

TP-LINK®

TL-WR843N

User Guide

300Mbps Wireless AP/Client Router

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview	3
1. 2. Appearance.....	3
Chapter 2. Connect the Hardware.....	5
2. 1. Position Your Router.....	6
2. 2. Connect Your Router	6
Chapter 3. Set Up Internet Connection Via Quick Setup Wizard	9
3. 1. Log into the Router.....	10
3. 2. Configure the Router	10
Chapter 4. Configure the Router in WISP Client Router Mode	16
4. 1. Status.....	17
4. 2. WPS	18
4. 3. Working Mode	20
4. 4. Network	21
4. 5. Wireless.....	29
4. 6. Guest Network.....	35
4. 7. DHCP	37
4. 8. Forwarding	39
4. 9. Security.....	43
4. 10. Parental Controls.....	48
4. 11. Access Control	50
4. 12. Advanced Routing	52
4. 13. Bandwidth Control	54
4. 14. IP&MAC Binding.....	55
4. 15. Dynamic DNS	57
4. 16. System Tools	60
4. 17. Logout.....	68
Chapter 5. Configure the Router in Standard Wireless Router Mode.	69

5. 1.	Status.....	70
5. 2.	WPS	71
5. 3.	Working Mode	73
5. 4.	Network	73
5. 5.	Wireless.....	82
5. 6.	Guest Network.....	88
5. 7.	DHCP	90
5. 8.	Forwarding	92
5. 9.	Security.....	96
5. 10.	Parental Controls	101
5. 11.	Access Control	103
5. 12.	Advanced Routing	105
5. 13.	Bandwidth Control	107
5. 14.	IP&MAC Binding.....	108
5. 15.	Dynamic DNS	110
5. 16.	IPv6 Support	113
5. 17.	System Tools	119
5. 18.	Logout.....	127

Chapter 6. Configure the Router in Repeater Mode 129

6. 1.	Status.....	130
6. 2.	Working Mode	131
6. 3.	Network	131
6. 4.	Wireless.....	132
6. 5.	DHCP	139
6. 6.	System Tools	141
6. 7.	Logout.....	148

FAQ..... 149

About This Guide

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

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

Conventions

In this guide the following conventions are used:

Convention	Description
<i>Blue Italic</i>	Hyperlinks are in blue italic. You can click to redirect to a website or a specific section.
Blue	Contents to be emphasized and texts on the web page are in blue, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	Indicates important information that helps you make better use of your device.

More Info

- The latest software, management app and utility can be found at [Download Center](http://www.tp-link.com/support) at <http://www.tp-link.com/support>.
- The Quick Installation Guide (QIG) can be found where you find this guide or inside the package of the router.
- Specifications can be found on the product page at <http://www.tp-link.com>.
- A Technical Support Forum is provided for you to discuss our products at <http://forum.tp-link.com>.
- Our Technical Support contact information can be found at the [Contact Technical Support](http://www.tp-link.com/support) page at <http://www.tp-link.com/support>.

Chapter 1

Get to Know About Your Router

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

This chapter contains the following sections:

- *Product Overview*
- *Appearance*



1.1. Product Overview




The TP-LINK router, with multiple operation modes, is designed to meet the wireless needs of almost any situation you might encounter. It is specially designed for Wireless ISP users, enabling wireless access to the Internet in areas with no wired ISP infrastructure. With a high wireless speed, it is ideal for interruption-sensitive applications like HD video streaming. It can also serve as a normal wireless router. Moreover, it supports Passive Power over Ethernet, which is quite convenient for deployment in areas without power supply, such as in a backyard or an attic.

1.2. Appearance



LED Explanation

LED	Status	Indication
 (Power)	On	The router is on.
	Off	The router is off.
	Blinking	The router is initializing or upgrading.
 (Wi-Fi)	On	The wireless is working properly.
	Off	The wireless is disabled.

LED	Status	Indication
 (LAN)	On	A device is connected to the corresponding LAN port.
	Off	No device is connected to the corresponding LAN port.
 (WAN)	Green	The router is connected to the Internet.
	Orange	The INTERNET port is connected, but there is no Internet connection.
	Off	The INTERNET port is not connected.
 (WPS)	Slow blinking	WPS connection is in progress.
	On	WPS connection is successful. The LED will go off in 5 minutes.
	Quick blinking	WPS connection fails.

Port and Button Description

Item	Description
ON/OFF	To turn on or off the router, press the ON/OFF button.
POWER	Connect the router to the provided power adapter.
INTERNET	Connect a DSL/cable modem to the INTERNET port.
LAN (1-4)	Connect an Ethernet-enabled device to the local network.
Operation Mode Switch	Toggle to select the router's operation mode between ROUTER and WISP. You can also set the mode via the router's web interface, after which the operation mode switch will be disabled.
WPS/RESET	To establish WPS connection, press the WPS/RESET button.
	To restore the router to its factory defaults, press and hold the WPS/RESET button for more than 5 seconds.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- *Position Your Router*
- *Connect Your Router*

2.1. Position Your Router

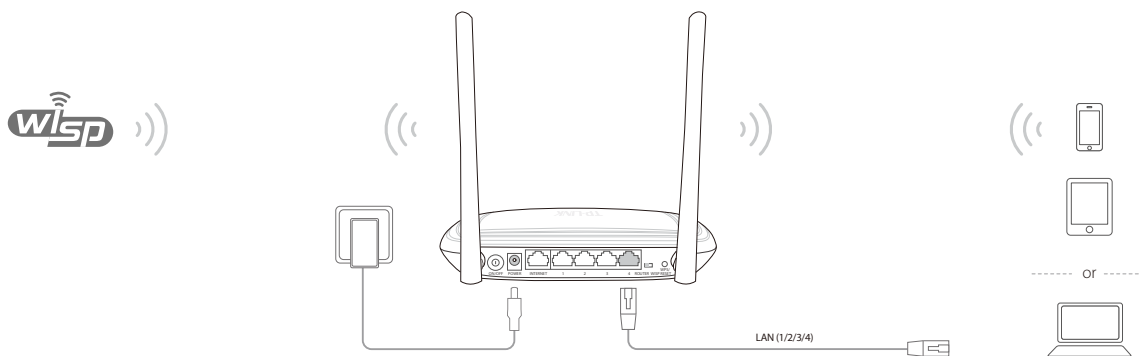
- The router should not be located where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so that they do not create a tripping hazard.
- The router can be placed on a shelf or desktop.
- Keep the router away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.2. Connect Your Router

There are three operation modes supported by this router: WISP Client Router, Standard Wireless Router and Repeater. Please determine the operation mode you need and carry out the corresponding steps.

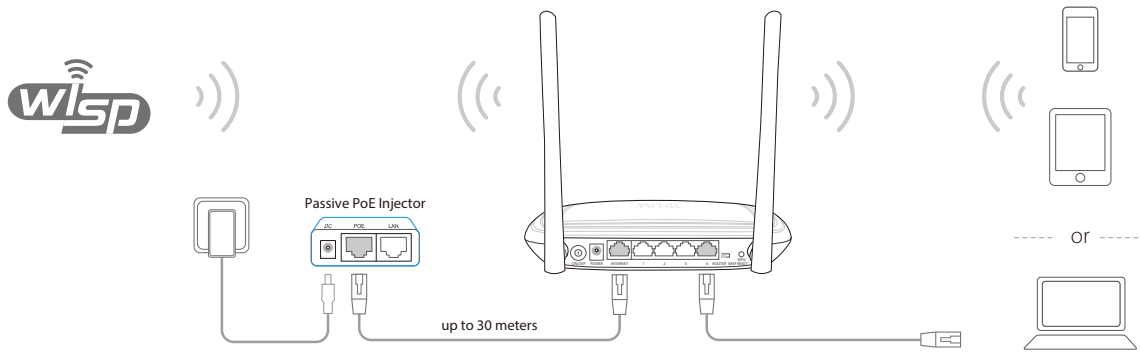
WISP Client Router Mode

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



1. Connect the power adapter to your router and plug the power adapter into an outlet, and then press the **ON/OFF** button to turn on the router.
2. Connect your device to the router wirelessly or via an Ethernet cable. The Wi-Fi network name and password are on the router's label.

When the router is installed in a location far from a power outlet, power the router with the included passive PoE injector.

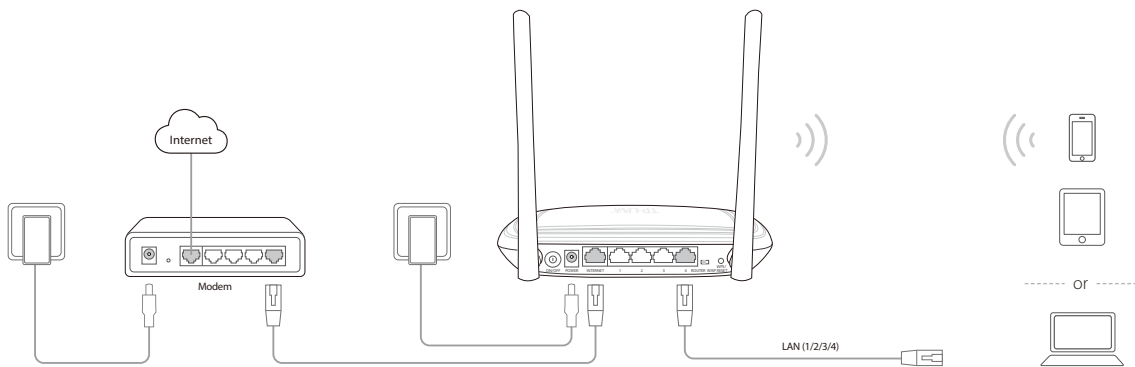


Note:

If you need to use a longer Ethernet cable (not exceeding 100 meters), TP-LINK's 48V PoE adapters such as TL-POE200, TL-POE150S and TL-POE10R are recommended.

Standard Wireless Router Mode

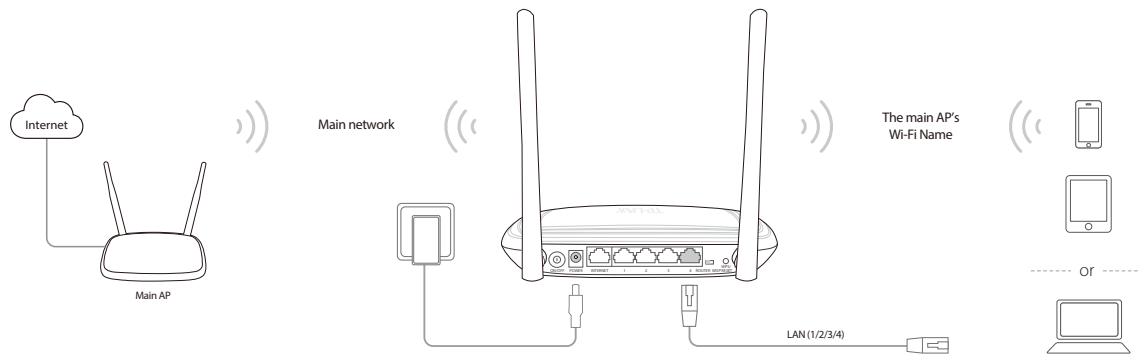
Create an instant private wireless network and share Internet to multiple Wi-Fi devices. This mode is suitable for hotel rooms and home networks.



1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to the INTERNET port on the router via an Ethernet cable and press the **ON/OFF** button on the router.
3. Turn on the modem and wait for it to restart.
4. Connect your device to the router wirelessly or via an Ethernet cable. The Wi-Fi network name and password are on the router's label.

Repeater Mode

Repeat signal from an existing wireless network. This mode is suitable to extend wireless coverage, reaching devices that were previously too far from your primary AP to maintain a stable wireless connection. The repeated signal will display the same network name and password as those of your existing wireless network.



1. Connect the power adapter to your router and plug the power adapter into an outlet, and then press the **ON/OFF** button to turn on the router.
2. Connect your device to the router wirelessly or via an Ethernet cable. The Wi-Fi network name and password are on the router's label.

Chapter 3

Set Up Internet Connection Via Quick Setup Wizard

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

This chapter contains the following sections:

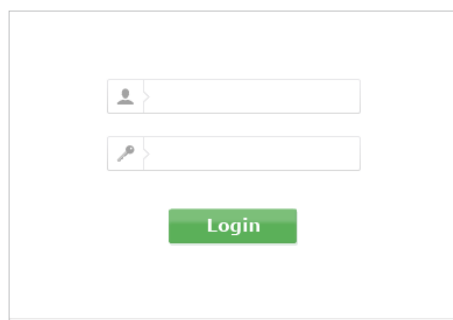
- *Log into the Router*
- *Configure the Router*

3.1. Log into the Router

With a 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 into your router.

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

A screenshot of a web-based login form. It features two input fields: the top one has a person icon and the bottom one has a key icon. Below the fields is a green button labeled "Login".

Note:

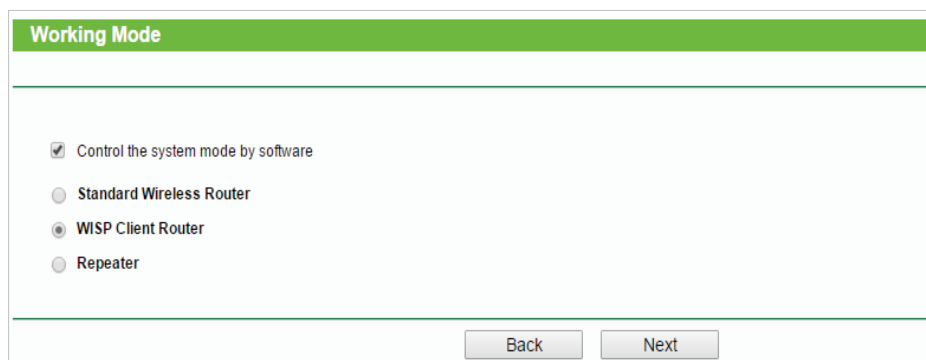
If the login window does not appear, please refer to the [FAQ](#) Section.

3.2. Configure the Router

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

1. Go to [Quick Setup](#) and click [Next](#) to start.
2. Check [Control the system mode by software](#), choose the working mode you need and then click [Next](#). Then follow the corresponding steps to connect your router to the Internet.

Note: When [Control the system mode by software](#) is checked, the operation mode switch on the router will be disabled. If you want to enable it, please log into the web management page and go to [Working Mode](#) to uncheck [Control the system mode by software](#).

A screenshot of the "Working Mode" configuration screen. It has a green header bar with the text "Working Mode". Below the header, there is a checked checkbox labeled "Control the system mode by software". Underneath, there are three radio button options: "Standard Wireless Router", "WISP Client Router" (which is selected), and "Repeater". At the bottom of the screen, there are two buttons: "Back" and "Next".

WISP Client Router Mode

1. Select the [WAN Connection Type](#). When using the router in a hotel room or a small office, select [Dynamic IP](#).

Quick Setup - WAN Connection Type

The Quick Setup is preparing to set up your internet connection, please choose one type below according to your ISP. The detailed description will be displayed after you choose the corresponding type.

- Dynamic IP (Most Common Cases)**
For Cable/DSL/Broadband connection which makes your computer immediately online without any setting or signing-in.
- Static IP**
- PPPoE/Russian PPPoE**
- L2TP/Russian L2TP**
- PPTP/Russian PPTP**

Note: For users in some areas (such as Russia, Ukraine etc.), please contact your ISP to choose connection type manually.

Back Next

2. In this case, we take dynamic IP that requires no more parameters for instance. For other connection types, please enter the parameters provided by your ISP.
3. Click [Survey](#) to find the public Wi-Fi network and click [Connect](#). Enter the public Wi-Fi password in the [Password](#) field. In the [AP Setting](#) section, either customize your [Local SSID](#) and [Wireless Password](#) or keep the default ones, and then click [Next](#).

Quick Setup - Wireless

Client Setting

SSID:

BSSID: Example:00-1D-0F-11-22-33

Key type:

WEP Index:

Auth type:

Password:

AP Setting

Local SSID:

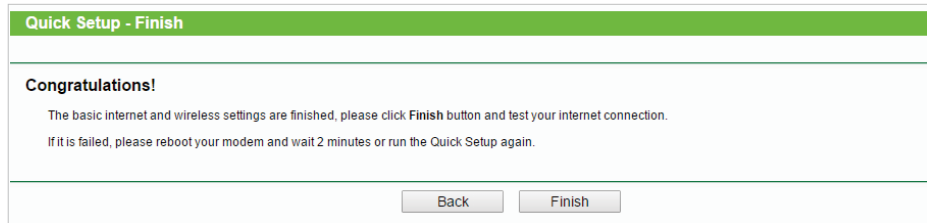
Wireless Security Mode:

Wireless Password:

You can 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. For good security it should be of ample length and should not be a commonly known phrase.

