TP-LINK®

User Guide

TL-WA701ND

150Mbps Wireless Lite N Access Point

Rev: 2.0.3
1910010372

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.

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

FCC RF Radiation Exposure Statement

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

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

CE Mark Warning

CE 1588 ⓘ

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

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 V2.1.1:2009

EN60950-1:2006

Recommendation 1999/519/EC

EN62311:2008

Directives 2004/108/EC

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

EN 55022:2006 +A1:2007

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

EN 61000-3-2:2006

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

Directives 2006/95/EC

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

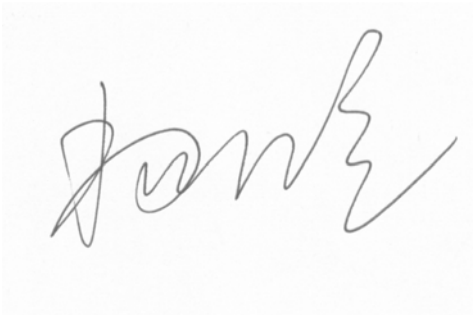
EN60950-1:2006

Directive（ErP） 2009/125/EC

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

EN62075:2008

Person is responsible for marking this declaration:

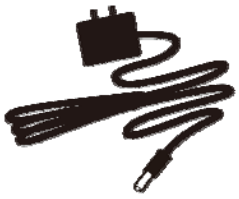


Yang Hongliang
Product Manager of International Business

TP-LINK TECHNOLOGIES CO., LTD.
South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan,
Shenzhen, P. R. China

CONTENTS

Package Contents

	TL-WA701ND 150Mbps Wireless Lite N Access Point
	Resource CD, including: ● This User Guide ● Other Helpful Information
	Power Adapter for TL-WA701ND 150Mbps Wireless Lite N Access Point
	Power Injectors
	Ethernet Cables
	Quick Installation Guide
	PoE Guide

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.

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.

Overview of This Guide

Package Contents:	Tells what are contained in the box.
Chapter 1 Introduction:	Gives an introduction for the TL-WA701ND 150Mbps Wireless Lite N Access Point.
1.1 Product Overview:	Introduces advantages of using this AP.
1.2 Main Feature:	Introduces main features and their benefits.
1.3 Appearance:	Gives descriptions of LEDs, ports and buttons on the front and rear panel.
Chapter 2 Hardware Installation:	Tells how to connect the AP and the requirements.
2.1 Before You Begin:	Gives suggestions for better performance of the wireless network.
2.2 Basic Requirement:	Introduces some basic requirements for successful installation and long-term use
2.3 Connecting the Device:	Introduces steps to connect the AP.
Chapter 3 Configure the PC:	Tells how to configure the IP address of your PC in order to access the AP.
Chapter 4 Configure the Device:	Tells how to configure the AP via the web-based management page.
4.1 Login:	Tells how to log on to the web-based management page.
4.2 Status:	Gives information about the AP's current configuration.
4.3 QSS	Guides how to add a new wireless device to an existing network quickly.
4.4 Network:	Tells how to configure the IP parameters of AP.
4.5 Wireless:	Guides to establish the wireless network in different wireless modes and deploy the security features appropriate to your needs.
4.6 DHCP:	Introduces how to set your AP to be a DHCP server so that the AP will automatically assign an IP address for your PC.
4.7 System Tools:	Provides some useful tools.

Chapter 1 Introduction

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

1.1 Product Overview

The TL-WA701ND 150Mbps Wireless Lite N Access Point is dedicated to Small Office/Home Office (SOHO) wireless network solutions. It allows for greater range and mobility within your wireless network while also allowing you to connect the wireless devices to a wired environment. Increased mobility and the absence of cabling will be beneficial for your network.

With using IEEE 802.11n wireless technology, your device can transmit wireless data at the rate of up to 150Mbps. With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi protected Access (WPA2- PSK, WPA- PSK), the TL-WA701ND 150Mbps Wireless Lite N Access Point delivers complete data privacy. 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.

It supports an easy, web-based setup for installation and management. Even though you may not be familiar with the Access Point, you can easily configure it with the help of this Guide. Before installing the AP, please look through this Guide to get the full information of the TL-WA701ND 150Mbps Wireless Lite N Access Point.

1.2 Main Features

Features	Benefits
Make use of IEEE 802.11n wireless technology	Allows your device to transmit wireless data at the rate of up to 150Mbps
Provides multiple encryption security Types including: 64/128/152-bit WEP WPA/WPA2 WPA-PSK/WPA2-PSK	Secures your data while the data packets are being transmitted
Supports Built-in DHCP server	Supports dynamic IP address distributing
Supports MAC address filtering	Allows you to control the access rights of the wireless stations, depending on the stations' MAC addresses
Supports multiple operating modes including: ● Access Point	Makes the AP an ideal solution for your wireless local area network You can create a wireless local area network
● Multi-SSID	Allows the wireless adapter to access to different LANs appropriate to your needs by connecting to different SSID
● Client	Wirelessly connects Ethernet devices
● Repeater（Universal Repeater）	Relays signal between its stations and the root AP for greater wireless range
● Bridge with AP (Point to Point, Point to Multi-point)	Bridges the AP and another AP also in bridge mode to connect two or more wired LANs
Supports Firmware Upgrade	You can easily upgrade the firmware to the latest version through the web-based management page
Supports Remote and Web management	Allows you to manage your wireless LAN easily through the web-based management page, while the management by remote computer is also available

1.3 Appearance

1.3.1 The Front Panel

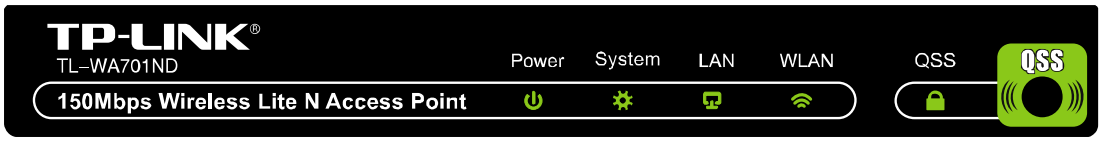


Figure 1-1

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

LED Explanation

Name	Status	Indication
Power	Off	No Power
	On	Power on
System	Off	The device has a system error
	On	The device is initialising
	Flashing	The device is working properly
LAN	Off	There is no device linked to the corresponding port
	On	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
WLAN	Off	The Wireless function is disabled
	Flashing	The Wireless function is enabled
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 1-1

1.3.2 The Rear Panel

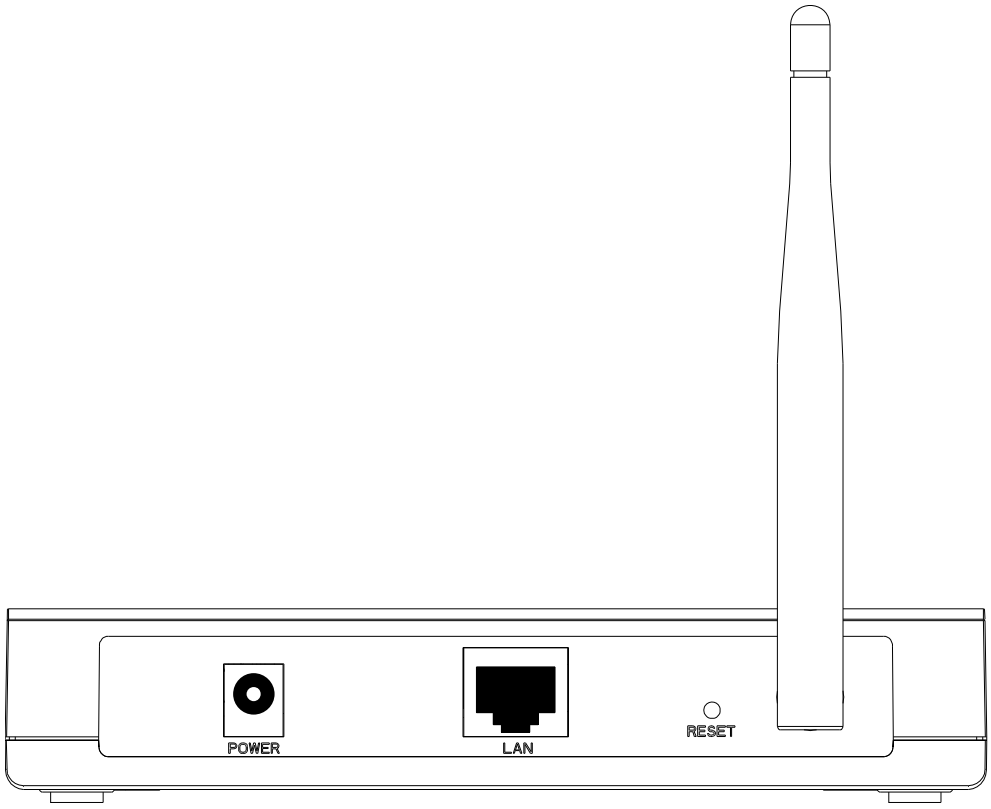


Figure 1-2

Viewed from left to right, the following parts are located on the rear panel of TL-WA701ND.

POWER: The power port connects to the power adapter provided with the TL-WA701ND 150Mbps Wireless Lite N Access Point.

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

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

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

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

☞ **Note:**

Ensure the AP is powered on before it restarts completely.

Chapter 2 Hardware Installation

2.1 Before You Begin

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

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

1). Avoid redundant obstacles and interference between the wireless devices.

2). Keep your AP away from appliances with a strong electric field or magnetic field, such as a microwave oven or refrigerator.

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

2.2 Basic Requirements

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

2.3 Connecting the Device

Figure 2-1 is an example of the typical application of TL-WA701ND in the infrastructure network. An Infrastructure network contains an access point or a wireless router.

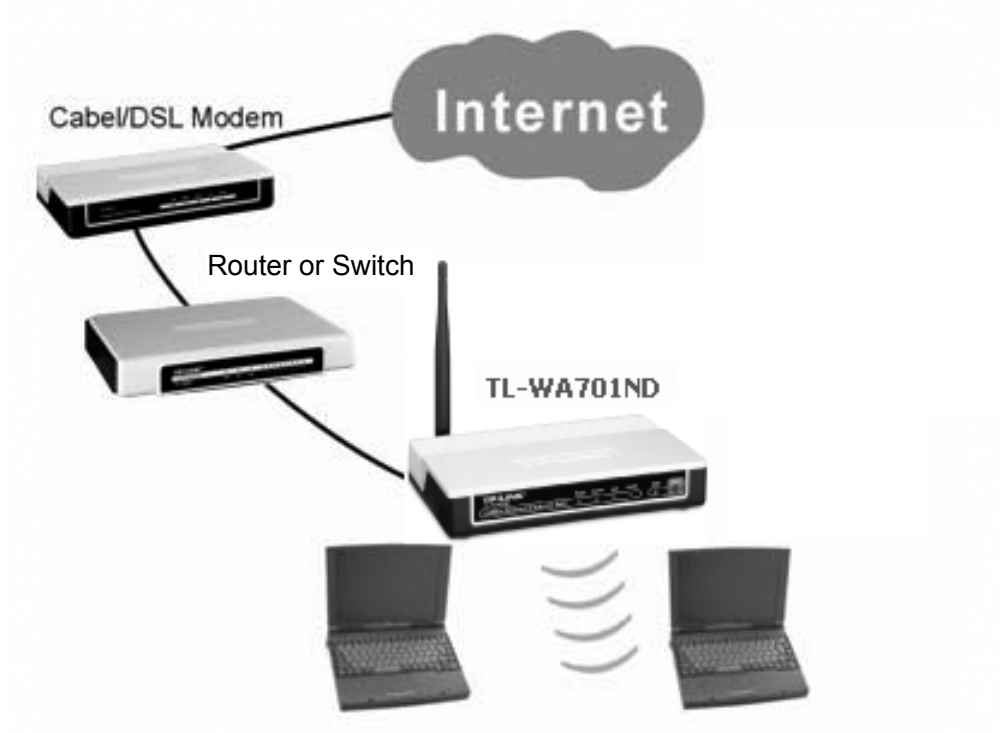


Figure 2-1 The Example of Infrastructure Network Incorporating the TL-WA701ND

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

1. Connect the Cable or DSL modem to a Router.
2. Locate an optimum location for the AP. The best place is usually near the center of the area in which your PC(s) will wirelessly connect.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the Ethernet Broadband Router to the TL-WA701ND Access Point. Power on the AP.
5. Then you can connect a desktop PC or laptop to your network. (Make sure your computer or laptop is equipped with a Wireless Adapter.)

☞ **Note:**

If you are not so clear about how to connect your devices to the network, please refer to **Appendix A Application Example**.

Chapter 3 Configure the PC

This chapter will guide you to configure your PC to communicate with the AP. The wireless adapter-equipped computers in your network must be in the same IP Address range without overlap with each other. Manually configure the **IP address** as 192.168.1.* (* is any integer between 1 to 253), and the **Subnet mask** as 255.255.255.0 for your PC by following the instructions below.

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

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

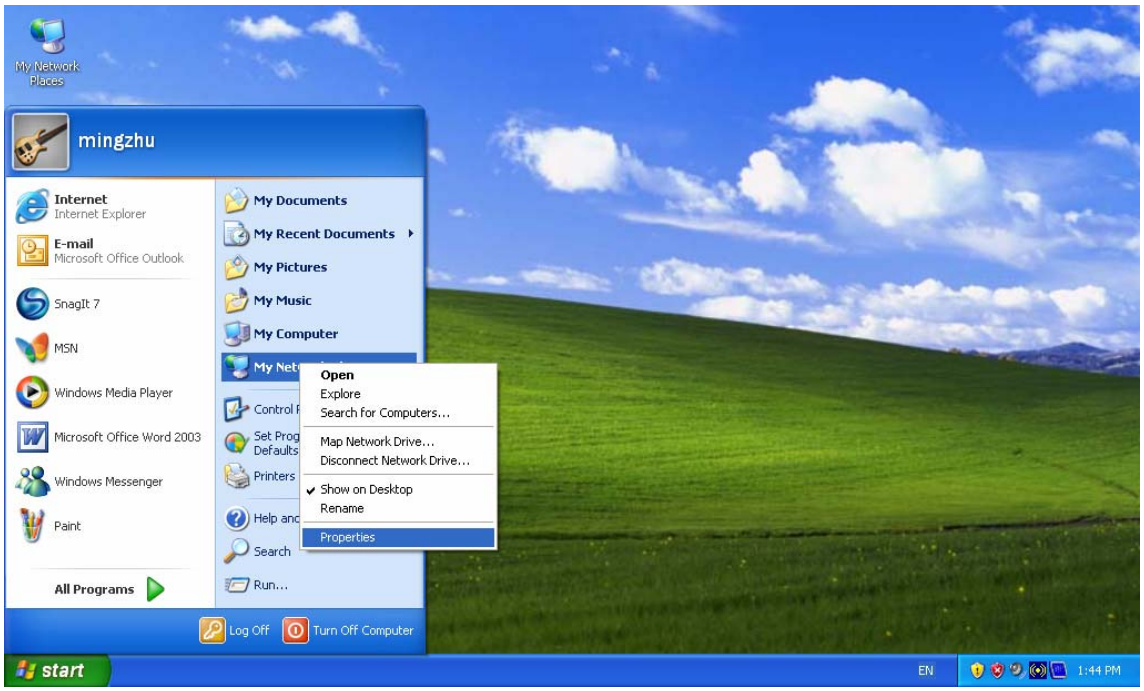


Figure 3-1

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

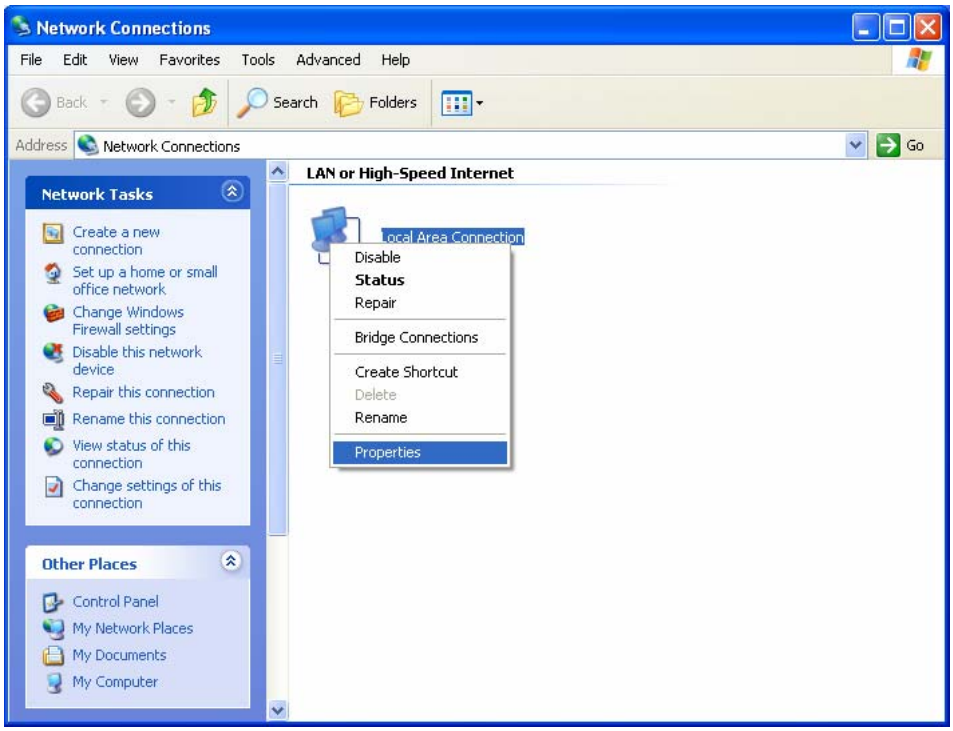


Figure 3-2

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

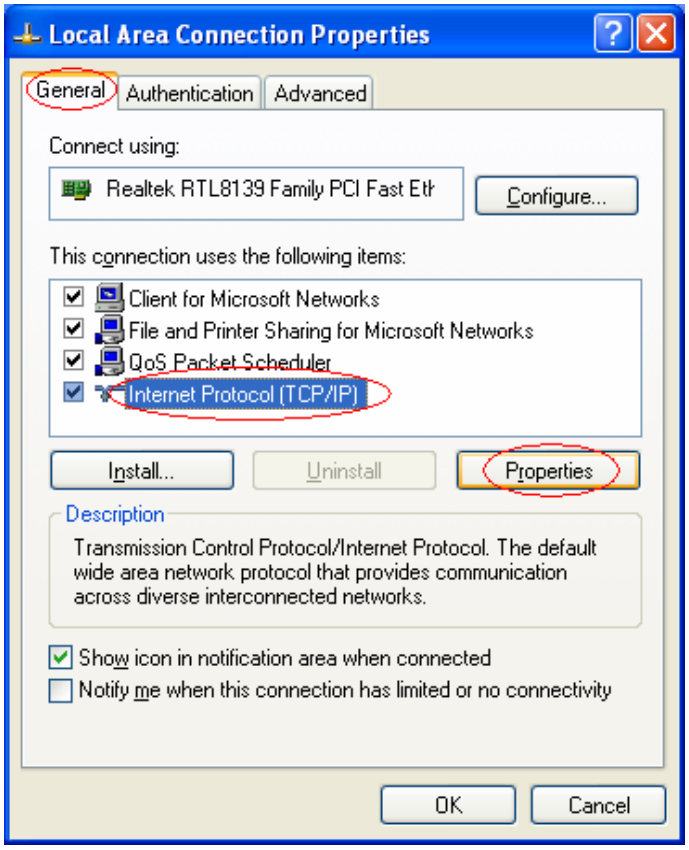


Figure 3-3

4. Configure the IP address manually.

   1) Select **Use the following IP address**.

   2) Enter 192.168.1.* (* is any integer between 1 to 253) into the **IP address** filed, 255.255.255.0 into the **Subnet mask** filed.

