



User Guide

300Mbps Wireless N Router
TL-WR841N

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview.....	3
1. 2. Panel Layout.....	3
1. 2. 1.Top View	3
1. 2. 2.The Back Panel.....	4
Chapter 2. Connect to the Internet	5
2. 1. Position Your Router	6
2. 2. Connect to the Internet	6
2. 2. 1.Wireless Router Mode.....	6
2. 2. 2.WISP Mode	8
2. 2. 3.Range Extender Mode.....	9
2. 2. 4.Access Point Mode.....	10
Chapter 3. Log In to the Router	12
Chapter 4. Configure the Router in Wireless Router Mode	14
4. 1. Status	15
4. 2. Operation Mode	16
4. 3. Network	17
4. 3. 1. WAN.....	17
4. 3. 2. LAN	24
4. 3. 3. IPTV.....	24
4. 3. 4.MAC Clone.....	25
4. 4. Wireless	26
4. 4. 1.Wireless Settings	26
4. 4. 2. WPS.....	27
4. 4. 3.Wireless Security	28
4. 4. 4.Wireless MAC Filtering	30
4. 4. 5.Wireless Advanced.....	31
4. 4. 6.Wireless Statistics	33
4. 5. Guest Network.....	33
4. 6. DHCP.....	34

4. 6. 1.DHCP Settings	35
4. 6. 2.DHCP Clients List	36
4. 6. 3.Address Reservation	36
4. 7. Forwarding	37
4. 7. 1.Virtual Server	37
4. 7. 2.Port Triggering	38
4. 7. 3. DMZ.....	39
4. 7. 4. UPnP.....	40
4. 8. Security	41
4. 8. 1.Basic Security.....	41
4. 8. 2.Advanced Security	43
4. 8. 3.Local Management.....	44
4. 8. 4.Remote Management	45
4. 9. Parental Controls	46
4. 10. Access Control	47
4. 11. Advanced Routing	50
4. 11. 1.Static Route List	50
4. 11. 2.System Routing Table.....	51
4. 12. Bandwidth Control.....	51
4. 13. IP & MAC Binding	53
4. 13. 1.Binding Settings	53
4. 13. 2.ARP List	53
4. 14. Dynamic DNS.....	54
4. 15. IPv6	57
4. 15. 1.IPV6 Status	57
4. 15. 2.IPV6 WAN.....	57
4. 15. 3.IPV6 LAN.....	61
4. 16. System Tools	61
4. 16. 1.Time Settings.....	61
4. 16. 2.Diagnostic	63
4. 16. 3.Firmware Upgrade	64
4. 16. 4.Factory Defaults	64
4. 16. 5.Backup & Restore	65
4. 16. 6.Reboot	65
4. 16. 7.Password	67
4. 16. 8.System Log.....	68
4. 16. 9.Statistics	68
4. 17. Logout	68

Chapter 5. Configure the Router in WISP Mode	69
5. 1. Status	70
5. 2. Operation Mode	71
5. 3. Network	72
5. 3. 1. WAN.....	72
5. 3. 2. LAN	79
5. 3. 3.MAC Clone.....	79
5. 4. Wireless	80
5. 4. 1.Wireless Settings	80
5. 4. 2. WPS.....	81
5. 4. 3.Wireless Security	83
5. 4. 4.Wireless MAC Filtering	85
5. 4. 5.Wireless Advanced.....	86
5. 4. 6.Wireless Statistics	87
5. 5. Guest Network.....	88
5. 6. DHCP.....	89
5. 6. 1.DHCP Settings	89
5. 6. 2.DHCP Clients List	90
5. 6. 3.Address Reservation	91
5. 7. Forwarding	91
5. 7. 1.Virtual Server	92
5. 7. 2.Port Triggering	93
5. 7. 3. DMZ.....	94
5. 7. 4. UPnP.....	95
5. 8. Security	96
5. 8. 1.Basic Security.....	96
5. 8. 2.Advanced Security.....	97
5. 8. 3.Local Management.....	99
5. 8. 4.Remote Management	99
5. 9. Parental Controls	100
5. 10. Access Control	101
5. 11. Advanced Routing	104
5. 11. 1.Static Route List	104
5. 11. 2.System Routing Table.....	105
5. 12. Bandwidth Control.....	106
5. 13. IP & MAC Binding	107
5. 13. 1.Binding Settings	107
5. 13. 2.ARP List	108
5. 14. Dynamic DNS.....	109

5. 15. IPv6	111
5. 15. 1.I Pv6 Status	111
5. 15. 2.I Pv6 WAN.....	112
5. 15. 3.I Pv6 LAN.....	115
5. 16. System Tools	116
5. 16. 1.Time Settings.....	116
5. 16. 2.Diagnostic	117
5. 16. 3.Firmware Upgrade	119
5. 16. 4.Factory Defaults	119
5. 16. 5.Backup & Restore	119
5. 16. 6.Reboot	120
5. 16. 7.Password	122
5. 16. 8.System Log.....	122
5. 16. 9.Statistics	123
5. 17. Logout	123

Chapter 6. Configure the Router in Access Point Mode 124

6. 1. Status	125
6. 2. Operation Mode	126
6. 3. Network	126
6. 3. 1. LAN	126
6. 4. Wireless	127
6. 4. 1.Basic Settings.....	127
6. 4. 2. WPS.....	128
6. 4. 3.Wireless Security	129
6. 4. 4.Wireless MAC Filtering	131
6. 4. 5.Wireless Advanced.....	132
6. 4. 6.Wireless Statistics	134
6. 4. 7.Throughput Monitor.....	134
6. 5. DHCP.....	135
6. 5. 1.DHCP Settings	135
6. 5. 2.DHCP Clients List	136
6. 5. 3.Address Reservation	137
6. 6. System Tools	137
6. 6. 1.Time Settings	137
6. 6. 2.Diagnostic	139
6. 6. 3.SNMP Settings.....	140
6. 6. 4.Ping WatchDog	141

6. 6. 5.Firmware Upgrade	142
6. 6. 6.Factory Defaults	142
6. 6. 7.Backup & Restore	143
6. 6. 8.Reboot.....	143
6. 6. 9.Password	145
6. 6. 10.System Log.....	145
6. 7. Logout	146

Chapter 7. Configure the Router in Range Extender Mode 147

7. 1. Status	148
7. 2. Operation Mode	149
7. 3. Network	149
7. 3. 1. LAN	149
7. 4. Wireless	150
7. 4. 1.Connect to Network.....	150
7. 4. 2.Extended Network	151
7. 4. 3.Wireless MAC Filtering	151
7. 4. 4.Wireless Advanced.....	153
7. 4. 5.Wireless Statistics	154
7. 5. DHCP.....	154
7. 5. 1.DHCP Settings.....	154
7. 5. 2.DHCP Clients List	156
7. 6. System Tools	157
7. 6. 1.Time Settings	157
7. 6. 2.Diagnostic	158
7. 6. 3.Firmware Upgrade.....	159
7. 6. 4.Factory Defaults	159
7. 6. 5.Backup & Restore	160
7. 6. 6.Reboot.....	160
7. 6. 7.Password	162
7. 6. 8.System Log.....	162
7. 7. Logout	163

FAQ..... 164

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.

■ Note:

Features available in this router may vary by software version, region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

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, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
■ Note:	Ignoring this type of note might result in a malfunction or damage to the device.
⌚ Tips:	Indicates important information that helps you make better use of your device.

More Info

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

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

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

TP-Link Community is provided for you to discuss our products and share knowledge at <https://community.tp-link.com>.

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

Speed/Coverage Disclaimer

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

- [Product Overview](#)
- [Panel Layout](#)

1. 1. Product Overview

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

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

1. 2. Panel Layout

1. 2. 1. Top View



The router's LEDs are located on the front panel. You can check the router's working status by following the LED Explanation table.

LED	Status	Indication
④ (Internet)	Solid Orange	Router Mode: The WAN port is connected, but internet is not available. Access Point Mode: The WAN port is not connected. Range Extender Mode: The router is not connected to the host network. WISP Mode: Internet is not available.
	Blinking Orange	The WAN port is not connected while in Router Mode.
	Solid Green	Router/WISP Mode: Internet is available. Access Point Mode: The WAN port is connected. Range Extender Mode: The router is connected to the host network.
	Blinking Green	The system is starting up or firmware is being upgraded. <small>* To avoid device damage, do not disconnect or power off your router during the upgrade.</small>

LED	Status	Indication
 (LAN)	Solid Green	At least one LAN port is connected.
 (Wi-Fi)	Solid Green	Wireless function is enabled.
	Blinking Green	WPS connection is in progress. This may take up to 2 minutes.

1.2.2. The Back Panel



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

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet port.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
WPS/RESET Button	To enable the WPS function, press this button for 1 second. If you have a WPS-supported device, you can press this button to quickly establish connection between the router and the client device and automatically configure wireless security for your wireless network.
	Press and hold this button for more than 5 seconds to reset the router to its factory default settings.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect to the Internet

This chapter contains the following sections:

- [Position Your Router](#)
- [Connect to the Internet](#)

2. 1. Position Your Router

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

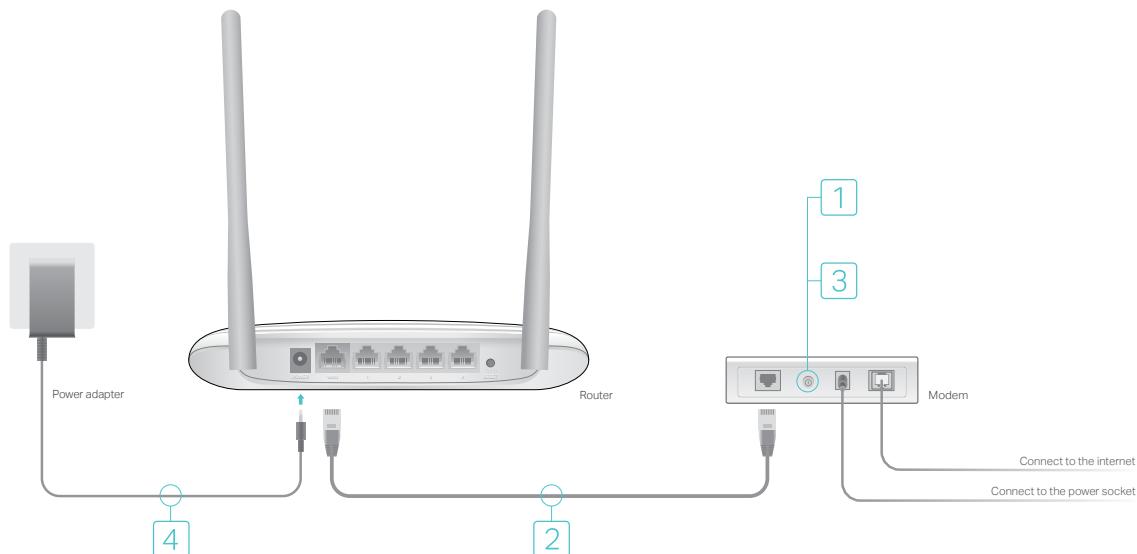
2. 2. Connect to the Internet

The Router provides four working modes: Wireless Router, WISP, Range Extender and Access Point. You can choose the mode to better suit your network needs and follow the guide to complete the configuration.

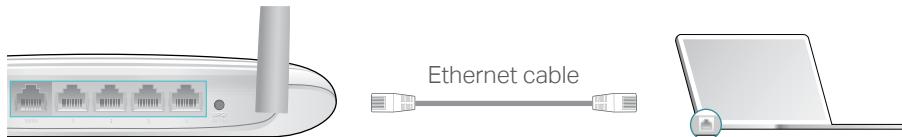
2. 2. 1. Wireless Router Mode

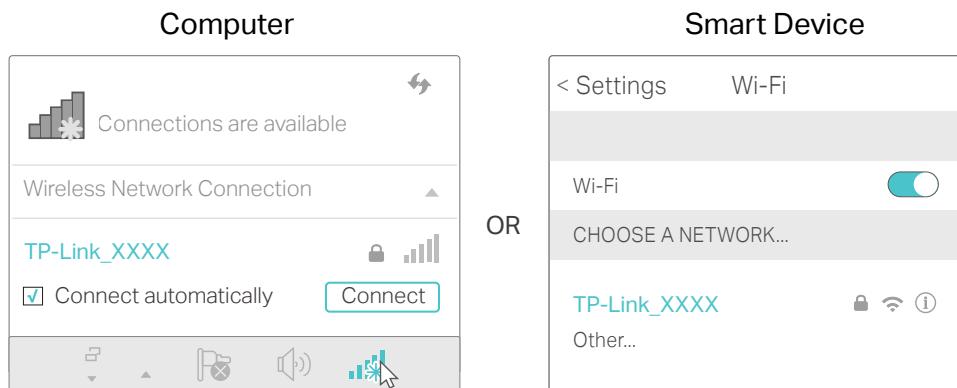
1. Follow the steps below to connect your router.

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



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

- 2) Connect the modem to the router's **WAN** port with an Ethernet cable.
 - 3) Turn on the modem, and then wait about **2 minutes** for it to restart.
 - 4) Connect the power adapter to the router and power on the router.
2. Connect your computer to the router.
- **Method 1: Wired**
- Turn off the Wi-Fi on your computer and connect the devices as shown below.
- 
- **Method 2: Wirelessly**
- 1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the router.
 - 2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.



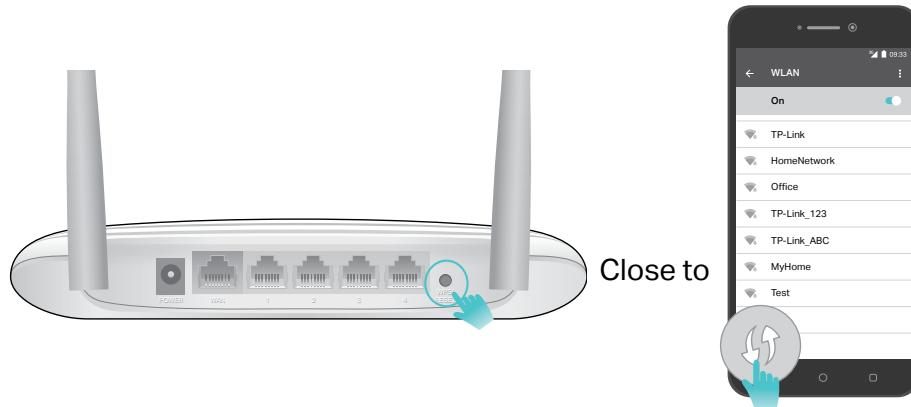
- **Method 3: Use the WPS button**

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

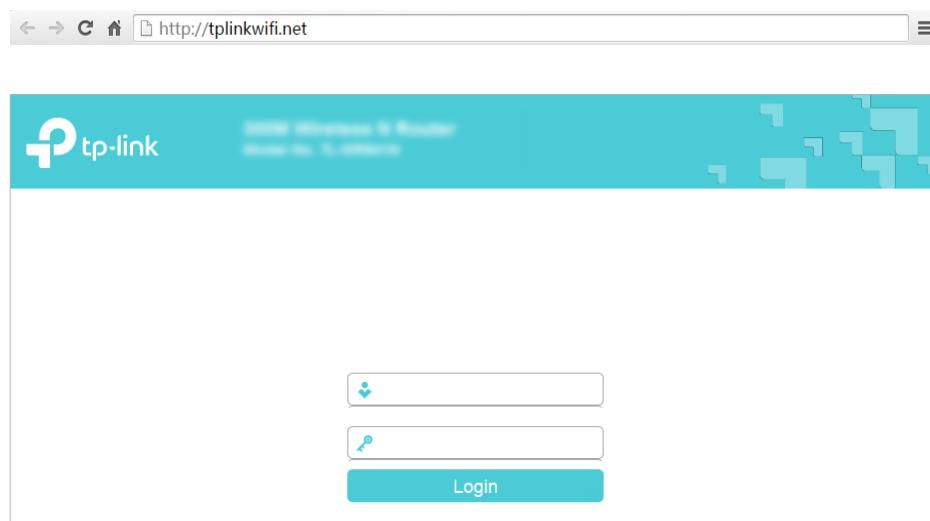
 **Note:**

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

- 1) Tap the WPS icon on the device's screen. Here we take an Android phone as an example.
- 2) Immediately press the WPS button on your router.



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



 Note:

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

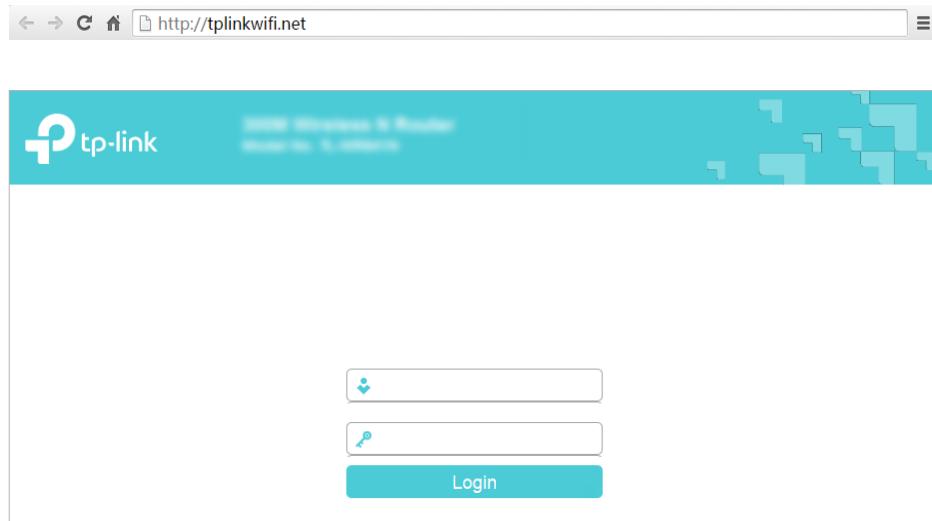
4. After successfully login, select **Wireless Router** and follow the **Quick Setup** to set up the internet connection.
5. **Enjoy!** For wireless devices, you may have to reconnect to the wireless network if you have customized the SSID (wireless name) and password during the configuration.

2.2.2. WISP Mode

This mode connects to the ISP network wirelessly in areas without wired service.



1. Connect the power adapter to the router and power on the router.
2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (wireless name) and password printed on the bottom label of the router.
3. Enter <http://tplinkwifi.net> in the address bar of a web browser. Use **admin** for both username and password, and then click **Login**.

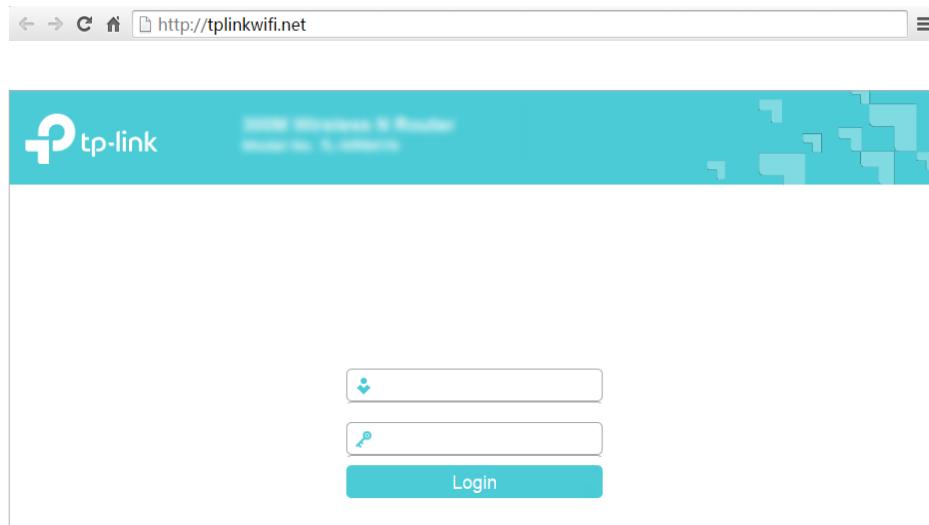


4. After successfully login, select **WISP** mode and follow the **Quick Setup** to set up the internet connection.
5. **Enjoy!** Connect your devices to the wireless network and enjoy the internet.

2.2.3. Range Extender Mode

This mode boosts your home wireless coverage.

1. Place the router next to your host router and power it on.
2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (wireless name) and password printed on the bottom label of the router.
3. Enter <http://tplinkwifi.net> in the address bar of a web browser. Use **admin** for both username and password, and then click **Login**.



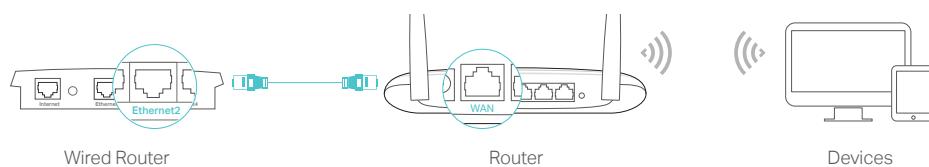
4. After successfully login, select **Range Extender** mode and follow the **Quick Setup** to set up the internet connection.
5. **Relocate:** Place the router between your host router and the Wi-Fi dead zone. The location you choose must be within the range of your existing host network.



6. **Enjoy!** The extended network shares the same wireless password as that of your host network, but may have different network name if you have customized it during the configuration.

