TP-LINK®

User Guide

TL-WA701ND

150Mbps Wireless Lite N Access Point

Rev: 2.0.0
1910010249

COPYRIGHT & TRADEMARKS

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.

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

CE1588ⓘ

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.

TP-LINK TP-LINK TECHNOLOGIES CO., LTD

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **150Mbps Wireless Lite N Access Point**

Model No.: **TL-WA701ND**

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 V1.3.2:2008

EN 61000-3-2:2006

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

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

Person is responsible for marking this declaration:

Yang Hongliang

Product Manager of International Business

CONTENTS

Package Contents

The following items should be found in your package:

- One TL-WA701ND 150Mbps Wireless Lite N Access Point
- One DC power Adapter for TL-WA701ND 150Mbps Wireless Lite N Access Point
- One Power Injector
- Quick Installation Guide
- One Resource CD, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1 Introduction

Thank you for choosing the TL-WA701ND 150Mbps Wireless Lite N Access Point.

1.1 Product Overview

This device provides connectivity between Ethernet wired networks and radio-equipped wireless devices.

It is an easy, web-based setup for installation and management. Even though you may not be familiar with the device, this guide will make configuring the device easy. Before installing the device, please look through this guide to get to know all the device's functions.

1.2 Main Features

- Make use of IEEE 802.11n* wireless technology to provide a wireless data rate of up to 150Mbpsbps.
- Provides 64/128/152-bit WEP encryption security
- Provides WPA/WPA2 and WPA-PSK/WPA2-PSK authentication and TKIP/AES encryption security
- Built-in DHCP server supporting dynamic IP address distributing
- Supports MAC address filtering
- Supports multiple operating modes (Access Point, Multi-SSID, Client, Repeater, Universal Repeater, Bridge with AP)
- Supports TCP/IP, DHCP
- Supports Traffic statistics
- Supports firmware upgrade
- Supports Remote and Web management

☞ **Note:**

"*" This device leverages some 802.11n features to provide improved performance and coverage compared to 802.11a/g devices, and fully interoperates with 802.11n products if they are Wi-Fi CERTIFIED, but it does not conform to all of the requirements in the IEEE specification and is not classified as "n" in the Wi-Fi CERTIFIED program.

1.3 Conventions

The AP or TL-WA701ND, or device mentioned in this User guide stands for TL-WA701ND 150Mbps Wireless Lite N Access Point 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 2 Hardware Installation

2.1 The Front Panel

The front panel of the TL-WA701ND consists of several LED indicators, which is designed to indicate connections. View from left to right, Table 2-1 describes the LEDs on the front panel of the AP.

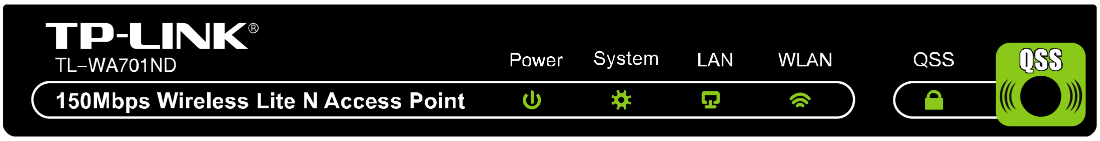


Figure 2-1

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
QSS	Slow Flash	A wireless device is connecting to the network by QSS function. This process will last in the first 2 minutes.
	On	A wireless device has been successfully added to the network by QSS function.
	Quick Flash	A wireless device failed to be added to the network by QSS function.

Table 2-1

2.2 The Back Panel

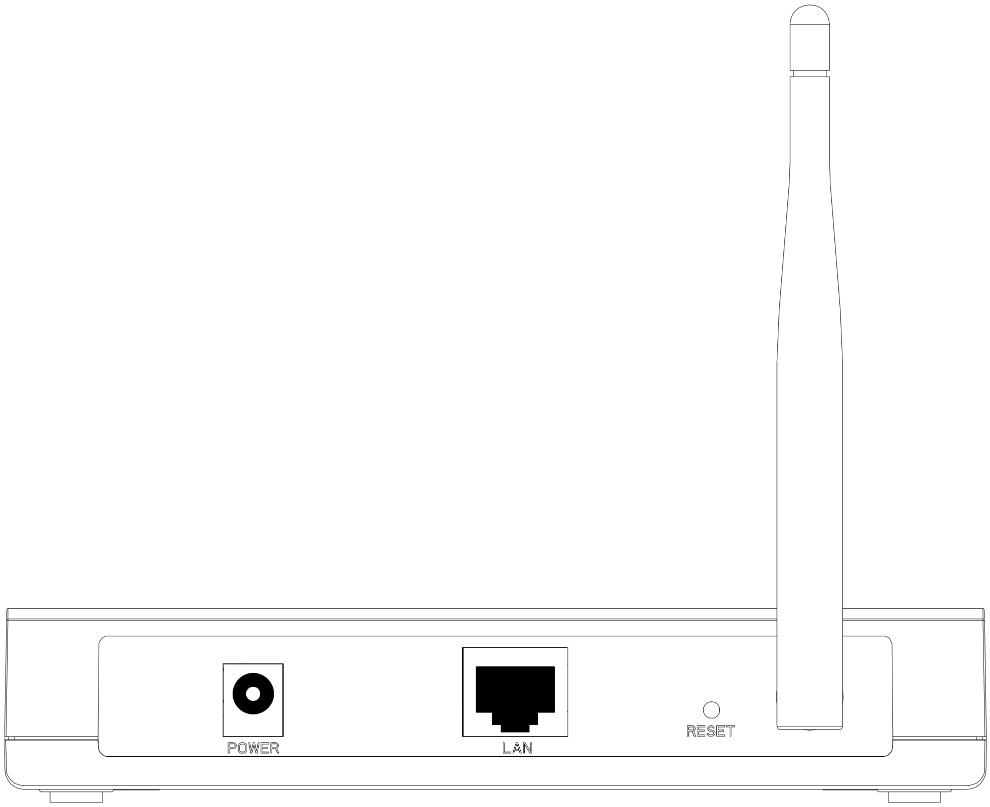


Figure 2-2

- Wireless antenna
- Factory Default **Reset** button

There are two ways to reset the device's factory defaults:

- Use the **Factory Defaults** function on "**System Tools** → **Factory Defaults**" page in the AP's Web-based Utility.
- Use the Factory Default **Reset** button: 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.

☞ **Note:**

Ensure the device is powered on before it restarts completely.

- One LAN 10/100Mbps RJ45 port for connecting the device to hub or switch.
- Power socket: only use the power adapter supplied with the TL-WA701ND 150Mbps Wireless Lite N Access Point, use of a different adapter may result in product damage.

2.3 System Requirements

- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
- 802.11n, 802.11g or 802.11b-compliant devices, such as the TL-WN721N Wireless Adapter

2.4 Installation Environment Requirements

- Place the AP in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the AP
- Operating Temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

2.5 Connecting the Device

Figure 2-3 is an example of an infrastructure network incorporating the TL-WA701ND. An Infrastructure network contains an access point or a wireless router. For a typical connection of the device, please do the following:

1. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office). Consult with your Cable or DSL provider for proper installation of the modem.
2. Connect the Cable or DSL modem to a Router. Quickly install the router.
3. Locate an optimum location for the device. The best place is usually near the center of the area in which your PC(s) will wirelessly connect. The place must accord with the Installation Environment Requirements.
4. Adjust the direction of the antenna. Normally, upright is a good direction.
5. Connect the Ethernet Broadband Router to the TL-WA701ND Access Point. Power on the Access Point.
6. If you are connecting a desktop PC or laptop to your network, install the TP-LINK Wireless Adapter on the PC.

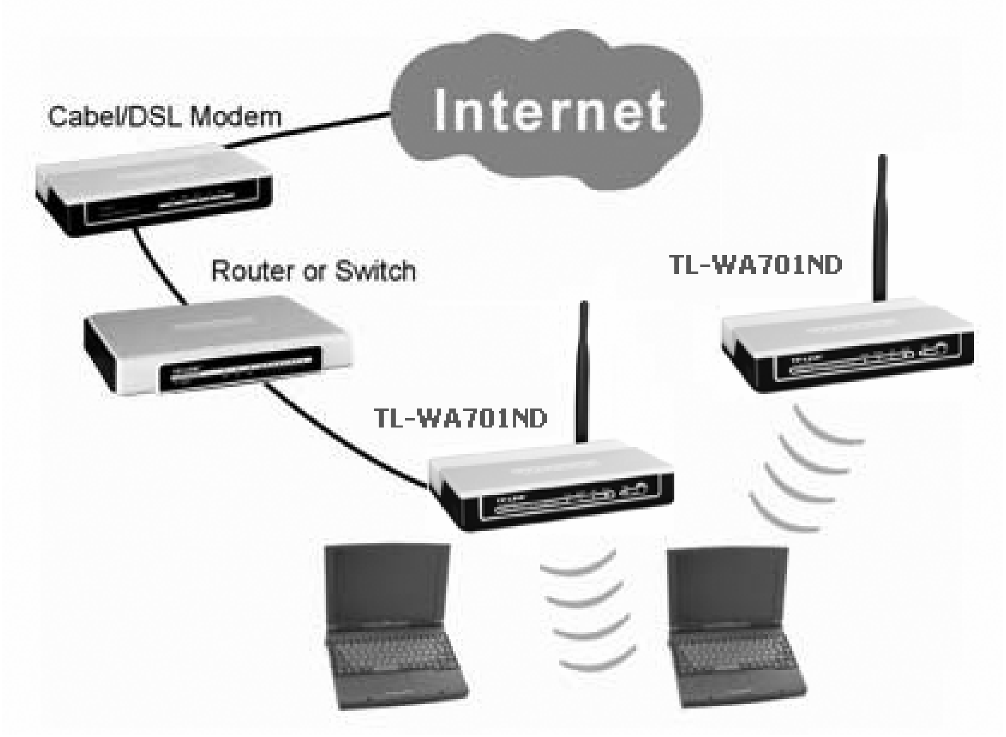


Figure 2-3 The Example of Infrastructure Network Incorporating the TL-WA701ND

2.6 Configure PC

After connecting the TL-WA701ND AP into your network, you should configure it. The default IP address of the TL-WA701ND 150Mbps Wireless Lite N Access Point is 192.168.1.254, and the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

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

1. From the **Start** menu on your desktop, go to **Settings**, and then click on Network Connections.

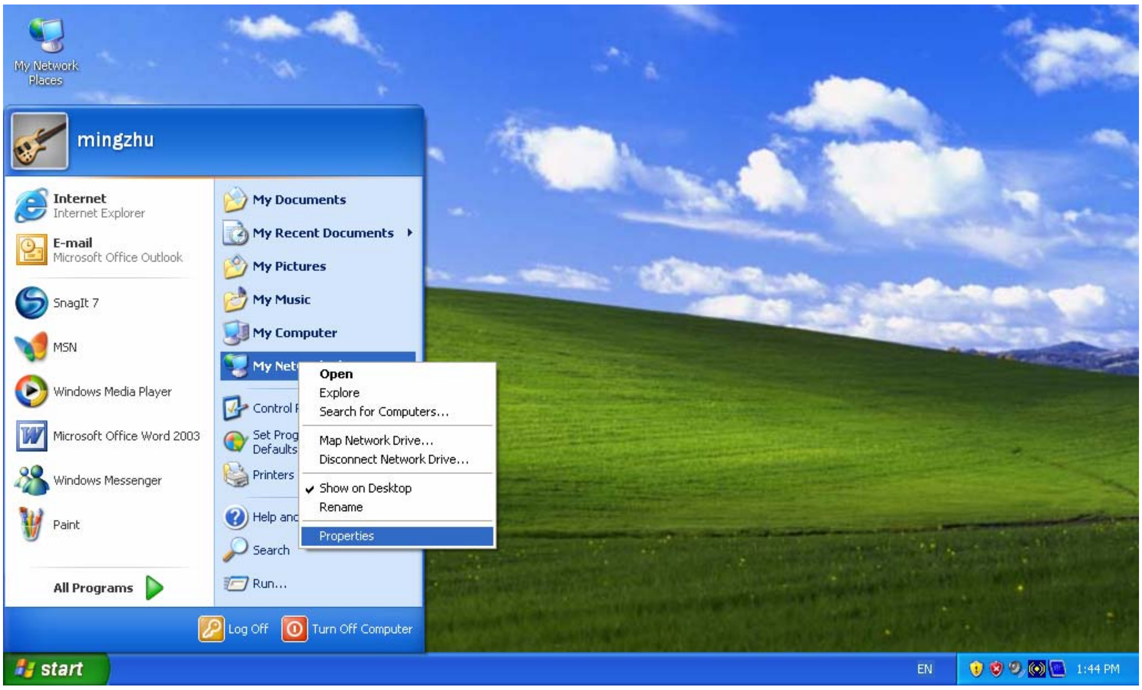


Figure 2-4

2. In the **Network Connections** window, right-click on LAN (Local Area Connection), then click Properties.

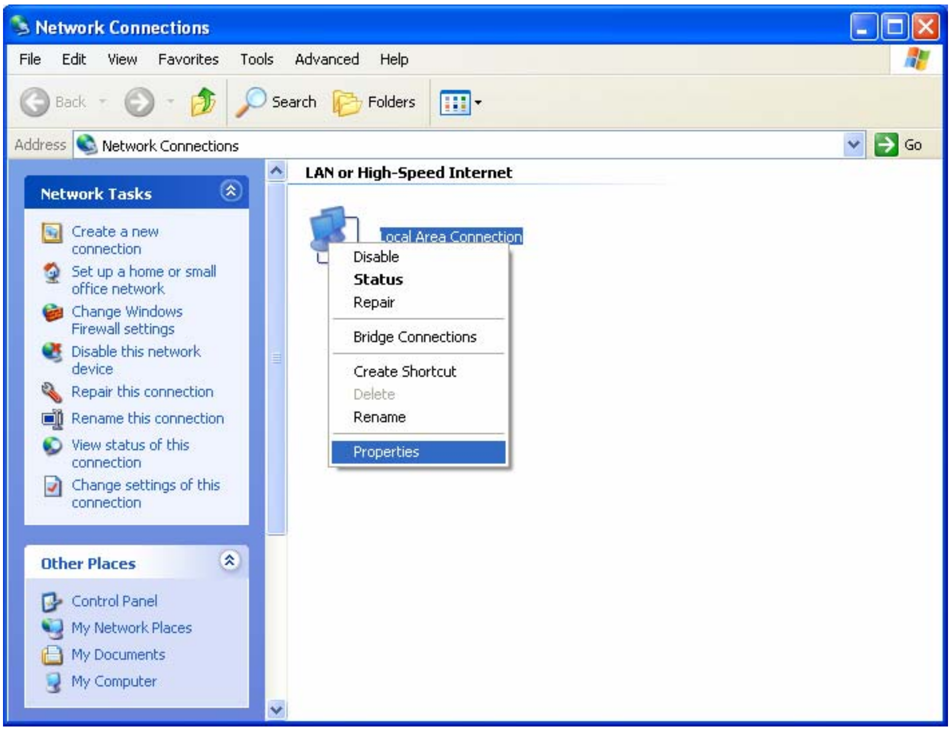
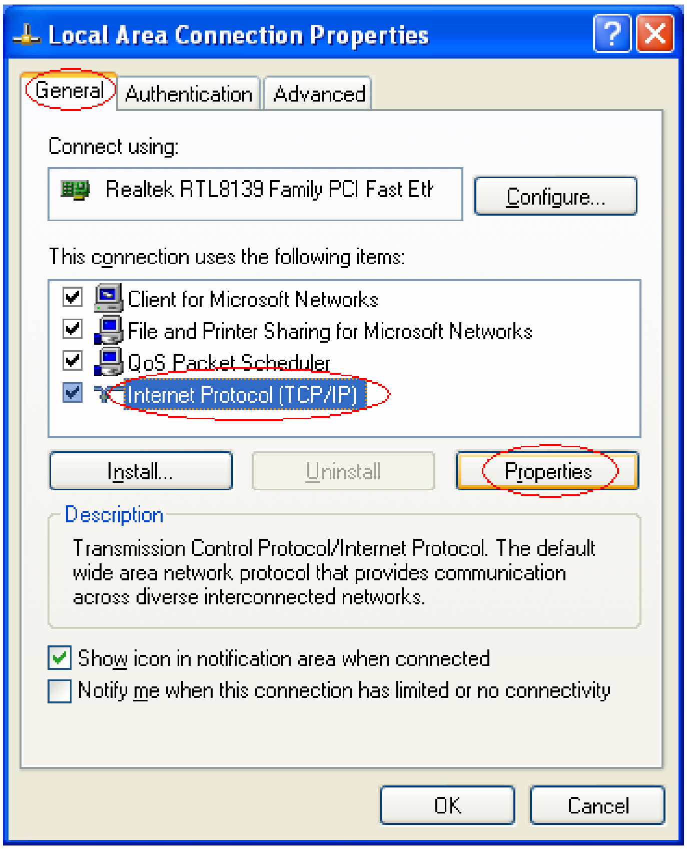


Figure 2-5

3. In the **General** tab of **Internet Protocol (TCP/IP) Properties** menu, highlight Internet Protocol (TCP/IP) under "This connection uses the following items:" by clicking on it once. Click on the Properties button.


Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

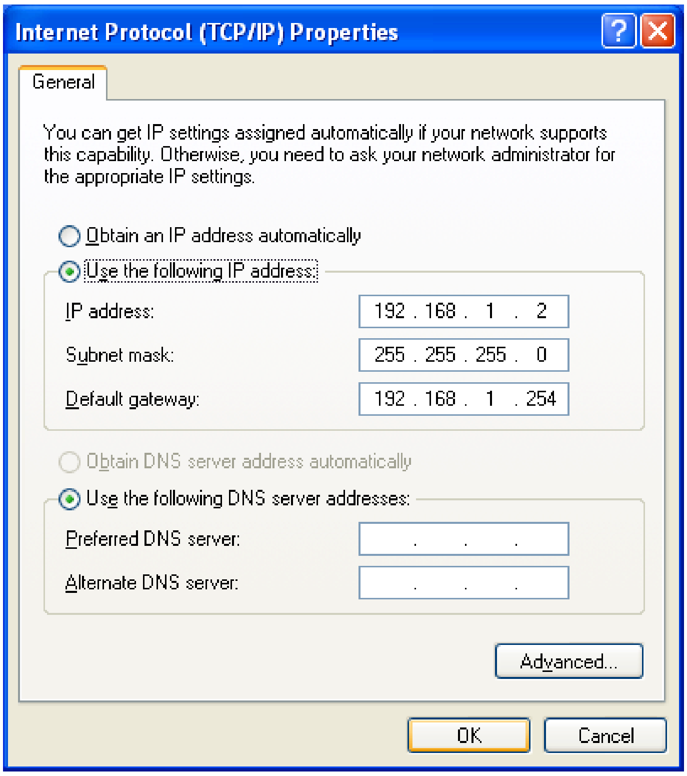
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
□ Notify me when this connection has limited or no connectivity

Figure 2-6

4. Configure the IP address manually. Click **OK**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

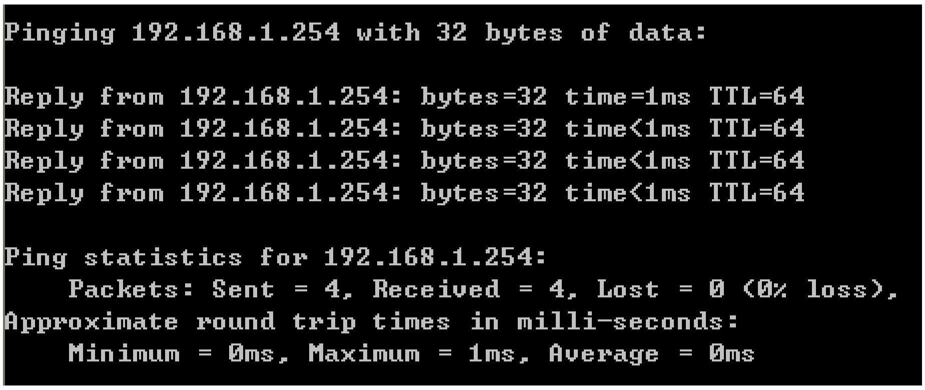
Figure 2-7

1) Open TCP/IP Properties of the LAN card in your PC, enter the IP address as 192.168.1.* (* is any value between 1 to 253, Subnet mask is 255.255.255.0, Gateway is 192.168.1.254, DNS address is the value provided by ISP).

