NextG | High Power USB WiFi Adapter

This manual walks though the steps of setting up the NextG High Power USB WiFi Adapter from quick start followed by detailed explanation of what each parameter does.

# Instruction Manual

## Linux Open Source Code

Certain products include software code developed by third parties, software code is subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Please see the **GNU** (www.gnu.org) and **LPGL**(www.gnu.org) Websites to view the terms of each license. The GPL Code and LGPL Code used in products are distributed without any warranty and are subject to the copyrights of their authors. For details, see the GPL Code and LGPL Code licenses.

# Table of Contents

# 2. Quick Start

## 2.1 Installation and Device Connection

Install the CD-ROM software driver before you plug in the USB adapter to you PC or laptop computer. This avoids the USB adapter being recognized by another existing WiFi software driver which might not be fully compatible with the original software driver.

Before making any device and cable connection to the computer, you have to install the CD software driver and utility from fresh.

Insert the CD-ROM into the CD/DVD drive of your computer.

As soon as the AutoPlay window appears, double click "SETUP.EXE" to install the software driver. If the AutoPlay window does not pop up, you could also go to the CD/DVD drive under "My Computer" and double click the SETUP icon.

Reboot your computer.

Once completed, you could plug in the USB adapter to any spare USB port of your computer using the USB2.0 cable supplied in the kit.

# 1. Scanning the WiFi Signal – A Quick Guide

## 1.1 RALINK WIRELESS UTILITY (RaUI) OR WINDOWS ZERO CONFIGURATION (WZC)

As the title suggests, two types of wireless utilities are possible. The Windows Zero Configuration provides the basic wireless networking configuration whose user interface is consistent across various Windows Operating Systems from XP, VISTA to Windows 7; and the more sophisticated RaLink Wireless Utility with the WPA supplicant functionality.

As soon as Windows starts, you could find the RaUI icon at the lower right hand corner of the computer screen. Right-click RaUI allows you to toggle between RaUI and WZC.


RaUI can work in parallel with WZC. When WZC is active, RaUI provides only the monitoring function, such as showing the link stats, network status, statistic counters, advance feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions.



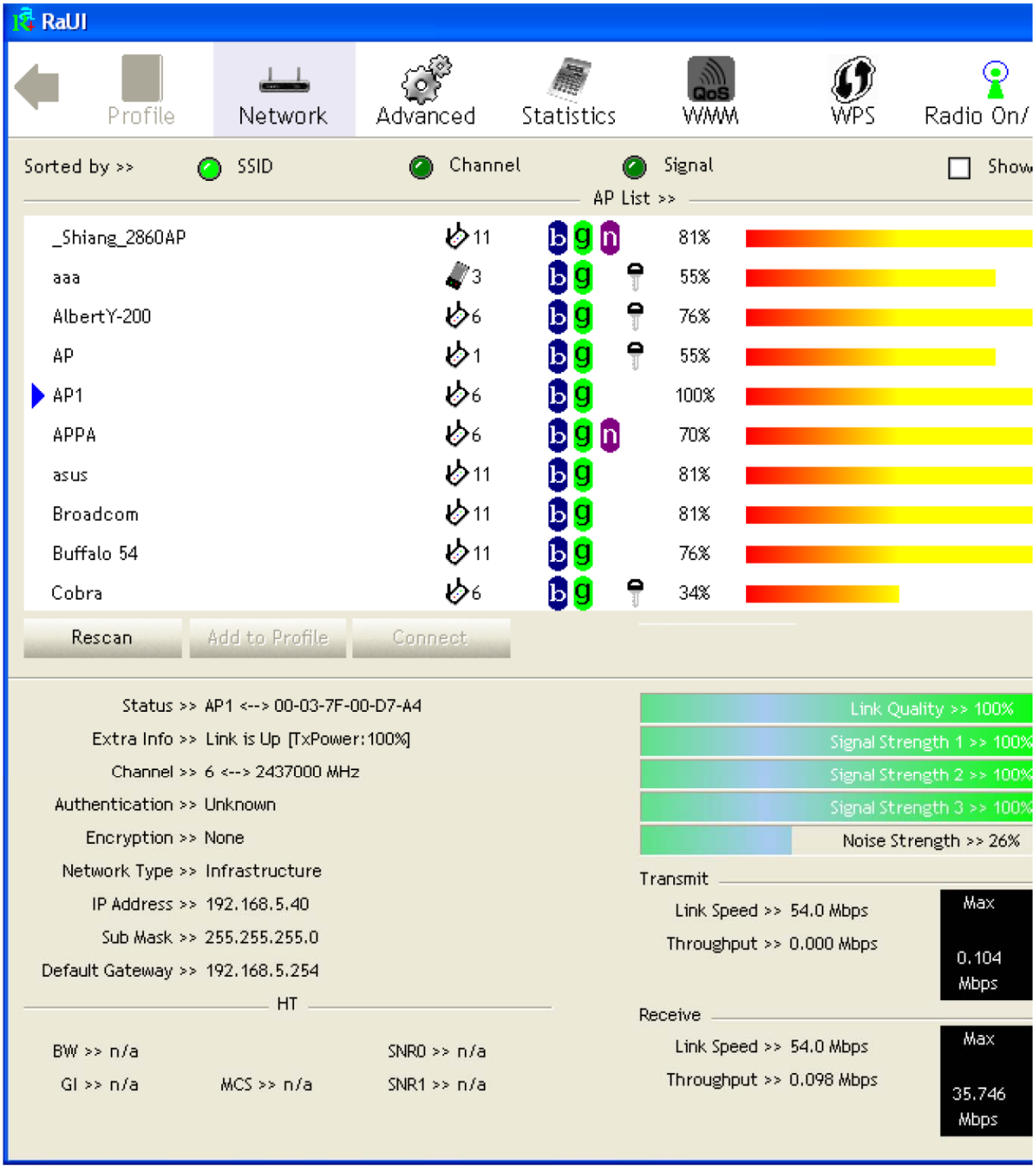
## 1.2 Working with WZC

Go to Section 1.3 if you want to use RaUI instead.

When WZC is activated, the RaUI screen becomes:

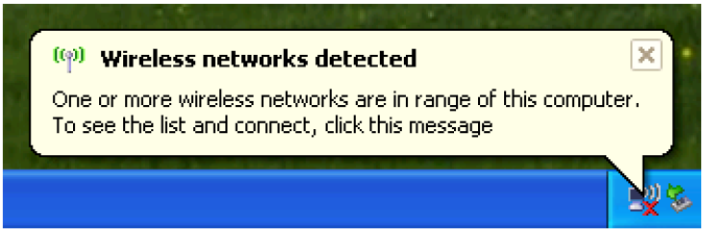
(i) The Profile button turns grey. The profile function is removed since the NIC (i.e. Network Interface Card) is now being controlled by WZC.

(ii) The Connect and Add Profile functions turn grey.

