuration form includes:

- MAC Address: [- - - - -] [Scan]
- IP Address: [. . .]
- Group: [Default]
- Enable This Entry
- [Cancel] [OK]

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 Controller.
6. Select the **Enable This Entry** checkbox and click **OK** to make the settings effective.

9.5. Configure IPv6 LAN Settings

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

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

9.5.1. Configure the RADVD Address Type

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Advanced Settings > DHCP Server**.
3. Select **IPv6** to configure IPv6 LAN parameters.

DHCP Server IPv4 | IPv6

Group: Default

Address Type: RADVD DHCPv6 Server

RDDNS: Enable

Enable ULA Prefix: Enable

Site Prefix Type: Delegated Static

WAN Connection:

[Save](#)

- 4) 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.

- 5) 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.
 - 6) Keep **WAN Connection** as default.
4. Click **Save** to make the settings effective.

9.5.2. Configure the DHCPv6 Server Address Type

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > Advanced Settings > DHCP Server**.
3. Select **IPv6** to configure IPv6 LAN parameters.

DHCP Server IPv4 | IPv6

Group: Default

Address Type: RADVD DHCPv6 Server

Starting IPv6 Address: (1~FFFE)

Ending IPv6 Address: (1~FFFE)

Address Lease Time: seconds

Site Prefix Type: Delegated Static

WAN Connection:

- 1) Select the **DHCPv6 Server** address type to make the Controller assign IPv6 addresses to hosts.
 - 2) Specify the **Start/End IPv6 Address** for the IPv6 suffixes. The Controller will generate IPv6 addresses within the specified range.
 - 3) Keep **Address Lease Time** as default.
 - 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 setting.
4. Click **Save** to make the settings effective.

9.6. 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 192.168.1.x) to the router.

To set up DDNS, please follow the instructions below:


1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Settings > Advanced Settings > Dynamic DNS**.
3. Select the **Service Provider** (Dyndns or NO-IP).

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 log out first, and then log in with the new account.

Chapter 10

Manage Your Controller

This chapter introduces how to change the system settings and administrate your home network.

This chapter contains the following sections:

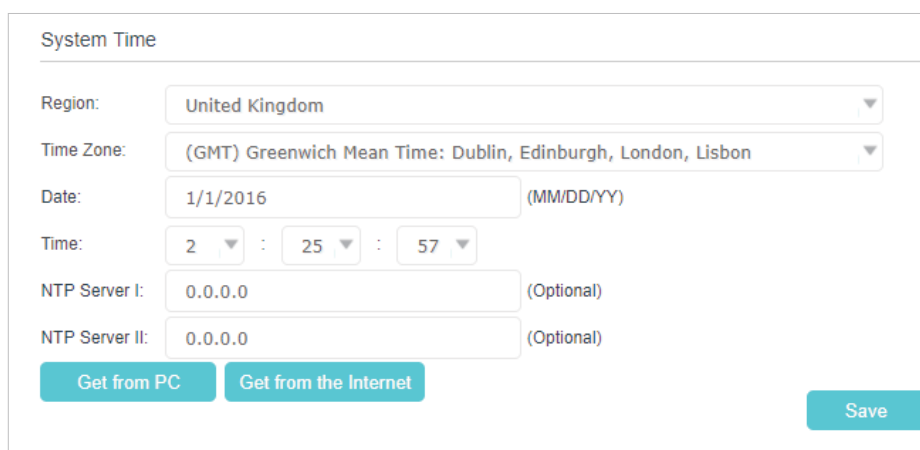
- [Set System Time](#)
- [Test the Network Connectivity](#)
- [Update the Firmware](#)
- [Back Up and Restore Configuration Settings](#)
- [Change the Login Password](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [CWMP Settings](#)
- [Monitor the Internet Traffic Statistics](#)

10.1. Set System Time

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

Follow the steps below to set your system time.