   3) Click **OK** to keep your settings.

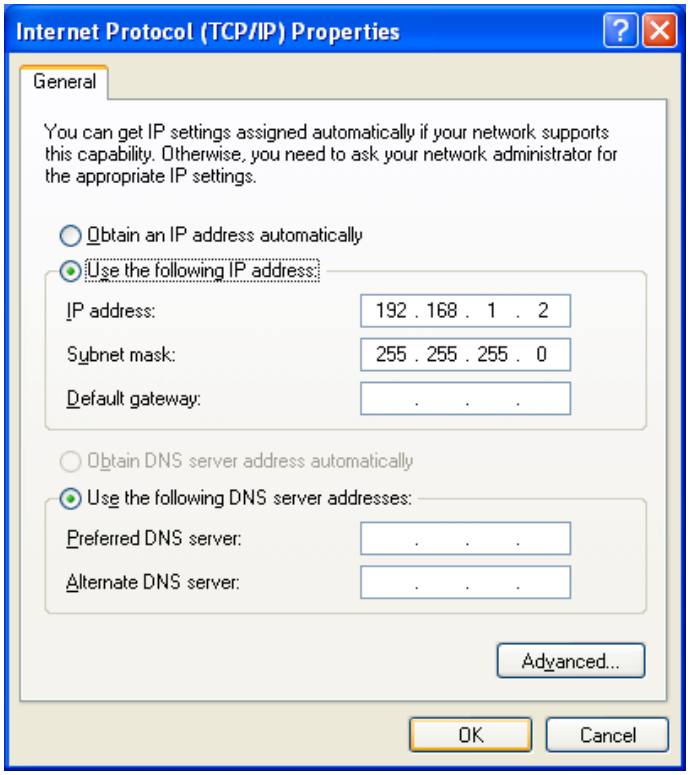


Figure 3-4

5. Verify the network connection between your PC and the AP via the *Ping* command. The following example is in Windows XP Operating System.

   1) Click **Start > Run** tab. Enter **cmd** in the filed and click **OK**.

   2) Type *ping 192.168.1.254* on the screen that displays and then press **Enter**.

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

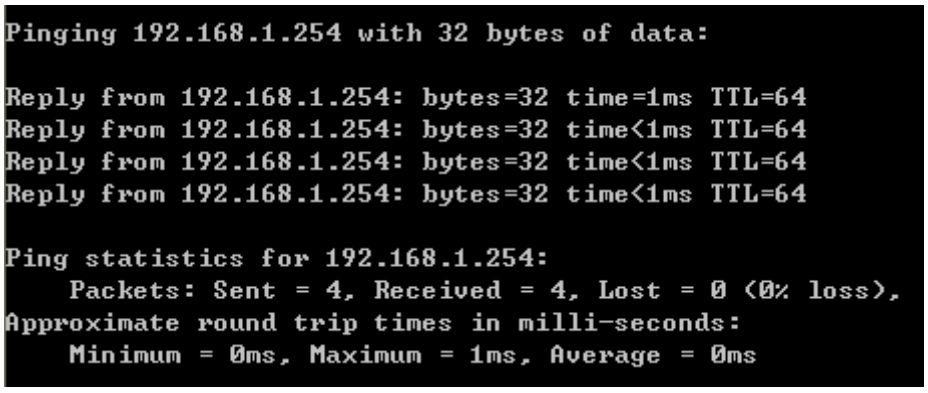


Figure 3-5

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

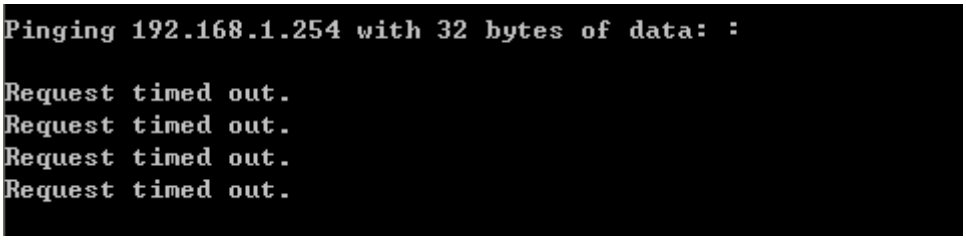


Figure 3-6

Please check following these steps:

a) Check to see if your PC and the AP are right connected. The LED of LAN port which you link to on the device and the LED on your PC's adapter should be lit up.

b) Make sure the TCP/IP for your PC is right configured. If the AP's IP address is 192.168.1.254, your PC's IP address must be within the range of 192.168.1.1 ~ 192.168.1.253.

Chapter 4 Configure the Device

This Chapter describes how to configure your Access Point via the web-based management page. The TL-WA701ND 150Mbps Wireless Lite N Access Point is easy to configure and manage with the Web-based (Internet Explorer, Netscape® Navigator, Firefox, Safari, Opera or Chrome) management page, which can be launched on any windows, Macintosh or UNIX OS with a web browser.

4.1 Login

Open your web browser. Type in IP address *http://192.168.1.254* in the address field of web browser and press Enter.

Figure 4-1 Login to the AP

Enter **admin** for the User Name and Password (both in lower case letters) in Figure 4-2 below. Then click **OK** or press Enter.

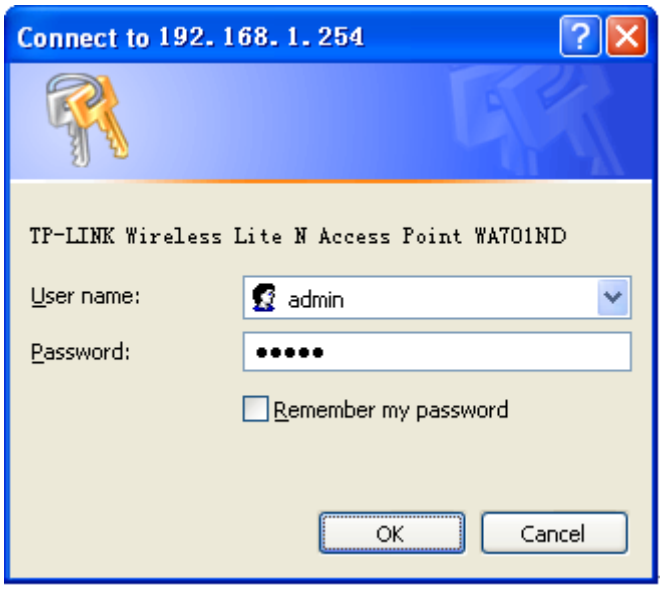


Figure 4-2 Login Windows

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

4.2 Status

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

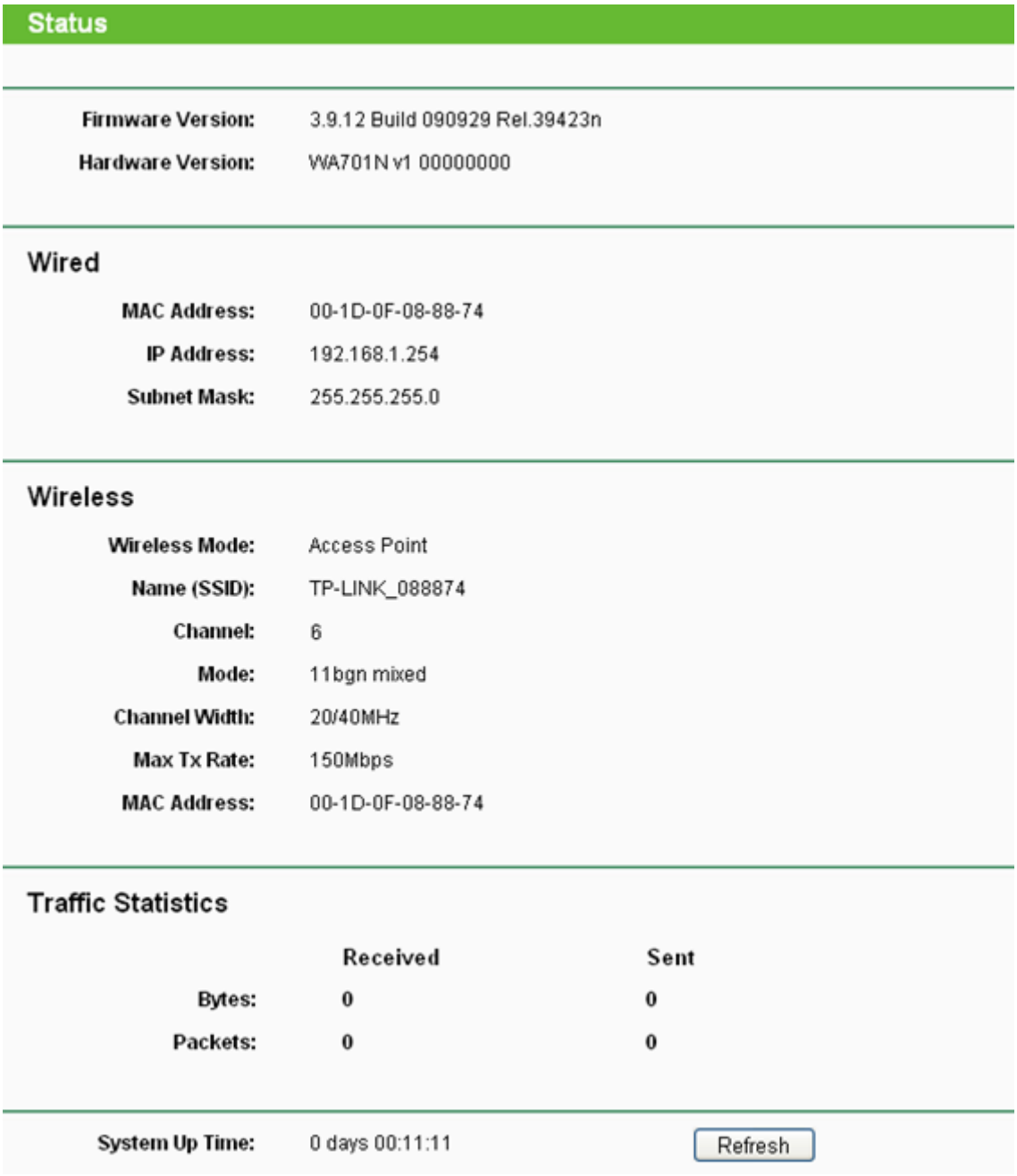
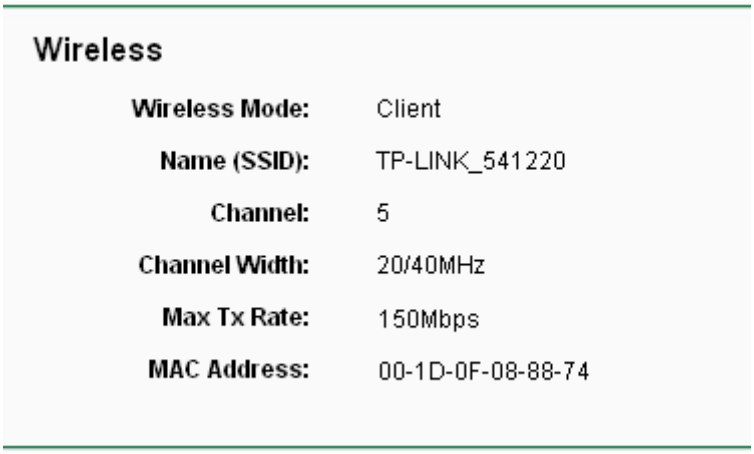


Figure 4-3 Device Status

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

Note:

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



4.3 QSS

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

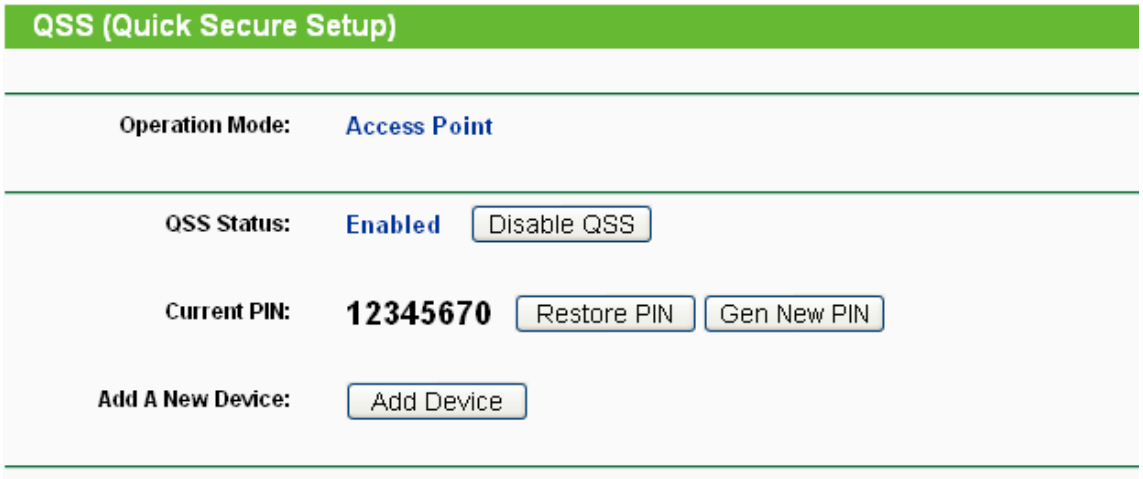


Figure 4-4 QSS

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

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.

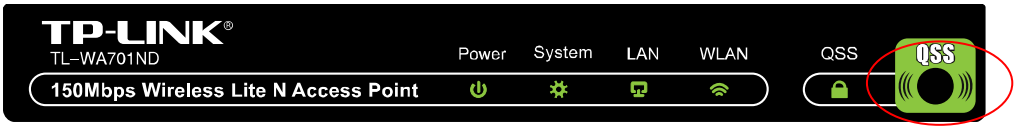
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

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.

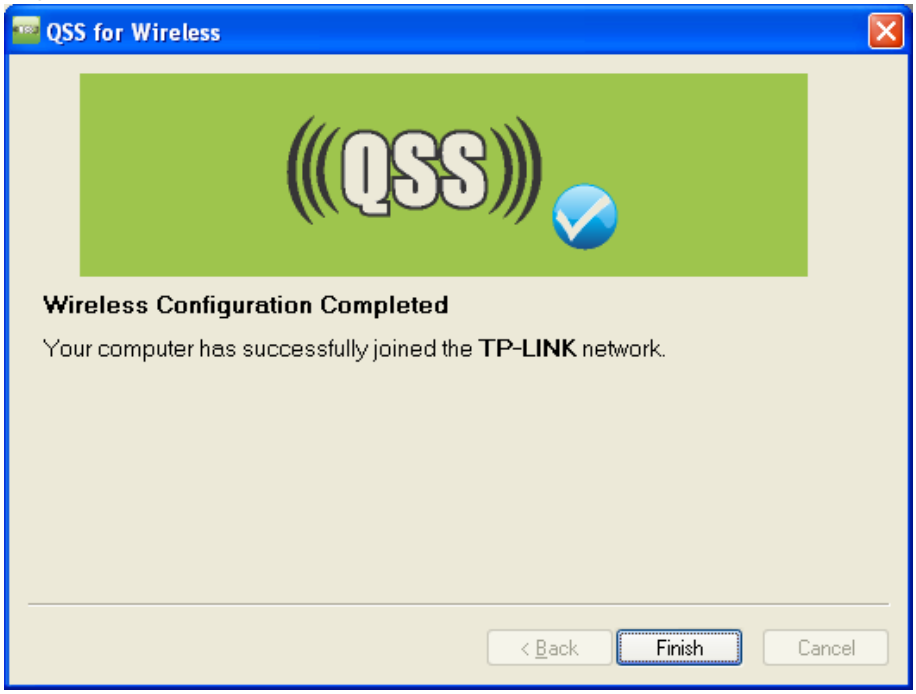
Method One:

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.

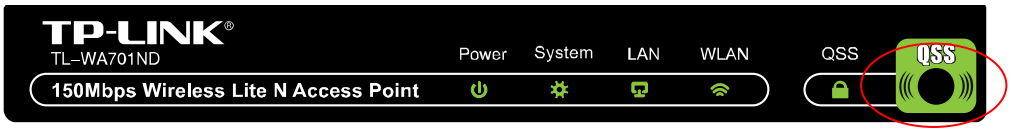
Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



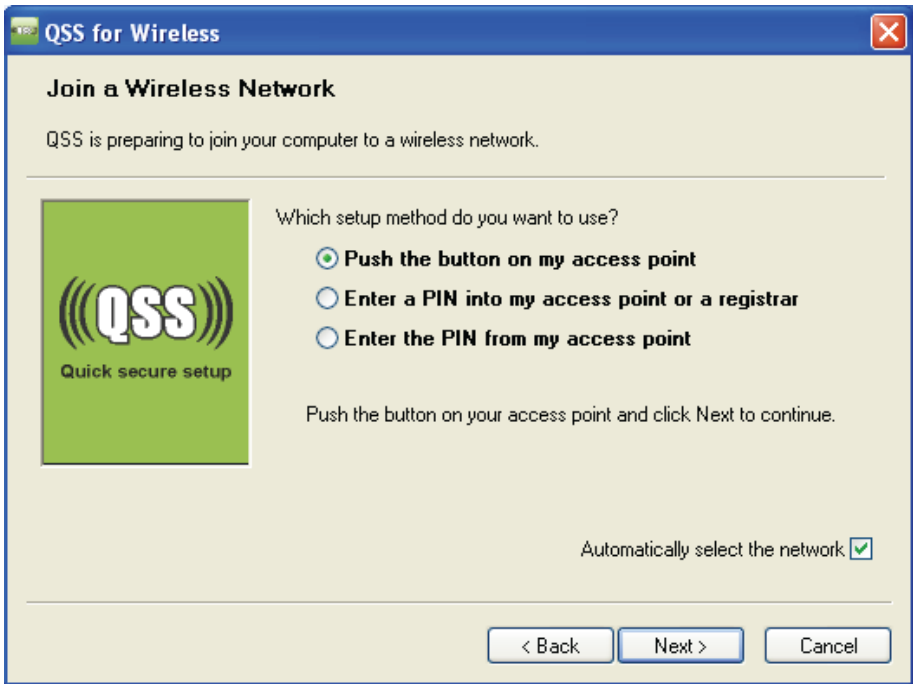
The QSS Configuration Screen of Wireless Adapter

Method Two:

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

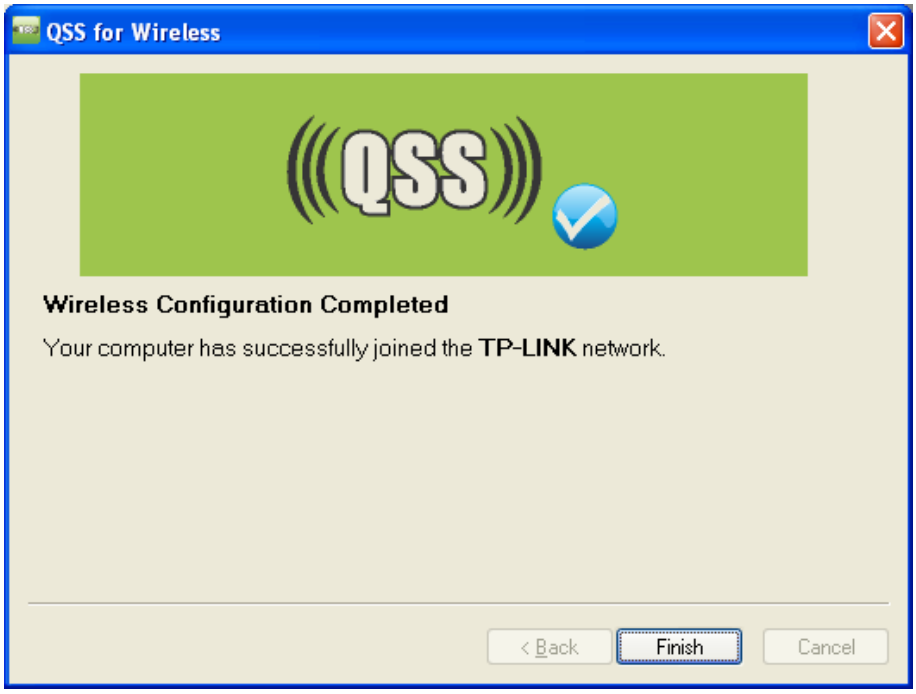


Step 2: For the configuration of the wireless adapter, please choose "**Push the button on my access point**" in the configuration utility of the QSS as below, and click **Next**.



