

# TP-LINK®

## User Guide

**TL-WA830RE**

**300Mbps Wireless N Range Extender**



## **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 © 2011 TP-LINK TECHNOLOGIES CO., LTD.

All rights reserved.

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

## FCC STATEMENT



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

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

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

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

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

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

### FCC RF Radiation Exposure Statement

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

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

### CE Mark Warning



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

## National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

## DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **300Mbps Wireless N Range Extender**

Model No.: **TL-WA830RE**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

**ETSI EN 300 328 V1.7.1: 2006**

**ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009**

**EN60950-1:2006**

Recommendation 1999/519/EC

**EN62311:2008**

Directives 2004/108/EC

The above product is in conformity with the following standards or other normative documents

**EN 55022:2006 +A1:2007**

**EN 55024:1998+A1:2001+A2:2003**

**EN 61000-3-2:2006**

**EN 61000-3-3:1995+A1:2001+A2:2005**

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents

**EN60950-1:2006**

Directive (ErP) 2009/125/EC

Audio/Video, information and communication technology equipment- Environmentally conscious design

**EN62075:2008**

Person is responsible for marking this declaration:



**Yang Hongliang**

**Product Manager of International Business**

#### Industry Canada Statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

#### IMPORTANT NOTE:

##### Radiation Exposure Statement:

This equipment complies with Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

- (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

#### NOTE IMPORTANTE:

##### 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.

#### NCC Notice:

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及功能。

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

#### Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음

# CONTENTS

<b>Package Contents</b> .....	<b>I</b>
<b>Chapter 1 Introduction</b> .....	<b>1</b>
1.1 Product Overview.....	1
1.2 Main Features .....	2
1.3 Appearance.....	2
1.3.1 The Front Panel.....	2
1.3.2 The Rear Panel.....	3
<b>Chapter 2 Hardware Installation</b> .....	<b>4</b>
2.1 Before You Begin.....	4
2.2 Basic Requirements.....	4
2.3 Connecting the Device.....	4
<b>Chapter 3 Quick Installation Guide</b> .....	<b>6</b>
3.1 Configure the PC .....	6
3.2 Quick Setup .....	9
<b>Chapter 4 Configure the Device</b> .....	<b>17</b>
4.1 Status.....	17
4.2 Quick Setup .....	18
4.3 Range Extender .....	18
4.4 Network.....	23
4.5 Wireless .....	23
4.5.1 Wireless Settings.....	24
4.5.2 Wireless Security.....	27
4.5.3 Wireless MAC Filtering.....	32
4.5.4 Wireless Advanced.....	34
4.5.5 Throughput Monitor .....	35
4.5.6 Wireless Statistics.....	36
4.6 DHCP .....	36
4.6.1 DHCP Settings.....	37
4.6.2 DHCP Clients List.....	38
4.6.3 Address Reservation .....	38
4.7 System Tools .....	39
4.7.1 SNMP .....	40
4.7.2 Diagnostic.....	41
4.7.3 Ping Watch Dog.....	43
4.7.4 Firmware Upgrade .....	44

4.7.5	Factory Defaults.....	45
4.7.6	Backup & Restore.....	45
4.7.7	Reboot.....	46
4.7.8	Password.....	47
4.7.9	System Log.....	47
<b>Appendix A: Application Example.....</b>		<b>49</b>
<b>Appendix B: Factory Defaults.....</b>		<b>52</b>
<b>Appendix C: Troubleshooting.....</b>		<b>53</b>
<b>Appendix D: Specifications.....</b>		<b>54</b>
<b>Appendix E: Glossary.....</b>		<b>55</b>



# Package Contents

The following items should be found in your package:

- One TL-WA830RE 300Mbps Wireless N Range Extender
- Ethernet Cable
- One Power Adapter for TL-WA830RE 300Mbps Wireless N Range Extender
- Quick Installation Guide
- One Resource CD for TL-WA830RE 300Mbps Wireless N Range Extender, including:
  - This User Guide
  - Other helpful information

## **Note:**

Make sure that the package contains the above items. If any of the listed items is damaged or missing, please contact with your distributor.

# Conventions

The AP or TL-WA830RE, or Device mentioned in this User guide stands for TL-WA830RE 300Mbps Wireless N Range Extender without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation. You can set the parameters according to your demand.

# Chapter 1 Introduction

Thank you for choosing the **TL-WA830RE 300Mbps Wireless N Range Extender**.

## 1.1 Product Overview

The TL-WA830RE 300Mbps Wireless N Range Extender is dedicated to Small Office/Home Office (SOHO) wireless network solutions. It allows for greater range and mobility within your wireless network while also allowing you to connect the wireless devices to a wired environment. Increased mobility and the absence of cabling will be beneficial for your network.

With using IEEE 802.11n wireless technology, your device can transmit wireless data at the rate of up to 300Mbps. With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi protected Access (WPA2-PSK, WPA-PSK), the TL-WA830RE 300Mbps Wireless N Range Extender delivers complete data privacy.

It supports an easy, web-based setup for installation and management. Even though you may not be familiar with the Access Point, you can easily configure it with the help of this Guide. Before installing the AP, please look through this Guide to get the full information of the TL-WA830RE 300Mbps Wireless N Range Extender.

## 1.2 Main Features

- Make use of IEEE 802.11n wireless technology
- Provides multiple encryption security Types including: 64/128/152-bit WEP WPA/WPA2 WPA-PSK/WPA2-PSK
- Supports Built-in DHCP server
- Supports MAC address filtering
- Supports multiple operating modes including: Range Extender, Access Point
- Supports Firmware Upgrade
- Supports Remote and Web management

## 1.3 Appearance

### 1.3.1 The Front Panel

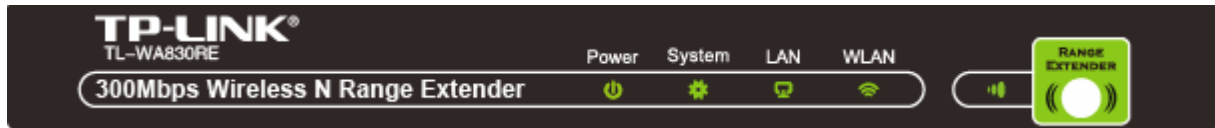


Figure 1-1

The front panel of the TL-WA830RE consists of several LED indicators, which is designed to indicate connections. View from left to right, Table 1-1 describes the LEDs on the front panel of the device.

#### LED Explanation

Name	Status	Indication
Power	Off	No Power
	On	Power on
System	Off	The device has a system error
	On	The device is initialising
	Flashing	The device is working properly
LAN	Off	There is no device linked to the corresponding port
	On	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
WLAN	Off	The Wireless function is disabled
	Flashing	The Wireless function is enabled
Range Extender	On	The Range Extender has connected the Router successfully
	Flashing	The Range Extender is connecting the Router
	Off	The Range Extender has not connected any Router yet

Table 1-1

### 1.3.2 The Rear Panel

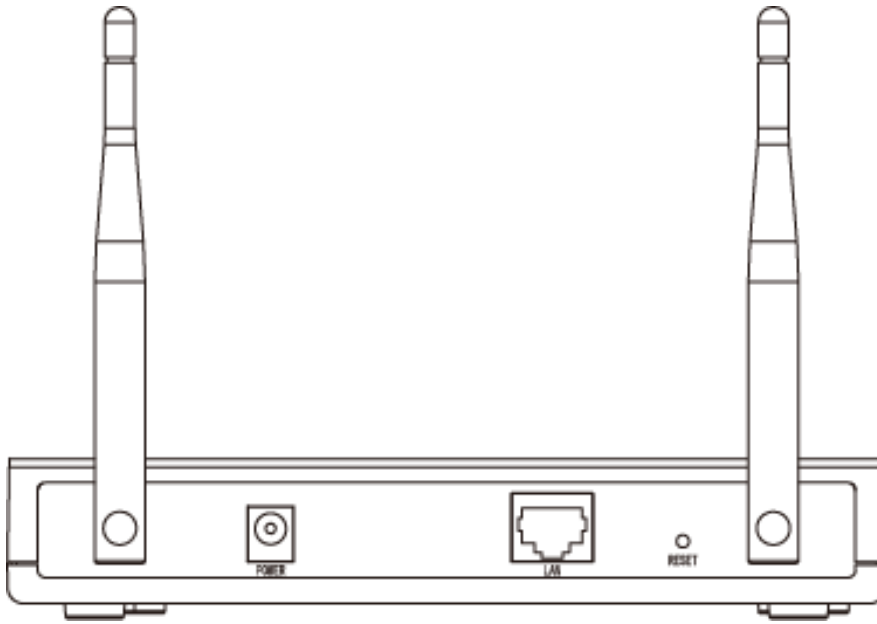


Figure 1-2

Viewed from left to right, the following parts are located on the rear panel of TL-WA830RE.

**Wireless antenna:** The external antenna is used to transmit and receive wireless data.

**POWER:** The power port connects to the power adapter provided with the TL-WA830RE 300Mbps Wireless N Range Extender.

**LAN:** One LAN 10/100Mbps RJ45 port connects to a network device, such as a switch or a router.

**RESET:** The Reset button is used to restore the AP's factory default settings. There are two ways to reset the Access Point's factory defaults:

- **Method one:** With the AP powered on, use a pin to press and hold the Reset button (about 5 seconds) until the System LED becomes quick-flash from slow-flash. And then release the button and wait the AP to reboot to its factory default settings.
- **Method two:** Restore the default settings from "**System Tools > Factory Defaults**" of the AP's Web-based management page.

 **Note:**

Ensure the AP is powered on before it restarts completely.

## Chapter 2 Hardware Installation

### 2.1 Before You Begin

Please read this User Guide carefully before installing and using the equipment. The operating distance range of your wireless connection can vary significantly depending on the physical position of the wireless devices. Factors that can weaken signals by getting in the way of your network's radio waves are metal appliances or obstructions, and walls. Typical ranges vary base on the types of materials and background RF (radio frequency) noise in your home or office.

For best performance of your wireless network, you are suggested to:

- 1). Avoid redundant obstacles and interference between the wireless devices.
- 2). Keep your AP away from appliances with a strong electric field or magnetic field, such as a microwave oven or refrigerator.

Place the AP near the center of the area in which your computers operates.

### 2.2 Basic Requirements

- Use only the power adapter provided with your AP
- The electrical outlet shall be installed near the device and shall be easily accessible
- Place your AP in a well ventilated place far from direct sunlight, any heater or heating vent
- Leave at least 2 inches (5cm) space around the device for heat dissipation
- Turn off your AP and unplug the power adapter in a lighting storm to avoid damage
- Web browser, such as Microsoft Internet Explorer 5.0 or above, Netscape Navigator 6.0 or above
- Operating temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

### 2.3 Connecting the Device

Figure 2-1 is an example of the typical application of TL-WA830RE in the infrastructure network. An Infrastructure network contains an access point or a wireless router.

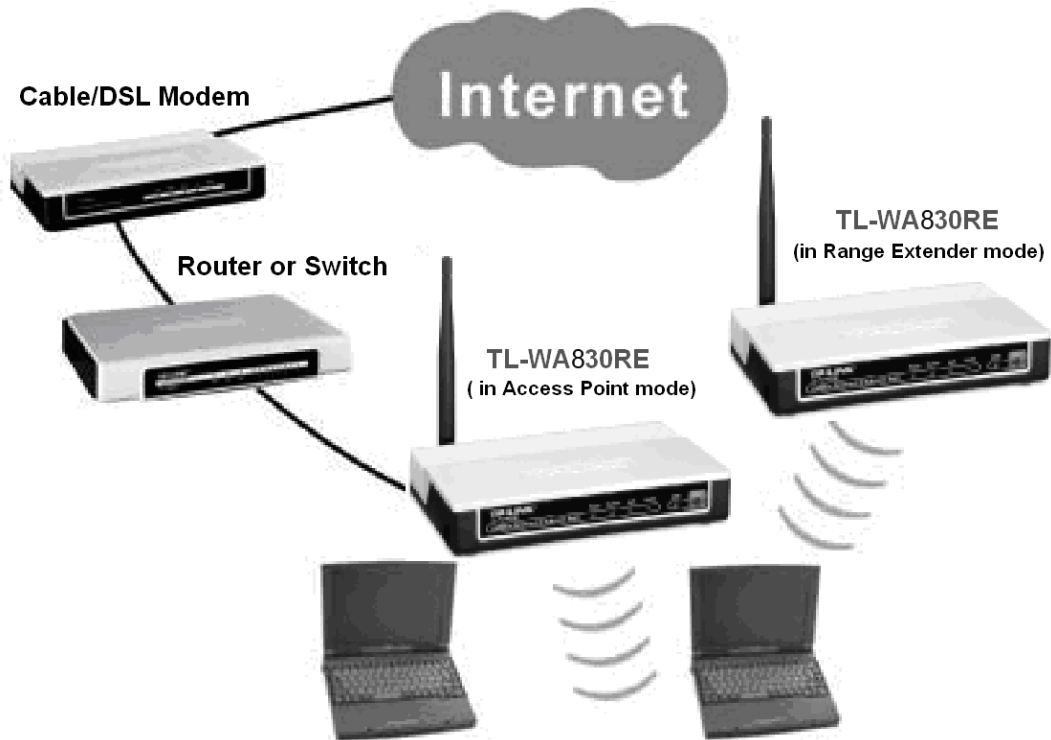


Figure 2-1 The Example of Infrastructure Network Incorporating the TL-WA830RE

To establish a typical connection of the AP, please take the following steps:

1. Connect the Cable or DSL modem to a Router.
2. Locate an optimum location for the AP. The best place is usually near the center of the area in which your PC(s) will wirelessly connect.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the Ethernet Broadband Router to the TL-WA830RE Access Point. Power on the AP.
5. Then you can connect a desktop PC or laptop to your network. (Make sure your computer or laptop is equipped with a Wireless Adapter.)