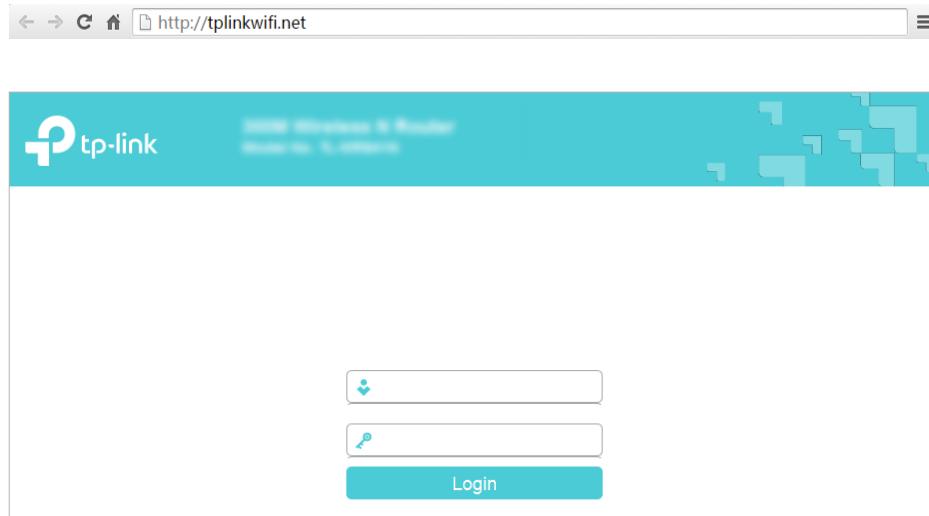
2.2.4. Access Point Mode

This mode transforms your existing wired network to a wireless network.



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

2. Connect the router to your wired host router's Ethernet port via an Ethernet cable as shown above.
3. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and password printed on the bottom label of the router.
4. Enter <http://tplinkwifi.net> in the address bar of a web browser. Use **admin** for username and password, and then click **Login**.



 Note:

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

5. After successfully login, select **Access Point** mode and follow the **Quick Setup** to set up the internet connection.
6. **Enjoy!** Connect your devices to the wireless network and enjoy the internet.

Chapter 3

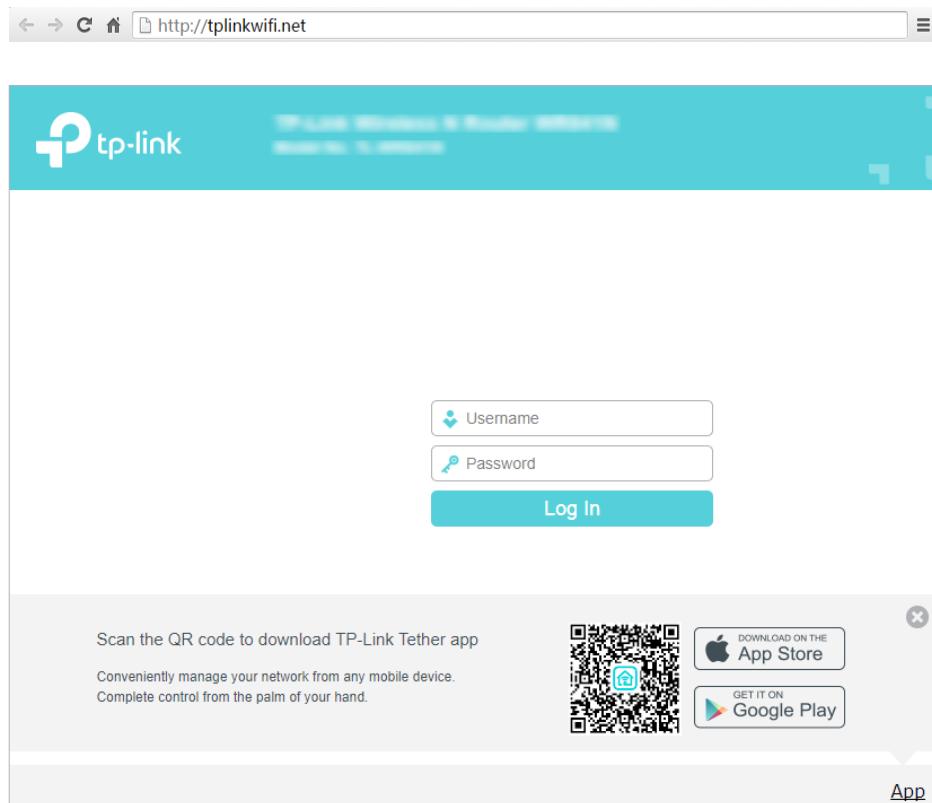
Log In to the Router

This chapter introduces how to log in to the Web-based Utility of the router.

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

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. The default one is [admin](#) (all lowercase) for both username and password.



Note:

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

Chapter 4

Configure the Router in Wireless Router Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [Guest Network](#)
- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Controls](#)
- [Access Control](#)
- [Advanced Routing](#)
- [Bandwidth Control](#)
- [IP & MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6](#)
- [System Tools](#)
- [Logout](#)

4. 1. Status

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. The default one is **admin** (all lowercase) for both username and password.
2. Go to **Status**. You can view the current status information of the router.

Status	
Firmware Version:	TL-WR841N V1.0
Hardware Version:	V1.0, 2010.03.02
LAN	
MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Router
Wireless Radio:	Enabled
Name(SSID):	TP-Link_0969
Mode:	11bgn mixed
Channel:	Auto(Channel 2)
Channel Width:	Auto
MAC Address:	00:0A:EB:13:09:69
WAN	
MAC Address:	00:0A:EB:13:09:6A
IP Address:	0.0.0.0(Dynamic IP)
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0 Unplugged
DNS Server:	0.0.0.0 0.0.0.0
System Up Time: 1 day(s) 06:50:47	
<input type="button" value="Refresh"/>	

- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Network > LAN** page.
 - **MAC address** - The physical address of the router.
 - **IP address** - The LAN IP address of the router.
 - **Subnet Mask** - The subnet mask associated with the LAN IP address.
- **Wireless** - This field displays the basic information or status of the wireless function, and you can configure them on the **Wireless > Basic Settings** page.

- **Operation Mode** - The current wireless working mode in use.
- **Wireless Radio** - Indicates whether the wireless radio feature of the router is enabled or disabled.
- **Name(SSID)** - The SSID of the router.
- **Mode** - The current wireless mode which the router works on.
- **Channel** - The current wireless channel in use.
- **Channel Width** - The current wireless channel width in use.
- **MAC Address** - The physical address of the router.
- **WAN** - This field displays the current settings of the WAN, and you can configure them on the [Network > WAN](#) page.
 - **MAC Address** - The physical address of the WAN port.
 - **IP Address** - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no internet connection.
 - **Subnet Mask** - The subnet mask associated with the WAN IP Address.
 - **Default Gateway** - The Gateway currently used is shown here. When you use Dynamic IP as the internet connection type, click [Renew](#) or [Release](#) here to obtain new IP parameters dynamically from the ISP or release them.
 - **DNS Server** - The IP addresses of DNS (Domain Name System) server.
- **System Up Time** - The length of the time since the router was last powered on or reset.

Click [Refresh](#) to get the latest status and settings of the router.

4. 2. Operation Mode

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Operation Mode](#).
3. Select the working mode as **Wireless Router** and click **Save**.

Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

Save

4.3. Network

4.3.1. WAN

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

Dynamic IP

If your ISP provides the DHCP service, please select **Dynamic IP**, and the router will automatically get IP parameters from your ISP.

Click **Renew** to renew the IP parameters from your ISP.

Click **Release** to release the IP parameters.

The screenshot shows the 'WAN Settings' configuration page. The 'Connection Type' dropdown is set to 'Dynamic IP'. Below it, there are fields for 'IP Address', 'Subnet Mask', and 'Gateway', each containing placeholder text. Underneath these are two buttons: 'Renew' and 'Release'. A 'Hide' button is located to the right of the 'Renew' button. Below this section, there is a field for 'MTU(Bytes)' with a value of '1500' and a note '(1500 as default, do not change unless necessary)'. There are also checkboxes for 'Get IP with Unicast' and 'Set DNS server manually'. The 'Host Name' field contains placeholder text. At the bottom of the page is a 'Save' button.

- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Get IP with Unicast** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (It is rarely required.)
- **Set DNS server manually** - If your ISP gives you one or two DNS addresses, select Set DNS server manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned automatically from your ISP.
- **Host Name** - This option specifies the name of the router.

Static IP

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

The screenshot shows the 'WAN Settings' configuration page. At the top, the 'Connection Type' dropdown is set to 'Static IP' with a 'Detect' button next to it. Below this, there are fields for 'IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS Server', and 'Secondary DNS Server', all currently set to '0.0.0.0'. A note '(optional)' is shown next to the Secondary DNS field. At the bottom of the form, there is a 'MTU(Bytes)' field containing '1500' with a note '(1500 as default, do not change unless necessary)', a 'Save' button, and a 'Hide' button.

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- **Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary/Secondary DNS Server** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.

PPPoE

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

The screenshot shows the 'WAN Settings' configuration page for PPPoE. Key fields include:

- Connection Type:** Set to PPPoE.
- PPP Username:** [Input field]
- PPP Password:** [Input field]
- Confirm password:** [Input field]
- Secondary Connection:** Radio button set to 'Disabled'.
- Connection Mode:** Radio button set to 'Always on'.
- Max Idle Time:** Set to 15 minutes.
- Authentication Type:** Set to AUTO_AUTH.
- Advanced Settings:** Includes fields for Service Name, Server Name, MTU (1480), Use IP address specified by ISP, Echo request interval (0), and Set DNS server manually.
- Buttons:** 'Save' at the bottom, and 'Connect' and 'Disconnect' buttons below the main settings.

- **PPP Username/Password** - Enter the user name and password provided by your ISP. These fields are case-sensitive.
- **Confirm Password** - Enter the Password provided by your ISP again to ensure the password you entered is correct.
- **Secondary Connection** - It's available only for PPPoE connection. If your ISP provides an extra connection type, select **Dynamic IP** or **Static IP** to activate the secondary connection.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically

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

- **Authentication Type** - Choose an authentication type.

■ Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

- **Service Name/Server Name** - The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **MTU(Bytes)** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Use IP Address Specified by ISP** - If your ISP does not automatically assign IP addresses to the router, please select this item and enter the IP address provided by your ISP in dotted-decimal notation.
- **Echo Request Interval** - The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.
- **Set DNS Server Manually** - If your ISP does not automatically assign DNS addresses to the router, please select this item and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

L2TP

If your ISP provides L2TP connection, please select [L2TP](#).

WAN Settings

Connection Type:	<input type="text" value="L2TP"/> <input type="button" value="Detect"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	
Addressing Type:	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
Server IP Address/Name:	<input type="text"/>
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS Server:	0.0.0.0, 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0, 0.0.0.0
MTU(Bytes):	<input type="text" value="1460"/> (1460 as default, do not change unless necessary)
Connection Mode:	<input checked="" type="radio"/> Always on <input type="radio"/> Connect on demand <input type="radio"/> Connect manually
Max Idle Time:	<input type="text" value="15"/> minutes (0 meaning connection remains active at all times)
<input type="button" value="Save"/>	

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Server IP Address/Name** - Enter server IP address or domain name provided by your ISP.
- **MTU(Bytes)** - The default MTU size is 1460 bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

■ Note:

Sometimes the connection cannot be terminated although you have specified the **Max Idle Time** because some applications are visiting the internet continually in the background.

PPTP

If your ISP provides PPTP connection, please select **PPTP**.

The screenshot shows the 'WAN Settings' configuration page for a PPTP connection. The 'Connection Type' dropdown is set to 'PPTP'. Below it, there are fields for 'Username' and 'Password', and buttons for 'Connect' and 'Disconnect'. Under 'Addressing Type', the 'Dynamic IP' radio button is selected. The 'Server IP Address/Name' field contains '0.0.0.0'. Other fields show placeholder values: 'IP Address: 0.0.0.0', 'Subnet Mask: 0.0.0.0', 'Gateway: 0.0.0.0', 'DNS Server: 0.0.0.0, 0.0.0.0', 'Internet IP Address: 0.0.0.0', and 'Internet DNS: 0.0.0.0, 0.0.0.0'. The 'MTU(Bytes)' field is set to '1420'. Under 'Connection Mode', the 'Always on' radio button is selected. The 'Max Idle Time' field is set to '15' minutes. A 'Save' button is located at the bottom right.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Server IP Address/Name** - Enter server IP address or domain name provided by your ISP.
- **MTU(Bytes)** - The default MTU size is 1420 bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically

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

■ Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

BigPond Cable

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

The screenshot shows the 'WAN Settings' configuration page. At the top, the 'Connection Type' dropdown is set to 'BigPond Cable' with a 'Detect' button next to it. Below this, there are fields for 'Username' and 'Password'. Further down are fields for 'Auth Server' and 'Auth Domain'. An 'MTU(Bytes)' field is set to 1500 with a note '(1500 as default, do not change unless necessary)'. Under 'Connection Mode', the 'Always on' radio button is selected. A 'Max Idle Time' field contains the value 15, with a note '(0 meaning connection remains active at all times)'. At the bottom of the form are 'Connect' and 'Disconnect' buttons, and a 'Save' button.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
- **MTU(Bytes)** - The default MTU size is 1500 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically

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

4.3.2. LAN

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

LAN Settings	
MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
<input type="button" value="Save"/>	

- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router (the default one is 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

■ Note:

- If you have changed the IP address, you must use the new IP address or <http://tplinkwifi.net> to log in.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.3.3. IPTV

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

The screenshot shows the 'IPTV Settings' page. It includes fields for enabling IGMP Snooping (checked), enabling IGMP Proxy (checked), selecting IGMP Version (V3), and enabling IPTV (unchecked). Below these are four dropdown menus for LAN ports 1 through 4, all set to 'Internet'. A 'Save' button is at the bottom.

- **IGMP Snooping** - IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. IGMP snooping is especially useful for bandwidth-intensive IP multicast applications such as IPTV.
- **IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **IGMP Version** - Select the IGMP (Internet Group Management Protocol) Proxy Version, either V2 or V3, according to your ISP.
- **IPTV** - Select to enable the IPTV feature.
- **IPTV Mode** - Select the appropriate mode according to your ISP.
- **LAN 1/2/3/4** - Assign your LAN port to whether function as the internet supplier or as the IPTV supplier.

4. 3. 4. MAC Clone

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Network > **MAC Clone**.
3. Configure the WAN MAC address and click **Save**.

The screenshot shows the 'MAC Clone' page. It has fields for 'WAN MAC Address' (00:0A:EB:13:09:6A) with a 'Restore Factory MAC' button, and 'Your PC's MAC Address' (40:8D:5C:89:74:B5) with a 'Clone MAC Address' button. A 'Save' button is at the bottom.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC

address in this field. Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click **Clone MAC Address** and this MAC address will be filled in the **WAN MAC Address** field.

■ Note:

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

4. 4. Wireless

4. 4. 1. Wireless Settings

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

Wireless Basic Settings	
Wireless:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Network Name:	TP-Link_0969 (Also called SSID)
Mode:	11bgn mixed
Channel:	Auto
Channel Width:	Auto
<input checked="" type="checkbox"/> Enable SSID Broadcast	
Save	

- **Wireless** - Enable or disable wireless network.
- **Wireless Network Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Mode** - You can choose the appropriate "Mixed" mode.
- **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems

with another nearby access point. If you select **Auto**, then AP will choose the best channel automatically.

- **Enable SSID Broadcast** - If enabled, the router will broadcast the wireless network name (SSID).

4. 4. 2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router's network quickly via WPS.

■ Note:

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

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

Method ONE: Press the WPS Button on Your Client Device

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

WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 12345670

Disable device PIN

Add a new device:

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

WPS Settings

Enter new device PIN.
PIN:

Press the WPS button of the new device within the next two minutes.

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

Method TWO: Enter the Client's PIN

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

The screenshot shows the 'WPS (Wi-Fi Protected Setup)' configuration page. At the top, it says 'WPS: Enabled' with a 'Disable' button. Below that, the 'Current PIN:' field displays '12345670' with 'Restore PIN' and 'Generate New PIN' buttons. There is also a checked checkbox for 'Disable device PIN'. At the bottom, there is an 'Add a new device:' field and an 'Add device' button.

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

The screenshot shows the 'WPS Settings' page. It has two options: 'Enter new device PIN.' (selected) and 'Press the WPS button of the new device within the next two minutes.' Below these options are 'Connect' and 'Back' buttons.

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

Method Three: Enter the Router's PIN

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

This screenshot is identical to the one above, showing the 'WPS (Wi-Fi Protected Setup)' configuration page with 'WPS: Enabled', a 'Current PIN:' of '12345670', and an 'Add device' button at the bottom.

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

4.4.3. Wireless Security

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

3. Configure the security settings of your wireless network and click **Save**.

- **Disable Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router without a password. It's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-Personal** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - **Version** - Select [Auto](#), [WPA-PSK](#) or [WPA2-PSK](#).
 - **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **Wireless Password** - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- **WPA /WPA2-Enterprise** - It's based on Radius Server.
 - **Authentication Type** - Select [Auto](#), [WPA](#) or [WPA2](#).
 - **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **Radius Server IP** - Enter the IP address of the Radius server.

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

4. 4. 4. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

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

For example, you want the wireless client A with the MAC address 00:0A:EB:B0:00:0B and the wireless client B with the MAC address 00:0A:EB:00:07:5F to access the router, but other wireless clients cannot access the router

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless MAC Filtering**.
3. Click **Enable** to enable the Wireless MAC Filtering function.

4. Select **Allow the stations specified by any enabled entries in the list to access** as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click **Add New** and fill in the blank.

Add or Modify Wireless MAC Address Filtering entry

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address:	00:0A:EB:B0:00:0B
Description:	Client A
Status:	Enabled

Save **Back**

- 1) Enter the MAC address 00:0A:EB:B0:00:0B / 00:0A:EB:00:07:5F in the MAC Address field.
- 2) Enter wireless client A/B in the Description field.
- 3) Select **Enabled** in the Status drop-down list.
- 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering:	Enabled	Disable																		
Filtering Rules																				
<input type="radio"/> Deny	the stations specified by any enabled entries in the list to access.																			
<input checked="" type="radio"/> Allow	the stations specified by any enabled entries in the list to access.																			
<table border="1"> <thead> <tr> <th></th> <th>MAC Address</th> <th>Status</th> <th>Host</th> <th>Description</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>00:0A:EB:B0:00:0B</td> <td>Enabled</td> <td>TP-Link_7AFF</td> <td>client A</td> <td>Edit</td> </tr> <tr> <td><input type="checkbox"/></td> <td>00:0A:EB:00:07:5F</td> <td>Enabled</td> <td>TP-Link_7AFF</td> <td>Client B</td> <td>Edit</td> </tr> </tbody> </table>				MAC Address	Status	Host	Description	Edit	<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-Link_7AFF	client A	Edit	<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	Edit
	MAC Address	Status	Host	Description	Edit															
<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-Link_7AFF	client A	Edit															
<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	Edit															
Add New Enable Selected Disable Selected Delete Selected																				

Done!

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

4.4.5. Wireless Advanced

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Advanced**.
3. Configure the advanced settings of your wireless network and click **Save**.

Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

The screenshot shows the 'Wireless Advanced' configuration page. It includes the following settings:

- Transmit Power: High (selected from a dropdown menu)
- Beacon Interval: 100 (value in input field, range 40-1000)
- RTS Threshold: 2346 (value in input field, range 1-2346)
- Fragmentation Threshold: 2346 (value in input field, range 256-2346)
- DTIM Interval: 1 (value in input field, range 1-15)
- Enable Short GI
- Enable Client Isolation
- Enable WMM

A 'Save' button is located at the bottom right of the form.

- **Transmit Power** - Select **High**, **Middle** or **Low** which you would like to specify for the router. **High** is the default setting and recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable Client Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

4.4.6. Wireless Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Statistics** to check the data packets sent and received by each client device connected to the router.

Wireless Stations Status					
Wireless Stations Currently Connected: 1					Refresh
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	WPS_XXXXXX

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

4.5. Guest Network

Guest Network allows you to provide Wi-Fi access for guests without disclosing your host network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network settings to ensure network security and privacy.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Guest Network**.
3. Enable the **Guset Network** function.
4. Create a network name for your guest network.
5. Select the **Security** type and create the **Password** of the guest network.
6. Select **Schedule** from the **Access Time** drop-down list and customize it for the guest network.
7. Click **Save**.