Back Next

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

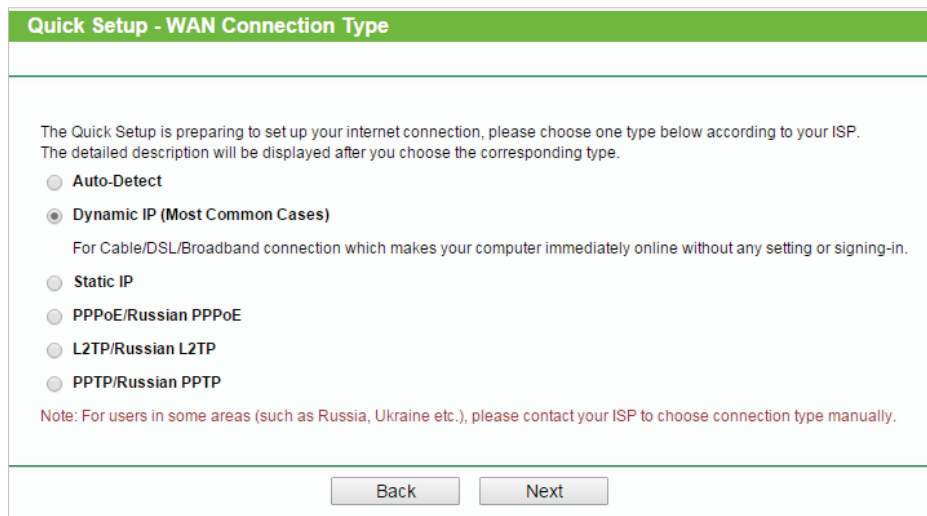


Standard Wireless Router Mode

1. Select the [WAN Connection Type](#). When using the router in a hotel room or a small office, select [Dynamic IP](#).

Note:

- If you use DSL line and you are only provided an account name and a password by your ISP, select [PPPoE](#).
- If you use cable TV or fiber cable, select [Dynamic IP](#).
- If you are provided with more information such as an IP address, Subnet Mask and Default Gateway, select [Static IP](#).
- Contact your ISP if you are not sure about the WAN connection information. You can also select [Auto-Detect](#) to let the router detect your connection type automatically.



2. In this case, we take dynamic IP for instance. Please select to clone the mac address or not and click [Next](#). For other connection types, please enter the parameters provided by your ISP, and then click [Next](#).

Quick Setup - MAC Clone

MAC(Media Access Control) address is a unique identifier that identifies your computer or device in the network. Some of the ISPs may register the MAC address of your computer which firstly connects to their services, and would not allow the Internet connection for any new computer or router.TP-LINK router can help you to "clone" or replicate the registered MAC address of your first computer.

In most of the cases, there is no need to clone the MAC address. But if you can't get the Internet connection after Quick Setup, please run it again and clone the MAC address for a try.

No, I do NOT need to clone MAC address.
 YES, I need to clone MAC address.

Note: please make sure your current computer is the one initially connected to your modem or ISP's device.

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

Quick Setup - Wireless

The Internet settings have been completed, now please configure the wireless settings.

Wireless Radio: (dropdown menu)

Wireless Network Name: (Also called the SSID)

Wireless Security:

Disable Security
 WPA-PSK/WPA2-PSK

Wireless Password:
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

No Change
(use the current security settings.)

More Advanced Wireless Settings

4. Click [Reboot](#) to complete the configuration. Now your computers and wireless devices can connect to the Internet!

Quick Setup - Finish

Congratulations!

The basic internet and wireless settings are finished, please click **Finish** button and test your internet connection.
If it is failed, please reboot your modem and wait 2 minutes or run the Quick Setup again.

The change of working mode config will not take effect until this device reboot.

Repeater Mode

1. Click [Survey](#) to find your host network and click [Connect](#). Enter the host network's password in the [Wireless Password](#) field, and then click [Next](#).

The screenshot shows the 'Quick Setup - Wireless' configuration page. The title bar is green with the text 'Quick Setup - Wireless'. Below the title bar, the page is titled 'Repeater Mode Setting:'. There are several fields and options:

- Wireless Name of Root AP:** A text input field with the note '(also called SSID)' to its right.
- MAC Address of Root AP:** A text input field.
- Survey:** A button.
- WDS Mode:** A dropdown menu set to 'Auto'.
- Wireless Security Mode:** A dropdown menu set to 'Most Secure(WPA/WPA2-PSK)'. Below this is a note: 'All security settings, for example the wireless password should match the Root AP.'
- Wireless Password:** A text input field containing '01234567'. Below this is a note: 'You can 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. For good security it should be of ample length and should not be a commonly known phrase.'

At the bottom of the page are two buttons: 'Back' and 'Next'.

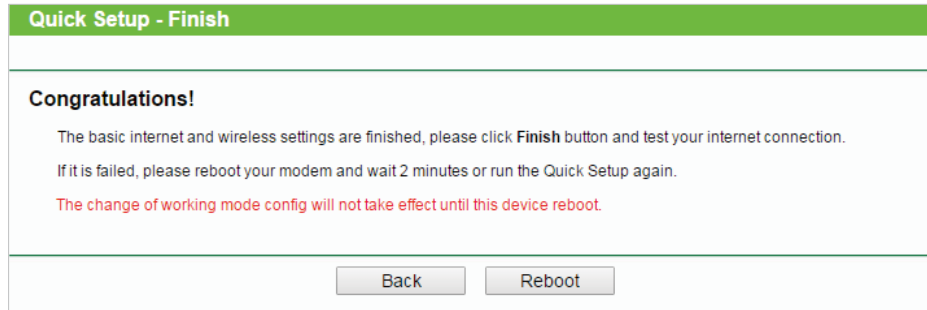
2. Select the LAN IP type of the router or leave the default setting [Smart IP](#) for most cases, and then click [Next](#).

The screenshot shows the 'Quick Setup - Network Setting' configuration page. The title bar is green with the text 'Quick Setup - Network Setting'. Below the title bar, the page is titled 'Network Setting:'. There are several fields and options:

- Type:** A dropdown menu set to 'Smart IP(DHCP)'. Below this is a note: '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).'
- IP Address:** A text input field containing '192.168.0.254'.
- Subnet Mask:** A dropdown menu set to '255.255.255.0'. Below this is a note: 'We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.'
- DHCP Server:** Two radio buttons: 'Disable' (selected) and 'Enable'.

At the bottom of the page are two buttons: 'Back' and 'Next'.

3. Click [Reboot](#) to complete the configuration.



4. Relocate the router about **halfway** between your host AP and the Wi-Fi dead zone. The extended network shares the **same network name** and **password** as those of your host network.

Chapter 4

Configure the Router in WISP Client Router Mode

This chapter presents how to configure the various features of the router working as a WISP Client Router.

This chapter contains the following sections:

- *Status*
- *WPS*
- *Working Mode*
- *Network*
- *Wireless*
- *Guest Network*
- *DHCP*
- *Forwarding*
- *Security*
- *Parental Controls*
- *Access Control*
- *Advanced Routing*
- *Bandwidth Control*
- *IP&MAC Binding*
- *Dynamic DNS*
- *System Tools*
- *Logout*

4.1. 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 in WISP Client Router Mode.

Status		
Firmware Version:	3.16.9 Build 151119 Rel.64285n	
Hardware Version:	V02.10n v1 20090908	
LAN		
MAC Address:	00-0A-EB-13-09-19	
IP Address:	192.168.0.254	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_0919	
Channel:	3	
Mode:	11bgn mixed	
Channel Width:	Automatic	
MAC Address:	00-0A-EB-13-09-19	
Client Status:	Init...	
WAN		
MAC Address:	00-0A-EB-13-09-1A	
IP Address:	192.168.1.104 Dynamic IP	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.161 <input type="button" value="Release"/>	
DNS Server:	192.168.1.161, 0.0.0.0	
Traffic Statistics		
	Received	Sent
Bytes:	0	0
Packets:	0	0
System Up Time: 0 days 00:02:14 <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 > Wireless Settings](#) page.
 - **Wireless Radio** - Indicates whether the wireless feature is enabled or not.
 - **Name (SSID)** - The SSID of the router.
 - **Channel** - The current wireless channel in use.
 - **Mode** - The current wireless working mode in use.

- [Channel Width](#) - The current wireless channel width in use.
- [MAC Address](#) - The physical address of the router.
- [Client Status](#) - The status of client. [Init](#): Connection is down; [Scan](#): Try to find the AP; [Auth](#): Try to authenticate; [ASSOC](#): Try to associate; [Run](#): Associated successfully.
- [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 WAN 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.
- [Traffic Statistics](#) - The router's traffic statistics.
 - [Received \(Bytes\)](#) - Traffic in bytes received from the WAN port.
 - [Received \(Packets\)](#) - Traffic in packets received from the WAN port.
 - [Sent \(Bytes\)](#) - Traffic in bytes sent out from the WAN port.
 - [Sent \(Packets\)](#) - Traffic in packets sent out from the WAN port.
- [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. 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.

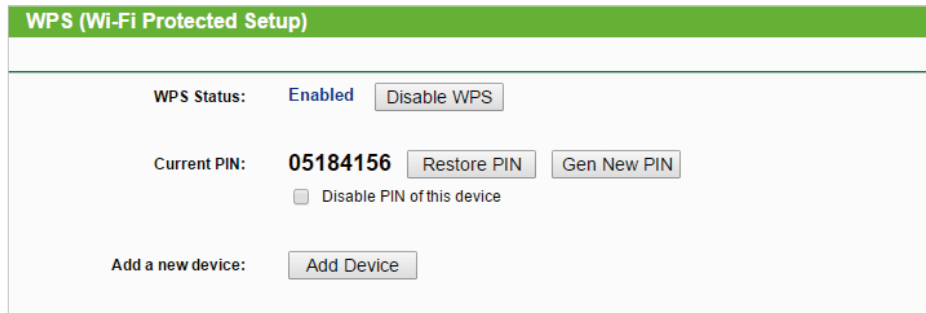
■ **Note:**

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 [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)

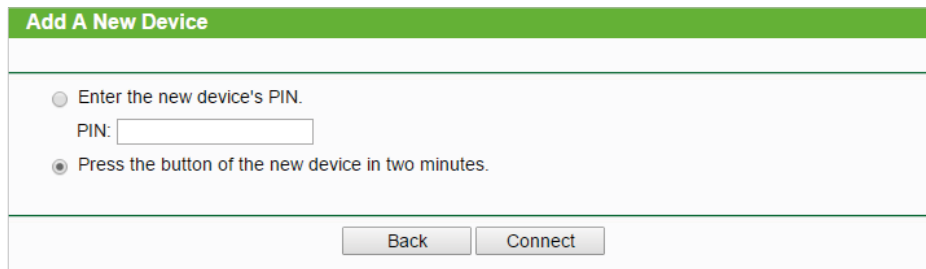
WPS Status: [Enabled](#)

Current PIN: **05184156**

Disable PIN of this device

Add a new device:

2. Select [Press the button of the new device in two minutes](#) and click [Connect](#).



Add A New Device

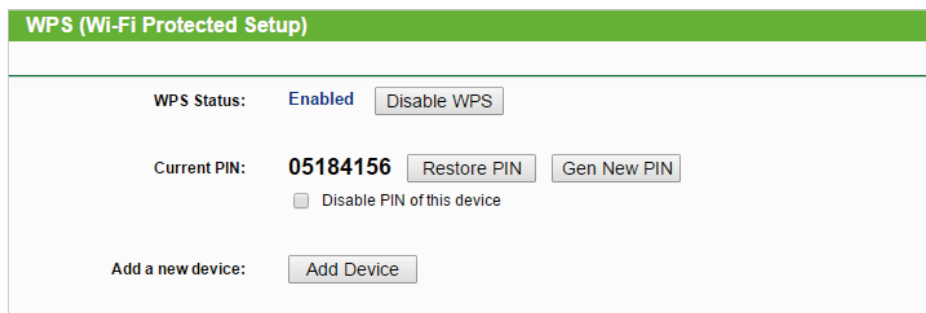
Enter the new device's PIN.
PIN:

Press the button of the new device in 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](#).



WPS (Wi-Fi Protected Setup)

WPS Status: [Enabled](#)

Current PIN: **05184156**

Disable PIN of this device

Add a new device:

2. Select [Enter the new device's PIN](#), enter your client device's current PIN in the [PIN](#) field and click [Connect](#).

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.

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

4.3. Working Mode

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

Note: When **Control the system mode by software** is checked, the operation mode switch on the router will be disabled. If you want to enable it, please log into the web management page and go to **Working Mode** to uncheck **Control the system mode by software**.

4.4. Network

4.4.1. 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 LAN 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.

WAN

WAN Connection Type:

IP Address: 192.168.1.104
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Use These DNS Servers
Primary DNS:
Secondary DNS: (Optional)

Host Name:

Get IP with Unicast DHCP (It is usually not required.)

- [MTU Size](#) - 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.
- [Use These DNS Servers](#) - If your ISP provides you one or two DNS addresses, select [Use These DNS Servers](#) and enter the primary and secondary addresses. Otherwise, the DNS servers will be assigned dynamically from your ISP.
- [Host Name](#) - This option specifies the name of the router.
- [Get IP with Unicast DHCP](#) - 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.)

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 configuration interface with the following fields and values:

- WAN Connection Type:** Static IP (selected in dropdown), with a Detect button.
- IP Address:** 0.0.0.0
- Subnet Mask:** 0.0.0.0
- Default Gateway:** 0.0.0.0
- MTU Size (in bytes):** 1500 (The default is 1500, do not change unless necessary.)
- Primary DNS:** 0.0.0.0
- Secondary DNS:** 0.0.0.0 (Optional)
- Save** button 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.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - 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.
- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

PPPoE/Russia PPPoE

If your ISP provides a PPPoE connection, select [PPPoE/Russia PPPoE](#).

The screenshot shows the WAN configuration interface with the following fields and values:

- WAN Connection Type:** PPPoE/Russia PPPoE (selected in dropdown), with a Detect button.
- PPPoE Connection:**
 - User Name:** username
 - Password:** *****
 - Confirm Password:** *****
- Secondary Connection:**
 - Disabled
 - Dynamic IP
 - Static IP (For Dual Access/Russia PPPoE)
- Wan Connection Mode:**
 - Connect on Demand
 - Max Idle Time: 15 minutes (0 means remain active at all times.)
 - Connect Automatically
 - Time-based Connecting
 - Period of Time: from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
 - Connect Manually
 - Max Idle Time: 15 minutes (0 means remain active at all times.)
- Connect** | **Disconnect** | **Disconnected!** buttons.
- Save** | **Advanced** buttons at the bottom.

- **User Name/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.
- **WAN Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **Time-based Connecting** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).
 - **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:

1. Only when you have configured the system time on the [System Tools > Time Settings](#) page, will the Time-based Connecting function take effect.
2. 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.

If you want to do some advanced configurations, please click [Advanced](#).

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

Use IP Address Specified by ISP

ISP Specified IP Address:

Detect Online Interval: Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)

Use The Following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

- **MTU Size** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the router, please select **Use IP address specified by ISP** and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online 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.
- **Primary DNS/Secondary DNS** - If your ISP does not automatically assign DNS addresses to the router, please select **Use the following DNS servers** 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.

BigPond Cable

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

The screenshot shows the WAN configuration interface with a green header labeled 'WAN'. The 'WAN Connection Type' is set to 'BigPond Cable'. Below this, there are input fields for 'User Name', 'Password', 'Auth Server' (containing 'sm-server'), and 'Auth Domain'. The 'MTU Size (in bytes)' is set to '1500' with a note: '(The default is 1500, do not change unless necessary.)'. Under 'Connection Mode', there are three radio buttons: 'Connect on Demand' (with a 'Max Idle Time' of 15 minutes), 'Connect Automatically' (which is selected), and 'Connect Manually' (with a 'Max Idle Time' of 15 minutes). At the bottom, there are 'Connect', 'Disconnect', and 'Disconnected!' buttons, and a 'Save' button at the very bottom.

- **User Name/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 Size** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Connection Mode**

- **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 Automatically** - The connection can be re-established automatically when it is down.
- **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.

L2TP/Russia L2TP

If your ISP provides L2TP connection, please select **L2TP/Russia L2TP**.

The screenshot shows the WAN configuration interface for L2TP/Russia L2TP. The page has a green header with the text 'WAN'. Below the header, the 'WAN Connection Type' is set to 'L2TP/Russia L2TP'. The 'User Name' field contains 'username', and the 'Password' and 'Confirm Password' fields are masked with asterisks. There are three buttons: 'Connect', 'Disconnect', and 'Disconnected!'. The 'Dynamic IP' radio button is selected, and the 'Static IP' radio button is unselected. The 'Server IP Address/Name' field is empty. The 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS' fields all contain '0.0.0.0'. The 'Internet IP Address' field contains '0.0.0.0' and the 'Internet DNS' field contains '0.0.0.0, 0.0.0.0'. The 'MTU Size (in bytes)' field contains '1460' with a note '(The default is 1460, do not change unless necessary.)'. The 'Max Idle Time' field contains '15' with a note 'minutes (0 means remain active at all times.)'. The 'Connection Mode' section has three radio buttons: 'Connect on Demand' (unselected), 'Connect Automatically' (selected), and 'Connect Manually' (unselected). A 'Save' button is at the bottom.