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.



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 4-4, then the following screen will appear.

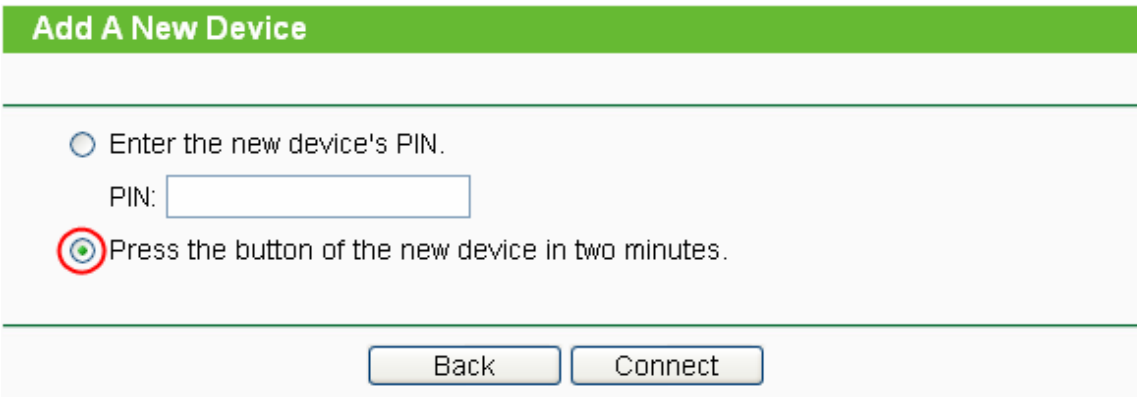
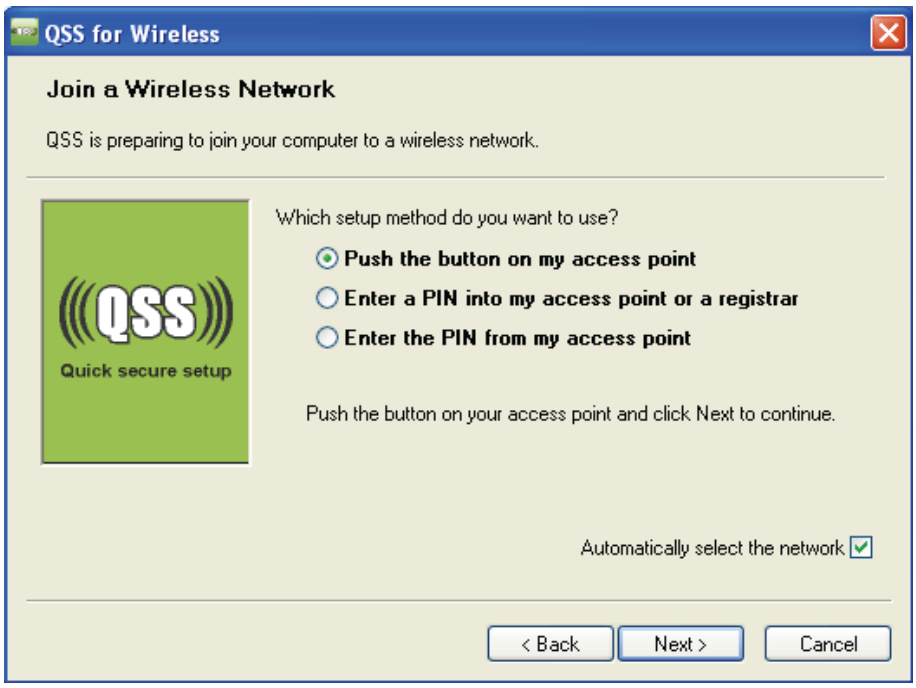


Figure 4-5 Add A New Device

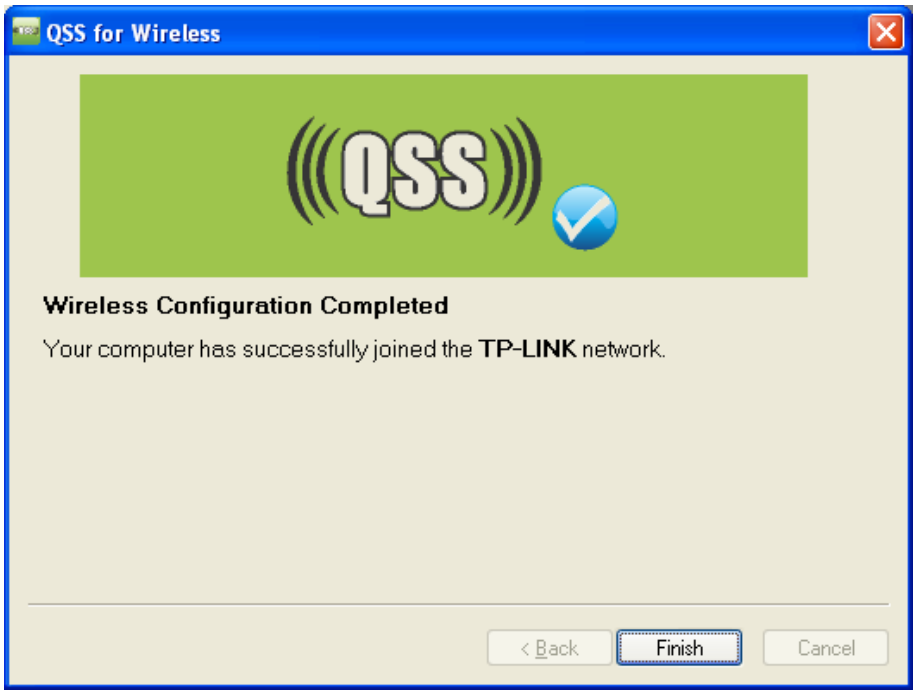
Step 2: Choose "**Press the button of the new device in two minutes**" and click **Connect**.

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**.



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.



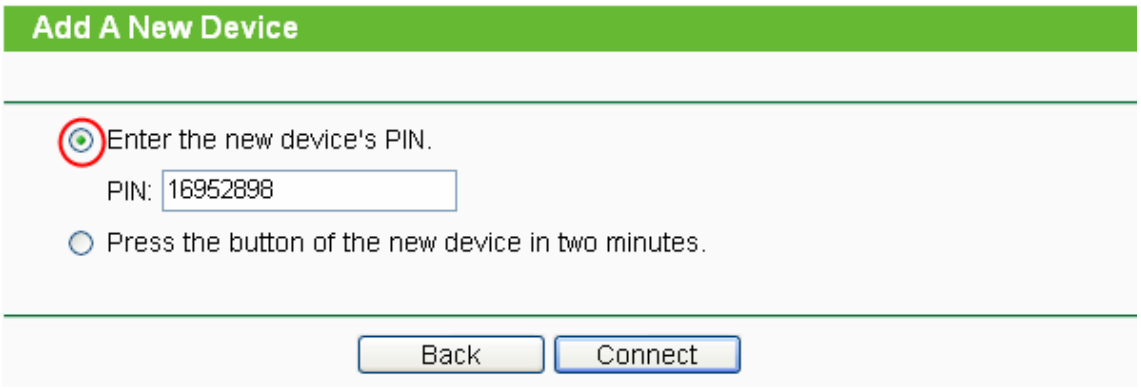
The QSS Configuration Screen of Wireless Adapter

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 4-4, then the following screen will appear.

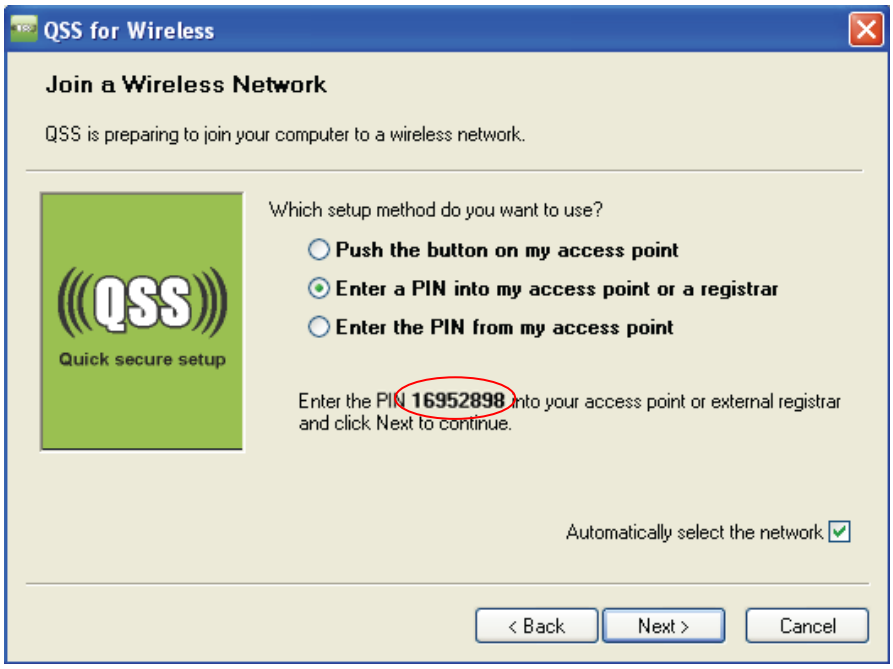


Step 2: Choose "**Enter the new device's PIN**" and enter the PIN code （take 16952898 for example）of the wireless adapter in the field after **PIN** as shown in the figure above. Then click **Connect.**

☞ **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.**



The QSS Configuration Screen of Wireless Adapter

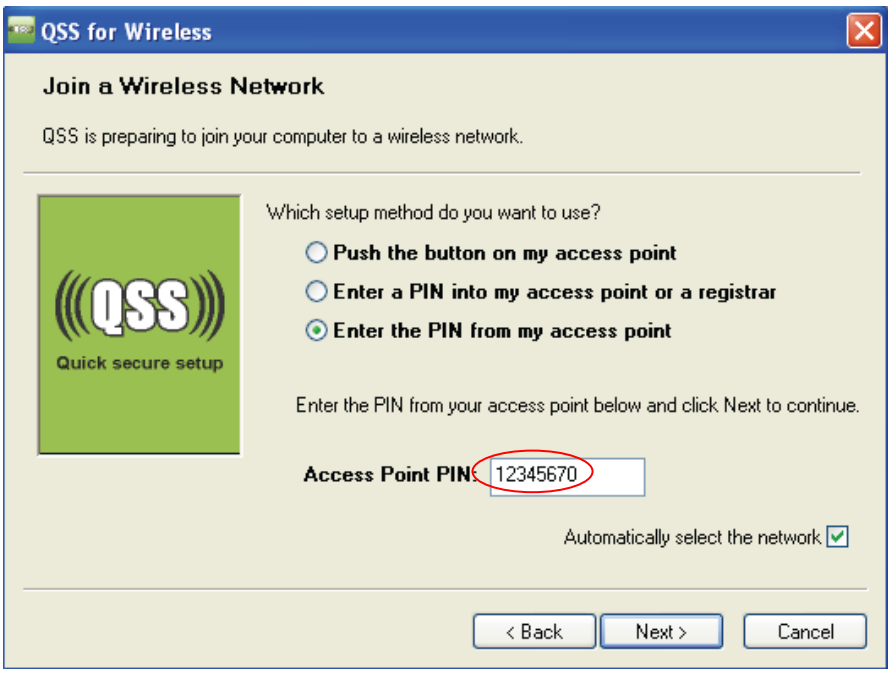
Note:

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 4-4 (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**.

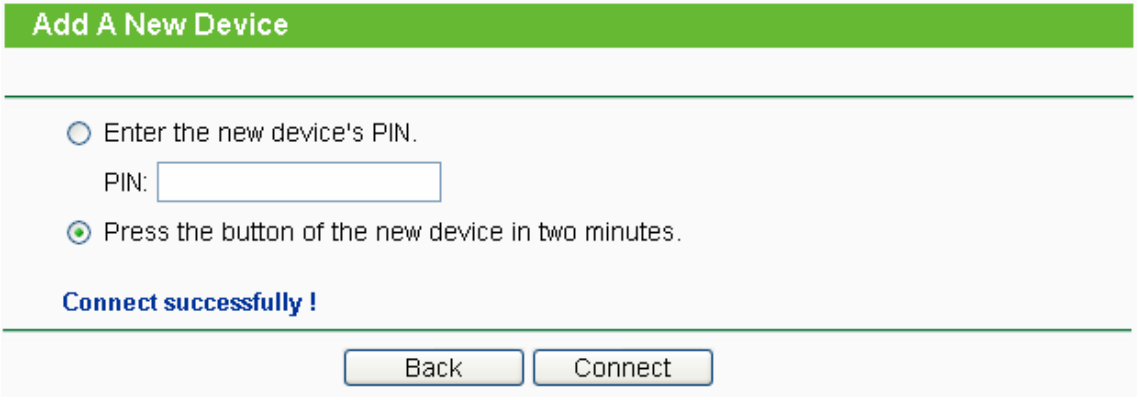


The QSS Configuration Screen of Wireless Adapter

Note:

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

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



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.

4.4 Network

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

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

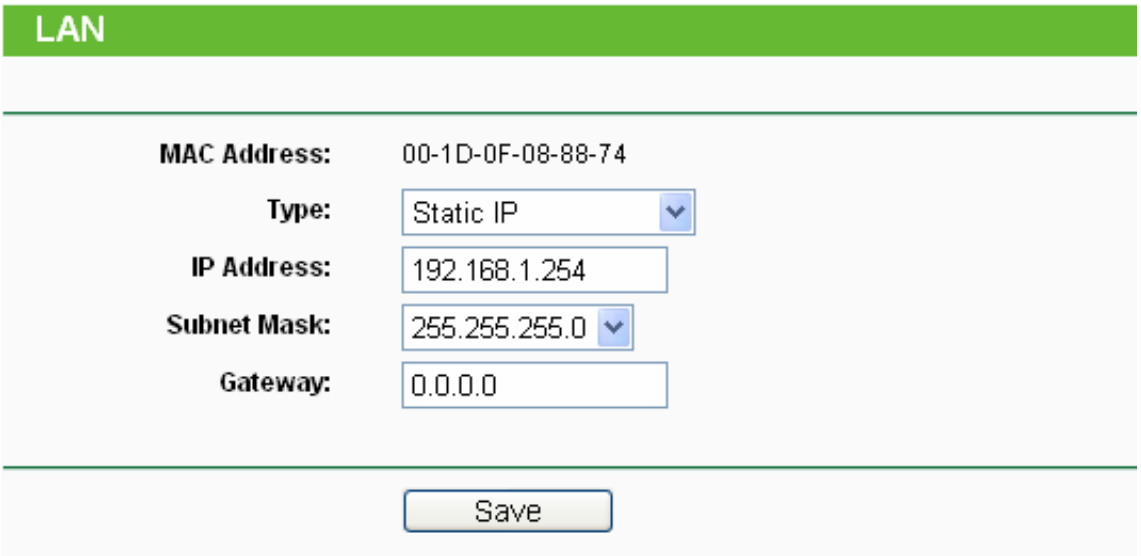


Figure 4-6 Network

- **Type -** Select **Dynamic IP** to get IP address from DHCP server or select **Static IP** to configure IP address manually from the drop-down list.
- **IP Address -** Enter the IP address of your AP in dotted-decimal notation (factory default setting is 192.168.1.254).

- **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. The value can't be changed.

Note:

1 If you change the IP Address, you must use the new IP Address to log in the AP.

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

4.5 Wireless

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

There are six submenus under the Wireless menu (shown in Figure 4-7): **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.

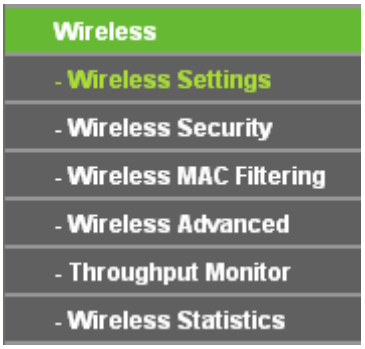


Figure 4-7 Wireless menu

4.5.1 Wireless Settings

Selecting **Wireless** > **Wireless Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 4-8).This page allows you to configure the wireless mode for your device. 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.

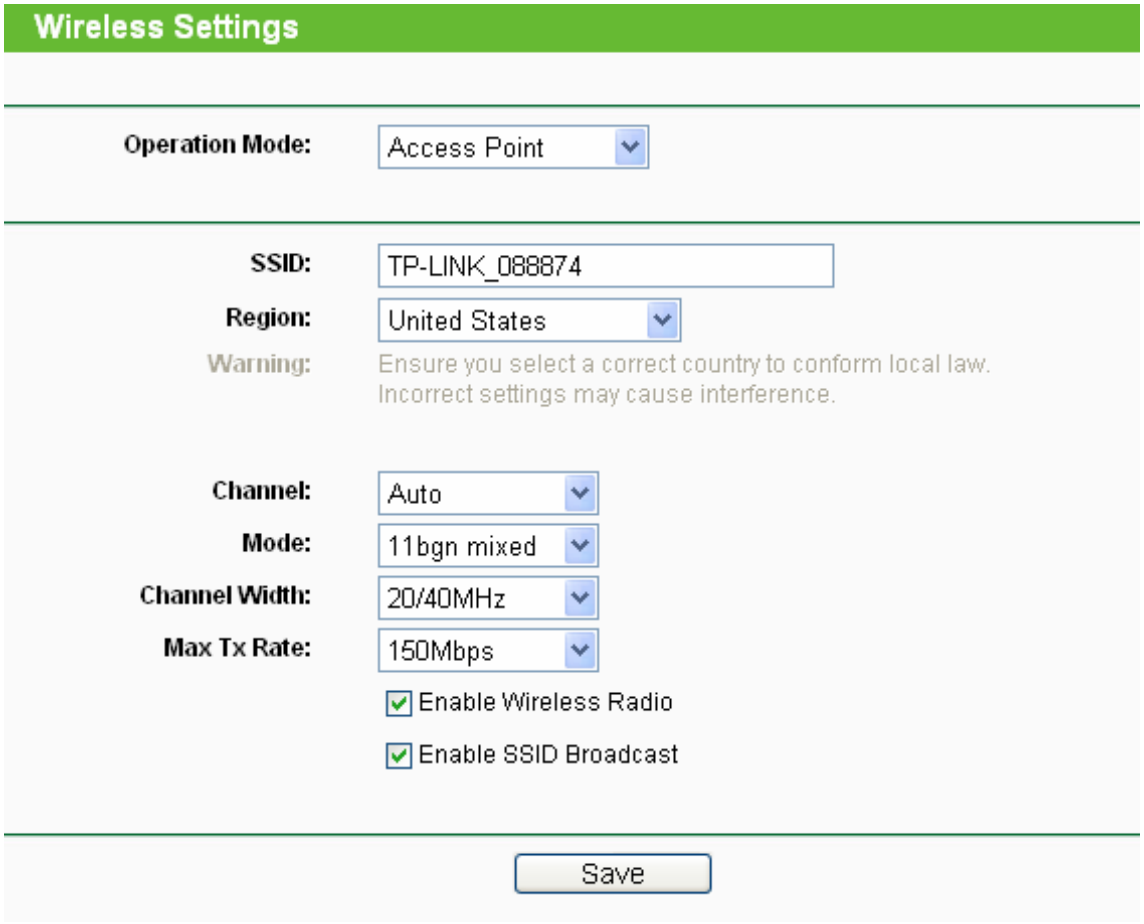


Figure 4-8 Wireless Settings in Access Point mode

- **SSID** (Set Service Identifier) **-** Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-LINK_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region -** 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**.