**Note:**

If you are not so clear about how to connect your devices to the network, please refer to [Appendix A Application Example](#).

## Chapter 3 Quick Installation Guide

This chapter will guide you to configure your PC to communicate with the AP and to configure and manage the TL-WA830RE 300Mbps Wireless N Range Extender easily with a Web-based utility.

### 3.1 Configure the PC

The wireless adapter-equipped computers in your network must be in the same IP Address range without overlap with each other. Manually configure the **IP address** as 192.168.0.\* (\* is any integer between 1 to 253), and the **Subnet mask** as 255.255.255.0 for your PC by following the instructions below.

Connect the local PCs to the LAN ports on the AP and configure the IP address manually for your PCs.

1. Click **Start** (in the lower left corner of the screen), right-click **My Network Connections** and choose **Properties**.

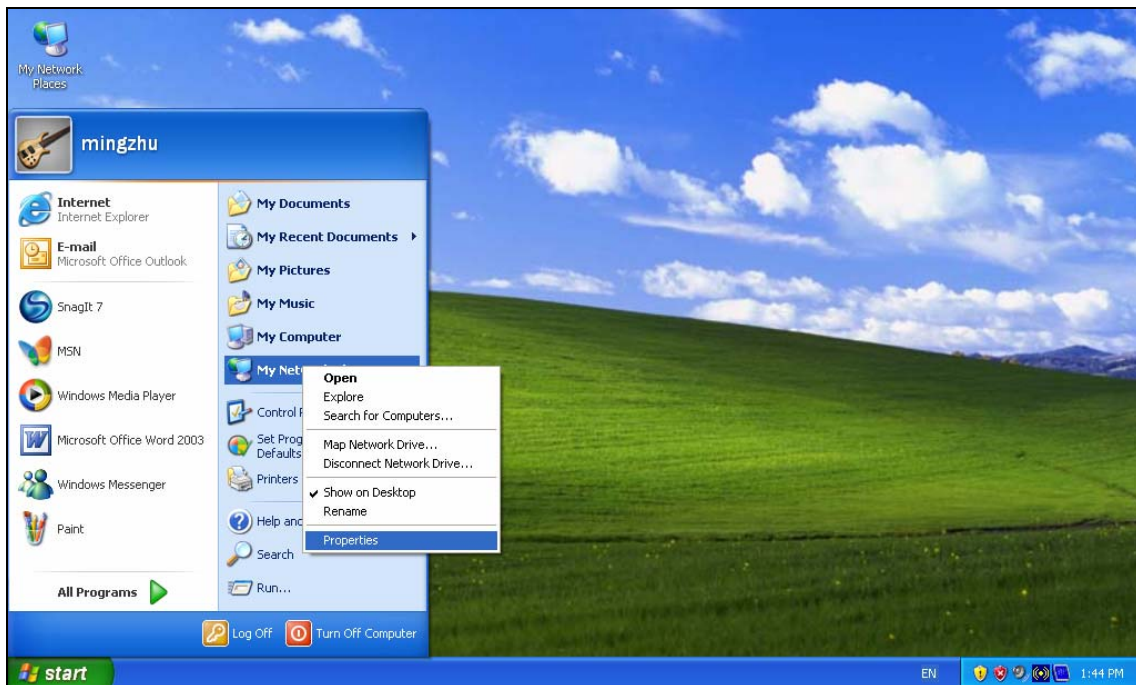


Figure 3-1

2. On the **My Network Connections** window shown as Figure 3-2 below, right-click **LAN (Local Area Connection)** and choose **Properties**.

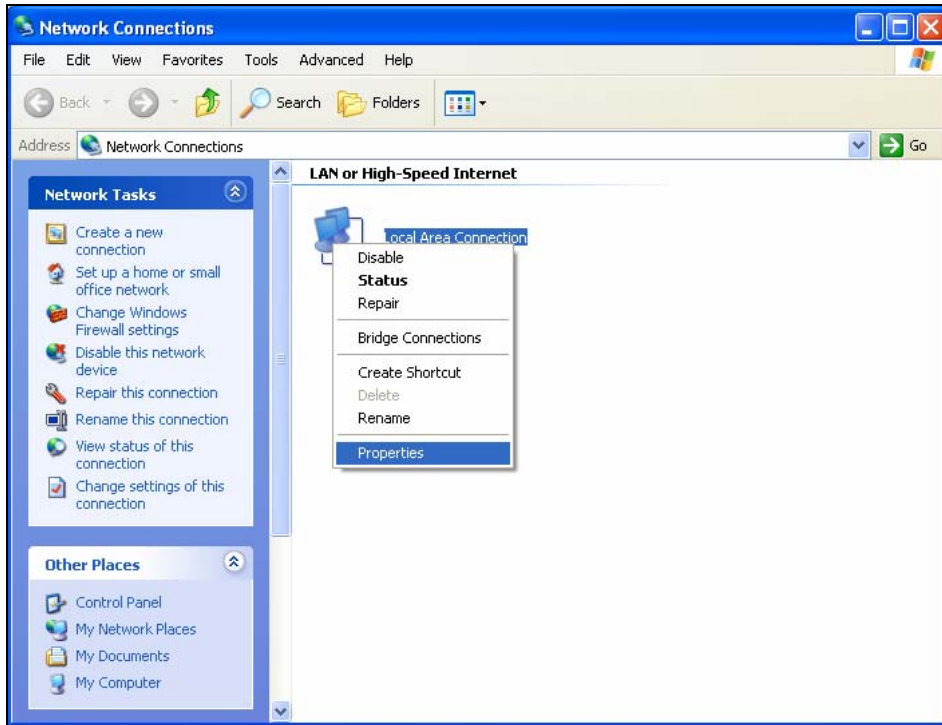


Figure 3-2

3. In the **General** tab of **Internet Protocol (TCP/IP) Properties** window, highlight **Internet Protocol (TCP/IP)** and click **Properties**.

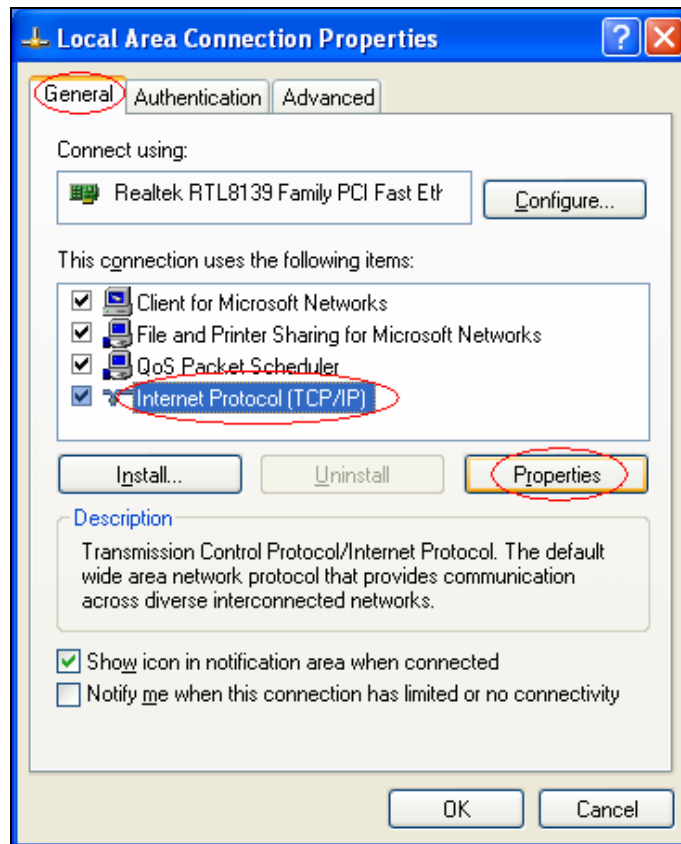


Figure 3-3



4. Configure the IP address manually.
  - 1) Select **Use the following IP address**.
  - 2) Enter 192.168.0.\* (\* is any integer between 1 to 253) into the **IP address** filed, 255.255.255.0 into the **Subnet mask** filed and 192.168.0.254 into the **Default gateway** filed.
  - 3) Click **OK** to keep your settings.

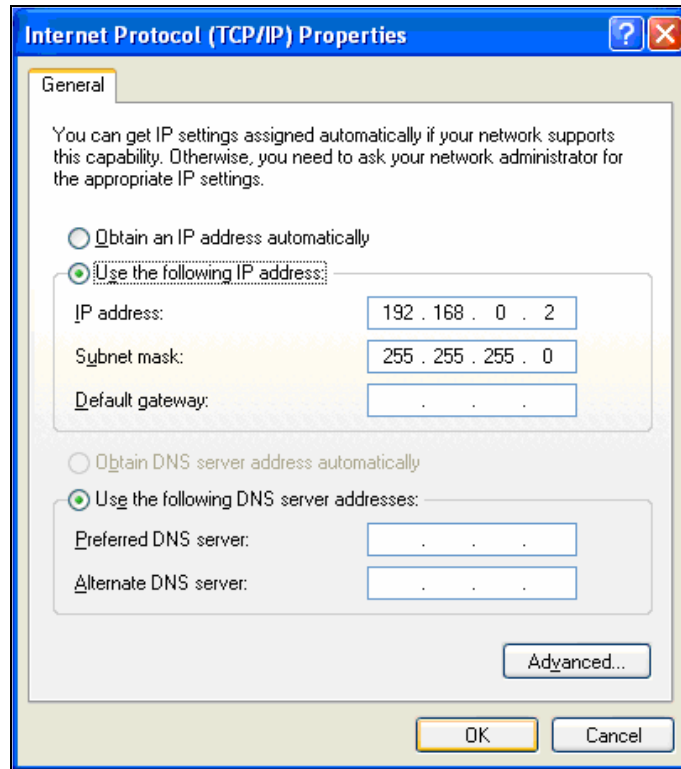


Figure 3-4

5. Verify the network connection between your PC and the AP via the Ping command. The following example is in Windows XP Operating System.
  - 1) Click **Start > Run** tab. Enter **cmd** in the filed and click **OK**.
  - 2) Type ping 192.168.0.254 on the screen that displays and then press **Enter**.

If the result displayed is similar to that shown as Figure 3-5 below, the connection between your PC and the AP has been successfully established.

```
Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 3-5

If the result displayed is similar to that shown as Figure 3-6 below, it means that your PC has not connected to the AP.

```
Pinging 192.168.0.254 with 32 bytes of data: :
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Figure 3-6

Please check following these steps:

- a) Check to see if your PC and the AP are right connected. The LED of LAN port which you link to on the device and the LED on your PC's adapter should be lit up.
- b) Make sure the TCP/IP for your PC is right configured. If the AP's IP address is 192.168.0.254, your PC's IP address must be within the range of 192.168.0.1 ~ 192.168.0.253.

### 3.2 Quick Setup

With a Web-based utility, it is easy to configure and manage the TL-WA830RE 300Mbps Wireless N Range Extender. 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.

1. To access the configuration utility, open a web-browser and type in the default address *http://192.168.0.254* in the address field of the browser.



Figure 3-7 Login to the AP

After a moment, a login window will appear, similar to the Figure 3-8. Enter **admin** for the User Name and Password (both in lower case letters). Then click **OK** or press Enter.



Figure 3-8 Login Windows

**Note:**

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

2. After successfully logging in, click the Quick Setup menu to quickly configure your AP and the following figure will display. Click Next to continue.