- **User Name/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.
- **Connect/Disconnect** - Click this button to connect or disconnect immediately.

- **Dynamic IP/ Static IP** - Select either as required by your ISP. If **Static IP** is selected, please enter the IP address, subnet mask, gateway and DNS also provided by your ISP.
- **Internet IP Address/ Internet DNS** - The Internet IP address and DNS server address assigned by L2TP server.
- **Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **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/Russia PPTP

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

The screenshot shows the WAN configuration interface. At the top, there's a green header with the text 'WAN'. Below it, the 'WAN Connection Type' is set to 'PPTP/Russia PPTP'. The 'User Name' field contains 'username', and both 'Password' and 'Confirm Password' fields are masked with asterisks. There are 'Connect', 'Disconnect', and 'Disconnected!' buttons. Under 'Server IP Address/Name', 'Dynamic IP' is selected. The 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS' fields all contain '0.0.0.0'. The 'Internet IP Address' and 'Internet DNS' fields also contain '0.0.0.0'. The 'MTU Size (in bytes)' is set to '1420' with a note '(The default is 1420, do not change unless necessary.)'. The 'Max Idle Time' is set to '15' minutes. Under 'Connection Mode', 'Connect Automatically' is selected. A 'Save' button is at the bottom.

- **User Name/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.
- **Connect/Disconnect** - Click this button to connect or disconnect immediately.
- **Dynamic IP/ Static IP** - Select either as required by your ISP. If **Static IP** is selected, please enter the IP address, subnet mask, gateway and DNS also provided by your ISP.
- **Internet IP Address/ Internet DNS** - The Internet IP address and DNS server address assigned by L2TP server.
- **Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **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.

4.4.2. 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](#).

- [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:

1. You can only use the MAC Address Clone function for PCs on the LAN.
2. 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.

4.4.3. 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](#).

- [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 (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.
- **IGMP Proxy** - The Internet Group Management Protocol (IGMP) feature allow you to watch TV on IPTV-supported devices in the LAN .

■ **Note:**

1. If you have changed the IP address, you must use the new IP address to login.
2. 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.

4.5. Wireless

4.5.1. Wireless Settings

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

Wireless Settings

Client Setting

SSID:

BSSID: Example:00-1D-0F-11-22-33

Key type:

WEP Index:

Auth type:

Password:

AP Setting

Local SSID:

Enable Wireless Router Radio

Enable SSID Broadcast

Disable Local Wireless Access

- **Client Setting** - The settings of the public Wi-Fi your router is going to connect to.
 - **SSID** - The SSID of the public Wi-Fi your router is going to connect to as a client.
 - **BSSID** - The MAC address of the public Wi-Fi your router is going to connect to as a client.

- [Survey](#) - Click this button to search the public Wi-Fi.
- [Key type](#) - Select the key type according to the public Wi-Fi's security configuration. It is recommended that the key type is the same as the public Wi-Fi's security type.
- [WEP Index](#) - Select which of the four keys will be used if the key type is WEP (ASCII) or WEP (HEX).
- [Auth Type](#) - Select the authorization type if the key type is WEP (ASCII) or WEP (HEX).
- [Password](#) - Enter the public Wi-Fi's password if required.
- [AP Setting](#) - The wireless settings of your router.
 - [Local SSID](#) - Enter a string of up to 32 characters. It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
 - [Enable Wireless Router Radio](#) - The wireless radio of the router can be enabled or disabled to allow or deny wireless access. If enabled, the wireless clients will be able to access the router.
 - [Enable SSID Broadcast](#) - If enabled, the router will broadcast the wireless network name (SSID).
 - [Disable Local Wireless Access](#) - If you select this option, the wireless clients will not be able to connect to the router.

4.5.2. 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

Disable Security

WPA/WPA2 - Personal(Recommended)

Version:

Encryption:

Wireless Password:
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds
(Keep it default if you are not sure, minimum is 30, 0 means no update)

WPA/WPA2 - Enterprise

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

WEP

Type:

WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 2: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 3: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 4: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>

- **Disable 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 **Automatic**, **WPA-PSK** or **WPA2-PSK**.
 - **Encryption** - Select **Automatic**, **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 **Automatic**, **WPA** or **WPA2**.
 - **Encryption** - Select **Automatic**, **TKIP** or **AES**.
 - **Radius Server IP** - Enter the IP address of the Radius server.
 - **Radius Port** - Enter the port that Radius server used.
 - **Radius 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.

- **Type** - The default setting is **Automatic**, 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, 128-bit or 152-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.
- **152-bit** - Enter 32 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 16 ASCII characters.

4.5.3. 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.

- 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) Leave the status as **Enabled**.
 - 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete

Done!

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

4.5.4. 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.

- **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.
- **RTSThreshold** - 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 WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

4.5.5. 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 Statistics						
Current Connected Wireless Stations numbers:					1	<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure	
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	<input type="button" value="Allow"/>	

- [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.
- [Configure](#) - The button is used for loading the item to the Wireless MAC Filtering list.
 - [Allow](#) - If the Wireless MAC Filtering function is enabled, click this button to allow the client to access your network.
 - [Deny](#) - If the Wireless MAC Filtering function is enabled, click this button to deny the client to access your network.

4.6. Guest Network

This function 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 > Wireless Settings](#).
3. Enable the [Guest Network](#) function.
4. Create a network name for your guest network.
5. Select the [Wireless 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](#).

- **Allow Guest To Access My Local Network** - If enabled, clients on the guest network can also access the local network.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.
- **Egress Bandwidth For Guest Network** - The upload speed through the INTERNET port for the guest network.
- **Ingress Bandwidth For Guest Network** - The download speed through the INTERNET port for the guest network.
- **Guest Network** - Check to enable **Guest Network**.
- **Network Name** - Enter a string of up to 32 characters. It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
- **Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router's guest network without a password. It's strongly recommended to choose **WPA/WPA2 - Personal** as the security type.

If WPA/WPA2 - Personal is selected:

- **Version** - Select **Automatic**, **WPA-PSK** or **WPA2-PSK**.
- **Encryption** - Select **Automatic**, **TKIP** or **AES**.
- **PSK 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.

- **Access Time** - During this period, devices on the guest network can access the router.

4.7. 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.

4.7.1. 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:	<input type="text" value="192.168.0.100"/>
End IP Address:	<input type="text" value="192.168.0.199"/>
Address Lease Time:	<input type="text" value="120"/> minutes (1~2880 minutes, the default value is 1 minute)
Default Gateway:	<input type="text" value="192.168.0.254"/> (Optional)
Default Domain:	<input type="text"/> (Optional)
Primary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
Secondary DNS:	<input type="text" value="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 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.
- **Primary DNS (Optional)** - Input the DNS IP address provided by your ISP.

- **Secondary DNS (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](#).

4.7.2. DHCP Client List

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

DHCP Client List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the dynamic IP 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](#).

4.7.3. 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 blank.

- 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**.

4.8. Forwarding

Router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the Internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external 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 in the LAN and realize some specific functions.

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

4.8.1. Virtual Servers

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.

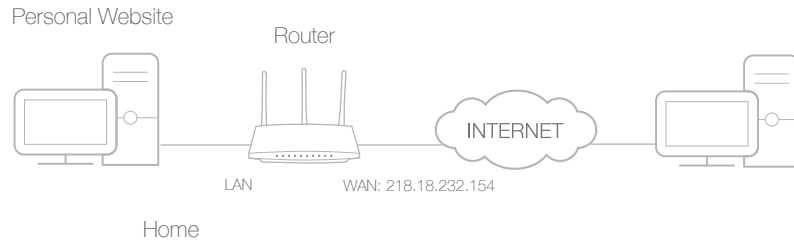
Virtual Servers can be used to set up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service 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 in 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 Servers**.
4. Click **Add New**. Select **HTTP** from the **Common Service Port** list. The service port, internal port and protocol will be automatically filled with contents. Enter the PC's IP address 192.168.0.100 in the **IP Address** field.

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text" value="80"/> (XX-XX or XX)
Internal Port:	<input type="text" value="80"/> (XX, Enter a specific port number or leave it blank)
IP Address:	<input type="text" value="192.168.0.100"/>
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 in the Internet can enter [http:// WAN IP](http://WAN IP) (in this example: [http:// 218.18.232.154](http://218.18.232.154)) to visit your personal website.

Note:

If you have changed the default **Service Port**, you should use [http:// WAN IP: Service Port](http://WAN IP: Service Port) to visit the website.

4.8.2. 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 and video players. Common applications include MSN Gaming Zone, Dialpad and QuickTime 4 players, etc.

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 with contents. The following picture takes application [MSN Gaming Zone](#) as an example.

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

Note:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the [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.

4.8.3. 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 hazard. If DMZ is not in use, please disable it in time.

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

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

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.

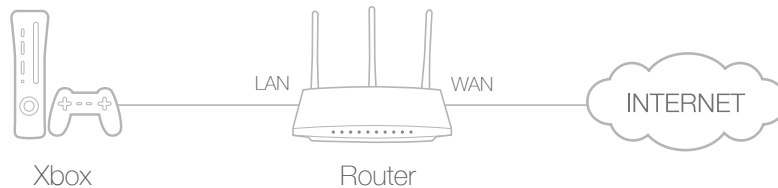
4.8.4. UPnP

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

Tips:

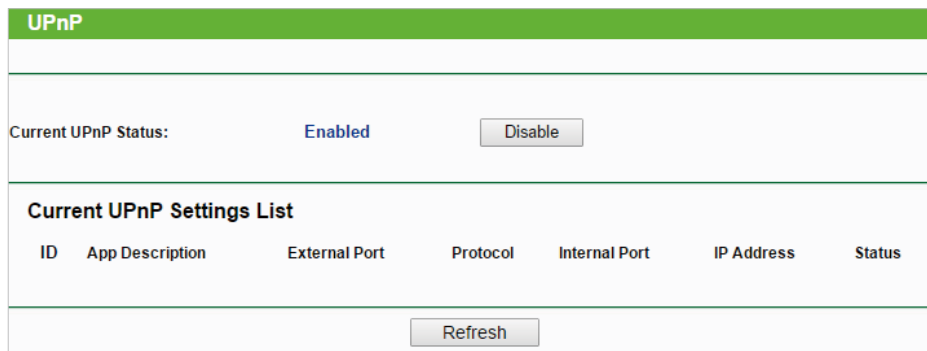
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.



4.9. Security

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

4.9.1. 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

SPI Firewall: Enable Disable

VPN

PPTP Passthrough: Enable Disable

L2TP Passthrough: Enable Disable

IPSec Passthrough: Enable Disable

ALG

FTP ALG: Enable Disable

TFTP ALG: Enable Disable

H323 ALG: Enable Disable

RTSP ALG: Enable Disable

SIP ALG: Enable 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**.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.
- **SIP ALG** - To allow some multimedia clients to communicate across NAT, click **Enable**.

3. Click **Save**.

4.9.2. 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

Packets Statistics Interval (5 ~ 60): Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering
ICMP-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Enable UDP-FLOOD Filtering
UDP-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Enable TCP-SYN-FLOOD Attack Filtering
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Ignore Ping Packet from WAN Port to Router
 Forbid Ping Packet from LAN Port to Router

- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The **Packets Statistics Interval** value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **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** - Check the box 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 Filtering** - Check the box to enable or disable 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** - Check the box 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.
- **Ignore 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.

4.9.3. 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 a web interface titled "Local Management" with a green header. Below the header, there is a section titled "Management Rules". It contains two radio button options:

- 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

 Below these options are four input fields labeled "MAC 1:", "MAC 2:", "MAC 3:", and "MAC 4:". At the bottom of this section, there is a label "Your PC's MAC Address:" followed by an input field containing the text "6C-62-6D-F7-2E-82" and a yellow "Add" button. At the very bottom of the interface is a blue "Save" button.

For example, if you want to allow PCs with specific MAC addresses to access the router's web management page 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 built-in web pages to perform administrator tasks.
- 3) Click [Add](#), 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, press and hold the [Reset](#) button to reset the router to the factory defaults.

4.9.4. 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:	<input type="text" value="80"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all)
<input type="button" value="Save"/>	

- **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:

1. 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 management page.
2. Be sure to change the router's default password for security purposes.

4. 10. 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 [Access Control](#) > [Schedule](#).
3. Click [Add New](#) to create a new schedule entry with [Schedule Description](#) as `Schedule_1`, [Day](#) as `Sat` and [Time](#) as `all day-24 hours`. And click [Save](#).

Advance Schedule Settings

Note: The Schedule is based on the time of the Router.

Schedule Description:

Day: Everyday Select Days

Mon Tue Wed Thu Fri Sat Sun

Time: all day-24 hours:

Start Time: (HHMM)

Stop Time: (HHMM)

4. Go to [Parental Control](#).
5. Select [Enable](#) and enter the MAC address 00-11-22-33-44-BB in the [MAC Address of Parental PC](#) field.
6. Click [Add New](#).

Add or Modify Parental Control Entry

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

MAC Address of Children's PC:

All MAC Address In Current LAN:

Website Description:

Allowed Website Name:

Effective Time:

The time schedule can be set in "Access Control -> [Schedule](#)"

Status:

7. Enter appropriate parameters in corresponding fields.
 - Enter 00-11-22-33-44-AA in the [MAC Address of Children's PC](#) field.
 - Enter Allow TP-LINK in the [Website Description](#) field.
 - Enter www.tp-link.com in the [Allowed Website Name](#) field.
 - Select Schedule_1 you created just now from the [Effective Time](#) drop-down list.
 - In the [Status](#) field, select [Enabled](#).
8. Click [Save](#).

Then you can go back to the Parental Control Settings page to check the following list.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow TP-LINK	Schedule_1	<input checked="" type="checkbox"/>	Edit Delete

4. 11. 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 item and content restrictions.

For example, If you want to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA in 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 [Host Description](#) field and enter 00-11-22-33-44-AA in the [MAC Address](#) field.

Add or Modify a Host Entry

Mode:

Host Description:

MAC Address:

- 3) Click [Save](#).
3. Go to [Access Control](#) > [Target](#) and configure the target settings:
 - 1) Click [Add New](#).
 - 2) Select [Domain Name](#) 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 [Domain Name](#) field.

Note:

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

Add or Modify an Access Target Entry

Mode:

Target Description:

Domain Name:

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.

Advance Schedule Settings

Note: The Schedule is based on the time of the Router.

Schedule Description:

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

Time: all day-24 hours:

Start Time: (HHMM)

Stop Time: (HHMM)

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 [Rule Name](#) field. Select [host_1](#) from the host drop-down list; select [target_1](#) from the target drop-down list; select [schedule_1](#) from the schedule drop-down list.

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**.

Done!

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

4. 12. 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. 12. 1. Static Routing 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 Routing**.
- **To add static routing entries:**
1. Click **Add New**.
 2. Enter the following information.

Add or Modify a Static Route Entry

Destination Network:
Subnet Mask:
Default Gateway:
Status: Enabled

- **Destination Network** - 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.
 - **Default Gateway** - This is the IP Address of the default gateway device that allows the contact between the router and the network or host.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
 4. Click **Save**.

You can also do the following operations to modify the current settings.

- Click **Delete** to delete the entry.
- Click **Enable All** to enable all the entries.
- Click **Disable All** to disable all the entries.
- Click **Delete All** to delete all the entries.
- Click **Previous** to view the information on the previous screen and **Next** to view the information on the next screen.

4. 12. 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

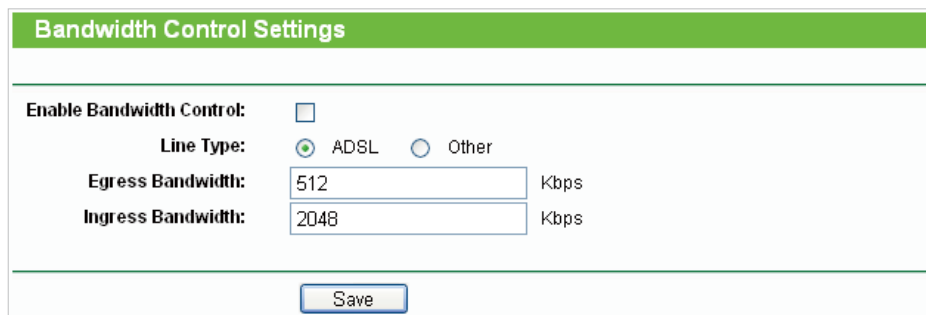
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	0.0.0.0	0.0.0.0	192.168.1.1	WAN

- **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 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. 13. Bandwidth Control

4. 13. 1. Control Settings

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



Bandwidth Control Settings	
Enable Bandwidth Control:	<input type="checkbox"/>
Line Type:	<input checked="" type="radio"/> ADSL <input type="radio"/> Other
Egress Bandwidth:	<input type="text" value="512"/> Kbps
Ingress Bandwidth:	<input type="text" value="2048"/> Kbps
<input type="button" value="Save"/>	

The values you configure for the Egress Bandwidth and Ingress Bandwidth should be less than 100,000Kbps. For optimal control of the bandwidth, please select the right Line Type and consult your ISP for the total egress and ingress bandwidth.