Note Dialog

Note:

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

- **Channel -** Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** Select the desired wireless mode. The options are:
  - **11b only -** Only 802.11b wireless stations can connect to the device.
  - **11g only -** Only 802.11g wireless stations can connect to the device.
  - **11n only -** Only 802.11n wireless stations can connect to the device.
  - **11bg mixed -** Both 802.11b and 802.11g wireless stations can connect to the device.
  - **11bgn mixed -** All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

☞ **Note:**

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

2) Multi-SSID: This mode allows the device to support up to four SSIDs.

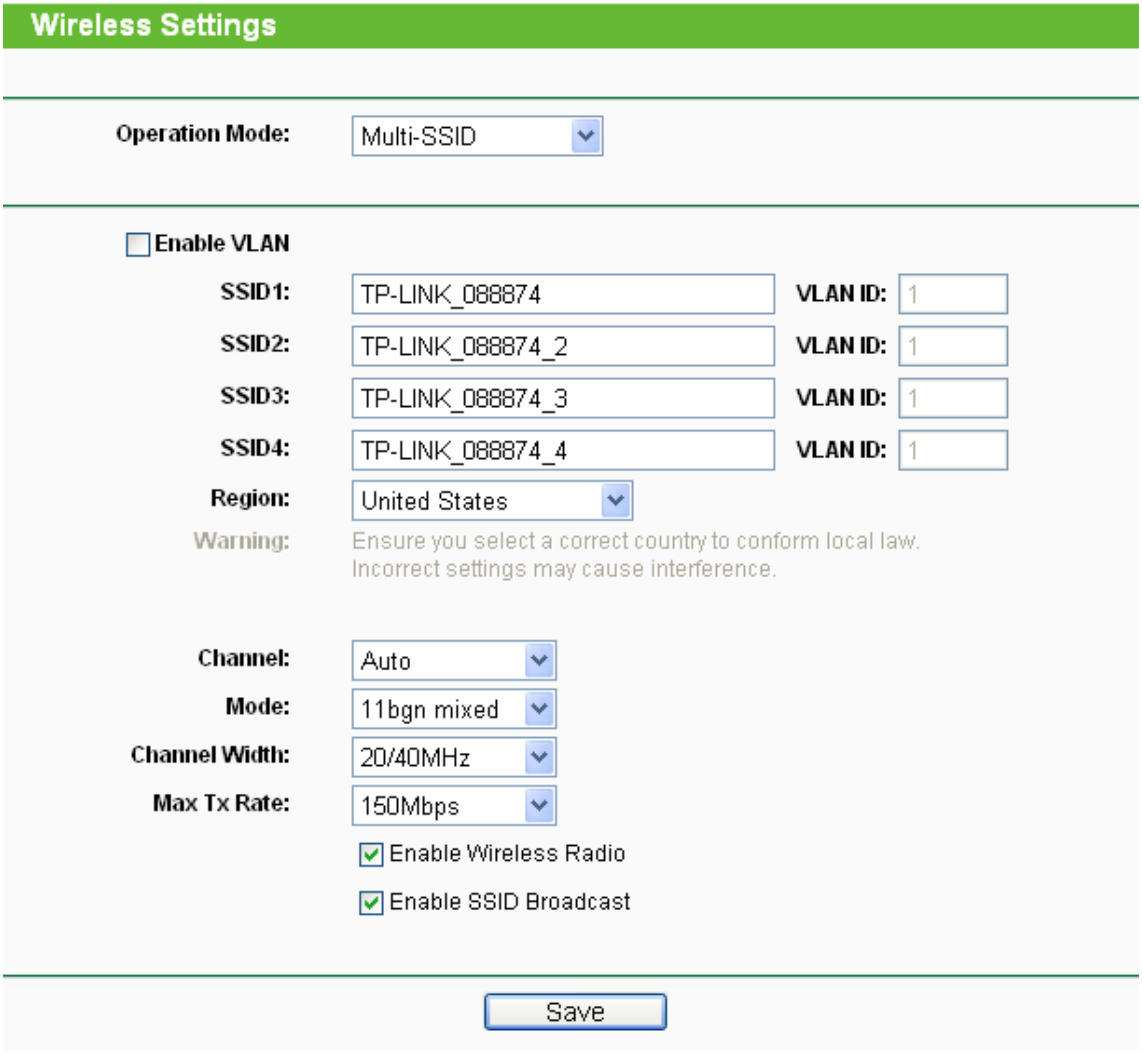


Figure 4-9 Wireless Settings in Multi-SSID mode

- **Enable VLAN -** Check this box and then you can change the **VLAN ID** 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 four SSIDs for each BSS (Basic Service Set) 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 VLAN ID can communicate with the PC connecting to the port with the same VLAN ID on the Switch.
- **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**.

Note Dialog

Note:

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

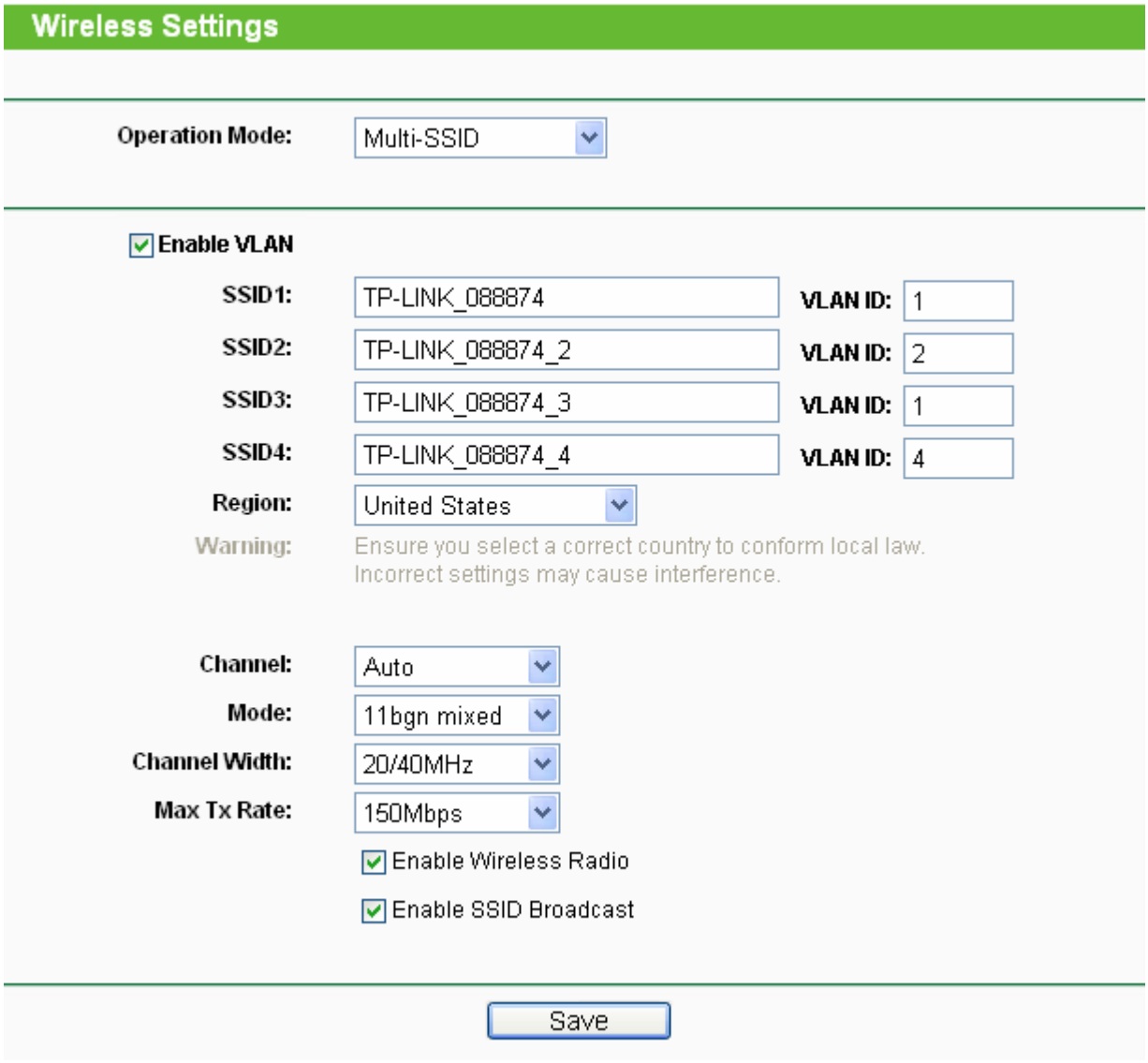
- **Channel -** Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** This field determines the wireless mode which the device works on.
  - **11b only -** Only 802.11b wireless 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 -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

Note:

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

You are suggested to implement Multi-SSID function with a switch that supports Tag VLAN feature. Here is an example of how to configure Multi-SSID. Please take the following steps:

1. Configure the Access Point



Configure the Access Point

- Select Multi-SSID as the operation mode of TL-WA701ND.
- Select the checkbox before Enable VLAN to enable VLAN function for this access point.
- Configure the SSID and its corresponding VLAN ID. The detailed parameters are shown as the above figure.
- STA1, STA2, STA3 and STA4 join to the wireless network with SSID1, SSID2, SSID3 and SSID4 respectively.

Note:

1) The wireless STAs join to the network with different VLAN IDs cannot communicate with each other, for example, STA1 and STA2.
2) The wireless STAs join to the network with the same VLAN ID can communicate with each other, for example, STA1 and STA3.
3) All wireless STAs can log on to the Web management page of TL-WA701ND and manage the access point, for example, STA1, STA2, STA3 and STA4.
4) All the packets received in the wired network from the wireless STA will be added a corresponding VLAN Tag of the wireless STA, unless the VLAN ID of the wireless network is set to 1.

2. Configure the Switch.

- Enable 802.1Q Tag VLAN function on the switch.
- Make sure the Untag frames are forwarded.

The following table shows the detailed configuration for the switch

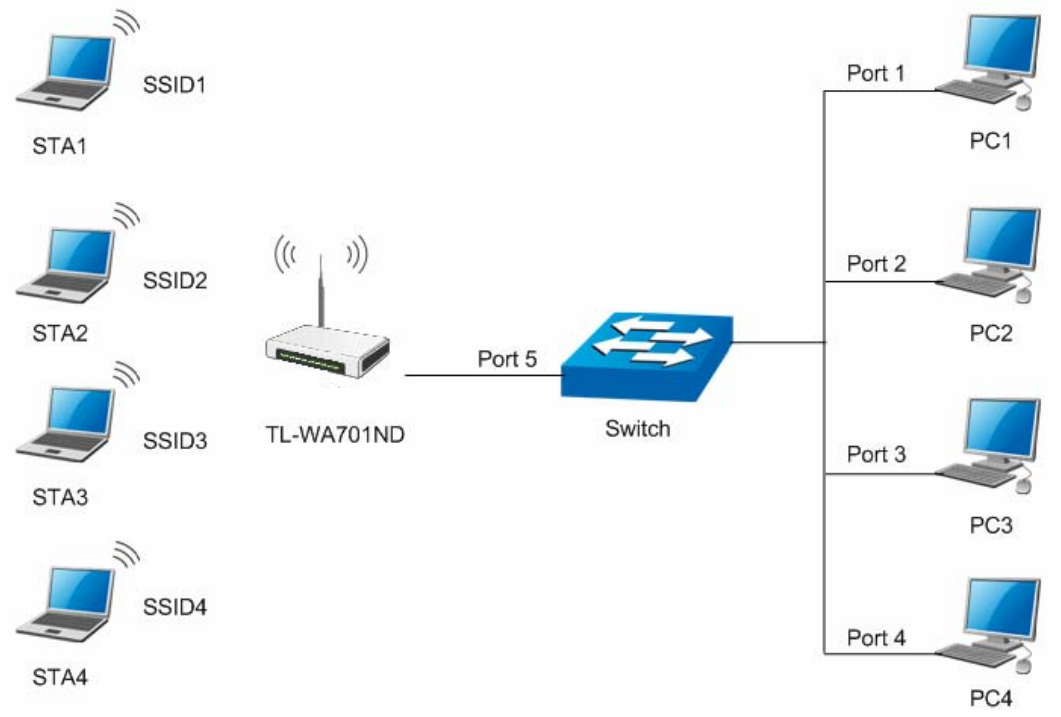
Port	VLAN ID	PVID	Egress Rule	Processing mode of Utag Frames
1	1	1	Untag	Forwarding
2	2	2	Untag	Forwarding
3	3	3	Untag	Forwarding
4	4	4	Untag	Forwarding
5	Port5 belongs to all VLANs	1	Tag	Forwarding

Table 4-1 Configure the Tag VLAN Switch

- Connect PC1, PC2, PC3 and PC4 to port1, port2, port3 and port4 of the switch respectively. The corresponding VLAN IDs of the four ports are 1, 2, 3 and 4.
- Configure port5 of the switch to be the member of VLAN1, VLAN2, VLAN3 and VLAN4 and connect it to the LAN port of TL-WA701ND.
- Configure the VLAN ID of the PC that can log on to the Web management page of TL-WA701ND via the LAN port equal to the PVID of port 5.

3. Verify the communication status after the above configuration is completed.

- If VLAN ID of the PC connected to the switch is different from the VLAN ID of the wireless STA, the two cannot communicate with each other, for example, PC1 and STA2.
- If the PC connected to the switch and the wireless STA have the same VLAN ID, the two can communicate with each other, for example PC2 and STA2.



Multi-SSID+VLAN

Note:

If the LAN port of TL-WA701ND is not connected to a switch but directly to a PC,

1) The PC can directly log on to the Web management page of TL-WA701ND and manage the access point.
2) Only the wireless STA with its VLAN ID set to 1 can communicate with the wired PC.

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

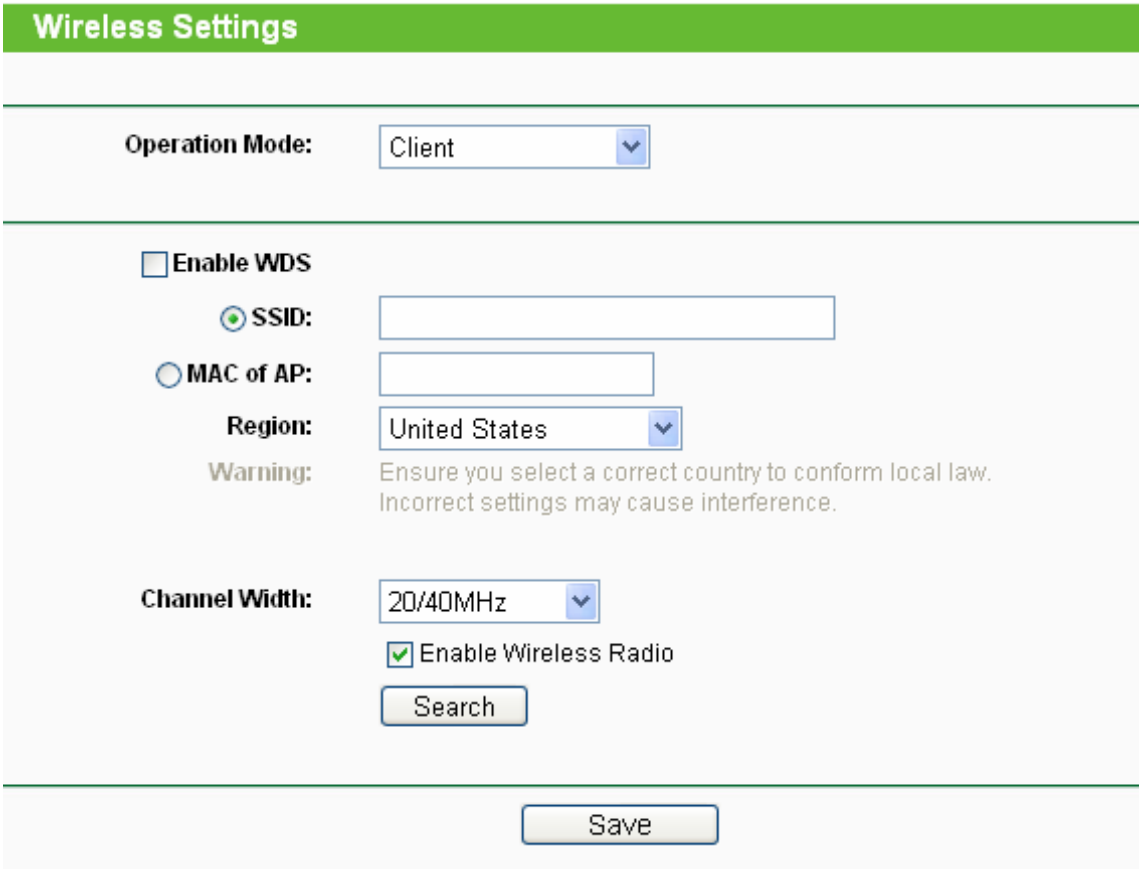


Figure 4-10 Wireless Settings in Client mode

- **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**.

Note Dialog

Note:

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

- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.

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.

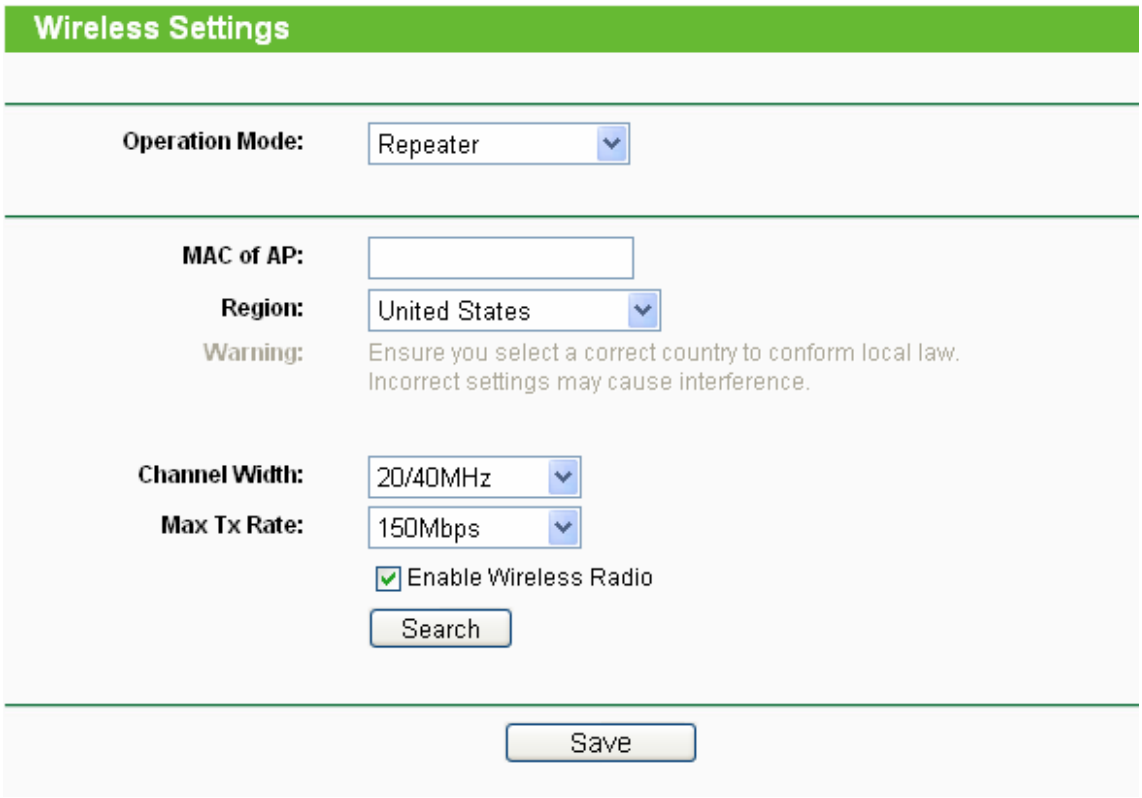


Figure 4-11 Wireless Settings in Repeater mode

- **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**.