Guest Network

Allow Guests To Access My Local Network:	<input type="button" value="Disable"/>																																																																																																																																
Guest Network Isolation:	<input type="button" value="Disable"/>																																																																																																																																
Guest Network Bandwidth Control:	<input type="button" value="Disable"/>																																																																																																																																
Guest Network: <input checked="" type="radio"/> Enable <input type="radio"/> Disable Network Name: <input type="text" value="TP-Link_Guest_0969"/> Max Guests number: <input type="text" value="32"/> Security: <input type="button" value="WPA/WPA2 - Personal"/> Authentication Type: <input type="button" value="Auto"/> Encryption: <input type="button" value="Auto"/> Wireless Password: <input type="text" value="01234567"/> <small>(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)</small> Group Key Update Period: <input type="text" value="0"/> (seconds, minimum is 30, 0 means no update) Access Time: <input type="button" value="Schedule"/>																																																																																																																																	
<small>Click the schedule table or use the 'Add' button to choose the period on which you need the guest network off automatically!</small> <small>The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time Settings".</small>																																																																																																																																	
Wireless Schedule: <input type="radio"/> Enable <input checked="" type="radio"/> Disable																																																																																																																																	
Apply To	Start Time <input type="button" value="00:00"/> End Time <input type="button" value="24:00"/> Add																																																																																																																																
Each Day	<table border="1"> <tr> <td>Time</td> <td>0:00</td> <td>1:00</td> <td>2:00</td> <td>3:00</td> <td>4:00</td> <td>5:00</td> <td>6:00</td> <td>7:00</td> <td>8:00</td> <td>9:00</td> <td>10:00</td> <td>11:00</td> <td>12:00</td> <td>13:00</td> <td>14:00</td> </tr> <tr> <td>Sun.</td> <td></td> </tr> <tr> <td>Mon.</td> <td></td> </tr> <tr> <td>Tues.</td> <td></td> </tr> <tr> <td>Wed.</td> <td></td> </tr> <tr> <td>Thur.</td> <td></td> </tr> <tr> <td>Fri.</td> <td></td> </tr> <tr> <td>Sat.</td> <td></td> </tr> </table>	Time	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	Sun.																Mon.																Tues.																Wed.																Thur.																Fri.																Sat.															
Time	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																																																																																																																		
Sun.																																																																																																																																	
Mon.																																																																																																																																	
Tues.																																																																																																																																	
Wed.																																																																																																																																	
Thur.																																																																																																																																	
Fri.																																																																																																																																	
Sat.																																																																																																																																	
<input type="button" value="Clear Schedule"/>																																																																																																																																	
<input type="button" value="Save"/>																																																																																																																																	

- **Allow Guest To Access My Local Network** - If enabled, guests can access the local network and manage it.
- **Guest Network Isolation** - If enabled, guests are isolated from each other.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.

Note:

The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the [Bandwidth Control](#) page.

4. 6. DHCP

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

4.6.1. DHCP Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > DHCP Settings**.
3. Specify DHCP server settings and click **Save**.

DHCP Settings	
DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Lease Time:	120 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	0.0.0.0 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
<input type="button" value="Save"/>	

- **DHCP Server** - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

 Note:

- To use the DHCP server function of the router, you must configure all computers on the LAN as [Obtain an IP Address automatically](#).

4.6.2. DHCP Clients List

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

DHCP Clients List				
This page displays information of all DHCP clients on the network.				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camille	40:8D:5C:89:74:B5	192.168.0.100	00:00:32
2	iPhone	34:E2:FD:14:1D:0D	192.168.0.101	00:00:55

[Refresh](#)

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

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

4.6.3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > Address Reservation**.
3. Click [Add New](#) and fill in the blanks.

DHCP Address Reservation	
The static IP address of the DHCP Server can be configured on this page.	
MAC Address:	<input type="text"/>
IP Address:	<input type="text"/>
Status:	<input type="button" value="Disabled"/>
	<input type="button" value="Save"/> <input type="button" value="Back"/>

- 1) Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the **Status** as **Enabled**.
- 4) Click **Save**.

4.7. Forwarding

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

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

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

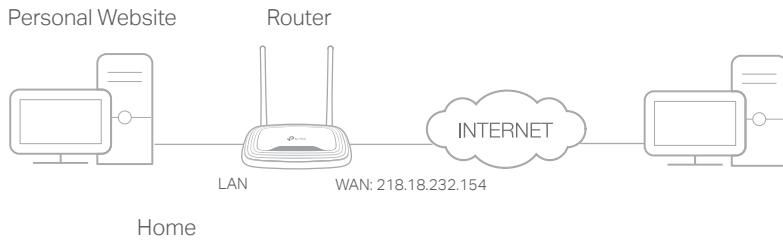
4.7.1. Virtual Server

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

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

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

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



1. Set your PC to a static IP address, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to **Forwarding > Virtual Server**.
4. Click **Add New**. Select **HTTP** from the **Common Service Port** list. The service port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the **IP Address** field.

Virtual Server	
Service Port:	<input type="text" value="80"/> (XX-XX or XX)
IP Address:	<input type="text" value="192.168.0.100"/>
Internal Port:	<input type="text" value="80"/> (XX or keep empty. If it's empty, internal port equals to Service port)
Protocol:	<input type="text" value="TCP"/>
Status:	<input type="text" value="Enabled"/>
Common Service Port:	<input type="text" value="HTTP"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

5. Leave the status as **Enabled** and click **Save**.

Note:

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

Done!

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

Note:

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

4.7.2. Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external

ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad, Quick Time 4 players and more.

Follow the steps below to configure the port triggering rules:

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Forwarding > Port Triggering**.
3. Click **Add New**. Select the desired application from the **Common Applications** list. The trigger port and incoming ports will be automatically filled in. The following picture takes application **MSN Gaming Zone** as an example.

Port Trigger	
Trigger Port:	47624 (XX)
Trigger Protocol:	ALL
Open Port:	2300-2400,28800-29 (XX or XX-XX or XX-XX,XX)
Open Protocol:	ALL
Status:	Enabled
Common Service Port:	MSN Gaming Zone

Save Back

4. Leave the status as **Enabled** and click **Save**.

■ Note:

- You can add multiple port triggering rules as needed.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the **Common Applications** list, please enter the parameters manually. You should verify the incoming ports the application uses first and enter them in **Incoming Ports** field. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

4.7.3. DMZ

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

■ Note:

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

I want to:

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

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [Forwarding > DMZ](#).
4. Select [Enable](#) and enter the IP address 192.168.0.100 in the [DMZ Host IP Address](#) filed.

The screenshot shows a configuration interface for a DMZ host. At the top, the word "DMZ" is written in blue. Below it, there's a section titled "Current DMZ Status" with two radio buttons: one for "Enable" (which is selected) and one for "Disable". Underneath this is a "DMZ Host IP Address" field containing the value "192.168.0.100". At the bottom right of the form is a "Save" button.

5. Click [Save](#).

Done!

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

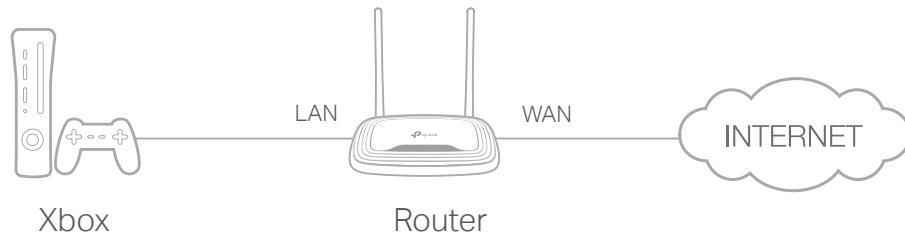
4.7.4. UPnP

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

» Tips:

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

For example, when you connect your Xbox to the router which is connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Forwarding > UPnP**.
3. Click **Disable** or **Enable** according to your needs.

4. 8. Security

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

4. 8. 1. Basic Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Basic Security**, and you can enable or disable the security functions.

Basic Security
Firewall Enable SPI Firewall: <input checked="" type="checkbox"/>
VPN PPTP Pass-through: <input checked="" type="radio"/> Enable <input type="radio"/> Disable L2TP Pass-through: <input checked="" type="radio"/> Enable <input type="radio"/> Disable IPSec Pass-through: <input checked="" type="radio"/> Enable <input type="radio"/> Disable
ALG FTP ALG: <input checked="" type="radio"/> Enable <input type="radio"/> Disable TFTP ALG: <input checked="" type="radio"/> Enable <input type="radio"/> Disable H323 ALG: <input checked="" type="radio"/> Enable <input type="radio"/> Disable SIP ALG: <input checked="" type="radio"/> Enable <input type="radio"/> Disable RTSP ALG: <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Save

- **Firewall** - A firewall protects your network from internet attacks.
 - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by default.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP or L2TP protocols to pass through the router's firewall.
 - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. If you want to allow PPTP tunnels to pass through the router, you can keep the default (Enabled).
 - **L2TP Passthrough** - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer 2 level. If you want to allow L2TP tunnels to pass through the router, you can keep the default (Enabled).
 - **IPSec Passthrough** - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. If you want to allow IPSec tunnels to pass through the router, you can keep the default (Enabled).

- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default **Enable**.
 - **SIP ALG** - To allow some multimedia clients to communicate across NAT, click **Enable**.
 - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

3. Click **Save**.

4.8.2. Advanced Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Advanced Security**, and you can protect the router from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood.

Advanced Security

DoS Protection: Enable Disable

Enable ICMP-Flood Attack Filtering
ICMP-Flood Packets Threshold (5~3600): packets/second

Enable UDP-Flood Attack Filtering
UDP-Flood Packets Threshold (5~3600) : packets/second

Enable TCP-SYN-Flood Attack Filtering
TCP-SYN-Flood Packets Threshold (5~3600) : packets/second

Forbid Ping Packet From WAN Port
 Forbid Ping Packet From LAN Port

Save **Blocked DOS Host List**

- **DoS Protection** - Denial of Service protection. Select **Enable** or **Disable** to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

Note:

Dos Protection will take effect only when the Statistics in [System Tool > Statistics](#) is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Tick the checkbox to enable or disable this function.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current ICMP-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Enable UDP-FLOOD Attack Filtering** - Tick the checkbox to enable this function.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the number of the current UPD-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Tick the checkbox to enable or disable this function.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current TCP-SYN-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Forbit Ping Packet From WAN Port** - The default setting is disabled. If enabled, the ping packet from the internet cannot access the router.
- **Forbid Ping Packet From LAN Port** - The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

3. Click **Save**.

4. Click **Blocked DoS Host List** to display the DoS host table by blocking.

4. 8. 3. Local Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Local Management**, and you can block computers on the LAN from accessing the router.

Local Management

Management Rules

All the PCs on the LAN are allowed to access the Router's Web-Based Utility
 Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC:

Your PC's MAC Address:

For example, if you want to allow PCs with specific MAC addresses to access the router's Web-based Utility locally from inside the network, please follow the instructions below:

- 1) Select Only the PCs listed can browse the built-in web pages to perform Administrator tasks.
- 2) Enter the MAC address of each PC separately. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). Only the PCs with the listed MAC addresses can use the password to browse the Web-based Utility to perform administrator tasks.
- 3) Click Set, and your PC's MAC address will also be listed.
- 4) Click Save.

■ Note:

If your PC is blocked but you want to access the router again, reset the router to the factory defaults.

4.8.4. Remote Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Security > Remote Management, and you can manage your router from a remote device via the internet.

The screenshot shows a configuration interface titled "Remote Management". It contains two input fields: "Web Management Port" with the value "80" and "Remote Management IP Address" with the value "0.0.0.0". A note next to the IP address field says "(Enter 255.255.255.255 for all)". At the bottom is a "Save" button.

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For higher security, you can change the remote management web port to a custom port by entering a number between 1 and 65534 but do not use the number of any common service port.
- **Remote Management IP Address** - This is the address you will use when accessing your router via a remote device. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function, change 0.0.0.0 to a valid IP address. If it is set to 255.255.255.255, then all the remote devices can access the router from the internet.

Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's Web-based Utility.
- Be sure to change the router's default password for security purposes.

4.9. Parental Controls

Parental Controls allows you to block inappropriate and malicious websites, and control access to specific websites at specific time for your children's devices.

For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Parental Controls.
3. Tick the **Enable Parental Controls** checkbox, enter the MAC address 00:11:22:33:44:BB in the **MAC Address of Parental PC** field and then click **Save**.

Parental Controls

Parental Controls can be used to administer all Internet activity including limiting usage and/or access to specific websites to all clients on the network for a specified period of time. The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Settings](#)".

Enable Parental Controls

MAC Address Of Parental PC:

MAC Address of Current PC:

4. Enter 00:11:22:33:44:AA in the **MAC Address 1** field.

MAC Address - 1:

MAC Address - 2:

MAC Address - 3:

MAC Address - 4:

MAC Address in current LAN: Copy to

5. Select **Each Week** from the **Apply To** drop-down list, and select **Sat**. Select **00:00** as the **Start Time** and Select **24:00** as the **End Time**. And then click **Add**.

Apply To: Each Week Start Time: 00:00 End Time: 24:00 Add

Mon. Tues. Wed. Thur. Fri. Sat. Sun.

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

Clear Schedule

6. Enter www.tp-link.com in the **Add URL** field. Click **Add**.

Add URL: www.tp-link.com Add

Details

Delete Selected (Will not take effect until you save these changes)

7. Click **Save**.

4. 10. Access Control

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

I want to: Deny or allow specific client devices to access my network with access time and content restrictions.

For example, if you want to restrict the internet activities of host with MAC address 00:11:22:33:44:AA on the LAN to access www.tp-link.com only, please follow the steps below:

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Access Control > Host** and configure the host settings:
 - 1) Click **Add New**.
 - 2) Select **MAC Address** as the mode type. Create a unique description (e.g. **host_1**) for the host in the **Description** field and enter 00:11:22:33:44:AA in the **MAC Address** field.

Add or Edit A Host Entry

Mode:

Description:

MAC Address:

3) Click [Save](#).

3. Go to [Access Control > Target](#) and configure the target settings:

1) Click [Add New](#).

2) Select [URL Address](#) as the mode type. Create a unique description (e.g. [target_1](#)) for the target in the [Target Description](#) field and enter the domain name, either the full name or the keywords (for example TP-Link) in the [Add URL Address](#) field. And then Click [Add](#).

Note:

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

Add or Edit A Target Entry

Mode:

Description:

Add URL Address:

Detail

(Will not take effect until you save these changes)

3) Click [Save](#).

4. Go to [Access Control > Schedule](#) and configure the schedule settings:

1) Click [Add New](#).

2) Create a unique description (e.g. [schedule_1](#)) for the schedule in the [Schedule Description](#) field and set the day(s) and time period. And then click [Add](#).

Add or Edit A Schedule Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Settings](#)".

Description:	Schedule_1														
Apply To:	Each Day	Start Time	00:00	End Time	24:00	Add									
Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

[Clear Schedule](#)

[Save](#) [Back](#)

3) Click [Save](#).

5. Go to [Access Control](#) > [Rule](#) and add a new access control rule.
 - 1) Click [Add New](#).
 - 2) Give a name for the rule in the [Description](#) field. Select [host_1](#) from the LAN host drop-down list; select [target_1](#) from the target drop-down list; select [schedule_1](#) from the schedule drop-down list.

Add Internet Access Control Entry

Description:	rule_1	
LAN Host:	host_1	Add LAN Host
Target:	target_1	Add Target
Schedule:	Schedule_1	Add Schedule
Rule:	Allow	
Status:	Enabled	
Direction:	IN	
Protocol:	ALL	

[Save](#) [Back](#)

3) Leave the status as [Enabled](#) as click [Save](#).

6. Select [Enable Internet Access Control](#) to enable Access Control function.

7. Select Allow the packets specified by any enabled access control policy to pass through the Router as the default filter policy and click Save.

The screenshot shows the 'Access Control Rule Management' page. It includes a note about restricting Internet activity for LAN hosts and managing network effectively. A checkbox for 'Enable Internet access control' is checked. Under 'Default Filtering Rules', there are two options: 'Allow the packets not specified by any filtering rules to passthrough this device.' (selected) and 'Deny the packets not specified by any filtering rules to passthrough this device.' A 'Save' button is at the bottom.

Done!

Now only the specific host(s) can visit the target(s) within the scheduled time period.

4.11. Advanced Routing

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

4.11.1. Static Route List

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Advanced Routing > Static Route List.
 - To add static routing entries:
 1. Click Add New.
 2. Enter the following information.

The screenshot shows the 'Static Route' configuration page. It has fields for Destination IP Address, Subnet Mask, Gateway, Interface (optional), and Status (Enabled). At the bottom are 'Save' and 'Back' buttons.

- **Destination IP Address** - The Destination Network is the address of the network or host that you want to assign to a static route.

- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
 - **Gateway** - This is the IP address of the default gateway device that allows the contact between the router and the network or host.
 - **Interface** - It is empty by default. Please select a connection from the dropdown list if the Gateway is left empty or is not on the same network segment as LAN/WAN interface.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click **Save**.

4.11.2. System Routing Table

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Advanced Routing > System Routing Table**, and you can view all the valid route entries in use.

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
Refresh				

- **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), or the WAN (Internet).

Click **Refresh** to refresh the data displayed.

4.12. Bandwidth Control

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Bandwidth Control**.
3. Tick the **Enable Bandwidth Control** checkbox, and configure the **Egress Bandwidth** and **Ingress Bandwidth**, and then click **Save**. The **Egress/Ingress Bandwidth** is the

upload/download speed through the WAN port. The value should be less than 100,000Kbps.

The screenshot shows a configuration page titled "Bandwidth Control". It has a checkbox labeled "Enable Bandwidth Control" which is checked. Below it are two input fields: "Egress Bandwidth" set to 512 Kbps and "Ingress Bandwidth" set to 2048 Kbps. At the bottom is a "Save" button.

4. Click [Add New](#), fill in the blanks and click [Save](#).

The screenshot shows a more detailed configuration page for "Bandwidth Control". It includes fields for "Enable" (checked), "IP Range" (two input fields), "Port Range" (two input fields), "Protocol" (a dropdown menu showing "ALL"), "Priority" (a dropdown menu showing "5" with a note "(1 meaning highest priority)", "Min Bandwidth(Kbps)" and "Max Bandwidth(Kbps)" fields for both "Egress Bandwidth" and "Ingress Bandwidth". At the bottom are "Save" and "Back" buttons.

- **IP Range** - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are ALL, TCP, UDP.
- **Priority** - Priority of Bandwidth Control rules. '1' stands for the highest priority while '8' stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port.

4. 13. IP & MAC Binding

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

4. 13. 1. Binding Settings

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

The screenshot shows a web-based configuration interface for 'Binding Settings'. At the top, it says 'Binding Settings'. Below that, there is a section for 'ARP Binding' with two radio buttons: 'Enable' (selected) and 'Disable'. A 'Save' button is located to the right of the binding settings area.

- To add IP & MAC Binding entries:

1. Click Add New.
2. Enter the MAC address and IP address.
3. Tick the Bind checkbox and click Save.

The screenshot shows the 'Binding Settings' page with a note: 'This page allows you to set IP-MAC Binding entries.' It has fields for 'MAC Address' and 'IP Address', both with empty input boxes. There is also a 'Bind' checkbox which is checked. At the bottom are 'Save' and 'Back' buttons.

- To modify or delete an existing entry:

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

4. 13. 2. ARP List

To manage a device, you can observe the device on the LAN by checking its MAC address and IP address on the ARP list, and you can also configure the items. This page displays the ARP list which shows all the existing IP & MAC Binding entries.

ARP List				
	MAC Address	IP Address	Status	
<input type="checkbox"/>	00:E0:4C:00:07:BE	192.168.0.4	Bound	
<input type="checkbox"/>	40:8D:5C:89:74:B5	192.168.0.100	Unloaded	

[Load Selected](#) [Delete Selected](#)

[Refresh](#)

- **MAC Address** - The MAC address of the listed computer on the LAN.
- **IP Address** - The assigned IP address of the listed computer on the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - Load or delete an item.
 - **Load** - Load the item to the IP & MAC Binding list.
 - **Delete** - Delete the item.
- Click the **Load Selected** button to load the selected items to the IP & MAC Binding list.
- Click the **Delete Selected** button to delete the selected items to the IP & MAC Binding list.
- Click the **Refresh** button to refresh all items.

 Note:

An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, **Load All** only loads the items without interference to the IP & MAC Binding list.

4. 14. Dynamic DNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address. Thus your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.noip.com. The Dynamic DNS client service provider will give you a password or key.

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

Dyndns DDNS

If the dynamic DNS Service Provider you select is www.dyn.com, the following page will appear.

The screenshot shows the 'DDNS Settings' page for the 'DynDNS (dyn.com/dns)' service provider. The page includes fields for 'Domain Name', 'Username', and 'Password'. It also features an 'Enable DDNS' checkbox, which is currently unchecked, and a 'Connection Status' indicator showing 'Disconnected'. At the bottom are 'Login', 'Logout', and 'Save' buttons.

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** you received from dynamic DNS service provider here.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Click **Login**.
5. Click **Save**.
 - **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Logout** - Click **Logout** to log out of the DDNS service.

No-IP DDNS

If the dynamic DNS Service Provider you select is www.noip.com, the following page will appear.

The screenshot shows the 'DDNS Settings' page for the 'No-IP (www.noip.com)' service provider. The page includes fields for 'Domain Name', 'Username', and 'Password'. It also features an 'Enable DDNS' checkbox, which is currently unchecked, and a 'Connection Status' indicator showing 'Disconnected'. At the bottom are 'Login', 'Logout', and 'Save' buttons.

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** you received from dynamic DNS service provider.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Click **Login**.
5. Click **Save**.
 - **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Logout** - Click **Logout** to log out of the DDNS service.

Comexe DDNS

If the dynamic DNS Service Provider you select is www.comexe.cn, the following page will appear.

DDNS Settings

Service Provider:	<input type="text" value="Comexe (www.comexe.cr)"/> Go to register...
Domain Name1:	<input type="text"/>
Domain Name2:	<input type="text"/>
Domain Name3:	<input type="text"/>
Domain Name4:	<input type="text"/>
Domain Name5:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
Enable DDNS:	<input type="checkbox"/>
Connection Status:	Disconnected
<input type="button" value="Login"/> <input type="button" value="Logout"/>	
<input type="button" value="Save"/>	

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** received from your dynamic DNS service provider.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Click **Login**.
5. Click **Save**.
 - **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Logout** - Click **Logout** to log out of the DDNS service.