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



The screenshot shows the 'System Time' configuration page. It includes the following fields and buttons:

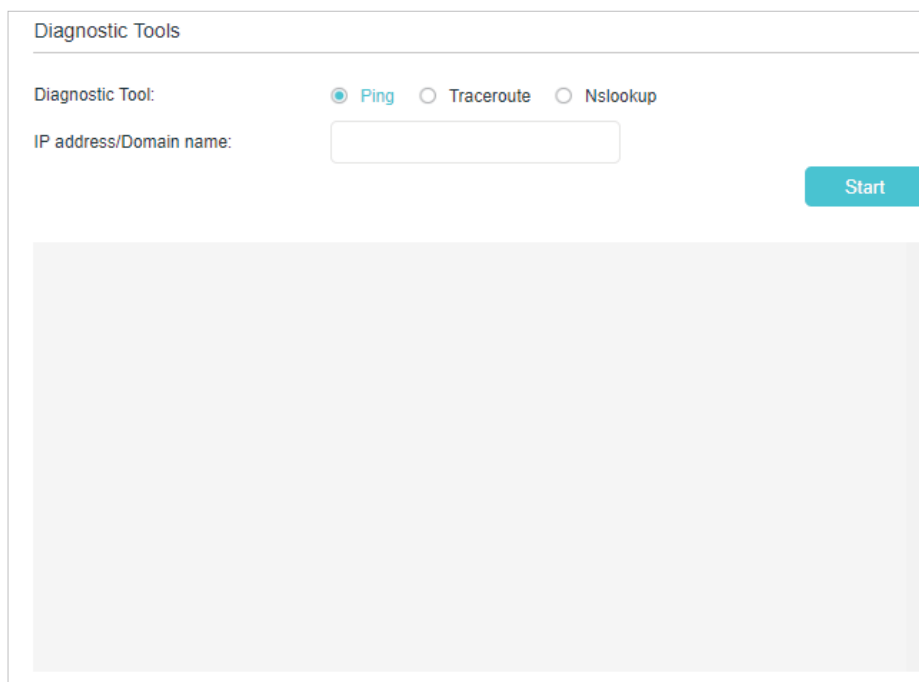
- Region:** A dropdown menu set to 'United Kingdom'.
- Time Zone:** A dropdown menu set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'.
- Date:** A text input field containing '1/1/2016' with '(MM/DD/YY)' as a placeholder.
- Time:** Three dropdown menus for hours, minutes, and seconds, set to '2', '25', and '57' respectively.
- NTP Server I:** A text input field containing '0.0.0.0' with '(Optional)' as a placeholder.
- NTP Server II:** A text input field containing '0.0.0.0' with '(Optional)' as a placeholder.
- Buttons:** Two buttons labeled 'Get from PC' and 'Get from the Internet' are positioned below the NTP server fields. A 'Save' button is located at the bottom right of the form.

3. Configure the system time using the following methods:
 - Manually:** Select your region, time zone, enter the date and select the local time.
 - Get from PC:** Click this button if you want to use the current time of your PC.
 - Get from the Internet:** Click this button if you want to get time from the internet. Make sure your router can access the internet before you select this way to get system time.
4. Click [Save](#).

10.2. Test the Network Connectivity

Diagnostic tools are 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 Controller.
2. Go to [Settings > System Tools > Diagnostics](#).



3. Select **Ping**, **Traceroute** or **Nslookup** as the diagnostic tool to test the connectivity;
 - **Ping** is used to test the connectivity between the router and the tested host, and measure the round-trip time.
 - **Traceroute** is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.
 - **Nslookup** is used to query the DNS to obtain domain name or IP address mapping or for any other specific DNS record.
4. Enter the **IP Address** or **Domain Name** of the host to be tested.
5. Click **Start** to start the diagnostics and you will find the test results in the gray box.