Note Dialog

Note:

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

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

Click the **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.

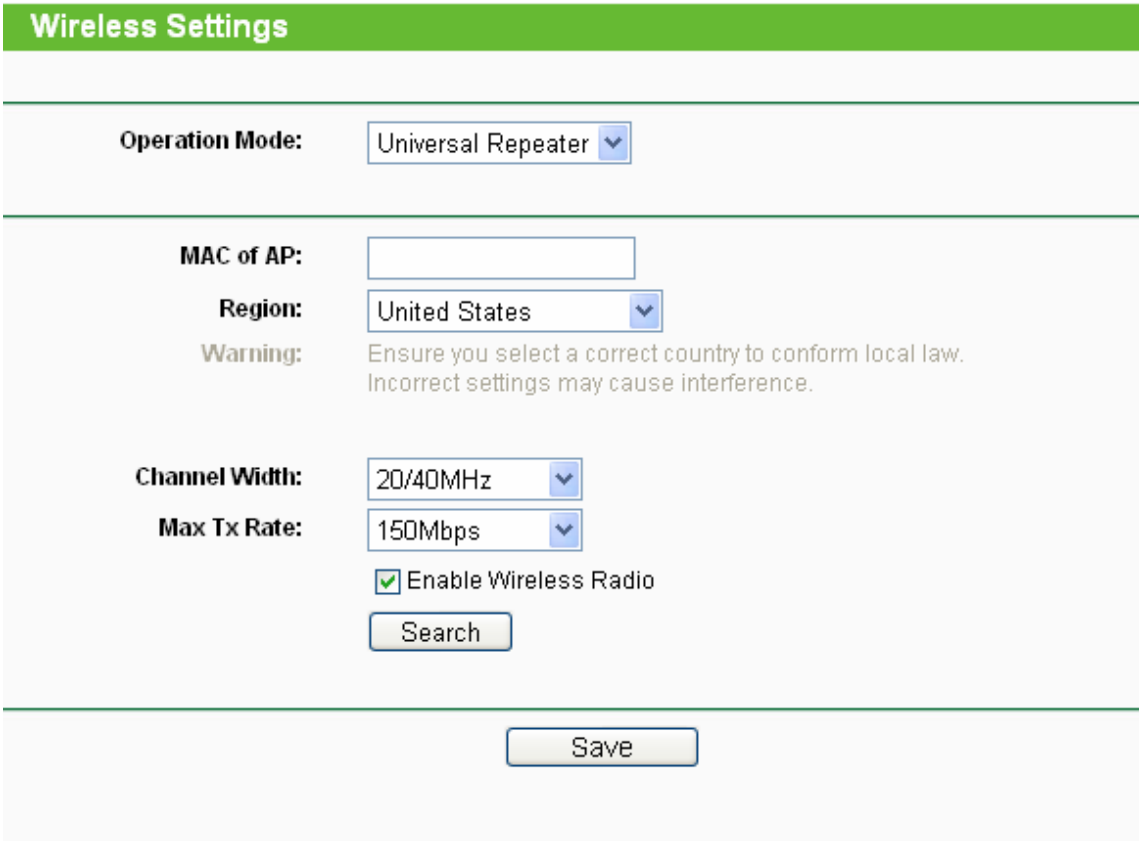


Figure 4-12 Wireless Settings in Universal Repeater mode

- **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**.

Note Dialog

☞ **Note:**

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

- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.

- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.

Click the **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.

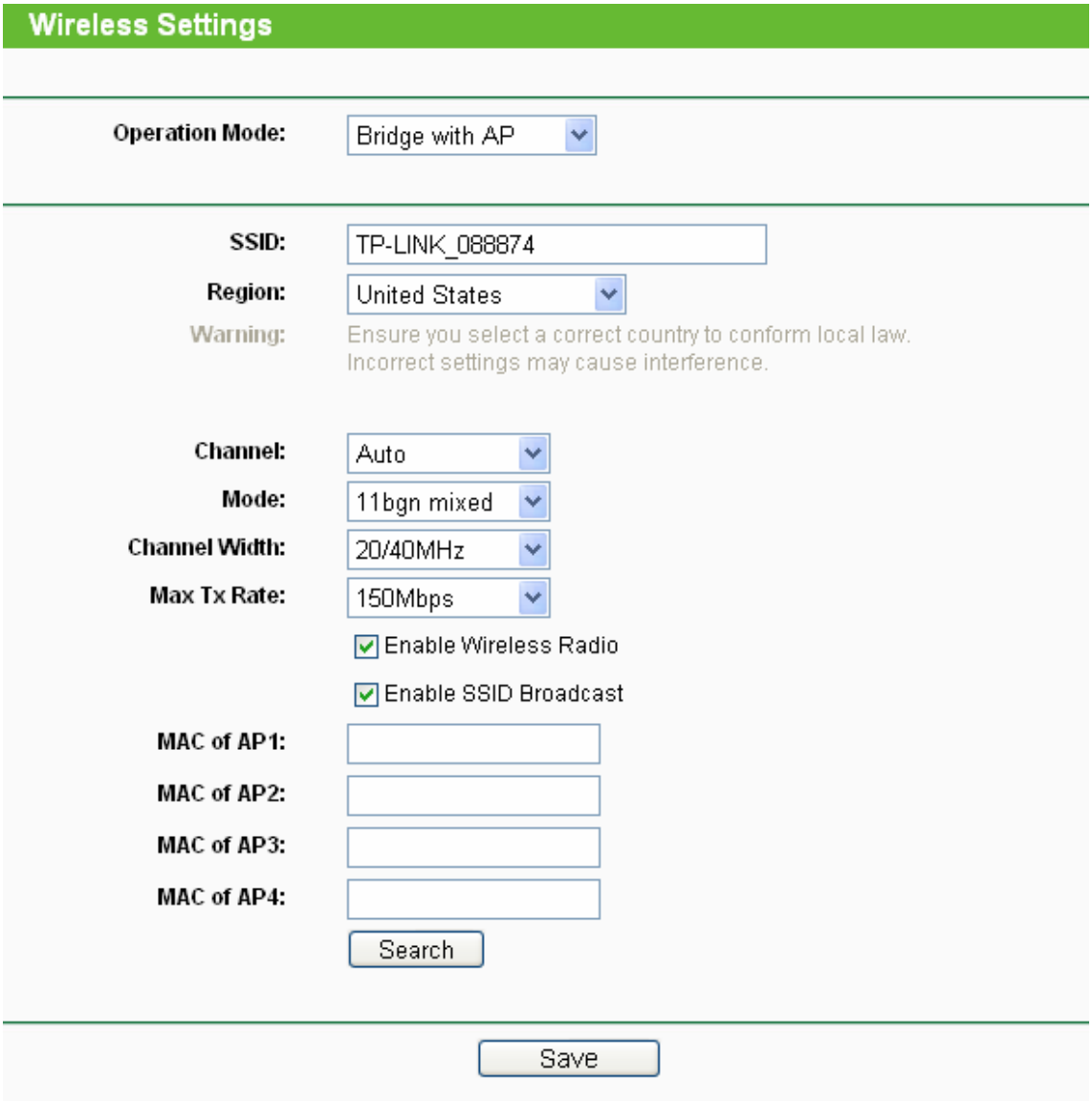


Figure 4-13 Wireless Settings in Bridge with AP mode

- **SSID** (Set Service Identifier) **-** Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-LINK_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- **Region -** 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**.

Note Dialog

Note:

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

- **Channel -** Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** 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 -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.
- **MAC of AP (1-4) -** Enter the MAC address of other AP(s).

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.

4.5.2 Wireless Security

Selecting **Wireless** > **Wireless Security** will enable you to configure wireless security for your

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

1) Access Point

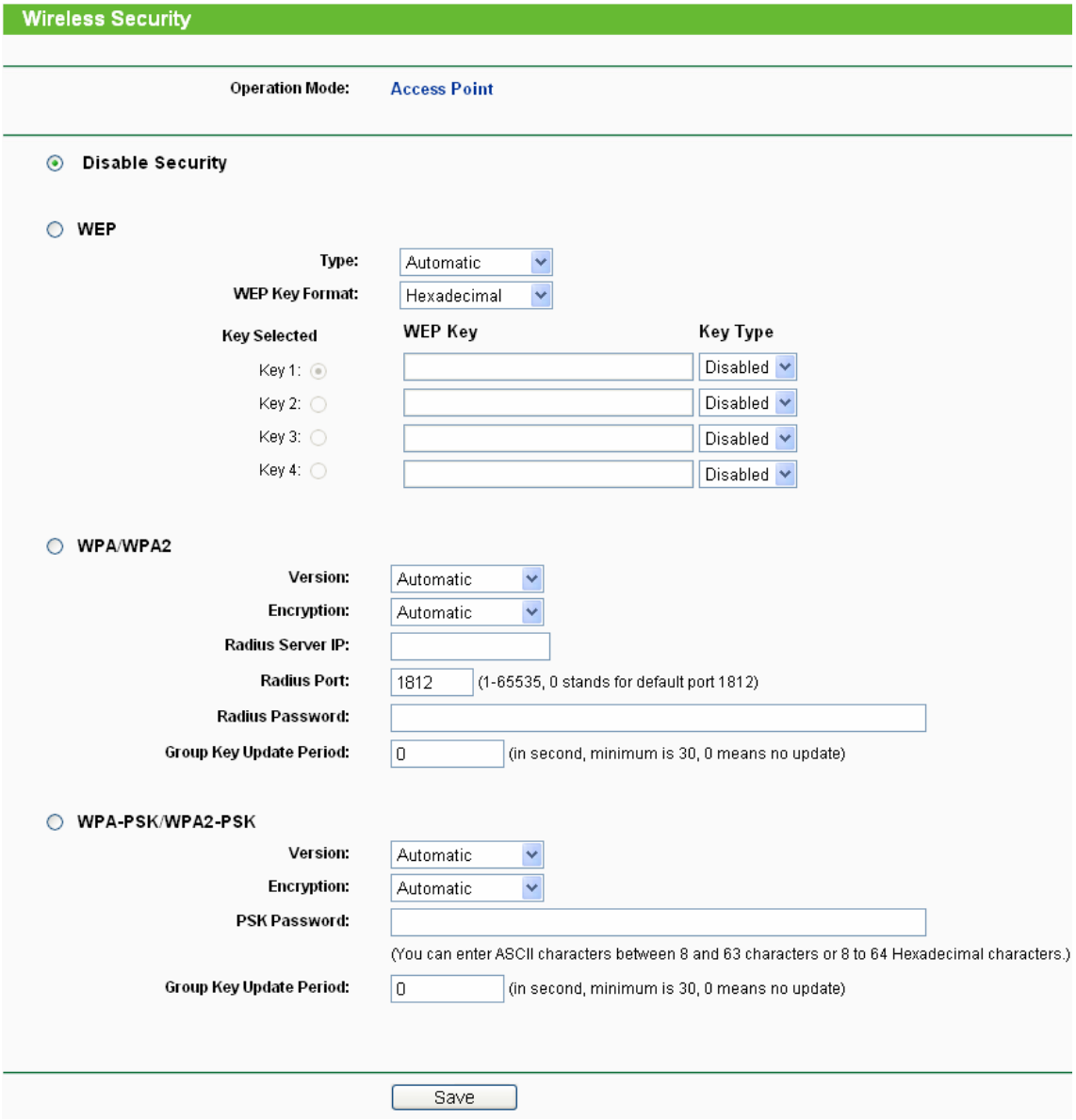


Figure 4-14 Wireless Security - Access Point

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.

  1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

2) **Shared Key** - Select 802.11 **Shared Key** authentication type.

3) **Open System** - Select 802.11 **Open System** authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

➢ **WPA/WPA2 -** Select WPA/WPA2 based on Radius Server.

- **Version -** You can select one of following versions.

1) **Automatic -** Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

2) **WPA -** Wi-Fi Protected Access.

3) **WPA2 -** WPA version 2.

- **Encryption** - You can select either **Automatic**, **TKIP** or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port used by radius service.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version -** You can select one of following versions.

1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2) **WPA-PSK -** Pre-shared key of WPA.

3) **WPA2-PSK -** Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

Note:

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

2) Multi-SSID

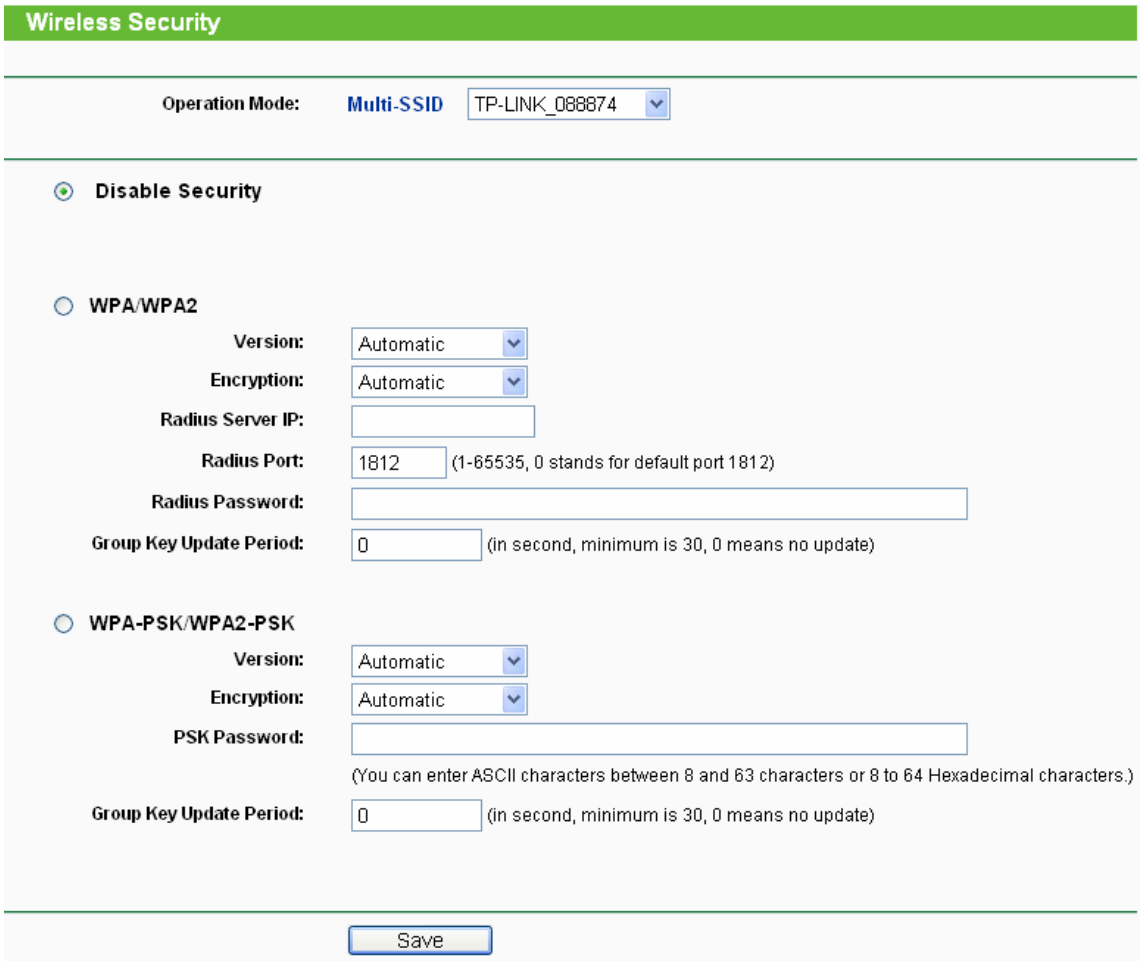


Figure 4-15 Wireless Security – Multi-SSID

- **Operation Mode -** Shows the current operation mode. You can choose one of the 4 SSID from the pull-down list.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **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 4-9 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

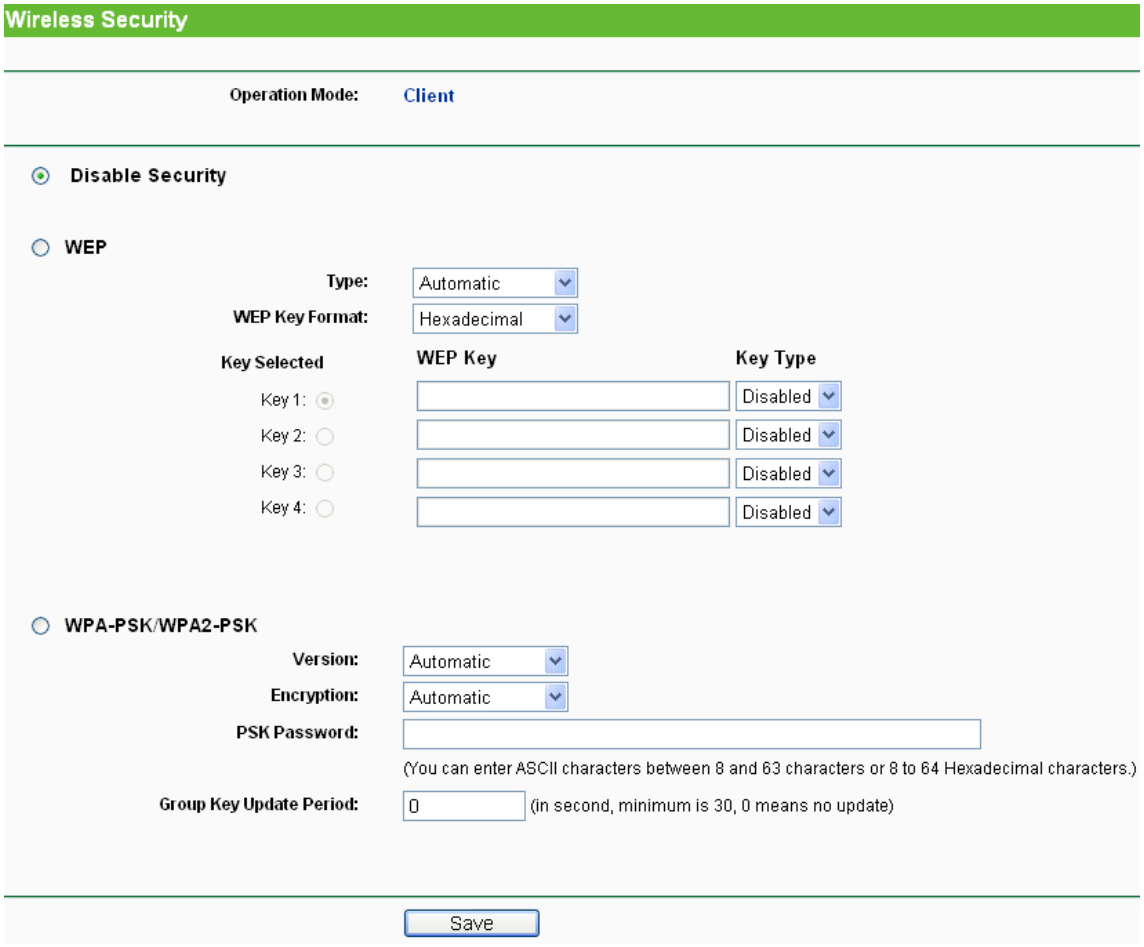


Figure 4-16 Wireless Security – Client

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.

  1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
  3) **Open System** - Select 802.11 **Open System** authentication.

  - **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2) **WPA-PSK** - Pre-shared key of WPA.