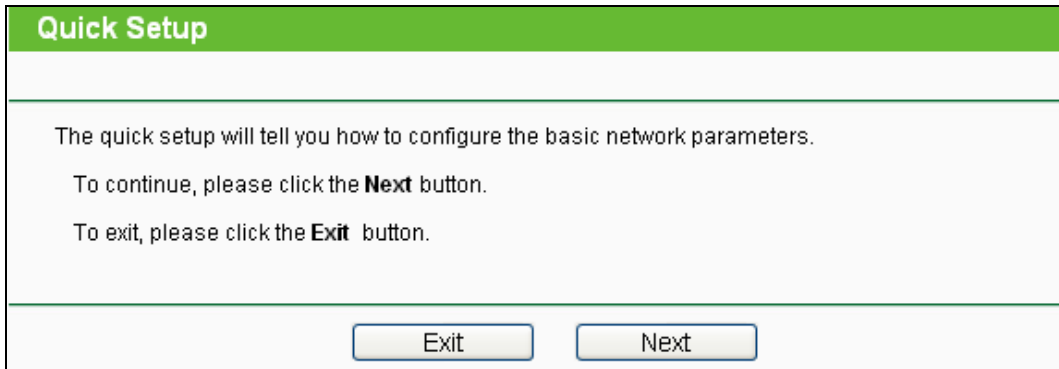


Figure 3-9 Quick Setup

3. And then **Wireless** page will appear shown in Figure 3-10. There are two Operation Modes, including Range Extender and Access Point. The available setting options are different in different operation modes, and they are explained below.

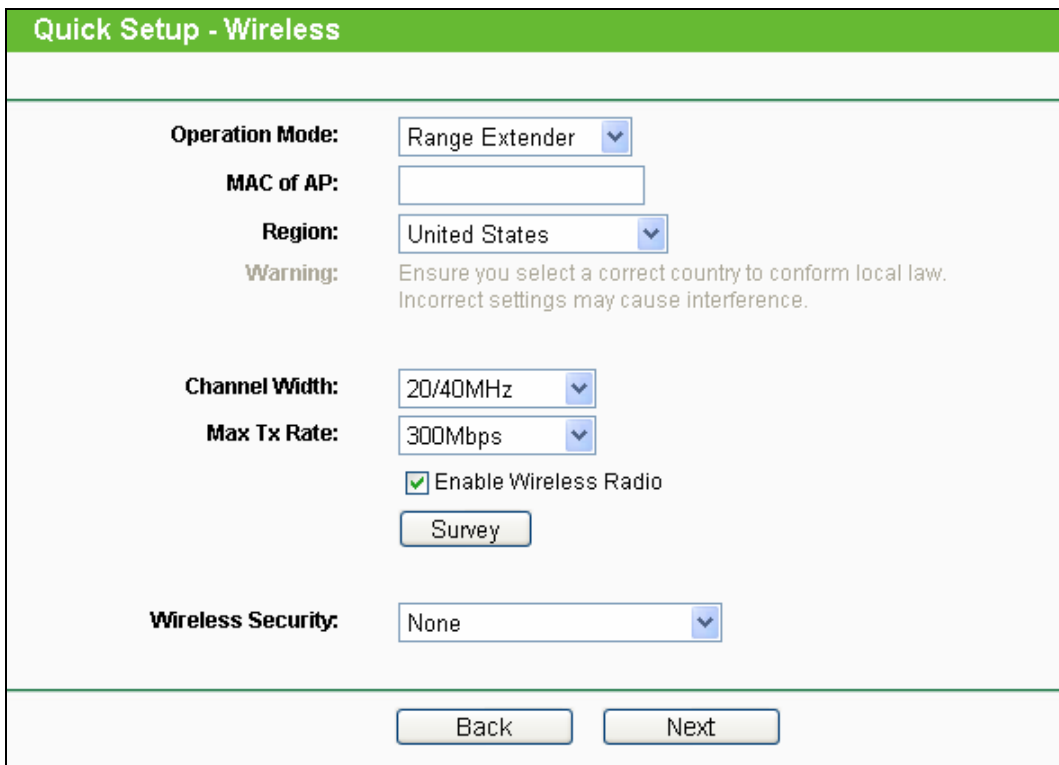


Figure 3-10 Quick Setup - Wireless

- A. When you choose **Range Extender**, take the following steps:
  - 1) Click **Survey** on the Wireless page shown as Figure 3-10 , and then AP List page will appear, shown in Figure 3-11.

AP List						
AP Count: 15						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-AA-BB-01-23-45	3631_8	4dB	1	OFF	<a href="#">Connect</a>
2	E0-05-C5-00-00-01	BrcmAP0	6dB	1	OFF	<a href="#">Connect</a>
3	5C-63-BF-53-19-84	TP-LINK_531984	10dB	1	OFF	<a href="#">Connect</a>
4	10-9A-DD-85-2E-3B	apple_lee	15dB	1	ON	<a href="#">Connect</a>
5	00-25-12-39-00-71		15dB	2	ON	<a href="#">Connect</a>
6	00-27-19-DF-DC-72		21dB	6	ON	<a href="#">Connect</a>
7	D8-5D-4C-65-6D-4E	123	13dB	6	OFF	<a href="#">Connect</a>
8	40-16-9F-BF-50-F2	TP-LINK_BF50F2	13dB	6	ON	<a href="#">Connect</a>
9	54-E6-FC-B8-4F-74	qiao12_25_2012	14dB	8	ON	<a href="#">Connect</a>
10	00-89-74-10-03-21	TP-LINK_100321	2dB	11	ON	<a href="#">Connect</a>
11	00-0A-EB-13-09-69	TP-LINK_130969	15dB	11	OFF	<a href="#">Connect</a>
12	00-11-22-33-44-55	TP-LINK_334455	4dB	11	OFF	<a href="#">Connect</a>
13	00-1D-0F-88-89-36	TP-LINK_888936	11dB	11	OFF	<a href="#">Connect</a>
14	40-16-9F-BF-50-F6	TP-LINK_BF50F6	23dB	11	OFF	<a href="#">Connect</a>
15	00-11-22-33-44-57	zyzyzy	9dB	11	OFF	<a href="#">Connect</a>
<input type="button" value="Refresh"/>						

Figure 3-11 AP List

- Find the SSID of the Access Point / Router you want to access, and click **Connect** in the corresponding row. For example, the first item is selected. The MAC address will be automatically filled into the corresponding box which is shown as the Figure 3-12 .

**Quick Setup - Wireless**

**Operation Mode:** Range Extender

**MAC of AP:** 40-16-9F-BF-50-F6

**Region:** United States

**Warning:** Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

**Channel Width:** 20/40MHz

**Max Tx Rate:** 300Mbps

Enable Wireless Radio

Survey

**Wireless Security:** None

Back Next

Figure 3-12 Quick Setup – Range Extender Mode

- **Operation Mode** - Two Operation Modes are supported, including: Range Extender and Access Point.
- **MAC of AP** - The MAC address of the desired AP. The AP client will connect to the desired AP according to MAC address.

**Note:**

1. In Range Extender mode, the wireless repeater relays signal between its stations and the root AP for greater wireless range. The MAC address of root AP can be automatically filled into corresponding box by clicking the **Survey** button and selecting the desired item.
2. If you know the MAC address of the desired AP, you can also input it into the field "MAC of AP" manually.

- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

**Note:**

Restricted by local law regulations, version for North America does not have region selection option.

- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate** - Specifies the maximum transmit rate of the device through this field.

- **Enable Wireless Radio** - Select or deselect this check box to allow or deny wireless stations to access the device.
- **Wireless Security** - Wireless Security will enable you to configure wireless security for your wireless network to protect your data from intruders. There are four options, which are explained below.
  - **None** - If the network of the desired AP/ Router is unsecured, please choose this option.
  - **WEP** - If the Wireless Security of the desired AP/ Router is WEP, please select this option, then you will see the page display as shown below.

The screenshot shows a configuration page for WEP. It includes the following fields and options:

- Wireless Security:** WEP (selected in a dropdown menu)
- Type:** Automatic (selected in a dropdown menu)
- WEP Key Format:** Hexadecimal (selected in a dropdown menu)
- WEP Index:** 1 (selected in a dropdown menu)
- WEP Password:** An empty text input field.

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

**Type** - Select the authentication type from the drop-down list. It must be the same as the desired AP/ Router's.

**WEP Key Format** - Select WEP Key format from the drop-down list, which must be the same as the desired AP/ Router's.

**WEP Index** - Select the index of the desired AP/ Router's WEP Password.

**WEP Password** - Enter the desired AP/ Router's WEP Password here.

- **WPA-PSK/ WPA2-PSK** - Select this option, the page will display as shown below.

The screenshot shows a configuration page for WPA-PSK/WPA2-PSK. It includes the following fields and options:

- Wireless Security:** WPA-PSK/WPA2-PSK (selected in a dropdown menu)
- Version:** Automatic (selected in a dropdown menu)
- Encryption:** Automatic (selected in a dropdown menu)
- PSK Password:** An empty text input field.

Below the PSK Password field, there is a note: "(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)"

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

**Version** - Select the authentication version from the drop-down list. It must be the same as the desired AP/ Router's.

**Encryption** - Select the Encryption from the drop-down list, which must be the same as the desired AP/ Router's.

**PSK Password** - Enter the desired AP/ Router's PSK Password here.

- **No Change** - If you choose this option, wireless security configuration will not change.

**B.** When you choose **Access Point**, you will see the following figure as shown below.

**Quick Setup - Wireless**

**Operation Mode:** Access Point

**SSID:** TP-LINK\_F1A6A7

**Region:** United States

**Warning:** Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

**Channel:** Auto

**Mode:** 11bgn mixed

**Channel Width:** 20/40MHz

**Max Tx Rate:** 300Mbps

Enable Wireless Radio

Enable SSID Broadcast

**Wireless Security:** None

Back Next

Figure 3-13 Quick Setup – Access Point Mode

- **Operation Mode** - Two Operation Modes are supported, including: Access Point and Range Extender.
- **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK\_XXXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

 **Note:**

Restricted by local law regulations, version for North America does not have region selection option.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. (Only channel 1-11 can be used in the United States according to the law.)
- **Mode** - This field determines the wireless mode which the AP works on.
- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate** - Specifies the maximum transmit rate of the device through this field.

- **Enable Wireless Radio** - Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast** - Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.
- **Wireless Security** - Wireless Security will enable you to configure wireless security for your wireless network to protect your data from intruders. There are four options, which are explained below.
  - **None** - If you choose this option, the wireless stations will be able to connect to this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
  - **WEP** - Select this option, the page will display as shown below.

**Type** - Select the authentication type from the drop-down list. It is recommended to choose **Automatic**.

**WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

**WEP Index** - Select the index for **WEP Password**.

**WEP Password** - Enter a password for your wireless network here. If you select **ASCII** for **WEP Key Format**, the password should be 5/13/16 ASCII characters, and if you select **Hexadecimal** for **WEP Key Format**, the password should be 10/26/32 hexadecimal digits.

- **WPA-PSK/ WPA2-PSK** - Select this option, the page will display as shown below.

**Version** - Select the authentication version from the drop-down list. It is recommended to choose **Automatic**.



**Encryption** - When you select WPA-PSK or WPA2-PSK for Authentication Type, you can select either Automatic, TKIP or AES as Encryption.

**PSK Password** - Enter a password for your wireless network here, which should be ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.

- **No Change** - If you choose this option, wireless security configuration will not change.

These settings are only for basic wireless parameters, for advanced settings, please refer to [Section 4.5: "Wireless."](#)

4. Click the **Next** button. You will then see the **Finish** page.

Because there are something changed on the **Wireless** page, you will see the **Finish** page as shown in Figure 3-14. Click the **Reboot** button to make your wireless configuration to take effect and finish the **Quick Setup**.

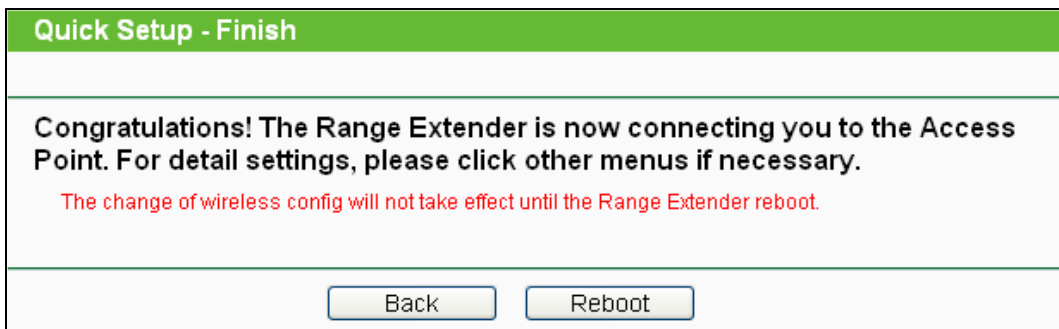


Figure 3-14 Quick Setup – Finish

If you don't make any changes on the **Wireless** page, you will see the **Finish** page as shown in Figure 3-15. Click the **Finish** button to finish the **Quick Setup**.