2) Now, you can run the Ping command in the command prompt to verify the network connection between your PC and the AP. The following example is in Windows XP Operating System.

3) Open a command prompt. From the Start menu on your desktop, select run tab, type **cmd** in the field, and type *ping 192.168.1.254* on the screen that appears, and then press Enter.

If the result displayed is similar to that shown in Figure below, the connection between your PC and the AP has been established.



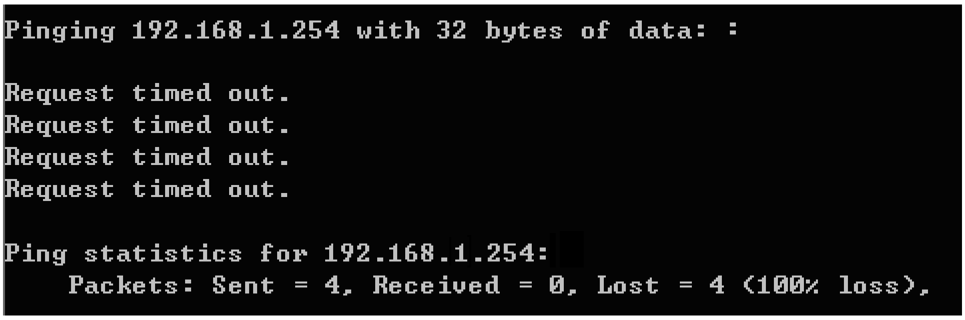
```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 2-8

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



```
Pinging 192.168.1.254 with 32 bytes of data: :

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 2-9

Please check it following these steps:

☞ **Note:**

If the connection between your PC and the AP is correct?

The LED of LAN port which you link to on the device and LED on your PC's adapter should be lit.

If the TCP/IP configuration for your PC is correct?

If the AP's IP address is 192.168.1.254, your PC's IP address must be within the range of 192.168.1.1 ~ 192.168.1.253.

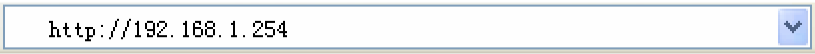
Chapter 3 Software Configuration

This User Guide recommends using the “Quick Installation Guide” for first-time installation, For advanced users, if you want to know more about this device and make use of its functions adequately, you need to read this chapter and configure advanced settings through the Web-based Utility.

3.1 Login

The TL-WA701ND 150Mbps Wireless Lite N Access Point is easy to configure and manage With a Web-based (Internet Explorer or Netscape® Navigator) utility. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

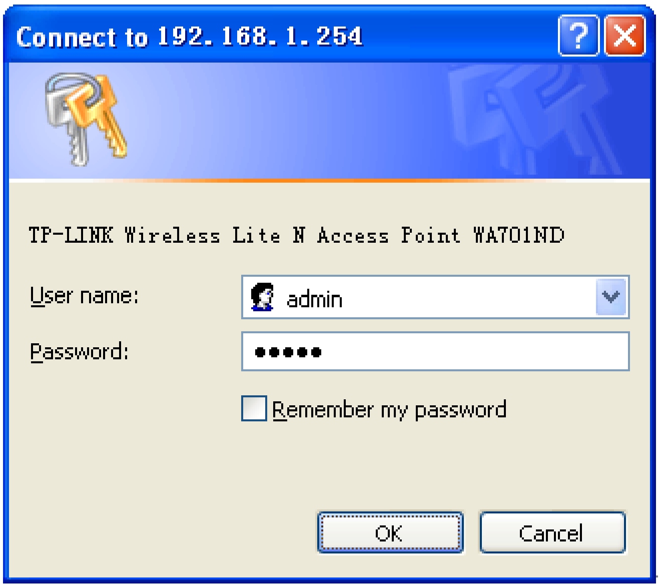
Connect to the AP by typing *http://192.168.1.254* in the address field of web browser.



http://192.168.1.254

Figure 3-1 Login to the AP

After a moment, a login window will appear similar to that shown in Figure 3-2. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Connect to 192.168.1.254

TP-LINK Wireless Lite N Access Point WA701ND

User name: admin

Password: ●●●●●

Figure 3-2 Login Windows

☞ **Note:**

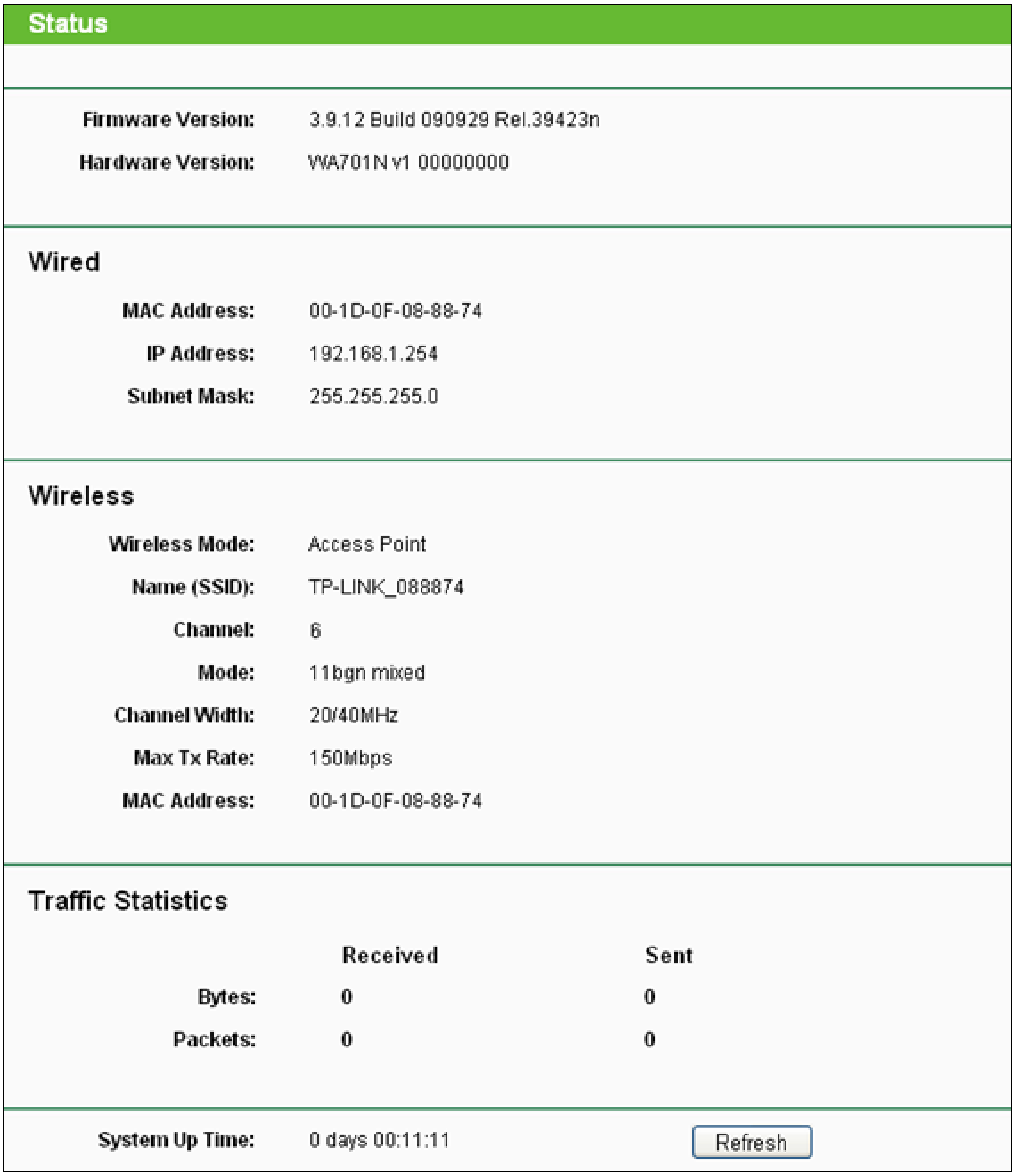
If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

After your successful login, you can configure and manage the AP. There are six main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. The six main menus are: **Status**, **QSS**, **Network**, **Wireless**, **DHCP and System Tools.** On the right of the web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

There are the detailed explanations for each web page's key functions below.

3.2 Status

The Status page displays the device's current status and configuration. All information is read-only.



Status

Firmware Version: 3.9.12 Build 090929 Rel.39423n

Hardware Version: WA701N v1 00000000

Wired

MAC Address: 00-1D-0F-08-88-74

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Wireless

Wireless Mode: Access Point

Name (SSID): TP-LINK_088874

Channel: 6

Mode: 11bgn mixed

Channel Width: 20/40MHz

Max Tx Rate: 150Mbps

MAC Address: 00-1D-0F-08-88-74

Traffic Statistics

	Received	Sent
Bytes:	0	0
Packets:	0	0

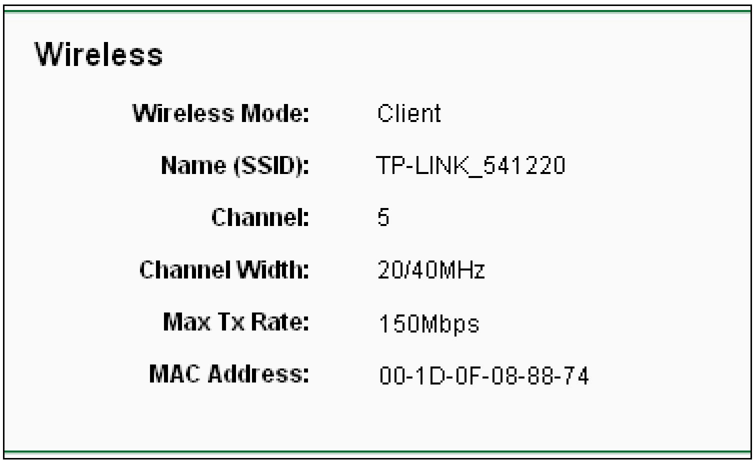
System Up Time: 0 days 00:11:11

Figure 3-3 Device Status

- **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 **Operating Mode, SSID, Channel, Mode,** and **MAC Address.**
- **Traffic Statistics -** This field displays the device's traffic statistics.
- **System Up Time -** The time of the device running from it's powered on or reset.

☞ **Note:**

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

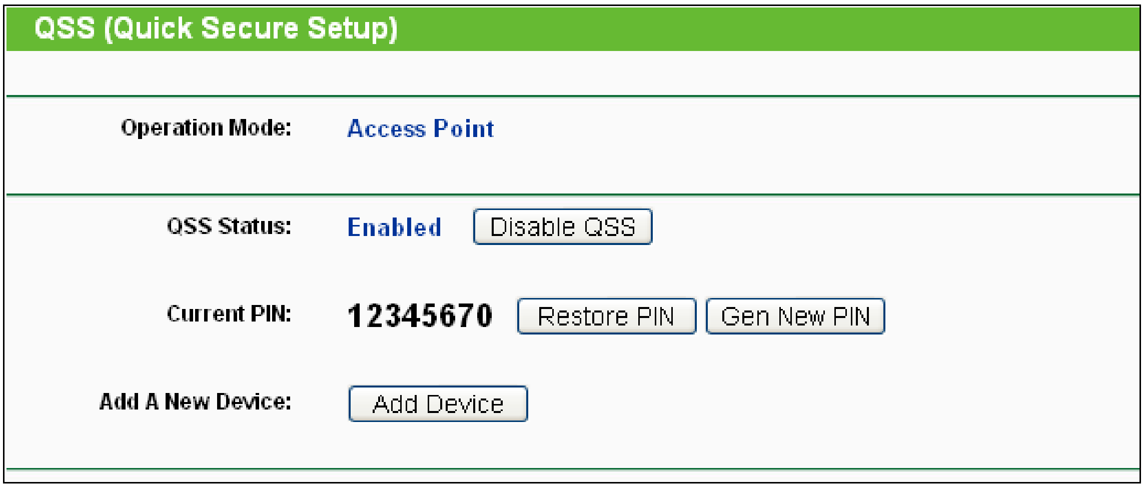


Wireless

Wireless Mode:	Client
Name (SSID):	TP-LINK_541220
Channel:	5
Channel Width:	20/40MHz
Max Tx Rate:	150Mbps
MAC Address:	00-1D-0F-08-88-74

3.3 QSS

This section will guide you to add a new wireless device to an existing network quickly by **QSS (Quick Secure Setup)** function. The QSS function is only available when the Operation Mode is set to Access Point and Multi-SSID. Here we take the Access Point mode for example. Choose menu "**QSS**", you will see the next screen (shown in Figure 3-4).



QSS (Quick Secure Setup)

Operation Mode: Access Point

QSS Status: Enabled

Current PIN: 12345670

Add A New Device:

Figure 3-4 QSS

- **QSS Status -** 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.

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.

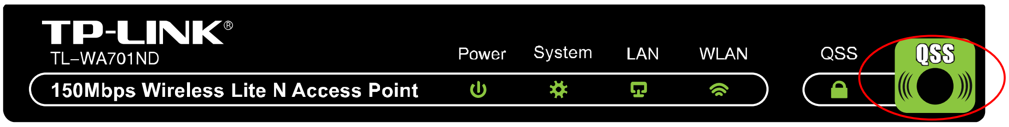
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

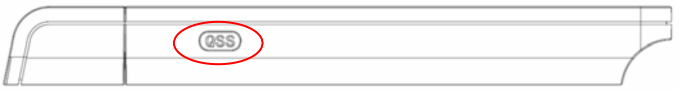
If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

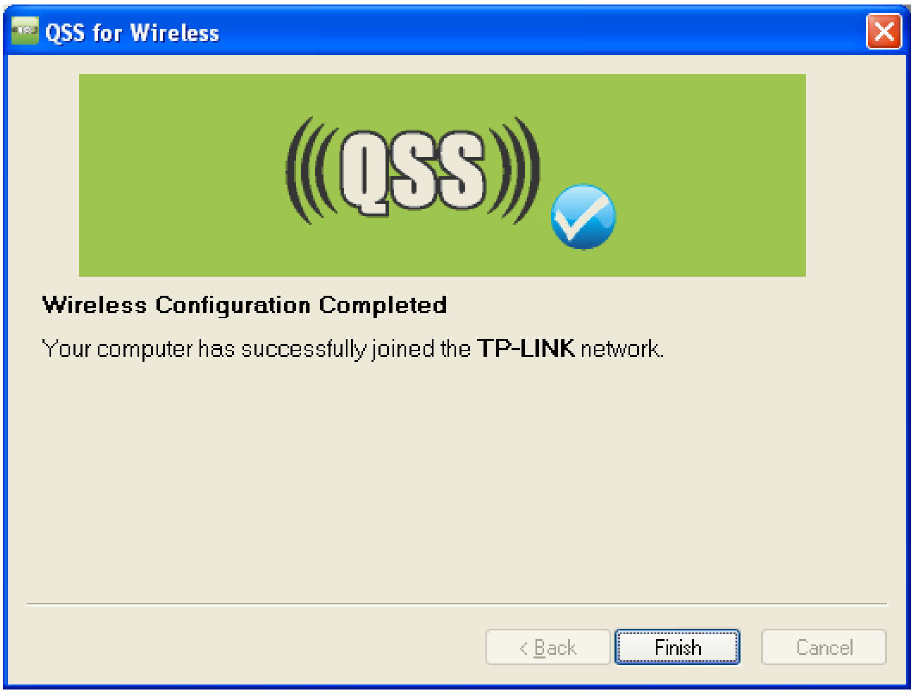
Step 1: Press the QSS button on the front panel of the device.



Step 2: Press and hold the QSS button of the adapter directly for 2 or 3 seconds.



Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



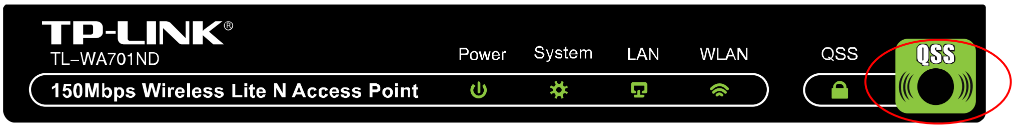
Wireless Configuration Completed

Your computer has successfully joined the TP-LINK network.

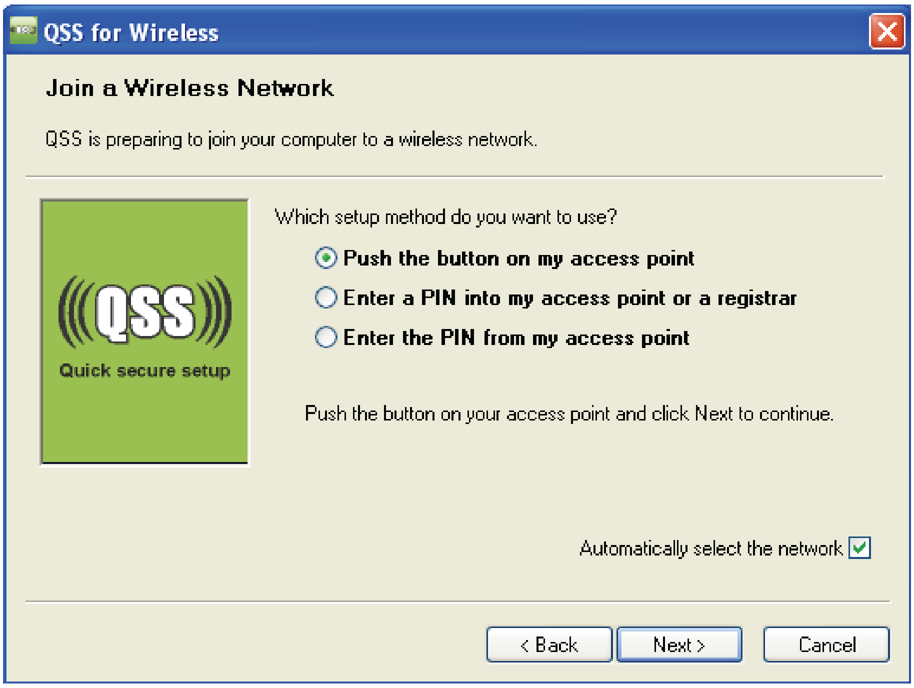
The QSS Configuration Screen of Wireless Adapter

Method Two:

Step 1: Press the QSS button on the front panel of the device.



Step 2: 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**.



Join a Wireless Network

QSS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

● Push the button on my access point

○ Enter a PIN into my access point or a registrar

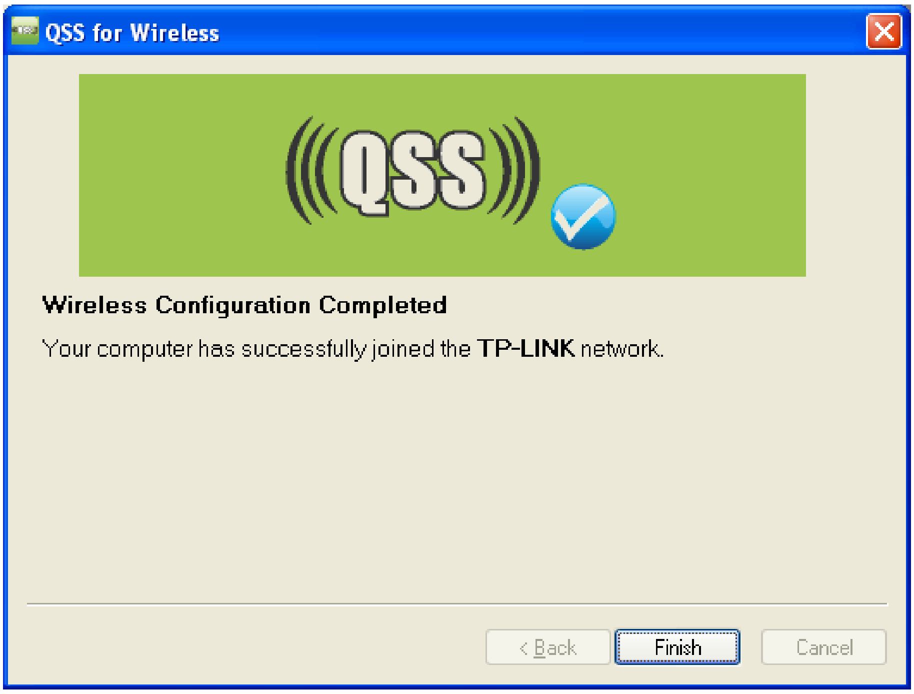
○ Enter the PIN from my access point

Push the button on your access point and click Next to continue.