3) **WPA2-PSK** - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

☞ **Note:**

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

4) Repeater

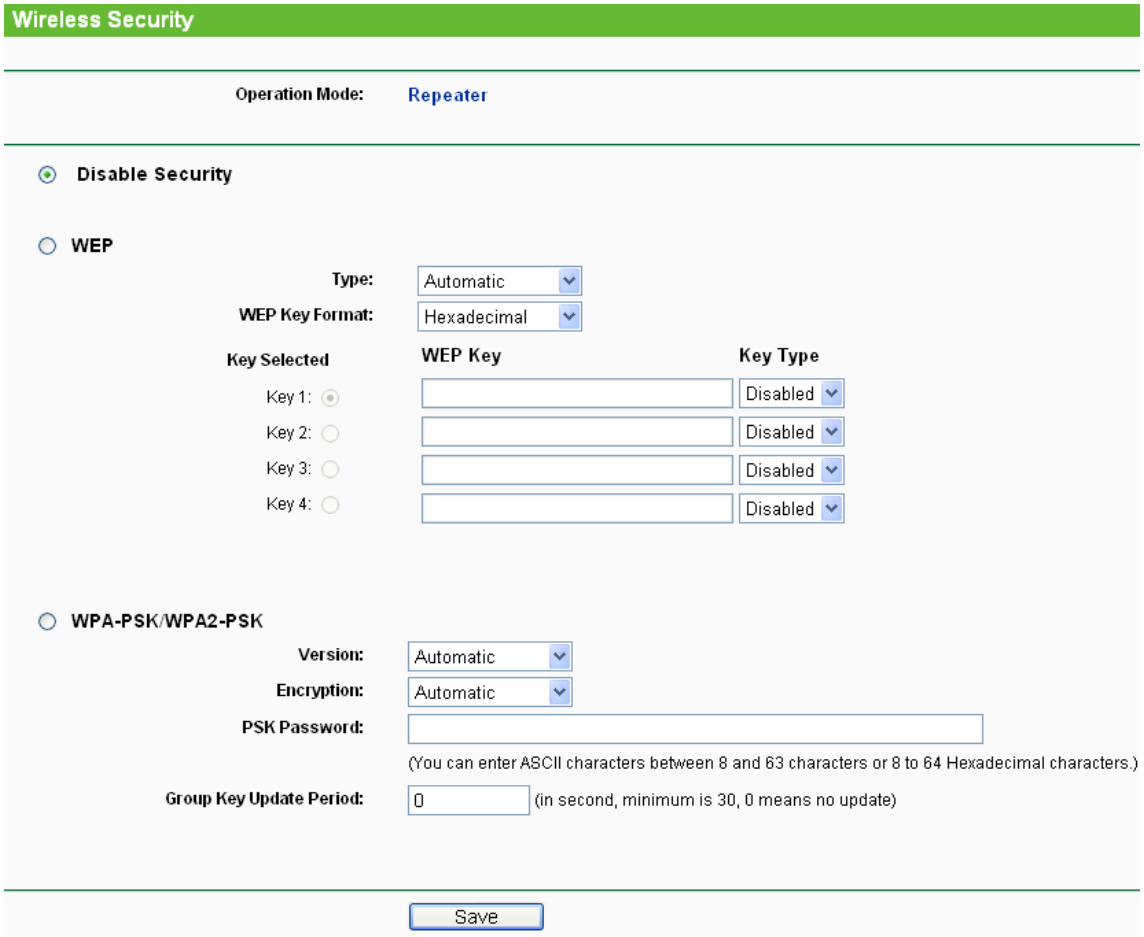


Figure 4-17 Wireless Security – Repeater

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.
    1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
    2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
    3) **Open System** - Select 802.11 Open System authentication.
  - **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
  - **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2) **WPA-PSK** - Pre-shared key of WPA.

3) **WPA2-PSK** - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

☞ **Note:**

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

5) Universal Repeater

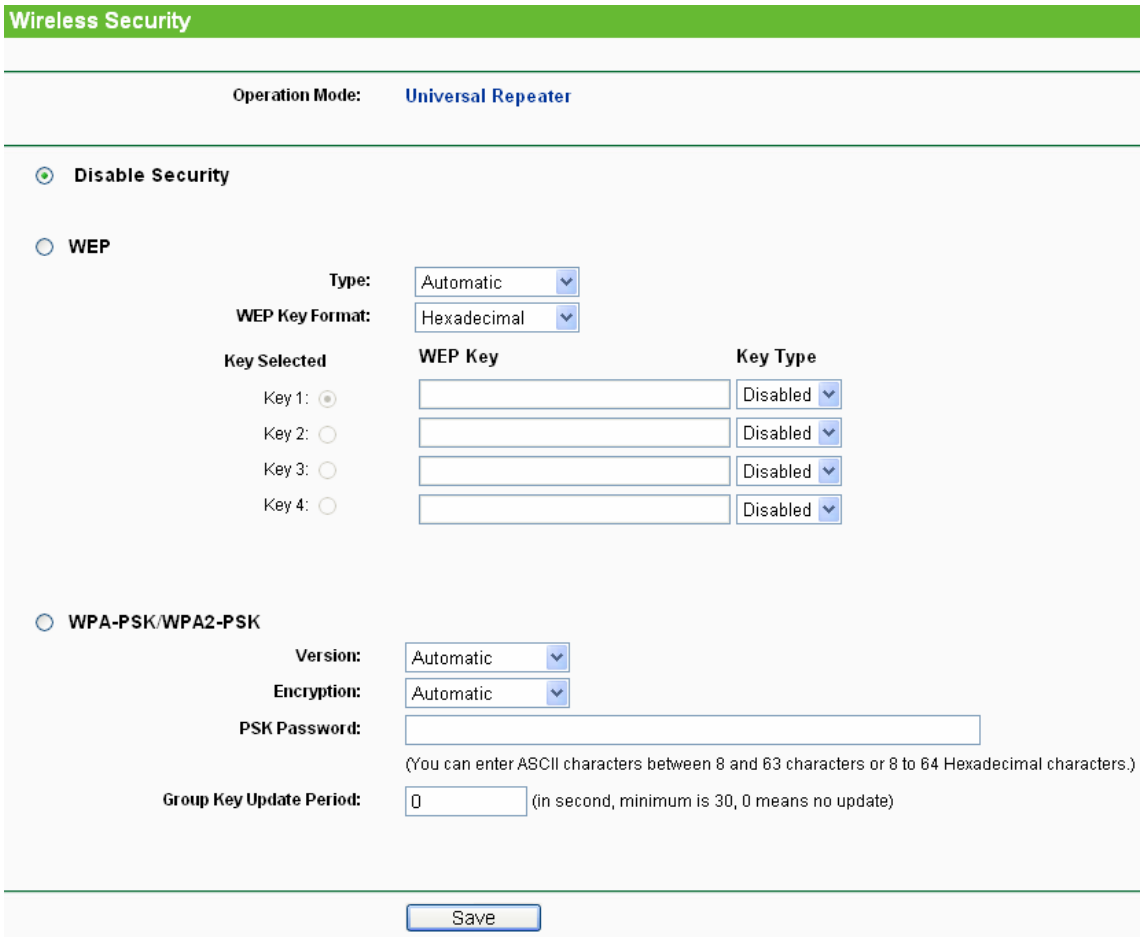


Figure 4-18 Wireless Security – Universal Repeater

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.

  1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
  3) **Open System** - Select 802.11 Open System authentication.

  - **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2) **WPA-PSK** - Pre-shared key of WPA.

3) **WPA2-PSK** - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select either **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

☞ **Note:**

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

6) Bridge with AP

Figure 4-19 Wireless Security – Bridge with AP

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

- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

Note:

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.

4.5.3 Wireless MAC Filtering

Selecting **Wireless** > **Wireless MAC Filtering** will allow you to set up some filtering rules to control wireless stations accessing the device, which depend on the station's MAC address on the following screen as shown Figure 4-20. 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.

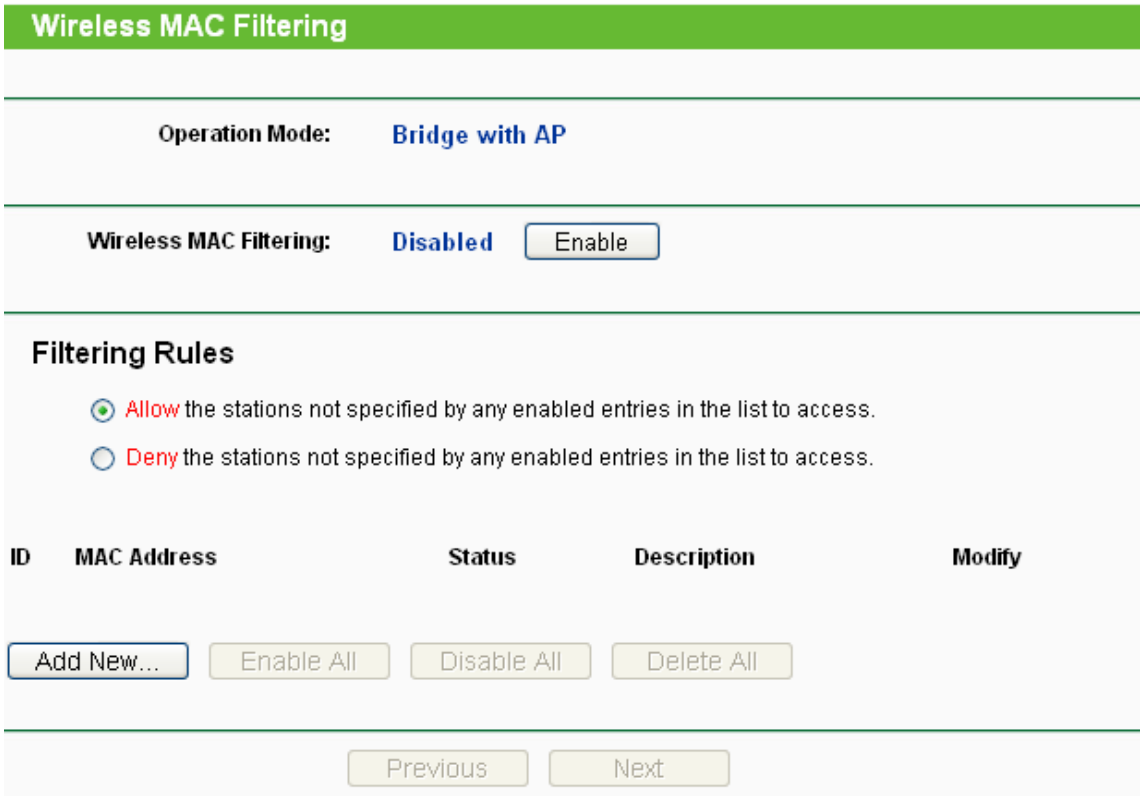


Figure 4-20 Wireless MAC address Filtering

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 -** Shows the current operation mode.

- **Wireless MAC Filtering -** Click the **Enable** button to enable the Wireless MAC Address Filtering. The default setting is disabled.

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The “Add or Modify Wireless MAC Address Filtering entry" page will appear, shown in Figure 4-21

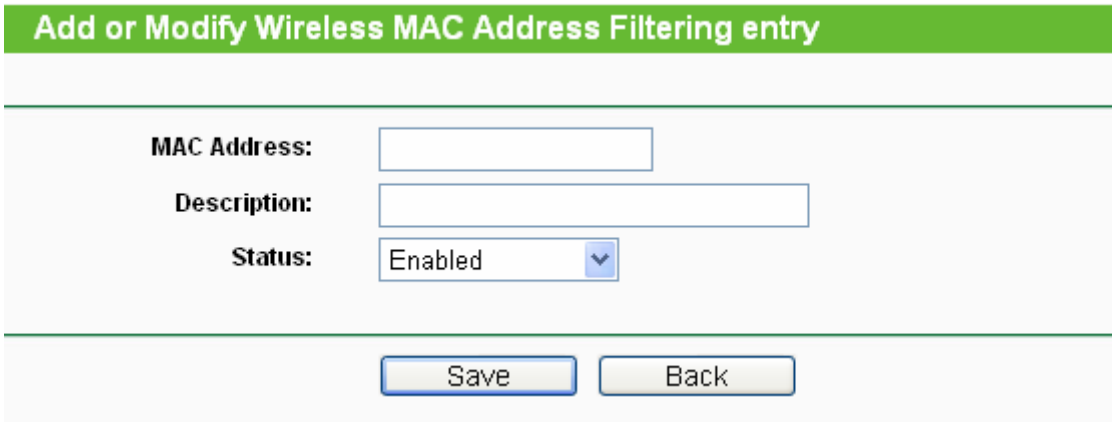


Figure 4-21 Add or Modify Wireless MAC Address Filtering entry

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

To set up an entry, follow these instructions:

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

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

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

To add additional entries, repeat steps 1-4.

To modify or delete an existing entry:

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

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

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

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

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

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

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

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

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

4.5.4 Wireless Advanced

Selecting **Wireless** > **Wireless Advanced** will allow you to do some advanced settings for the device in the following screen shown in Figure 4-22. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.

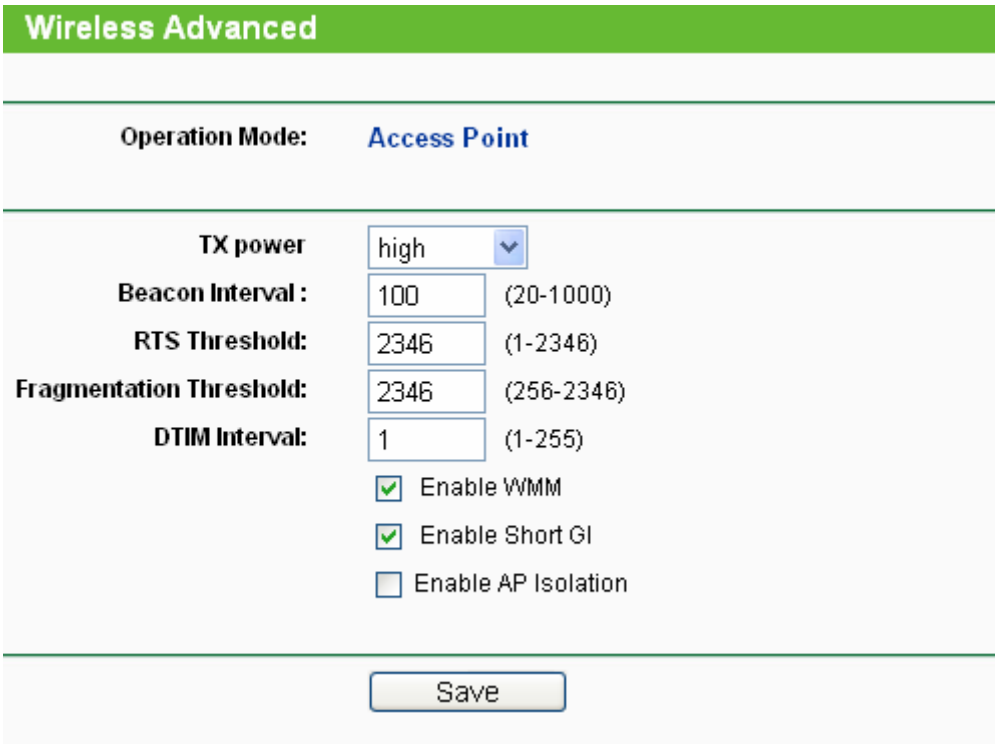


Figure 4-22 Wireless Advanced

- **Operation Mode -** Shows the current Operation Mode.
- **Tx Power -** Specifies the transmit power of the device. You can select **High**, **Middle** or **Low** which you would like. **High** is the default setting and is recommended.
- **Beacon Interval -** Specifies a value between 20-1000 milliseconds. The beacons are the packets sent by the device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Specifies the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** Determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM -** WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation -** Isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

4.5.5 Throughput Monitor

Selecting **Wireless** > **Throughput Monitor** will helps to watch wireless throughput information in the following screen shown in Figure 4-23.

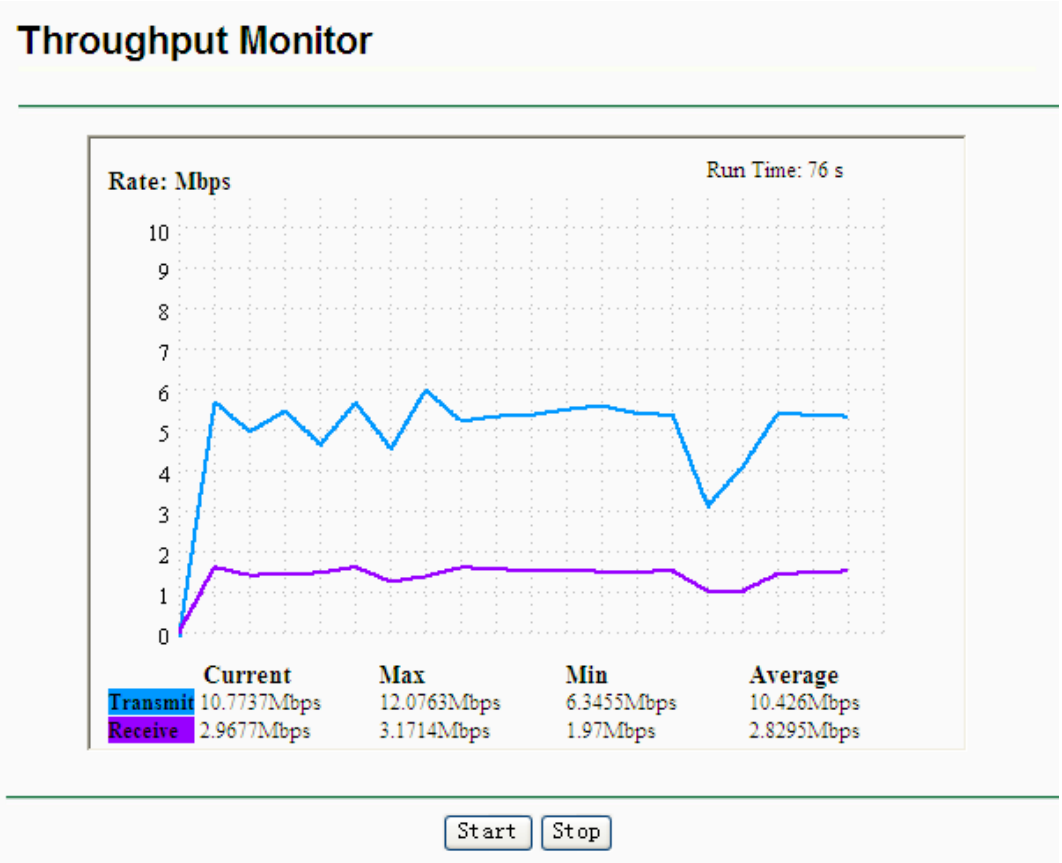


Figure 4-23 Throughput Monitor

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

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

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

4.5.6 Wireless Statistics

Selecting **Wireless** > **Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 4-24.