- **Enable Bandwidth Control** - Check this box so that the Bandwidth Control settings can take effect.
- **Line Type** - Select the right type for you network connection. If you are not sure, please consult your ISP.
- **Egress Bandwidth** - The upload speed through the INTERNET port.
- **Ingress Bandwidth** - The download speed through the INTERNET port.

4. 13. 2. Rules List

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

- Go to [Bandwidth Control > Rules List](#), and you can view and configure the Bandwidth Control rules.

Bandwidth Control Rule List							
ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							
Add New...		Delete All					
Previous		Next		Current No. 1	Page		

- Description** - This is the information about the rules such as address range.
- Egress Bandwidth** - This field displays the max and min upload bandwidth through the WAN port. The default is 0.
- Ingress Bandwidth** - This field displays the max and min download bandwidth through the WAN port. The default is 0.
- Enable** - This field displays the status of the rule.
- Modify** - Click [Modify/Delete](#) to edit/delete the rule.

➤ **To add a Bandwidth control rule:**

- Click [Add New](#).
- Enter the information like the figure shown below.

Bandwidth Control Rule Settings			
Enable:	<input checked="" type="checkbox"/>		
IP Range:	192.168.0.2	-	192.168.0.23
Port Range:	21	-	
Protocol:	TCP		
	Min Bandwidth(Kbps)		Max Bandwidth(Kbps)
Egress Bandwidth:	0		1000
Ingress Bandwidth:	0		4000
Save		Back	

- Click [Save](#).

4. 14. 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.

4.14.1. 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.

4. Click [Save](#).

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

1. Click [Add New](#).
2. Select the [Bind](#) checkbox.

3. Enter the MAC address and IP address.
4. Click [Save](#).

➤ **To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click [Modify](#) or [Delete](#) in the Modify column.

➤ **To find an existing entry:**

1. Click [Find](#).
2. Enter the MAC address or IP address in the corresponding field.
3. Click [Find](#) on this page as shown below.

Find IP & MAC Binding Entry

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind Link
2	00-14-5E-91-19-E3	192.168.1.56	<input checked="" type="checkbox"/> To page

4.14.2. ARP List

To manage a device, you can observe the device in 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

ID	MAC Address	IP Address	Status	Configure
1	40-61-86-FC-74-93	192.168.0.100	Unbound	Load Delete

- **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 **Bind All** to bind all the current items.
- Click **Load All** to load all items to the IP & MAC Binding list.
- Click **Refresh** 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.

4.15. 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.no-ip.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](#).

Comexe DDNS

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

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) received from your dynamic DNS service provider.
 2. Enter the [User Name](#) 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.

Dyndn DDNS

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

The screenshot shows the DDNS configuration interface. At the top, there is a green header with the text "DDNS". Below the header, the "Service Provider" is set to "DynDNS (dyn.com/dns)" with a dropdown arrow and a link "Go to register...". There are three input fields: "User Name:", "Password:", and "Domain Name:". Below these fields is a checkbox labeled "Enable DDNS" which is currently unchecked. The "Connection Status" is displayed as "DDNS not launching!". At the bottom of the form, there are two buttons: "Login" and "Logout". A "Save" button is located at the very bottom of the page.

To set up for DDNS, follow these instructions:

1. Enter the [User Name](#) for your DDNS account.
 2. Enter the [Password](#) for your DDNS account.
 3. Enter the [Domain Name](#) you received from dynamic DNS service provider here.
 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 configuration interface for No-IP. At the top, there is a green header with the text "DDNS". Below the header, the "Service Provider" is set to "No-IP (www.noip.com)" with a dropdown arrow and a link "Go to register...". There are three input fields: "User Name:", "Password:", and "Domain Name:". Below these fields is a checkbox labeled "Enable DDNS" which is currently unchecked. The "Connection Status" is displayed as "DDNS not launching!". At the bottom of the form, there are two buttons: "Login" and "Logout". A "Save" button is located at the very bottom of the page.

To set up for DDNS, follow these instructions:

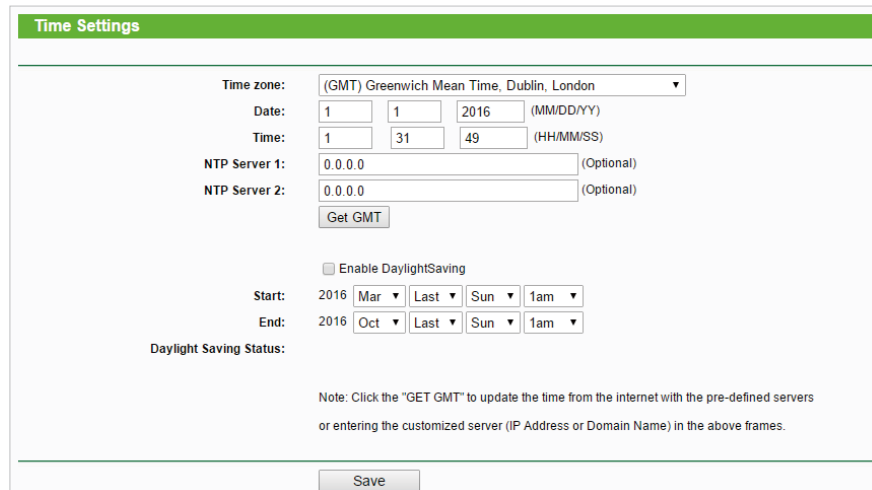
1. Enter the [User Name](#) for your DDNS account.
2. Enter the [Password](#) for your DDNS account.
3. Enter the [Domain Name](#) you received from dynamic DNS service provider.

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.

4.16. System Tools

4.16.1. Time Settings

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](#) and configure the system time as needed.



Time Settings

Time zone: (GMT) Greenwich Mean Time, Dublin, London

Date: 1 / 1 / 2016 (MM/DD/YY)

Time: 1 : 31 : 49 (HH/MM/SS)

NTP Server 1: 0.0.0.0 (Optional)

NTP Server 2: 0.0.0.0 (Optional)

[Get GMT](#)

Enable DaylightSaving

Start: 2016 Mar Last Sun 1am

End: 2016 Oct Last Sun 1am

Daylight Saving Status:

Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.

[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:

1. Select your local time zone.
2. Enter the address or domain of the [NTP Server I](#) or [NTP Server II](#).
3. Click [Get GMT](#) to get time from the Internet if you have connected to the Internet.

➤ To set Daylight Saving Time:

1. Select [Enable DaylightSaving](#).

2. Select the start time from the drop-down list in the **Start** field.
3. Select the end time from the drop-down list in the **End** field.
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 login 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**.