Automatically select the network ☑

The QSS Configuration Screen of Wireless Adapter

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



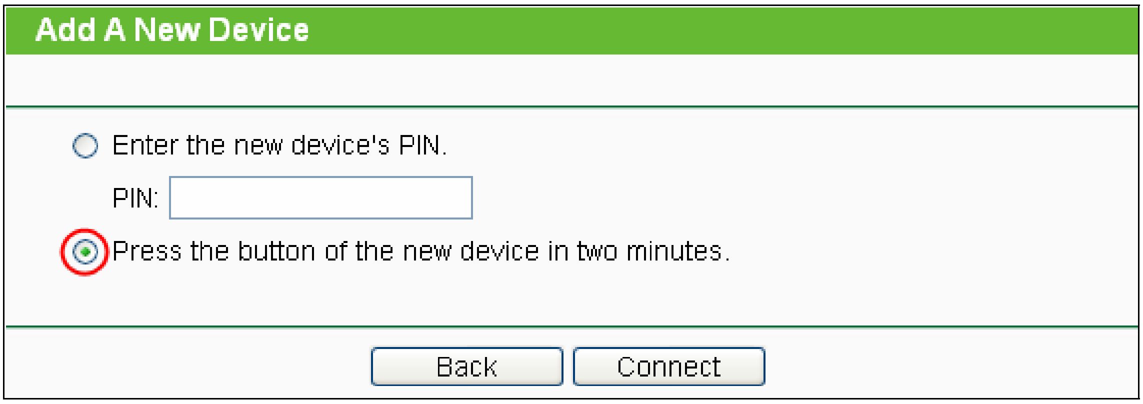
Wireless Configuration Completed

Your computer has successfully joined the **TP-LINK** network.

The QSS Configuration Screen of Wireless Adapter

Method Three:

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 3-4, then the following screen will appear.



Add A New Device

○ Enter the new device's PIN.

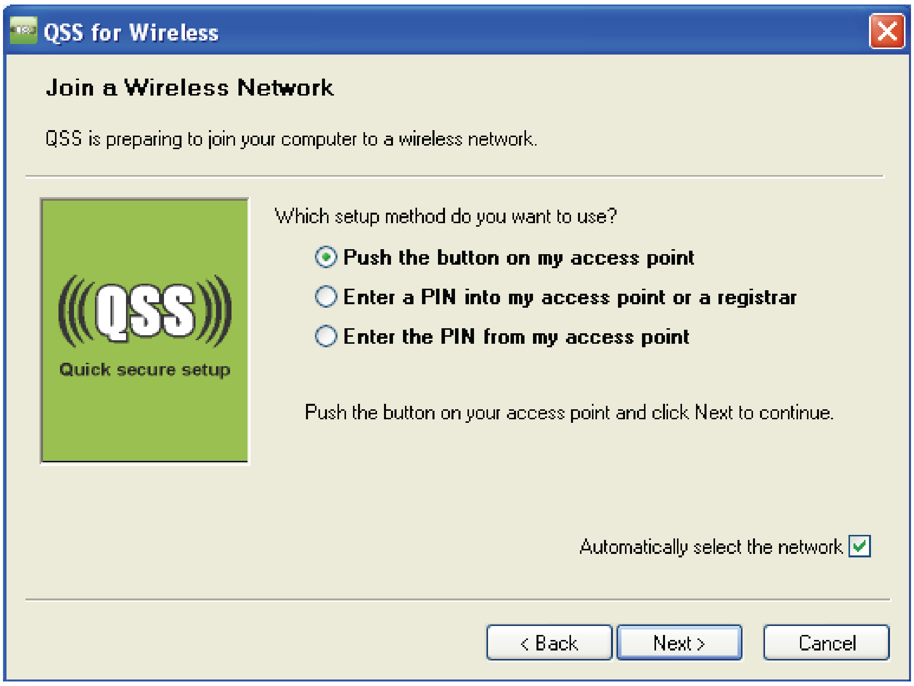
PIN:

● Press the button of the new device in two minutes.

Figure 3-5 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**.



QSS for Wireless

Join a Wireless Network

QSS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

● Push the button on my access point

○ Enter a PIN into my access point or a registrar

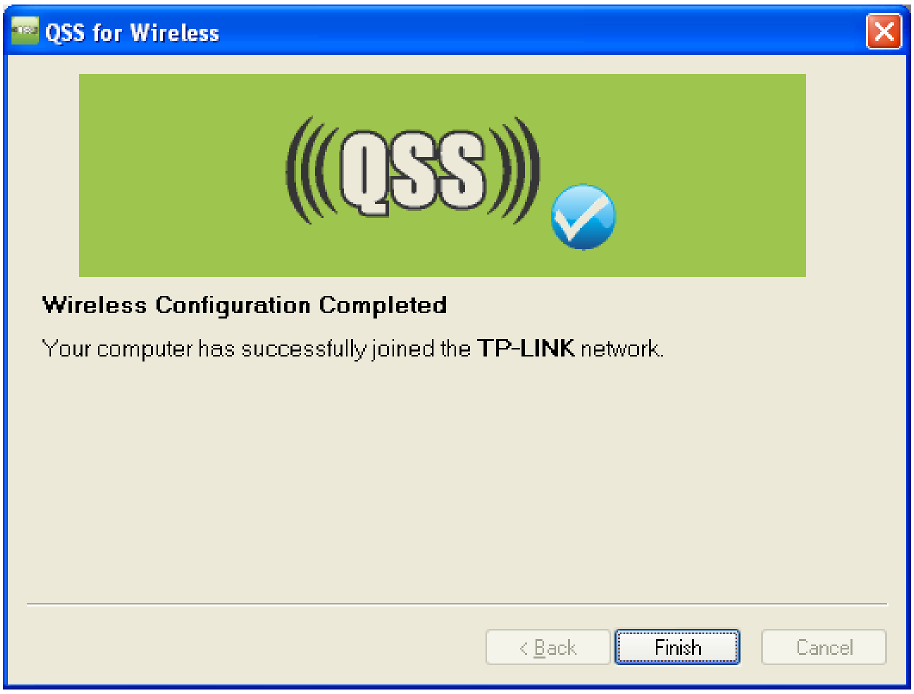
○ Enter the PIN from my access point

Push the button on your access point and click Next to continue.

Automatically select the network ☑

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.



QSS for Wireless

Wireless Configuration Completed

Your computer has successfully joined the **TP-LINK** network.

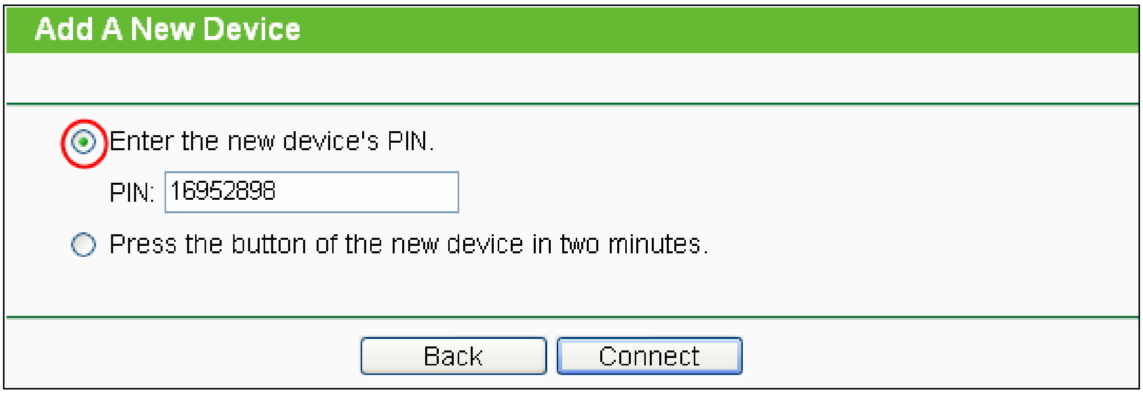
The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my AP

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 3-4, then the following screen will appear.



Add A New Device

● Enter the new device's PIN.

PIN: 16952898

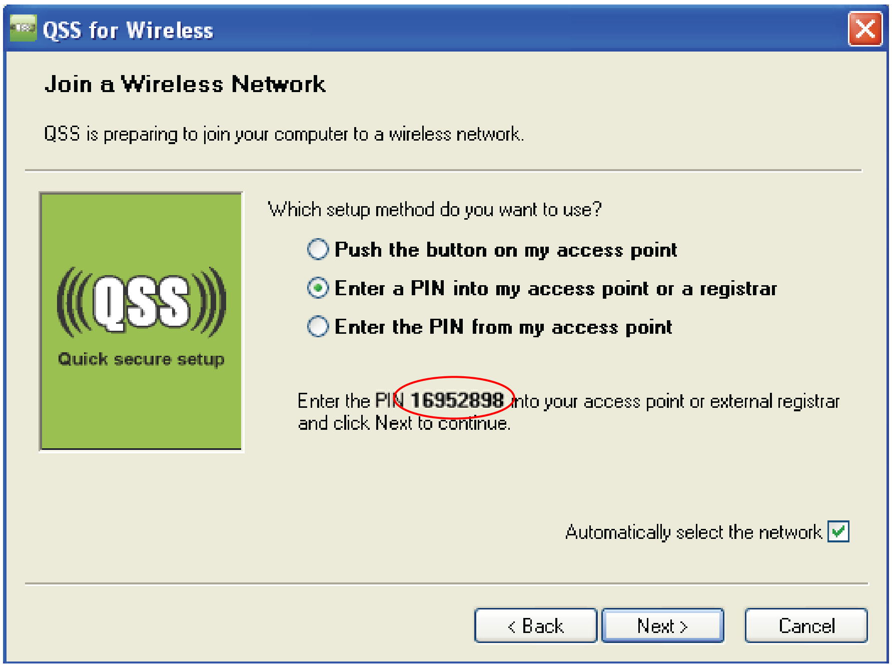
○ Press the button of the new device in two minutes.

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.**



Join a Wireless Network

QSS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

○ Push the button on my access point

● Enter a PIN into my access point or a registrar

○ Enter the PIN from my access point

Enter the PIN 16952898 into your access point or external registrar and click Next to continue.

Automatically select the network ☑

The QSS Configuration Screen of Wireless Adapter

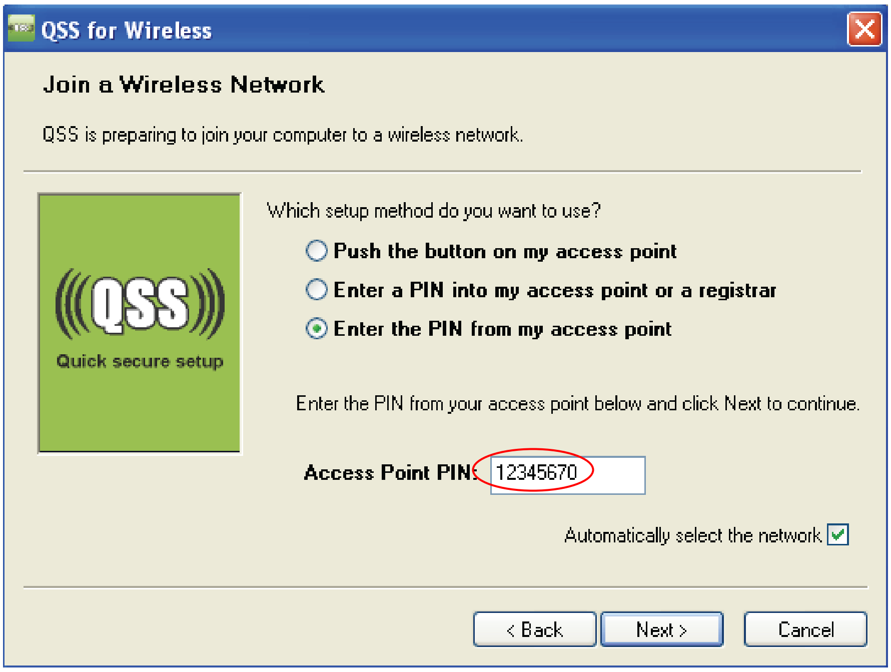
☞ **Note:**

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

Method Two: Enter the PIN from my AP

Step 1: Get the Current PIN code of the AP in Figure 3-4 (each AP has its unique PIN code. Here takes the PIN code 12345670 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**.



Join a Wireless Network

QSS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

○ Push the button on my access point

○ Enter a PIN into my access point or a registrar

● Enter the PIN from my access point

Enter the PIN from your access point below and click Next to continue.

Access Point PIN: 12345670

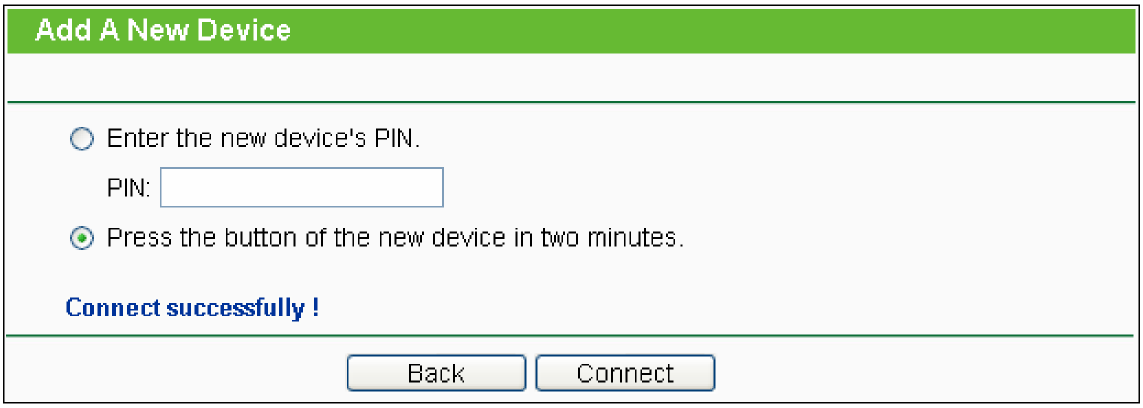
Automatically select the network ☑

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 3-4.

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



Add A New Device

○ Enter the new device's PIN.

PIN:

● Press the button of the new device in two minutes.

Connect successfully !

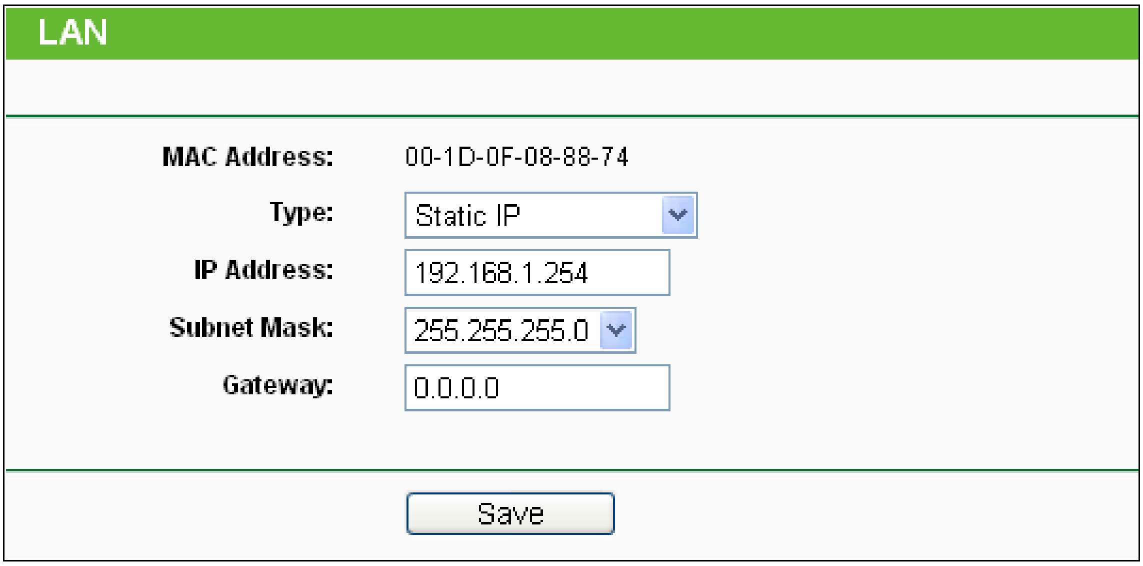
☞ **Note:**

a. The QSS LED on the AP will light green for five minutes if the device has been successfully added to the network.

b. 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.

3.4 Network

You can configure the IP parameters of Network on this page.



LAN

MAC Address: 00-1D-0F-08-88-74

Type: Static IP

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Figure 3-6 Network

- **Type -** Choosing Dynamic IP (DHCP) to get IP address from DHCP server, or choosing Static IP to configure IP address manually.
- **IP Address -** Enter the IP address of your AP in dotted-decimal notation (factory default: 192.168.1.254).
- **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, as seen from the LAN. 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 you select the type of Dynamic IP (DHCP), the DHCP server in this device will no startup.
3. If the new IP address you set is not in the same subnet, the IP Address pool in the DHCP server will not take effect, until they are re-configured.
4. The device will reboot automatically after you click the **Save** button.

3.5 Wireless

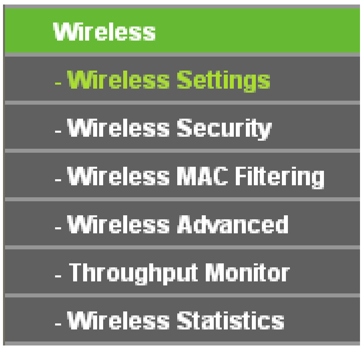


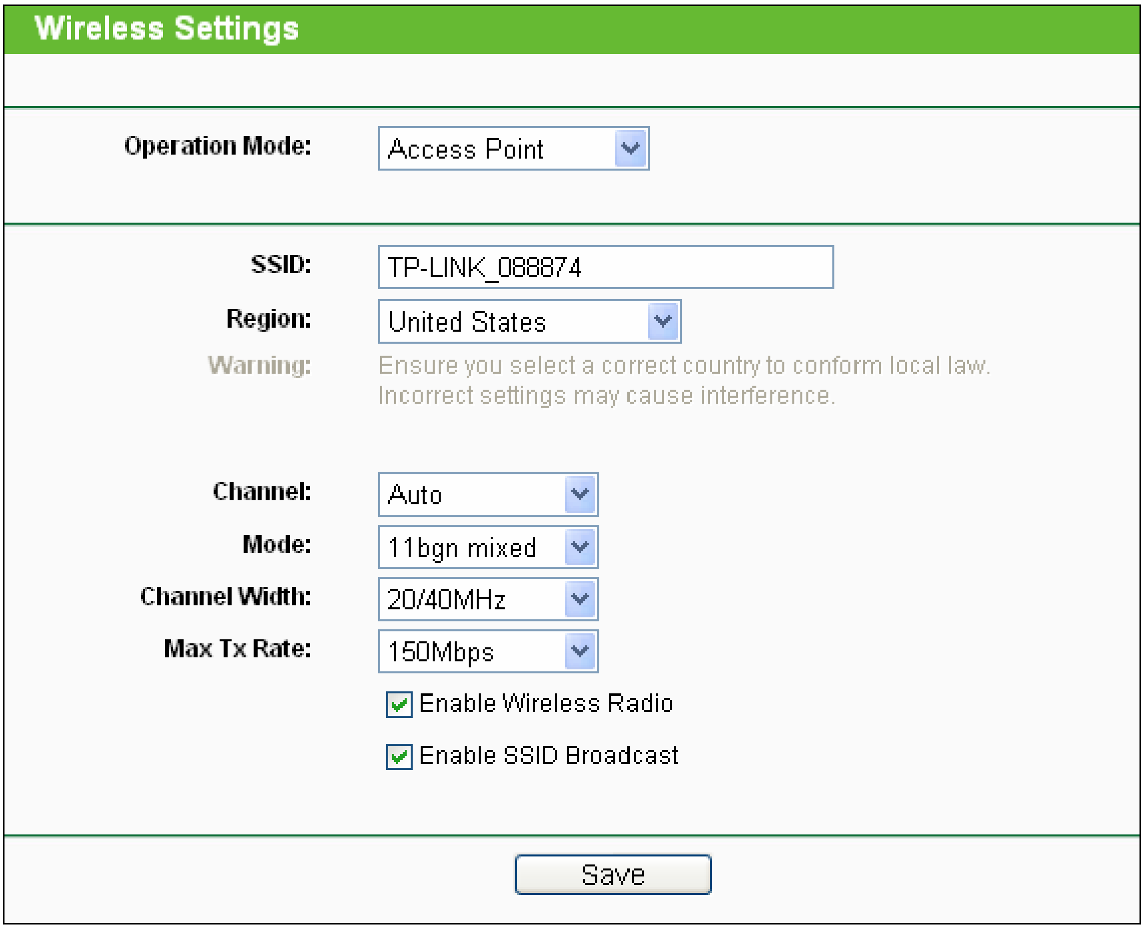
Figure 3-7 Wireless menu

There are six submenus under the Wireless menu (shown in Figure 3-7): **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.