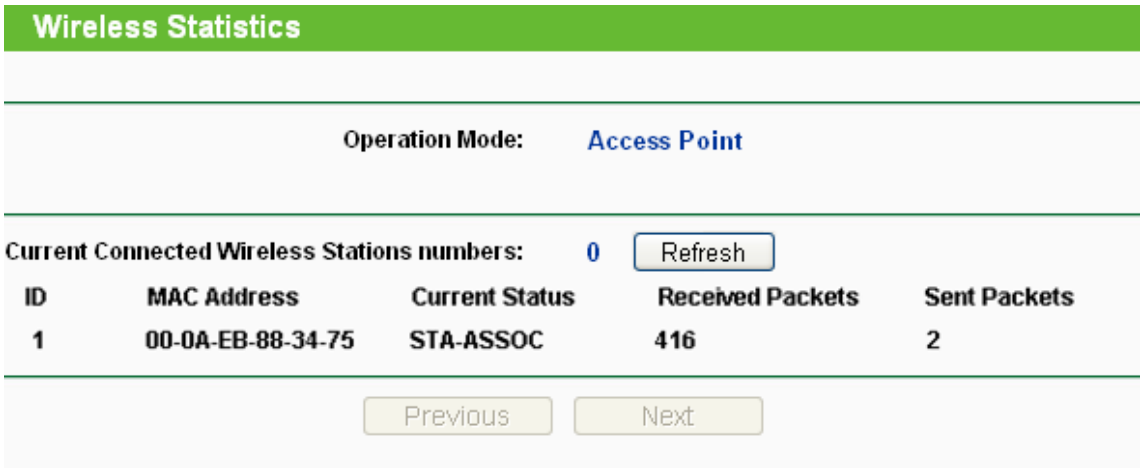


Figure 4-24 Statistics of the device attached wireless stations

- **Operation Mode -** Shows the current operation mode. If Multi-SSID is selected, all connected wireless stations will be shown here
- **MAC Address -** Shows the connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected
- **Received Packets -** packets received by the station
- **Sent Packets -** packets sent by the station

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

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

Note:

This page will be refreshed automatically every 5 seconds.

4.6 DHCP

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

There are three submenus under the DHCP menu (shown as Figure 4-25): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

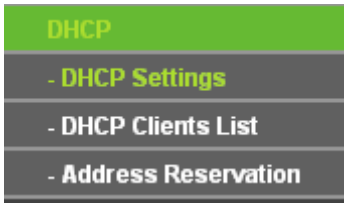


Figure 4-25 The DHCP menu

4.6.1 DHCP Settings

Selecting **DHCP** > **DHCP Settings** will enable you to set up the AP as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server can be configured on the page (shown as Figure 4-26):

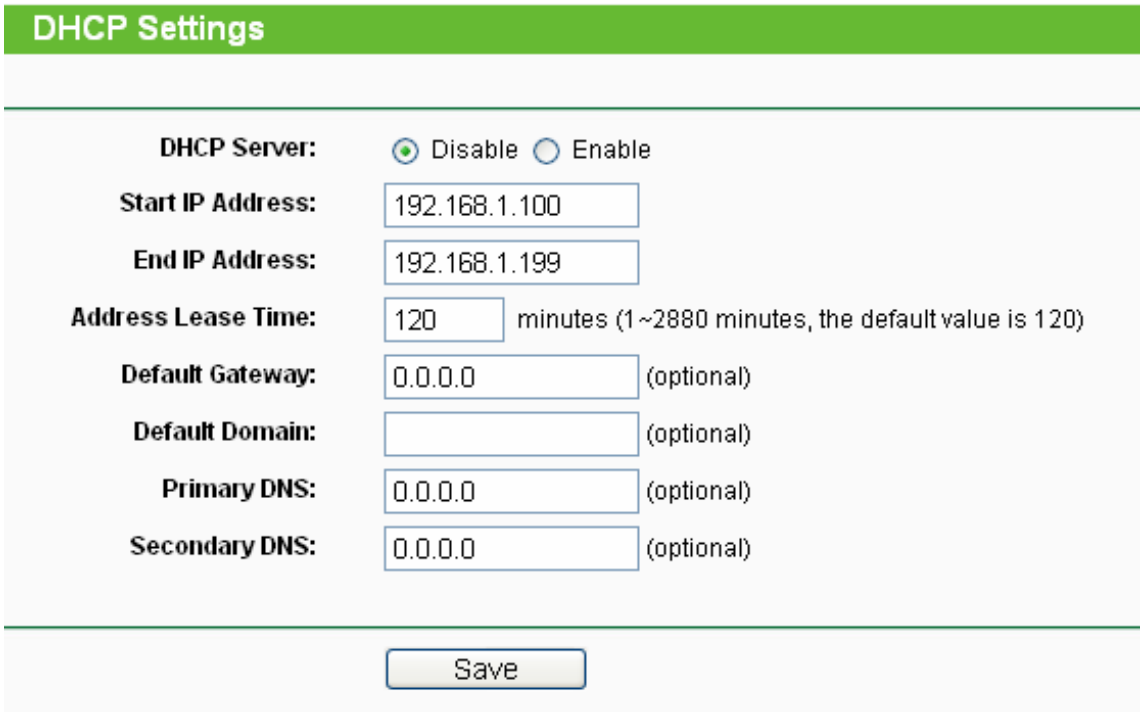


Figure 4-26 DHCP Settings

- **DHCP Server -** Selecting the radio button before **Disable/Enable** will disable/enable the DHCP server on your AP. The default setting is **Disable**. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address -** This field specifies the first address in the IP Address pool. 192.168.1.100 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 -** Enter the amount of time for the PC to connect to the AP with its current assigned dynamic IP address. The time is measured in minutes. After the time is up, the PC will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway (optional) -** Enter the IP address of the gateway for your LAN. The factory default setting is 0.0.0.0.
- **Default Domain (optional) -** Enter the domain name of the your DHCP server. You can leave the field blank.
- **Primary DNS (optional) -** Enter the DNS IP address provided by your ISP. Consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.
- **Secondary DNS (optional) -** Enter the IP address of another DNS server if your ISP provides two DNS servers. The factory default setting is 0.0.0.0.

Click **Save** to save the changes.

Note:

1 When the device is working on Dynamic IP mode, the DHCP Server function will be disabled.

2 To use the DHCP server function of the device, you should configure all computers in the LAN as "Obtain an IP Address automatically" mode. This function will not take effect until the device reboots.

4.6.2 DHCP Clients List

Selecting **DHCP** > **DHCP Clients List** will enable you to view the Client Name**,** MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 4-27).

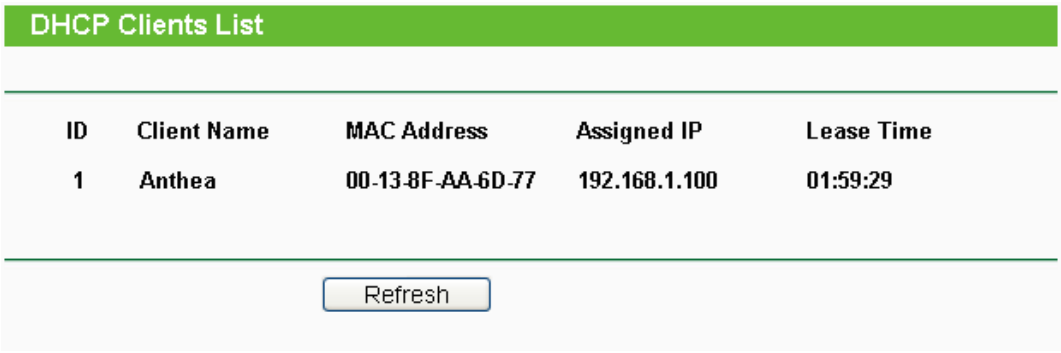


Figure 4-27 DHCP Clients List

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

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

4.6.3 Address Reservation

Selecting **DHCP** > **Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 4-28).

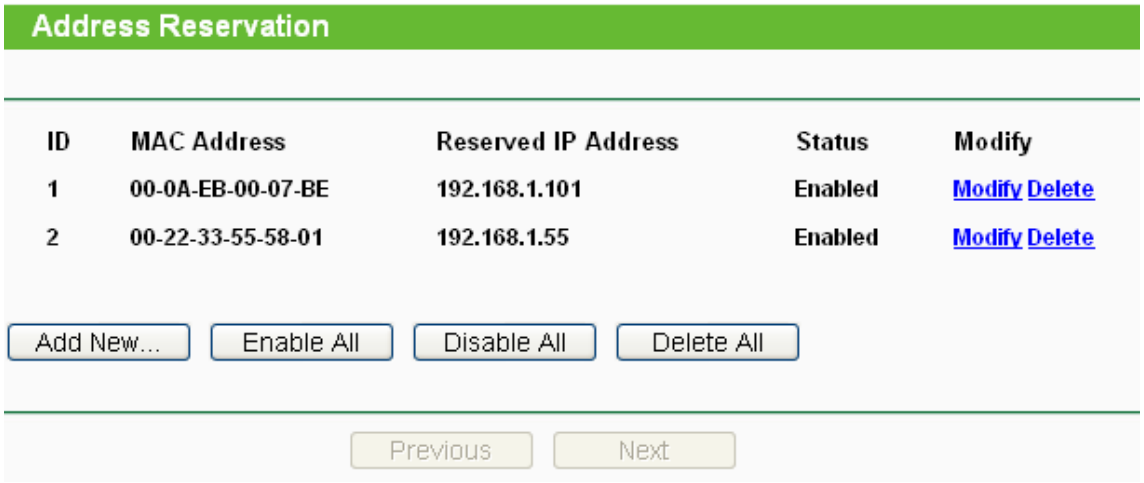


Figure 4-28 Address Reservation

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

To Reserve IP addresses:

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

To modify A Reserved IP address:

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

To delete all Reserved IP addresses:

1. Click **Clear All**.

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

Note:

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

4.7 System Tools

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

There are nine submenus under the **System Tools** menu (shown as Figure 4-29): **SNMP**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Reboot**, **Password**, and **System Log**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

Figure 4-29 The System Tools menu

4.7.1 SNMP

Selecting **System Tools** > **SNMP** to enable this function will allow the network management station to retrieve statistics and status from the SNMP agent in this device. Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol, used to refer to a collection of specifications for network management that include the protocol itself. To use this function, select Enable and enter the following parameters in Figure 4-30.

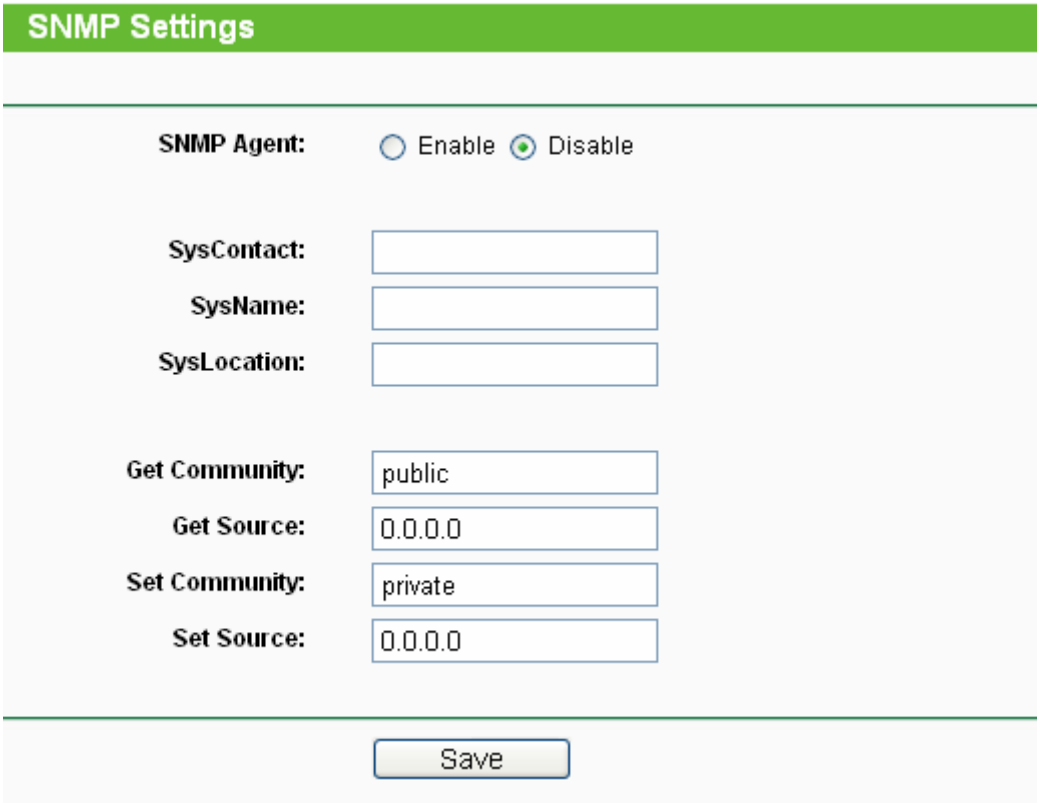


Figure 4-30 SNMP Settings

- **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.

4.7.2 Diagnostic

Selecting **System Tools** > **Diagnostic** allow you to check the connections of your network components on the screen shown in Figure 4-31.

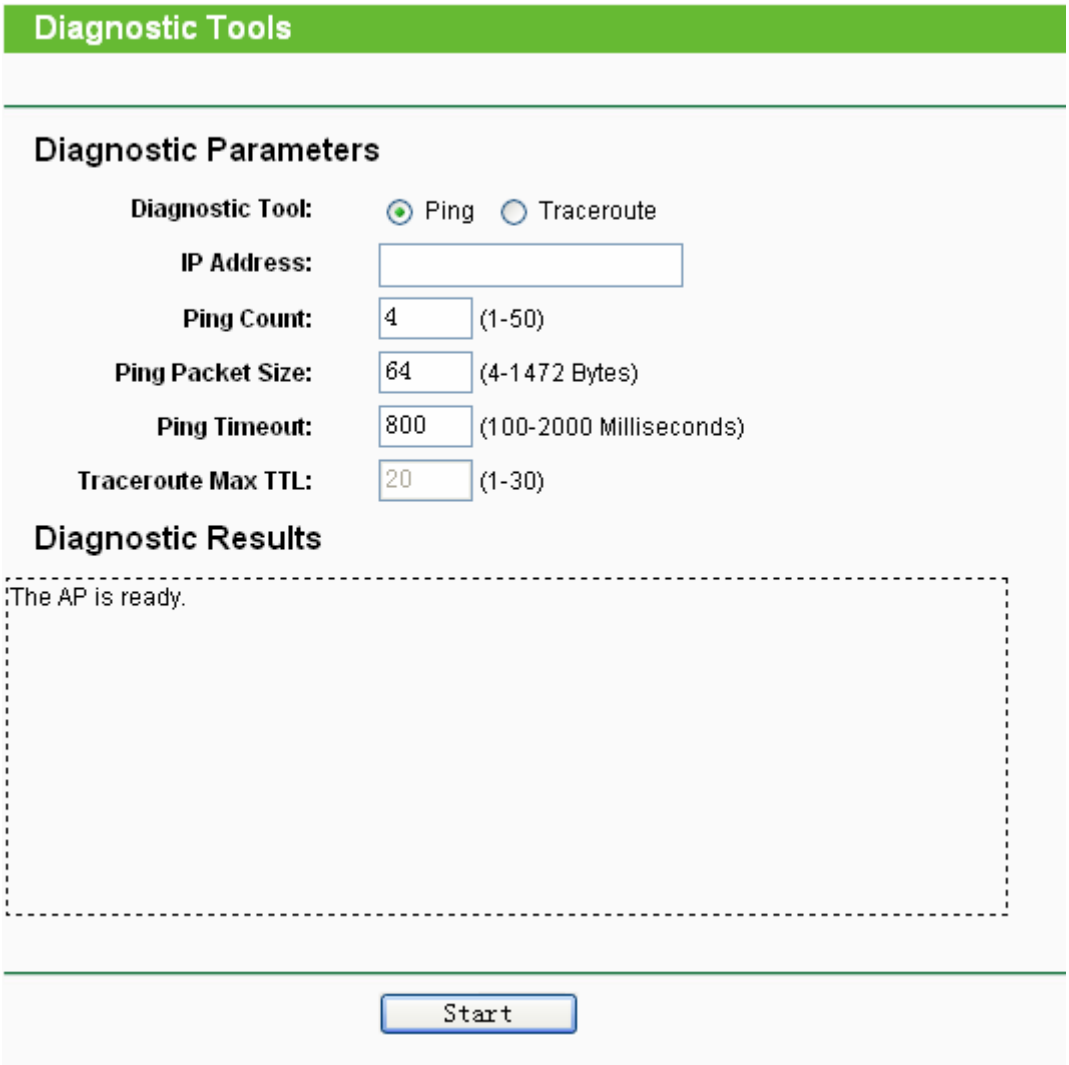


Figure 4-31 Diagnostic

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.

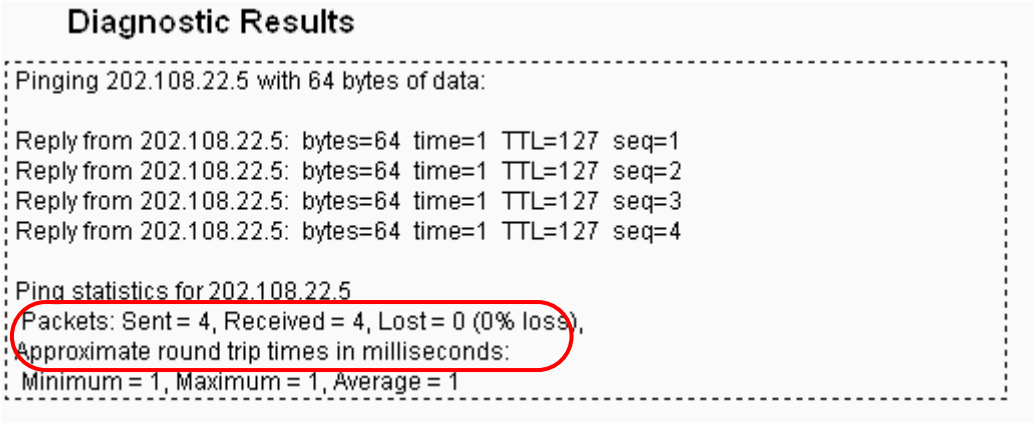


Figure 4-32 Diagnostic Results

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.

4.7.3 Firmware Upgrade

Selecting **System Tools** > **Firmware Upgrade** allows you to upgrade the latest version of firmware for the device on the screen shown in Figure 4-33.

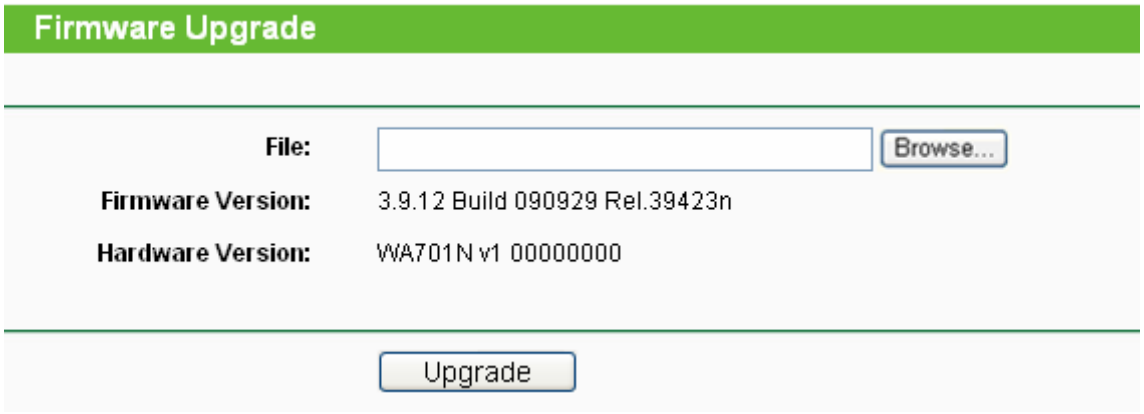


Figure 4-33 Firmware Upgrade

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

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

Note:

1 There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the device itself, you can try to upgrade the firmware.

2 Before upgrading the device's firmware, you should write down some of your customized settings to avoid losing important configuration settings of device.

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

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

Note:

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

4.7.4 Factory Defaults

Selecting **System Tools** > **Factory Default** allows you to restore the factory default settings for the device on the screen shown in Figure 4-34.