10.3. Update the Firmware

TP-Link is dedicated to improving 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. The latest firmware can also be downloaded 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. Back up your router configuration before upgrading the firmware.
3. DO NOT turn off the router during the firmware upgrade.

Follow the steps below to update the firmware:

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 password you set for the Controller.
3. Go to **Settings > System Tools > Firmware Upgrade**.
4. Focus on the **Controller Information** section. Make sure the downloaded firmware file matches with the **Hardware Version**.
5. Locate the **Firmware Upgrade** section. Click **Browse** to load the downloaded new firmware file, and click **Upgrade**.

Firmware Upgrade

New Firmware File: [Browse](#)

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

Note: We recommend that your Controller and the Satellites run on the same firmware. You can check the firmware versions of the Satellites in the [Satellite Version List](#) table.

Satellite Version List					
ID	Device Name	Firmware Version	Hardware Version	Status	Synced
1	For Study	1.0.2.0.9	HC220-G1 v1 00000000	Online	Yes
2	For Living Room	1.0.2.0.9	HC220-G1 v1 00000000	Online	Yes

10.4. 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 Controller to a previous settings by the backup file when needed. Moreover, you can erase the current settings and reset the router to its default factory settings.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Settings > System Tools > Backup & Restore**.

➤ To back up configuration settings:

Click **Backup** to save a copy of the current settings to your local computer. A "conf. bin" file will be stored to your computer.

Backup

Save a copy of your current settings. [Backup](#)

➤ **To restore configuration settings:**

- 1) Click [Browse](#) to load the previous backup configuration file, and click [Restore](#).

The screenshot shows a web interface titled "Restore". Below the title is a horizontal line. Underneath, the text reads "Restore previous settings from a saved file." Below this text is a "File:" label followed by an empty text input field. To the right of the input field is a teal "Browse" button. Further to the right is a larger teal "Restore" button.

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

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

- 1) Click [Factory Restore](#) to reset the Controller to its factory default settings.

The screenshot shows a web interface titled "Factory Default Restore". Below the title is a horizontal line. Underneath, the text reads "Restore all the configuration settings to their default values." To the right of this text is a teal "Factory Restore" button.

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

■ **Note:**

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

10.5. Change the Login Password

A login password is required when you are trying to log in to the Controller's web management page. You will be asked to create a password at the first login. You can change it on the web management page.

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

The screenshot shows a web interface titled "Account Management". Below the title is a horizontal line. Underneath, there are three password input fields: "Old Password:", "New Password:", and "Confirm New Password:". Each field has a small eye icon to its right. Below the "New Password:" field, there are three buttons labeled "Low", "Middle", and "High" for password strength selection. At the bottom right of the form is a teal "Save" button.

3. Enter the old password, and enter the new password twice.

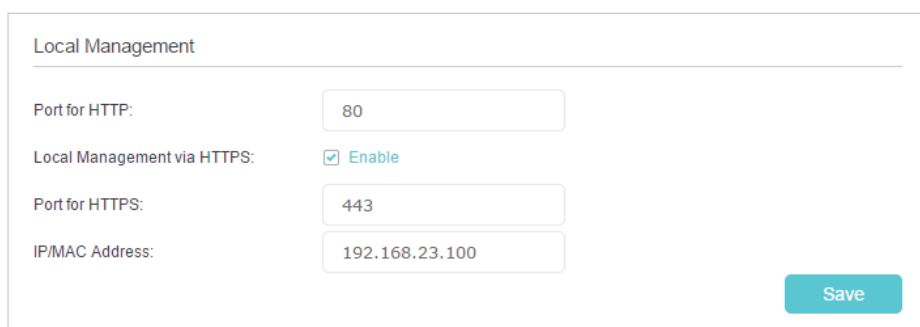
4. Click [Save](#) to make the settings effective.