4. 15. IPv6

This function allows you to enable IPv6 function and set up the parameters of the router's Wide Area Network (WAN) and Local Area Network (LAN).

4. 15. 1. IPv6 Status

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

IPv6 Status	
WAN	Connection Type: Disabled
IPv6 LAN	IPv6 Address Type: RADVD Prefix Length: 64 IPv6 Address: N/A

- **WAN** - This section shows the current IPv6 **Connection Type**.
- **TPv6 LAN** - This section shows the current IPv6 information of the router's LAN port, including **IPv6 Address Type**, **Prefix Length** and **IPv6 Address**.

4. 15. 2. IPv6 WAN

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

The screenshot shows the 'IPv6 WAN' configuration interface. At the top, 'Enable IPv6' is checked and 'Connection Type' is set to 'Dynamic IPv6'. Below this, 'IPv6 Address' is shown as '::', 'Prefix Length' as '0', and 'IPv6 Gateway' as '::'. The 'Addressing Type' dropdown is set to 'DHCPv6'. A note below says '(1500 as default, do not change unless necessary)'. There are checkboxes for 'Enable MLD Proxy' and 'Set IPv6 DNS Server manually', both of which are unchecked. The 'Host Name' field contains a redacted value. At the bottom right is a 'Save' button.

3. Select the **WAN Connection Type** and fill in the blanks according to your ISP, and then click **Save**.
 - **Dynamic IPv6** - Connections which use dynamic IPv6 address assignment.
 - **Static IPv6** - Connections which use static IPv6 address assignment.
 - **PPPoEv6** - Connections which use PPPoEv6 that requires a username and password.
 - **Tunnel 6to4** - Connections which use 6to4 address assignment.

Dynamic IPv6

This screenshot is identical to the one above, showing the 'IPv6 WAN' configuration with 'Dynamic IPv6' selected as the connection type. The fields for IPv6 Address, Prefix Length, and IPv6 Gateway are all set to their default values of '::'. The MTU is set to 1500 bytes. The Addressing Type is set to 'DHCPv6'. The Host Name field is redacted. The 'Save' button is at the bottom right.

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the

MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

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

 **Note:**

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

Static IPv6



The screenshot shows the 'IPv6 WAN' configuration page. The 'Enable IPv6' checkbox is checked. The 'Connection Type' dropdown is set to 'Static IPv6'. The 'IPv6 Address' field contains a placeholder IP address. The 'Prefix Length' field is set to 64. The 'IPv6 Gateway' field is empty and marked as optional. The 'IPv6 DNS Server' and 'Secondary IPv6 DNS Server' fields are empty and marked as optional. Below these fields, there is a note: 'MTU(Bytes): 1500 (1500 as default, do not change unless necessary)'. The 'Enable MLD Proxy' checkbox is unchecked. At the bottom right is a 'Save' button.

- **IPv6 Address** - Enter the IPv6 address provided by your ISP.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **IPv6 DNS Server** - Enter the DNS IPv6 address provided by your ISP.
- **Secondary IPv6 DNS Server** - Enter another DNS IPv6 address provided by your ISP.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

PPPoEv6

IPv6 WAN

Enable IPv6:

Connection Type: **PPPoEv6**

PPPoE same session with IPv4 connection

PPP Username:

PPP Password:

Confirm password:

Authentication Type: **AUTO_AUTH**

Addressing Type: **DHCPv6**

Service Name: (do not change unless necessary)

Server Name: (do not change unless necessary)

MTU(Bytes): **1480** (1480 as default, do not change unless necessary)

Enable MLD Proxy:

Use IPv6 address specified by ISP:

Set IPv6 DNS Server manually:

Save

- PPP Username/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Authentication Type** – Choose one authentication type from AUTO-AUTH, PAP, CHAP and MS-CHAP.
- Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1480 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- Use IPv6 address specified by ISP** - Input a static IPv6 address from the ISP.
- Set IPv6 DNS Server manually** - Enter the IP address of the IPv6 DNS server and secondary IPv6 DNS server.

Tunnel 6to4

IPv6 WAN

Enable IPv6:

Connection Type: **Tunnel 6to4**

WAN Connection: **[REDACTED]**

Save

- **WAN Connection** - Display the available wan connection.

4. 15. 3. IPv6 LAN

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 LAN** and configure the IPv6 LAN settings as needed.

The parameters of IPv6 LAN can be configured on this page when IPv6 enabled.
Note: Only the default group will support IPv6 at this moment.

Group: Default

Address Auto-Configuration Type: RADVD DHCPv6 Server

Enable RDNSS:

Enable ULA Prefix:

Site Prefix Configuration Type: Delegated Static

Prefix Delegated WAN Connection: No available interface.

Save

- **Address Auto-Configuration Type** - Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided.
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the **Site Prefix** and **Site Prefix Length** manually. Please contact your ISP to get more information before you configure them.

 Note:

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

4. 16. System Tools

4. 16. 1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

2. Go to System Tools > Time Settings.

The screenshot shows the 'Time Settings' configuration page. At the top, it says 'Time Settings'. Below that, there are sections for 'Time Zone', 'Date', 'Time', 'NTP Server 1', 'NTP Server 2', and 'Daylight Saving'. The 'Time Zone' dropdown is set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'. The 'Date' section has fields for Year (1970), Month (1), and Day (1). The 'Time' section has fields for Hour (0), Minute (28), and Second (46). There are also 'Get from PC' and 'Get GMT' buttons. The 'NTP Server 1' and 'NTP Server 2' fields are both empty and labeled '(optional)'. Below these, there are dropdown menus for 'Start' (Mar, Last, Sun, 01:00) and 'End' (Oct, Last, Sun, 02:00). A 'Save' button is located at the bottom right of each section.

- To set time manually:**

1. Select your local [Time Zone](#).
2. Enter the [Date](#) in Month/Day/Year format.
3. Enter the [Time](#) in Hour/Minute/Second format.
4. Click [Save](#).

- To set time automatically:**

5. Select your local [Time Zone](#).
6. Enter the address or domain of the [NTP Server 1](#) or [NTP Server 2](#).
7. Click [Get GMT](#) to get time from the internet if you have connected to the internet.

- To set Daylight Saving Time:**

1. Select [Enable Daylight Saving](#).
2. Select the start time from the drop-down list in the [Start](#) fields.
3. Select the end time from the drop-down list in the [End](#) fields.
4. Click [Save](#).

Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

4.16.2. Diagnostic

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

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

The screenshot shows the 'Diagnostic Tools' page with 'Diagnostic Parameters'. It includes fields for IP address/Domain name, Ping Count (4), Ping Packet Size (64), Ping Timeout (1), and Traceroute Max TTL (20). A 'Start' button is visible.

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

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- **Ping Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

3. Click **Start** to check the connectivity of the internet.
4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

Diagnostic Results

```
Pinging 192.168.0.1 with 64 bytes of data:
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4

Ping statistics for 192.168.0.1
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1
```

4.16.3. Firmware Upgrade

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

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

Firmware Upgrade

Firmware File Path:	Choose File	No file chosen
Firmware version:	<input type="text"/>	
Hardware version:	<input type="text"/>	
Upgrade		

4.16.4. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.

Factory Defaults

Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults.

[Restore](#)

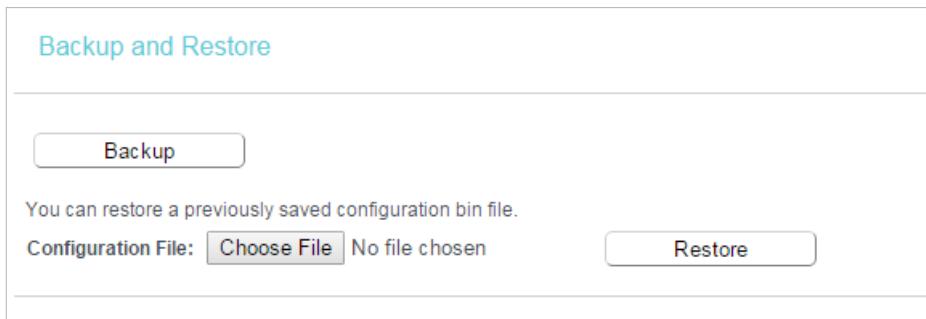
- Default [Username](#): admin

- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

4. 16. 5. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

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



- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

■ Note:

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

4. 16. 6. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

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

- **To reboot the router manually:**

Click **Reboot**, and wait a few minutes for the router to rebooting.

The screenshot shows a web-based configuration interface for a router. The title bar says "System Reboot". Below it is a message: "Click Reboot to restart the device without applying any changes to your current settings." At the bottom is a large blue "Reboot" button.

- **To set the router reboot every a couple of hours:**

1. Select **Timeout** from the **Auto Reboot Time** drop-down list.
2. Specify a time interval. The router will reboot automatically after every this interval.
3. Click **Save**.

The screenshot shows the same "System Reboot" page as before, but with additional settings for scheduled reboots. It includes fields for "Auto Reboot Time" (set to "Timeout"), "Hours" (1), and "Minutes" (0). There is also a "Remaining Time" display and a "Save" button at the bottom.

- **To schedule the router to reboot at a specific time:**

1. Select **Schedule** from the **Auto Reboot Time** drop-down list.
2. Specify the **Day(s)** and **Time** for the router to reboot.
3. Click **Save**.

System Reboot

Click Reboot to restart the device without applying any changes to your current settings.

Reboot

Auto Reboot Time: **Schedule**

Day: Everyday Select Days
 Mon Tue Wed Thu Fri Sat Sun

Time: **00** **00** (Hour:Minute)

The Schedule is based on the time of the Router.
The time can be set in "System Tools -> [Time Settings](#)".

Save

4. 16. 7. Password

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Password**, and you can change the factory default username and password of the router.

Password

Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:

Old Password:

New User Name:

New Password:

Confirm password:

Save **Clear All**

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

■ Note:

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

3. Click **Save**.

4.16.8. System Log

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

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

Refresh Clear Log Save Log Log Settings

- Log Type** - By selecting the log type, only logs of this type will be shown.
- Log Level** - By selecting the log level, only logs of this level will be shown.
- Refresh** - Refresh the page to show the latest log list.
- Clear Log** - All the logs will be deleted from the router permanently, not just from the page.

4.16.9. Statistics

- Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
- Go to **System Tools > Traffic Statistics**.
- Select **Enable** and click **Save**. You can view the network traffic of each PC on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.

IP Address MAC Address	Total		Current					Operation
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
	Current list is blank							

Reset All Delete All Refresh

4.17. Logout

Click **Logout** at the bottom of the main menu, and you will log out of the Web-based Utility and return to the login window.

Chapter 5

Configure the Router in WISP Mode

This chapter presents how to configure the various features of the router working in WISP mode.

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [Guest Network](#)
- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Controls](#)
- [Access Control](#)
- [Advanced Routing](#)
- [Bandwidth Control](#)
- [IP & MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6](#)
- [System Tools](#)
- [Logout](#)

5. 1. Status

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. The default one is **admin** (all lowercase) for both username and password.
2. Go to **Status**. You can view the current status information of the router.

The screenshot shows the 'Status' page of a TP-Link router. It includes sections for Firmware Version, LAN, Wireless 2.4GHz, and WAN, along with system status and refresh controls at the bottom.

Status	
Firmware Version:	[REDACTED]
Hardware Version:	[REDACTED]

LAN	
MAC Address:	00:0A:EB:11:14:0A
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0

Wireless 2.4GHz	
Operation Mode:	WISP
Wireless Radio:	Enabled
Name(SSID):	TP-Link_140A
Mode:	11bgn mixed
Channel:	6
Channel Width:	Auto
MAC Address:	00:0A:EB:11:14:0A

WAN	
MAC Address:	00:0A:EB:11:14:0B
IP Address:	0.0.0.0(Dynamic IP)
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
DNS Server:	0.0.0.0 0.0.0.0

System Up Time: 0 day(s) 00:06:18

- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the [Network > LAN](#) page.
 - **MAC address** - The physical address of the router.
 - **IP address** - The LAN IP address of the router.
 - **Subnet Mask** - The subnet mask associated with the LAN IP address.
- **Wireless** - This field displays the basic information or status of the wireless function, and you can configure them on the [Wireless > Basic Settings](#) page.
 - **Operation Mode** - The current wireless working mode in use.

- **Wireless Radio** - Indicates whether the wireless radio feature of the router is enabled or disabled.
 - **Name(SSID)** - The SSID of the router.
 - **Mode** - The current wireless mode which the router works on.
 - **Channel** - The current wireless channel in use.
 - **Channel Width** - The current wireless channel width in use.
 - **MAC Address** - The physical address of the router.
- **WAN** - This field displays the current settings of the WAN, and you can configure them on the [Network > WAN](#) page.
 - **MAC Address** - The physical address of the WAN port.
 - **IP Address** - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no internet connection.
 - **Subnet Mask** - The subnet mask associated with the WAN IP Address.
 - **Default Gateway** - The Gateway currently used is shown here. When you use Dynamic IP as the internet connection type, click [Renew](#) or [Release](#) here to obtain new IP parameters dynamically from the ISP or release them.
 - **DNS Server** - The IP addresses of DNS (Domain Name System) server.
 - **System Up Time** - The length of the time since the router was last powered on or reset.

Click [Refresh](#) to get the latest status and settings of the router.

5.2. Operation Mode

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Operation Mode](#).
3. Select the working mode as **WISP** and click **Save**.

Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

Save

5.3. Network

5.3.1. WAN

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

Dynamic IP

If your ISP provides the DHCP service, please select **Dynamic IP**, and the router will automatically get IP parameters from your ISP.

Click **Renew** to renew the IP parameters from your ISP.

Click **Release** to release the IP parameters.

The screenshot shows the 'WAN Settings' configuration page. The 'Connection Type' dropdown is set to 'Dynamic IP'. Below it, there are fields for 'IP Address', 'Subnet Mask', and 'Gateway', each containing placeholder text. Underneath these are two buttons: 'Renew' and 'Release'. Further down, there's a field for 'MTU(Bytes)' with a value of '1500' and a note '(1500 as default, do not change unless necessary)'. There are also checkboxes for 'Get IP with Unicast' and 'Set DNS server manually'. A 'Host Name' input field is present. At the bottom right is a 'Save' button.

- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Get IP with Unicast** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (It is rarely required.)
- **Set DNS server manually** - If your ISP gives you one or two DNS addresses, select Set DNS server manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned automatically from your ISP.
- **Host Name** - This option specifies the name of the router.

Static IP

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

The screenshot shows the 'WAN Settings' configuration page. At the top, the 'Connection Type' dropdown is set to 'Static IP' with a 'Detect' button next to it. Below this, there are fields for 'IP Address' (0.0.0.0), 'Subnet Mask' (0.0.0.0), 'Gateway' (0.0.0.0), 'Primary DNS Server' (0.0.0.0), and 'Secondary DNS Server' (0.0.0.0) which is noted as optional. An 'MTU(Bytes)' field is set to 1500 with a note that it's 1500 as default and should not be changed unless necessary. A 'Save' button is at the bottom.

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- **Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary/Secondary DNS Server** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.

PPPoE

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

The screenshot shows the 'WAN Settings' configuration page for PPPoE. Key fields include:

- Connection Type:** Set to PPPoE.
- PPP Username:** [Input field]
- PPP Password:** [Input field]
- Confirm password:** [Input field]
- Secondary Connection:** Radio button set to 'Disabled'.
- Connection Mode:** Radio button set to 'Always on'.
- Max Idle Time:** Set to 15 minutes.
- Authentication Type:** Set to AUTO_AUTH.
- Advanced Settings:** Includes fields for Service Name, Server Name, MTU (1480), Use IP address specified by ISP, Echo request interval (0), and Set DNS server manually.
- Buttons:** 'Connect' and 'Disconnect' buttons at the bottom of the main section, and a 'Save' button at the bottom of the advanced section.

- **PPP Username/Password** - Enter the user name and password provided by your ISP. These fields are case-sensitive.
- **Confirm Password** - Enter the Password provided by your ISP again to ensure the password you entered is correct.
- **Secondary Connection** - It's available only for PPPoE connection. If your ISP provides an extra connection type, select **Dynamic IP** or **Static IP** to activate the secondary connection.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically

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

- **Authentication Type** - Choose an authentication type.

■ Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

- **Service Name/Server Name** - The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **MTU(Bytes)** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Use IP Address Specified by ISP** - If your ISP does not automatically assign IP addresses to the router, please select this item and enter the IP address provided by your ISP in dotted-decimal notation.
- **Echo Request Interval** - The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.
- **Set DNS Server Manually** - If your ISP does not automatically assign DNS addresses to the router, please select this item and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

L2TP

If your ISP provides L2TP connection, please select [L2TP](#).

WAN Settings

Connection Type:	<input type="button" value="L2TP"/> <input type="button" value="Detect"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	
Addressing Type:	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
Server IP Address/Name:	<input type="text"/>
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS Server:	0.0.0.0, 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0, 0.0.0.0
MTU(Bytes):	<input type="text" value="1460"/> (1460 as default, do not change unless necessary)
Connection Mode:	<input checked="" type="radio"/> Always on <input type="radio"/> Connect on demand <input type="radio"/> Connect manually
Max Idle Time:	<input type="text" value="15"/> minutes (0 meaning connection remains active at all times)
<input type="button" value="Save"/>	

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Server IP Address/Name** - Enter server IP address or domain name provided by your ISP.
- **MTU(Bytes)** - The default MTU size is 1460 bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

■ Note:

Sometimes the connection cannot be terminated although you have specified the **Max Idle Time** because some applications are visiting the internet continually in the background.

PPTP

If your ISP provides PPTP connection, please select **PPTP**.

The screenshot shows the 'WAN Settings' configuration page for a PPTP connection. The 'Connection Type' is set to 'PPTP'. The 'Addressing Type' is set to 'Dynamic IP'. The 'Server IP Address/Name' field contains '0.0.0.0'. Below it, the 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS Server' fields all show '0.0.0.0'. The 'Internet IP Address' and 'Internet DNS' fields also show '0.0.0.0'. The 'MTU(Bytes)' field is set to '1420'. The 'Connection Mode' is set to 'Always on'. The 'Max Idle Time' field is set to '15 minutes'. A 'Save' button is located at the bottom right.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Server IP Address/Name** - Enter server IP address or domain name provided by your ISP.
- **MTU(Bytes)** - The default MTU size is 1420 bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically.

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

Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

BigPond Cable

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

The screenshot shows the 'WAN Settings' configuration page. At the top, the 'Connection Type' is set to 'BigPond Cable' with a 'Detect' button. Below this are fields for 'Username' and 'Password'. Under 'Auth Server' and 'Auth Domain', there are empty input fields. The 'MTU(Bytes)' field is set to '1500' with a note '(1500 as default, do not change unless necessary)'. The 'Connection Mode' section contains three radio buttons: 'Always on' (selected), 'Connect on demand', and 'Connect manually'. The 'Max Idle Time' field is set to '15' minutes. At the bottom are 'Connect' and 'Disconnect' buttons, and a 'Save' button.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
- **MTU(Bytes)** - The default MTU size is 1500 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Connection Mode**
 - **Always on** - In this mode, the internet connection will be active all the time.
 - **Connect on demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on demand** mode. The internet connection can be disconnected automatically

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

5.3.2. LAN

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

The screenshot shows the 'LAN Settings' configuration page. It includes fields for MAC Address (00:0A:EB:13:09:69), IP Address (192.168.0.1), and Subnet Mask (255.255.255.0). A 'Save' button is located at the bottom right.

- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router (the default one is 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

■ Note:

- If you have changed the IP address, you must use the new IP address or <http://tplinkwifi.net> to log in.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

5.3.3. MAC Clone

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

The screenshot shows the 'MAC Clone' configuration page. It includes fields for WAN MAC Address (00:0A:EB:13:09:6A), Your PC's MAC Address (40:8D:5C:89:74:B5), and buttons for 'Restore Factory MAC' and 'Clone MAC Address'. A 'Save' button is located at the bottom right.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address in this field. Click [Restore Factory MAC](#) to restore the MAC address of WAN port to the factory default value.
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click [Clone MAC Address](#) and this MAC address will be filled in the [WAN MAC Address](#) field.