- **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

```

Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

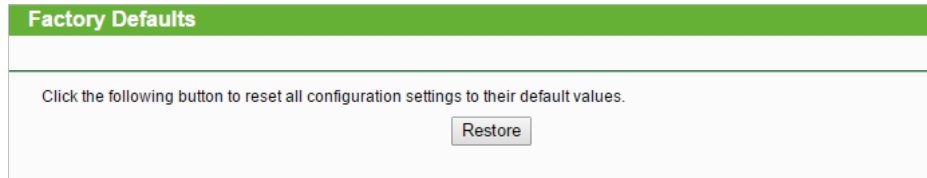
4.16.3. Firmware Upgrade

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. You can download the latest firmware file from the [Support](#) page of our website www.tp-link.com 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 **Browse** to locate the downloaded firmware file, and click **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.

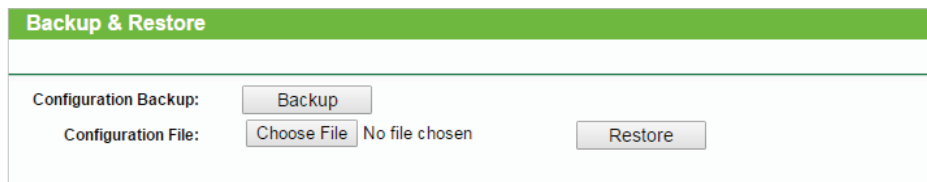


- The default **Username**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.1
- The default **Subnet Mask**: 255.255.255.0

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:**

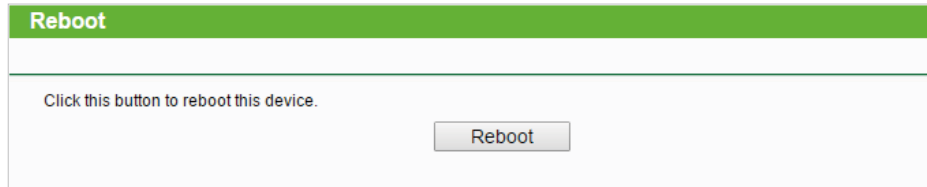
1. Click [Choose File](#) to locate the backup configuration file stored in your computer, and click [Restore](#).
2. Wait a few minutes for the restoring and rebooting.

■ **Note:**

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

4.16.6. Reboot

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.

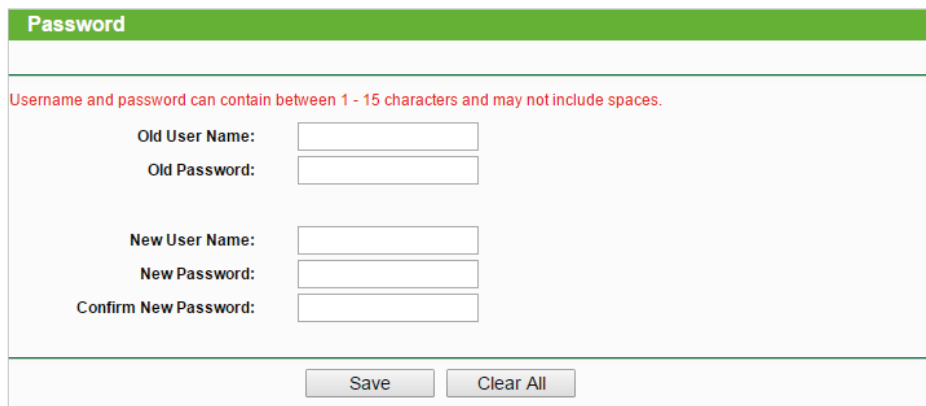


Some settings of the router will take effect only after rebooting, including:

- 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).

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.



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

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.

System Log

Auto Mail Feature: **Disabled** Mail Settings

Log Type: ALL Log Level: ALL

Index	Time	Type	Level	Log Content
5	1st day 03:05:45	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
4	1st day 03:05:41	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
3	1st day 03:05:39	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
2	1st day 03:05:37	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
1	1st day 03:04:59	DHCP	INFO	DHCPS:Recv INFORM from C0:4A:00:1A:C3:45

Time = 2016-01-01 3:13:05 11587s
H-Ver = XXXXXXXXXX : S-Ver = XXXXXXXXXX
L = 192.168.0.254 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Refresh
Save Log
Mail Log
Clear Log

Previous
Next
Current No. 1
Page

- [Auto Mail Feature](#) - Indicates whether the auto mail feature is enabled or not.
- [Mail Settings](#) - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

- **From** - Your mail box address. The router will connect it to send logs.
- **To** - Recipient's mail address. The destination mailbox which will receive logs.
- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the **From** field. You can log on the relevant website for help if you are not clear with the address.
- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need user name and password to log in.

Note:

Only when you select Authentication, do you have to enter the user name and password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is included.
- **Password** - Your mail account password.
- **Confirm The Password** - Enter the password again to confirm.
- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field.

Click **Save** to apply your settings.

Click **Back** to return to the previous page.

- **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.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.

- [Clear Log](#) - All the logs will be deleted from the router permanently, not just from the page.

Click [Next](#) to go to the next page, or click [Previous](#) to return to the previous page.

4. 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](#) > [Statistics](#), and you can view the statistics of the router, including total traffic and the value of the last Packet Statistic Interval in seconds.

- [Current Statistics Status](#) - Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will disabled.
- [Packets Statistics Interval \(5-60\)](#) - The default value is 10. Select a value between 5 and 60 in the drop-down list. The Packets Statistic Interval indicates the time section of the packets statistic.
- [Sorted Rules](#) – Choose how displayed statistics are sorted.
- Select [Auto-refresh](#) to refresh automatically. Click [Refresh](#) to refresh immediately.
- Click [Reset All](#) to reset the values of all the entries to zero.
- Click [Delete All](#) to delete all entries in the table.

Statistics Table

IP/MAC Address	The IP and MAC address are displayed with related statistics.	
Total	Packets	The total number of packets received and transmitted by the router.
	Bytes	The total number of bytes received and transmitted by the router.

Current	Packets	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
Modify	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	Reset	Reset the value of the entry to zero.
	Delete	Delete the existing entry in the table.

4.17. Logout

Click [Logout](#) at the bottom of the main menu, and you will log out of the web page and return to the login window.

Chapter 5

Configure the Router in Standard Wireless Router Mode

This chapter presents how to configure the various features of the router working as a Standard Wireless Router.

This chapter contains the following sections:

- *Status*
- *WPS*
- *Working Mode*
- *Network*
- *Wireless*
- *Guest Network*
- *DHCP*
- *Forwarding*
- *Security*
- *Parental Controls*
- *Access Control*
- *Advanced Routing*
- *Bandwidth Control*
- *IP&MAC Binding*
- *Dynamic DNS*
- *IPv6 Support*
- *System Tools*
- *Logout*

5.1. 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 in Standard Wireless Router Mode.

Status		
Firmware Version:	3.16.9 Build 151119 Rel.64285n	
Hardware Version:	V02.10n v1 20090908	
LAN		
MAC Address:	00-0A-EB-13-09-19	
IP Address:	192.168.0.254	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_0919	
Mode:	11bgn mixed	
Channel Width:	Automatic	
Channel:	Auto (Current channel 3)	
MAC Address:	00-0A-EB-13-09-19	
WDS Status:	Disable	
WAN		
MAC Address:	00-0A-EB-13-09-1A	
IP Address:	192.168.1.104 Dynamic IP	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.161 <input type="button" value="Release"/>	
DNS Server:	192.168.1.161, 0.0.0.0	
Traffic Statistics		
	Received	Sent
Bytes:	0	0
Packets:	0	0
System Up Time: 0 days 00:02:14 <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 > Wireless Settings](#) page.
 - **Wireless Radio** - Indicates whether the wireless feature is enabled or not.
 - **Name (SSID)** - The SSID of the router.
 - **Mode** - The current wireless working mode in use.
 - **Channel Width** - The current wireless channel width in use.

- [Channel](#) - The current wireless channel in use.
- [MAC Address](#) - The physical address of the router.
- [WDS Status](#) - The status of WDS connection.
- [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 WAN 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.
- [Traffic Statistics](#) - The router's traffic statistics.
 - [Received \(Bytes\)](#) - Traffic in bytes received from the WAN port.
 - [Received \(Packets\)](#) - Traffic in packets received from the WAN port.
 - [Sent \(Bytes\)](#) - Traffic in bytes sent out from the WAN port.
 - [Sent \(Packets\)](#) - Traffic in packets sent out from the WAN port.
- [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. 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 [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](#).

2. Select [Press the button of the new device in two minutes](#) and click [Connect](#).

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](#).

2. Select [Enter the new device's PIN](#), enter your client device's current PIN in the [PIN](#) field and click [Connect](#).

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.

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

5.3. Working Mode

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

Note: When [Control the system mode by software](#) is checked, the operation mode switch on the router will be disabled. If you want to enable it, please log into the web management page and go to [Working Mode](#) to uncheck [Control the system mode by software](#).

5.4. Network

5.4.1. 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 LAN 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 configuration interface. At the top, there is a green header with the text 'WAN'. Below this, the 'WAN Connection Type' is set to 'Dynamic IP' in a dropdown menu, with a 'Detect' button to its right. The IP configuration section includes:

- IP Address: 192.168.1.104
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- Buttons: 'Renew' and 'Release'

 The 'MTU Size (in bytes)' is set to '1500' with a note: '(The default is 1500, do not change unless necessary.)'. Below this, there is a checkbox for 'Use These DNS Servers'. Underneath, the 'Primary DNS' is '192.168.1.1' and the 'Secondary DNS' is '0.0.0.0' (Optional). The 'Host Name' field contains 'TL-ER6120'. At the bottom, there is a checkbox for 'Get IP with Unicast DHCP (It is usually not required.)' and a 'Save' button.

- [MTU Size](#) - 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.
- [Use These DNS Servers](#) - If your ISP provides you one or two DNS addresses, select [Use These DNS Servers](#) and enter the primary and secondary addresses. Otherwise, the DNS servers will be assigned dynamically from your ISP.
- [Host Name](#) - This option specifies the name of the router.
- [Get IP with Unicast DHCP](#) - 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.)

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 configuration interface with the following fields and values:

- WAN Connection Type:** Static IP (selected), Detect button
- IP Address:** 0.0.0.0
- Subnet Mask:** 0.0.0.0
- Default Gateway:** 0.0.0.0
- MTU Size (in bytes):** 1500 (The default is 1500, do not change unless necessary.)
- Primary DNS:** 0.0.0.0
- Secondary DNS:** 0.0.0.0 (Optional)
- Save** 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.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - 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.
- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

PPPoE/Russia PPPoE

If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE**.

The screenshot shows the WAN configuration interface with the following fields and values:

- WAN Connection Type:** PPPoE/Russia PPPoE (selected), Detect button
- PPPoE Connection:**
 - User Name:** username
 - Password:** *****
 - Confirm Password:** *****
- Secondary Connection:** Disabled Dynamic IP Static IP (For Dual Access/Russia PPPoE)
- Wan Connection Mode:**
 - Connect on Demand
 - Max Idle Time: 15 minutes (0 means remain active at all times.)
 - Connect Automatically
 - Time-based Connecting
 - Period of Time: from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
 - Connect Manually
 - Max Idle Time: 15 minutes (0 means remain active at all times.)
- Connect** **Disconnect** **Disconnected!**
- Save** **Advanced** buttons

- **User Name/Password** - Enter the username 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.
- **WAN Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **Time-based Connecting** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).
 - **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:

1. Only when you have configured the system time on the **System Tools > Time Settings** page, will the Time-based Connecting function take effect.
2. 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.

If you want to do some advanced configurations, please click **Advanced**.

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

Use IP Address Specified by ISP

ISP Specified IP Address:

Detect Online Interval: Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)

Use The Following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

- **MTU Size** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.

- **Service Name/AC Name** - The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the router, please select **Use IP address specified by ISP** and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online 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.
- **Primary DNS/Secondary DNS** - If your ISP does not automatically assign DNS addresses to the router, please select **Use the following DNS servers** 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.

BigPond Cable

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

The screenshot shows the WAN configuration interface for a BigPond Cable connection. The page has a green header with the text 'WAN'. Below the header, the 'WAN Connection Type' is set to 'BigPond Cable' in a dropdown menu. There are input fields for 'User Name', 'Password', 'Auth Server' (containing 'sm-server'), and 'Auth Domain'. The 'MTU Size (in bytes)' is set to '1500' with a note: '(The default is 1500, do not change unless necessary.)'. Under 'Connection Mode', there are three radio buttons: 'Connect on Demand' (unselected), 'Connect Automatically' (selected), and 'Connect Manually' (unselected). Each mode has a 'Max Idle Time' field set to '15' minutes. At the bottom, there are 'Connect', 'Disconnect', and 'Disconnected!' buttons, and a 'Save' button at the very bottom.

- **User Name/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 Size** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Connection Mode**
 - **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 Automatically](#) - The connection can be re-established automatically when it is down.
- [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.

L2TP/Russia L2TP

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

The screenshot shows the WAN configuration interface for L2TP/Russia L2TP. The 'WAN Connection Type' is set to 'L2TP/Russia L2TP'. The 'User Name' field contains 'username', and the 'Password' and 'Confirm Password' fields are masked with asterisks. There are 'Connect', 'Disconnect', and 'Disconnected!' buttons. The 'Dynamic IP' radio button is selected. The 'Server IP Address/Name' field is empty. The 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS' fields are all set to '0.0.0.0'. The 'Internet IP Address' is '0.0.0.0' and 'Internet DNS' is '0.0.0.0, 0.0.0.0'. The 'MTU Size (in bytes)' is '1460' and 'Max Idle Time' is '15' minutes. The 'Connection Mode' has three options: 'Connect on Demand', 'Connect Automatically' (selected), and 'Connect Manually'. A 'Save' button is at the bottom.

- [User Name/Password](#) - Enter the username 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.
- [Connect/Disconnect](#) - Click this button to connect or disconnect immediately.
- [Dynamic IP/ Static IP](#) - Select either as required by your ISP. If [Static IP](#) is selected, please enter the IP address, subnet mask, gateway and DNS also provided by your ISP.

- **Internet IP Address/ Internet DNS** - The Internet IP address and DNS server address assigned by L2TP server.
- **Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **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/Russia PPTP

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

WAN

WAN Connection Type: PPTP/Russia PPTP

User Name:

Password:

Confirm Password:

Disconnected!

Dynamic IP
 Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 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 Size (in bytes): (The default is 1420, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Connection Mode:

 Connect on Demand

 Connect Automatically

 Connect Manually

- **User Name/Password** - Enter the username 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.
- **Connect/Disconnect** - Click this button to connect or disconnect immediately.
- **Dynamic IP/ Static IP** - Select either as required by your ISP. If **Static IP** is selected, please enter the IP address, subnet mask, gateway and DNS also provided by your ISP.
- **Internet IP Address/ Internet DNS** - The Internet IP address and DNS server address assigned by L2TP server.
- **Connection Mode**
 - **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 Automatically** - The connection can be re-established automatically when it is down.
 - **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.

5.4.2. 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**.

MAC Clone	
WAN MAC Address:	<input type="text" value="00-0A-EB-13-09-1A"/> <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="50-E5-49-1E-06-80"/> <input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>	

- **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:

1. You can only use the MAC Address Clone function for PCs on the LAN.
2. 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.

5.4.3. 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

MAC Address: 00-0A-EB-13-09-19

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

IGMP Proxy: Enable

Note:IGMP(Internet Group Management Protocol) works for IPTV multicast stream.The device supports both IGMP proxy with enabled/disabled option and IGMP snooping.

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 (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.
- **IGMP Proxy** - The Internet Group Management Protocol (IGMP) feature allow you to watch TV on IPTV-supported devices in the LAN .

Note:

1. If you have changed the IP address, you must use the new IP address to login.
2. 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.

5.5. Wireless

5.5.1. Wireless Settings

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

The screenshot shows the 'Wireless Settings' configuration page. The 'Wireless Network Name' field is set to 'TP-LINK_32EB'. The 'Mode' is set to '11bgn mixed', 'Channel Width' is 'Auto', and 'Channel' is 'Auto'. The 'Enable Wireless Router Radio', 'Enable SSID Broadcast', and 'Enable WDS Bridging' checkboxes are present, with the first two checked.

- **Wireless Network Name** - Enter a string of up to 32 characters. The default SSID is TP-LINK_XXXX (XXXX indicates the last unique four numbers of each Router's MAC address). It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
- **Mode** - Select the desired mode. It is strongly recommended that you keep the default setting **11bgn mixed**, so that all of 802.11b/g/n wireless stations can connect to the router.

Note:

If 11bg mixed mode is selected, the **Channel Width** field will turn gray and the value will become 20M, and cannot be changed.

- **Channel Width** - Select any channel width from the drop-down list. The default setting is **Auto**, which can automatically adjust the channel width for your clients.
- **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.
- **Enable Wireless Router Radio** - The wireless radio of the router can be enabled or disabled to allow or deny wireless access. If enabled, the wireless clients will be able to access the router.

- **Enable SSID Broadcast** - If enabled, the router will broadcast the wireless network name (SSID).
- **Enable WDS Bridging** - If enabled, the router can bridge two or more WLANs. Please fill in the parameters below.

SSID (to be bridged):	<input type="text"/>
BSSID (to be bridged):	<input type="text"/> Example:00-1D-0F-11-22-33
	<input type="button" value="Survey"/>
WDS Mode:	Auto ▼
Key type:	None ▼
WEP Index:	1 ▼
Auth type:	open ▼
Password:	<input type="password"/>
<input type="button" value="Save"/>	

- **SSID (to be bridged)** - The SSID of the AP the router is going to connect to. Click [Survey](#) and the [AP List](#) page will appear. Find the SSID of the AP you want to connect to, and click [Connect](#) in the corresponding row. The target network's SSID and BSSID (MAC address) will be automatically filled into the corresponding box.
- **BSSID (to be bridged)** - The BSSID (MAC address) of the AP the router is going to connect to.
- **WDS Mode** - Select [Auto](#), [WDS1](#) or [WDS2](#). It is recommended to leave it to Auto.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended to select the same type as that of the AP.
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization of the AP.
- **Password** - Enter the network password of the AP your router is connected to.

5.5.2. 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 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 **Automatic**, **WPA-PSK** or **WPA2-PSK**.
 - **Encryption** - Select **Automatic**, **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 **Automatic**, **WPA** or **WPA2**.
 - **Encryption** - Select **Automatic**, **TKIP** or **AES**.
 - **Radius Server IP** - Enter the IP address of the Radius server.
 - **Radius Port** - Enter the port that Radius server used.
 - **Radius 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.

- **Type** - The default setting is **Automatic**, 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, 128-bit or 152-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.
- **152-bit** - Enter 32 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 16 ASCII characters.

5.5.3. 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.

- 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) Leave the status as **Enabled**.
 - 4) Click **Save** and click **Back**.
7. The configured filtering rules should be listed as the picture shows below.

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete

Done!

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

5.5.4. 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.

- **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 WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

5.5.5. 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 Statistics						
Current Connected Wireless Stations numbers:					1	<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure	
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	<input type="button" value="Allow"/>	

- [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.
- [Configure](#) - The button is used for loading the item to the Wireless MAC Filtering list.
 - [Allow](#) - If the Wireless MAC Filtering function is enabled, click this button to allow the client to access your network.
 - [Deny](#) - If the Wireless MAC Filtering function is enabled, click this button to deny the client to access your network.

5.6. Guest Network

This function 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 > Wireless Settings](#).
3. Enable the [Guest Network](#) function.
4. Create a network name for your guest network.
5. Select the [Wireless 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](#).

- **Allow Guest To Access My Local Network** - If enabled, clients on the guest network can also access the local network.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.
- **Egress Bandwidth For Guest Network** - The upload speed through the INTERNET port for the guest network.
- **Ingress Bandwidth For Guest Network** - The download speed through the INTERNET port for the guest network.
- **Guest Network** - Check to enable **Guest Network**.
- **Network Name** - Enter a string of up to 32 characters. It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
- **Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router's guest network without a password. It's strongly recommended to choose **WPA/WPA2 - Personal** as the security type.

If WPA/WPA2 - Personal is selected:

- **Version** - Select **Automatic**, **WPA-PSK** or **WPA2-PSK**.
- **Encryption** - Select **Automatic**, **TKIP** or **AES**.
- **PSK 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.
- **Access Time** - During this period, devices on the guest network can access the router.

5.7. 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.

5.7.1. 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 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.
- **Primary DNS (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS (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](#).

5.7.2. DHCP Client List

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

DHCP Client List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router 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](#).

5.7.3. 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 blank.

Add or Modify an Address Reservation Entry	
MAC Address:	<input type="text"/>
Reserved IP Address:	<input type="text"/>
Status:	<input type="text" value="Enabled"/>
<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**.

5.8. Forwarding

Router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the Internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external 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 in the LAN and realize some specific functions.

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

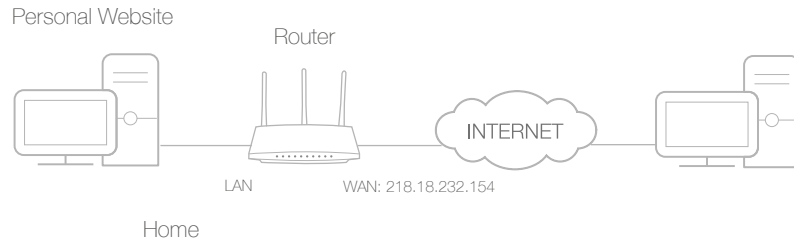
5.8.1. Virtual Servers

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 in 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 Servers](#).