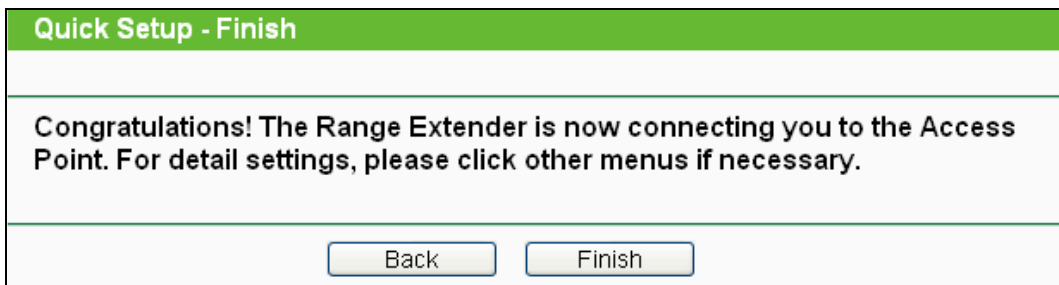


Figure 3-15 Quick Setup - Finish

## Chapter 4 Configure the Device

This Chapter describes how to configure your Access Point via the web-based management page. The TL-WA830RE 300Mbps Wireless N Range Extender is easy to configure and manage with the Web-based (Internet Explorer, Netscape® Navigator, Firefox, Safari, Opera or Chrome) management page, which can be launched on any windows, Macintosh or UNIX OS with a web browser.

After a successful login, you can configure and manage the device. There are seven main menus on the leftmost column of the web-based management page: **Status**, **Quick Setup**, **Range Extender**, **Network**, **Wireless**, **DHCP** and **System Tools**. Submenus will be available after clicking one of the main menus. On the right of the web-based management page lies the detailed explanations and instructions for the corresponding page.

### 4.1 Status

Selecting **Status** will enable you to view the AP's current status and configuration, all of which is read-only.

Status		
<b>Firmware Version:</b>	3.12.15 Build 110819 Rel.33218n	
<b>Hardware Version:</b>	WA830RE v1 00000000	
<b>Wired</b>		
<b>MAC Address:</b>	B0-48-7A-F1-A6-A7	
<b>IP Address:</b>	192.168.0.254	
<b>Subnet Mask:</b>	255.255.255.0	
<b>Wireless</b>		
<b>Operation Mode:</b>	Range Extender	
<b>Name (SSID):</b>	TP-LINK_F1A6A7	
<b>Channel:</b>	6	
<b>Channel Width:</b>	20/40MHz	
<b>Max Tx Rate:</b>	300Mbps	
<b>MAC Address:</b>	B0-48-7A-F1-A6-A7	
<b>Traffic Statistics</b>		
	<b>Received</b>	<b>Sent</b>
<b>Bytes:</b>	<b>0</b>	<b>0</b>
<b>Packets:</b>	<b>0</b>	<b>0</b>
<b>System Up Time:</b>	0 days 00:13:55	<input type="button" value="Refresh"/>

Figure 4-1 Device Status

- **Firmware Version** - This field displays the current firmware version of the AP.
- **Hardware Version** - This field displays the current hardware version of the AP

- **Wired** - This field displays the current settings or information for the Network, including the **MAC address, IP address** and **Subnet Mask**.
- **Wireless** - This field displays basic information or status for wireless function, including **Wireless Mode, SSID, Channel, Mode, Channel Width, Max Tx Rate** and **MAC Address**.
- **Traffic Statistics** - This field displays the AP's traffic statistics.
- **System Up Time** - This field displays the run time of the AP since it's powered on or reset.

 **Note:**

If you select Access Point mode in Figure 3-10, the wireless status in Figure 4-1 will change, similar to the figure below:

Wireless	
<b>Operation Mode:</b>	Access Point
<b>Name (SSID):</b>	TP-LINK_F1A6A7
<b>Channel:</b>	0
<b>Mode:</b>	11bgn mixed
<b>Channel Width:</b>	20/40MHz
<b>Max Tx Rate:</b>	300Mbps
<b>MAC Address:</b>	B0-48-7A-F1-A6-A7

## 4.2 Quick Setup

Please refer to [Section 3.2: "Quick Installation Guide."](#)

## 4.3 QSS

**QSS (Quick Secure Setup)** can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to an existing network quickly by function. Select menu "QSS", you will see the next screen shown in Figure 4-2.

**QSS (Quick Secure Setup)**

---

**Operation Mode:** Access Point

---

**QSS Status:** Enabled

**Current PIN:** 96980088

**Add A New Device:**

The change of wireless config will not take effect until the AP reboots, please [click here](#) to reboot.

Figure 4-2 QSS

- **Operation Mode** - Displays the current operation mode of the device.

- **QSS Status** - To enable or disable the QSS function here.
- **Current PIN** - The current value of the device's PIN is displayed here. The default PIN of the device can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the device to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the device's PIN. You can ensure the network security by generating a new PIN.
- **Add device** - You can add a new device to the existing network manually by clicking this button.

 **Note:**

The QSS function is only available when the Operation Mode is set to Access Point.

**To add a new device:**

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and device using either Push Button Configuration (PBC) method or PIN method.

 **Note:**

To build a successful connection by QSS, you should also do the corresponding configuration of the new device for QSS function meanwhile.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

**Method One:**

Step 1: Keep the QSS Status as **Enabled** and click the **Add device** button in Figure 4-2, then the following screen will appear.

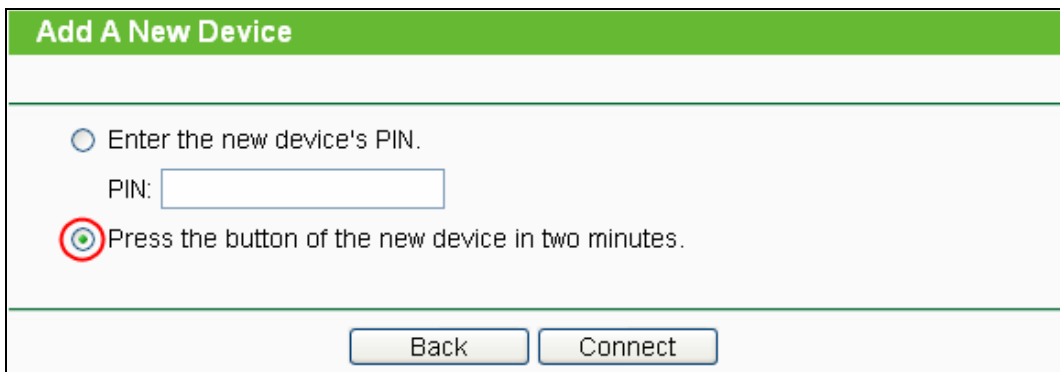


Figure 4-3 Add A New Device

Step 2: Choose **“Press the button of the new device in two minutes”** and click **Connect**.

Step 3: For the configuration of the wireless adapter, please choose **“Push the button on my access point”** in the configuration utility of the QSS as below, and click **Next**.

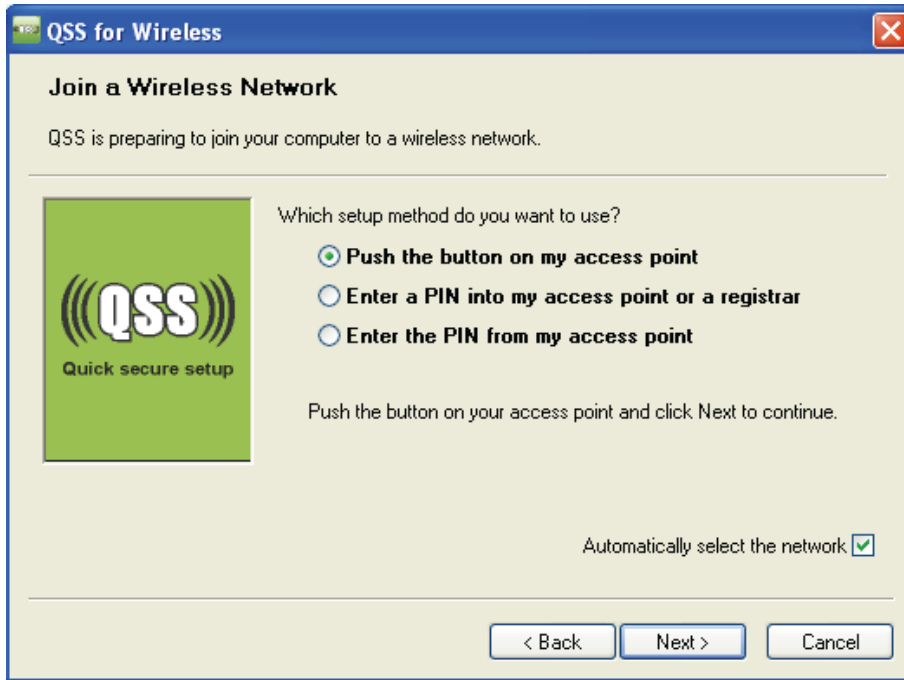


Figure 4-4 The QSS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.

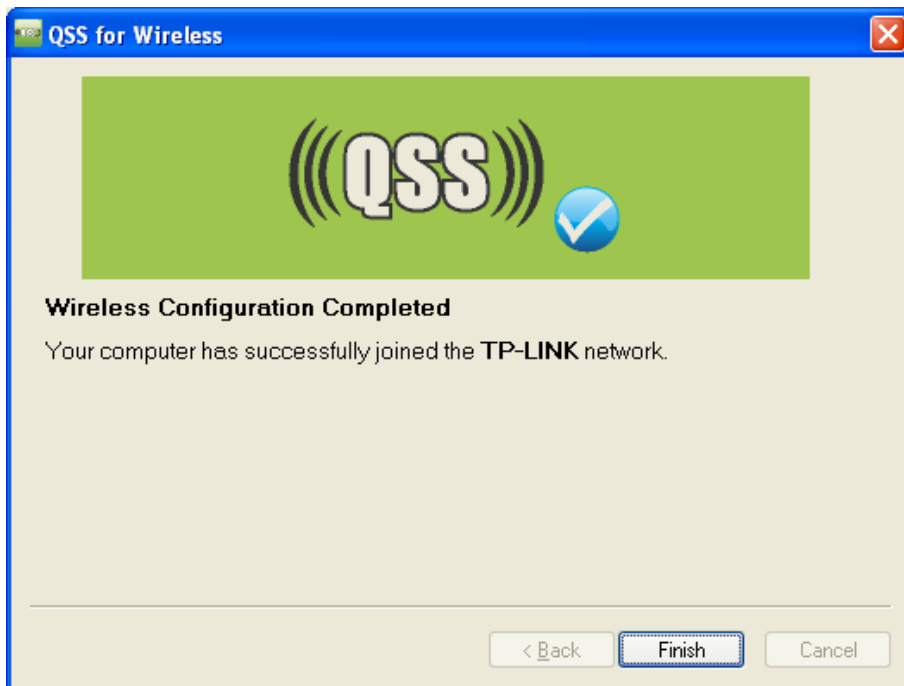


Figure 4-5 The QSS Configuration Screen of Wireless Adapter

**Method Two:** Enter the PIN into my AP

Step 1: Keep the QSS Status as **Enabled** and click the **Add device** button in Figure 4-2, then the following screen will appear.

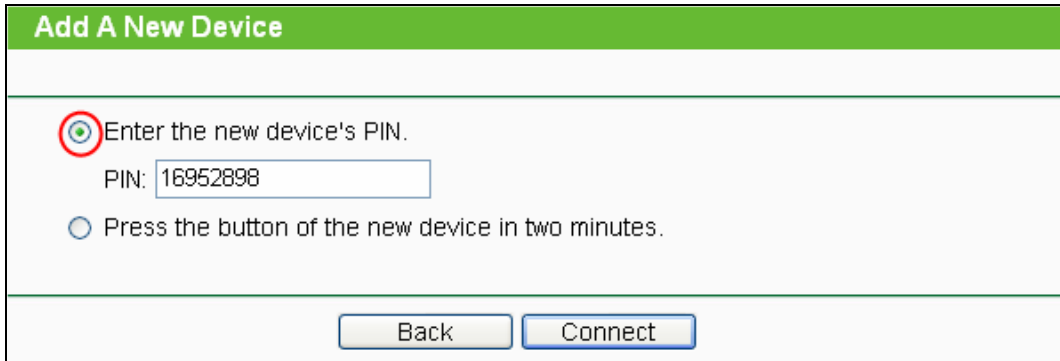


Figure 4-6

Step 2: Choose “**Enter the new device's PIN**” and enter the PIN code (take 16952898 for example) of the wireless adapter in the field after **PIN** as shown in the figure above. Then click **Connect**.

**Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen as shown in the following figure.

Step 3: For the configuration of the wireless adapter, please choose “**Enter a PIN into my access point or a registrar**” in the configuration utility of the QSS as below, and click **Next**.