3.5.1 Wireless Settings

This page allows you to configure the wireless mode for your device. The wireless settings for the wireless network in each operation mode are set on this page. Six operation modes are supported here, including **Access Point**, **Multi-SSID**, **Client**, **Repeater**, **Universal Repeater** and **Bridge with AP**. The available setting options for each operation mode are different from those of the other.

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



Wireless Settings

Operation Mode: Access Point

SSID: TP-LINK_088874

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: 150Mbps

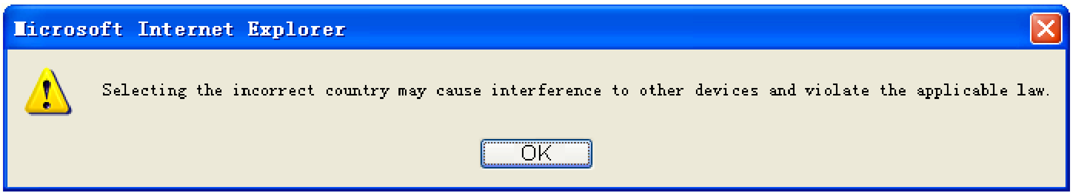
☑ Enable Wireless Radio

☑ Enable SSID Broadcast

Figure 3-8 Wireless Settings in Access Point mode

- **SSID -** Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is TP-LINK_xxxxxx (xxxxxx indicates the last six unique characters of each device's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.



Microsoft Internet Explorer

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ **Note:**

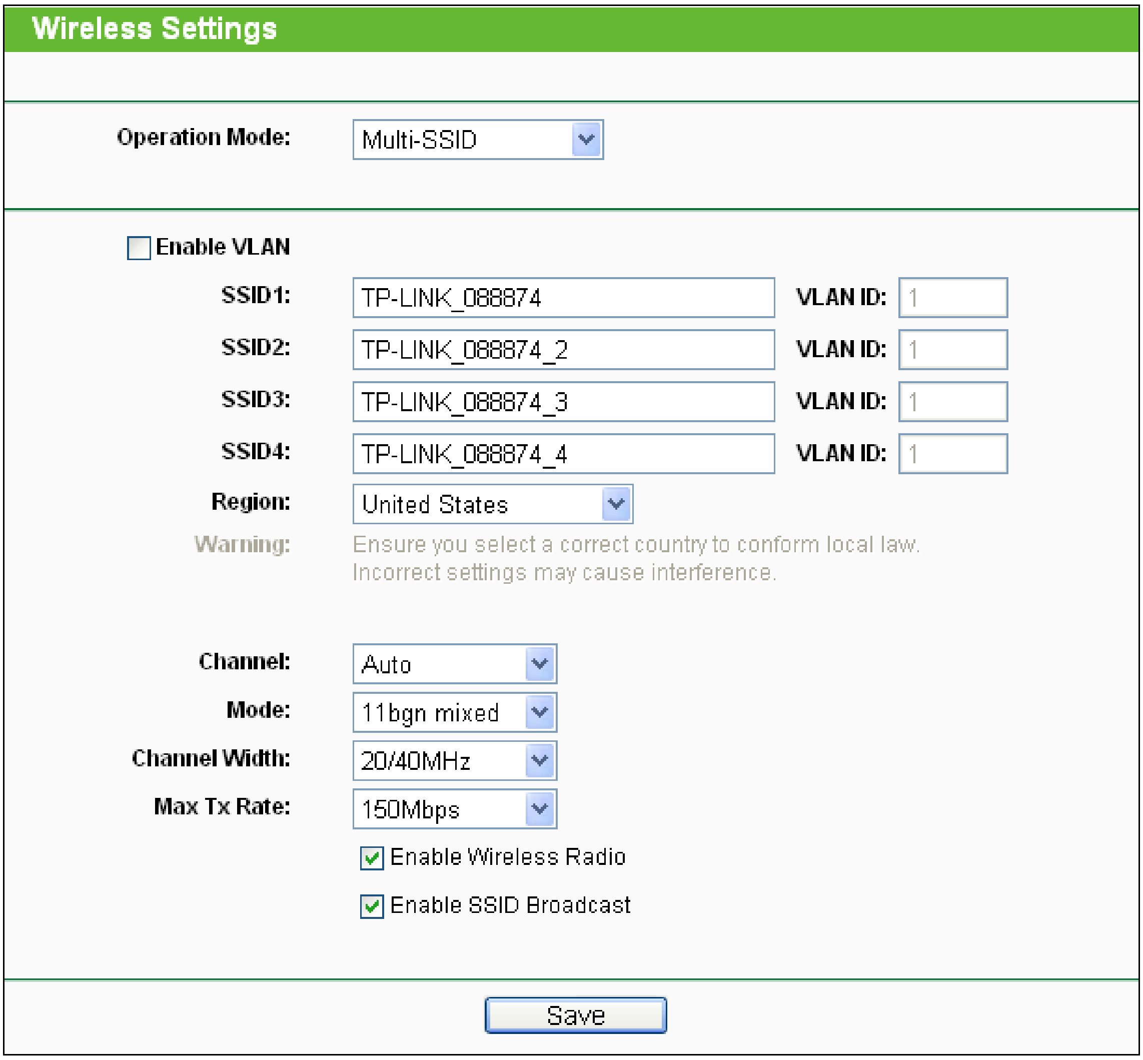
Limited by local law regulations, version for North America does not have region selection option.

- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice problems with another nearby access point.
- **Mode -** This field determines the wireless mode which the device works on.
  - **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** - Select the channel width from the pull-down list.
- **Max Tx Rate -** You can limit the maximum tx rate of the device through this field.
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled to allow or deny wireless stations to access.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device. If you select the **Enable SSID Broadcast** checkbox, the device will broadcast its name (SSID) on the air.

☞ **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) **Multi-SSID:** This mode allows the device to support up to 4 SSIDs.



Wireless Settings

Operation Mode: Multi-SSID

□ Enable VLAN

SSID1:	TP-LINK_088874	VLAN ID:	1
SSID2:	TP-LINK_088874_2	VLAN ID:	1
SSID3:	TP-LINK_088874_3	VLAN ID:	1
SSID4:	TP-LINK_088874_4	VLAN ID:	1

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: 150Mbps

☑ Enable Wireless Radio

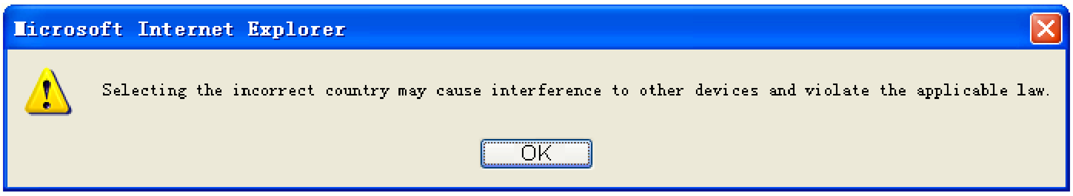
☑ Enable SSID Broadcast

Figure 3-9 Wireless Settings in Multi-SSID mode

- **Enable VLAN -** Check this box and then you can change the **VLANID** of each SSID. If you want to configure the Guest and Internal networks on VLAN, the switch you are using must support VLAN. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard, and enable this field.
- **SSID (1-4) -** Up to 4 SSIDs for each BSS can be entered in the filed SSID1 ~ SSID4. The name can be up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. If **Enable VLAN** is checked, the wireless stations connecting to SSID of different VLANID can not communicate with each other.
- **VLANID (1-4) -** Provide a number between 1 and 4095 for VLAN. This will cause the device to send packets with VLAN tags. The switch connecting with the device must support VLAN IEEE802.1Q frames. The wireless stations connecting to the SSID of a specified VLANID can communicate with the PC connecting to the port with the same VLANID on the Switch.
- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice problems with another nearby access point.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of

the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.



Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ **Note:**

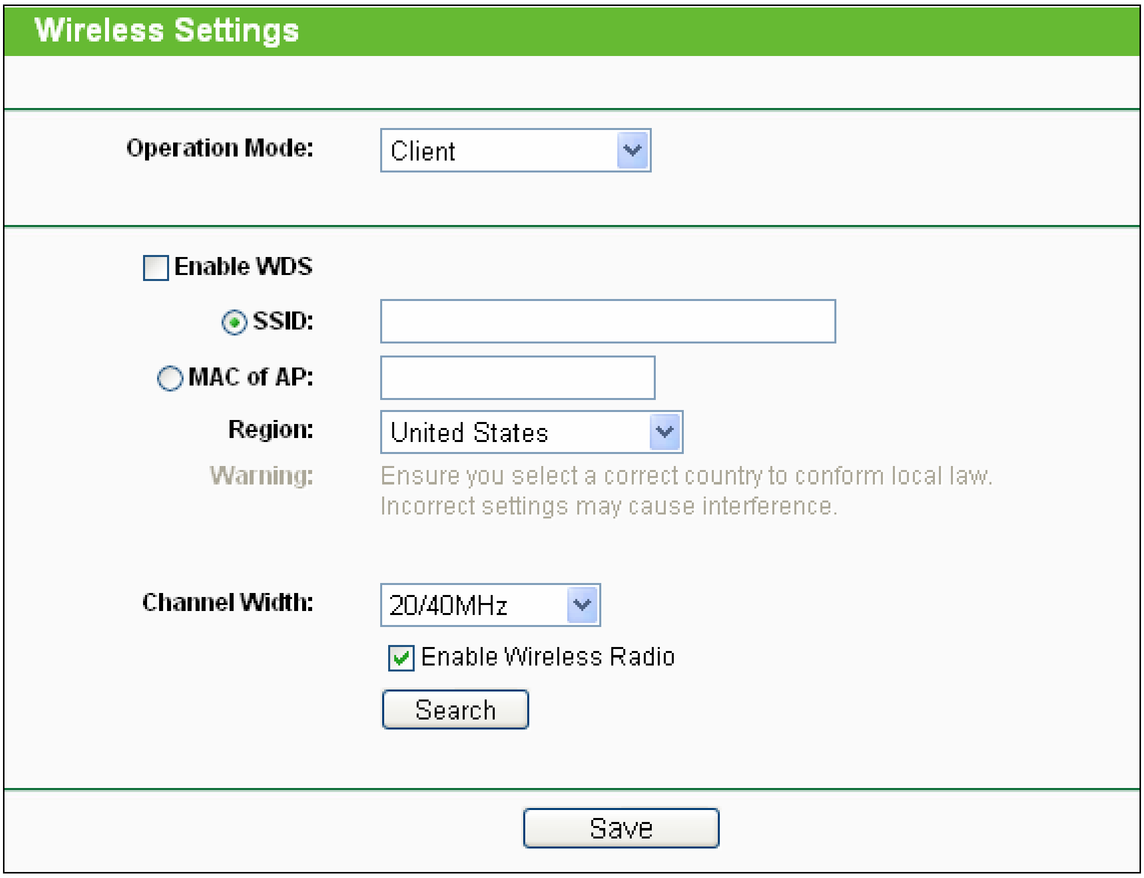
Limited by local law regulations, version for North America does not have region selection option.

- **Mode -** This field determines the wireless mode which the device works on.
  - **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 -** Select the channel width from the pull-down list.
- **Max Tx Rate -** You can limit the maximum tx rate of the device through this field.
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled to allow or deny wireless stations to access.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device. If you select the **Enable SSID Broadcast** checkbox, the device will broadcast its name (SSID) on the air.

☞ **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.

3) **Client:** This mode allows the device to act as a wireless station to enable wired host(s) to access an AP.



Wireless Settings

Operation Mode: Client

□ Enable WDS

● SSID:

○ MAC of AP:

Region: United States

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

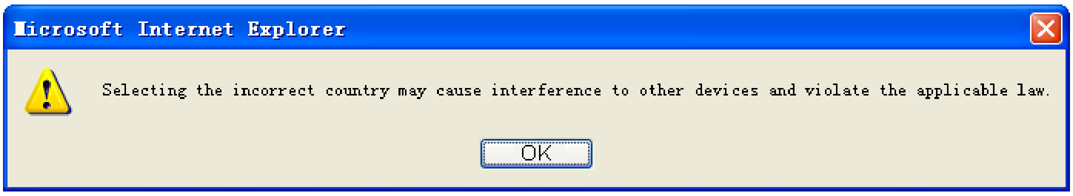
Channel Width: 20/40MHz

☑ Enable Wireless Radio

Figure 3-10 Wireless Settings in Client mode

- **Enable WDS -** The client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please enable this option.
- **SSID -** If you select the radio button before **SSID**, the AP client will connect to the AP according to SSID. Enter the SSID of AP that you want to access.
- **MAC of AP -** If you select the radio button before **MAC of AP**, the AP client will connect to the AP according MAC address. Enter the MAC address of AP that you want to access.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.



Microsoft Internet Explorer

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ **Note:**

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

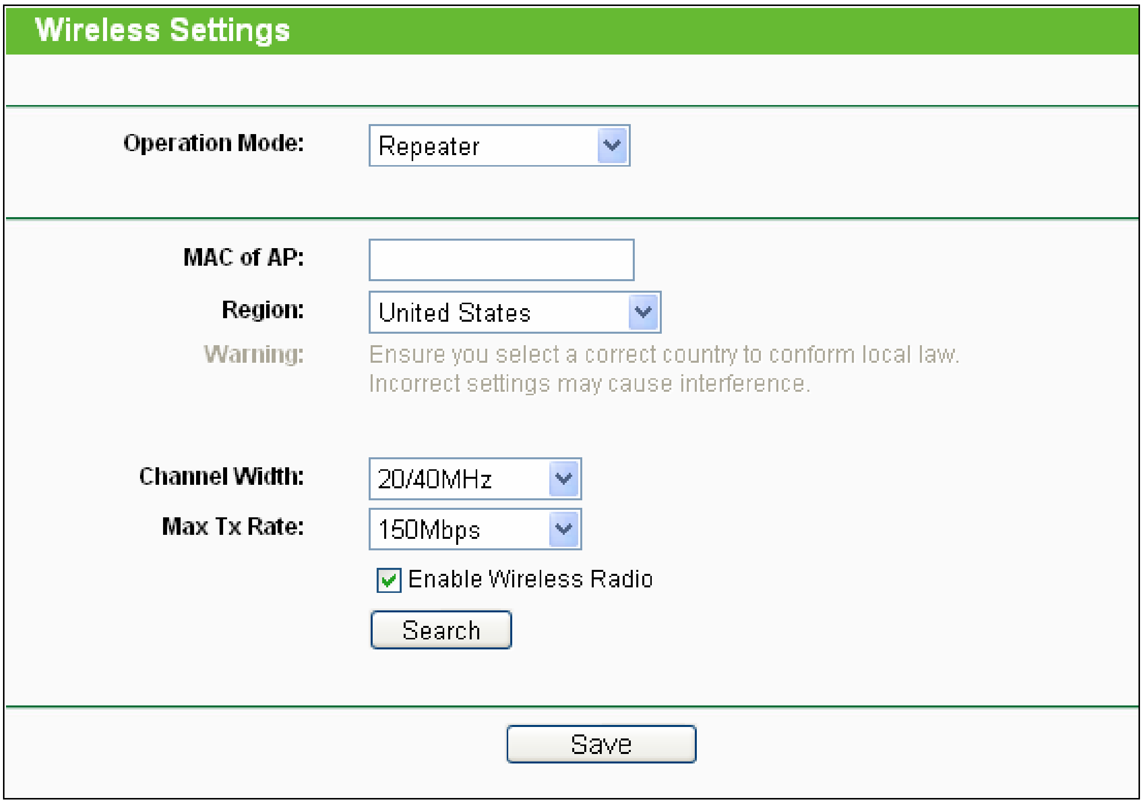
- **Channel Width -** Select the channel width from the pull-down list.
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled by selecting or deselecting this checkbox.

Click the **Search** button to detect the SSIDs in the local area.

☞ **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) **Repeater:** This mode allows the AP with its own BSS to relay data to a root AP to which it is associated with WDS enabled. The wireless repeater relays signal between its stations and the root AP for greater wireless range.



Wireless Settings

Operation Mode: Repeater

MAC of AP:

Region: United States

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

Channel Width: 20/40MHz

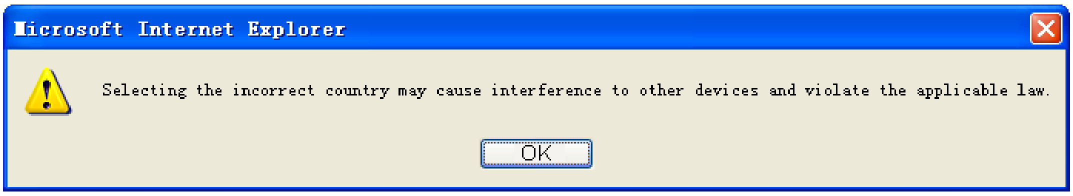
Max Tx Rate: 150Mbps

☑ Enable Wireless Radio

Figure 3-11 Wireless Settings in Repeater mode

- **MAC of AP -** Enter the MAC address of the root AP of which you want to expand wireless range.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.