10.6. Local Management

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

Follow the steps below to allow only the specific device to manage the Controller via the local management over HTTPS.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to [Settings](#) > [System Tools](#) > [Administration](#) and locate the [Local Management](#) section.
3. Select the [Enable](#) checkbox for [Local Management via HTTPS](#), and keep the [Port for HTTP](#) and [Port for HTTPS](#) as the default settings. Enter the [IP address](#) or [MAC address](#) of the local device to manage the Controller.



Local Management	
Port for HTTP:	<input type="text" value="80"/>
Local Management via HTTPS:	<input checked="" type="checkbox"/> Enable
Port for HTTPS:	<input type="text" value="443"/>
IP/MAC Address:	<input type="text" value="192.168.23.100"/>
<input type="button" value="Save"/>	

4. Click [Save](#) to make the settings effective.

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

Note: If you want all local devices can manage the router, just leave the [IP/MAC Address](#) field blank.

10.7. Remote Management

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

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 manage the Controller over HTTPS.

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

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** button

3. Enable [Remote Management](#) and [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 Controller. If you just want to allow a specific device to manage the Controller, 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 controller 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 Controller's web management page at [Settings > System Tools > Administration](#).

The screenshot shows a 'Certificate' section with a single button labeled '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.

10.8. 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 may 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 password you set for the Controller.
2. Click **Advanced** > **System Tools** > **System Log** page.

The screenshot shows the 'System Log' page. At the top, there are two dropdown menus: 'Type' set to 'ALL' and 'Level' set to 'Alert'. To the right of these are two buttons: 'Refresh' (with a circular arrow icon) and 'Delete All' (with a minus sign icon). Below this is a table with the following structure:

ID	Time	Type	Level	Log Content
--	--	--	--	--

At the bottom of the page, there are two buttons: 'Log Settings' and 'Save 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 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.

The screenshot shows the 'Log Settings' page. It has two checked checkboxes: 'Save Locally' and 'Save Remotely'. Below 'Save Locally' is a dropdown menu for 'Minimum Level' set to 'Information'. Below 'Save Remotely' is another dropdown menu for 'Minimum Level' set to 'Warning'. There are three input fields: 'Server IP' (empty), 'Server Port' (containing '514'), and 'Local Facility Name' (set to 'User'). At the bottom right, there are two buttons: 'Back' and 'Save'.

- **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.

10.9. CWMP Settings

The Controller supports CWMP (CPE WAN Management Protocol), also called TR-069. This collects information, performs diagnostics and configures the devices automatically via ACS (Auto-Configuration Server).

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

CWMP Settings

CPE WAN Management Protocol (also called TR-069) allows Auto-Configuration Server (ACS) to perform auto-configuration, provision, connection, and diagnostics to this device. You may configure this function under your ISP's instructions.

CWMP:

Inform:

Inform Interval:

ACS URL:

ACS Username:

ACS Password:

Interface used by TR-069 client:

Display SOAP messages on serial console:

Connection Request Authentication

Username:

Password:

Path:

Port:

URL:

- **CWMP:** Enable or disable the CWMP (CPE WAN Management Protocol) function.

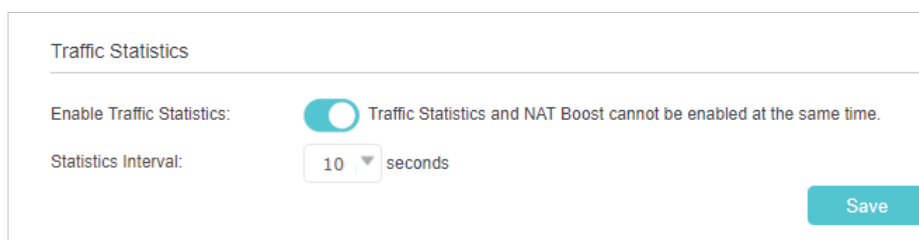
- **Inform:** Enable or disable the function of sending an inform message to the ACS (Auto Configuration Server) periodically.
- **Inform Interval:** Set the time interval in seconds when the Inform message will be sent to the ACS.
- **ACS URL:** Set the web address of the ACS which is provided by your ISP.
- **ACS Username/Password:** Set 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:** Enable or disable this function.
- **Connection Request Authentication:** Select this checkbox to enable authentication for the connection request.
- **Username/Password:** Set 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 this button to get the methods to support CWMP.