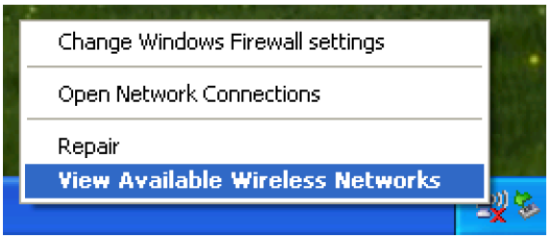



## *1.2.1 Configuration of NIC by using WZC*

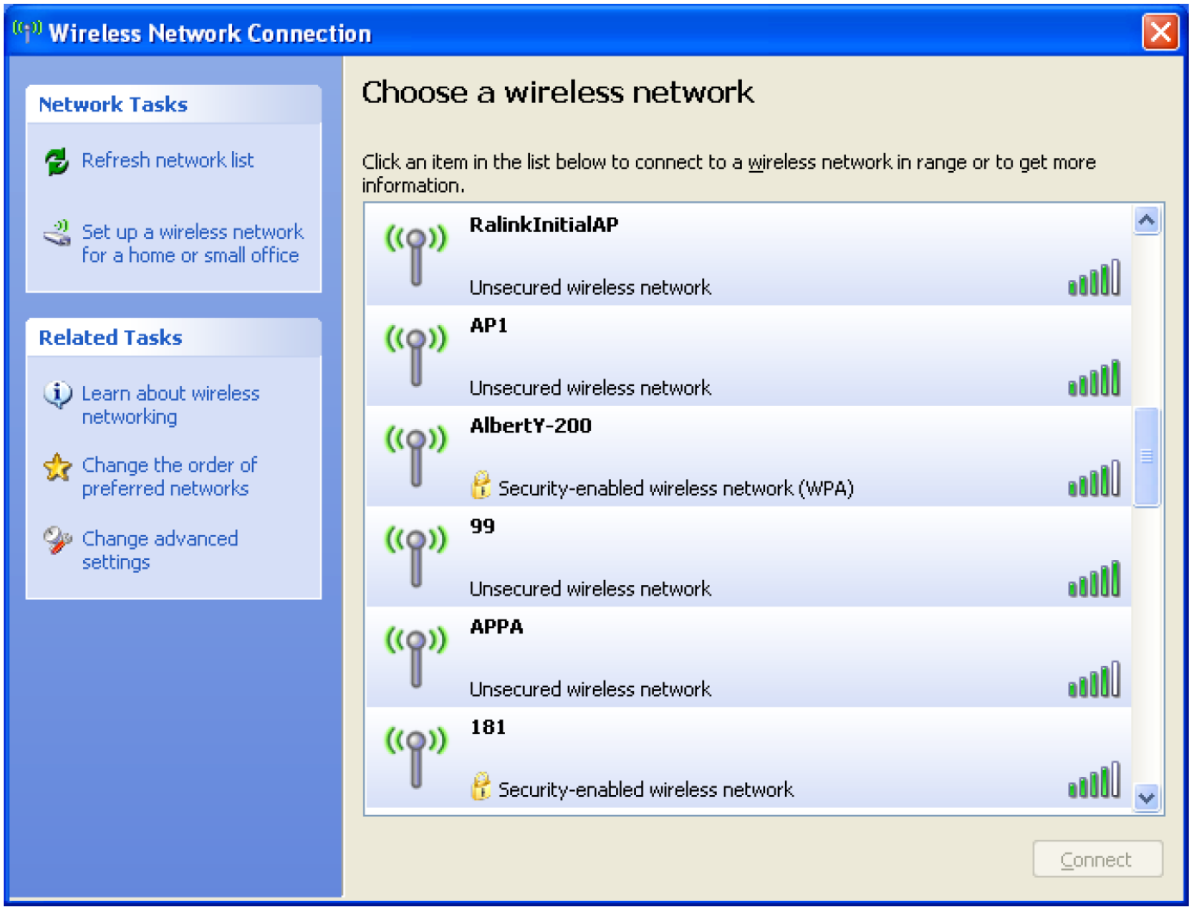
Before you connect to any wireless network, the status prompt pops up like this:



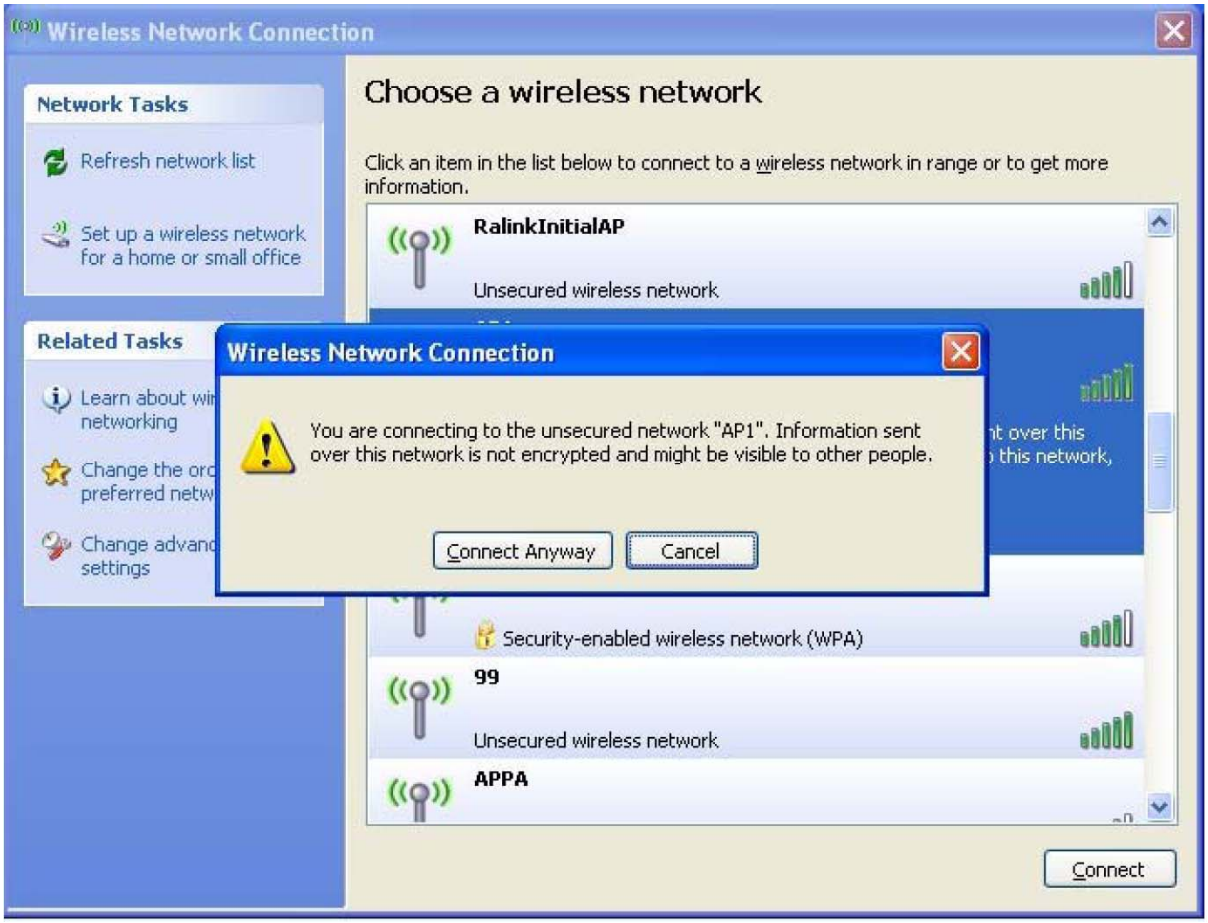
Right click the Network Connection icom in the task bar, and select "View Available Wireless Networks:

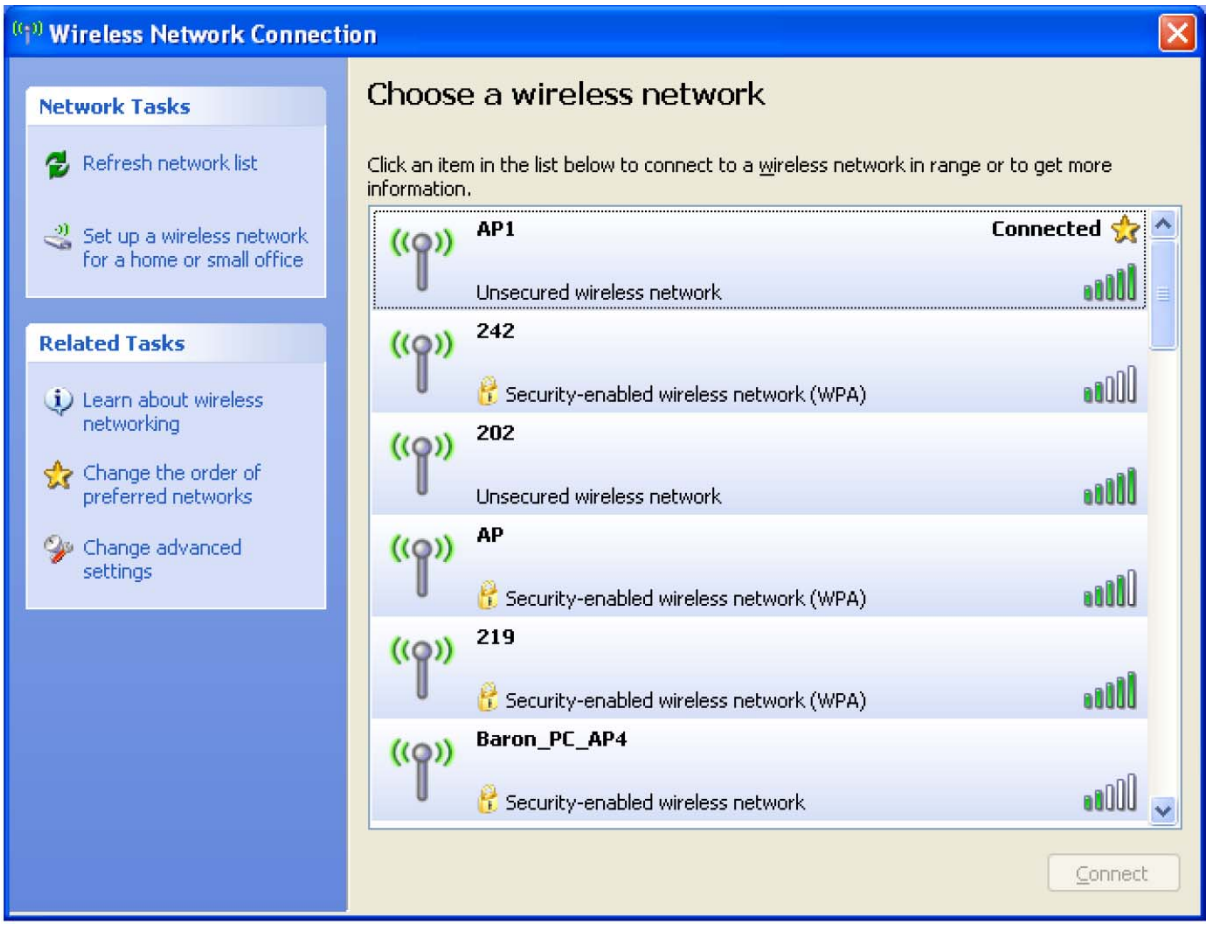



A new window pops up showing the list of AP available for connection.