Microsoft Internet Explorer

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ **Note:**

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

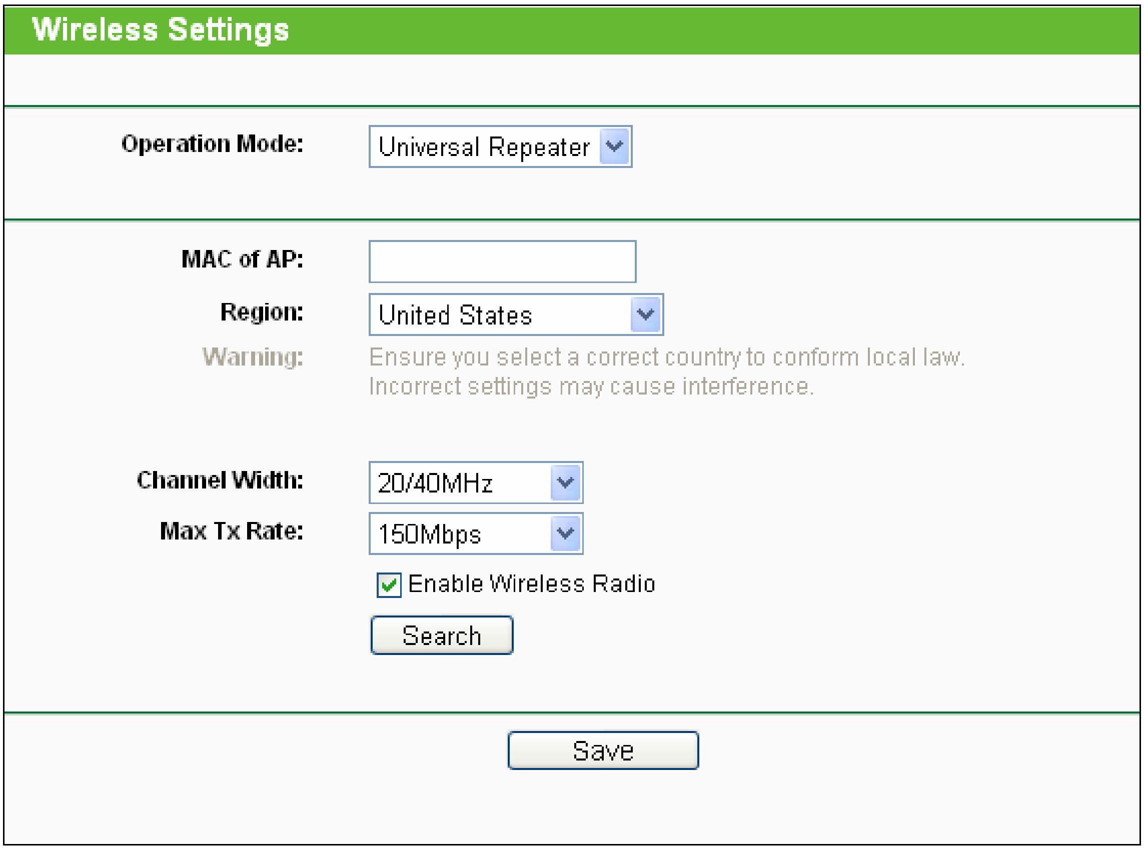
- **Channel Width -** Select the channel width from the pull-down list.
- **Max Tx Rate -** You can limit the maximum tx rate of the device through this field.
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled by selecting or deselecting this checkbox.

Click the **Search** button to detect the SSIDs in the local area.

☞ **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.

5) **Universal Repeater:** This mode allows the AP with its own BSS to relay data to a root AP to which it is associated with WDS disabled. The wireless repeater relays signal between its stations and the root AP for greater wireless range.



Wireless Settings

Operation Mode: Universal Repeater

MAC of AP:

Region: United States

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

Channel Width: 20/40MHz

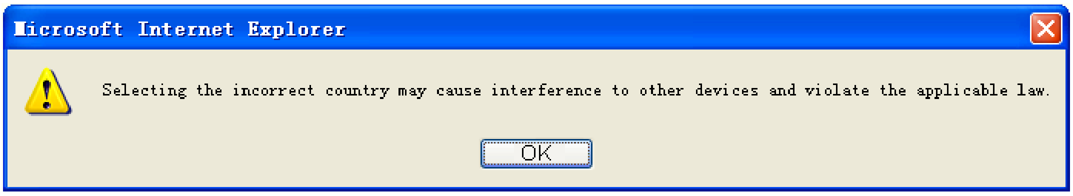
Max Tx Rate: 150Mbps

☑ Enable Wireless Radio

Figure 3-12 Wireless Settings in Repeater mode

- **MAC of AP -** Enter the MAC address of the root AP of which you want to expand wireless range.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.


Microsoft Internet Explorer

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ Note:

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

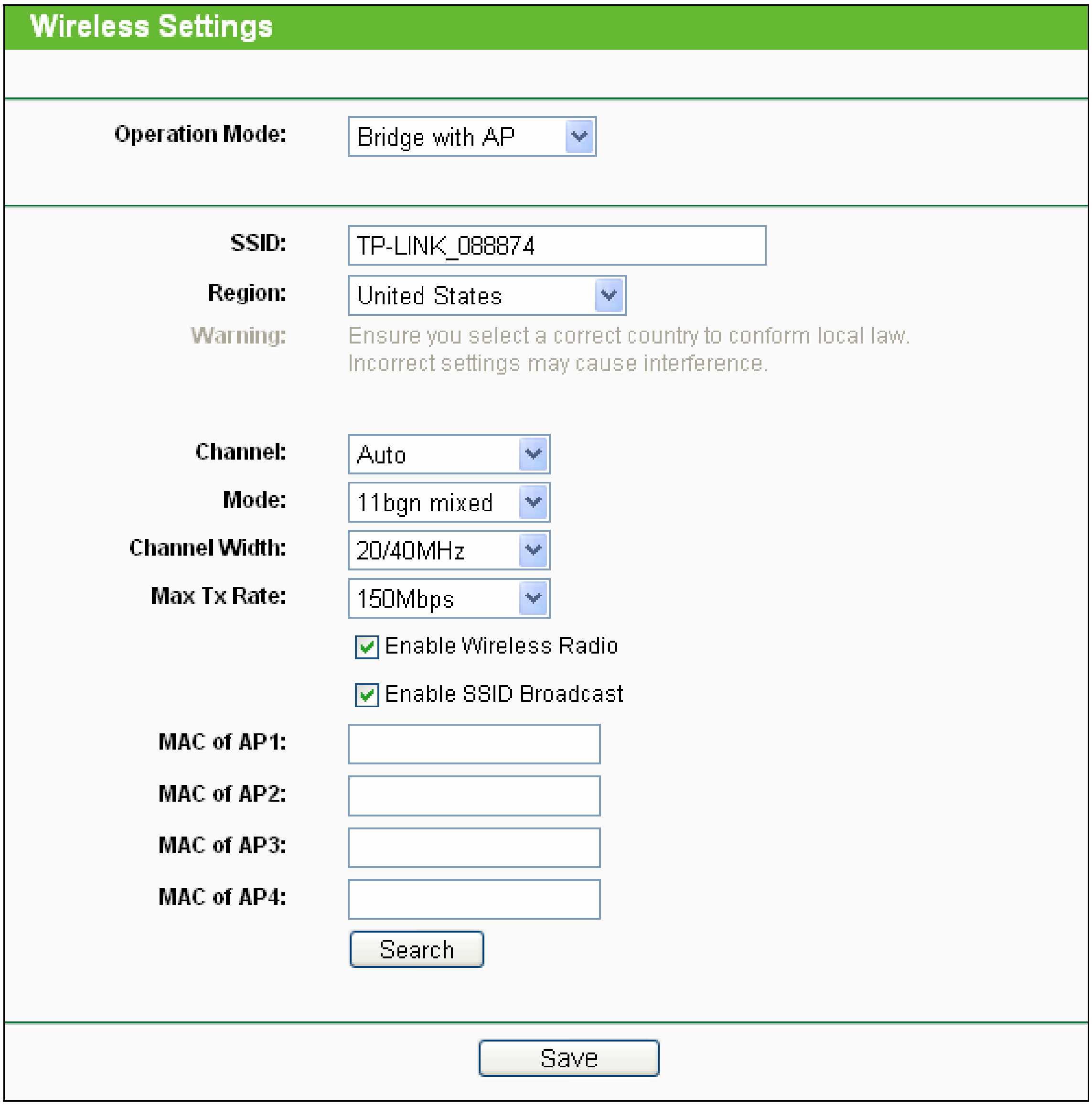
- **Channel Width -** Select the channel width from the pull-down list.
- **Max Tx Rate -** You can limit the maximum tx rate of the device through this field.
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled by selecting or deselecting this checkbox.

Click the **Search** button to detect the SSIDs in the local area.

☞ 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.

6) **Bridge with AP:** This mode can bridge the AP and up to 4 APs also in bridge mode to connect two or more wired LANs.



Wireless Settings

Operation Mode: Bridge with AP

SSID: TP-LINK_088874

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: 150Mbps

☑ Enable Wireless Radio

☑ Enable SSID Broadcast

MAC of AP1:

MAC of AP2:

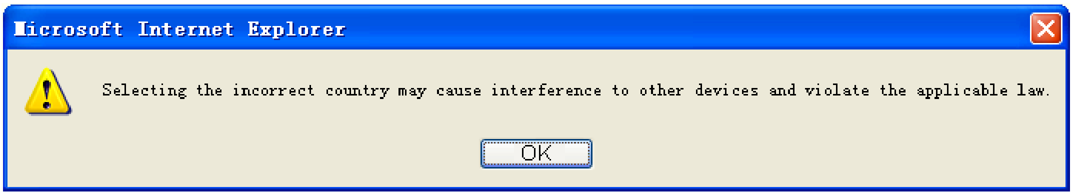
MAC of AP3:

MAC of AP4:

Figure 3-13 Wireless Settings in Repeater mode

- **SSID -** Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is TP-LINK_xxxxxx (xxxxxx indicates the last six unique characters of each device's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the **Save** button**,** then the Note Dialog appears. Click **OK**.



Microsoft Internet Explorer

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

Note Dialog

☞ **Note:**

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

- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice problems with another nearby access point.
- **Mode -** This field determines the wireless mode which the device works on.
  - **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 -** Select the channel width from the pull-down list.
- **Max Tx Rate -** You can limit the maximum tx rate of the device through this field.
- **MAC of AP (1-4) -** Enter the MAC address of other AP(s).
- **Enable Wireless Radio -** The wireless radio of this device can be enabled or disabled to allow or deny wireless stations to access.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the AP. If you select the **Enable SSID Broadcast** checkbox, the AP will broadcast its name (SSID) on the air.

Click the **Search** button to detect the SSIDs in the local area.

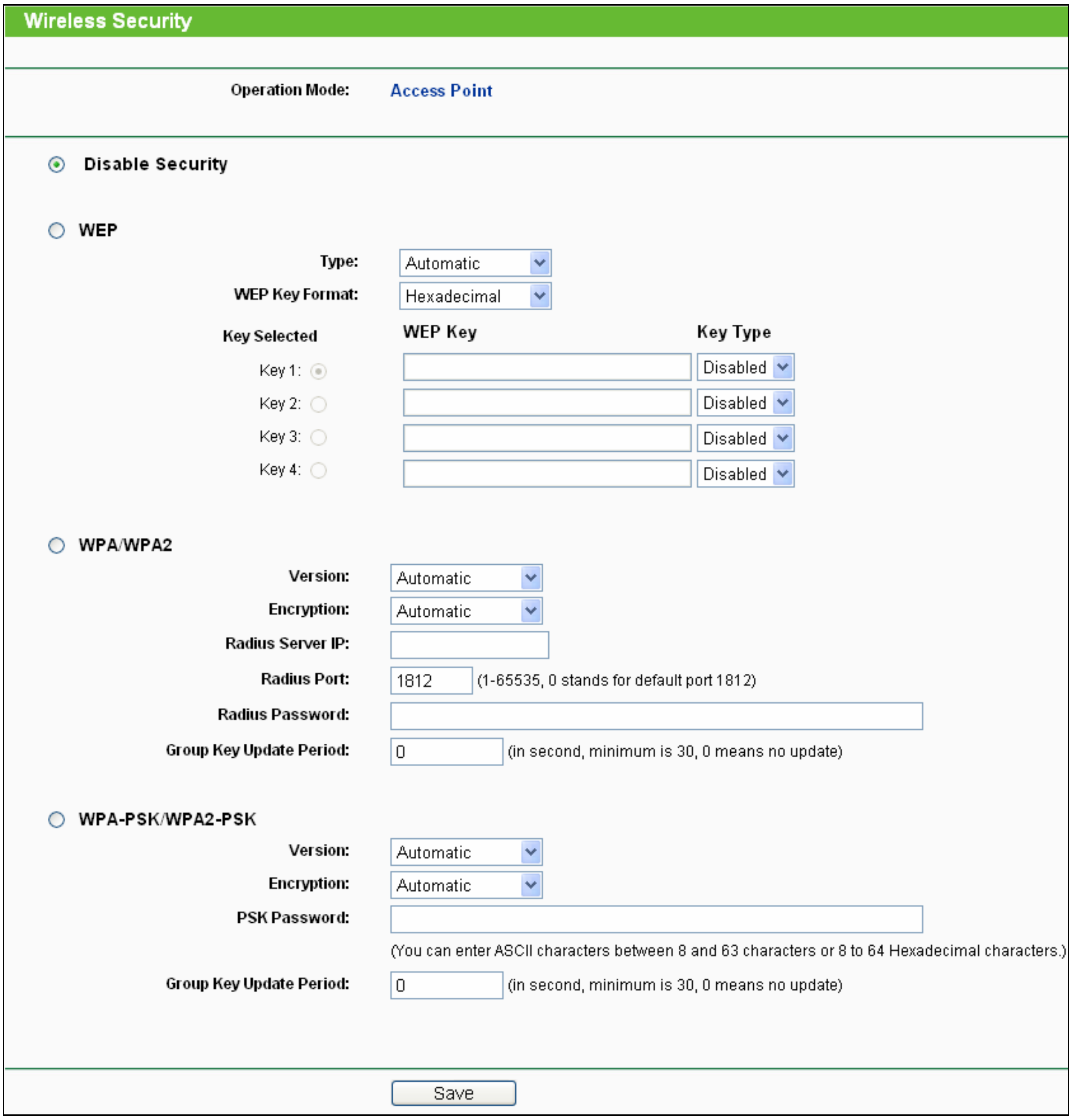
☞ **Note:**

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.

3.5.2 Wireless Security

The security options are different for different operation mode.

1) Access Point



Wireless Security

Operation Mode: Access Point

● Disable Security

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

○ WPA/WPA2

Version: Automatic

Encryption: Automatic

Radius Server IP:

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

Radius Password:

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

○ WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Password:

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

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

Figure 3-14 Wireless Security - Access Point

- **Operation Mode -** Current operation mode is shown here.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of options 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.

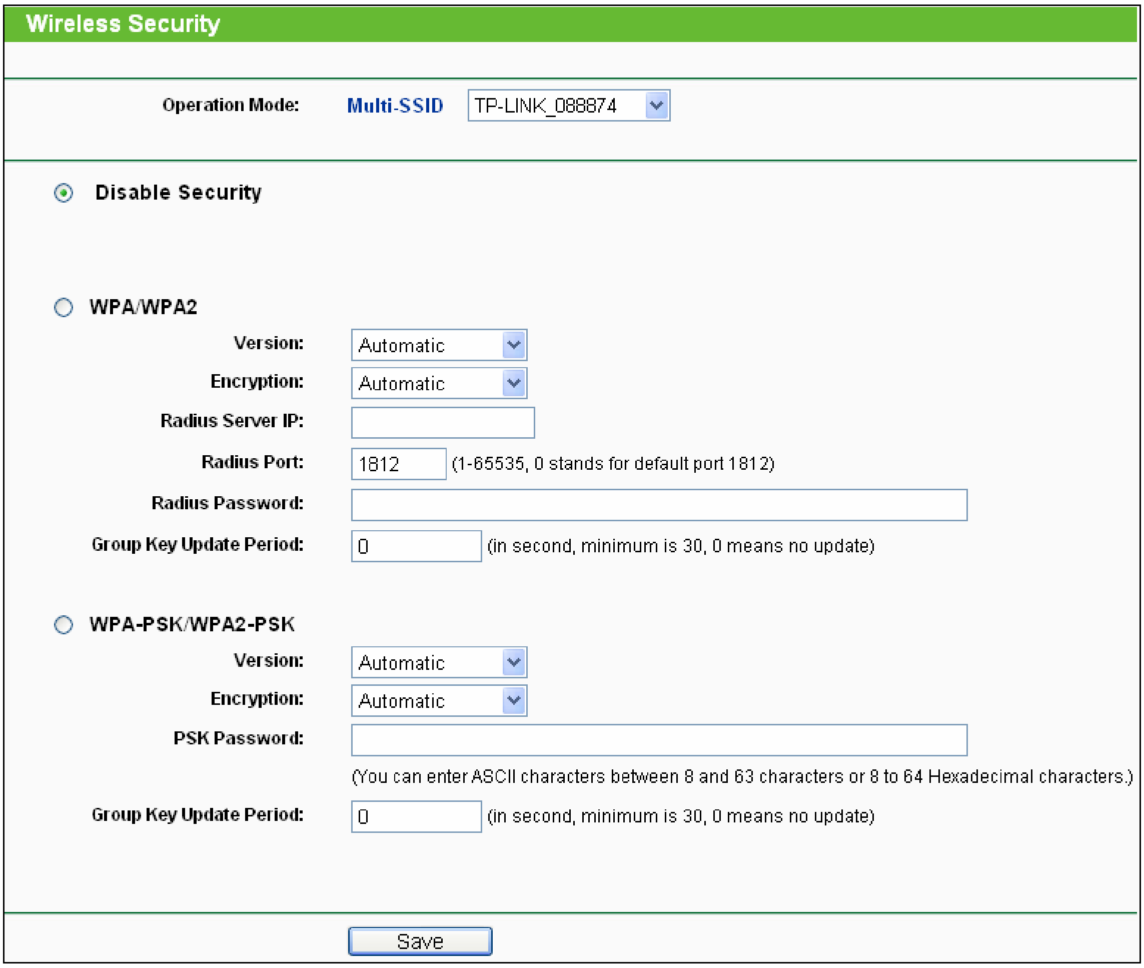
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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.

2) Multi-SSID



Wireless Security

Operation Mode: Multi-SSID TP-LINK_088874

● Disable Security

○ WPA/WPA2

Version: Automatic

Encryption: Automatic

Radius Server IP:

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

Radius Password:

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

○ WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Password:

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

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

Figure 3-15 Wireless Security – Multi-SSID

- **Operation Mode -** Current operation mode is shown here. You can choose one of the 4 SSID from the pull-down list.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of options to enable security.
- **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.

☞ **Note:**

This security option will become unavailable, if the **Enable VLAN** box in Figure 3-9 is checked.

➢ **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.

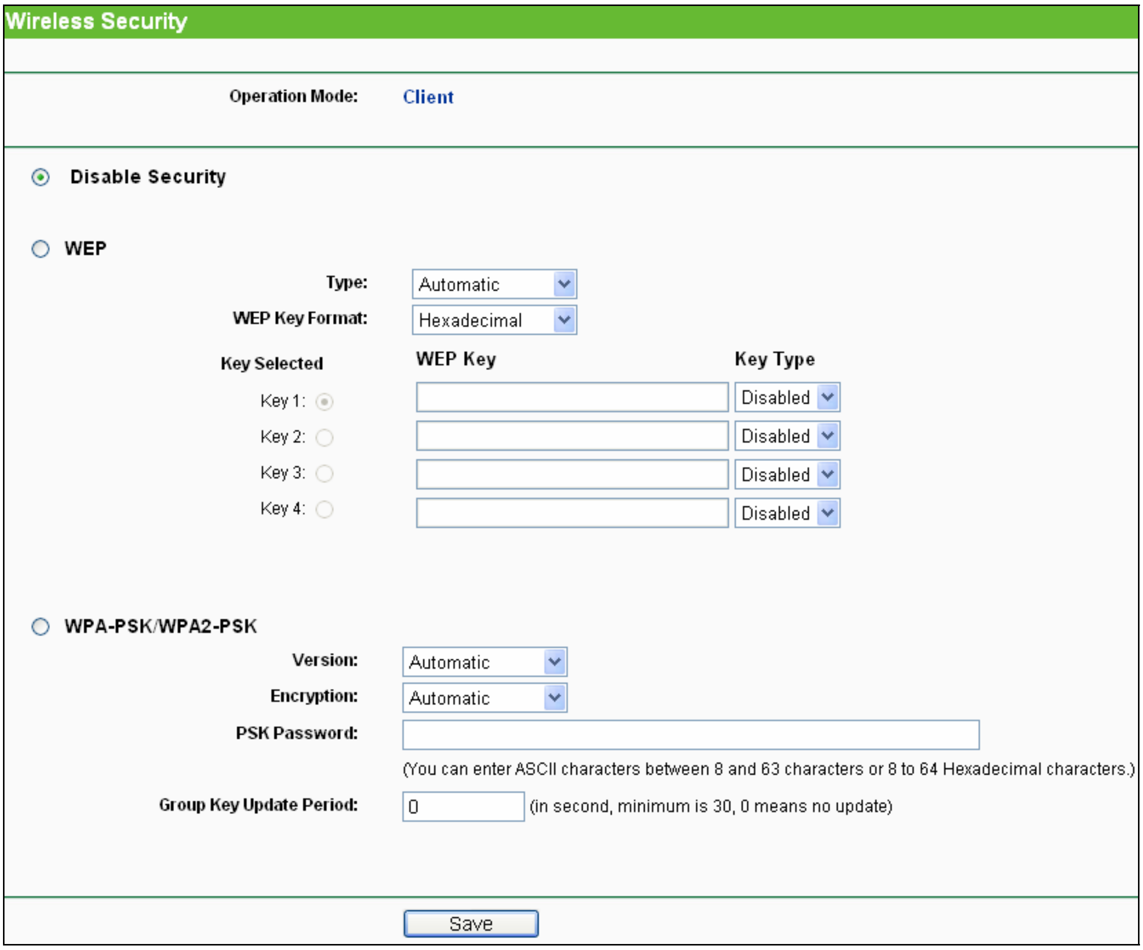
- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The 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.