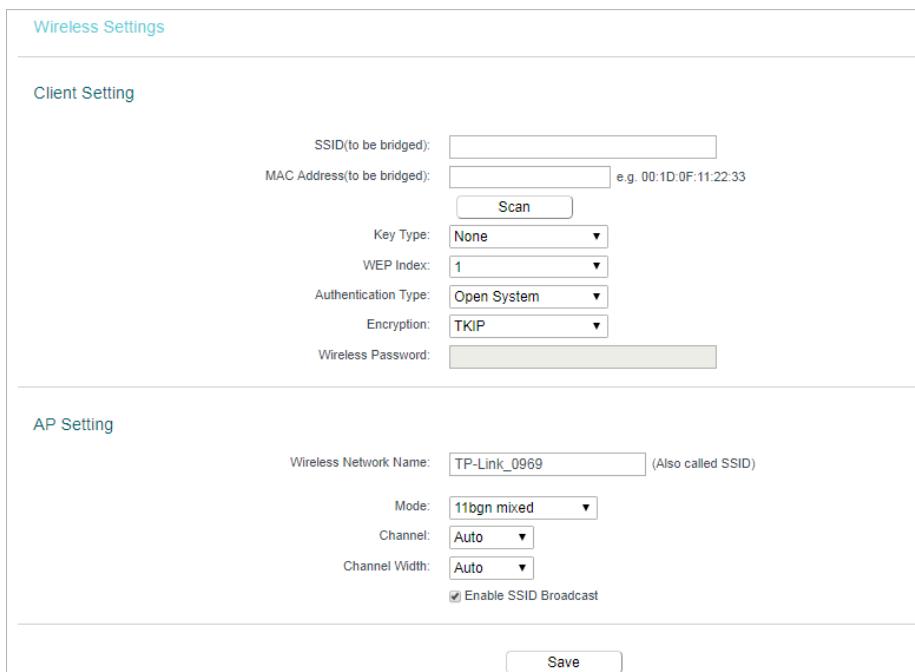
 Note:

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

5. 4. Wireless

5. 4. 1. Wireless Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Wireless > Basic Settings](#).
3. Click [Scan](#), select the client's network from the [AP List](#) and click [Conenct](#).
4. Enter the selected network's wireless password in the [Password](#) field.
5. Configure the AP settings for the wireless network and click [Save](#).



The screenshot shows the 'Wireless Settings' page with two main sections: 'Client Setting' and 'AP Setting'.

Client Setting

- SSID(to be bridged):
- MAC Address(to be bridged): e.g. 00:1D:0F:11:22:33
Scan
- Key Type: None
- WEP Index: 1
- Authentication Type: Open System
- Encryption: TKIP
- Wireless Password:

AP Setting

- Wireless Network Name: TP-Link_0969 (Also called SSID)
- Mode: 11bgn mixed
- Channel: Auto
- Channel Width: Auto
- Enable SSID Broadcast

Save

- **Wireless Network Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

- **Mode** - You can choose the appropriate "Mixed" mode.
- **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select **Auto**, then AP will choose the best channel automatically.
- **Enable SSID Broadcast** - If enabled, the router will broadcast the wireless network name (SSID).

5.4.2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router's network quickly via WPS.

■ Note:

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

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

Method ONE: Press the WPS Button on Your Client Device

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

WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 12345670
 Disable device PIN

Add a new device:

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

The screenshot shows the 'WPS Settings' page. It contains two radio button options: one for entering a new device PIN and another for pressing the WPS button on the client device. Below these options is a text input field labeled 'PIN'. At the bottom right are two buttons: 'Connect' and 'Back'.

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

Method TWO: Enter the Client's PIN

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

The screenshot shows the 'WPS (Wi-Fi Protected Setup)' page. It displays the current WPS status as 'Enabled' with a 'Disable' button. Below it is a 'Current PIN' field containing '12345670' with 'Restore PIN' and 'Generate New PIN' buttons. There is also a checked checkbox for 'Disable device PIN'. At the bottom are buttons for 'Add a new device' and 'Add device'.

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

The screenshot shows the 'WPS Settings' page again, but this time the radio button for 'Enter new device PIN' is selected. The 'PIN' field is empty. Below it is the option to 'Press the WPS button of the new device within the next two minutes'. At the bottom right are 'Connect' and 'Back' buttons.

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

Method Three: Enter the Router's PIN

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

WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 12345670
 Disable device PIN

Add a new device:

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

5.4.3. Wireless Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Security**.
3. Configure the security settings of your wireless network and click **Save**.

Wireless Security Settings

Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled.
For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption.

Disable Wireless Security
 WPA/WPA2 - Personal(Recommended)
 WPA/WPA2 - Enterprise
 WEP

Version: WPA2-PSK
Encryption: AES
Wireless Password: 12345670
Group Key Update Period: 0

Version: Auto
Encryption: Auto
RADIUS Server IP:
RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)
RADIUS Server Password:
Group Key Update Period: 0

Authentication Type: Open System
WEP Key Format: Hexadecimal
Selected Key: WEP Key
Key 1:
Key 2:
Key 3:
Key 4:

- **Disable Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router without a password. It's strongly recommended to choose one of the following modes to enable security.

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

5.4.4. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

I want to:

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

For example, you want the wireless client A with the MAC address 00:0A:EB:B0:00:0B and the wireless client B with the MAC address 00:0A:EB:00:07:5F to access the router, but other wireless clients cannot access the router

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless MAC Filtering**.
3. Click **Enable** to enable the Wireless MAC Filtering function.
4. Select **Allow the stations specified by any enabled entries in the list to access** as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click **Add New** and fill in the blank.

The screenshot shows a configuration interface for adding a new MAC filtering entry. The title bar says "Add or Modify Wireless MAC Address Filtering entry". Below it, a message states: "You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page." There are three input fields: "MAC Address" containing "00:0A:EB:B0:00:0B", "Description" containing "Client A", and "Status" set to "Enabled". At the bottom are "Save" and "Back" buttons.

- 1) Enter the MAC address 00:0A:EB:B0:00:0B / 00:0A:EB:00:07:5F in the MAC Address field.
 - 2) Enter wireless client A/B in the Description field.
 - 3) Select **Enabled** in the Status drop-down list.
 - 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: Enabled

Filtering Rules

Deny the stations specified by any enabled entries in the list to access.
 Allow the stations specified by any enabled entries in the list to access.

	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	00:0A:EB:00:00:0B	Enabled	TP-Link_7AFF	client A	<input type="button" value="Edit"/>
<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	<input type="button" value="Edit"/>

Done!

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

5.4.5. Wireless Advanced

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Advanced**.
3. Configure the advanced settings of your wireless network and click **Save**.

Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

Wireless Advanced

Transmit Power:

Beacon Interval: (40-1000)

RTS Threshold: (1-2346)

Fragmentation Threshold: (256-2346)

DTIM Interval: (1-15)

Enable Short GI
 Enable Client Isolation
 Enable WMM

- **Transmit Power** - Select **High**, **Middle** or **Low** which you would like to specify for the router. **High** is the default setting and recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames

to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable Client Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

5.4.6. Wireless Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Statistics** to check the data packets sent and received by each client device connected to the router.

Wireless Stations Status					
Wireless Stations Currently Connected: 1					
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	TP-LINK_52C9E9

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

5.5. Guest Network

Guest Network allows you to provide Wi-Fi access for guests without disclosing your host network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network settings to ensure network security and privacy.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Guest Network**.
3. Enable the **Guest Network** function.
4. Create a network name for your guest network.
5. Select the **Security** type and create the **Password** of the guest network.
6. Select **Schedule** from the **Access Time** drop-down list and customize it for the guest network.
7. Click **Save**.

Guest Network

Allow Guests To Access My Local Network:	Disable
Guest Network Isolation:	Disable
Guest Network Bandwidth Control:	Disable
Guest Network:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Name:	TP-Link_Guest_0969
Max Guests number:	32
Security:	WPA/WPA2 - Personal
Authentication Type:	Auto
Encryption:	Auto
Wireless Password:	01234567 <small>(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)</small>
Group Key Update Period:	0 (seconds, minimum is 30, 0 means no update)
Access Time:	Schedule
<small>Click the schedule table or use the 'Add' button to choose the period on which you need the guest network off automatically! The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time Settings".</small>	
Wireless Schedule:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Apply To:	Each Day
Start Time:	00:00
End Time:	24:00
Time:	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
Sun.	
Mon.	
Tues.	
Wed.	
Thur.	
Fri.	
Sat.	
<input type="button" value="Clear Schedule"/>	<input type="button" value="Save"/>

- **Allow Guest To Access My Local Network** - If enabled, guests can access the local network and manage it.
- **Guest Network Isolation** - If enabled, guests are isolated from each other.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.

■ Note:

The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the [Bandwidth Control](#) page.

5. 6. DHCP

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

5. 6. 1. DHCP Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [DHCP > DHCP Settings](#).
3. Specify DHCP server settings and click **Save**.

DHCP Settings	
DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Lease Time:	120 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	0.0.0.0 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
Save	

- **DHCP Server** - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.

- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

■ Note:

- To use the DHCP server function of the router, you must configure all computers on the LAN as [Obtain an IP Address automatically](#).

5. 6. 2. DHCP Clients List

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

DHCP Clients List				
This page displays information of all DHCP clients on the network.				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camilie	40:8D:5C:89:74:B5	192.168.0.100	00:00:32
2	iPhone	34:E2:FD:14:1D:0D	192.168.0.101	00:00:55

[Refresh](#)

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

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

5.6.3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > Address Reservation**.
3. Click **Add New** and fill in the blanks.

The static IP address of the DHCP Server can be configured on this page.

MAC Address:	<input type="text"/>
IP Address:	<input type="text"/>
Status:	<input type="button" value="Disabled"/>

Save Back

- 1) Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the **Status** as **Enabled**.
- 4) Click **Save**.

5.7. Forwarding

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

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

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

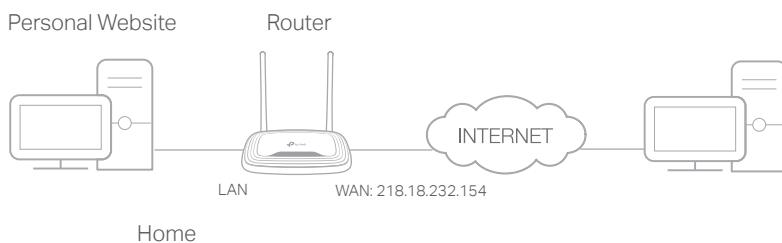
5.7.1. Virtual Server

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

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

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

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



1. Set your PC to a static IP address, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to **Forwarding > Virtual Server**.
4. Click **Add New**. Select **HTTP** from the **Common Service Port** list. The service port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the **IP Address** field.

Virtual Server	
Service Port:	<input type="text" value="80"/> (XX-XX or XX)
IP Address:	<input type="text" value="192.168.0.100"/>
Internal Port:	<input type="text" value="80"/> (XX or keep empty. If it's empty, internal port equals to Service port)
Protocol:	<input type="text" value="TCP"/>
Status:	<input type="text" value="Enabled"/>
Common Service Port:	<input type="text" value="HTTP"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

5. Leave the status as **Enabled** and click **Save**.

Note:

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

Done!

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

Note:

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

5.7.2. Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad, Quick Time 4 players and more.

Follow the steps below to configure the port triggering rules:

- Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
- Go to **Forwarding > Port Triggering**.
- Click **Add New**. Select the desired application from the **Common Applications** list. The trigger port and incoming ports will be automatically filled in. The following picture takes application **MSN Gaming Zone** as an example.

Port Trigger	
Trigger Port:	<input type="text" value="47624"/> (XX)
Trigger Protocol:	<input type="button" value="ALL"/>
Open Port:	<input type="text" value="2300-2400,28800-29"/> (XX or XX-XX or XX-XX,XX)
Open Protocol:	<input type="button" value="ALL"/>
Status:	<input type="button" value="Enabled"/>
Common Service Port:	<input type="button" value="MSN Gaming Zone"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

- Leave the status as **Enabled** and click **Save**.

Note:

- You can add multiple port triggering rules as needed.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the **Common Applications** list, please enter the parameters manually. You should verify the incoming ports the application uses first and enter them in **Incoming Ports** field. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

5.7.3. DMZ

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

Note:

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

I want to:

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

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to **Forwarding > DMZ**.
4. Select **Enable** and enter the IP address 192.168.0.100 in the **DMZ Host IP Address** filed.

DMZ	
Current DMZ Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DMZ Host IP Address:	192.168.0.100
Save	

5. Click **Save**.

Done!

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

5.7.4. UPnP

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

 **Tips:**

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

For example, when you connect your Xbox to the router which is connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Forwarding > UPnP**.
3. Click **Disable** or **Enable** according to your needs.

UPnP						
Current UPnP Status: <input checked="" type="button"/> Enabled <input type="button"/> Disable						
Current UPnP Settings List						
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
<input type="button"/> Refresh						

5.8. Security

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

5.8.1. Basic Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Security > **Basic Security**, and you can enable or disable the security functions.

The screenshot shows the 'Basic Security' configuration interface. It is divided into three main sections: Firewall, VPN, and ALG. The Firewall section contains an 'Enable SPI Firewall' checkbox which is checked. The VPN section contains three radio button groups for PPTP, L2TP, and IPSec Pass-through, all of which have 'Enable' selected. The ALG section contains five radio button groups for FTP, TFTP, H323, SIP, and RTSP ALG, all of which have 'Enable' selected. At the bottom right of the form is a 'Save' button.

- **Firewall** - A firewall protects your network from internet attacks.
 - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by default.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP or L2TP protocols to pass through the router's firewall.

- **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. If you want to allow PPTP tunnels to pass through the router, you can keep the default (Enabled).
- **L2TP Passthrough** - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer 2 level. If you want to allow L2TP tunnels to pass through the router, you can keep the default (Enabled).
- **IPSec Passthrough** - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. If you want to allow IPSec tunnels to pass through the router, you can keep the default (Enabled).
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default **Enable**.
 - **SIP ALG** - To allow some multimedia clients to communicate across NAT, click **Enable**.
 - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

3. Click **Save**.

5.8.2. Advanced Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Advanced Security**, and you can protect the router from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood.

Advanced Security

DoS Protection: Enable Disable

Enable ICMP-Flood Attack Filtering
ICMP-Flood Packets Threshold (5~3600): packets/second

Enable UDP-Flood Attack Filtering
UDP-Flood Packets Threshold (5~3600) : packets/second

Enable TCP-SYN-Flood Attack Filtering
TCP-SYN-Flood Packets Threshold (5~3600) : packets/second

Forbid Ping Packet From WAN Port
 Forbid Ping Packet From LAN Port

- **DoS Protection** - Denial of Service protection. Select **Enable** or **Disable** to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

 Note:

Dos Protection will take effect only when the Statistics in [System Tool > Statistics](#) is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Tick the checkbox to enable or disable this function.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current ICMP-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Enable UDP-FLOOD Attack Filtering** - Tick the checkbox to enable this function.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the number of the current UPD-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** -Tick the checkbox to enable or disable this function.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current TCP-SYN-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- **Forbit Ping Packet From WAN Port** - The default setting is disabled. If enabled, the ping packet from the internet cannot access the router.
- **Forbid Ping Packet From LAN Port** - The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

3. Click **Save**.

4. Click **Blocked DoS Host List** to display the DoS host table by blocking.

5.8.3. Local Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Local Management**, and you can block computers on the LAN from accessing the router.

The screenshot shows the 'Local Management' configuration page. Under 'Management Rules', the option 'Only the PCs listed' is selected. A MAC address input field contains '40:8D:5C:89:74:B5'. Below this, a table lists a single entry: 'Your PC's MAC Address: 40:8D:5C:89:74:B5'. At the bottom are 'Set' and 'Save' buttons.

For example, if you want to allow PCs with specific MAC addresses to access the router's Web-based Utility locally from inside the network, please follow the instructions below:

- 1) Select **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**.
- 2) Enter the MAC address of each PC separately. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). Only the PCs with the listed MAC addresses can use the password to browse the Web-based Utility to perform administrator tasks.
- 3) Click **Set**, and your PC's MAC address will also be listed.
- 4) Click **Save**.

■ Note:

If your PC is blocked but you want to access the router again, reset the router to the factory defaults.

5.8.4. Remote Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security > Remote Management**, and you can manage your router from a remote device via the internet.

Remote Management

Web Management Port:

Remote Management IP Address: (Enter 255.255.255.255 for all)

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For higher security, you can change the remote management web port to a custom port by entering a number between 1 and 65534 but do not use the number of any common service port.
- **Remote Management IP Address** - This is the address you will use when accessing your router via a remote device. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function, change 0.0.0.0 to a valid IP address. If it is set to 255.255.255.255, then all the remote devices can access the router from the internet.

■ Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's Web-based Utility.
- Be sure to change the router's default password for security purposes.

5.9. Parental Controls

Parental Controls allows you to block inappropriate and malicious websites, and control access to specific websites at specific time for your children's devices.

For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Parental Controls.
3. Tick the **Enable Parental Controls** checkbox, enter the MAC address 00:11:22:33:44:BB in the **MAC Address of Parental PC** field and then click **Save**.

Enable Parental Controls

MAC Address Of Parental PC:

MAC Address of Current PC:

4. Enter 00:11:22:33:44:AA in the MAC Address 1 field.

MAC Address - 1:

MAC Address - 2:

MAC Address - 3:

MAC Address - 4:

MAC Address in current LAN:

5. Select **Each Week** from the **Apply To** drop-down list, and select Sat. Select **00:00** as the **Start Time** and Select **24:00** as the **End Time**. And then click **Add**.

Apply To:

Start Time:

End Time:

Mon. Tues. Wed. Thur. Fri. Sat. Sun.

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

6. Enter www.tp-link.com in the **Add URL** field. Click **Add**.

Add URL:

(Will not take effect until you save these changes)

7. Click **Save**.

5. 10. Access Control

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

I want to:

Deny or allow specific client devices to access my network with access time and content restrictions.

For example, if you want to restrict the internet activities of host with MAC address 00:11:22:33:44:AA on the LAN to access www.tp-link.com only, please follow the steps below:

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Access Control > Host** and configure the host settings:
 - 1) Click [Add New](#).
 - 2) Select **MAC Address** as the mode type. Create a unique description (e.g. [host_1](#)) for the host in the **Description** field and enter 00:11:22:33:44:AA in the **MAC Address** field.

The screenshot shows a web-based configuration interface for adding a host entry. The title bar says "Add or Edit A Host Entry". Below it, there's a form with the following fields:

- Mode:** A dropdown menu currently set to "MAC Address".
- Description:** An empty input field.
- MAC Address:** An empty input field.

At the bottom of the form are two buttons: "Save" and "Back".

- 3) Click [Save](#).
3. Go to **Access Control > Target** and configure the target settings:
 - 1) Click [Add New](#).
 - 2) Select **URL Address** as the mode type. Create a unique description (e.g. [target_1](#)) for the target in the **Target Description** field and enter the domain name, either the full name or the keywords (for example TP-Link) in the **Add URL Address** field. And then Click [Add](#).

Note:

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

Add or Edit A Target Entry

Mode: URL Address

Description:

Add URL Address:

(Will not take effect until you save these changes)

- 3) Click **Save**.
4. Go to **Access Control > Schedule** and configure the schedule settings:
 - 1) Click **Add New**.
 - 2) Create a unique description (e.g. `schedule_1`) for the schedule in the **Schedule Description** field and set the day(s) and time period. And then click **Add**.

Add or Edit A Schedule Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Settings](#)".

Description: Schedule_1

Apply To: Each Day Start Time: 00:00 End Time: 24:00

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

- 3) Click **Save**.
5. Go to **Access Control > Rule** and add a new access control rule.
 - 1) Click **Add New**.
 - 2) Give a name for the rule in the **Description** field. Select `host_1` from the LAN host drop-down list; select `target_1` from the target drop-down list; select `schedule_1` from the schedule drop-down list.

Add Internet Access Control Entry

Description:	<input type="text" value="rule_1"/>
LAN Host:	<input type="text" value="host_1"/> Add LAN Host
Target:	<input type="text" value="target_1"/> Add Target
Schedule:	<input type="text" value="Schedule_1"/> Add Schedule
Rule:	<input type="text" value="Allow"/> Allow
Status:	<input type="text" value="Enabled"/> Enabled
Direction:	<input type="text" value="IN"/> IN
Protocol:	<input type="text" value="ALL"/> ALL

[Save](#) [Back](#)

3) Leave the status as **Enabled** as click **Save**.

6. Select **Enable Internet Access Control** to enable Access Control function.
7. Select **Allow** the packets specified by any enabled access control policy to pass through the Router as the default filter policy and click **Save**.

Access Control Rule Management

This device can restrict Internet activity for specified LAN hosts. You can set and combine access control rules to effectively manage your network.

Enable Internet access control

Default Filtering Rules:

Allow the packets not specified by any filtering rules to passthrough this device.
 Deny the packets not specified by any filtering rules to passthrough this device.

[Save](#)

Done!

Now only the specific host(s) can visit the target(s) within the scheduled time period.

5.11. Advanced Routing

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

5.11.1. Static Route List

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Advanced Routing > **Static Route List**.

- To add static routing entries:

1. Click Add New.
2. Enter the following information.

The screenshot shows a 'Static Route' configuration form. At the top, it says 'Static Route'. Below that are five input fields: 'Destination IP Address', 'Subnet Mask', 'Gateway', 'Interface' (with a note '(optional)'), and 'Status' (set to 'Enabled'). At the bottom are two buttons: 'Save' and 'Back'.

- **Destination IP Address** - The Destination Network is the address of the network or host that you want to assign to a static route.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the default gateway device that allows the contact between the router and the network or host.
- **Interface** - It is empty by default. Please select a connection from the dropdown list if the Gateway is left empty or is not on the same network segment as LAN/WAN interface.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click **Save**.

5.11.2. System Routing Table

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Advanced Routing > System Routing Table, and you can view all the valid route entries in use.

The screenshot shows a 'System Routing Table' page. At the top, it says 'System Routing Table'. Below that is a table with columns: ID, Destination Network, Subnet Mask, Gateway, and Interface. One row is shown with ID 1, Destination Network 192.168.0.0, Subnet Mask 255.255.255.0, Gateway 0.0.0.0, and Interface LAN & WLAN. At the bottom is a 'Refresh' button.

ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN

- **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), or the WAN (Internet).

Click [Refresh](#) to refresh the data displayed.

5. 12. Bandwidth Control

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Bandwidth Control](#).
3. Tick the [Enable Bandwidth Control](#) checkbox, and configure the [Egress Bandwidth](#) and [Ingress Bandwidth](#), and then click [Save](#). The [Egress/Ingress Bandwidth](#) is the upload/download speed through the WAN port. The value should be less than 100,000Kbps.

The screenshot shows a simplified 'Bandwidth Control' configuration page. It has a title bar 'Bandwidth Control'. Below it is a checkbox labeled 'Enable Bandwidth Control' which is checked. Underneath are two input fields: 'Egress Bandwidth' with the value '512 Kbps' and 'Ingress Bandwidth' with the value '2048 Kbps'. At the bottom is a blue 'Save' button.

4. Click [Add New](#), fill in the blanks and click [Save](#).

The screenshot shows an advanced 'Bandwidth Control' configuration page. It includes fields for 'Enable' (checked), 'IP Range', 'Port Range', 'Protocol' (set to 'ALL'), 'Priority' (set to '5'), and dropdowns for 'Min Bandwidth(Kbps)' and 'Max Bandwidth(Kbps)'. It also has sections for 'Egress Bandwidth' and 'Ingress Bandwidth'. At the bottom are 'Save' and 'Back' buttons.

- **IP Range** - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are ALL, TCP, UDP.
- **Priority** - Priority of Bandwidth Control rules. '1' stands for the highest priority while '8' stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port.

5. 13. IP & MAC Binding

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

5. 13. 1. Binding Settings

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

The screenshot shows a web-based configuration interface for 'Binding Settings'. At the top, the title 'Binding Settings' is displayed. Below the title, there is a section for 'ARP Binding' with two radio button options: 'Enable' (which is selected) and 'Disable'. A 'Save' button is located to the right of the binding settings section. The entire form is enclosed in a light gray border.

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

1. Click **Add New**.
2. Enter the MAC address and IP address.
3. Tick the **Bind** checkbox and click **Save**.

Binding Settings

This page allows you to set IP-MAC Binding entries.

MAC Address:	<input type="text"/>
IP Address:	<input type="text"/>
Bind:	<input checked="" type="checkbox"/>

[Save](#) [Back](#)

- **To modify or delete an existing entry:**
 1. Select the desired entry in the table.
 2. Click [Edit](#) or [Delete Selected](#).

5.13.2. ARP List

To manage a device, you can observe the device on the LAN by checking its MAC address and IP address on the ARP list, and you can also configure the items. This page displays the ARP list which shows all the existing IP & MAC Binding entries.

ARP List

	MAC Address	IP Address	Status
<input type="checkbox"/>	00:E0:4C:00:07:BE	192.168.0.4	Bound
<input type="checkbox"/>	40:8D:5C:89:74:B5	192.168.0.100	Unloaded

[Load Selected](#) [Delete Selected](#)

[Refresh](#)

- [MAC Address](#) - The MAC address of the listed computer on the LAN.
- [IP Address](#) - The assigned IP address of the listed computer on the LAN.
- [Status](#) - Indicates whether or not the MAC and IP addresses are bound.
- [Configure](#) - Load or delete an item.
 - [Load](#) - Load the item to the IP & MAC Binding list.
 - [Delete](#) - Delete the item.
- Click the [Load Selected](#) button to load the selected items to the IP & MAC Binding list.
- Click the [Delete Selected](#) button to delete the selected items to the IP & MAC Binding list.
- Click the [Refresh](#) button to refresh all items.

Note:

An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, [Load All](#) only loads the items without interference to the IP & MAC Binding list.

5.14. Dynamic DNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address. Thus your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.noip.com. The Dynamic DNS client service provider will give you a password or key.

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

Dyndns DDNS

If the dynamic DNS Service Provider you select is www.dyn.com, the following page will appear.

The screenshot shows the 'DDNS Settings' page. At the top, it says 'DDNS Settings'. Below that, there's a dropdown menu for 'Service Provider' set to 'Dyndns (dyn.com/dns)' with a link 'Go to register...'. There are four input fields: 'Domain Name', 'Username', and 'Password', each with a corresponding text input box. Below these is a checkbox 'Enable DDNS' which is unchecked. To the right of the checkbox, it says 'Connection Status: Disconnected'. At the bottom of the form are two buttons 'Login' and 'Logout', and a 'Save' button.

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) you received from dynamic DNS service provider here.
 2. Enter the [Username](#) for your DDNS account.
 3. Enter the [Password](#) for your DDNS account.
 4. Click [Login](#).
 5. Click [Save](#).
- [Connection Status](#) - The status of the DDNS service connection is displayed here.

- **Logout** - Click [Logout](#) to log out of the DDNS service.

No-IP DDNS

If the dynamic DNS Service Provider you select is www.noip.com, the following page will appear.

The screenshot shows a web-based configuration interface for No-IP DDNS settings. At the top, it says "DDNS Settings". Below that, there's a dropdown menu labeled "Service Provider" set to "No-IP (www.noip.com)", with a link "Go to register..." next to it. There are four input fields: "Domain Name", "Username", and "Password", each with a corresponding text input box below it. Below these fields are two status indicators: "Enable DDNS:" with a checked checkbox and "Connection Status: Disconnected". At the bottom of the form are three buttons: "Login" (in red), "Logout" (in blue), and "Save".

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) you received from dynamic DNS service provider.
 2. Enter the [Username](#) for your DDNS account.
 3. Enter the [Password](#) for your DDNS account.
 4. Click [Login](#).
 5. Click [Save](#).
- [Connection Status](#) - The status of the DDNS service connection is displayed here.
 - [Logout](#) - Click [Logout](#) to log out of the DDNS service.

Comexe DDNS

If the dynamic DNS Service Provider you select is www.comexe.cn, the following page will appear.

The screenshot shows the 'DDNS Settings' page. At the top, it says 'Service Provider: Comexe (www.comexe.cr)' with a dropdown arrow and a link 'Go to register...'. Below that are five input fields for 'Domain Name1' through 'Domain Name5'. Further down are fields for 'Username' and 'Password'. A checkbox labeled 'Enable DDNS' is checked. The 'Connection Status' is shown as 'Disconnected'. At the bottom are three buttons: 'Login', 'Logout', and 'Save'.

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** received from your dynamic DNS service provider.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Click **Login**.
5. Click **Save**.
 - **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Logout** - Click **Logout** to log out of the DDNS service.

5. 15. IPv6

This function allows you to enable IPv6 function and set up the parameters of the router's Wide Area Network (WAN) and Local Area Network (LAN).

5. 15. 1. IPv6 Status

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

IPv6 Status	
WAN	
Connection Type: Disabled	
IPv6 LAN	
IPv6 Address Type: RADVD	
Prefix Length: 64	
IPv6 Address: N/A	

- **WAN** - This section shows the current IPv6 Connection Type.
- **IPv6 LAN** - This section shows the current IPv6 information of the router's LAN port, including IPv6 Address Type, Prefix Length and IPv6 Address.

5. 15. 2. IPv6 WAN

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

IPv6 WAN	
Enable IPv6: <input checked="" type="checkbox"/>	
Connection Type: Dynamic IPv6	
IPv6 Address: ::	
Prefix Length: 0	
IPv6 Gateway: ::	
Addressing Type: DHCPv6	
MTU(Bytes): <input type="text" value="1500"/> (1500 as default, do not change unless necessary)	
Enable MLD Proxy: <input type="checkbox"/>	
Set IPv6 DNS Server manually: <input type="checkbox"/>	
Host Name: <input type="text"/>	
Save	

3. Select the **WAN Connection Type** and fill in the blanks according to your ISP, and then click **Save**.
 - **Dynamic IPv6** - Connections which use dynamic IPv6 address assignment.
 - **Static IPv6** - Connections which use static IPv6 address assignment.
 - **PPPoEv6** - Connections which use PPPoEv6 that requires a username and password.
 - **Tunnel 6to4** - Connections which use 6to4 address assignment.

Dynamic IPv6

The screenshot shows the 'IPv6 WAN' configuration page. At the top, 'Enable IPv6:' is checked and 'Connection Type:' is set to 'Dynamic IPv6'. Below this, 'IPv6 Address:' is ::, 'Prefix Length:' is 0, and 'IPv6 Gateway:' is ::. The 'Addressing Type:' dropdown is set to 'DHCPv6'. A note below says '(1500 as default, do not change unless necessary)'. Under 'Advanced' settings, 'Enable MLD Proxy:' is unchecked and 'Set IPv6 DNS Server manually:' is checked. The 'Host Name:' field contains '██████████'. At the bottom right is a 'Save' button.

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Set IPv6 DNS Server manually** - If your ISP gives you one or two DNS IPv6 addresses, select Set IPv6 DNS Server manually and enter the **IPv6 DNS Server** and **Secondary IPv6 DNS Server** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

Note:

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

Static IPv6

The screenshot shows the 'IPv6 WAN' configuration page. The 'Connection Type' is set to 'Static IPv6'. The 'IPv6 Address' field contains a placeholder '...'. The 'Prefix Length' is set to '64'. The 'IPv6 Gateway' and 'IPv6 DNS Server' fields both have a '(optional)' note. The 'Secondary IPv6 DNS Server' field also has a '(optional)' note. Below these fields is a note: 'MTU(Bytes): 1500 (1500 as default, do not change unless necessary)'. There is a 'Save' button at the bottom.

- **IPv6 Address** - Enter the IPv6 address provided by your ISP.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **IPv6 DNS Server** - Enter the DNS IPv6 address provided by your ISP.
- **Secondary IPv6 DNS Server** - Enter another DNS IPv6 address provided by your ISP.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

PPPoEv6

The screenshot shows the 'IPv6 WAN' configuration page for PPPoEv6. The 'Connection Type' is set to 'PPPoEv6'. The 'PPP Username' and 'PPP Password' fields are present. The 'Confirm password' field is also present. The 'Authentication Type' is set to 'AUTO_AUTH'. The 'Addressing Type' is set to 'DHCPv6'. Below these fields are 'Service Name' and 'Server Name' fields, both with notes: '(do not change unless necessary)'. The 'MTU(Bytes)' is set to '1480'. At the bottom, there are checkboxes for 'Enable MLD Proxy', 'Use IPv6 address specified by ISP', and 'Set IPv6 DNS Server manually'. A 'Save' button is at the bottom.

- **PPP Username/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Authentication Type** – Choose one authentication type from AUTO-AUTH, PAP, CHAP and MS-CHAP.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1480 bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Use IPv6 address specified by ISP** - Input a static IPv6 address from the ISP.
- **Set IPv6 DNS Server manually** - Enter the IP address of the IPv6 DNS server and secondary IPv6 DNS server.

Tunnel 6to4

The screenshot shows a configuration interface for 'IPv6 WAN'. At the top, there's a header 'IPv6 WAN'. Below it, there are several input fields and dropdown menus:

- 'Enable IPv6': A checked checkbox.
- 'Connection Type': A dropdown menu set to 'Tunnel 6to4'.
- 'WAN Connection': A dropdown menu showing a blurred list of options.

At the bottom right of the form is a 'Save' button.

- **WAN Connection** - Display the available wan connection.

5. 15. 3. IPv6 LAN

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 LAN** and configure the IPv6 LAN settings as needed.

IPv6 LAN Settings

The parameters of IPv6 LAN can be configured on this page when IPv6 enabled.
Note: Only the default group will support IPv6 at this moment.

Group: Default
Address Auto-Configuration Type: RADVD DHCPv6 Server
Enable RDNSS:
Enable ULA Prefix:

Site Prefix Configuration Type: Delegated Static
Prefix Delegated WAN Connection: No available interface.

- **Address Auto-Configuration Type** - Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided.
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the **Site Prefix** and **Site Prefix Length** manually. Please contact your ISP to get more information before you configure them.

 Note:

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

5. 16. System Tools

5. 16. 1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

Time Settings:

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

Date: 1970 Year 1 Month 1 Day

Time: 0 Hour 28 Minute 46 Second Get from PC

NTP Server 1: (optional)

NTP Server 2: (optional)

Get GMT (Only when the Internet connection is active).

Save

- **To set time manually:**

1. Select your local **Time Zone**.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

- **To set time automatically:**

5. Select your local **Time Zone**.
6. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
7. Click **Get GMT** to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

1. Select **Enable Daylight Saving**.
2. Select the start time from the drop-down list in the **Start** fields.
3. Select the end time from the drop-down list in the **End** fields.
4. Click **Save**.

■ Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

5.16.2. Diagnostic

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

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

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP address/Domain name:

Ping Count: ping(1 - 50)

Ping Packet Size: (0 - 65500 Bytes)

Ping Timeout: (1 - 60 Seconds)

Traceroute Max TTL: (1 - 30)

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

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

3. Click **Start** to check the connectivity of the internet.
4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

Diagnostic Results

```
Pinging 192.168.0.1 with 64 bytes of data:

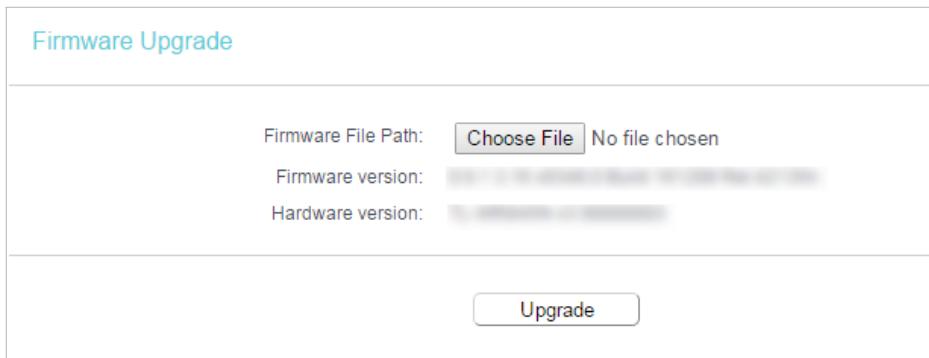
Reply from 192.168.0.1: bytes=64  time=1      TTL=64  seq=1
Reply from 192.168.0.1: bytes=64  time=1      TTL=64  seq=2
Reply from 192.168.0.1: bytes=64  time=1      TTL=64  seq=3
Reply from 192.168.0.1: bytes=64  time=1      TTL=64  seq=4

Ping statistics for 192.168.0.1
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
  Approximate round trip times in milliseconds:
    Minimum = 1, Maximum = 1, Average = 1
```

5. 16. 3. Firmware Upgrade

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

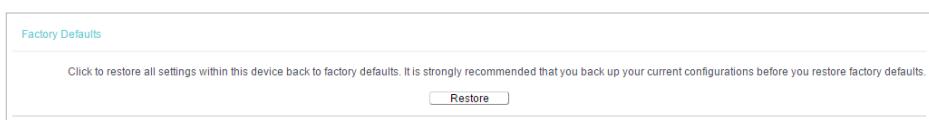
1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Choose File](#) to locate the downloaded firmware file, and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



The screenshot shows a web-based configuration interface for a firmware upgrade. At the top, it says "Firmware Upgrade". Below that, there are three input fields: "Firmware File Path" with a "Choose File" button and a message "No file chosen", "Firmware version" with a blurred value, and "Hardware version" with a blurred value. At the bottom right is a large red "Upgrade" button.

5. 16. 4. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.



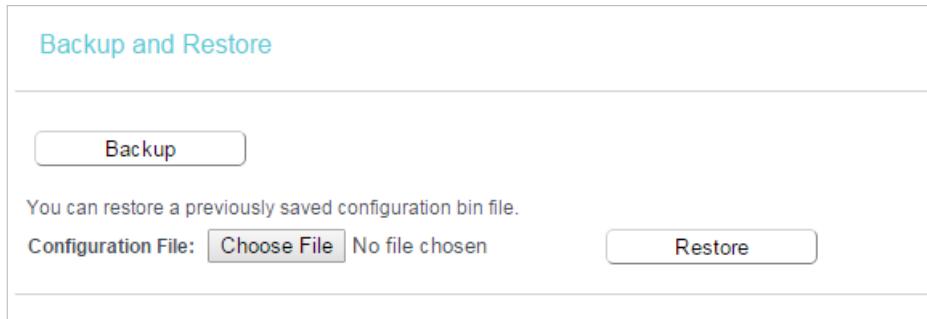
The screenshot shows a "Factory Defaults" page. It contains a warning message: "Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults." Below the message is a blue "Restore" button.

- Default [Username](#): admin
- Default [Password](#): admin
- Default [IP Address](#): 192.168.0.1
- Default [Subnet Mask](#): 255.255.255.0

5. 16. 5. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

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



- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

■ Note:

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

5. 16. 6. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

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

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

- **To reboot the router manually:**

Click **Reboot**, and wait a few minutes for the router to rebooting.

System Reboot

Click Reboot to restart the device without applying any changes to your current settings.

Reboot

- **To set the router reboot every a couple of hours:**

1. Select **Timeout** from the **Auto Reboot Time** drop-down list.
2. Specify a time interval. The router will reboot automatically after every this interval.
3. Click **Save**.

System Reboot

Click Reboot to restart the device without applying any changes to your current settings.

Reboot

Auto Reboot Time: **Timeout** ▾
1 Hours 0 Minutes

Remaining Time:

Save

- **To schedule the router to reboot at a specific time:**

1. Select **Schedule** from the **Auto Reboot Time** drop-down list.
2. Specify the **Day(s)** and **Time** for the router to reboot.
3. Click **Save**.

System Reboot

Click Reboot to restart the device without applying any changes to your current settings.

Reboot

Auto Reboot Time: **Schedule** ▾
Day: Everyday Select Days
 Mon Tue Wed Thu Fri Sat Sun
Time: **00** ▾ **00** ▾ (Hour:Minute)

The Schedule is based on the time of the Router.
The time can be set in "System Tools -> [Time Settings](#)".

Save

5.16.7. Password

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Password**, and you can change the factory default username and password of the router.

Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:	<input type="text"/>
Old Password:	<input type="password"/>
New User Name:	<input type="text"/>
New Password:	<input type="password"/>
Confirm password:	<input type="password"/>

Save **Clear All**

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

Note:

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

3. Click **Save**.

5.16.8. System Log

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

Log Type: ALL Log Level: Debug

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

Refresh **Clear Log** **Save Log** **Log Settings**

- **Log Type** -By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.

- **Clear Log** - All the logs will be deleted from the router permanently, not just from the page.

5.16.9. Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Traffic Statistics**.
3. Select **Enable** and click **Save**. You can view the network traffic of each PC on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.

Traffic Statistics

Traffic Statistics--LAN

Traffic Statistics: Enable Disable

Statistics Interval:

Statistics List

IP Address MAC Address	Total		Current				Operation
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	
Current list is blank							

5.17. Logout

Click **Logout** at the bottom of the main menu, and you will log out of the Web-based Utility and return to the login window.

Chapter 6

Configure the Router in Access Point Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Logout](#)

6. 1. Status

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

Status	
Firmware Version:	3.0.0.20191018-1950-1950
Hardware Version:	TL-WR841N
LAN	
MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Access Point
Wireless Radio:	Enabled
Name(SSID):	TP-Link_0969
Mode:	11bgn mixed
Channel:	Auto(Channel 2)
Channel Width:	Auto
MAC Address:	00:0A:EB:13:09:69
System Up Time:	0 day(s) 00:08:23
	<input type="button" value="Refresh"/>

- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Network > LAN** page.
 - **MAC address** - The physical address of the router.
 - **IP address** - The LAN IP address of the router.
 - **Subnet Mask** - The subnet mask associated with the LAN IP address.
- **Wireless** - This field displays the basic information or status of the wireless function, and you can configure them on the **Wireless > Basic Settings** page.
 - **Operation Mode** - The current wireless working mode in use.
 - **Wireless Radio** - Indicates whether the wireless radio feature of the router is enabled or disabled.
 - **Name(SSID)** - The SSID of the router.
 - **Mode** - The current wireless mode which the router works on.
 - **Channel** - The current wireless channel in use.
 - **Channel Width** - The current wireless channel width in use.

- **MAC Address** - The physical address of the router.
- **System Up Time** - The length of the time since the router was last powered on or reset.

Click **Refresh** to get the latest status and settings of the router.

6.2. Operation Mode

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Operation Mode**.
3. Select the working mode as **Access Point** and click **Save**.

The screenshot shows a configuration interface titled "Operation Mode". Under the heading "Select an Operation Mode:", there are four radio buttons: "Wireless Router", "WISP", "Access Point" (which is selected), and "Range Extender". At the bottom right of the form is a "Save" button.

6.3. Network

6.3.1. LAN

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

The screenshot shows a configuration interface titled "LAN Settings". Under "LAN Type:", a dropdown menu is set to "Smart IP(DHCP)". Below it, a note states: "Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP) (In this situation the device will help you configure the IP parameters automatically as you need)." At the bottom of the form are fields for "MAC Address" (00:0A:EB:13:09:69), "IP Address" (192.168.0.1), and "Subnet Mask" (255.255.255.0). A "Save" button is at the bottom right.

- **LAN Type** - Either select Smart IP(DHCP) to get IP address from DHCP server, or Static IP to configure IP address manually.

- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation if you select Static IP (factory default - 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

■ Note:

- If you have changed the IP address, you must use the new IP address to login.
- If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP Address pool in the DHCP Server will be configured.