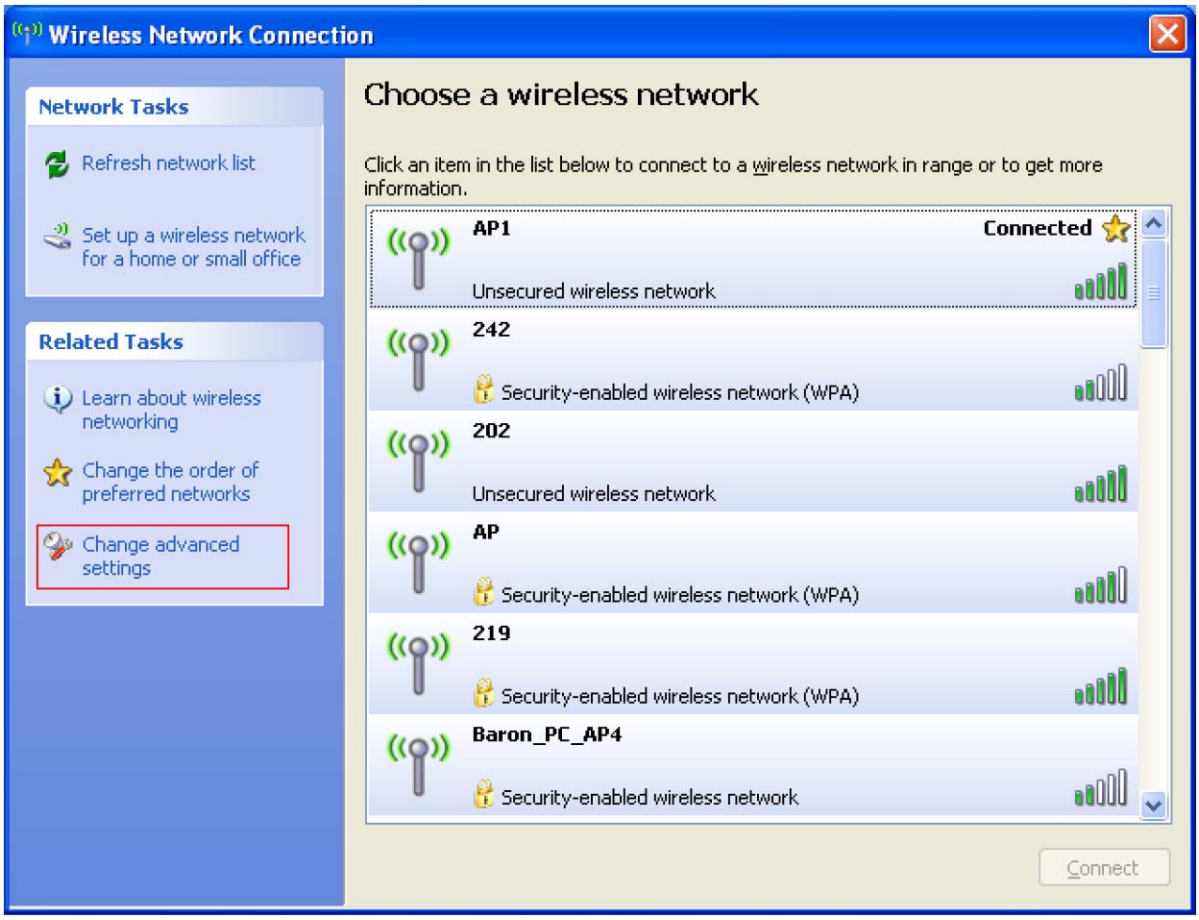



You may either double click the AP or highlight it with the mouse pointer followed by clicking "Connect Anyway".

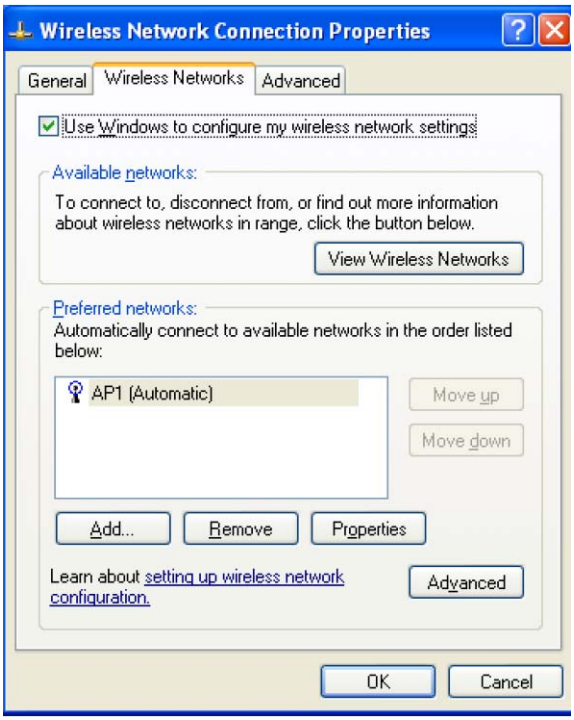

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wi networking
Change the orc preferred netw
Change advanc settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
RalinkInitialAP
Unsecured wireless network
Wireless Network Connection
You are connecting to the unsecured network "AP1". Information sent over this network is not encrypted and might be visible to other people.
Connect Anyway
Cancel
t over this this network,
Security-enabled wireless network (WPA)
99
Unsecured wireless network
APPA
Connect

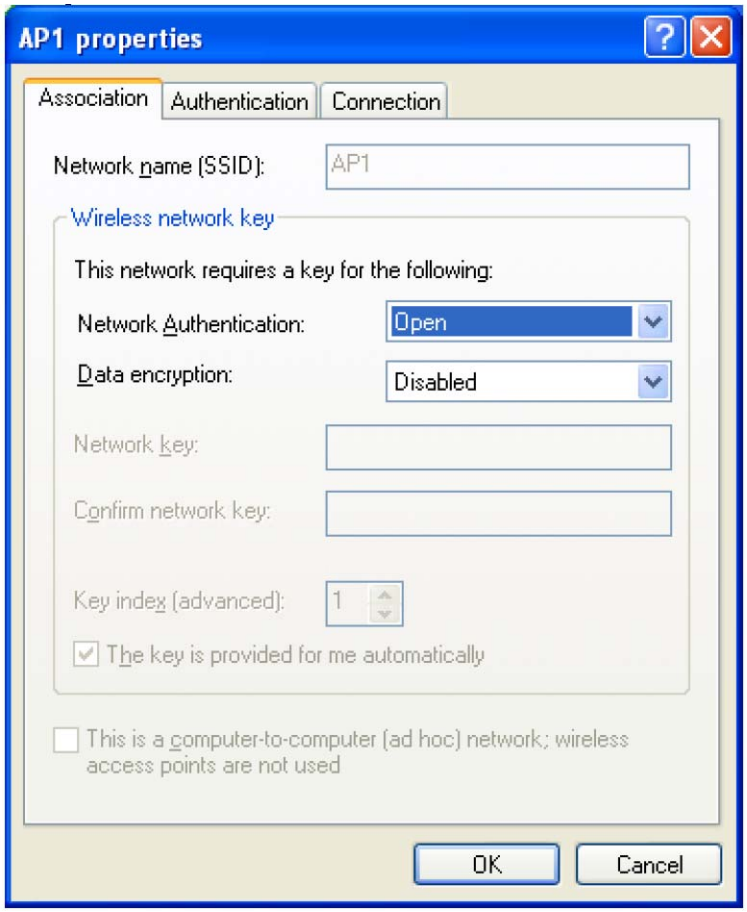

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
AP1
Connected
Unsecured wireless network
242
Security-enabled wireless network (WPA)
202
Unsecured wireless network
AP
Security-enabled wireless network (WPA)
219
Security-enabled wireless network (WPA)
Baron_PC_AP4
Security-enabled wireless network
Connect

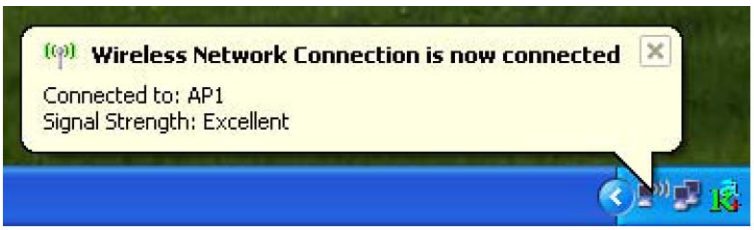
If you want to update the AP attributes, click “Change Advanced Settings”.




Then choose the “Wireless Networks”.