3) Client



Wireless Security

Operation Mode: Client

● Disable Security

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

○ WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Password:

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

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

Figure 3-16 Wireless Security – Client

- **Operation Mode -** Current operation mode is shown here.
- **Disable Security -** The wireless security function can be enabled or disabled. It is recommended strongly that you choose one of options 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.

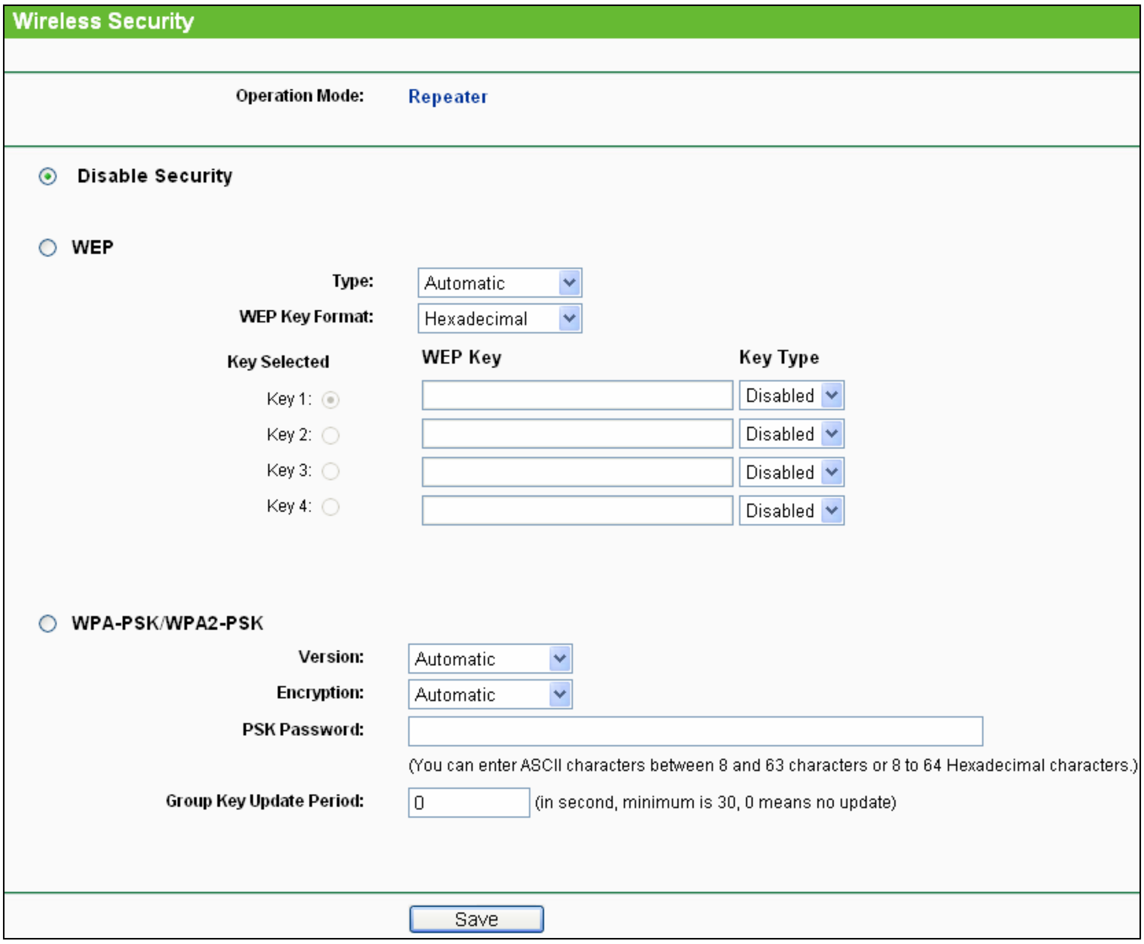
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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.

4) Repeater



Wireless Security

Operation Mode: Repeater

● Disable Security

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

○ WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Password:

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

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

Figure 3-17 Wireless Security – Repeater

- **Operation Mode -** Current operation mode is shown here.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless repeater can only replay signal of the root AP without encryption to its stations. It is recommended strongly that you choose one of options 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.

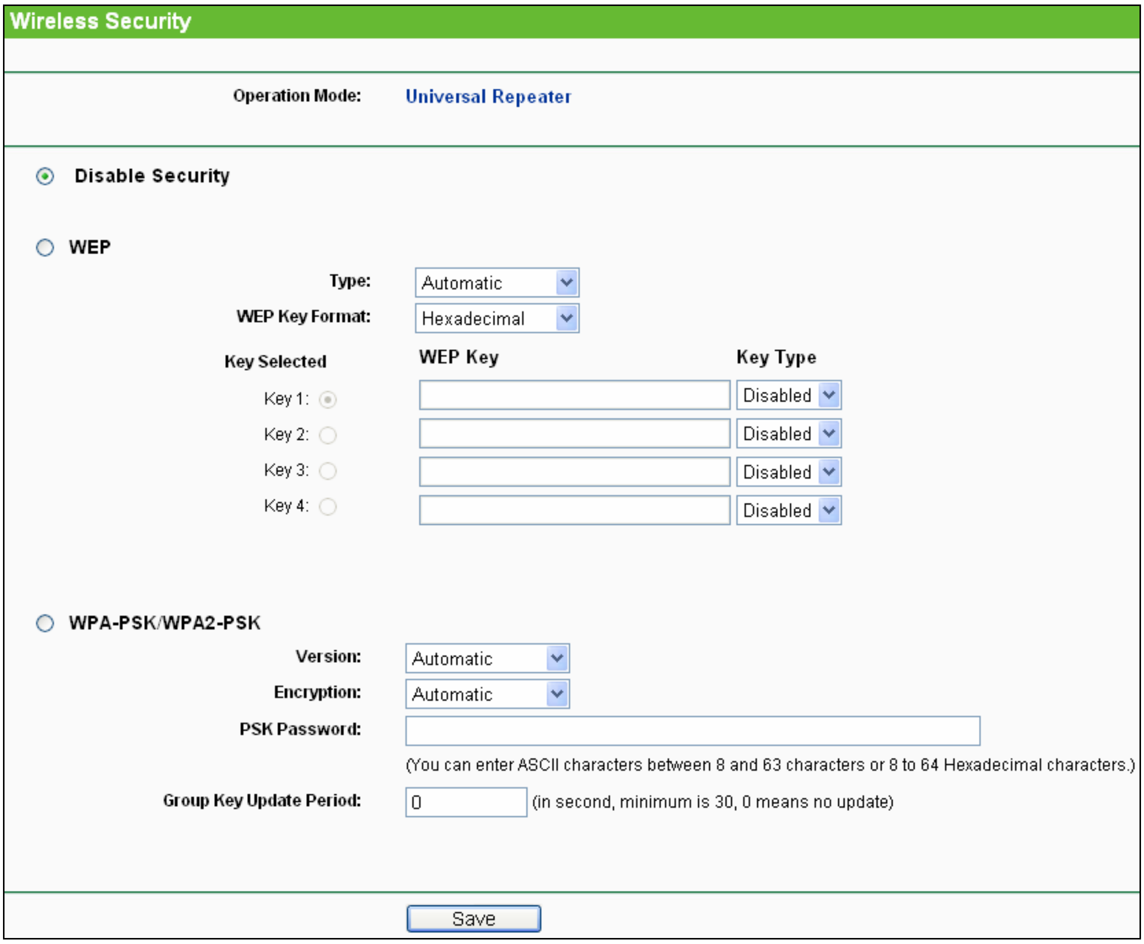
- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The 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.

5) Universal Repeater



Wireless Security

Operation Mode: Universal Repeater

● Disable Security

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

○ WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Password:

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

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

Figure 3-18 Wireless Security – Universal Repeater

- **Operation Mode -** Current operation mode is shown here.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of options 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.

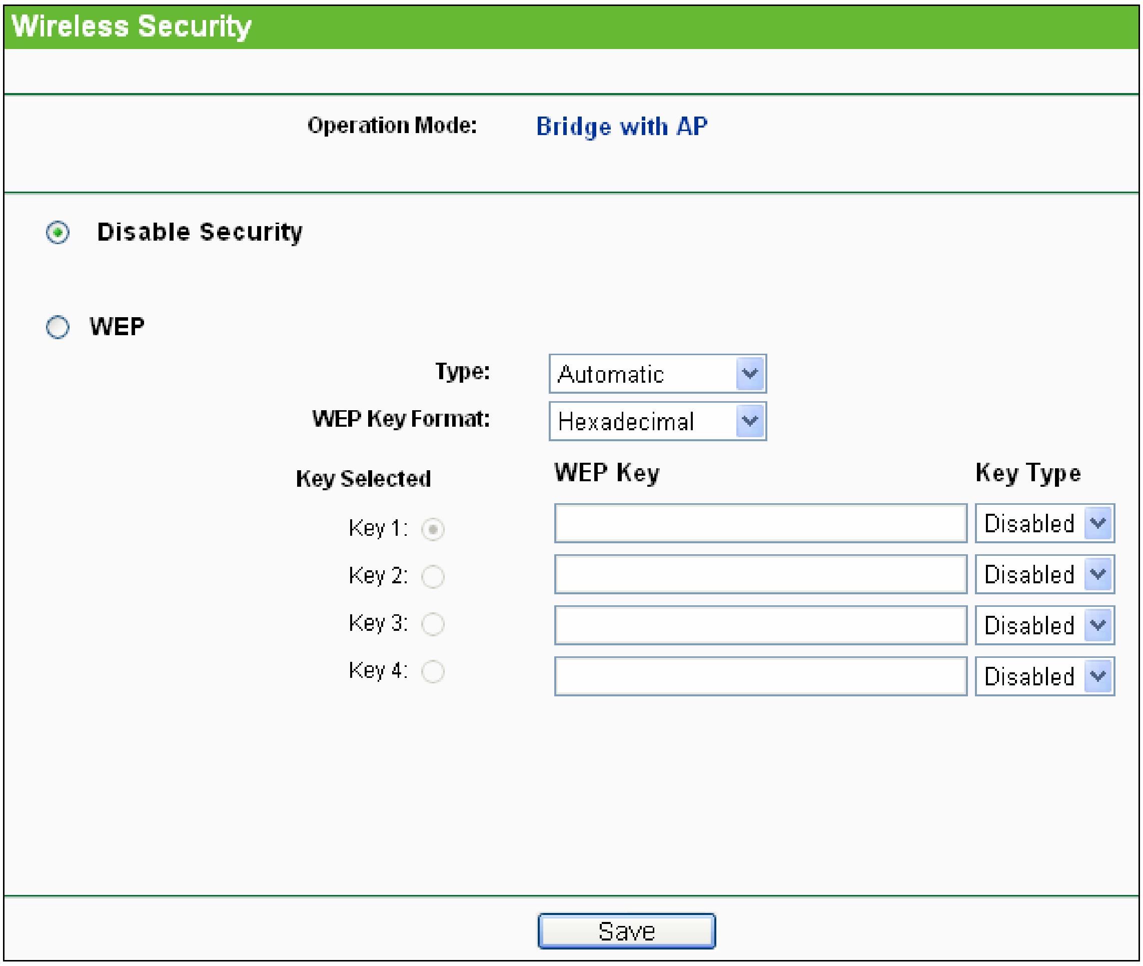
- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The 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.

6) Bridge with AP



Wireless Security

Operation Mode: Bridge with AP

● Disable Security

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

Figure 3-19 Wireless Security – Universal Repeater

- **Operation Mode -** Current operation mode is shown here.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of options 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.

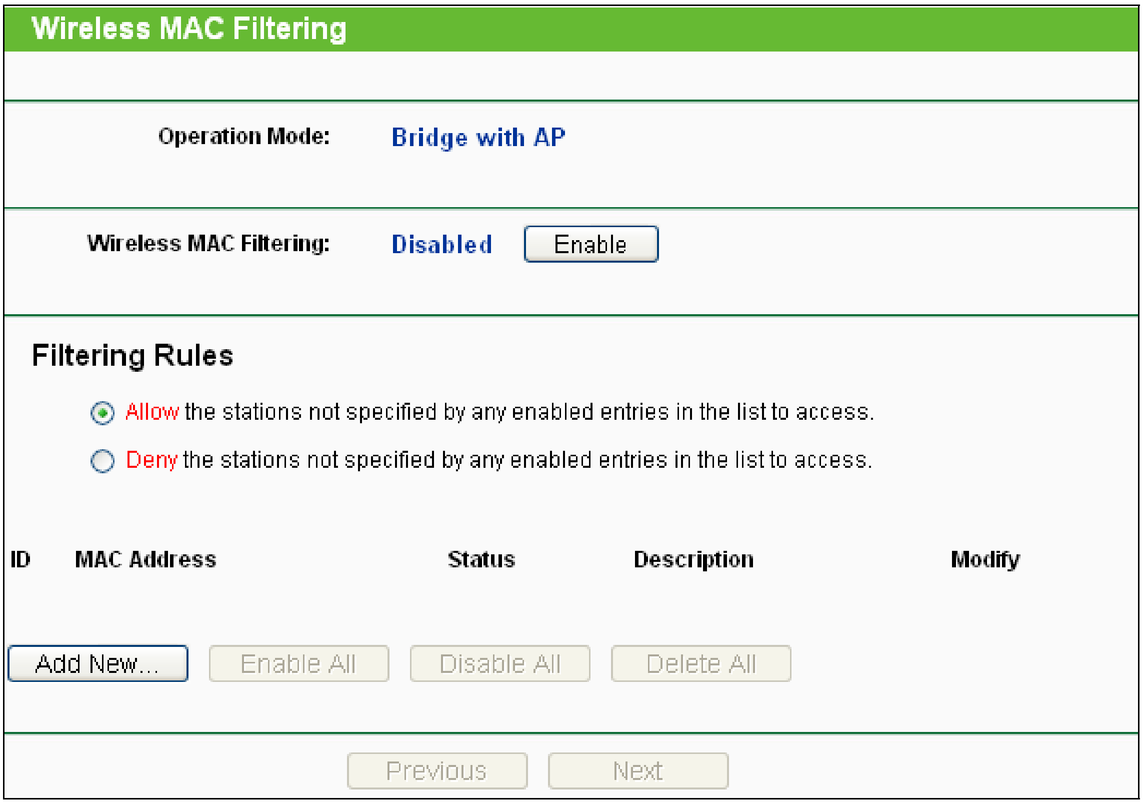
☞ **Note:**

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

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

3.5.3 Wireless MAC Filtering

The Wireless MAC Filtering for wireless networks is set on this page Figure 3-20. 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.



Wireless MAC Filtering

Operation Mode: Bridge with AP

Wireless MAC Filtering: Disabled

Filtering Rules

● Allow the stations not specified by any enabled entries in the list to access.

○ Deny the stations not specified by any enabled entries in the list to access.

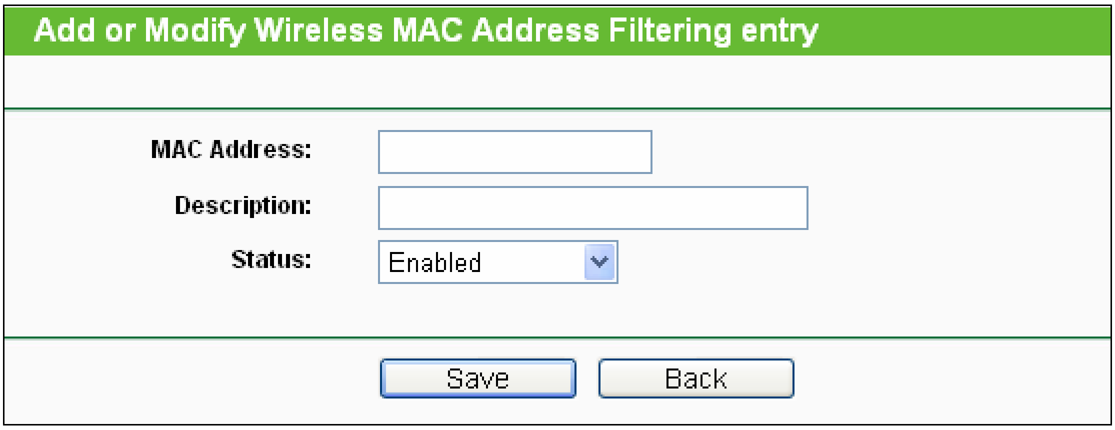
ID	MAC Address	Status	Description	Modify

Figure 3-20 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 -** Current operation mode is shown here.
- **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 3-21



Add or Modify Wireless MAC Address Filtering entry

MAC Address:

Description:

Status: Enabled

Figure 3-21 Add or Modify Wireless MAC Address Filtering entry

- **MAC Address -** The wireless station's MAC address that you want to access.
- **Description -** A simple description of the wireless station.
- **Status -** The status of 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 or modify 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.

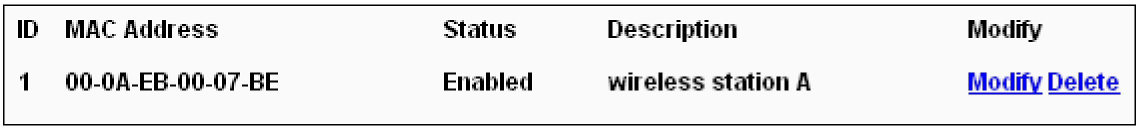
Click the **Delete All** button to delete all entries

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:



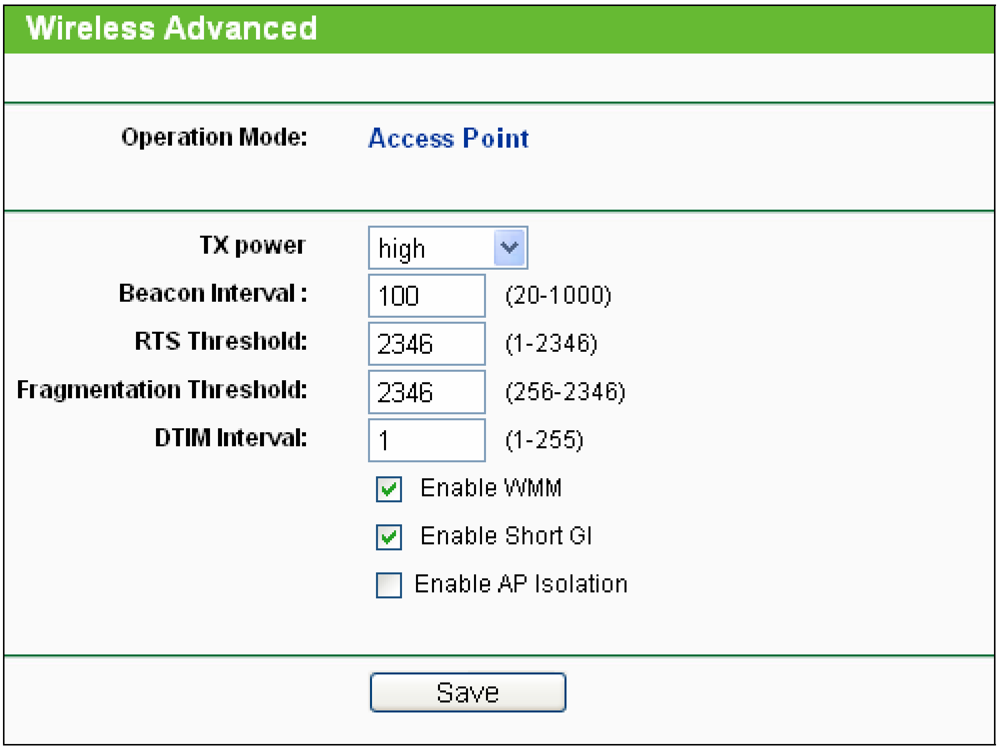
ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	wireless station A	Modify Delete

☞ **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.