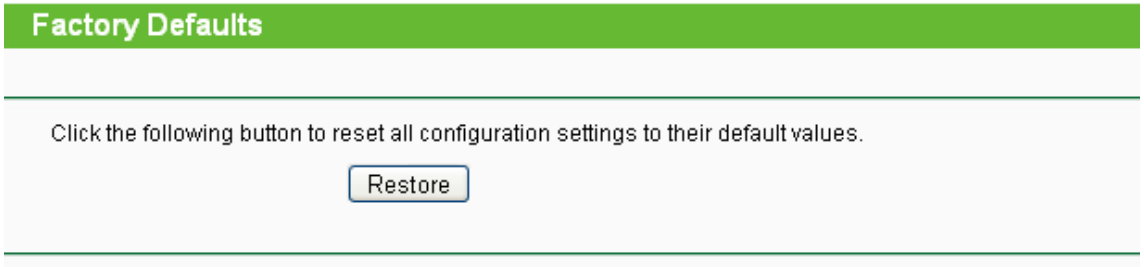


Figure 4-34 Restore Factory Defaults

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

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

Note:

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

4.7.5 Backup & Restore

Selecting **System Tools** > **Backup & Restore** allows you to save all configuration settings to your local computer as a file or restore the device's configuration on the screen shown in Figure 4-35.

Figure 4-35 Save or Restore the Configuration

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

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

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

Note:

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

4.7.6 Ping Watch Dog

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

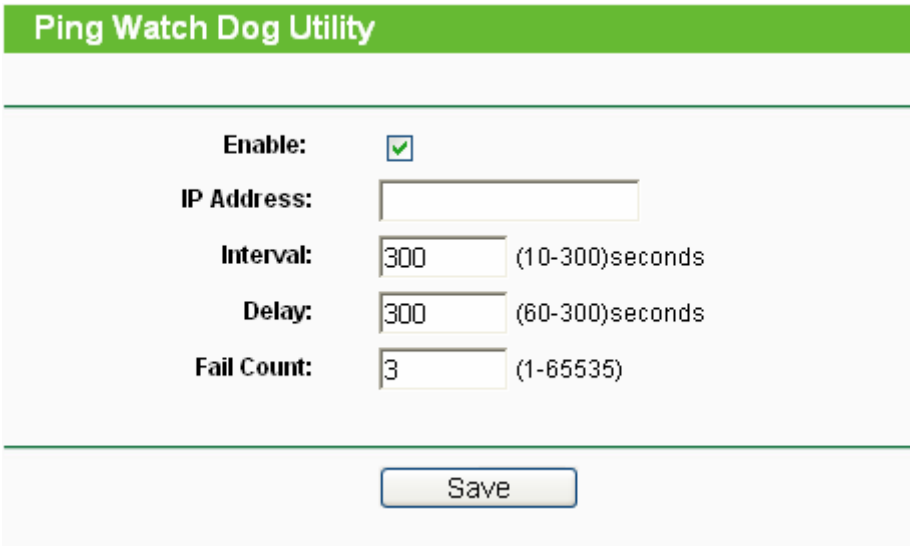


Figure 4-36 Ping Watch Dog Utility

- **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.

4.7.7 Reboot

Selecting **System Tools** > **Reboot** allows you to reboot the device on the screen shown in Figure 4-37.

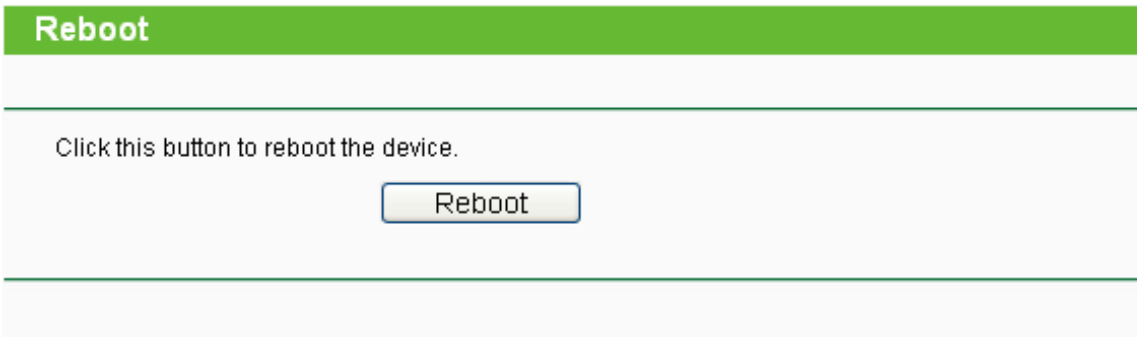


Figure 4-37 Reboot the device

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).

4.7.8 Password

Selecting **System Tools** > **Password** allows you to change the factory default user name and password of the device on the screen shown in Figure 4-38.

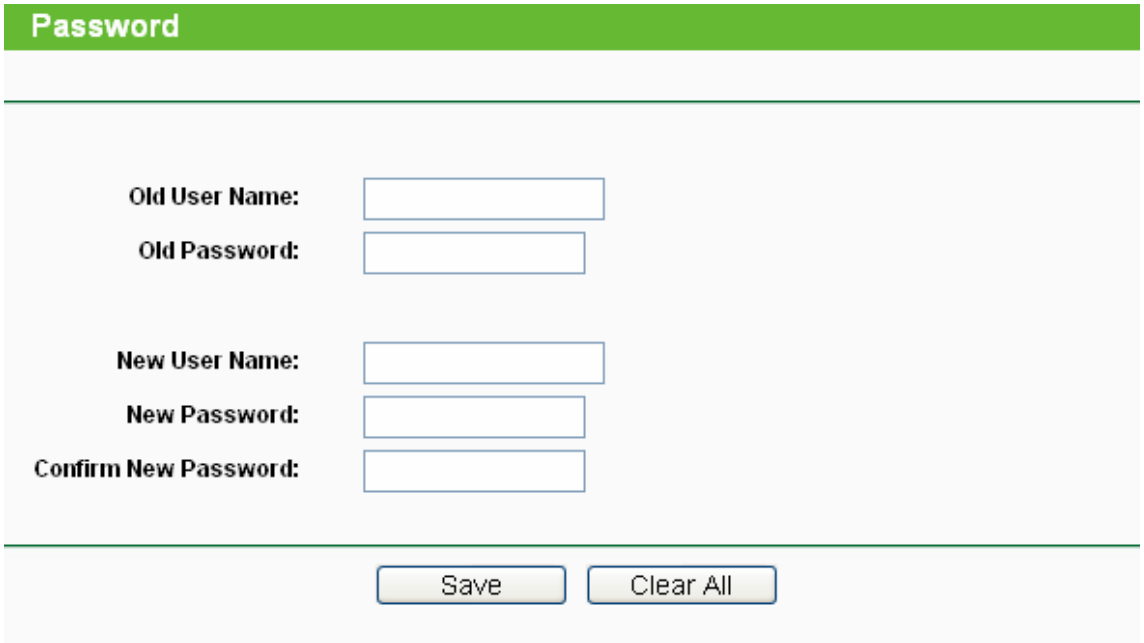


Figure 4-38 Password

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 management page or Quick Setup will be prompted for the device's user name and password.

Note:

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

Click **Save** when finished.

Click **Clear All** to clear all.

4.7.9 System Log

Selecting **System Tools** > **System Log** allows you to query the Logs of the device on the screen shown in Figure 4-39.

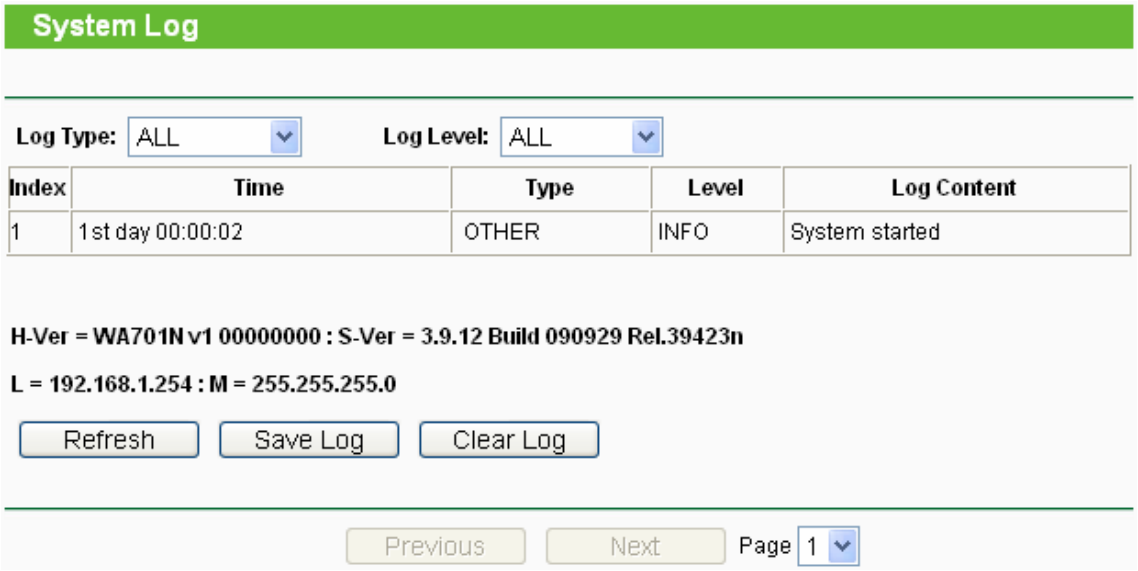


Figure 4-39 System Log

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.

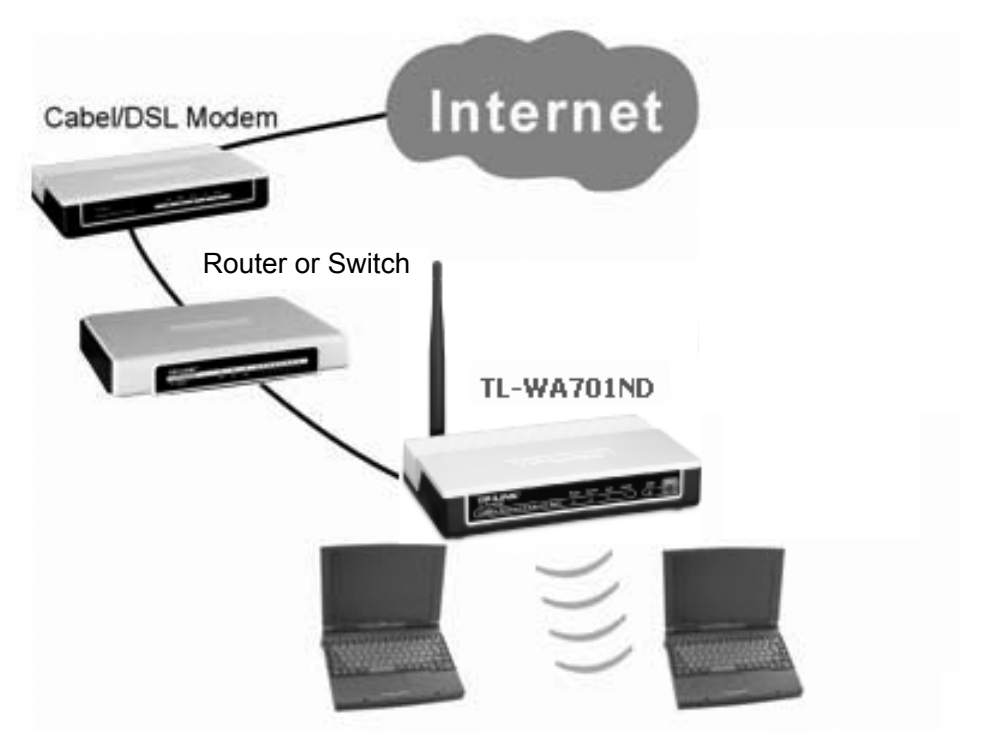
Click the **Clear Log** button to delete all the logs from the system permanently, not just from the page.

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

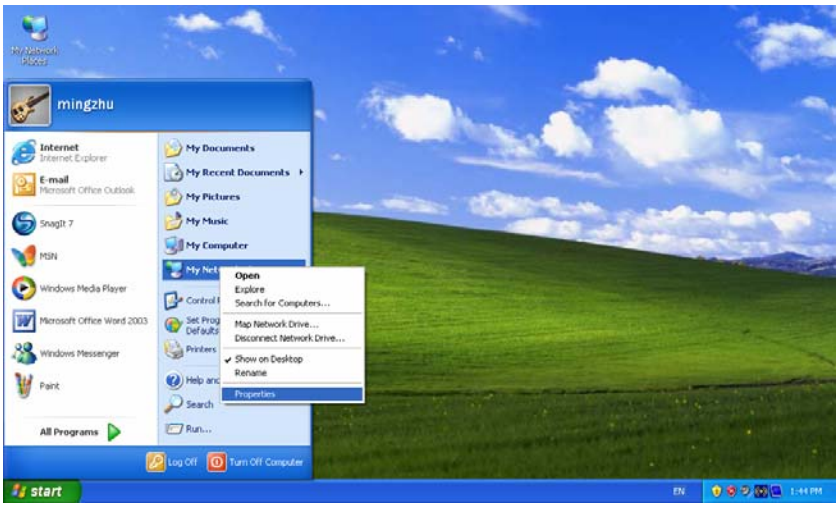
Appendix A: Application Example

The TL-WA701ND allows you to connect a wireless device to the wired network. Providing that you want to connect your computer equipped with wireless adapter to a wired network wirelessly, you can take the following instructions.

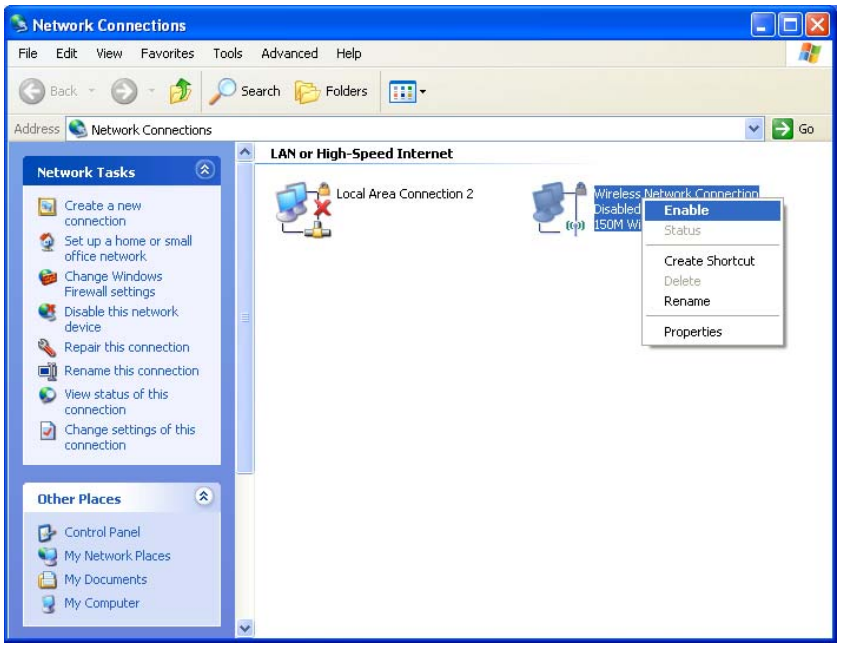
1. Configure the AP via a wired connection.
   1) Connect your AP to your PC with an Ethernet cable.
   2) Configure the IP address for your PC to communicate with the AP referring to **Chapter 3 Configure the PC**.
   3) Log on to the web-based management page. Configure your AP in the **Access Point**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



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

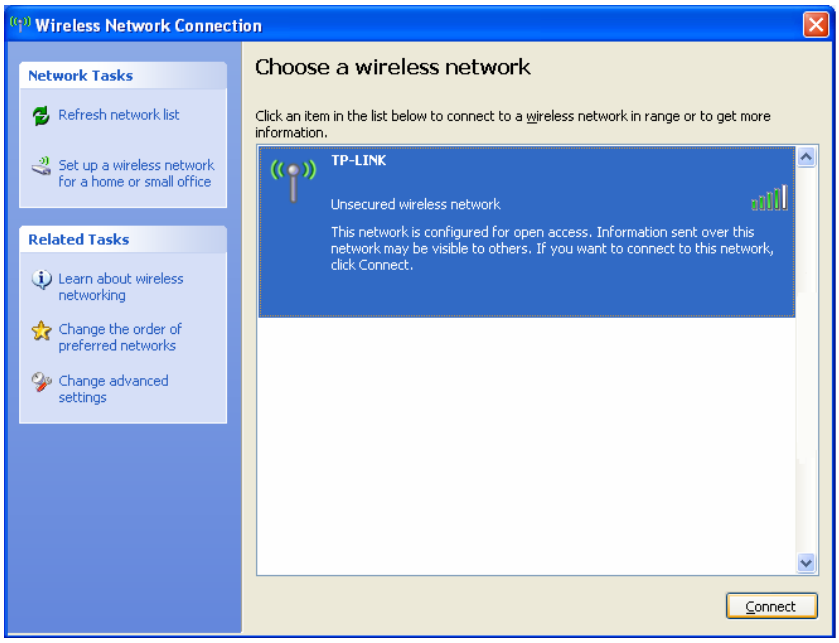


2) On the **My Network Connections** window, right-click **Wireless Network** and choose **Enable** to enable wireless network function.

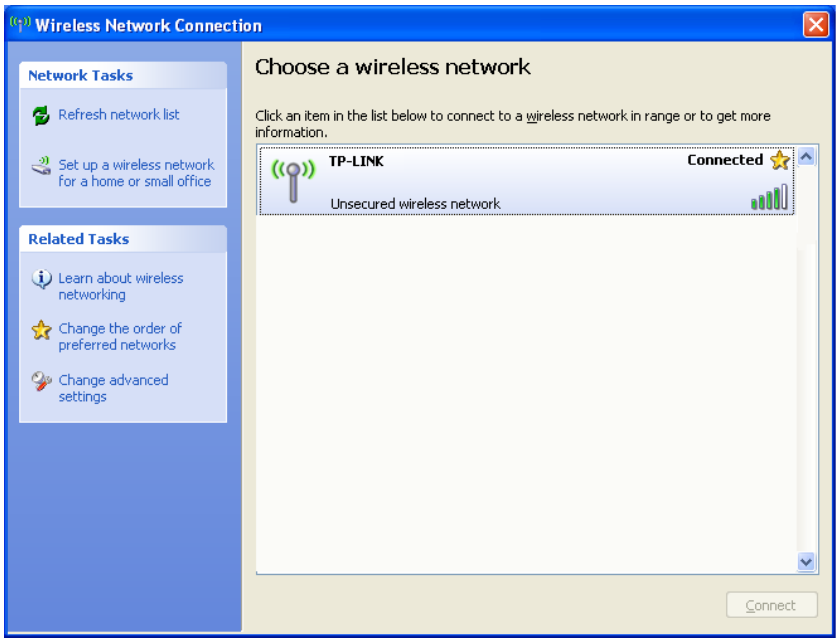


3) Right-click the wireless connection icon "" on the screen of the PC and then select **View Available Wireless Networks**.

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



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



Appendix B: Factory Defaults

Item	Default Value
Common Default Settings	
Username	admin
Password	admin
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Wireless	
SSID	TP-LINK_XXXXXX
Wireless Security	Disable
Wireless MAC Address Filtering	Disable
DHCP	
DHCP Server	Disable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Address Lease Time	120 minutes (Range:1 ~ 2880 minutes)
Default Gateway (optional)	0.0.0.0
Primary DNS (optional)	0.0.0.0
Secondary DNS (optional)	0.0.0.0

Note:

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

Appendix C: Troubleshooting

1. No LEDs are lit on the access point.

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

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

2. The LAN LED is not lit.

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

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

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

There is a configuration problem. Check the following items.

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

Appendix D: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11n, 802.11b and 802.11g, TCP/IP, DHCP
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, 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）
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
Antenna Gain	4dBi
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 E: Glossary

802.11b - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

802.11g - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

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.