Click **Save** to make the settings effective.

10. 10. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the traffic usage of all devices in the past 10 minutes/24 hours/7 days.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
2. Go to **Advanced > System Tools > Statistics**.
3. Turn on **Enable Traffic Statistics** to enable traffic statistics function, you can view the total number of packets and bytes received and transmitted by the router within the selected **Statistics Interval**. This function is disabled by default.



Traffic Statistics

Enable Traffic Statistics: Traffic Statistics and NAT Boost cannot be enabled at the same time.



Statistics Interval: 10 seconds

Save

4. You can refer to **Traffic Statistics List** for the detailed information about the traffic usage of all devices.

Traffic Statistics List

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

IP Address/ MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
192.168.23.100 C4B1D8A6	682	300,467	355	195,146	0	1	3	 

FAQ

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

The default wireless password is printed on the label of the router.

If the password has been altered:

1. Connect your computer to the Controller using an Ethernet cable.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the Controller.
3. Go to [Settings](#) > [Wireless](#) > [Wifi-Network](#) to retrieve or reset your wireless password.

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

- With the Controller powered on, use a pin or similar subject to press and hold the Reset button for at least 5 seconds to reset it, and then visit <http://tplinkwifi.net> to create a new login password.

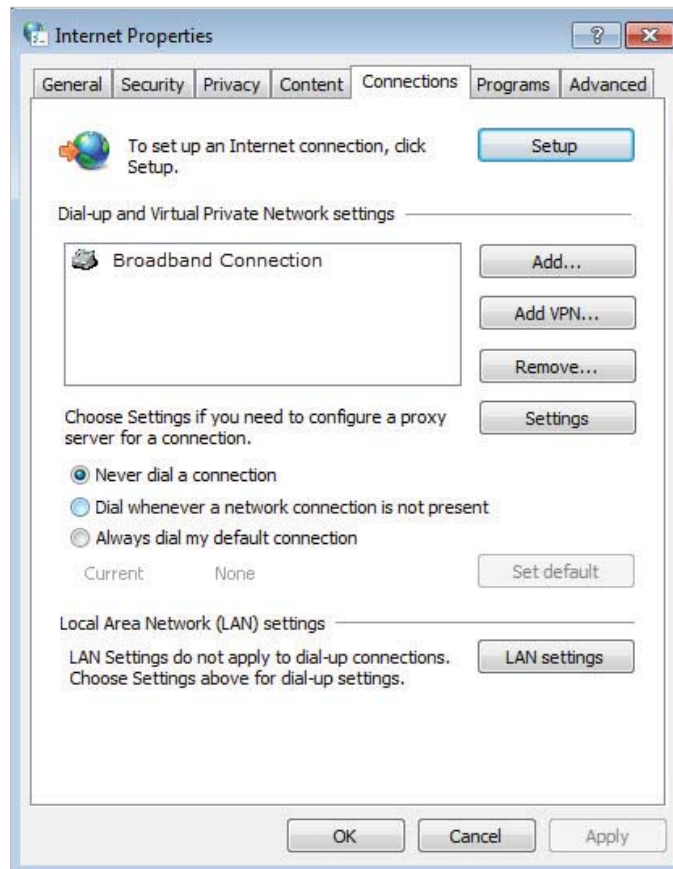
Note:

- You must reconfigure the controller to access the internet once it is reset, please note down your new password for future use.