3.5.4 Wireless Advanced

This page shows some advanced settings for the device. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.



Wireless Advanced

Operation Mode: Access Point

TX power: high

Beacon Interval : 100 (20-1000)

RTS Threshold: 2346 (1-2346)

Fragmentation Threshold: 2346 (256-2346)

DTIM Interval: 1 (1-255)

☑ Enable WMM

☑ Enable Short GI

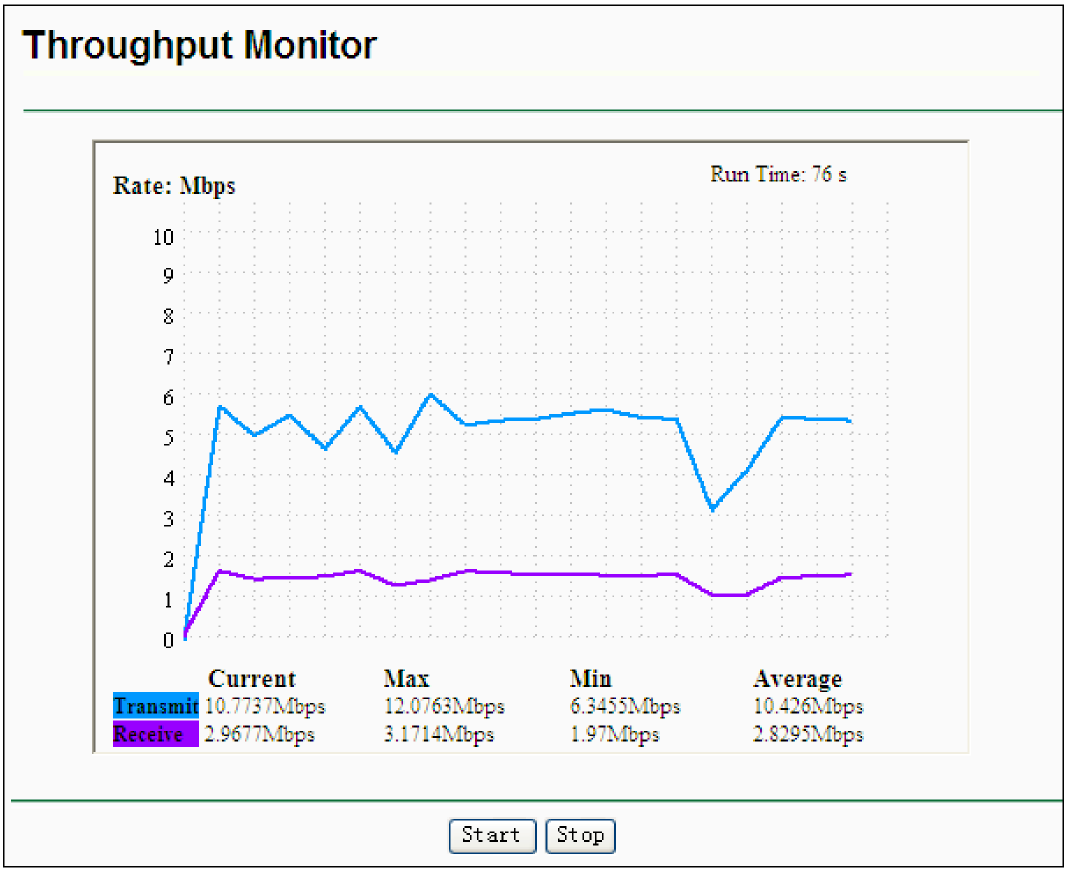
□ Enable AP Isolation

Figure 3-22 Wireless Advanced

- **Operation Mode -** Current Operation Mode is shown here.
- **Tx Power -** Here you can specify 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 -** The beacons are the packets sent by the device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the 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 -** This value 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 -** Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

3.5.5 Throughput Monitor

This page helps to watch wireless throughput information.



Throughput Monitor

	Current	Max	Min	Average
Transmit	10.7737Mbps	12.0763Mbps	6.3455Mbps	10.426Mbps
Receive	2.9677Mbps	3.1714Mbps	1.97Mbps	2.8295Mbps

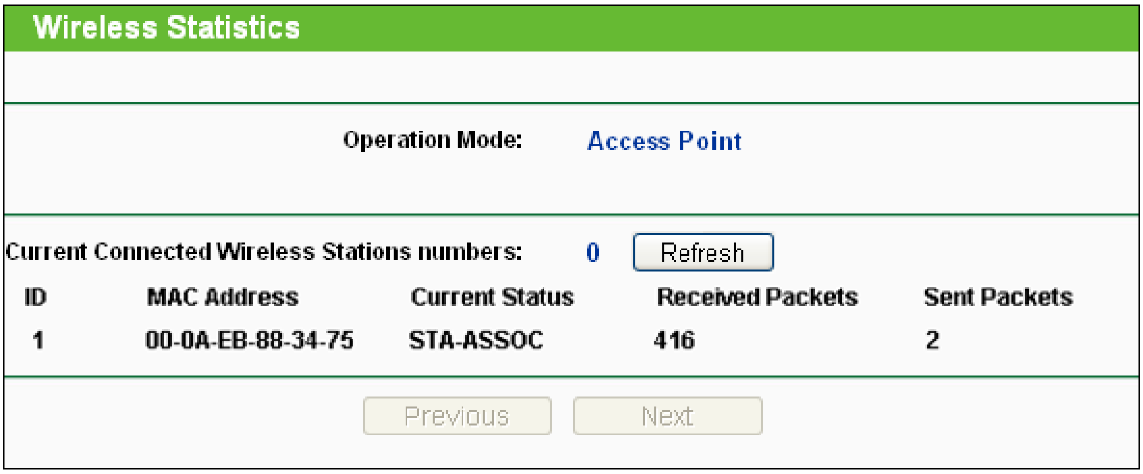
Figure 3-23 Wireless Advanced

- **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.

3.5.6 Wireless Statistics


Wireless Statistics

Operation Mode: Access Point

Current Connected Wireless Stations numbers: 0

ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-88-34-75	STA-ASSOC	416	2

Figure 3-24 Statistics of the device attached wireless stations

- **Operation Mode -** Current operation mode is shown at the top. If Multi-SSID is selected, all connected wireless stations will be shown here.
- **MAC Address -** 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 on 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.

3.6 DHCP

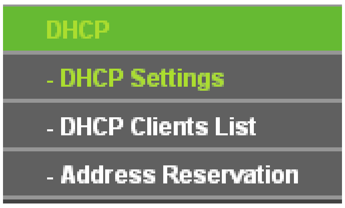
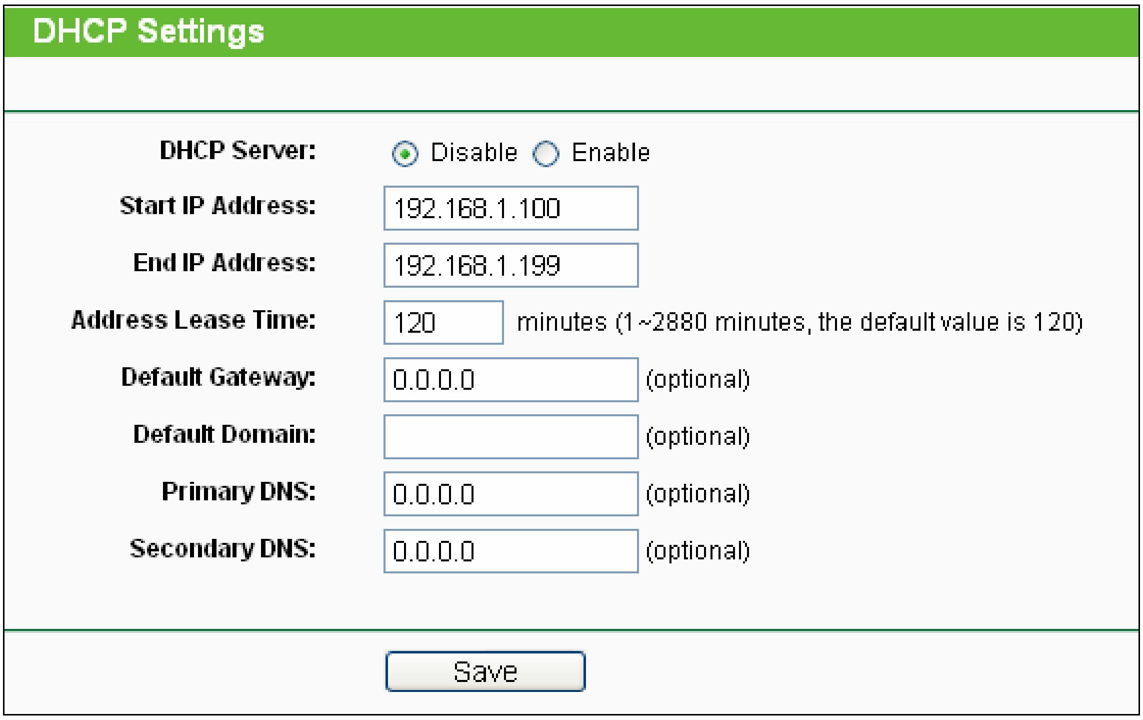


Figure 3-25 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 3-25): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

3.6.1 DHCP Settings

The System can be set up 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 in Figure 3-26):



DHCP Settings

DHCP Server:	● Disable ○ Enable
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.199
Address Lease Time:	120 minutes (1 ~2880 minutes, the default value is 120)
Default Gateway:	0.0.0.0 (optional)
Default Domain:	(optional)
Primary DNS:	0.0.0.0 (optional)
Secondary DNS:	0.0.0.0 (optional)

Figure 3-26 DHCP Settings

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually. This function is disabled by default.
- **Start IP Address -** This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
- **Address Lease Time -** The **Address Lease Time** is the amount of time a network user will be allowed connection to the system with their current dynamic IP Address. Enter the amount of time, in minutes, the user will be "leased" this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional.) Input the IP Address of the gateway.
- **Default Domain -** (Optional.) Input the domain name of your network.
- **Primary DNS -** (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

Click **Save** to save the changes.

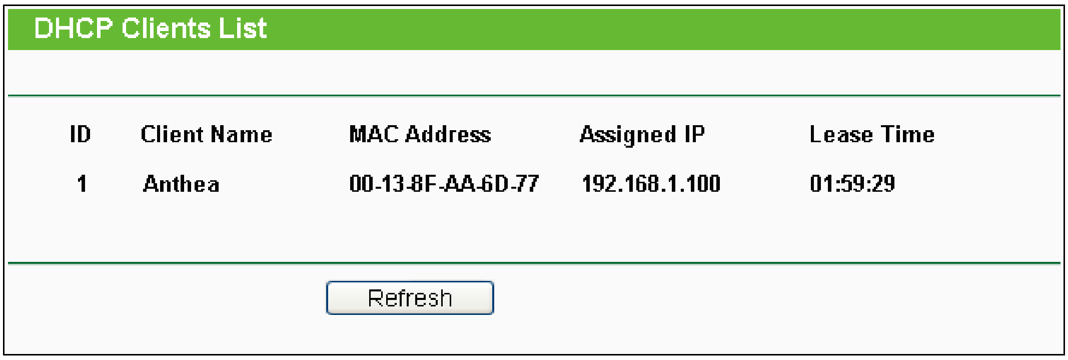
☞ **Note:**

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 take effect until the device reboots.

3.6.2 DHCP Clients List

This page shows **Client Name, MAC Address, Assigned IP** and **Lease Time** for each DHCP Client attached to the device (Figure 3-27):



DHCP Clients List

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Anthea	00-13-8F-AA-6D-77	192.168.1.100	01:59:29

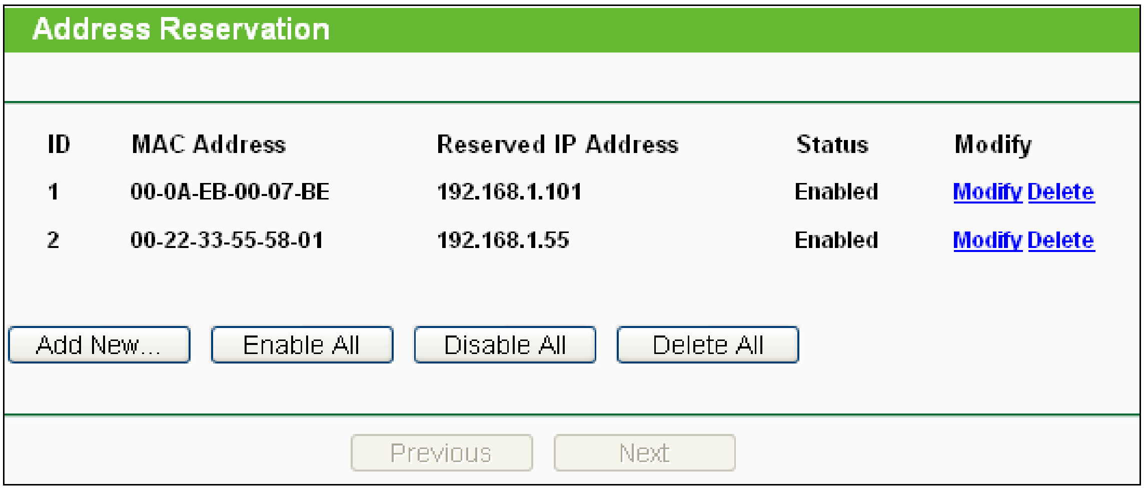
Figure 3-27 DHCP Clients List

- **ID -** The index of the DHCP Client.
- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the device has allocated to the DHCP client.
- **Lease Time -** 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.

3.6.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in Figure 3-28).



Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify
1	00-0A-EB-00-07-BE	192.168.1.101	Enabled	Modify Delete
2	00-22-33-55-58-01	192.168.1.55	Enabled	Modify Delete

Figure 3-28 Address Reservation

- **MAC Address -** The MAC Address of the PC which you want to reserve an IP address for.
- **Reserved IP Address -** The IP address that the device reserved.
- **Status -** It 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 (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

To modify A Reserved IP address:

1. Select the reserved address entry as you desire, and modify it. If you wish to delete the entry, make all of the entry fields blank.
2. Click the **Save** button.

To delete all Reserved IP addresses:

Click the **Clear All** button.

Click the **Save** button

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

☞ **Note:**

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

3.7 System Tools

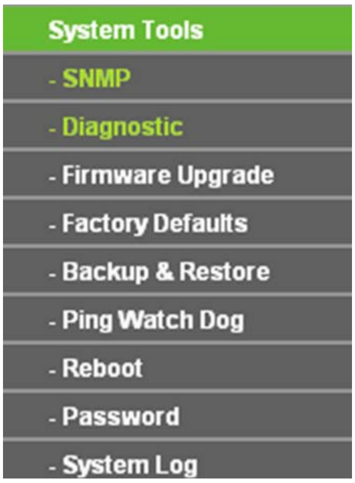
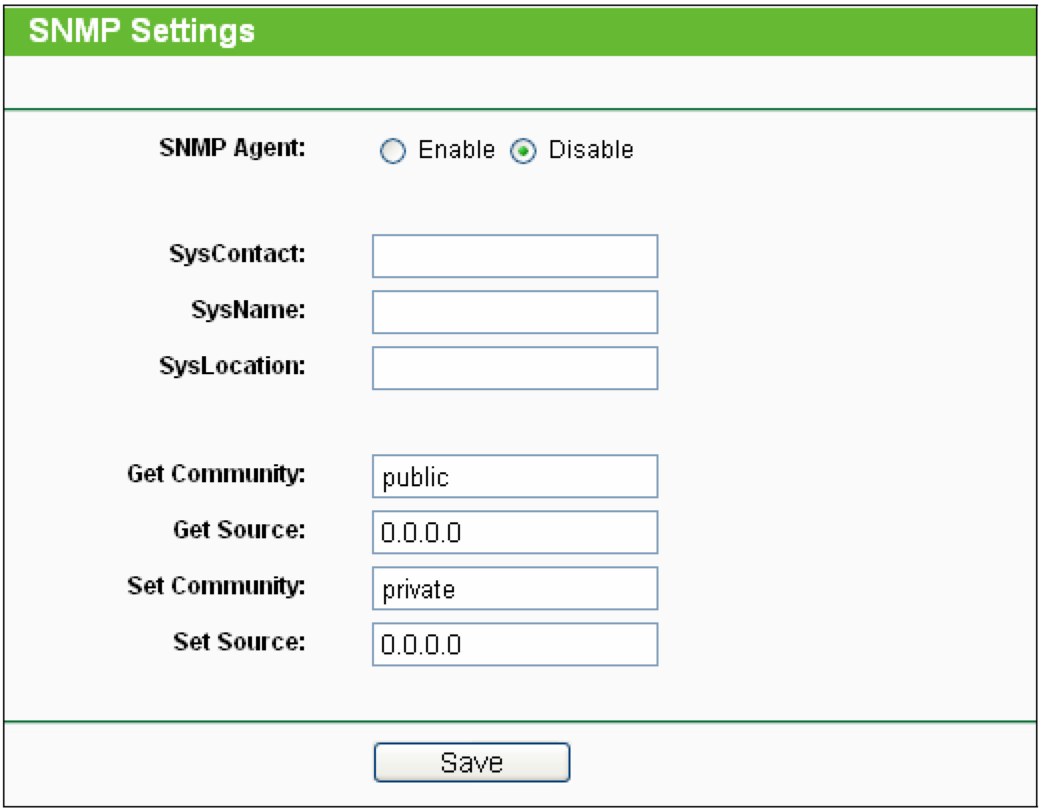


Figure 3-29 The System Tools menu

There are nine submenus under the System Tools menu (shown in Figure 3-29): **SNMP**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Reboot**, **Password**, **and System Log**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

3.7.1 SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol.



SNMP Settings

SNMP Agent: ○ Enable ● Disable

SysContact:

SysName:

SysLocation:

Get Community: public

Get Source: 0.0.0.0

Set Community: private

Set Source: 0.0.0.0

Figure 3-30 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.