4. Click [Add New](#). Select [HTTP](#) from the [Common Service Port](#) list. The service port, internal port and protocol will be automatically filled with contents. Enter the PC's IP address 192.168.0.100 in the [IP Address](#) field.

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text" value="80"/> (XX-XX or XX)
Internal Port:	<input type="text" value="80"/> (XX, Enter a specific port number or leave it blank)
IP Address:	<input type="text" value="192.168.0.100"/>
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 in 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.

5.8.2. 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 and video players. Common applications include MSN Gaming Zone, Dialpad and QuickTime 4 players, etc.

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 with contents. The following picture takes application [MSN Gaming Zone](#) as an example.

The screenshot shows a web form titled "Add or Modify a Port Triggering Entry". The form contains the following fields and values:

- Trigger Port: 47624
- Trigger Protocol: All
- Incoming Ports: 2300-2400,28800-29000
- Incoming Protocol: All
- Status: Enabled
- Common Applications: MSN Gaming Zone

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

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

Note:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the [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.

5.8.3. 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 hazard. If DMZ is not in use, please disable it in time.

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

For example, due to some port restriction, when playing the online games, you can login normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ 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](#) field.

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.

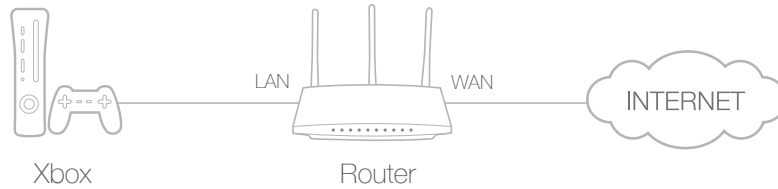
5.8.4. UPnP

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

Tips:

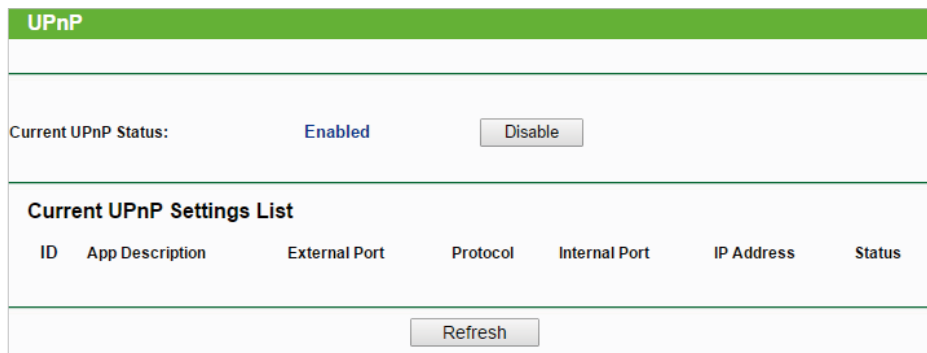
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.



5.9. Security

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

5.9.1. 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	
SPI Firewall:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN	
PPTP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec Passthrough:	<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
RTSP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SIP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="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**.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.
- **SIP ALG** - To allow some multimedia clients to communicate across NAT, click **Enable**.

3. Click **Save**.

5.9.2. 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

Packets Statistics Interval (5 ~ 60): Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering
ICMP-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Enable UDP-FLOOD Filtering
UDP-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Enable TCP-SYN-FLOOD Attack Filtering
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): Packets/Secs

Ignore Ping Packet from WAN Port to Router

Forbid Ping Packet from LAN Port to Router

- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The **Packets Statistics Interval** value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **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.

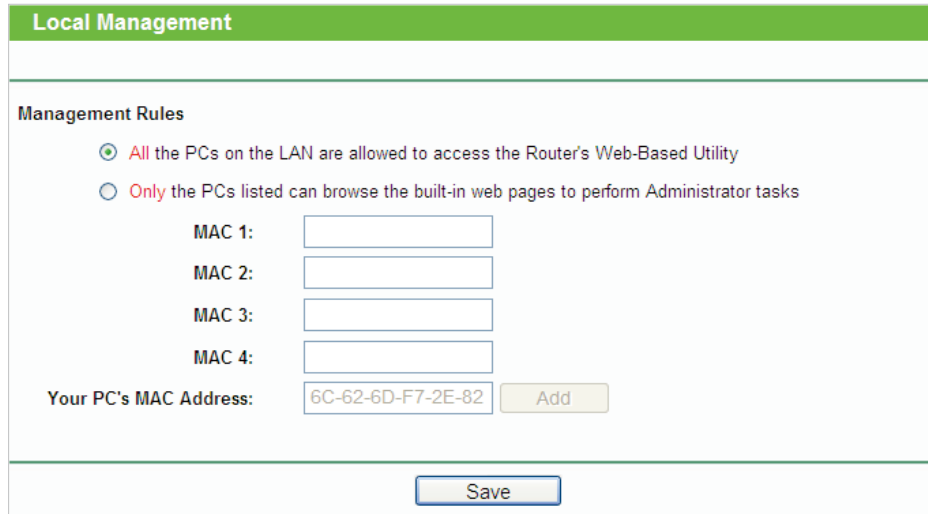
■ **Note:**

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

- **Enable ICMP-FLOOD Attack Filtering** - Check the box 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 Filtering** - Check the box to enable or disable 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** - Check the box 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.
 - **Ignore 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.

5.9.3. 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. At the top, there is a green header with the text 'Local Management'. Below this, the 'Management Rules' section is visible. It contains two radio button options: the first is selected and reads 'All the PCs on the LAN are allowed to access the Router's Web-Based Utility', and the second is unselected and reads 'Only the PCs listed can browse the built-in web pages to perform Administrator tasks'. Below these options are four input fields labeled 'MAC 1:', 'MAC 2:', 'MAC 3:', and 'MAC 4:'. At the bottom of this section, there is a label 'Your PC's MAC Address:' followed by an input field containing the text '6C-62-6D-F7-2E-82' and an 'Add' button. At the very bottom of the page, there is a 'Save' button.

For example, if you want to allow PCs with specific MAC addresses to access the router's web management page 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 built-in web pages to perform administrator tasks.
- 3) Click [Add](#), 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, press and hold the [Reset](#) button to reset the router to the factory defaults.

5.9.4. 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:	<input type="text" value="80"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all)
<input type="button" value="Save"/>	

- **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:

1. 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 management page.
2. Be sure to change the router's default password for security purposes.

5. 10. 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 [Access Control](#) > [Schedule](#).
3. Click [Add New](#) to create a new schedule entry with [Schedule Description](#) as Schedule_1, [Day](#) as Sat and [Time](#) as all day-24 hours. And click [Save](#).

4. Go to [Parental Control](#).
5. Select [Enable](#) and enter the MAC address 00-11-22-33-44-BB in the [MAC Address of Parental PC](#) field.
6. Click [Add New](#).
7. Enter appropriate parameters in corresponding fields.

- Enter 00-11-22-33-44-AA in the [MAC Address of Children's PC](#) field.
 - Enter Allow TP-LINK in the [Website Description](#) field.
 - Enter www.tp-link.com in the [Allowed Website Name](#) field.
 - Select Schedule_1 you created just now from the [Effective Time](#) drop-down list.
 - In the [Status](#) field, select [Enable](#).
8. Click [Save](#).

Then you can go back to the Parental Control Settings page to check the following list.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow TP-LINK	Schedule_1	<input checked="" type="checkbox"/>	Edit Delete

5.11. 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 in 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 [Host Description](#) field and enter 00-11-22-33-44-AA in the [MAC Address](#) field.

Add or Modify a Host Entry

Mode:

Host Description:

MAC Address:

- 3) Click [Save](#).
3. Go to [Access Control](#) > [Target](#) and configure the target settings:
 - 1) Click [Add New](#).
 - 2) Select [Domain Name](#) 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 [Domain Name](#) field.

Note:

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

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.

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 [Rule Name](#) field. Select [host_1](#) from the host drop-down list; select [target_1](#) from the target drop-down list; select [schedule_1](#) from the schedule drop-down list.

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**.

Done!

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

5. 12. 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. 12. 1. Static Routing 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 Routing**.
- **To add static routing entries:**
1. Click **Add New**.
 2. Enter the following information.

Add or Modify a Static Route Entry

Destination Network:
Subnet Mask:
Default Gateway:
Status: Enabled

- **Destination Network** - 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.
 - **Default Gateway** - This is the IP Address of the default gateway device that allows the contact between the router and the network or host.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
 4. Click **Save**.

You can also do the following operations to modify the current settings.

- Click **Delete** to delete the entry.
- Click **Enable All** to enable all the entries.
- Click **Disable All** to disable all the entries.
- Click **Delete All** to delete all the entries.
- Click **Previous** to view the information on the previous screen and **Next** to view the information on the next screen.

5.12.2. 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

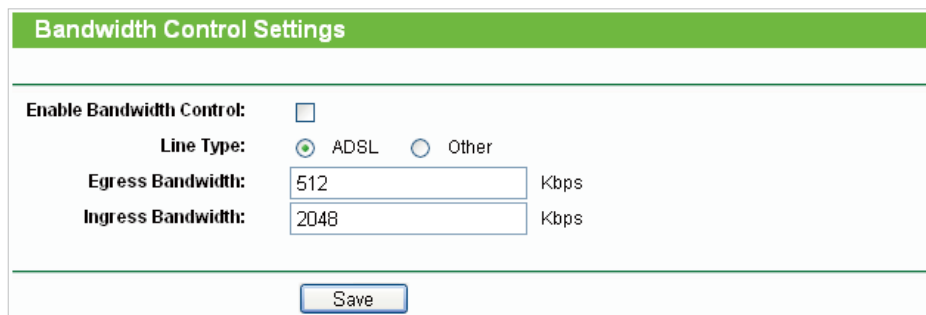
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	0.0.0.0	0.0.0.0	192.168.1.1	WAN

- **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 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.

5.13. Bandwidth Control

5.13.1. Control Settings

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



Bandwidth Control Settings	
Enable Bandwidth Control:	<input type="checkbox"/>
Line Type:	<input checked="" type="radio"/> ADSL <input type="radio"/> Other
Egress Bandwidth:	<input type="text" value="512"/> Kbps
Ingress Bandwidth:	<input type="text" value="2048"/> Kbps
<input type="button" value="Save"/>	

The values you configure for the Egress Bandwidth and Ingress Bandwidth should be less than 100,000Kbps. For optimal control of the bandwidth, please select the right Line Type and consult your ISP for the total egress and ingress bandwidth.

- **Enable Bandwidth Control** - Check this box so that the Bandwidth Control settings can take effect.
- **Line Type** - Select the right type for you network connection. If you are not sure, please consult your ISP.
- **Egress Bandwidth** - The upload speed through the INTERNET port.
- **Ingress Bandwidth** - The download speed through the INTERNET port.

5.13.2. Rules List

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

- Go to [Bandwidth Control](#) > [Rules List](#), and you can view and configure the Bandwidth Control rules.

Bandwidth Control Rule List							
ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							
Add New...		Delete All					
Previous		Next		Current No. 1	Page		

- Description** - This is the information about the rules such as address range.
- Egress Bandwidth** - This field displays the max and min upload bandwidth through the WAN port. The default is 0.
- Ingress Bandwidth** - This field displays the max and min download bandwidth through the WAN port. The default is 0.
- Enable** - This field displays the status of the rule.
- Modify** - Click [Modify/Delete](#) to edit/delete the rule.

➤ **To add a Bandwidth control rule:**

- Click [Add New](#).
- Enter the information like the figure shown below.

Bandwidth Control Rule Settings			
Enable:	<input checked="" type="checkbox"/>		
IP Range:	<input type="text" value="192.168.0.2"/>	-	<input type="text" value="192.168.0.23"/>
Port Range:	<input type="text" value="21"/>	-	<input type="text"/>
Protocol:	TCP ▾		
	Min Bandwidth(Kbps)		Max Bandwidth(Kbps)
Egress Bandwidth:	<input type="text" value="0"/>		<input type="text" value="1000"/>
Ingress Bandwidth:	<input type="text" value="0"/>		<input type="text" value="4000"/>
Save		Back	

- Click [Save](#).

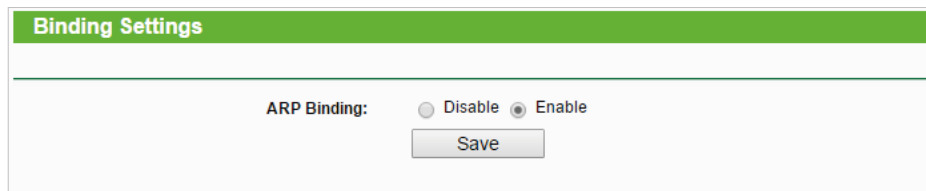
5. 14. IP&MAC Binding

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.

5.14.1. 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.



Binding Settings

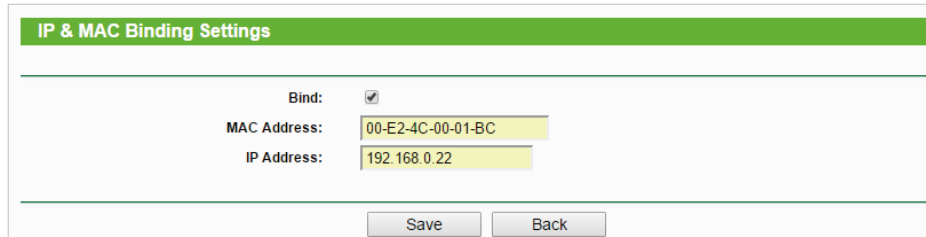
ARP Binding: Disable Enable

Save

4. Click [Save](#).

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

1. Click [Add New](#).
2. Select the [Bind](#) checkbox.



IP & MAC Binding Settings

Bind:

MAC Address: 00-E2-4C-00-01-BC

IP Address: 192.168.0.22

Save Back

3. Enter the MAC address and IP address.
4. Click [Save](#).

➤ **To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click [Modify](#) or [Delete](#) in the Modify column.

➤ **To find an existing entry:**

1. Click [Find](#).
2. Enter the MAC address or IP address in the corresponding field.
3. Click [Find](#) on this page as shown below.

Find IP & MAC Binding Entry

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind Link
2	00-14-5E-91-19-E3	192.168.1.56	<input checked="" type="checkbox"/> To page

5.14.2. ARP List

To manage a device, you can observe the device in 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

ID	MAC Address	IP Address	Status	Configure
1	40-61-86-FC-74-93	192.168.0.100	Unbound	Load Delete

- **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 **Bind All** to bind all the current items.
- Click **Load All** to load all items to the IP & MAC Binding list.
- Click **Refresh** 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.

5.15. 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.no-ip.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](#).

Comexe DDNS

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

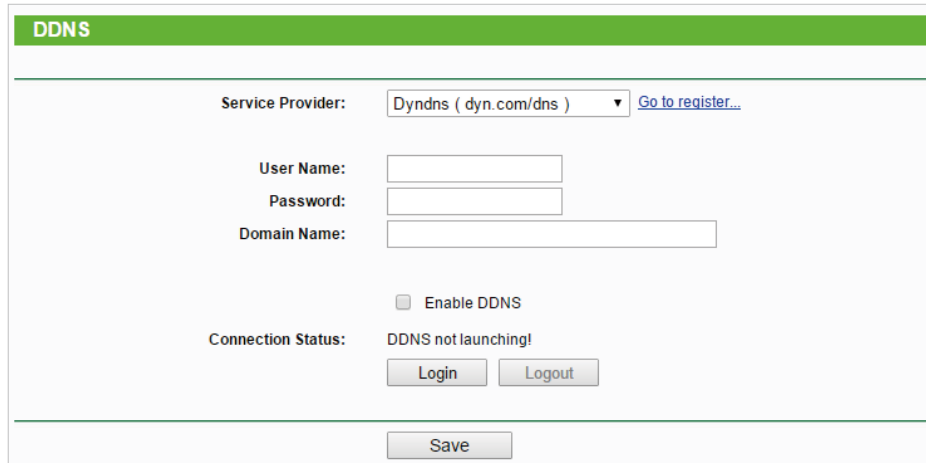
The screenshot shows the DDNS configuration interface. At the top, there is a green bar with the text "DDNS". Below this, the "Service Provider" is set to "Comexe (www.comexe.cn)" with a "Go to register..." link. There are five "Domain Name:" labels, each followed by an empty text input field. Below these are "User Name:" and "Password:" labels, each followed by an empty text input field. A checkbox labeled "Enable DDNS" is present and unchecked. The "Connection Status:" is "DDNS not launching!". There are "Login" and "Logout" buttons. At the bottom, there is a "Save" button.

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) received from your dynamic DNS service provider.
 2. Enter the [User Name](#) 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.

Dyndns DDNS

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



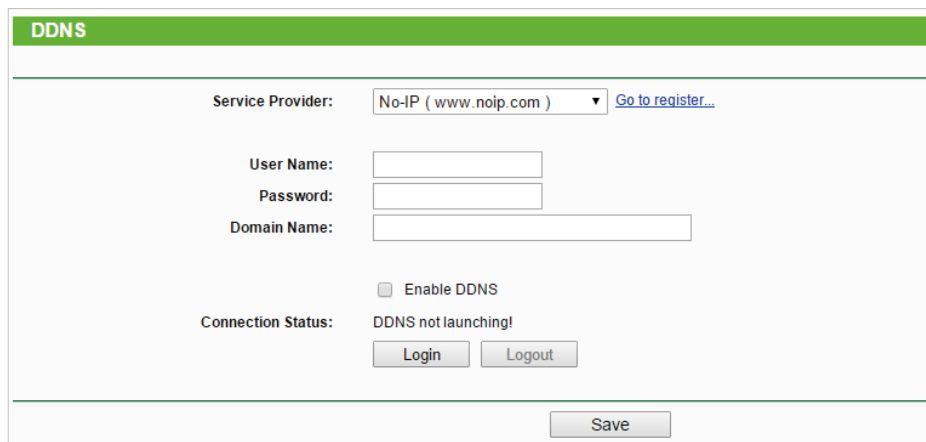
The screenshot shows the DDNS configuration interface. At the top, there is a green header with the text "DDNS". Below the header, the "Service Provider" is set to "DynDNS (dyn.com/dns)" with a dropdown arrow and a link "Go to register...". There are three input fields: "User Name:", "Password:", and "Domain Name:". Below these fields is a checkbox labeled "Enable DDNS" which is currently unchecked. The "Connection Status" is displayed as "DDNS not launching!". At the bottom of the form, there are two buttons: "Login" and "Logout". A "Save" button is located at the very bottom of the page.

To set up for DDNS, follow these instructions:

1. Enter the [User Name](#) for your DDNS account.
 2. Enter the [Password](#) for your DDNS account.
 3. Enter the [Domain Name](#) you received from dynamic DNS service provider here.
 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 configuration interface for No-IP. At the top, there is a green header with the text "DDNS". Below the header, the "Service Provider" is set to "No-IP (www.noip.com)" with a dropdown arrow and a link "Go to register...". There are three input fields: "User Name:", "Password:", and "Domain Name:". Below these fields is a checkbox labeled "Enable DDNS" which is currently unchecked. The "Connection Status" is displayed as "DDNS not launching!". At the bottom of the form, there are two buttons: "Login" and "Logout". A "Save" button is located at the very bottom of the page.

To set up for DDNS, follow these instructions:

1. Enter the [User Name](#) for your DDNS account.
2. Enter the [Password](#) for your DDNS account.
3. Enter the [Domain Name](#) you received from dynamic DNS service provider.

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.

5.16. IPv6 Support

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).

5.16.1. IPv6 Status

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

IPv6 Status	
WAN	
Connection Type:	PPPoE V6
IPv6 Address:	3ffe::dfb6:1910:ed55:1769/64
IPv6 Default Gateway:	fe80::b01c:b0bb:9b31:c661
Primary IPv6 DNS:	2000::ff
Secondary IPv6 DNS:	2000::fe
LAN	
IPv6 Address Assign Type:	Route Advertisement
IPv6 Address:	::
Link-local Address:	fe80::12f1:a2ff:fe7c:d39b/64

- **WAN** - This section shows the current IPv6 information of the router's WAN port, including [Connection Type](#), [IPv6 Address](#) information, [IPv6 Default Gateway](#), [Primary IPv6 DNS](#) and [Secondary IPv6 DNS](#).
- **LAN** - This section shows the current IPv6 information of the router's LAN port, including [IPv6 Address Assign Type](#), [IPv6 Address](#) and [Link-local Address](#).

5.16.2. IPv6 Setup

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [IPv6 Support](#) > [IPv6 Setup](#).

3. Select the **WAN Connection Type** according to your ISP network topology:
 - **SLAAC** - Connections which use RADVD IPv6 address assignment.
 - **DHCPv6** - 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.

SLAAC

The screenshot shows the 'WAN Setup' configuration page. The 'Enable IPv6' checkbox is checked. The 'WAN Connection Type' is set to 'SLAAC'. The 'IPv6 Address', 'IPv6 Address Prefix', and 'Default Gateway' fields are empty. Below these fields are 'Connect' and 'Disconnect' buttons, and a 'Disconnected!' status indicator. At the bottom, there are two radio button options for DNS: 'Get IPv6 DNS Server Automatically' (selected) and 'Use the following IPv6 DNS Servers'.

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Default Gateway** - Displays the default gateway in colon-hexadecimal notation provided by your ISP.
- **Connect** - Click **Connect** to connect to the IPv6 server of your ISP.
- **Disconnect** - Click **Disconnect** to disconnect from the IPv6 server of your ISP.
- **Get IPv6 DNS Server Automatically** - If your ISP does not give you any DNS IPv6 address, keep the default selection **Get IPv6 DNS Server Automatically**, and the DNS servers will be assigned from ISP dynamically.
 - **Primary IPv6 DNS** - Displays the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
 - **Secondary IPv6 DNS** - Displays another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Use the following IPv6 DNS Servers** - If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** in the corresponding fields.

Note:

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

DHCPv6

WAN Setup

Enable IPv6:

WAN Connection Type:

IPv6 Address:

Default Gateway:

Disconnected!

Get IPv6 DNS Server Automatically

Primary IPv6 DNS:

Secondary IPv6 DNS:

Use the following IPv6 DNS Servers

- [IPv6 Address](#) - The IPv6 address assigned by your ISP dynamically.
- [Default Gateway](#) - Displays the default gateway in colon-hexadecimal notation provided by your ISP.
- [Renew](#) - Click [Renew](#) to renew the IPv6 parameters from your ISP.
- [Release](#) - Click [Release](#) to release the IPv6 parameters from your ISP.
- [Get IPv6 DNS Server Automatically](#) - If your ISP does not give you any DNS IPv6 address, keep the default selection [Get IPv6 DNS Server Automatically](#), and the DNS servers will be assigned from ISP dynamically.
 - [Primary IPv6 DNS](#) - Displays the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
 - [Secondary IPv6 DNS](#) - Displays another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- [Use the following IPv6 DNS Servers](#) - If your ISP gives you one or two DNS IPv6 addresses, select [Use the following IPv6 DNS Servers](#) and enter the [Primary IPv6 DNS](#) and [Secondary IPv6 DNS](#) in the corresponding fields.

Note:

If you get "Address not found error" when you access a web site, 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 'WAN Setup' configuration page. At the top, there is a green header with the text 'WAN Setup'. Below this, the configuration options are as follows:

- Enable IPv6:** A checkbox that is checked.
- WAN Connection Type:** A dropdown menu set to 'Static IPv6'.
- IPv6 Address:** An empty text input field.
- Default Gateway:** An empty text input field with '(Optional)' to its right.
- MTU Size (in bytes):** A text input field containing '1500' with the text '(The default is 1500, do not change unless necessary.)' to its right.
- Primary DNS:** A text input field containing '2001:4860:4860::8888'.
- Secondary DNS:** A text input field containing '2001:4860:4860::8844' with '(Optional)' to its right.

- **IPv6 Address** - Enter the IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Default Gateway** - Enter the default gateway in colon-hexadecimal notation provided by your ISP.
- **MTU Size (in 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.
- **Primary DNS** - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Secondary DNS** - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

PPPoEv6

- **PPPoE Session** - The PPP session type for IPv6 connection. There are two types:
 - **Share with PPPoEv4** - The PPPoEv6 and PPPoEv4 use the same PPP session.
 - **Create a new Session** - The PPPoEv6 and PPPoEv4 use different PPP sessions. It is default to select this option.
- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Default Gateway** - Displays the default gateway in colon-hexadecimal notation provided by your ISP.
- **MTU (in bytes)** - The normal MTU (Maximum Transmission Unit) value is 1492 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.
- **Get IPv6 DNS Server Automatically** - If your ISP does not give you any DNS IPv6 address, keep the default selection **Get IPv6 DNS Server Automatically**, and the DNS servers will be assigned from ISP dynamically.
 - **Primary IPv6 DNS** - Displays the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
 - **Secondary IPv6 DNS** - Displays another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

- [Use the following IPv6 DNS Servers](#) - If your ISP gives you one or two DNS IPv6 addresses, select [Use the following IPv6 DNS Servers](#) and enter the [Primary IPv6 DNS](#) and [Secondary IPv6 DNS](#) in the corresponding fields.
- [Connection Mode](#) - The way to connect the ISP.
 - [Always On](#) - Connect automatically.
 - [Connect Manual](#) - Connect by the user manually.
- [Connect](#) - Click [Connect](#) to connect immediately.
- [Disconnect](#) - Click [Disconnect](#) to disconnect immediately.

Tunnel 6to4

The screenshot shows the WAN Setup configuration page. The 'WAN Connection Type' is set to 'Tunnel 6to4'. The 'Address', 'Subnet Mask', and 'Default Gateway' are all set to '0.0.0.0'. The 'Tunnel Address' field is empty. The 'MTU Size (in bytes)' is set to '1480'. The 'Use the following IPv6 DNS Servers' checkbox is checked. The 'Primary IPv6 DNS' is set to '2001:4860:4860::8888' and the 'Secondary IPv6 DNS' is set to '2001:4860:4860::8844'.

- [Address/Subnet Mask/Default Gateway](#) - The IPv4 address/ subnet mask/ default gateway assigned, in dotted-decimal notation.
 - [Tunnel Address](#) - The 6to4 tunnel address created by the device to access the IPv6 network.
 - [MTU Size](#) - 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 the following IPv6 DNS Servers](#) - If your ISP gives you one or two DNS IPv6 addresses, select [Use the following IPv6 DNS Servers](#) and enter the [Primary IPv6 DNS](#) and [Secondary IPv6 DNS](#) into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.
 - [Primary IPv6 DNS](#) - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
 - [Secondary IPv6 DNS](#) - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
4. Select the [Address Autoconfiguration Type](#) which determines the way how the router assigns IPv6 address for PCs in the LAN.

- **Address Autoconfiguration Type** - **RADVD** (Router Advertisement Daemon) and **DHCPv6** (Dynamic Host Configuration Protocol for IPv6) **Server**.
 - **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.
 - **LAN IPv6 Address** - Display the LAN IPv6 address created by the device.
5. Click **Save**.

5.17. System Tools

5.17.1. Time Settings

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** and configure the system time as needed.

➤ **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:**
1. Select your local time zone.
 2. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
 3. Click **Get GMT** to get time from the Internet if you have connected to the Internet.
- **To set Daylight Saving Time:**
1. Select **Enable DaylightSaving**.
 2. Select the start time from the drop-down list in the **Start** field.
 3. Select the end time from the drop-down list in the **End** field.
 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 login to the router successfully; otherwise, time-based functions will not take effect.

5.17.2. 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: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Timeout: (100-2000 Milliseconds)

Traceroute Max TTL: (1-30)

Diagnostic Results

This device is ready.

Start

- **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
-----