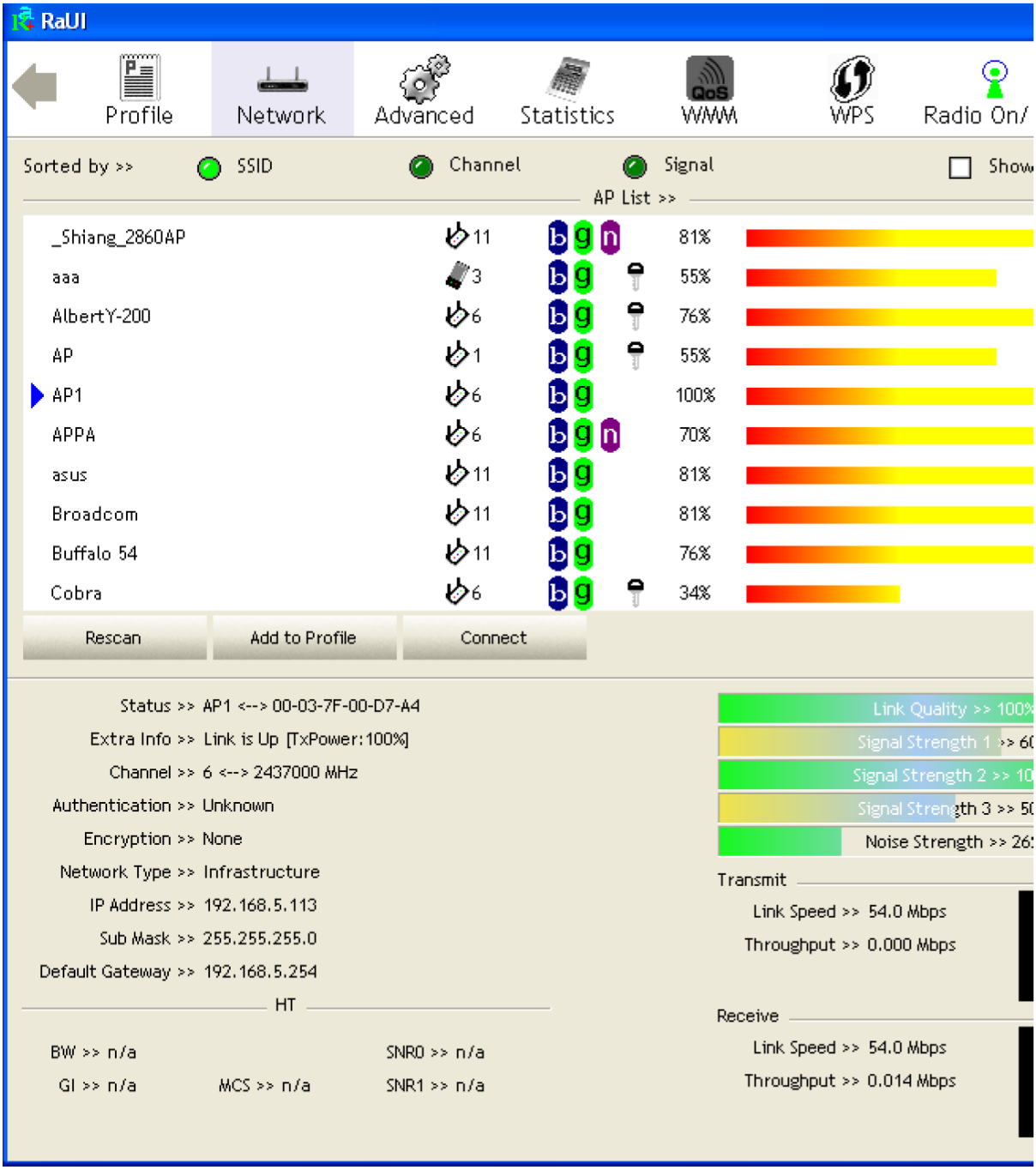



## 1.3 Working with RaUI

When RaUI is active, a small RaUI icon appears at the lower right hand corner of the screen.

Click on it to bring up the RaUI main window and you may see a list of AP picked up by the antenna. Each row contains the SSID, network type, channel used, wireless mode, security status and signal strength.




Simply highlight the AP and click “Connect”. If the AP is encrypted, you shall then be asked to enter the password for authentication.

Once connected, a small blue arrow appears on the left of the AP.

How does the RaUI icon represent the various network statuses? Here are the clues:

- Connected and signal strength is Good.
- Connected and signal strength is Normal.
- Not Connected.
- Wireless NIC not detected.
- Connected but signal strength is Weak.

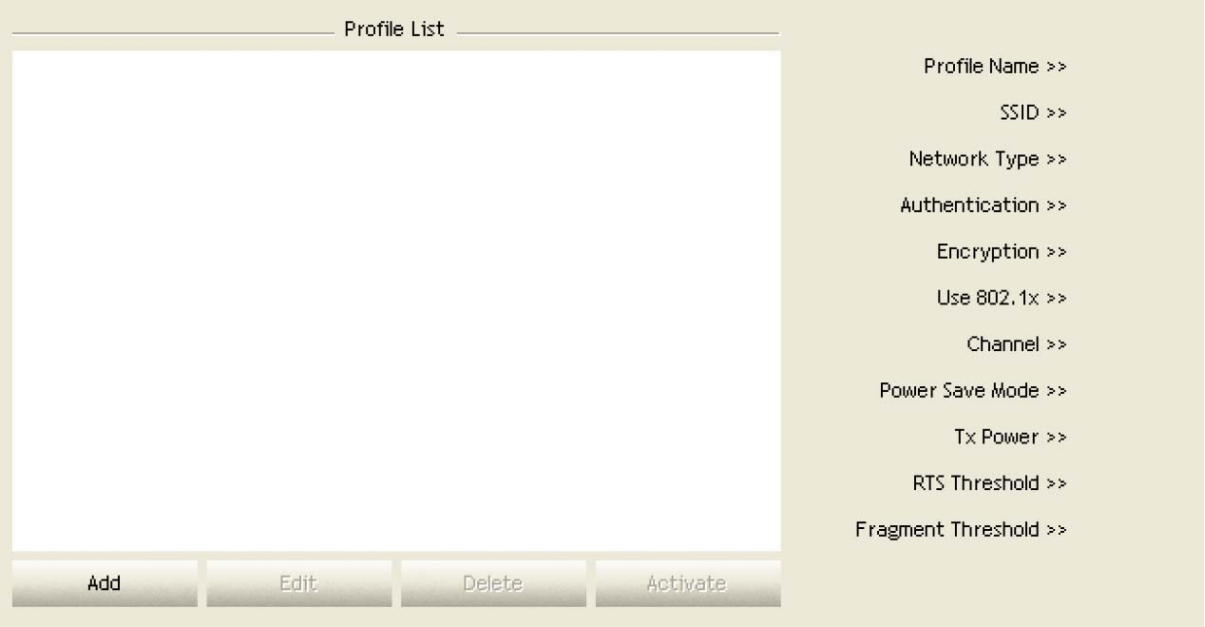
# 2. Advanced RaUI Features

Consists of:

PROFILE
NETWORK
ADVANCED
STATISTICS
WMM
WPS
RADIO ON/OFF

## 2.1 PROFILE

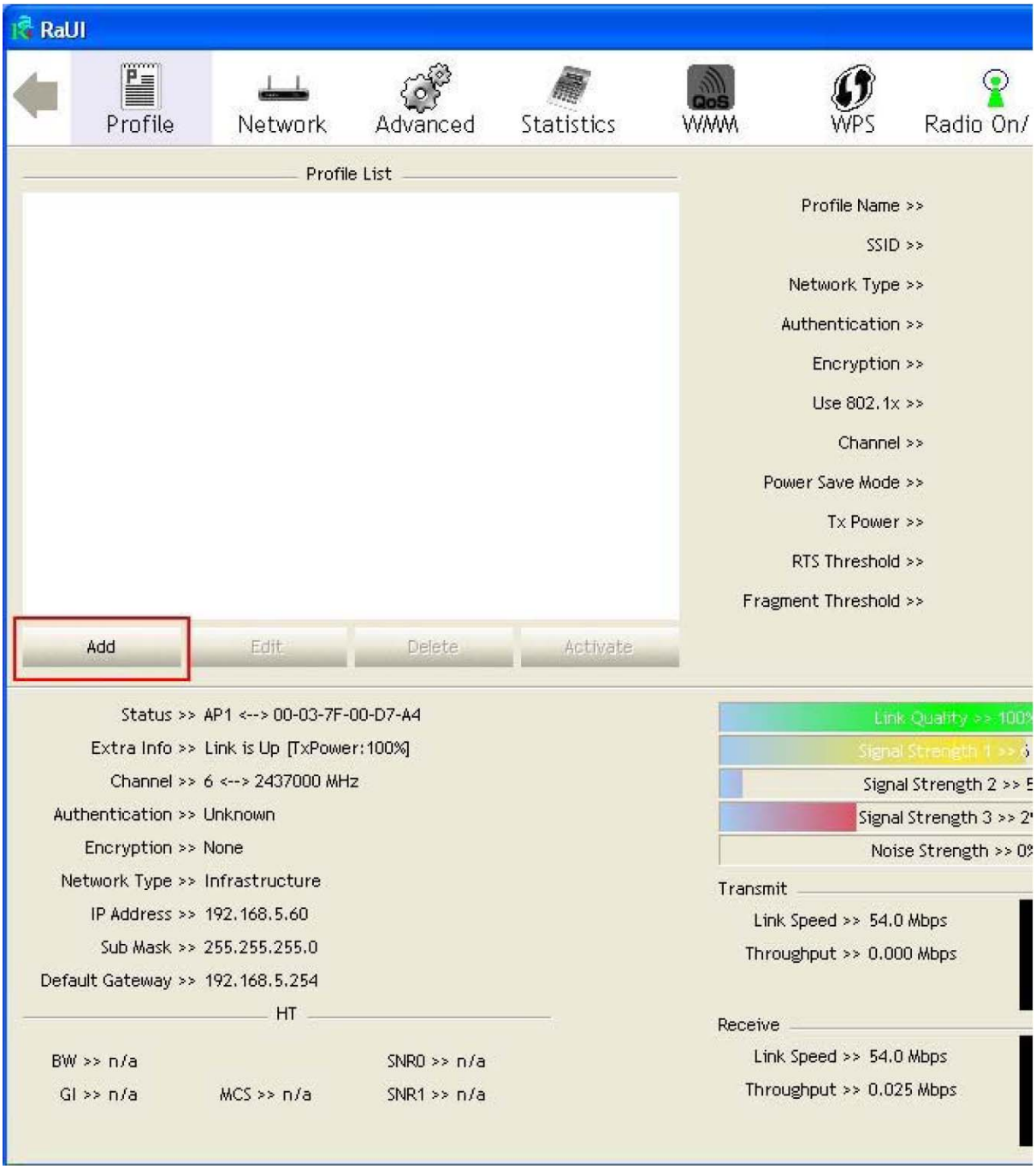
A place to save your favorite wireless networks for one-click connection.



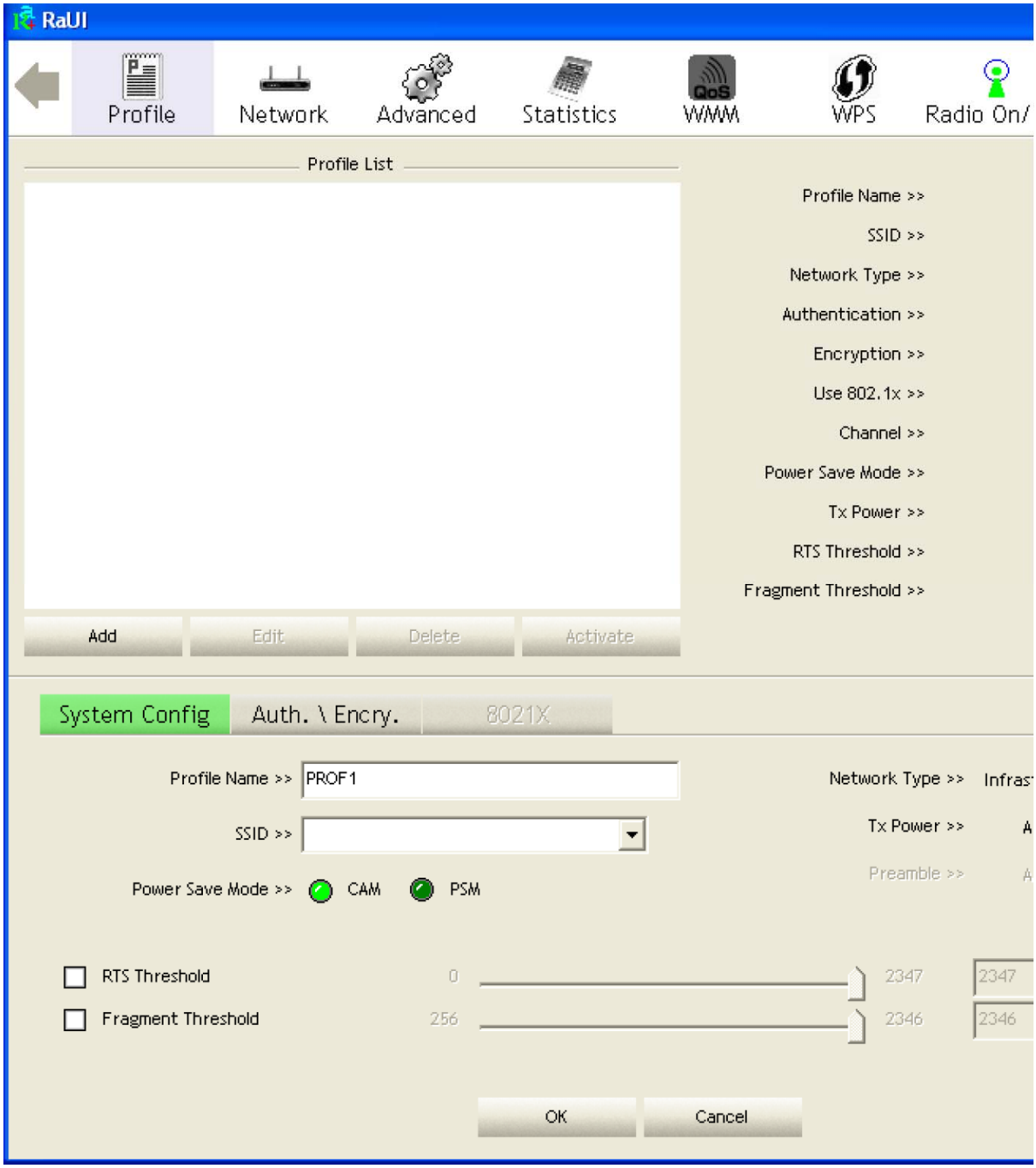

Profile Name: Default is PROF1
SSID: AP or Ad-Hoc name
Network Type: Infrastructure or Ad-Hoc
Authentication: Open, WPA/PSK, WPA2/PSK
Encryption: None, WEP, AES, TKIP
USB802.1x: NO or In use
Tx Power: Auto or Adjustable %
Channel: Auto or Specific channel
RTS Threshold: Data packet size which exceeds the Request To Send (RTS) Threshold will be sent out. Larger packet size favors data transmission whilst small pack size lowers the latency for real time traffic (voice and video).
Fragment Threshold: Longer data fragment increases data throughput performance with good signal quality. The opposite is true to keep shorter data fragment in poor signal quality to maintain an optimal data throughput.