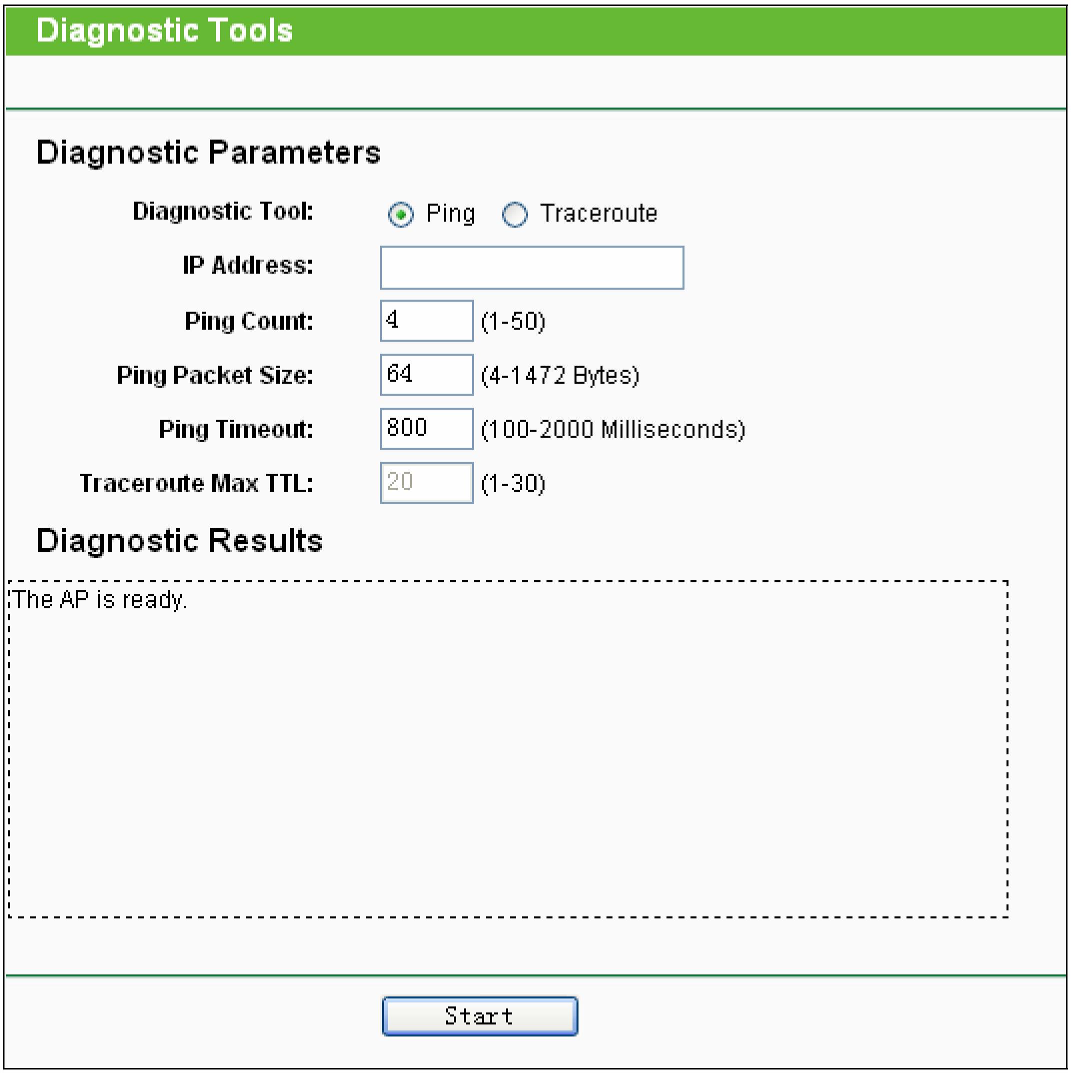
☞ **Note:**

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.

3.7.2 Diagnostic

The diagnostic tools (Ping and Traceroute) allow you to check the connections of your network components.



Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	● Ping ○ Traceroute
IP Address:	
Ping Count:	4 (1-50)
Ping Packet Size:	64 (4-1472 Bytes)
Ping Timeout:	800 (100-2000 Milliseconds)
Traceroute Max TTL:	20 (1-30)

Diagnostic Results

The AP is ready.

Figure 3-31 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.

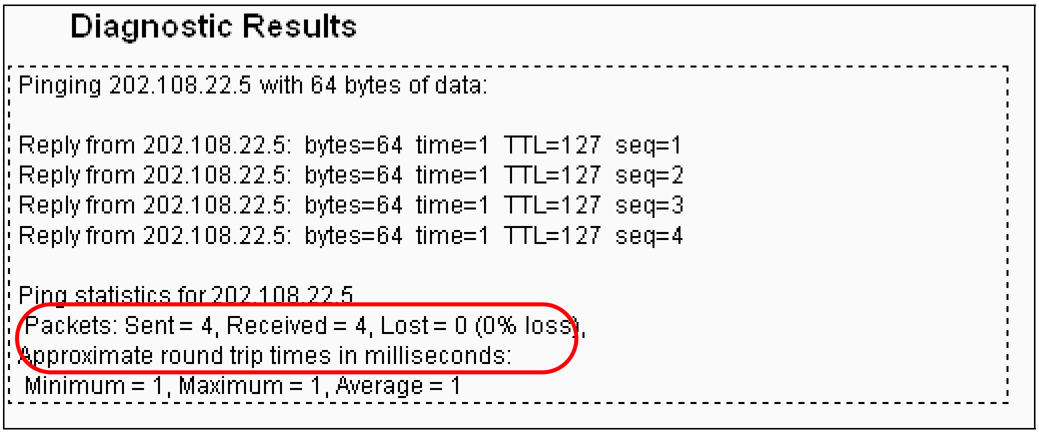
Ping Timeout - Specifies the time to wait for a response in milliseconds. The default is 800.

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.



Diagnostic Results

```
Pinging 202.108.22.5 with 64 bytes of data:

Reply from 202.108.22.5:  bytes=64  time=1  TTL=127  seq=1
Reply from 202.108.22.5:  bytes=64  time=1  TTL=127  seq=2
Reply from 202.108.22.5:  bytes=64  time=1  TTL=127  seq=3
Reply from 202.108.22.5:  bytes=64  time=1  TTL=127  seq=4

Ping statistics for 202.108.22.5
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
 Minimum = 1, Maximum = 1, Average = 1
```

Figure 3-32 Diagnostic Results

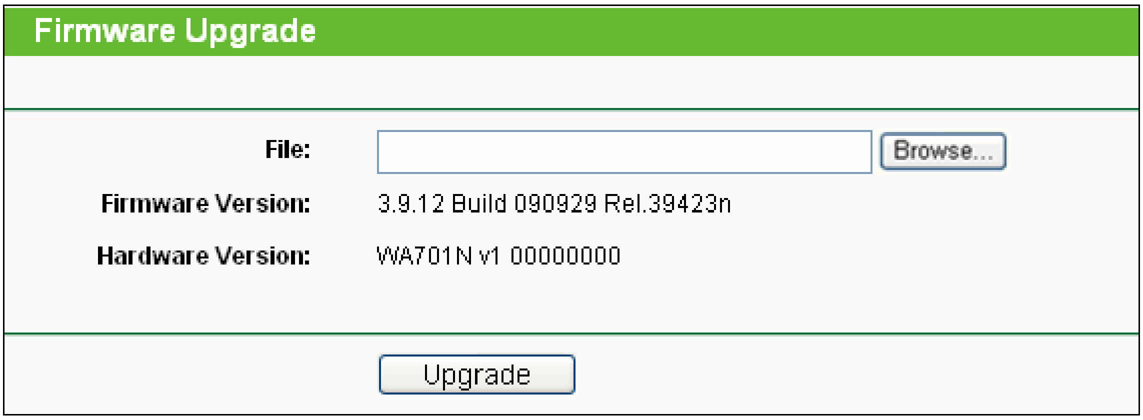
☞ **Note:**

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.

3.7.3 Firmware Upgrade

The page (shown in Figure 3-33) allows you to upgrade the latest version of firmware for the device.



File:

Firmware Version: 3.9.12 Build 090929 Rel.39423n

Hardware Version: WA701N v1 00000000

Figure 3-33 Firmware Upgrade

New firmware versions are posted at www.tp-link.com and can be downloaded for free.

- **Firmware Version -** Displays the current firmware version.
- **Hardware Version -** 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:

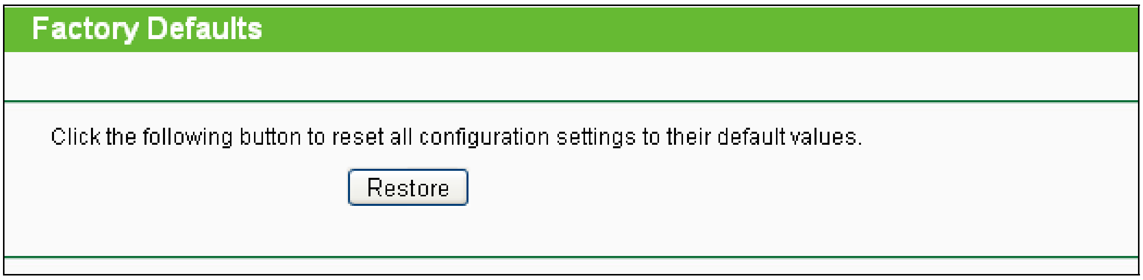
1. Download a more recent firmware upgrade file from the TP-LINK website (www.tp-link.com).
2. Enter the path name or click **Browse…** to select the downloaded file on the computer into the **File** blank.
3. Click the **Upgrade** button.

☞ **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.

3.7.4 Factory Defaults

This page (shown in Figure 3-34) allows you to restore the factory default settings for the device.



Factory Defaults

Click the following button to reset all configuration settings to their default values.

Figure 3-34 Restore Factory Defaults

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

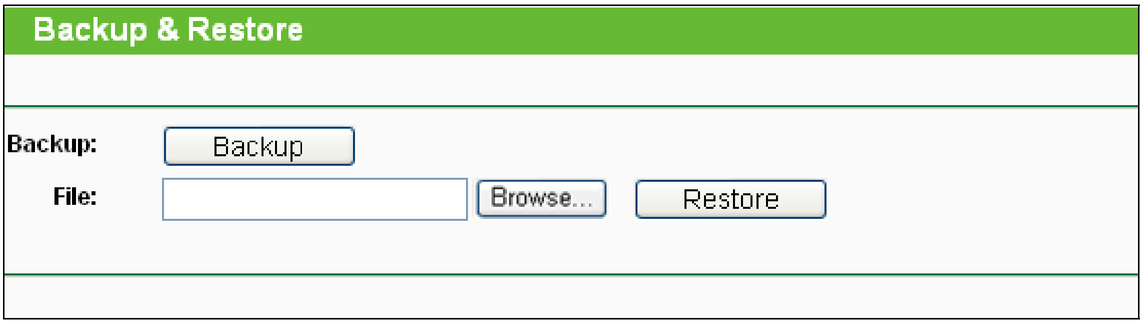
- Default **User Name**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.1.254
- Default **Subnet Mask**: 255.255.255.0

☞ **Note:**

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

3.7.5 Backup & Restore

This page (shown in Figure 3-35) allows you to save all configuration settings to your local computer as a file or restore the device's configuration.



Backup & Restore

Backup:

File:

Figure 3-35 Save or Restore the Configuration

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

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

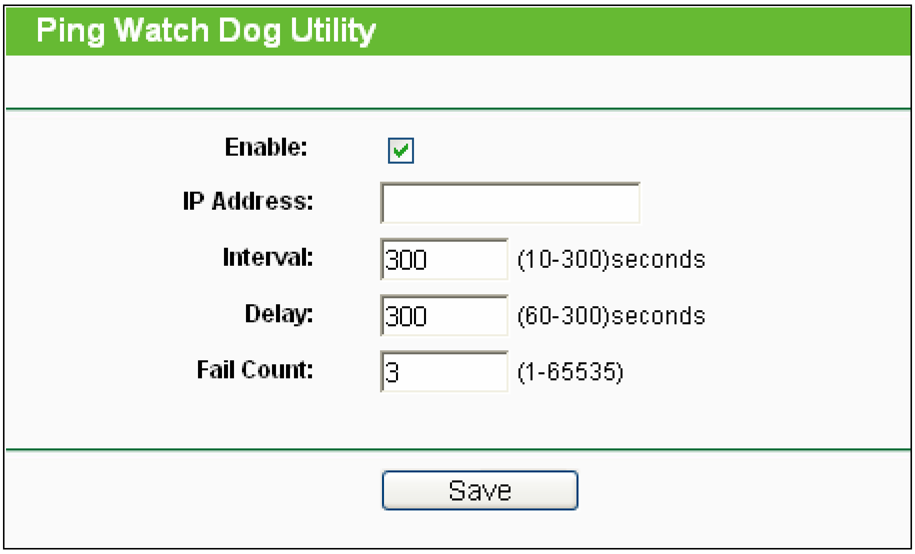
- Click the **Browse…** button to find the configuration file which you want to restore.
- Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

☞ **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the device will restart automatically then. Keep the power of the device on during the process, in case of any damage.

3.7.6 Ping Watch Dog

The **Ping Watch Dog** is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes 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.



Ping Watch Dog Utility

Enable: ☑

IP Address:

Interval: 300 (10-300)seconds

Delay: 300 (60-300)seconds

Fail Count: 3 (1-65535)

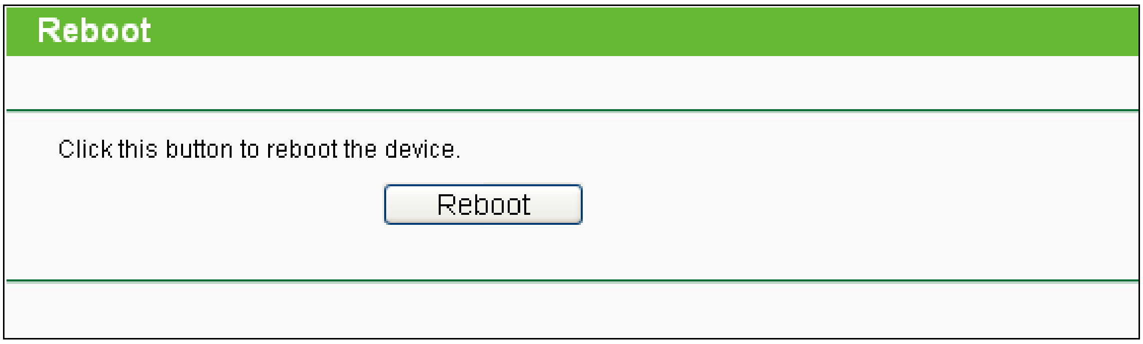
Figure 3-36 Ping Watch Dog Utility

- **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 internal 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.

3.7.7 Reboot

This page (shown in Figure 3-37) allows you to reboot the device.



Reboot

Click this button to reboot the device.

Figure 3-37 Reboot the device

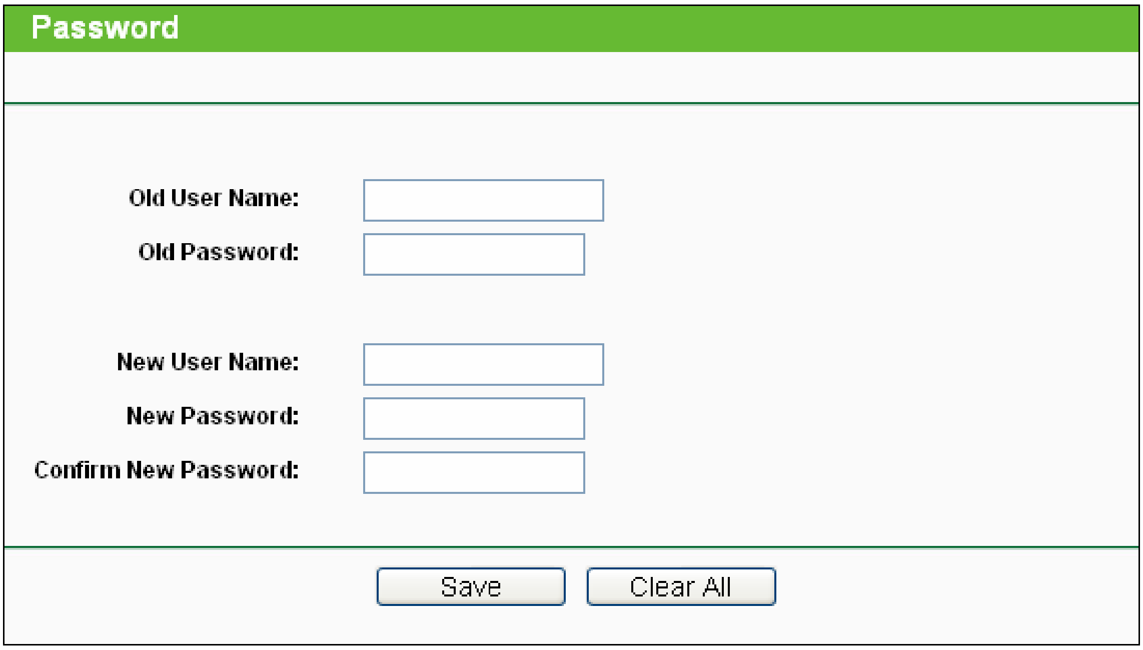
Click the **Reboot** button to reboot the device.

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).

3.7.8 Password

This page (shown in Figure 3-38) allows you to change the factory default user name and password of the device.



Old User Name:
Old Password:
New User Name:
New Password:
Confirm New Password:

Figure 3-38 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 utility will be prompted for the device's user name and password.

☞ **Note:**

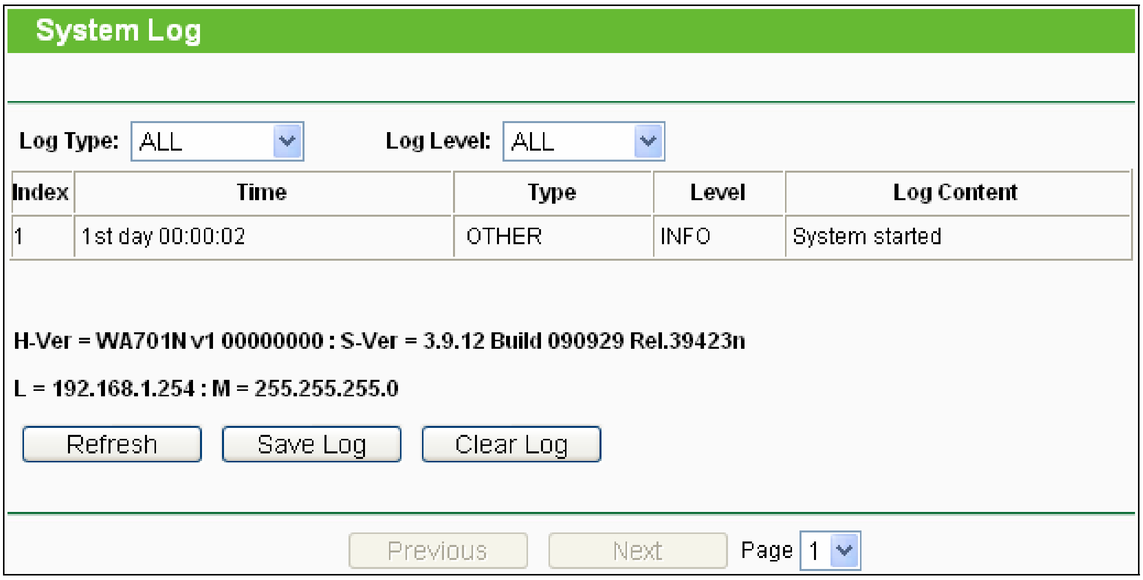
The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

3.7.9 System Log

This page (shown in Figure 3-39) allows you to query the Logs of the device.



System Log

Log Type: ALL

Log Level: ALL

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

H-Ver = WA701N v1 00000000 : S-Ver = 3.9.12 Build 090929 Rel.39423n

L = 192.168.1.254 : M = 255.255.255.0

Page 1

Figure 3-39 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: 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.

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 (**D**omain **N**ame **S**ystem) **–** 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 (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.

DSL (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.

ISP (**I**nternet **S**ervice **P**rovider) **-** 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 **S**ervice **S**et **Id**entification 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 (**W**ired **E**quivalent **P**rivacy) **-** 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 trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) **-** 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 **A**ccess**) -** 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.

Appendix B: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11b and 802.11g, TCP/IP, DHCP
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive PoE
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 150Mbps（Automatic） 11g：54/48/36/24/18/12/9/6M（Automatic） 11b：11/5.5/2/1M（Automatic）
Channels	13
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	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
RF Power	20dBm(max)
Antenna Gain	3dBi
Physical and Environment	
Working Temperature	0℃~40℃ (32℉~104℉)
Working Humidity	10% ~ 90% RH, Non-condensing
Storage Temperature	-40℃~70℃(-40℉~158℉)
Storage Humidity	5% ~ 90% RH, Non-condensing

Appendix C: FAQ

1. No lights are lit on the access point.

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point if the access point has no power.

1) Make sure the power cord is connected to the access point.
2) Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
3) Make sure you are using the correct TP-LINK power adapter supplied with your access point.

2. The LAN light is not lit.

There is a hardware connection problem. Check these 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) Be 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 cannot access the device with a wireless capable computer.

There is a configuration problem. Check these items:

1) You may not have restarted the computer with the wireless adapter to have 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 that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to “Obtain an IP address automatically.”
3) The access point’s default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.