6. 4. Wireless

6. 4. 1. Basic Settings

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

The screenshot shows the 'Wireless Basic Settings' configuration page. It includes fields for enabling/disabling the wireless network, setting the wireless network name (SSID), selecting the mode (11bgn mixed), choosing the channel (Auto), setting the channel width (Auto), and enabling SSID broadcast. A 'Save' button is at the bottom.

Wireless Basic Settings	
Wireless:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Network Name:	TP-Link_0969 (Also called SSID)
Mode:	11bgn mixed
Channel:	Auto
Channel Width:	Auto
<input checked="" type="checkbox"/> Enable SSID Broadcast	
Save	

- **Wireless** - Enable or disable wireless network.
- **Wireless Network Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Mode** - You can choose the appropriate "Mixed" mode.
- **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems

with another nearby access point. If you select **Auto**, then AP will choose the best channel automatically.

- **Enable SSID Broadcast** - If enabled, the router will broadcast the wireless network name (SSID).

6.4.2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router's network quickly via WPS.

■ Note:

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

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

Method ONE: Press the WPS Button on Your Client Device

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

WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 12345670
 Disable device PIN

Add a new device:

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

WPS Settings

Enter new device PIN.
PIN:
 Press the WPS button of the new device within the next two minutes.

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

Method TWO: Enter the Client's PIN

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

The screenshot shows the 'WPS (Wi-Fi Protected Setup)' configuration page. At the top, it says 'WPS: Enabled' with a 'Disable' button. Below that, the 'Current PIN:' field shows '12345670' with 'Restore PIN' and 'Generate New PIN' buttons. There is also a checked checkbox for 'Disable device PIN'. At the bottom, there is an 'Add a new device:' field with an 'Add device' button.

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

The screenshot shows the 'WPS Settings' page. It has two options: 'Enter new device PIN' (selected) with a PIN input field, and 'Press the WPS button of the new device within the next two minutes.' At the bottom are 'Connect' and 'Back' buttons.

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

Method Three: Enter the Router's PIN

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

This screenshot is identical to the one above, showing the 'WPS (Wi-Fi Protected Setup)' configuration page with 'WPS: Enabled', 'Current PIN: 12345670', and the 'Add device' button at the bottom.

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

6.4.3. Wireless Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Security**.
3. Configure the security settings of your wireless network and click **Save**.

Wireless Security Settings

Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled. For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption.

Disable Wireless Security

WPA/WPA2 - Personal(Recommended)

Version: <select>WPA2-PSK</select> Encryption: <select>AES</select> Wireless Password: <input value="12345670"/> Group Key Update Period: <input value="0"/>

WPA/WPA2 - Enterprise

Version: <select>Auto</select> Encryption: <select>Auto</select> RADIUS Server IP: <input/> RADIUS Server Port: <input value="1812"/> (1-65535, 0 stands for default port 1812) RADIUS Server Password: <input/> Group Key Update Period: <input value="0"/>

WEP

Authentication Type: <select>Open System</select> WEP Key Format: <select>Hexadecimal</select> Selected Key: <input checked="" type="radio"/> WEP Key Key 1: <input checked="" type="radio"/> <input/> Key 2: <input type="radio"/> <input/> Key 3: <input type="radio"/> <input/> Key 4: <input type="radio"/> <input/>	Key Type <input checked="" type="radio"/> Disabled <input type="radio"/> Disabled <input type="radio"/> Disabled <input type="radio"/> Disabled
--	---

- **Disable Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router without a password. It's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-Personal** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - **Version** - Select [Auto](#), [WPA-PSK](#) or [WPA2-PSK](#).
 - **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **Wireless Password** - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- **WPA /WPA2-Enterprise** - It's based on Radius Server.
 - **Version** - Select [Auto](#), [WPA](#) or [WPA2](#).
 - **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **Radius Server IP** - Enter the IP address of the Radius server.
 - **Radius Server Port** - Enter the port that Radius server used.

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

6.4.4. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

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

For example, you want the wireless client A with the MAC address 00:0A:EB:B0:00:0B and the wireless client B with the MAC address 00:0A:EB:00:07:5F to access the router, but other wireless clients cannot access the router

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless MAC Filtering**.
3. Click **Enable** to enable the Wireless MAC Filtering function.
4. Select **Allow the stations specified by any enabled entries in the list to access** as the filtering rule.

5. Delete all or disable all entries if there are any entries already.
6. Click **Add New** and fill in the blank.

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address:	00:0A:EB:B0:00:0B
Description:	Client A
Status:	Enabled

Save **Back**

- 1) Enter the MAC address 00:0A:EB:B0:00:0B / 00:0A:EB:00:07:5F in the MAC Address field.
- 2) Enter wireless client A/B in the Description field.
- 3) Select **Enabled** in the Status drop-down list.
- 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering:	Enabled	<input type="button" value="Disable"/>																		
Filtering Rules																				
<input type="radio"/> Deny	the stations specified by any enabled entries in the list to access.																			
<input checked="" type="radio"/> Allow	the stations specified by any enabled entries in the list to access.																			
<table border="1"> <thead> <tr> <th></th> <th>MAC Address</th> <th>Status</th> <th>Host</th> <th>Description</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>00:0A:EB:B0:00:0B</td> <td>Enabled</td> <td>TP-Link_7AFF</td> <td>client A</td> <td>Edit</td> </tr> <tr> <td><input type="checkbox"/></td> <td>00:0A:EB:00:07:5F</td> <td>Enabled</td> <td>TP-Link_7AFF</td> <td>Client B</td> <td>Edit</td> </tr> </tbody> </table> <input type="button" value="Add New"/> <input type="button" value="Enable Selected"/> <input type="button" value="Disable Selected"/> <input type="button" value="Delete Selected"/>				MAC Address	Status	Host	Description	Edit	<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-Link_7AFF	client A	Edit	<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	Edit
	MAC Address	Status	Host	Description	Edit															
<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-Link_7AFF	client A	Edit															
<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	Edit															

Done!

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

6.4.5. Wireless Advanced

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Advanced**.
3. Configure the advanced settings of your wireless network and click **Save**.

Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

The screenshot shows the 'Wireless Advanced' configuration page. It includes fields for Transmit Power (set to High), Beacon Interval (100), RTS Threshold (2346), Fragmentation Threshold (2346), and DTIM Interval (1). There are also three checkboxes: 'Enable Short GI' (checked), 'Enable Client Isolation' (unchecked), and 'Enable WMM' (checked). A 'Save' button is located at the bottom right.

- **Transmit Power** - Select **High**, **Middle** or **Low** which you would like to specify for the router. **High** is the default setting and recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable Client Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

6.4.6. Wireless Statistics

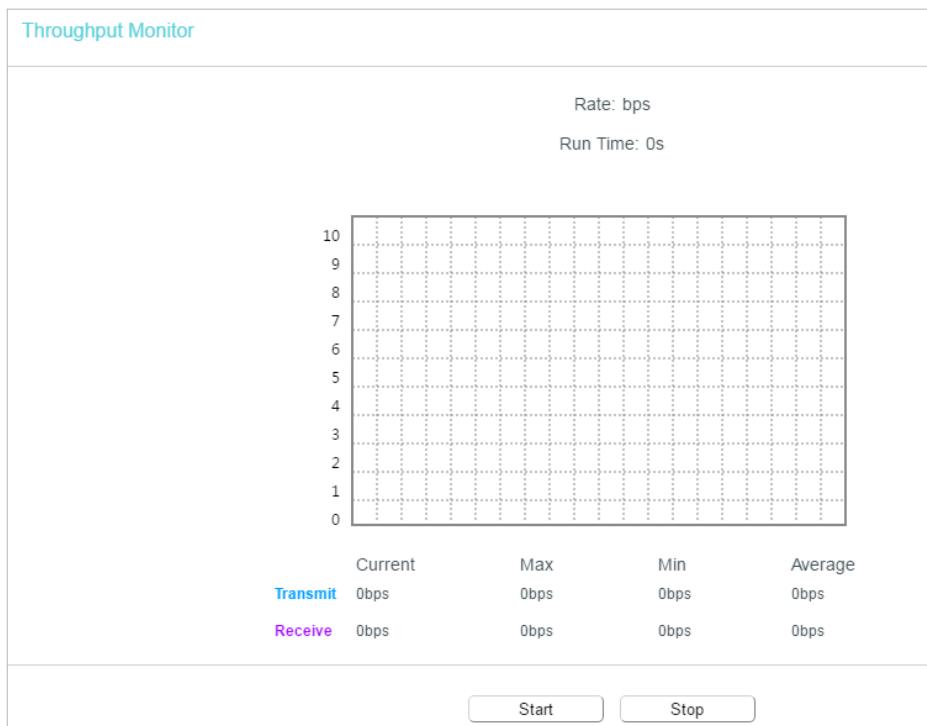
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Statistics** to check the data packets sent and received by each client device connected to the router.

Wireless Stations Status					
Wireless Stations Currently Connected: 1					<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	WPS_2019_10_10_10_10_10

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

6.4.7. Throughput Monitor

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Throughput Monitor** to view the wireless throughput information.



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

Click **Start/Stop** to start or stop wireless throughput monitor.

6.5. DHCP

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

6.5.1. DHCP Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > DHCP Settings**.
3. Specify DHCP server settings and click **Save**.

DHCP Settings	
DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Address Lease Time:	1 minutes (1~2880 minutes, the default value is 1)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	192.168.0.1 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
Save	

- **DHCP Server** - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.

- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 1.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

Note:

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

DHCP Settings

DHCP Server: Disable Enable

Start IP Address: 192.168.0.100

End IP Address: 192.168.0.199

Address Lease Time: 1 minutes (1~2880 minutes, the default value is 1)

Default Gateway: 192.168.0.1 (optional)

Default Domain: (optional)

DNS Server: 192.168.0.1 (optional)

Secondary DNS Server: 0.0.0.0 (optional)

Note: The DHCP Settings function cannot be configured if you have chosen Smart IP (DHCP) in Network->LAN (in this situation the device will help you configure the DHCP automatically as you need.)

Save

6.5.2. DHCP Clients List

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [DHCP > DHCP Clients List](#) to view the information of the clients connected to the router.

DHCP Clients List

This page displays information of all DHCP clients on the network.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camille	40:8D:5C:89:74:B5	192.168.0.100	00:00:32
2	iPhone	34:E2:FD:14:1D:0D	192.168.0.101	00:00:55

Refresh

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

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

6. 5. 3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > Address Reservation**.
3. Click **Add New** and fill in the blanks.

The static IP address of the DHCP Server can be configured on this page.

MAC Address:

IP Address:

Status:

- 1) Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the **Status** as **Enabled**.
- 4) Click **Save**.

6. 6. System Tools

6. 6. 1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

The screenshot shows the 'Time Settings' configuration page. At the top, it says 'Time Settings'. Below that, there are sections for 'Time Zone', 'Date', 'Time', 'NTP Server 1', 'NTP Server 2', and 'Daylight Saving'. The 'Time Zone' dropdown is set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'. The 'Date' fields show '1970' for year, '1' for month, and '1' for day. The 'Time' fields show '0' for hour, '28' for minute, and '46' for second. There are two 'NTP Server' input fields, both labeled '(optional)'. Below these is a 'Get GMT' button with the note '(Only when the Internet connection is active)'. A 'Save' button is at the bottom right. In the 'Daylight Saving' section, there are dropdown menus for 'Start' (set to Mar, Last Sun, 01:00) and 'End' (set to Oct, Last Sun, 02:00), with a 'Save' button at the bottom right.

- **To set time manually:**

1. Select your local **Time Zone**.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

- **To set time automatically:**

5. Select your local **Time Zone**.
6. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
7. Click **Get GMT** to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

1. Select **Enable Daylight Saving**.
2. Select the start time from the drop-down list in the **Start** fields.
3. Select the end time from the drop-down list in the **End** fields.
4. Click **Save**.

Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

6.6.2. Diagnostic

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

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

The screenshot shows the 'Diagnostic Tools' interface. Under 'Diagnostic Parameters', there are several configuration fields:

- 'Diagnostic Tool': A radio button group where 'Ping' is selected.
- 'IP address/Domain name': An input field.
- 'Ping Count': A numeric input field set to 4, with a note '(ping(1 - 50))'.
- 'Ping Packet Size': A numeric input field set to 64, with a note '(0 - 65500 Bytes)'.
- 'Ping Timeout': A numeric input field set to 1, with a note '(1 - 60 Seconds)'.
- 'Traceroute Max TTL': A numeric input field set to 20, with a note '(1 - 30)'.

A 'Start' button is located at the top right of the parameters area.

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

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- **Ping Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

3. Click **Start** to check the connectivity of the internet.
4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

Diagnostic Results

```
Pinging 192.168.0.1 with 64 bytes of data:  
  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4  
  
Ping statistics for 192.168.0.1  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)  
Approximate round trip times in milliseconds:  
Minimum = 1, Maximum = 1, Average = 1
```

6.6.3. SNMP Settings

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol, which allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to System Tools > SNMP Settings.
3. Specify SNMP settings and click Save.

SNMP Settings

Simple Network Management Protocol(SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

SNMP Agent: Enable Disable

Read Community:

Set Community:

System Name:

System Description:

System Location:

System Contact:

Trap Manager IP:

Save

- **SNMP Agent** - Enable or disable the SNMP agent. Choose Enable to open this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Choose Disable to close this function.
- **Read Community** - Enter the community name that allows Read-Only access to this device's SNMP information. The community name can be considered a group password. The default setting is public.

- **Set Community** - Enter the community name that allows Read/Write access to this device's SNMP information. The community name can be considered a group password. The default setting is private.
- **System Name** - An administratively-assigned name for this managed node.
- **System Description** - The software version information for this managed node.
- **System Location** - The physical location of this node.
- **System Contact** - The textual identification of the contact person for this managed node.
- **Trap Manager IP** - A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

 Note:

Specifying one of these values via the Device's Web-based Utility makes the corresponding object read-only. If there isn't such a config setting, then the write request will succeed (assuming suitable access control settings), but the new value would be forgotten the next time the agent was restarted.

6. 6. 4. Ping WatchDog

The Ping Watch Dog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Ping WatchDog**.
3. Specify the settings and click **Save**.

Ping WatchDog Settings

Ping WathDog will be the monitor to detect AP's network, reboot device while AP disconnected.

Switch: Disable Enable

Destination IP:

Interval: (10-300)s

Startup Delay: (60-300)s

Fail Count: (1-65535)

Save

- **Switch** - Enable/Disable Ping Watch Dog.

- **IP Address** - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval** - Time interval between two ping packets which are sent out continuously.
- **StartupDelay** - Time delay before first ping packet is sent out when this device is restarted.
- **Fail Count** - Upper limit of the ping packet this device can drop continuously. If this value is overrun, this device will restart automatically.

6.6.5. Firmware Upgrade

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

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

The screenshot shows a web-based configuration interface for a firmware upgrade. At the top, it says "Firmware Upgrade". Below that, there are three input fields: "Firmware File Path" with a "Choose File" button and the message "No file chosen", "Firmware version" with a blurred value, and "Hardware version" with a blurred value. At the bottom right is a large blue "Upgrade" button.

6.6.6. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Factory Defaults**. Click **Restore** to reset all settings to the default values.

The screenshot shows a "Factory Defaults" page. It contains a warning message: "Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults." Below the message is a blue "Restore" button.

- Default **Username**: admin

- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

6. 6. 7. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

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

Backup and Restore

Backup

You can restore a previously saved configuration bin file.

Configuration File: No file chosen **Restore**

- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

■ Note:

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

6. 6. 8. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

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

- **To reboot the router manually:**

Click **Reboot**, and wait a few minutes for the router to rebooting.

The screenshot shows a simple interface titled "System Reboot". Below the title is a descriptive message: "Click Reboot to restart the device without applying any changes to your current settings." At the bottom right is a single button labeled "Reboot".

- **To set the router reboot every a couple of hours:**

1. Select **Timeout** from the **Auto Reboot Time** drop-down list.
2. Specify a time interval. The router will reboot automatically after every this interval.
3. Click **Save**.

The screenshot shows the "System Reboot" page with the "Auto Reboot Time" section expanded. It includes a dropdown menu set to "Timeout", a "Hours" input field containing "1", a "Minutes" input field containing "0", and a "Remaining Time" status indicator. At the bottom is a "Save" button.

- **To schedule the router to reboot at a specific time:**

1. Select **Schedule** from the **Auto Reboot Time** drop-down list.
2. Specify the **Day(s)** and **Time** for the router to reboot.
3. Click **Save**.

The screenshot shows the 'System Reboot' configuration page. It includes a 'Reboot' button, a note about clicking it to restart the device without saving changes, and a 'Schedule' section. The 'Schedule' dropdown is set to 'Schedule'. Under 'Day:', 'Everyday' is selected, and specific days of the week are checked: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. Under 'Time:', the hour and minute are both set to 00. A note at the bottom states that the schedule is based on the router's time and can be changed in 'Time Settings'.

6.6.9. Password

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Password**, and you can change the factory default username and password of the router.

The screenshot shows the 'Password' configuration page. It has a note that user names and passwords can be between 1-15 characters and must not include spaces. There are five input fields: 'Old User Name', 'Old Password', 'New User Name', 'New Password', and 'Confirm password'. At the bottom are 'Save' and 'Clear All' buttons.

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

Note:

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

3. Click **Save**.

6.6.10. System Log

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

2. Go to [System Tools > System Log](#), and you can view the logs of the router.

The screenshot shows a web-based interface titled "System Log". At the top, there are dropdown menus for "Log Type" (set to "ALL") and "Log Level" (set to "Debug"). Below these are two log entries in a table:

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPCD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPCD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

At the bottom of the page are four buttons: "Refresh", "Clear Log", "Save Log", and "Log Settings".

- [Log Type](#) - By selecting the log type, only logs of this type will be shown.
- [Log Level](#) - By selecting the log level, only logs of this level will be shown.
- [Refresh](#) - Refresh the page to show the latest log list.
- [Clear Log](#) - All the logs will be deleted from the router permanently, not just from the page.

6.7. Logout

Click [Logout](#) at the bottom of the main menu, and you will log out of the Web-based Utility and return to the login window.

Chapter 7

Configure the Router in Range Extender Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Logout](#)

7.1. Status

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

Status	
Firmware Version:	0.9.1 3.16 v0001.0 Build 171220 Rel.74012n
Hardware Version:	TL-WR841N v14 00000014
LAN	
MAC Address:	50:C7:BF:B1:38:40
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless 2.4GHz	
Operation Mode:	Range Extender
Wireless Radio:	Enabled
Name(SSID) of Root AP:	
Name(SSID):	TP-Link_3840
Mode:	11bgn mixed
Channel:	6
Channel Width:	Auto
MAC Address:	50:C7:BF:B1:38:40
System Up Time:	0 day(s) 00:03:45
	<input type="button" value="Refresh"/>

- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the [Network > LAN](#) page.
 - **MAC address** - The physical address of the router.
 - **IP address** - The LAN IP address of the router.
 - **Subnet Mask** - The subnet mask associated with the LAN IP address.
- **Wireless** - This field displays the basic information or status of the wireless function, and you can configure them on the [Wireless > Basic Settings](#) page.
 - **Operation Mode** - The current wireless working mode in use.
 - **Wireless Radio** - Indicates whether the wireless radio feature of the router is enabled or disabled.
 - **Name(SSID) of Root AP** - The SSID of the root router.
 - **Name(SSID)** - The SSID of the router.
 - **Mode** - The current wireless mode which the router works on.
 - **Channel** - The current wireless channel in use.

- **Channel Width** - The current wireless channel width in use.
- **MAC Address** - The physical address of the router.
- **System Up Time** - The length of the time since the router was last powered on or reset.

Click **Refresh** to get the latest status and settings of the router.

7.2. Operation Mode

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Operation Mode**.
3. Select the working mode as **Range Extender** and click **Save**.

The screenshot shows a configuration interface titled "Operation Mode". Under the heading "Select an Operation Mode:", there are four radio buttons: "Wireless Router", "WISP", "Access Point", and "Range Extender". The "Range Extender" option is selected. At the bottom right of the form is a "Save" button.

7.3. Network

7.3.1. LAN

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

The screenshot shows a configuration interface titled "LAN Settings". Under "LAN Type:", a dropdown menu is set to "Smart IP(DHCP)". Below this, a note states: "Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)" and "(In this situation the device will help you configure the IP parameters automatically as you need)". At the bottom of the form are three input fields: "MAC Address" (00:0A:EB:13:09:69), "IP Address" (192.168.0.1), and "Subnet Mask" (255.255.255.0). At the bottom right is a "Save" button.

- **LAN Type** - Either select Smart IP(DHCP) to get IP address from DHCP server, or Static IP to configure IP address manually.
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation if you select Static IP (factory default - 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

 Note:

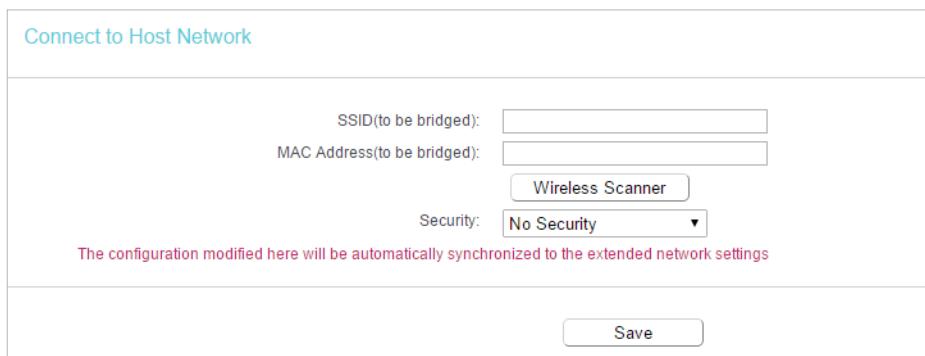
- If you have changed the IP address, you must use the new IP address to login.
- If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP Address pool in the DHCP Server will be configured.