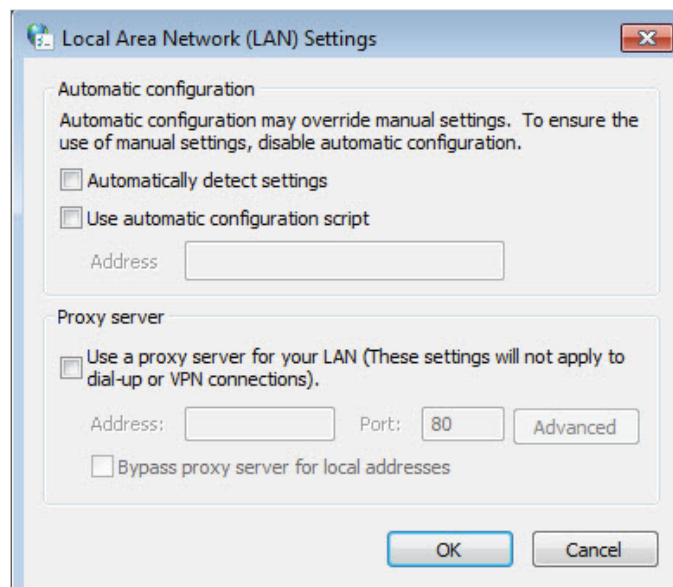
Q3. What should I do if I cannot log in to the Controller's web management page?

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

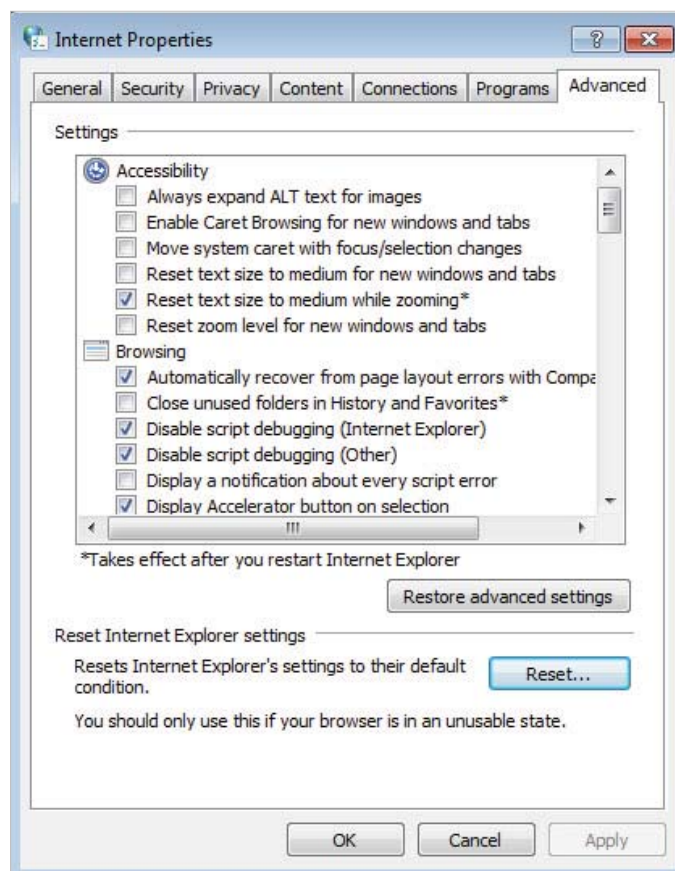
- Make sure your computer is connected to the Controller correctly.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkwifi.net> or <http://192.168.23.1> is correctly entered.
- 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](#).



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



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



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

Note: You must reconfigure the Controller to access the internet once it is reset.