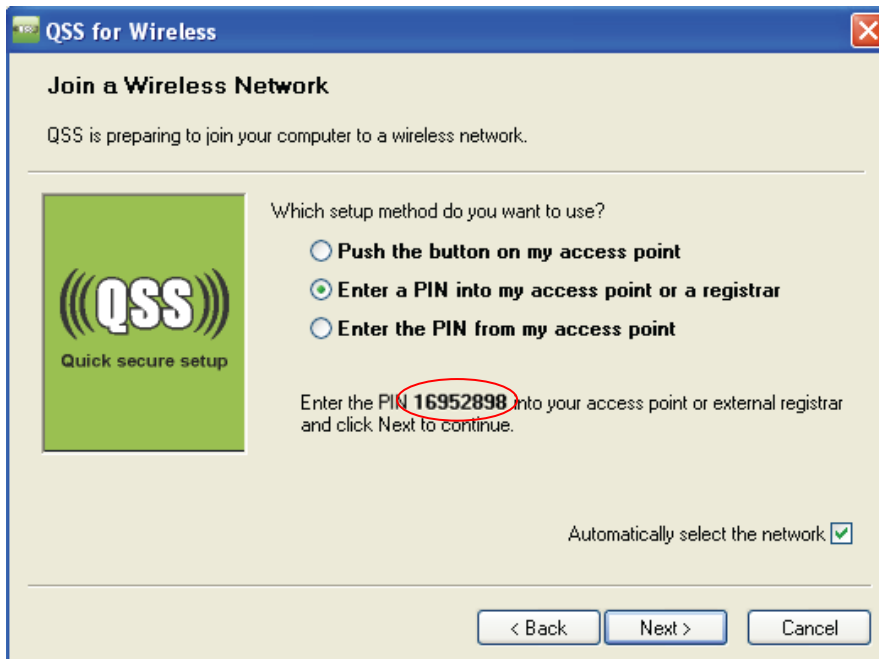


Figure 4-7 The QSS Configuration Screen of Wireless Adapter

**Note:**

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

**Method Three:** Enter the PIN from my AP

Step 1: Get the Current PIN code of the AP in Figure 4-2 (each AP has its unique PIN code. Here takes the PIN code 96980088 of this AP for example).

Step 2: For the configuration of the wireless adapter, please choose “**Enter a PIN from my access point**” in the configuration utility of the QSS as below, and enter the PIN code of the AP into the field after “**Access Point PIN**”. Then click **Next**.

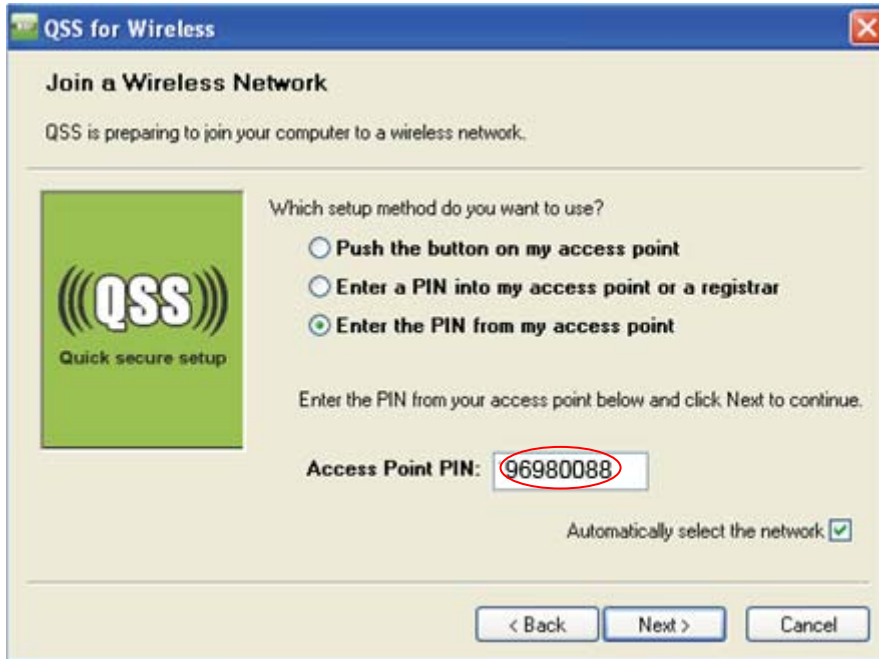


Figure 4-8 The QSS Configuration Screen of Wireless Adapter

**Note:**

The default PIN code of the AP can be found in its label or the QSS configuration screen as Figure 4-2.

You will see the following screen when the new device has successfully connected to the network.

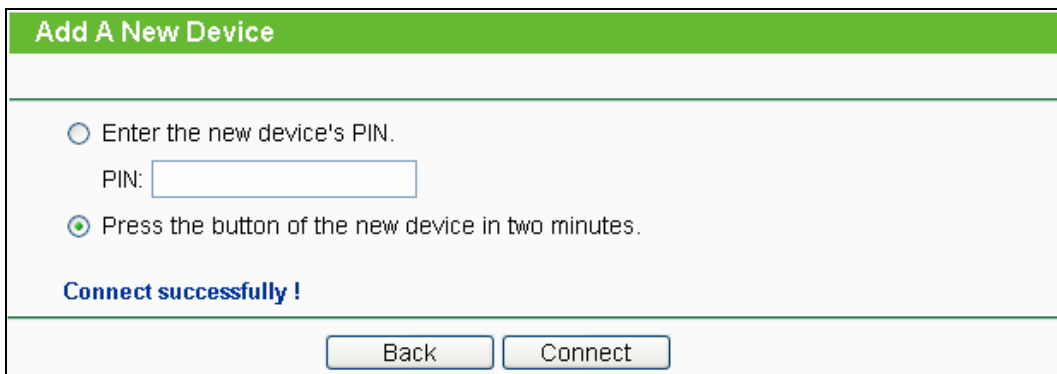


Figure 4-9

**Note:**

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

## 4.4 Network

The **Network** option allows you to customize your local network manually by changing the default settings of the AP.

Selecting **Network** will enable you to configure the IP parameters of Network on this page.

The screenshot shows the LAN configuration interface. At the top, there is a green header with the text 'LAN'. Below the header, the settings are as follows:

- MAC Address:** B0-48-7A-F1-A6-A7
- Type:** Static IP (selected from a dropdown menu)
- IP Address:** 192.168.0.254
- Subnet Mask:** 255.255.255.0 (selected from a dropdown menu)
- Gateway:** 0.0.0.0

At the bottom of the form, there is a 'Save' button.

Figure 4-10 Network

- **Type** - Select **Dynamic IP** to get IP address from DHCP server or select **Static IP** to configure IP address manually from the drop-down list.
- **IP Address** - Enter the IP address of your AP in dotted-decimal notation (factory default setting is 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **Gateway** - The gateway should be in the same subnet as your IP address.
- **MAC Address** - The physical address of the AP. The value can't be changed.

### Note:

1. If you change the IP Address, you must use the new IP Address to log in the AP.
2. If the new LAN IP Address you set is not in the same subnet with the IP Address pool of DHCP sever, the IP Address pool will not take effect until it is re-configured accordingly.

## 4.5 Wireless

The **Wireless** option, improving functionality and performance for wireless network, can help you make the AP an ideal solution for your wireless network. Here you can create a wireless local area network just through a few settings. Wireless Settings is used for the configuration of some basic parameters of the AP. Wireless Security provides three different security types to secure your data and thus provide greater security for your wireless network. MAC filtering allows you to control the access of wireless stations to the AP. Wireless Advanced allows you to configure some advanced parameters for the AP. Throughput Monitor helps to watch wireless throughput information. Wireless statistics enables you to get detailed information about the current connected wireless stations.

There are six submenus under the Wireless menu (shown in Figure 4-11): **Wireless Settings**,



**Wireless Security, Wireless MAC Filtering, Wireless Advanced, Throughput Monitor and Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

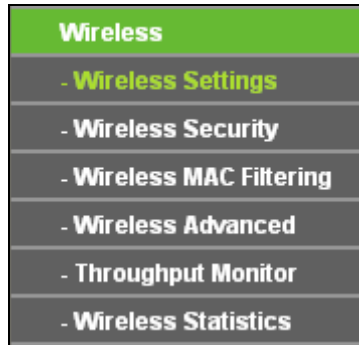


Figure 4-11 Wireless menu

### 4.5.1 Wireless Settings

Selecting **Wireless > Wireless Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 4-13). This page allows you to configure the wireless mode for your device. Six operation modes are supported here, including **Range Extender** and **Access Point**. The available setting options for each operation mode are different from those of the other.

- 1) **Range Extender:** In Range Extender mode, the AP with WDS disabled will relays data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range.

Figure 4-12 Wireless Settings in Range Extender mode

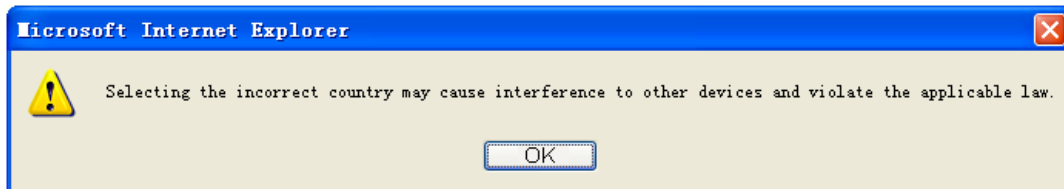
- **Operation Mode** - Two Operation Modes are supported, including: Access Point and Range Extender.
- **MAC of AP** - The MAC address of the desired AP. The AP client will connect to the desired AP according to MAC address.

**Note:**

1. In Range Extender mode, the wireless repeater relays signal between its stations and the root AP for greater wireless range. The MAC address of root AP can be automatically filled into corresponding box by clicking the **Survey** button and selecting the desired item.
  2. If you know the MAC address of the desired AP, you can also input it into the field "MAC of AP" manually.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

**Note:**

The default region is United States. When you select your local region from the pull-down list, the dialog shown in Figure appears below. Click **OK**.



Note Dialog

**Note:**

Restricted by local law regulations, version for North America does not have region selection option.

- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate** - Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio** - Select or deselect this check box to allow or deny wireless stations to access the device.

Click the **Survey** button to detect the MAC address of the desired AP you want to connect to.

**Note:**

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

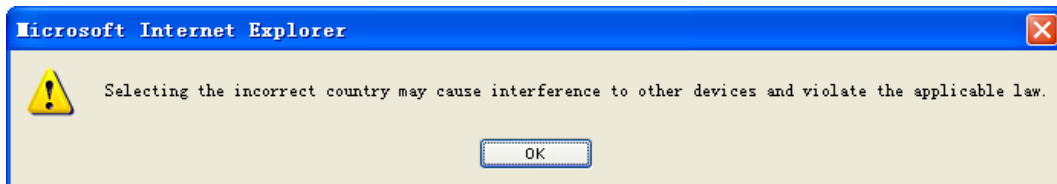
2) **Access Point:** This mode allows wireless stations to access this device.

Figure 4-13 Wireless Settings in Access Point mode

- **Operation Mode** - Two Operation Modes are supported, including: Access Point and Range Extender.
- **SSID** (Set Service Identifier) - Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-LINK\_XXXXXX (XXXXXX indicates the last unique six characters of each device’s MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

**Note:**

The default region is United States. When you select your local region from the pull-down list, the dialog shown in Figure appears below. Click **OK**.



**Note:**

Restricted by local law regulations, version for North America does not have region selection option.

- **Channel** - Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Mode** - Select the desired wireless mode. The options are:
  - **11b only** - Only 802.11b wireless stations can connect to the device.
  - **11g only** - Only 802.11g wireless stations can connect to the device.
  - **11n only** - Only 802.11n wireless stations can connect to the device.
  - **11bg mixed** - Both 802.11b and 802.11g wireless stations can connect to the device.
  - **11bgn mixed** - All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate** - Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio** - Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast** - Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

 **Note:**

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

#### 4.5.2 Wireless Security

Selecting **Wireless > Wireless Security** will enable you to configure wireless security for your wireless network to protect your data from intruders. The AP provides three security types: WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK. Wireless security can be set on the following screen shown as Figure 4-14. The security options are different for different operation mode.

## 1) Range Extender

The screenshot displays the 'Wireless Security' configuration interface. At the top, the 'Operation Mode' is set to 'Range Extender'. There are three radio button options for security: 'Disable Security' (selected), 'WEP', and 'WPA/WPA2 - Personal(Recommended)'. Under 'WEP', there are dropdown menus for 'Type' (Automatic) and 'WEP Key Format' (Hexadecimal). Below this is a table for 'WEP Key' configuration with four rows (Key 1 to Key 4). Each row has a 'Key Selected' radio button (Key 1 is selected), a 'WEP Key' text input field, and a 'Key Type' dropdown menu (all set to 'Disabled'). Under 'WPA/WPA2 - Personal(Recommended)', there are dropdown menus for 'Version' (Automatic(Recommended)) and 'Encryption' (Automatic(Recommended)), a 'PSK Password' text input field, and a 'Group Key Update Period' text input field set to '0' with a note '(in second, minimum is 30, 0 means no update)'. A 'Save' button is located at the bottom of the form.