### *2.1.1 Example to Add a PROFILE*

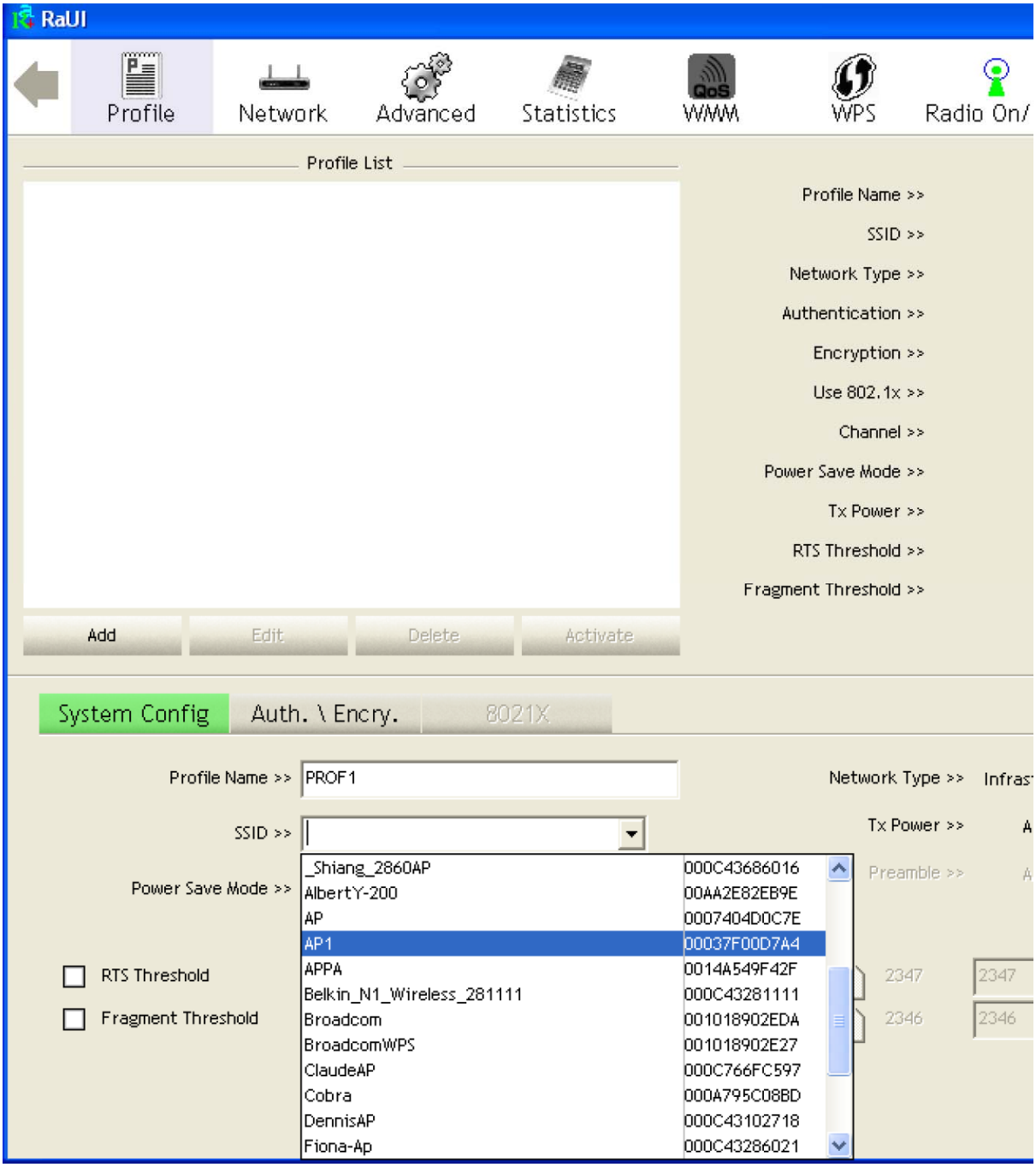
Click “Add” under PROFILE



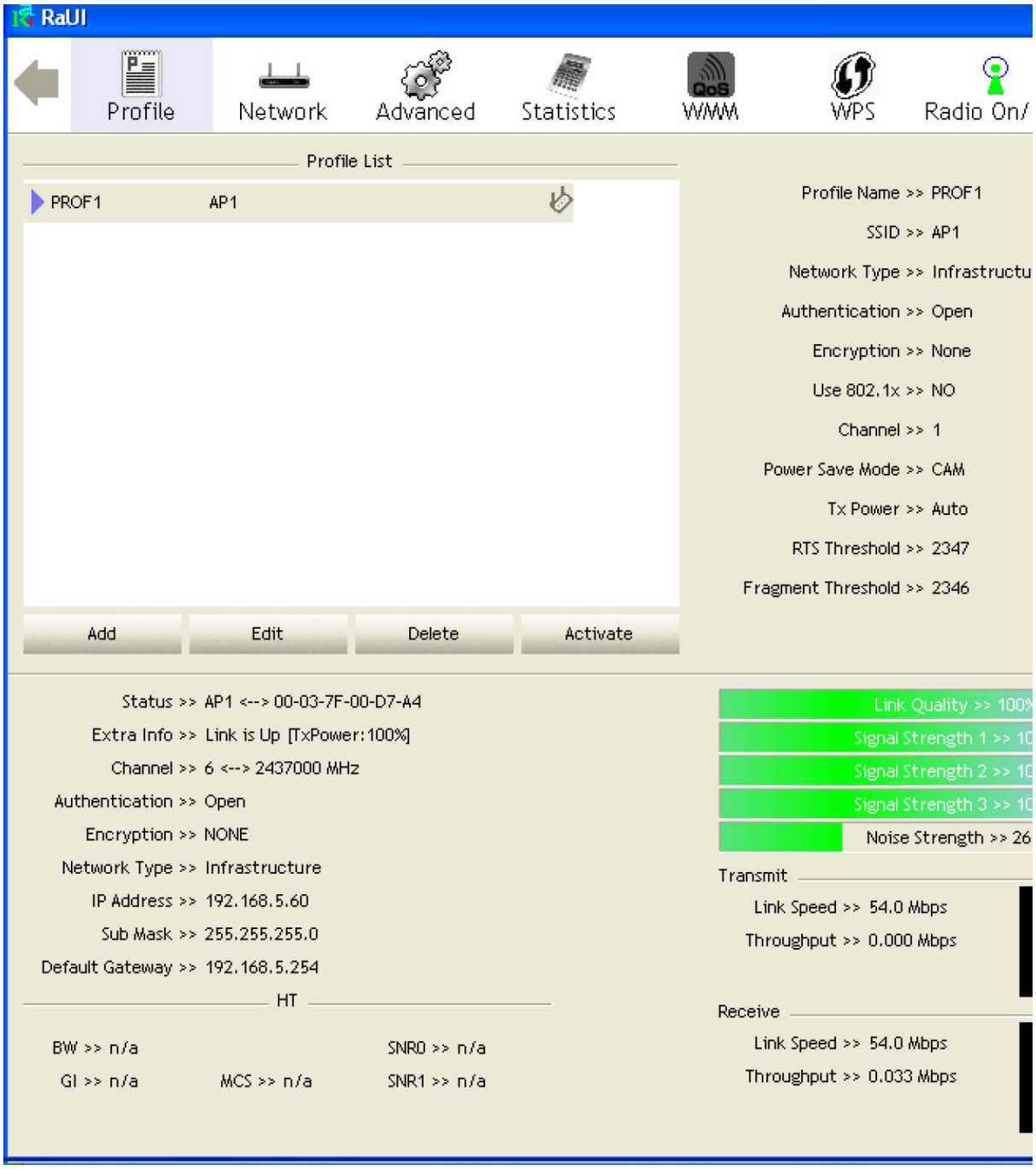

The Add Profile page will then pop up.




The default Profile Name is PROF1 which you may change to a different name. Now move the mouse to the SSID pull down menu and select the AP from an active list.




Suppose that you have chosen AP1 to save the profile, you could now highlight it and click “Activate” to connect.


RaUI
Profile
Network
Advanced
Statistics
WMM
WPS
Radio On/
Profile List
PROF1 AP1
Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructu
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346
Add
Edit
Delete
Activate
Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254
HT
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a
Link Quality >> 100%
Signal Strength 1 >> 10
Signal Strength 2 >> 10
Signal Strength 3 >> 10
Noise Strength >> 26
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps

## 2.2 Network

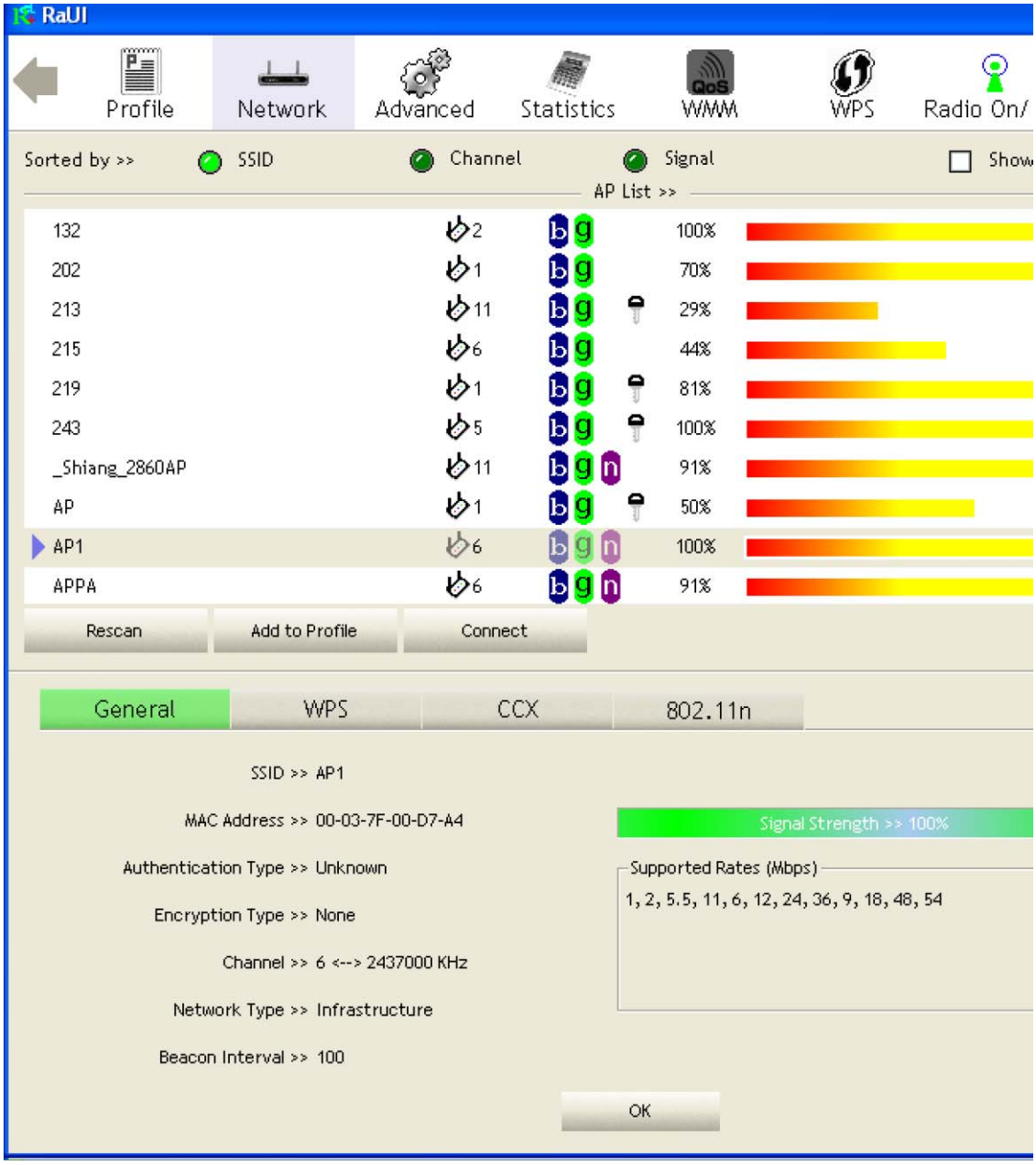
A list of AP picked up by the antenna.