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

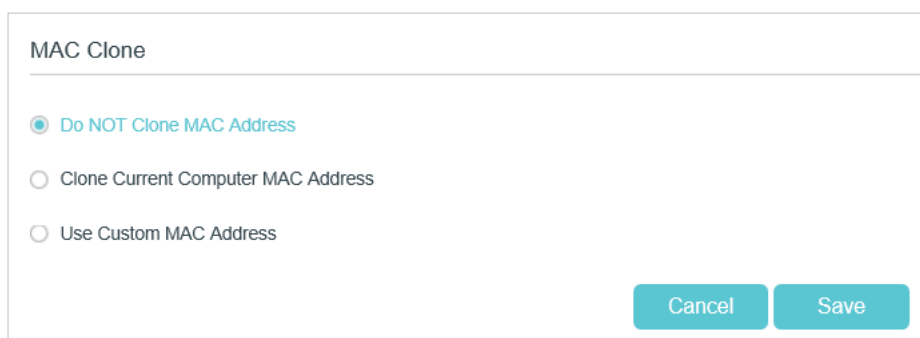
1. Check if the internet is working normally by connecting a computer directly to the modem via an Ethernet cable. If it is not, contact your internet service provider.
2. Check to see if all the connectors are connected well, including the Ethernet cables and power adapter.
3. Check to see if you can log in to the web management page of the Controller. If you cannot, please adjust your computer's settings according to [Q3](#) and then see if you can access the internet. If the problem persists, please go to the next step.
4. Consult your ISP and make sure the connection type, username and password are correct. If there are any mistakes, please run the Quick Setup again to correct the settings.
5. Refer to [Q5](#) to clone the MAC address.

6. If you still cannot access the internet, please restore the Controller to its factory default settings and reconfigure it by following the instructions in [Use Quick Setup Wizard](#).
7. Please contact our Technical Support if the problem persists.

Q5. How to configure MAC address?

You can manually change the MAC address of the Controller. 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://tplinkwif.net>, and log in with the password you set for the Controller.
2. Go to [Settings](#) > [Advanced Settings](#) > [Internet](#) and click the [Add](#) icon, and scroll down to find the [MAC Clone](#) section.



MAC Clone

Do NOT Clone MAC Address

Clone Current Computer MAC Address

Use Custom MAC Address

Cancel Save

- If you are using the computer with the authenticated MAC address to access the modem router, please select [Use 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.

Tips:

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

Q6. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

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

- Make sure the wireless function of your device is enabled if you're using a laptop with 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 Wireless LED indicator on your Controller or Satellites.
- Make sure your computer/device is still in the range of your Wi-Fi coverage. Move it closer if it is currently too far away.
- Go to [Settings](#) > [Wireless](#) to check the wireless settings. Double check your wireless network name(s) is not hidden.

If you can find your wireless network but failed 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 routers.



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


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

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

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

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

COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2019 TP-Link Technologies Co., Ltd. All rights reserved.

FCC compliance information statement



Product Name: AC2200 Home Wi-Fi System

Model Number: HC2220-G1u

Component Name	Model
I.T.E POWER SUPPLY	EVSA+24120-2001

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

FCC compliance information statement



Product Name: I.T.E POWER SUPPLY

Model Number: EVSA+24120-2001

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the

user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2019.7.25

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)

2400 MHz - 2483.5 MHz (20dBm)

5150 MHz - 5250 MHz (23dBm)

EU declaration of conformity

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

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

RF Exposure Information

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

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

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

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

Canadian Compliance Statement

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

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

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables

aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

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

Caution:

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

Avertissement:

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

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

注意！

依據 低功率電波輻射性電機管理辦法

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

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；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。

4.7.9.1應避免影響附近雷達系統之操作。

4.7.9.2高增益指向性天線只得應用於固定式點對點系統。

BSMI Notice

安全諮詢及注意事項

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

限用物質含有情況標示聲明書


產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	-	○	○	○	○	○
備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 系指限用物質之百分比含量超出百分比含量基準值。						
備考2. “○” 系指該項限用物質之百分比含量未超出百分比含量基準值。						
備考3. “-” 系指該項限用物質為排除項目。						



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






Safety Information

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

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

Explanations of the symbols on the product label

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