Figure 4-14 Wireless Security – Range Extender

- **Operation Mode** - Shows the current operation mode.
- **Disable Security** - Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP** - Select 802.11 WEP security.
  - **Type** - You can select one of following types.
    - 1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
    - 2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
    - 3) **Open System** - Select 802.11 **Open System** authentication.
  - **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
- 1) For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
- 2) For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
- 3) For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

 **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA-PSK/ WPA2-PSK** - Select WPA based on pre-shared key.
  - **Version** - You can select one of following versions.
    - 1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
    - 2) **WPA-PSK** - Pre-shared key of WPA.
    - 3) **WPA2-PSK** - Pre-shared key of WPA2.
  - **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
  - **PSK Passphrase** - Enter a passphrase here.
  - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

 **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

## 2) Access Point

Wireless Security

Operation Mode: Access Point

**Disable Security**

**WEP**

Type:

WEP Key Format:

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

**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)

**WPA/WPA2 - Personal(Recommended)**

Version:

Encryption:

PSK Password:

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

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

Figure 4-15 Wireless Security - Access Point

- **Operation Mode** - Shows the current operation mode.
- **Disable Security** - Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP** - Select 802.11 WEP security.
  - **Type** - You can select one of following types.
    - 1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
    - 2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
    - 3) **Open System** - Select 802.11 **Open System** authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
  - 1) For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
  - 2) For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
  - 3) For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

 **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA/WPA2** - Select WPA/WPA2 based on Radius Server.
  - **Version** - You can select one of following versions.
    - 1) **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
    - 2) **WPA** - Wi-Fi Protected Access.
    - 3) **WPA2** - WPA version 2.
  - **Encryption** - You can select either **Automatic**, **TKIP** or **AES**.
  - **Radius Server IP** - Enter the IP address of the Radius Server.
  - **Radius Port** - Enter the port used by radius service.
  - **Radius Password** - Enter the password for the Radius Server.
  - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.
- **WPA-PSK/ WPA2-PSK** - Select WPA based on pre-shared key.
  - **Version** - You can select one of following versions.
    - 1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
    - 2) **WPA-PSK** - Pre-shared key of WPA.
    - 3) **WPA2-PSK** - Pre-shared key of WPA2.
  - **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
  - **PSK Passphrase** - Enter a passphrase here.



- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

**Note:**

You will be reminded to reboot the device after clicking the **Save** button.

### 4.5.3 Wireless MAC Filtering

Selecting **Wireless > Wireless MAC Filtering** will allow you to set up some filtering rules to control wireless stations accessing the device, which depend on the station’s MAC address on the following screen as shown Figure 4-16. This function is not available when the operation is set to Client. As the configuration is the same in each operation mode, here we just take the Access Point for example.

Figure 4-16 Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the device, which depend on the station's MAC addresses.

- **Operation Mode** - Shows the current operation mode.
- **Wireless MAC Filtering** - Click the **Enable** button to enable the Wireless MAC Address Filtering. The default setting is disabled.

To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The “Add or Modify Wireless MAC Address Filtering entry” page will appear, shown in Figure 4-17.

Add or Modify Wireless MAC Address Filtering entry	
MAC Address:	<input type="text"/>
Description:	<input type="text"/>
Status:	Enabled <input type="button" value="v"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 4-17 Add or Modify Wireless MAC Address Filtering entry

- **MAC Address** - Enter the wireless station's MAC address that you want to control.
- **Description** - Give a simple description of the wireless station.
- **Status** - Select a status for this entry, either **Enabled** or **Disabled**.

#### To set up an entry, follow these instructions:

First, you must decide whether the unspecified wireless stations can access the device or not. If you desire that the unspecified wireless stations can access the device, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**, otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

#### To add a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

#### To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

**For example:** If you desire that the wireless station A with MAC address 00-0A-EB-00-07-BE is able to access the device, while all other wireless stations cannot access the device, you should configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter Wireless Station A in the **Description** field and select **Enabled** in the **Status** pull-down list. Click the **Save** button.

The filtering rules that configured should be similar to the following list:

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	wireless station A	<a href="#">Modify</a> <a href="#">Delete</a>

**Note:**

If you enable the function and select the “**Deny the stations not specified by any enabled entries in the list to access**” for **Filtering Rules**, and there are not any enabled entries in the list, thus, no wireless stations can access the device.

#### 4.5.4 Wireless Advanced

Selecting **Wireless > Wireless Advanced** will allow you to do some advanced settings for the device in the following screen shown in Figure 4-18. As the configuration for each operation mode is almost the same, we take Range Extender mode for example here.

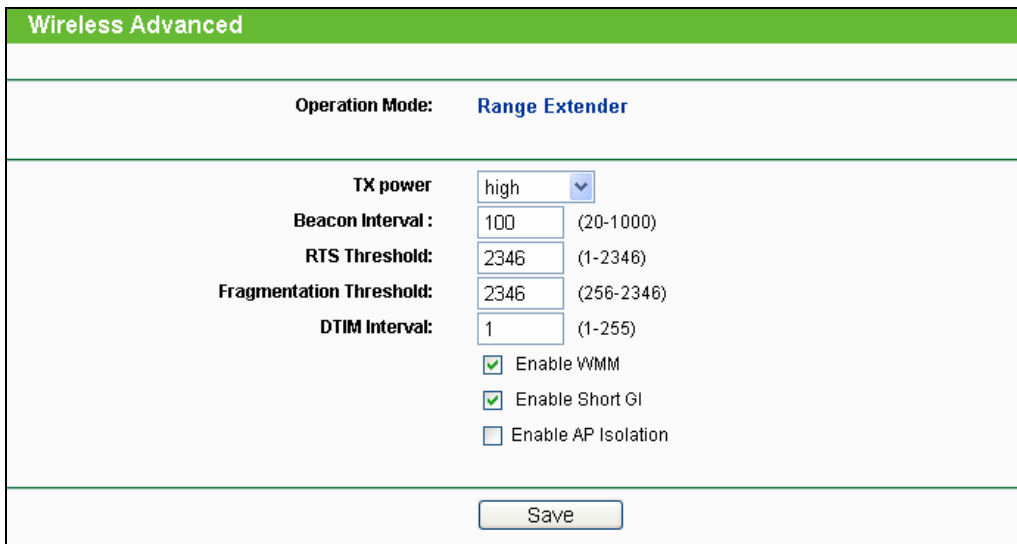


Figure 4-18 Wireless Advanced

- **Operation Mode** - Shows the current Operation Mode.
- **Tx Power** - Specifies the transmit power of the device. You can select **High**, **Middle** or **Low** which you would like. **High** is the default setting and is recommended.

- **Beacon Interval** - Specifies a value between 20-1000 milliseconds. The beacons are the packets sent by the device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold** - Specifies the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device 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 the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - Determines the interval of the Delivery Traffic Indication Message (DTIM). 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 enabled.
- **Enable Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - Isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.

#### 4.5.5 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 4-19.

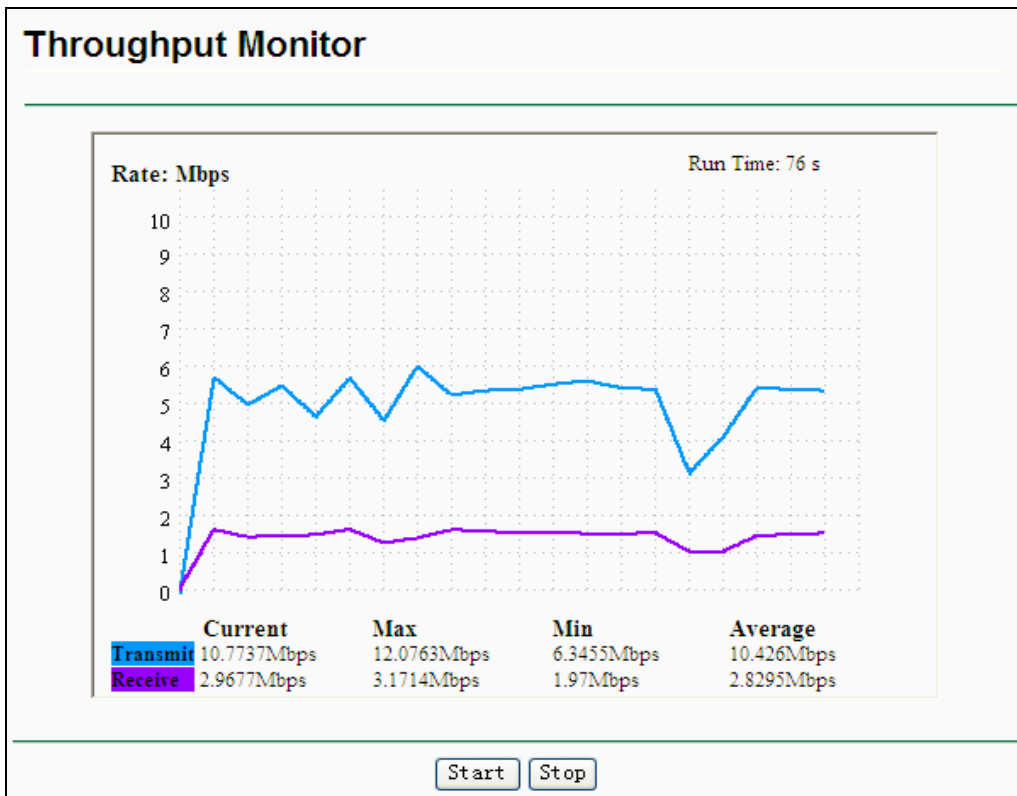


Figure 4-19 Throughput Monitor

- **Rate** - The Throughput unit.

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

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

#### 4.5.6 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 4-20.

Wireless Statistics				
Operation Mode: <b>Range Extender</b>				
Current Connected Wireless Stations numbers: <b>1</b> <input type="button" value="Refresh"/>				
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-1D-0F-01-06-18	AP-UP	0	0
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 4-20 Statistics of the device attached wireless stations

- **Operation Mode** - Shows the current operation mode
- **MAC Address** - Shows the connected wireless station's MAC address
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected
- **Received Packets** - packets received by the station
- **Sent Packets** - packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

 **Note:**

This page will be refreshed automatically every 5 seconds.

#### 4.6 DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the

need to manually assign new IP addresses.

There are three submenus under the DHCP menu (shown as Figure 4-21): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

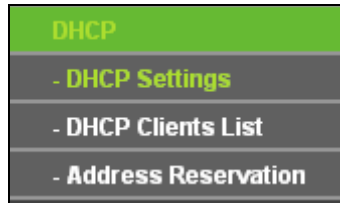


Figure 4-21 The DHCP menu

#### 4.6.1 DHCP Settings

Selecting **DHCP > DHCP Settings** will enable you to set up the AP as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server can be configured on the page (shown as Figure 4-22):

 A screenshot of a web configuration page titled 'DHCP Settings'. The page has a green header. Below the header, there are several configuration fields:
 

- DHCP Server:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Start IP Address:** Text input field containing '192.168.0.100'.
- End IP Address:** Text input field containing '192.168.0.199'.
- Address Lease Time:** Text input field containing '120', followed by the text 'minutes (1~2880 minutes, the default value is 120)'.
- Default Gateway:** Text input field containing '0.0.0.0', followed by '(optional)'.
- Default Domain:** Text input field, followed by '(optional)'.
- Primary DNS:** Text input field containing '0.0.0.0', followed by '(optional)'.
- Secondary DNS:** Text input field containing '0.0.0.0', followed by '(optional)'.

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

Figure 4-22 DHCP Settings

- **DHCP Server** - Selecting the radio button before **Disable/Enable** will disable/enable the DHCP server on your AP. The default setting is **Disable**. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first address in the IP Address pool. 192.168.0.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.0.199 is the default end IP address.
- **Address Lease Time** - Enter the amount of time for the PC to connect to the AP with its current assigned dynamic IP address. The time is measured in minutes. After the time is up, the PC will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

- **Default Gateway (optional)** - Enter the IP address of the gateway for your LAN. The factory default setting is 0.0.0.0.
- **Default Domain (optional)** - Enter the domain name of the your DHCP server. You can leave the field blank.
- **Primary DNS (optional)** - Enter the DNS IP address provided by your ISP. Consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.
- **Secondary DNS (optional)** - Enter the IP address of another DNS server if your ISP provides two DNS servers. The factory default setting is 0.0.0.0.

Click **Save** to save the changes.

 **Note:**

1. When the device is working on Dynamic IP mode, the DHCP Server function will be disabled.
2. To use the DHCP server function of the device, you should configure all computers in the LAN as "Obtain an IP Address automatically" mode. This function will not take effect until the device reboots.

### 4.6.2 DHCP Clients List

Selecting **DHCP > DHCP Clients List** will enable you to view the Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 4-23).