```

Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

5.17.3. 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. You can download the latest firmware file from the [Support](#) page of our website www.tp-link.com 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 [Browse](#) to locate the downloaded firmware file, and click [Upgrade](#).

5.17.4. 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 default [Username](#): admin
- The default [Password](#): admin
- The default [IP Address](#): 192.168.0.1
- The default [Subnet Mask](#): 255.255.255.0

5.17.5. 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:**

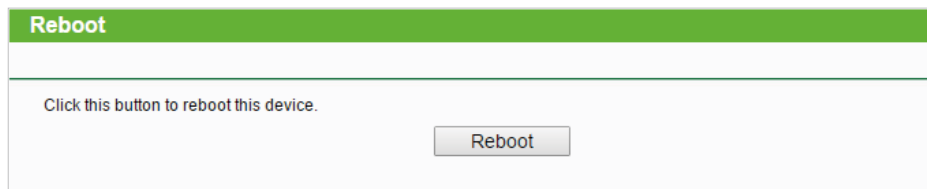
1. Click [Choose File](#) to locate the backup configuration file stored in your computer, and click [Restore](#).
2. Wait a few minutes for the restoring and rebooting.

■ **Note:**

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

5.17.6. Reboot

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.



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).

5.17.7. 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 New Password:

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](#).

5.17.8. 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.

System Log

Auto Mail Feature: **Disabled**

Log Type: Log Level:

Index	Time	Type	Level	Log Content
5	1st day 03:05:45	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
4	1st day 03:05:41	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
3	1st day 03:05:39	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
2	1st day 03:05:37	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
1	1st day 03:04:59	DHCP	INFO	DHCPS:Recv INFORM from C0:4A:00:1A:C3:45

Time = 2016-01-01 3:13:05 11587s
H-Ver = XXXXXXXXXX : S-Ver = XXXXXXXXXX
L = 192.168.0.254 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Current No. Page

- [Auto Mail Feature](#) - Indicates whether the auto mail feature is enabled or not.

- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

- **From** - Your mail box address. The router will connect it to send logs.
- **To** - Recipient's mail address. The destination mailbox which will receive logs.
- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the **From** field. You can log on the relevant website for help if you are not clear with the address.
- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need user name and password to log in.

Note:

Only when you select Authentication, do you have to enter the user name and password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is included.
- **Password** - Your mail account password.
- **Confirm The Password** - Enter the password again to confirm.
- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field.

Click **Save** to apply your settings.

Click **Back** to return to the previous page.

- **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.
- **Save Log** - Click to save all the logs in a txt file.

- [Mail Log](#) - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- [Clear Log](#) - All the logs will be deleted from the router permanently, not just from the page.

Click [Next](#) to go to the next page, or click [Previous](#) to return to the previous page.

5.17.9. Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools](#) > [Statistics](#), and you can view the statistics of the router, including total traffic and the value of the last Packet Statistic Interval in seconds.

- [Current Statistics Status](#) - Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will disabled.
- [Packets Statistics Interval \(5-60\)](#) - The default value is 10. Select a value between 5 and 60 in the drop-down list. The Packets Statistic Interval indicates the time section of the packets statistic.
- [Sorted Rules](#) – Choose how displayed statistics are sorted.
- Select [Auto-refresh](#) to refresh automatically. Click [Refresh](#) to refresh immediately.
- Click [Reset All](#) to reset the values of all the entries to zero.
- Click [Delete All](#) to delete all entries in the table.

Statistics Table

IP/MAC Address	The IP and MAC address are displayed with related statistics.	
Total	Packets	The total number of packets received and transmitted by the router.
	Bytes	The total number of bytes received and transmitted by the router.

Current	Packets	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
Modify	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	Reset	Reset the value of the entry to zero.
	Delete	Delete the existing entry in the table.

5.18. Logout

Click [Logout](#) at the bottom of the main menu, and you will log out of the web page and return to the login window.

Chapter 6

Configure the Router in Repeater Mode

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

This chapter contains the following sections:

- *Status*
- *Working 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 in Repeater Mode.

Status		
Firmware Version:		
Hardware Version:		
Wired		
MAC Address:	30-B5-C4-2F-32-EB	
IP Address:	192.168.0.1	
Subnet Mask:	255.255.255.0	
Wireless		
Working Mode:	Repeater	
Wireless Name of Root AP:		
Channel:	1	
Mode:	11bgn mixed	
Channel Width:	Automatic	
Max Tx Rate:	300Mbps	
MAC Address:	30-B5-C4-2F-32-EB	
Repeater Status:	Init...	
Traffic Statistics		
	Received	Sent
Bytes:	0	0
Packets:	0	0
System Up Time:	0 days 00:01:52	
		<input type="button" value="Refresh"/>

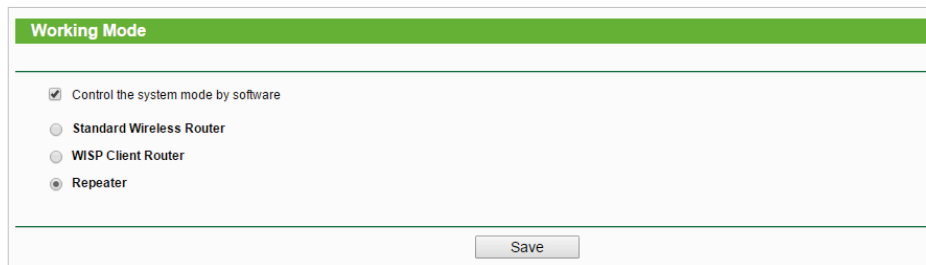
- [Firmware Version](#) - The version information of the router's firmware.
- [Hardware Version](#) - The version information of the router's hardware.
- [Wired](#) - This field displays the current settings of the LAN, and you can configure them on the [Network > LAN](#) page.
 - [MAC address](#) - 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 > Wireless Settings](#) page.
 - [Working Mode](#) - The current operation mode in use.
 - [Wireless Name of Root AP](#) - The SSID of the root router.

- [Channel](#) - The current wireless channel in use.
 - [Mode](#) - The current wireless working mode in use.
 - [Channel Width](#) - The current wireless channel width in use.
 - [MAC Address](#) - The physical address of the router.
 - [Repeater Status](#) - The status of the router working as a repeater.
 - [Traffic Statistics](#) - The router's traffic statistics.
 - [Received \(Bytes\)](#) - Traffic in bytes received from the WAN port.
 - [Received \(Packets\)](#) - Traffic in packets received from the WAN port.
 - [Sent \(Bytes\)](#) - Traffic in bytes sent out from the WAN port.
 - [Sent \(Packets\)](#) - Traffic in packets sent out from the WAN port.
 - [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. Working Mode

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

Note: When [Control the system mode by software](#) is checked, the operation mode switch on the router will be disabled. If you want to enable it, please log into the web management page and go to [Working Mode](#) to uncheck [Control the system mode by software](#).



The screenshot shows a web interface for configuring the router's working mode. The title bar is green and says "Working Mode". Below the title bar, there is a checkbox labeled "Control the system mode by software" which is checked. Underneath this checkbox are three radio button options: "Standard Wireless Router", "WISP Client Router", and "Repeater". The "Repeater" option is selected. At the bottom right of the form, there 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](#).

LAN

MAC Address: 30-B5-C4-2F-32-EB

Type: Smart IP(DHCP) ▼

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0 ▼

Gateway: 0.0.0.0

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).

Save

- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **Type** - Either select **Smart IP(DHCP)** to get IP address from DHCP server, or **Static IP** to configure IP address manually.
- **IP Address** - Enter the IP address in dotted-decimal notation if your 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.
- **Gateway** - The gateway should be in the same subnet as your IP address.

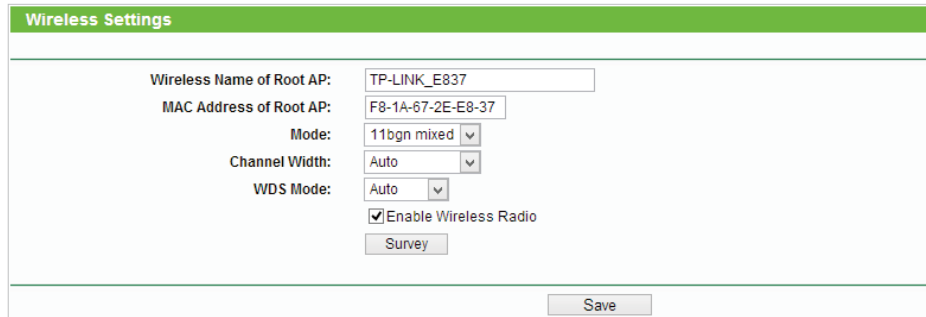
■ **Note:**

1. If you have changed the IP address, you must use the new IP address to login.
2. If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
3. 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.

6.4. Wireless

6.4.1. Wireless Settings

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



The image shows a web interface for configuring wireless settings. The title is "Wireless Settings". The form contains the following fields and options:

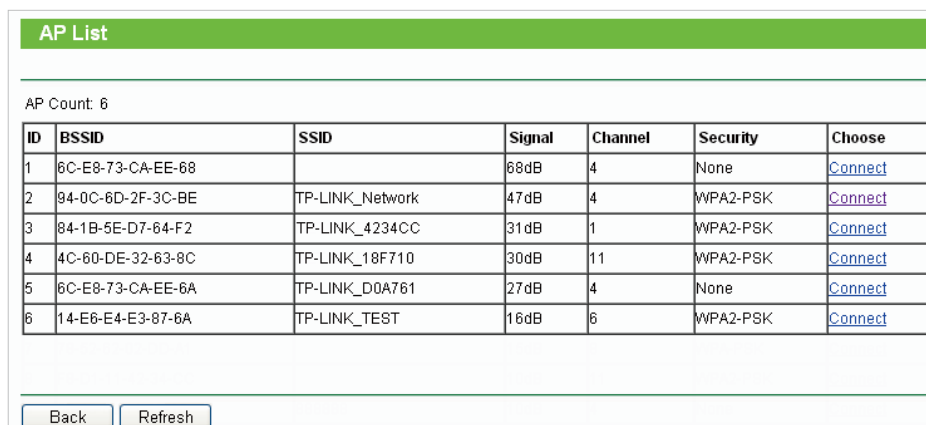
- Wireless Name of Root AP: TP-LINK_E837
- MAC Address of Root AP: F8-1A-67-2E-E8-37
- Mode: 11bgn mixed (dropdown)
- Channel Width: Auto (dropdown)
- WDS Mode: Auto (dropdown)
- Enable Wireless Radio
- Survey button
- Save button

- **Wireless Name of Root AP** - The SSID of AP that you want to connect to.
- **MAC Address of Root AP** - The MAC address of AP that you want to connect to.
- **Mode** - Select the desired mode. It is strongly recommended that you keep the default setting **11bgn mixed**, so that all of 802.11b/g/n wireless stations can connect to the router.