7.4. Wireless

7.4.1. Connect to Network

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

2. Go to Wireless > Connect to Network.



Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged):

Security: No Security

The configuration modified here will be automatically synchronized to the extended network settings

3. Click **Wireless Scanner**, select your host network from the **AP List** and click **Conenct**.



AP List

The scanned APs within the area:

APs: 45

ID	BSSID	SSID	Signal strength	Channel	Encryption	Connect
1	40:61:86:CF:1D:A1	TP-Link_1DA1	90	3	WPA-PSK/AES	Connect
2	2C:59:E5:DA:65:FE	HP-Print-FE-Officejet 7610	86	6	WPA2-PSK/AES	Connect
3	BC:5F:F6:12:2A:FF	MERCUSYS_2B00	81	10	None	Connect
4	3C:46:D8:E0:60:C4	TP-Link_60C4	78	1	WPA2-PSK/AES	Connect
5	CA:E7:D8:02:AA:EF	TP-Link_300re	77	1	WPA-PSK/AES	Connect

4. Enter your host network's wireless password in the **Password** field.

Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged):

Wireless Scanner

Security:

Password:

The configuration modified here will be automatically synchronized to the extended network settings

5. Click **Save**.

7.4.2. Extended Network

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to Wireless > Extended Network, you can view the SSID and password of the router (Range Extender)'s wireless network.
3. If you want to share the same SSID of the host router, click **Copy Host SSID** and click **Save**.

Extended Network Settings

Extended 2.4GHz SSID:

Extended 2.4GHz Security:

Extended 2.4GHz Password:

7.4.3. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

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

For example, you want the wireless client A with the MAC address 00:0A:EB:B0:00:0B and the wireless client B with the MAC address 00:0A:EB:00:07:5F to access the router, but other wireless clients cannot access the router

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless MAC Filtering**.
3. Click **Enable** to enable the Wireless MAC Filtering function.
4. Select **Allow the stations specified by any enabled entries in the list to access** as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click **Add New** and fill in the blank.

Add or Modify Wireless MAC Address Filtering entry

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address:	00:0A:EB:B0:00:0B
Description:	Client A
Status:	Enabled

Save **Back**

- 1) Enter the MAC address 00:0A:EB:B0:00:0B / 00:0A:EB:00:07:5F in the MAC Address field.
- 2) Enter wireless client A/B in the Description field.
- 3) Select **Enabled** in the Status drop-down list.
- 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-Link_7AFF	client A	Edit
<input type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-Link_7AFF	Client B	Edit

Add New **Enable Selected** **Disable Selected** **Delete Selected**

Done!

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

7.4.4. Wireless Advanced

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

3. Configure the advanced settings of your wireless network and click **Save**.

■ Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

The screenshot shows the 'Wireless Advanced' configuration page. At the top, the title 'Wireless Advanced' is displayed. Below the title, there are several configuration options:

- Transmit Power: A dropdown menu set to 'High'.
- Beacon Interval: An input field containing '100' with a range of '(40-1000)'.
- RTS Threshold: An input field containing '2346' with a range of '(1-2346)'.
- Fragmentation Threshold: An input field containing '2346' with a range of '(256-2346)'.
- DTIM Interval: An input field containing '1' with a range of '(1-15)'.
- Checkboxes:
 - Enable Short GI: Checked.
 - Enable Client Isolation: Unchecked.
 - Enable WMM: Checked.

At the bottom right of the form is a 'Save' button.

- **Transmit Power** - Select **High**, **Middle** or **Low** which you would like to specify for the router. **High** is the default setting and recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable Client Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.

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

7.4.5. Wireless Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Wireless > Wireless Statistics** to check the data packets sent and received by each client device connected to the router.

Wireless Stations Status					
Wireless Stations Currently Connected: 1					<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	[REDACTED]

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

7.5. DHCP

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

7.5.1. DHCP Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > DHCP Settings**.
3. Specify DHCP server settings and click **Save**.

DHCP Settings

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Address Lease Time:	1 minutes (1~2880 minutes, the default value is 1)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	192.168.0.1 (optional)
Secondary DNS Server:	0.0.0 (optional)

- **DHCP Server** - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 1.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

 Note:

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

DHCP Settings

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Address Lease Time:	1 minutes (1~2880 minutes, the default value is 1)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	192.168.0.1 (optional)
Secondary DNS Server:	0.0.0.0 (optional)

Note: The DHCP Settings function cannot be configured if you have chosen SmartIP (DHCP) in Network->LAN (in this situation the device will help you configure the DHCP automatically as you need).

7.5.2. DHCP Clients List

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

DHCP Clients List

This page displays information of all DHCP clients on the network.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camille	40:8D:5C:89:74:B5	192.168.0.100	00:00:32
2	iPhone	34:E2:FD:14:1D:0D	192.168.0.101	00:00:55

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

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

7.6. System Tools

7.6.1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

The screenshot shows the 'Time Settings' configuration page. At the top, it says 'Time Settings'. Below that, there's a section for 'Time Settings' with fields for 'Time Zone' (set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon'), 'Date' (Year 1970, Month 1, Day 1), and 'Time' (Hour 0, Minute 28, Second 46). There are also fields for 'NTP Server 1' and 'NTP Server 2', both marked as optional. A 'Get from PC' button is available. Below this, there's a 'Get GMT' button with a note '(Only when the Internet connection is active)' and a 'Save' button. At the bottom, there's a 'Daylight Saving' section with fields for 'Start' (Mar, Last Sun, 01:00) and 'End' (Oct, Last Sun, 02:00), followed by another 'Save' button.

- **To set time manually:**

1. Select your local **Time Zone**.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

- **To set time automatically:**

5. Select your local **Time Zone**.
6. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
7. Click **Get GMT** to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

1. Select **Enable Daylight Saving**.

2. Select the start time from the drop-down list in the **Start** fields.
3. Select the end time from the drop-down list in the **End** fields.
4. Click **Save**.

■ Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

7.6.2. Diagnostic

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

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

The screenshot shows the 'Diagnostic Tools' interface. Under 'Diagnostic Parameters', there are settings for a selected 'Ping' tool. The 'IP address/Domain name' field is empty. Below it, 'Ping Count' is set to 4, 'Ping Packet Size' is 64 bytes, 'Ping Timeout' is 1 second, and 'Traceroute Max TTL' is 20. A 'Start' button is visible at the top right of the form.

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

■ Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

3. Click **Start** to check the connectivity of the internet.

4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

The screenshot shows the 'Diagnostic Results' page with a red box highlighting the ping statistics section. The statistics show 4 packets sent, 4 received, and 0 lost, indicating 0% loss.

```
Pinging 192.168.0.1 with 64 bytes of data:  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3  
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4  
  
Ping statistics for 192.168.0.1  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)  
Approximate round trip times in milliseconds:  
Minimum = 1, Maximum = 1, Average = 1
```

7.6.3. Firmware Upgrade

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

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

The screenshot shows the 'Firmware Upgrade' page. It includes fields for 'Firmware File Path' (with a 'Choose File' button), 'Firmware version' (redacted), 'Hardware version' (redacted), and a large 'Upgrade' button.

7.6.4. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Factory Defaults**. Click **Restore** to reset all settings to the default values.

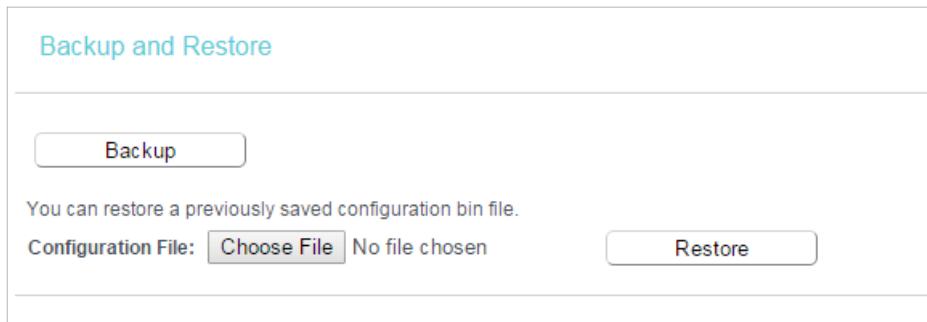
The screenshot shows the 'Factory Defaults' page with a warning message: 'Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults.' Below the message is a 'Restore' button.

- Default **Username**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

7.6.5. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

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



- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

■ Note:

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

7.6.6. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).

- Update the configuration with the file (system will reboot automatically).
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
 2. Go to **System Tools > Reboot**, and you can restart your router.

- **To reboot the router manually:**

Click **Reboot**, and wait a few minutes for the router to rebooting.

The screenshot shows a simple interface titled "System Reboot". Below the title, there is a message: "Click Reboot to restart the device without applying any changes to your current settings." At the bottom right is a red rectangular button labeled "Reboot".

- **To set the router reboot every a couple of hours:**

1. Select **Timeout** from the **Auto Reboot Time** drop-down list.
2. Specify a time interval. The router will reboot automatically after every this interval.
3. Click **Save**.

The screenshot shows the same "System Reboot" interface as before, but with additional settings below the "Reboot" button. It includes fields for "Auto Reboot Time" (set to "Timeout" for 1 hour), "Remaining Time" (showing 0 minutes), and a "Save" button at the bottom.

- **To schedule the router to reboot at a specific time:**

1. Select **Schedule** from the **Auto Reboot Time** drop-down list.
2. Specify the **Day(s)** and **Time** for the router to reboot.
3. Click **Save**.

The screenshot shows the 'System Reboot' configuration page. It includes a section for a one-time reboot with a 'Reboot' button, a scheduled reboot section with dropdown menus for 'Auto Reboot Time' (set to 'Schedule'), 'Day' (set to 'Everyday'), and 'Time' (set to 00:00), and a note about the schedule being based on the router's time. A 'Save' button is at the bottom.

7.6.7. Password

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Password**, and you can change the factory default username and password of the router.

The screenshot shows the 'Password' configuration page. It displays a note about character limits and includes fields for 'Old User Name', 'Old Password', 'New User Name', 'New Password', and 'Confirm password'. At the bottom are 'Save' and 'Clear All' buttons.

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

Note:

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

3. Click **Save**.

7.6.8. System Log

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

2. Go to [System Tools > System Log](#), and you can view the logs of the router.

The screenshot shows a web-based interface titled "System Log". At the top, there are dropdown menus for "Log Type" (set to "ALL") and "Log Level" (set to "Debug"). Below these are two log entries in a table:

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

At the bottom of the page are four buttons: "Refresh", "Clear Log", "Save Log", and "Log Settings".

- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Clear Log** - All the logs will be deleted from the router permanently, not just from the page.

7.7. Logout

Click [Logout](#) at the bottom of the main menu, and you will log out of the Web-based Utility and return to the login window.

FAQ

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

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

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

Q2. What should I do if I forget my login password of the Web-based Utility?

The default username and password of the Web-based Utility are **admin** (in lowercase).

If you have altered the username and password:

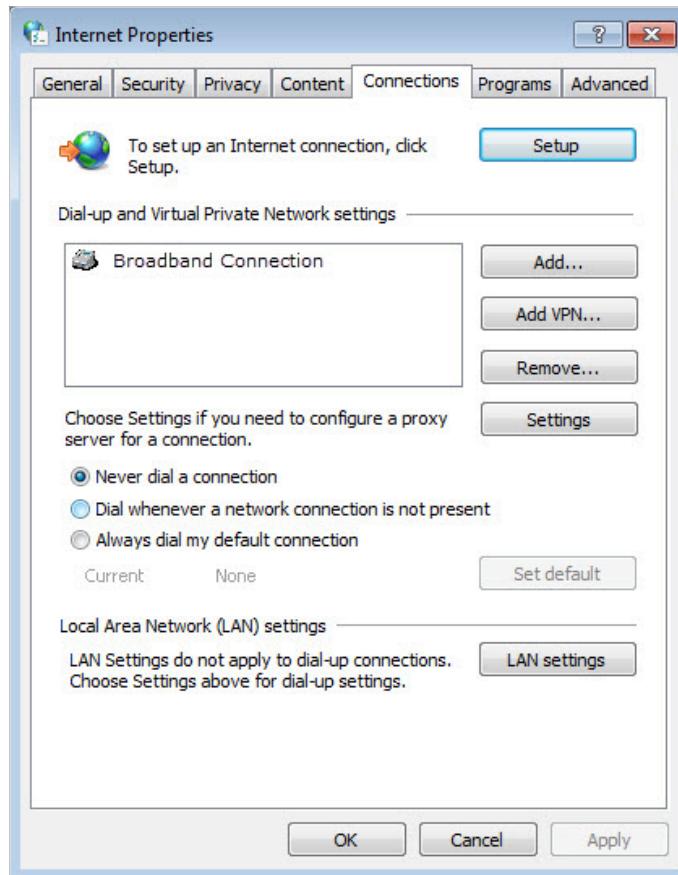
1. Reset the router to factory default settings;
2. Visit <http://tplinkwifi.net>, and enter **admin** (in lowercase) as both username and password to log in.

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

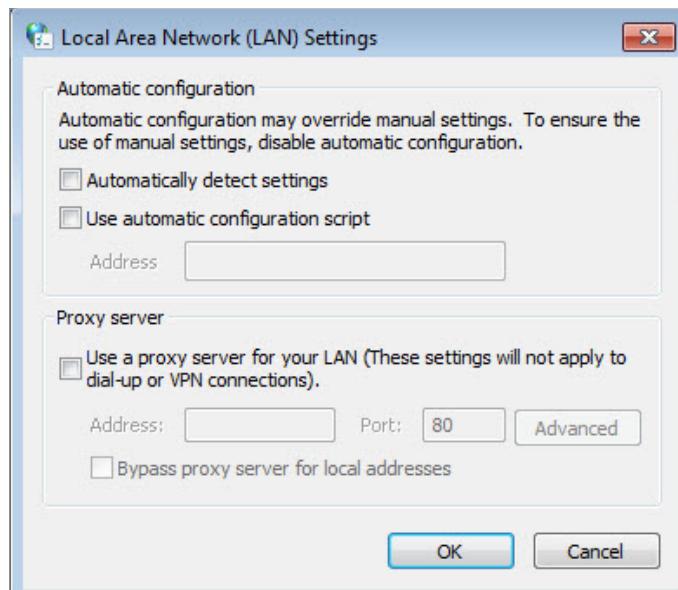
Q3. What should I do if I cannot log in to the router's Web-based Utility?

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

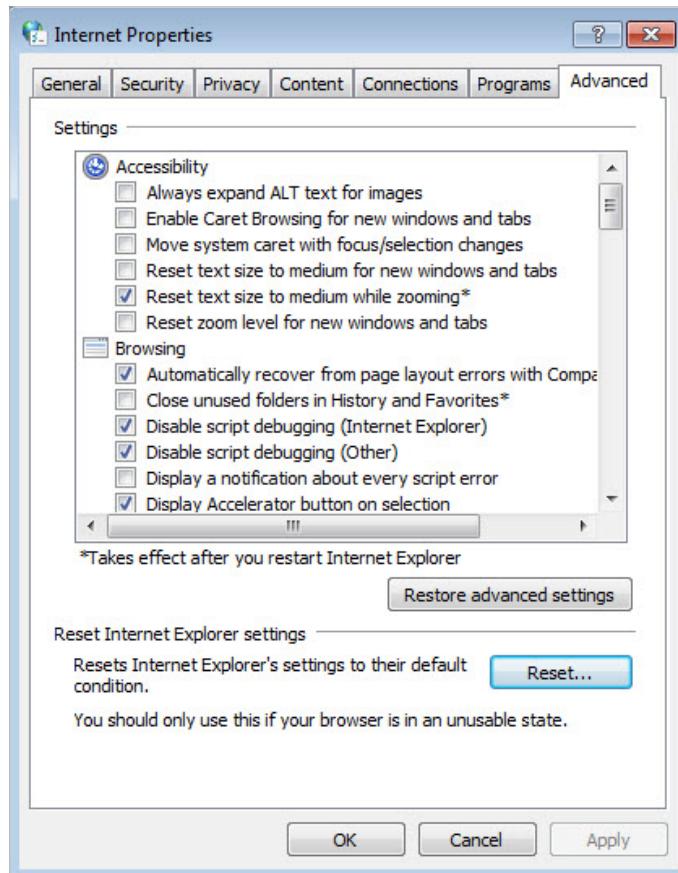
- Make sure your computer has connected to the router correctly and the corresponding LED lights up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure you enter the correct IP address to log in: <http://tplinkwifi.net> or 192.168.0.1.
- 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 deselect the following three options, and click **OK**.



- 5) Go to **Advanced** > **Restore advanced settings**, and click **OK**.



- Use another web browser or computer to log in again.
- Reset the router to factory default settings and try again. If the login still fails, please contact the technical support.
■ Note: You'll need to reconfigure the router to surf the internet once the router is reset.

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

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

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

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

- 1) Go to **DHCP**.
- 2) Enter 8.8.8.8 as Primary DNS, and click **Save**.

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

DHCP Settings

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Lease Time:	1 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	8.8.8.8 (optional)
Secondary DNS Server:	0.0.0.0 (optional)
<input type="button" value="Save"/>	

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

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

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

MAC Clone

WAN MAC Address:	50:C7:BF:B1:38:41	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	74:D4:35:A1:0C:CB	<input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>		

⌚ Tips:

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

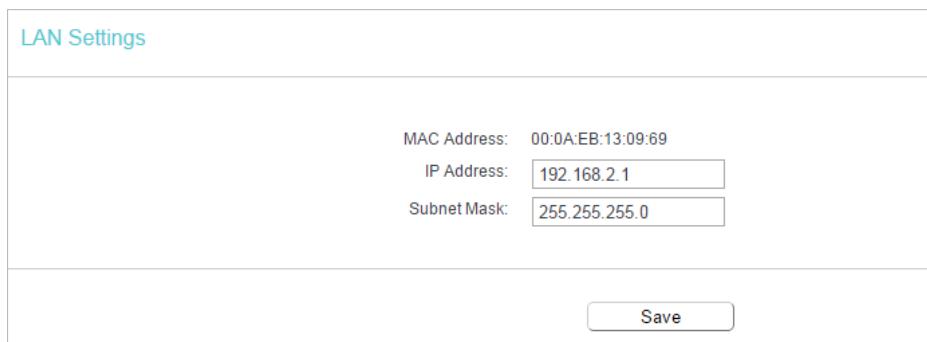
- The MAC addresses of a computer in wired connection and wireless connection are different.

- **Modify the LAN IP address of the router.**

 Note:

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

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



LAN Settings	
MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
<input type="button" value="Save"/>	

- **Restart the modem and the router.**

- 1) Power off your modem and the router, and leave them off for 1 minute.
- 2) Power on your modem first, and wait about 2 minutes.
- 3) Power on the router, and wait another 1 or 2 minutes and check the internet access.

- **Double check the Internet Connection Type.**

- 1) Confirm your Internet Connection Type, which can be learned from the ISP.
- 2) Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
- 3) Go to **Network > WAN**.
- 4) Select your **WAN Connection Type** and fill in other parameters.
- 5) Click **Save**.

- 6) Restart the modem and the router.
- Please upgrade the firmware of the router.
- If you've tried every method above but cannot access the internet, please contact the technical support.

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

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

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

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

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



- 2) If you cannot find the PIN or PIN failed, you may choose [Connecting using a security key instead](#), and then type in the [Wireless Password/Network Security Key](#).
- 3) If it continues to show note of [Network Security Key Mismatch](#), it is suggested to confirm the wireless password of your wireless router.

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

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
 - Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again.
 - Change the wireless Channel of the router to 1,6,or 11 to reduce interference from other networks.
 - Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.  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 © 2020 TP-Link Technologies Co., Ltd. All rights reserved.

FCC compliance information statement



Product Name: 300Mbps Wireless N Router

Model Number: TL-WR841N

Component Name	Model
I.T.E. Power Supply	T090060-2B1

Responsible party:

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

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

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

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

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

Issue Date: 2020-03-09

FCC compliance information statement

Product Name: I.T.E. Power Supply

Model Number: T090060-2B1

Responsible party:

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

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

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

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

Issue Date: 2020-03-09

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)

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.

Canadian Compliance Statement

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

1. This device may not cause interference, and
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.

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

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

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

安全諮詢及注意事項

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

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 з 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.

For EU/PL/RO Version

Power consumption	
Operating mode	Power consumption (W)
Off-mode condition	0.1
Networked standby when wired network ports are connected and all wireless network ports turn off	2.1
Networked standby when all LAN ports are disconnected and wireless network ports are activated	2.3
Networked standby when all wired network ports are connected and all wireless network ports are activated	3.2
Power management	
The default period of time after which the power management function, or a similar function, switches the equipment automatically into a condition providing networked standby	<1 minute