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Anthea	00-13-8F-AA-6D-77	192.168.0.100	01:59:29

Figure 4-23 DHCP Clients List

- **ID** - Here displays the index of the DHCP client.
- **Client Name** - Here displays the name of the DHCP client.
- **MAC Address** - Here displays the MAC address of the DHCP client.
- **Assigned IP** - Here displays the IP address that the AP has allocated to the DHCP client.
- **Lease Time** - Here displays the time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

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

### 4.6.3 Address Reservation

Selecting **DHCP > Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 4-24).

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-0A-EB-00-07-BE	192.168.0.101	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-22-33-55-58-01	192.168.0.55	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-24 Address Reservation

- **MAC Address** - Here displays the MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address** - Here displays the IP address that the AP is reserved.
- **Status** - Here shows whether the entry is enabled or not
- **Modify** - To modify or delete an existing entry.

#### To Reserve IP addresses:

1. Click the **Add New...** button to add a new Address Reservation entry.
2. Enter the MAC address in XX-XX-XX-XX-XX-XX format and IP address in dotted-decimal notation of the computer you wish to add.
3. Click **Save** when finished.

#### To modify A Reserved IP address:

1. Select the reserved address entry to your needs and click **Modify**. If you wish to delete the entry, click **Delete**.
2. Click **Save** to keep your changes.

#### To delete all Reserved IP addresses:

1. Click **Clear All**.

Click **Next** to go to the next page and Click **Previous** to return the previous page.

#### **Note:**

The changes won't take effect until the device reboots.

## 4.7 System Tools

**System Tools** option helps you to optimize the configuration of your device. SNMP can help you to manage the device locally or remotely with specified software. The diagnostic tools (Ping and Traceroute) allow you to check the connections of your network components. You can upgrade the AP to the latest version of firmware as well as backup or restore the AP's configuration files. Ping Watch Dog can help to continuously monitor a particular connection to a remote host. It's suggested that you change the default password to a more secure one because it controls access



to the device’s web-based management page. Besides, you can find out what happened to the system in System Log.

There are nine submenus under the **System Tools** menu (shown as Figure 4-25): **SNMP**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Reboot**, **Password**, and **System Log**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-25 The System Tools menu

#### 4.7.1 SNMP

Selecting **System Tools > SNMP** to enable this function will allow the network management station to retrieve statistics and status from the SNMP agent in this device. Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol, used to refer to a collection of specifications for network management that include the protocol itself. To use this function, select Enable and enter the following parameters in Figure 4-26.

The image shows the "SNMP Settings" configuration page. At the top is a green header with the text "SNMP Settings". Below the header, there are several configuration options:

- SNMP Agent:** Two radio buttons are present: "Enable" (unselected) and "Disable" (selected).
- SysContact:** An empty text input field.
- SysName:** An empty text input field.
- SysLocation:** An empty text input field.
- Get Community:** A text input field containing the value "public".
- Get Source:** A text input field containing the value "0.0.0.0".
- Set Community:** A text input field containing the value "private".
- Set Source:** A text input field containing the value "0.0.0.0".

At the bottom of the form is a "Save" button.

Figure 4-26 SNMP Settings

- **SNMP Agent** - Select the radio button before **Enable** will enable this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Select the radio button before **Disable** will disable this function. The default setting is **Disable**.
- **SysContact** - The textual identification of the contact person for this managed node.
- **SysName** - An administratively-assigned name for this managed node.
- **SysLocation** - The physical location of this node.

 **Note:**

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

- **Get Community** - Enter the community name that allows Read-Only access to the Device's SNMP information. The community name can be considered a group password. The default setting is **public**.
- **Get Source** - Get source defines the IP address or subnet for management systems that can read information from this 'get' community device.
- **Set Community** - Enter the community name that allows Read/Write access to the Device's SNMP information. The community name can be considered a group password. The default setting is **private**.
- **Set Source** - Set source defines the IP address or subnet for management systems that can control this 'set' community device.

 **Note:**

A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

Click the **Save** button to save your settings.

## 4.7.2 Diagnostic

Selecting **System Tools > Diagnostic** allow you to check the connections of your network components on the screen shown in Figure 4-27.

The screenshot shows a web interface titled "Diagnostic Tools". Under the heading "Diagnostic Parameters", there are two radio buttons: "Ping" (selected) and "Traceroute". Below these are several input fields: "IP Address" (empty), "Ping Count" (4, range 1-50), "Ping Packet Size" (64, range 4-1472 Bytes), "Ping Timeout" (800, range 100-2000 Milliseconds), and "Traceroute Max TTL" (20, range 1-30). Under the heading "Diagnostic Results", a dashed box contains the text "The AP is ready.". At the bottom of the interface is a "Start" button.

Figure 4-27 Diagnostic

**Diagnostic Tools** - Click the radio button to select one diagnostic tool

- Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway by using the Internet Control Message Protocol (ICMP) protocol's mandatory Echo Request datagram to elicit an ICMP Echo Response from a host or gateway. You can use ping to test both numeric IP address or domain name. If pinging the IP address is successful, but pinging 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.
- Traceroute** - This diagnostic tool determines the path taken to a given host by sending Internet Control Message Protocol (ICMP) Echo Request messages with varying Time to Live (TTL) values to the destination. Each gateway along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the gateway is expected to return an ICMP Time Exceeded response to your device. Traceroute determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 20 by default and can be specified in the field "Traceroute Max TTL". The path is determined by examining the ICMP Time Exceeded messages returned by intermediate gateways and

the Echo Reply message returned by the destination. However, some gateways do not return Time Exceeded messages for packets with expired TTL values and are invisible to the traceroute tool. In this case, a row of asterisks (\*) is displayed for that hop.

**IP Address** - Enter the IP Address (such as 202.108.22.5) of the PC whose connection you wish to diagnose.

**Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.

**Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.

**Ping Timeout** - Specifies the time to wait for a response in milliseconds. The default is 800.

**Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

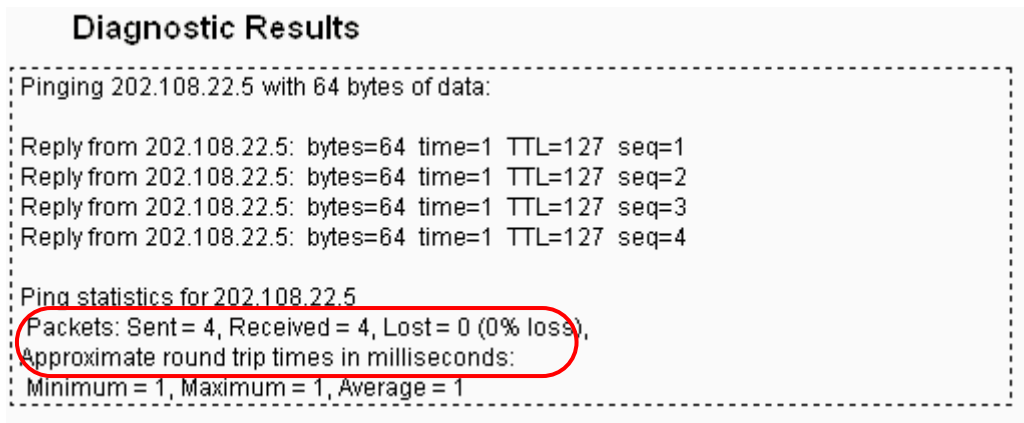


Figure 4-28 Diagnostic Results

**Note:**

1. Only one user can use this tool at one time.
2. Options “Number of Pings”, “Ping Size” and “Ping Timeout” are only available for Ping function. Option “Tracert Hops” is available only for Tracert function.

### 4.7.3 Ping Watch Dog

Selecting **System Tools > Ping Watch Dog** allows you to continuously monitor the particular connection between the device to a remote host. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

Figure 4-29 Ping Watch Dog Utility

- **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 device is restarted.
- **Fail Count** - Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Submit** button to make your settings in operation.

#### 4.7.4 Firmware Upgrade

Selecting **System Tools > Firmware Upgrade** allows you to upgrade the latest version of firmware for the device on the screen shown in Figure 4-30.

Figure 4-30 Firmware Upgrade

New firmware versions are posted at <http://www.tp-link.com> and can be downloaded for free.

- **Firmware Version** - Here displays the current firmware version.
- **Hardware Version** - Here displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

**Note:**

1. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the device itself, you can try to upgrade the firmware.
2. Before upgrading the device's firmware, you should write down some of your customized settings to avoid losing important configuration settings of device.

**To upgrade the device's firmware, follow these instructions:**

1. Download a more recent firmware upgrade file from the TP-LINK website (<http://www.tp-link.com>).
2. Enter the path name or click **Browse...** to select the downloaded file on the computer into the **File** blank.
3. Click **Upgrade**.

**Note:**

Do not turn off the device or press the **Reset** button while the firmware is being upgraded. The device will reboot after the Upgrading has been finished.

#### 4.7.5 Factory Defaults

Selecting **System Tools > Factory Default** allows you to restore the factory default settings for the device on the screen shown in Figure 4-31.

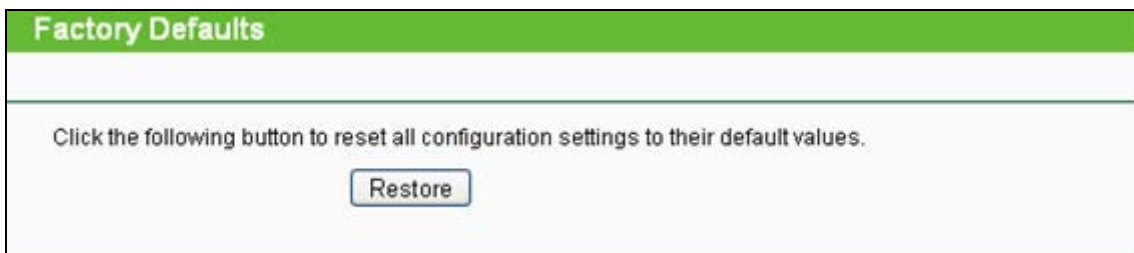


Figure 4-31 Restore Factory Defaults

Click **Restore** to reset all configuration settings to their default values.

- Default **User Name**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.0.254
- Default **Subnet Mask**: 255.255.255.0

**Note:**

Any settings you have saved will be lost when the default settings are restored.

#### 4.7.6 Backup & Restore

Selecting **System Tools > Backup & Restore** allows you to save all configuration settings to your local computer as a file or restore the device's configuration on the screen shown in Figure 4-32.

Figure 4-32 Save or Restore the Configuration

Click **Backup** to save all configuration settings to your local computer as a file.

**To restore the device's configuration, follow these instructions:**

- Click **Browse...** to find the configuration file which you want to restore.
- Click **Restore** to update the configuration with the file whose path is the one you have input or selected in the blank.

**Note:**

1. The current configuration will be covered with the uploading configuration file.
2. Wrong process will lead the device unmanaged.
3. The restoring process lasts for 20 seconds and restart automatically. Do not power off the device during the process to avoid any damage.

#### 4.7.7 Reboot

Selecting **System Tools > Reboot** allows you to reboot the device on the screen shown in Figure 4-33.

Figure 4-33 Reboot the device

Click the **Reboot** button to reboot the device.

Some settings of the device will take effect only after rebooting, which include:

- Change LAN IP Address (System will reboot automatically).
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the device (system will reboot automatically).
- Restore the device's settings to factory defaults (system will reboot automatically).
- Update the configuration with a file (system will reboot automatically).

### 4.7.8 Password

Selecting **System Tools > Password** allows you to change the factory default user name and password of the device on the screen shown in Figure 4-34.

Figure 4-34 Password

It is strongly recommended that you change the factory default user name and password of the device. All users who try to access the device's web-based management page or Quick Setup will be prompted for the device's user name and password.

**Note:**

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click **Save** when finished.

Click **Clear All** to clear all.

### 4.7.9 System Log

Selecting **System Tools > System Log** allows you to query the Logs of the device on the screen shown in Figure 4-35.

Index	Time	Type	Level	Log Content
1	1st day 00:00:02	OTHER	INFO	System started



Figure 4-35 System Log

The device can keep logs of all traffic. You can query the logs to find what happened to the device.

- **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.

Click the **Refresh** button to show the latest log list..

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

Click the **Clear Log** button to delete all the logs from the system permanently, not just from the page.