SSID: Name of Wireless Network
Network Type: Infrastructure or Ad-Hoc
Channel: Specific Channel in use
Wireless Mode: 802.11b, 802.11g or 802.11n
Security-Enable: The type of Encryption in use
Signal: Strength in %.

To connect to an AP, simply highlight it, followed by clicking the "Connect" button.

If the intended network has encryption other than "Not Use", the RaUL will bring up the security page which allows the user to enter the password to complete the connection.

When you double click the AP, you can see the AP's detailed information under the buttons of "General", "WPS", "CCX" and "802.11n".




## *2.2.1 Network – General*

The General information contains AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates (Mbps).

The Beacon Interval specifies the duration between beacon packets. Access Points broadcast Beacons or Traffic Indication Messages (TIM) in order to synchronize wireless networks. The default setting of 100 should be ideal for most situations. In a "noisy" environment - one with much interference - decreasing the Beacon Interval may improve network performance. In very remote locations (with few wireless nodes) this value may be increased.

### *2.2.2 Network – WPS*

Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless home network, created by the Wi-Fi Alliance and officially launched on January 8, 2007.
The goal of the WPS protocol is to simplify the process of configuring security on wireless networks, and so it was first named 'Wi-Fi Simple Config'. The protocol is meant to allow home users who know little of wireless security and may be intimidated by the available security options to configure Wi-Fi Protected Access, which is supported by all Wi-Fi certified devices.
The standard achieves its goal by putting much emphasis into usability and security, and the concept is implemented through four usage models that enable a user to establish a home network.

So, to add a new device to the Network the user can have up to the following two choices:
PIN Method, in which a PIN (Personal Identification Number) has to be read from either a sticker on the new wireless client device (STA) or a display, if there is one, and entered at the "representant" of the Network, either the wireless access point (AP) or a Registrar of the Network, cf below the Protocol Architecture.
This is the mandatory baseline model, every Wi-Fi Protected Setup certified product must support it.
PBC Method, in which the user simply has to push a button, either an actual or virtual one, on both the AP (or a Registrar of the Network) and the new wireless client device (STA).
Support of this model is mandatory for APs and optional for STAs.
This page addresses the common scenario involving an Infrastructure Network. The support of ad hoc networks (IBSS) are not supported by WPS.

The WPS information contains the authentication type, encryption type, config methods, device password ID, selected registrar, state, version, AP setup locked, UUID-E and RF bands.

Authentication Type - There are three types of authentication modes supported by RaConfig: OPEN, SHARED, WPA-PSK and WPA system.

Encryption Type – For OPEN and SHARED authentication mode, the selection of encryption type are NONE, WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP AND AES.

Config Methods – This corresponds to the methods the AP supports as an Enrollee for adding external Registrars.

| **Value** | **Hardware Interface** |
|---|---|
| 0x0001 | USBA (Flash Drive) |
| 0x0002 | Ethernet |
| 0x0004 | Label |
| 0x0008 | Display |
| 0x0010 | External NFC Token |
| 0x0020 | Integrated NFC Token |
| 0x0040 | NFC Interface |
| 0x0080 | Push Button |
| 0x0100 | Keypad |

Device Password ID – This indicates the method or indentifies password that the selected Registrar intends to use. AP in PBC mode must indicate 0x0004 within two minutes.

| Value | Description |
|---|---|
| 0x0000 | Default (PIN) |
| 0x0001 | User-specified |
| 0x0002 | Rekey |
| 0x0003 | Display |
| 0x0004 | Push Button (PBC) |
| 0x0005 | Registrar-specified |
| 0x0006-0x000F | Reserved |

Selected Registrar – This indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

State – The current configuration state on AP. The values are "Un-configured" and "Configured".

Version – WPS specified version.

AP Setup Locked – This indicate if the AP has entered a setup locked state.

UUID-E – The universally unique identifier (UUID) element generated by the Enrollee, a 16 bytes value.

RF Bands – This indicates all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

### *2.2.3 Network – CCX (Cisco Compatible Extensions)*

The Cisco Compatible Extensions program for Wi-Fi tags allows customers with a Cisco Unified Wireless Network and a Cisco Location solution to benefit from the latest innovation and technology advancements offered by Cisco's technology partners. This program offers improved consistency and interoperability among Cisco's Compatible Extensions technology partners.

The CCX information contains CCKM, Cmic and Ckip.

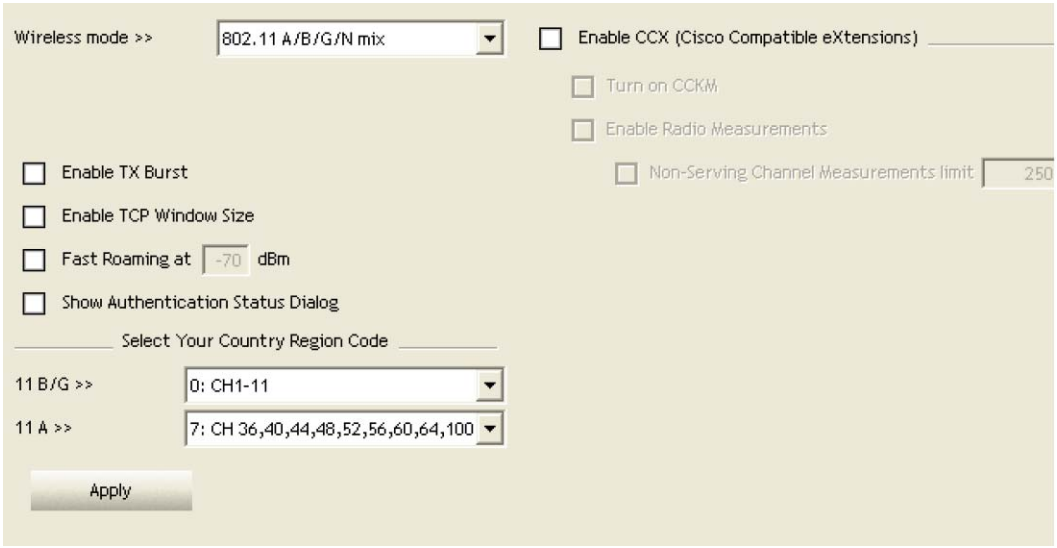
CCKM, CMIC and CKIP are Cisco proprietary protocols for Aironet 350.

### *2.2.4 Network – 802.11n*

The 802.11n button appears only for AP supporting it.

The box contains debugging information for internal RaLink engineer use.

## 2.3 ADVANCED




Wireless Mode – default with 802.11b/g/n mix at 2.4GHz

Enable Tx Burst: RaLink's proprietary frame burst mode.

Enable TCP Window Size – Select to enhance throughput under a low-noise environment.

Fast Roaming at: The threshold of Tx power to switch from one AP to another.

Select Your Country Code – Eight countries to choose. Default at 0: CH1-11. (the 11A box shows up only for A/B/G adapter).

Enable CCX (Cisco Compatible Extension) - On/Off.

## 2.4 STATISTICS

The statistics page displays the detail counter information based on 802.11 MIB counters.

### *2.4.1 Transmit Statistics*


Frames Transmitted Successfully – Frames successfully sent.

Frames Fail To Receive ACK After All Retries – Frames failed transmit after reaching the retry limit.