Note:

If 11bg mixed mode is selected, the **Channel Width** field will turn grey and the value will become 20M, and cannot be changed.

- **Channel Width** - Select any channel width from the drop-down list. The default setting is **Auto**, which can automatically adjust the channel width for your clients.
- **WDS Mode** - This field determines which WDS Mode will be used. It is not necessary to change the WDS mode unless you notice network communication problems with root AP. If you select **Auto**, then router will choose the appropriate WDS mode automatically.
- **Enable Wireless Router Radio** - The wireless radio of the router can be enabled or disabled to allow or deny wireless access. If enabled, the wireless clients will be able to access the router.
- **Survey** - Click this button, and the **AP List** page will appear. Find the SSID of the Access Point you want to connect to, and click **Connect** in the corresponding row. The target network's SSID and MAC address will be automatically filled into the corresponding box.



The image shows a table titled "AP List" with 6 columns: ID, BSSID, SSID, Signal, Channel, Security, and Choose. Below the table are "Back" and "Refresh" buttons.

ID	BSSID	SSID	Signal	Channel	Security	Choose
1	6C-E8-73-CA-EE-68		68dB	4	None	Connect
2	94-0C-6D-2F-3C-BE	TP-LINK_Network	47dB	4	WPA2-PSK	Connect
3	84-1B-5E-D7-64-F2	TP-LINK_4234CC	31dB	1	WPA2-PSK	Connect
4	4C-60-DE-32-63-8C	TP-LINK_18F710	30dB	11	WPA2-PSK	Connect
5	6C-E8-73-CA-EE-6A	TP-LINK_D0A761	27dB	4	None	Connect
6	14-E6-E4-E3-87-6A	TP-LINK_TEST	16dB	6	WPA2-PSK	Connect

6.4.2. 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 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 [Automatic](#), [WPA-PSK](#) or [WPA2-PSK](#).
 - **Encryption** - Select [Automatic](#), [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 [Automatic](#), [WPA](#) or [WPA2](#).
 - **Encryption** - Select [Automatic](#), [TKIP](#) or [AES](#).
 - **Radius Server IP** - Enter the IP address of the Radius server.
 - **Radius Port** - Enter the port that Radius server used.

- **Radius 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.
 - **Type** - The default setting is **Automatic**, 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, 128-bit or 152-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.
 - **152-bit** - Enter 32 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 16 ASCII characters.

6.4.3. 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

MAC Address:

Description:

Status:

- 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) Leave the status as [Enabled](#).
 - 4) Click [Save](#) and click [Back](#).
7. The configured filtering rules should be listed as the picture shows below.

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.

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete

Done!

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

6.4.4. 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.

- **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 WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

6.4.5. Wireless Statistics

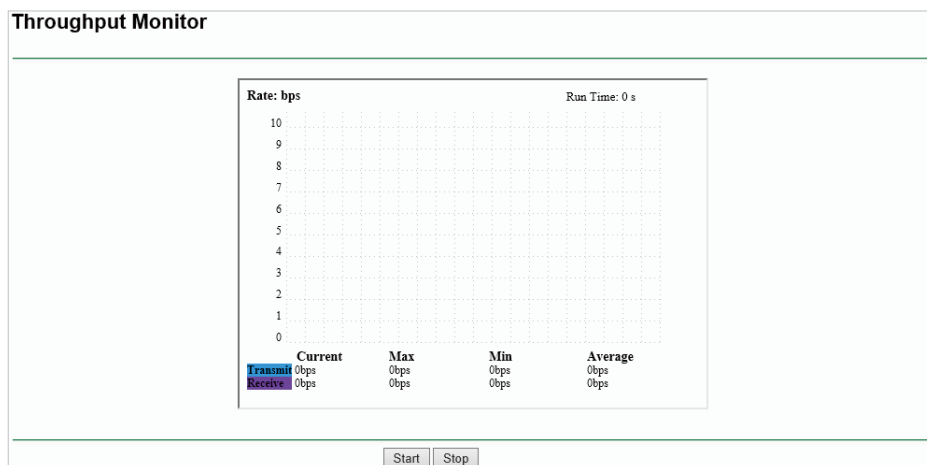
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Wireless > Wireless Statistics](#) to check the data packets sent and received by each client device connected to the router.

Wireless Statistics					
Current Connected Wireless Stations numbers: 1					<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure
1	70-73-CB-1F-C8-C9	STA-ASSOC	46	16	<input type="button" value="Allow"/>

- **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.
- **Configure** - The button is used for loading the item to the Wireless MAC Filtering list.
 - **Allow** - If the Wireless MAC Filtering function is enabled, click this button to allow the client to access your network.
 - **Deny** - If the Wireless MAC Filtering function is enabled, click this button to deny the client to access your network.

6.4.6. 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 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.
- **Primary DNS (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS (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.

6.5.2. DHCP Client List

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

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	tplink14129	6C-62-6D-F7-31-8D	192.168.0.100	01:15:47
2	Unknown	70-73-CB-1F-C8-C9	192.168.0.101	01:56:32

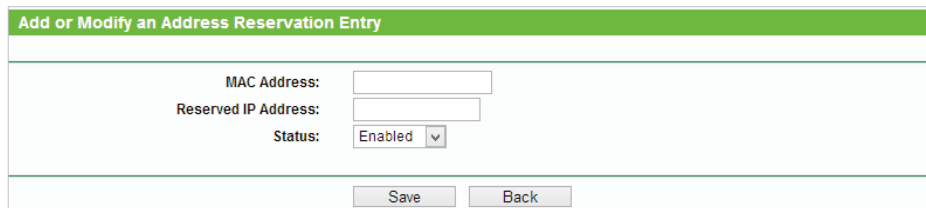
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic 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 blank.



The screenshot shows a web form titled "Add or Modify an Address Reservation Entry". The form contains three input fields: "MAC Address:", "Reserved IP Address:", and "Status:". The "Status" field is a dropdown menu with "Enabled" selected. At the bottom of the form, there are two buttons: "Save" and "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](#).

6.6. System Tools

6.6.1. 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: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Timeout: (100-2000 Milliseconds)

Traceroute Max TTL: (1-30)

Diagnostic Results

This device is ready.

- **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

```

■ **Note:**

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

6.6.2. Ping Watch Dog

The Ping Watch Dog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes the router 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, the router 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 Watch Dog**. Configure the settings and click **Save**.

Ping Watch Dog Utility

Enable:

IP Address:

Interval: (10-300) seconds

Delay: (60-300) seconds

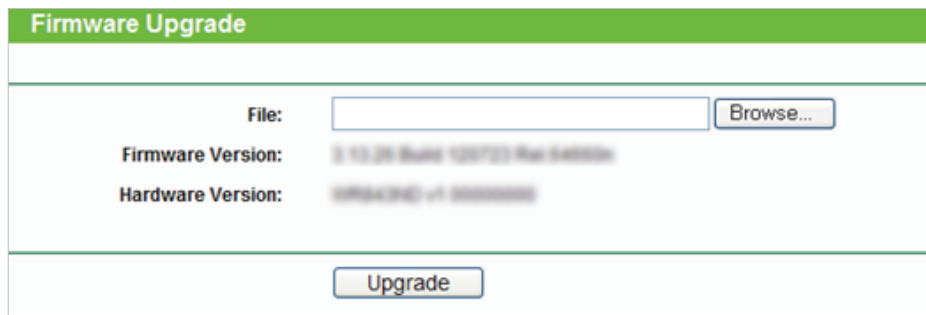
Fail Count: (1-65535)

- **Enable** - Turn on/off 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.
- **Delay** - Time delay before first ping packet is sent out when the router is restarted.
- **Fail Count** - Upper limit of the ping packets the router can drop continuously. If this value is overrun, the router will restart automatically.

6.6.3. 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. You can download the latest firmware file from the [Support](#) page of our website www.tp-link.com and upgrade the firmware to the latest version.

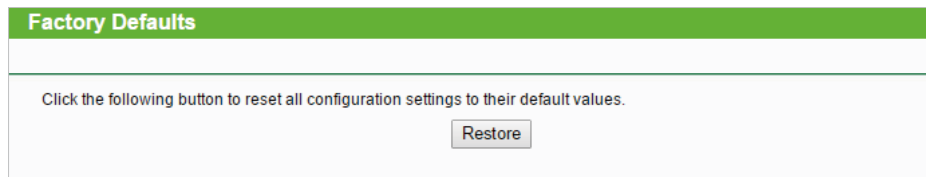
1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools](#) > [Firmware Upgrade](#).
4. Click [Browse](#) to locate the downloaded firmware file, and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



The screenshot shows the 'Firmware Upgrade' page. It features a green header with the title 'Firmware Upgrade'. Below the header, there is a 'File:' label followed by an empty text input field and a 'Browse...' button. Underneath, the 'Firmware Version:' is displayed as '3.13.26 Build 120723 Rev.00000' and the 'Hardware Version:' is 'VBRN4342 v1.000000'. At the bottom of the form, there is an 'Upgrade' button.

6.6.4. 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.



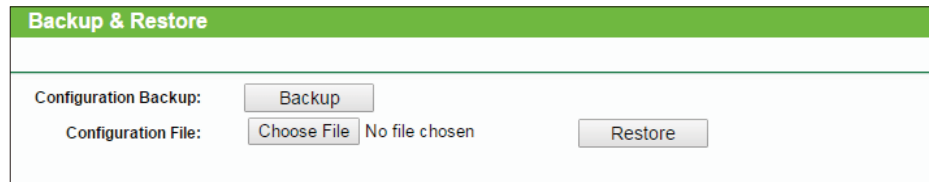
The screenshot shows the 'Factory Defaults' page. It has a green header with the title 'Factory Defaults'. Below the header, there is a text instruction: 'Click the following button to reset all configuration settings to their default values.' Below this text is a 'Restore' button.

- The default **Username**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.1
- The default **Subnet Mask**: 255.255.255.0

6.6.5. 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:**

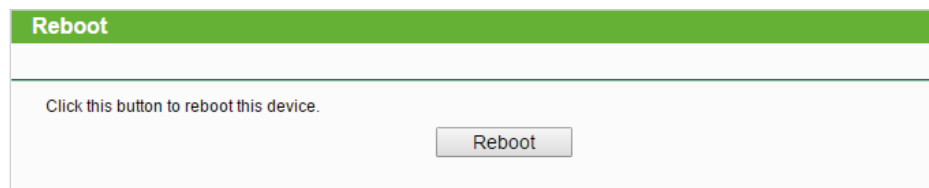
1. Click [Choose File](#) to locate the backup configuration file stored in your computer, and click [Restore](#).
2. Wait a few minutes for the restoring and rebooting.

■ **Note:**

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

6.6.6. Reboot

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.



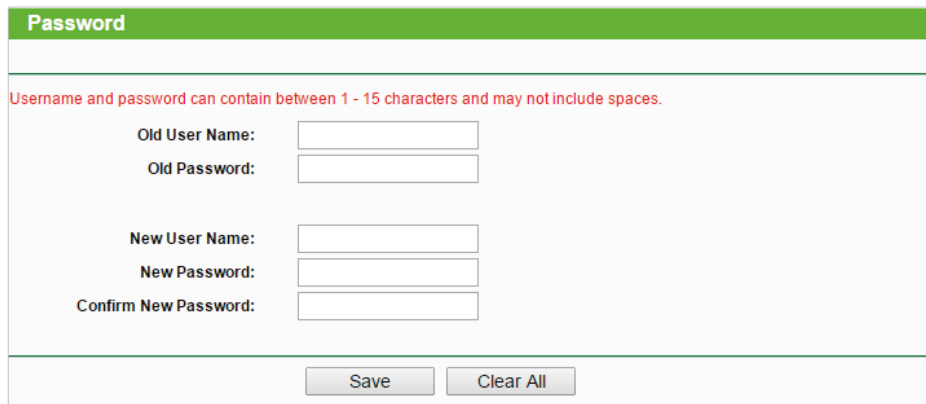
Some settings of the router will take effect only after rebooting, including:

- 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).

6.6.7. 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. At the top, there is a green header with the word 'Password'. Below the header, a red warning message states: 'Username and password can contain between 1 - 15 characters and may not include spaces.' The form contains six input fields: 'Old User Name:', 'Old Password:', 'New User Name:', 'New Password:', and 'Confirm New Password:'. At the bottom of the form, there are two buttons: 'Save' and '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](#).

6.6.8. 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.

System Log

Auto Mail Feature: Disabled Mail Settings

Log Type: ALL Log Level: ALL

Index	Time	Type	Level	Log Content
5	1st day 03:05:45	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
4	1st day 03:05:41	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
3	1st day 03:05:39	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
2	1st day 03:05:37	DHCP	INFO	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
1	1st day 03:04:59	DHCP	INFO	DHCPS:Recv INFORM from C0:4A:00:1A:C3:45

Time = 2016-01-01 3:13:05 11587s
H-Ver = XXXXXXXXXX : S-Ver = XXXXXXXXXX
L = 192.168.0.254 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Refresh
Save Log
Mail Log
Clear Log

Previous
Next
Current No. 1
Page

- [Auto Mail Feature](#) - Indicates whether the auto mail feature is enabled or not.
- [Mail Settings](#) - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

Mail Account Settings

From:

To:

SMTP Server:

Authentication

Enable Auto Mail Feature

Everyday, mail the log at : (HH:MM)

Mail the log every hours

Save
Back

- [From](#) - Your mail box address. The router will connect it to send logs.
- [To](#) - Recipient's mail address. The destination mailbox which will receive logs.
- [SMTP Server](#) - Your smtp server. It corresponds with the mailbox filled in the [From](#) field. You can log on the relevant website for help if you are not clear with the address.
- [Authentication](#) - Most SMTP Server requires Authentication. It is required by most mailboxes that need user name and password to log in.

Note:

Only when you select Authentication, do you have to enter the user name and password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is included.
- **Password** - Your mail account password.
- **Confirm The Password** - Enter the password again to confirm.
- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field.

Click [Save](#) to apply your settings.

Click [Back](#) to return to the previous page.

- **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.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Clear Log** - All the logs will be deleted from the router permanently, not just from the page.

Click [Next](#) to go to the next page, or click [Previous](#) to return to the previous page.

6.7. Logout

Click [Logout](#) at the bottom of the main menu, and you will log out of the web page and return to the login window.

FAQ

Q1. What can I do if I cannot access the Internet?

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

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

With the router powered on, press and hold the [WPS/Reset](#) button for 5 seconds until the Power LED starts flashing and then release the button.

Note: After resetting, all previous configurations will be cleared, and the router will reset to the mode that you have chosen via the operation mode switch.

Q3. What can I do if I forgot my wireless password?

- If you have not changed the default Wireless Password, it can be found on the label of the router.
- Otherwise, connect a computer to the router via an Ethernet cable. Log into the Web Management page, and go to [Wireless](#) > [Wireless Security](#) to retrieve or reset your wireless password.

Q4. What can I do if I forgot my login password of the web management page?

The default username and password of the web management page are [admin](#) (in lowercase). If you have altered the password:

1. Reset the router to factory default settings: With the router powered on, press and hold the [WPS/Reset](#) button for 5 seconds until the Power LED starts flashing and then release the button.
2. Visit <http://tplinkwifi.net>, and enter [admin](#) (in lowercase) as both username and password to login.

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

Q5. What do I need to do if I want to use NetMeeting?

If you start NetMeeting as a sponsor, you don't need to do anything with the router. If you start as a response, please follow the steps below to configure the router:

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

2. Enable DMZ: Go to [Forwarding](#) > [DMZ](#). Select [Enable](#) and enter your IP address in the [DMZ Host IP Address](#) field, and then Click [Save](#).

3. Enable H323 ALG: Go to [Security](#) > [Basic Security](#), enable [H323 ALG](#) and click [Save](#).

Now you can enjoy your net meeting normally.

Q6. What can I do if my wireless signal is unstable or weak?

It may be caused by too much interference.

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

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **TP-LINK** is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2016 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

FCC STATEMENT



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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

CE Mark Warning

CE 1588

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

RF Exposure Information

This device meets the EU requirements (1999/5/EC Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

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

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. Operation is subject to the following two conditions:

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

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

1. l'appareil ne doit pas produire de brouillage;
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, 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

注意！

依據 低功率電波輻射性電機管理辦法

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

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

BSMI Notice

安全諮詢及注意事項

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




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





Safety Information

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

- The plug considered as disconnect device of adapter.
-  Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	<p>RECYCLING</p> <p>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.</p> <p>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.</p>