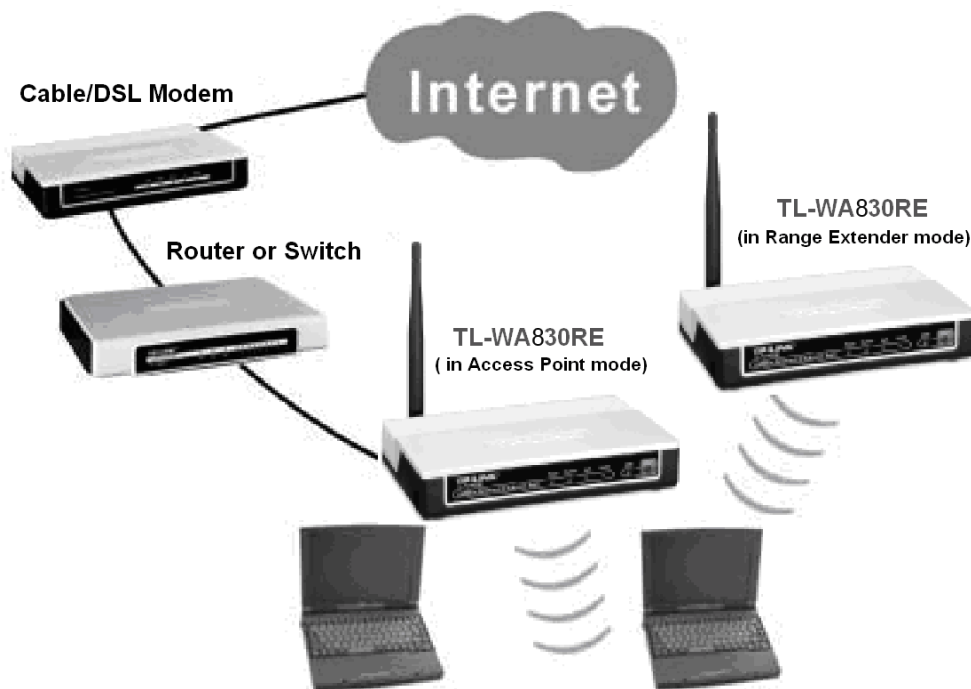
Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

## Appendix A: Application Example

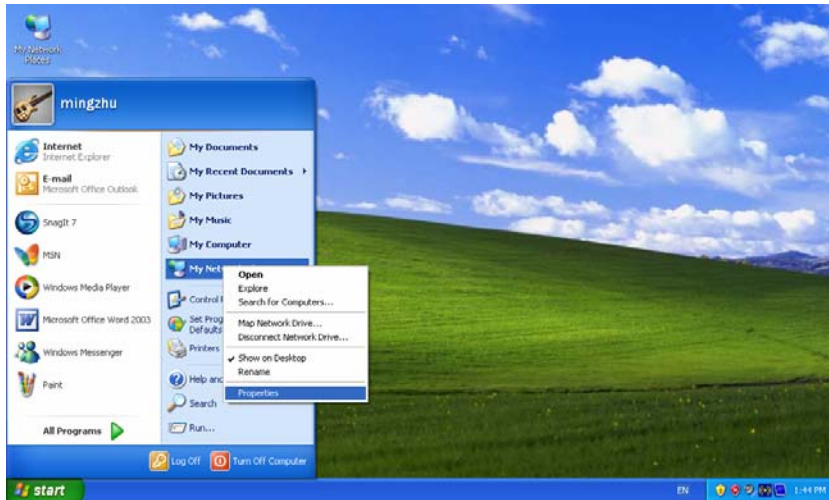
The TL-WA830RE relays signal between its stations and the root AP for greater wireless range. It allows you to connect the device with a Router around without any cable.

Providing that you want to connect your computer equipped with wireless adapter to a wired network wirelessly, you can take the following instructions.

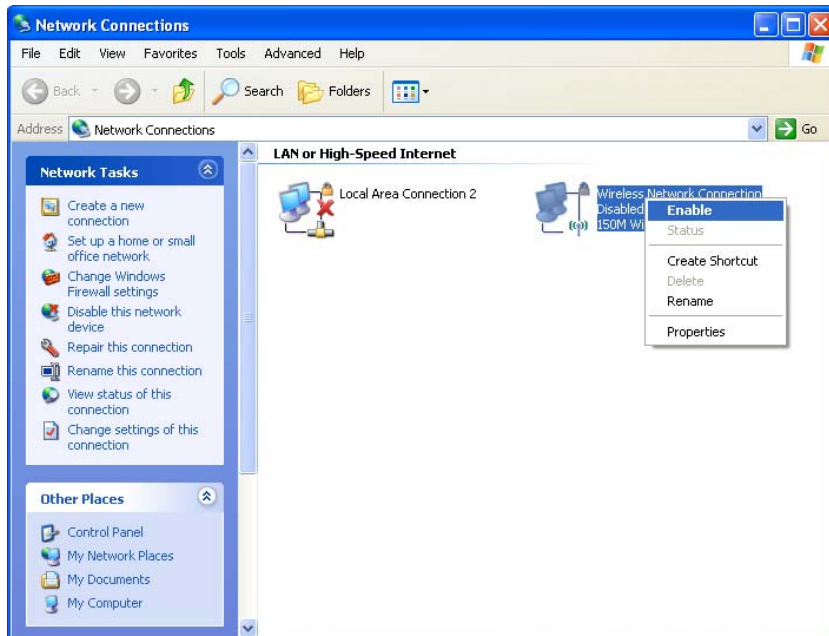
1. Configure the Range Extender via a wired connection.
  - 1) Connect your Range Extender to your PC with an Ethernet cable.
  - 2) Configure the IP address for your PC to communicate with the Range Extender referring to [3.1 Configure the PC](#).
  - 3) Log on to the web-based management page. Configure your Range Extender in the **Access Point** mode and check the **Enable SSID Broadcast** box referring to [4.5.1 Wireless Settings](#).
  - 4) View the **Wireless > Basic Settings** page and keep the SSID of the AP in mind. (Here we choose TP-LINK as the SSID for example.) You are suggested to change the SSID and secure your wireless network referring to [4.5.1 Wireless Settings](#) and [4.5.2 Wireless Security](#).
  - 5) Remove the Ethernet cable between the Range Extender and your PC.
2. Connect your Range Extender to the LAN port on the Router with an Ethernet cable.



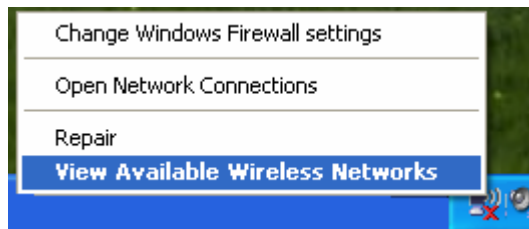
3. Configure your PC to connect to the network wirelessly.
  - 1) Click **Start** (in the lower left corner of the PC's screen), right-click **My Network Connections** and choose **Properties**.



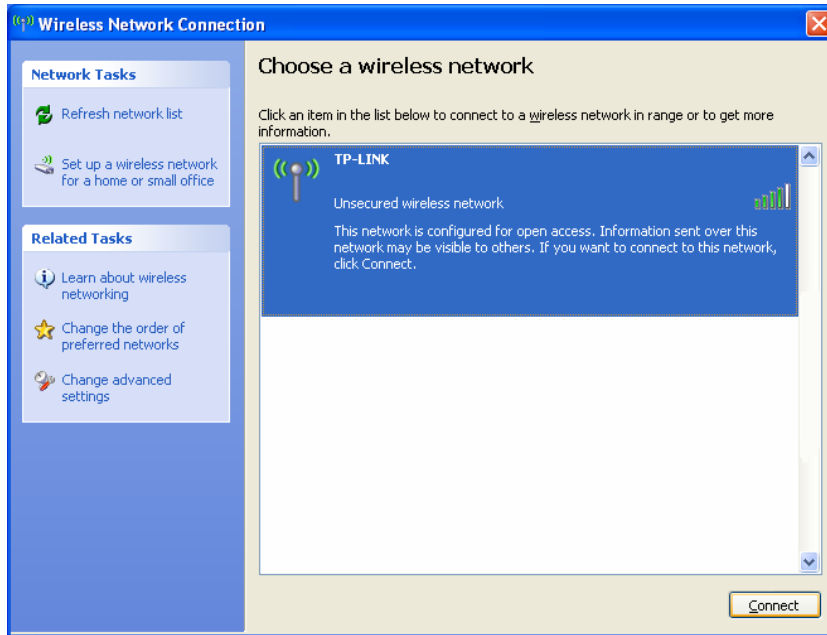
- 2) On the **My Network Connections** window, right-click **Wireless Network** and choose **Enable** to enable wireless network function.



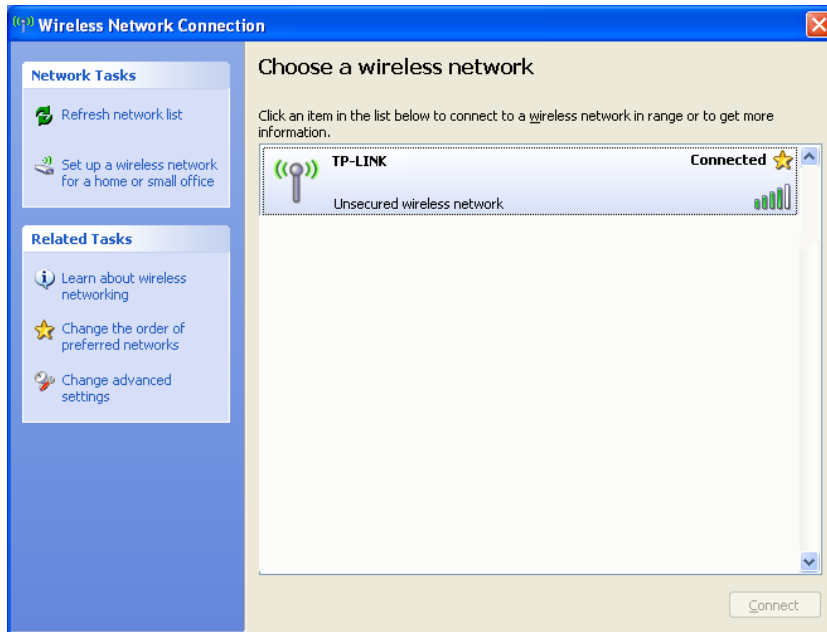
- 3) Right-click the wireless connection icon “” on the screen of the PC and then select **View Available Wireless Networks**.



- 4) Highlight the SSID of the Range Extender (Here is TP-LINK) and click **Connect** to add to the network.



5) Then the following page will display, which indicates you have been successfully added to the network wirelessly.



## Appendix B: Factory Defaults

Item	Default Value
<b>Common Default Settings</b>	
Username	admin
Password	admin
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
<b>Wireless</b>	
SSID	TP-LINK_XXXXXX
Wireless Security	Disable
Wireless MAC Address Filtering	Disable
<b>DHCP</b>	
DHCP Server	Disable
Start IP Address	192.168.0.100
End IP Address	192.168.0.199
Address Lease Time	120 minutes (Range:1 ~ 2880 minutes)
Default Gateway (optional)	0.0.0.0
Primary DNS (optional)	0.0.0.0
Secondary DNS (optional)	0.0.0.0

 **Note:**

The default SSID is TP-LINK\_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive.

## Appendix C: Troubleshooting

### 1. No LEDs are lit on the access point.

It takes a few seconds for the Power LED to light up. Wait a minute and check the status of Power LED. If there the LED is still off, check the following items.

- 1) Make sure the power cord is connected to the Access Point.
- 2) Make sure the power adapter is connected to a functioning electrical outlet and the switch of the electrical outlet is on.
- 3) Make sure you are using the correct TP-LINK power adapter provided with your Access Point.

### 2. The LAN LED is not lit.

There is a hardware connection problem. Check the following items.

- 1) Make sure the cable connectors are securely plugged in at the Access Point and the network device (hub, switch, or Router).
- 2) Make sure the connected device is turned on.
- 3) Make sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

### 3. I can not access the AP with a wireless capable computer.

There is a configuration problem. Check the following items.

- 1) You may not have the computer with the wireless adapter restarted to make TCP/IP changes take effect. Restart the computer.
- 2) The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check if TCP/IP is set up properly for that network. The usual setting for Windows is "Obtain an IP address automatically" in Network Properties.
- 3) The Access Point's default values may not work with your network. Check to see if the access point's default configuration conflicts the configuration of other devices in your network.

## Appendix D: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11n, 802.11b and 802.11g, TCP/IP, DHCP
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n: up to 300Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11b: 11/5.5/2/1M (Automatic)
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	270M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	4dBi
Physical and Environment	
Working Temperature	0°C~40°C (32°F~104°F)
Working Humidity	10% ~ 90% RH, Non-condensing
Storage Temperature	-40°C~70°C(-40°F~158°F)
Storage Humidity	5% ~ 95% RH, Non-condensing

## Appendix E: Glossary

- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **Access Point (AP)** - A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.
- **DNS (Domain Name System)** – An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **SSID - A Service Set Identification** is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** –A trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- **WPA (Wi-Fi Protected Access)** - WPA is a security technology for wireless networks that



improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP. One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use. This is similar to 802.1x support and requires a RADIUS server in order to implement. The Wi-Fi Alliance will call this, WPA-Enterprise. One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short - this provides an authentication alternative to an expensive RADIUS server. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. The Wi-Fi Alliance will call this, WPA-Personal.