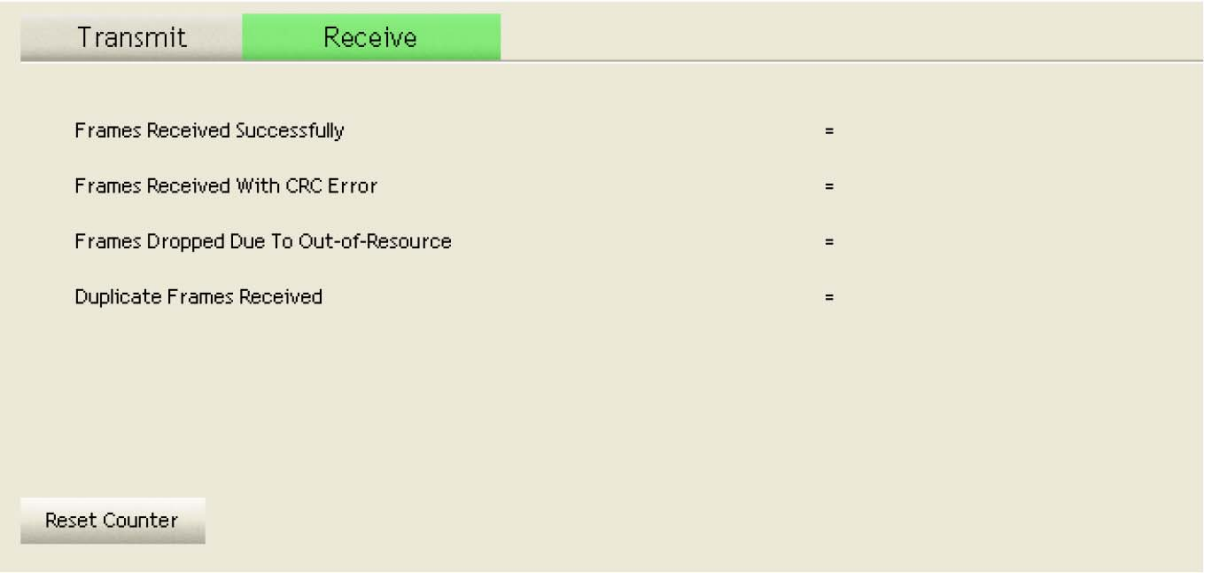
RTS Frames Successfully Receive CTS – Successfully receive CTS after sending RTS frame.

RTS Frames Fail To Receive CTS – Failed to receive CTS after sending RTS.

Frames Retransmitted Successfully – Successfully retransmitted frame numbers.

Reset Counter – Back to zero.

### *2.4.2 Receive Statistics*




Frames Received Successfully – Frames received successfully.

Frames Received With CRC Error – Frames received with CRC error.

Frames Dropped Due To Out-of-Resource – Frames dropped due to resource issue.

Duplicate Frames Received – Duplicate received frames.

Reset Counter – Back to zero.

## 2.5 WWM


WWM Enable – Enable to handle the QoS (Quality of Service) latency sensitive WiFi Multimedia (Audio, Video) traffic.

Power Save Enable – Enable WWM power saving in accordance to the various Multimedia IP traffic.

AC_BK – Backgound (Latency insensitive) IP traffic,

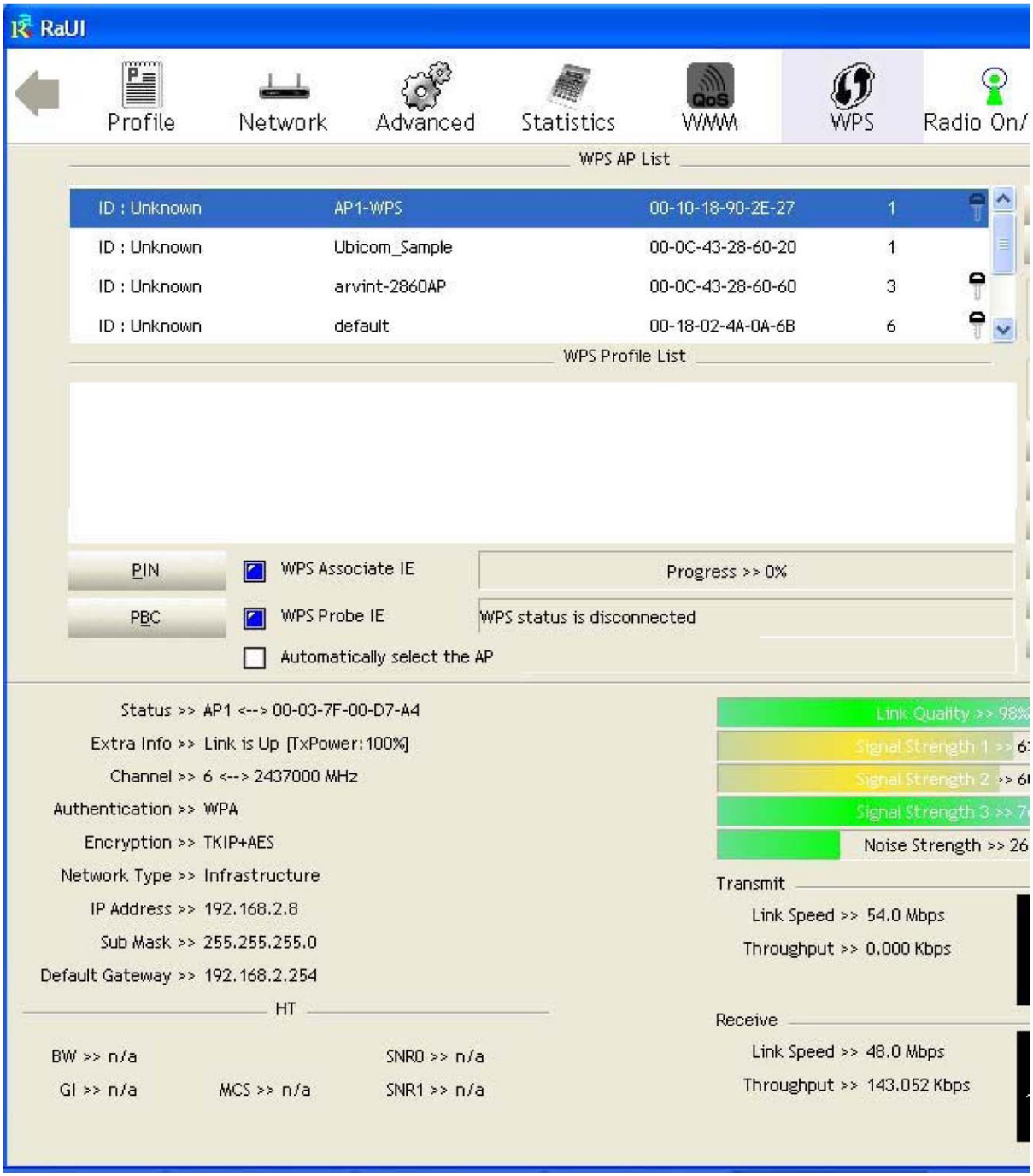
AC_BE – Best effort (Low latency) IP traffic.

AC_VI – Video (real time) IP traffic.

AC_VO – Voice (real time) IP traffic.

Enable Link Setup (DLS) Enable – This allows secured connection to an AP supporting DLS. Simply enter the MAC address in the box which is also registered in the AP. The timeout value ranges from 0 to 65536 seconds. 0 means always on. Default is 60 second.

## 2.6 WPS




WPS Configuration – The primary goal of WiFi Protected Setup (WiFi Simple Configuration) is to simplify the security setup and management of WiFi networks. Ralink STA as an Enrollee or external Registrar supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS AP List – Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID (Mac address of SSID), Channel, ID (Device Password ID), Security-Enabled status.

Rescan – Update the AP picked up by the adapter.

Information – Display the information about WPS IE on the selected network. List information includes Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF bands.
PIN Code – 8 digit numbers. It is required to enter PIN Code into Registrar using PIN method. When STA is Enrollee, you can use "Renew" button to regenerate a new PIN code.

Config Method – Correspond to the methods the AP supports as an Enrollee for adding an external Registrar.

Table of Credentials - Display all of credentials got from the Registrar. List information include SSID, MAC Address, Authentication and Encryption Type. If STA Enrollee, credentials are created as soon as each WPS success. If STA Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.

Control items on credentials:

Detail - Information about Security and Key in the credential.

Connect - Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile. Rotate - Command to rotate to connect to the next network inside credentials.

Disconnect - Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.

Export Profile - Export all credentials to Profile.

Delete - Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.

PIN - Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.

PBC - Start to add to AP using PBC configuration method.

*When you click PIN or PBC, please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart PIN/PBC or press Disconnect to stop WPS action.

WPS associate IE - Send the association request with WPS IE during WPS setup. It is optional for STA.

WPS probe IE - Send the probe request with WPS IE during WPS setup. It is optional for STA.

Progress Bar - Display rate of progress from Start to Connected status.

Status Bar - Display currently WPS Status.

Automatically select the AP - Start to add to AP by using to select the AP automatically in PIN method.

## 2.7 CCX (Cisco Compatible eXtensions)

CCX works with Cisco WiFi device. Consult Cisco proprietary protocols for Aironet 350 to fill in the corresponding value.

## 2.8 Radio On/OFF

Toggles On/Off to temporally disable the adapter.

End of Manual.

**FCC ID: AMB-JN7**

BearExtender

Model No.: JN7

Model name: Wireless USB Adapter

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

RF exposure statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with the FCC RF Exposure requirements the device must be generally operated with the USB cable marketed with this device to assure a minimum distance of 20 cm between the radiating part (antenna) and any human body.

Note: 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.