User Manual

Wireless-N PCI Adapter

Model: CWP-906

CNet Technology Inc.
www.CNet.com.tw

Table of Contents

1. Introduction

1.1 Welcome

PCI Adapter connects you with IEEE802.11n networks at receiving rate up to an incredible 150 Mbps! By using the reflection signal, 802.11n technology increases the range and reduces "dead spots" in the wireless coverage area. Unlike ordinary wireless networking of 802.11b/g standards that are confused by wireless reflections, 802.11n can actually use these reflections to increase four times transmission range of 802.11g products.

Besides, when both ends of the wireless link are 802.11n products, The PCI can utilize twice radio band to increase three times transmission speed of ordinary 802.11g standard products, and can comply with backwards 802.11b/802.11g standards. Soft AP supported by PCI Adapter can help you establish wireless LAN networking with lowest cost. Besides, WPS (PBC and PIN) encryption method can free you from remembering the long passwords. Complete WMM function makes your voice and video more smooth.

1.2 Product Feature

Complies with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b standards

Provides 32-bit PCI interface

Provides 150 Mbps receiving rate and 150 Mbps sending rate

Supports 20MHz/40MHz frequency width

Auto-detects and changes the network transmission rate

Provides two work modes: Infrastructure and Ad-Hoc

Supports Soft AP to establish your wireless LAN networking with lowest cost

Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standard

Supports WPS (PBC and PIN) encryption method to free you from remembering long passwords

Supports WMM to make your voice and video more smoothly

Supports Windows® 2000, XP 32/64, Vista 32/64, Win 7 32/64

1.3 Contents of Package

One PCI Adapter

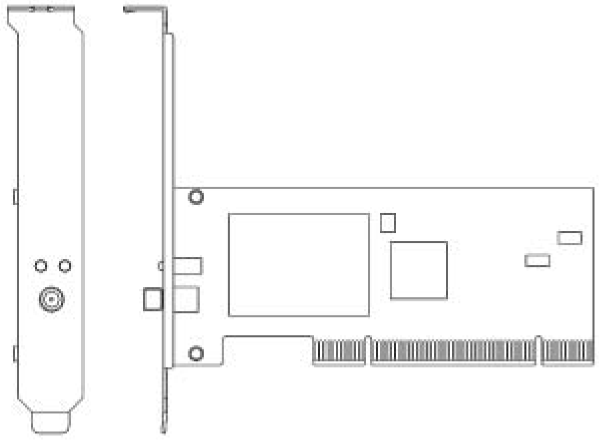
One Installation CD

One dipole antenna

Contact your local authorized reseller or the store where you purchased for any items damaged and/or missing.

2. Designing Your PCI Adapter

PCI Adapter supports up to 150 Mbps connections. It is fully compliant with the specifications defined in 802.11n standard



The status LED indicators of PCI Card are described in the following.

- Link/Act ON (Green): Indicates a valid connection.
- Link/Act Flashing: Indicates the Adapter is transmitting or receiving data

3. Installation

3.1 Install Your PCI Adapter

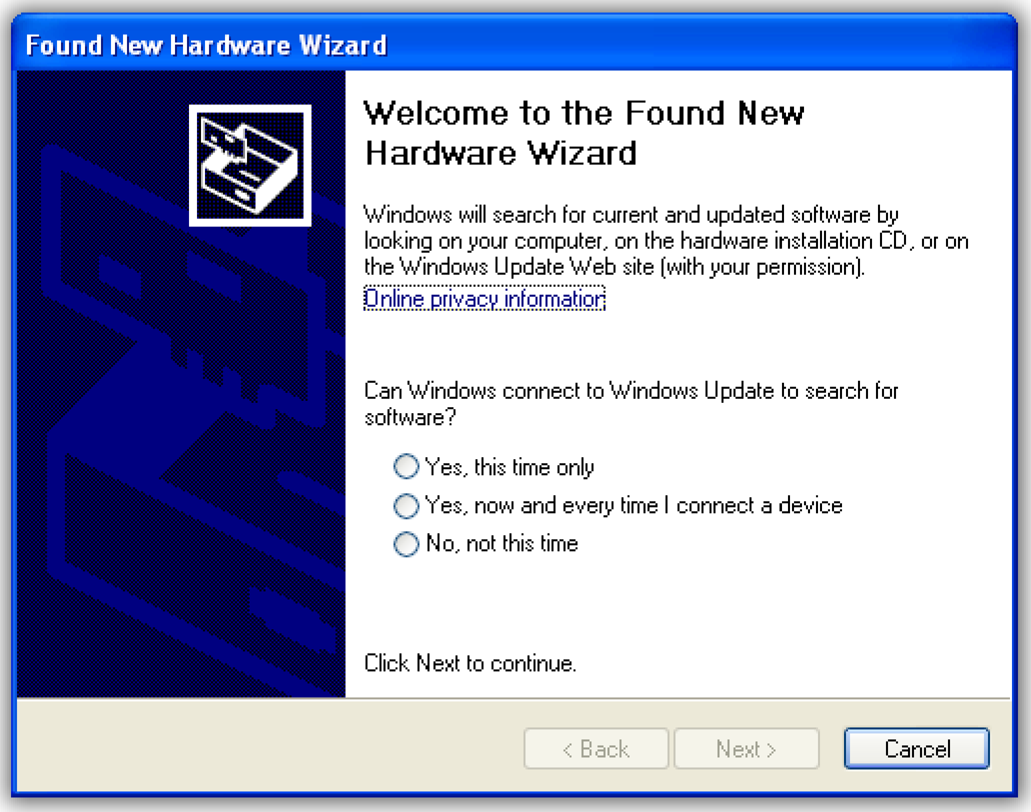
✓ Open your PC case and locate an available PCI on the motherboard.

Slide PCI Adapter into the PCI slot. Make sure that all of its pins are touching the slot's contacts. You may have to apply a bit of pressure to slide PCI Adapter all the way in. after it is firmly in to place, secure its fastening tab to your PC's chassis with a mounting screw. Then close your PC.

Attach the external antennas to PCI Adapter's antenna port.\

Power On the PC.

Note: Select **Cancel button,** when "Found New Hardware" window appears.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Online privacy information

Can Windows connect to Windows Update to search for software?

○ Yes, this time only

○ Yes, now and every time I connect a device

○ No, not this time

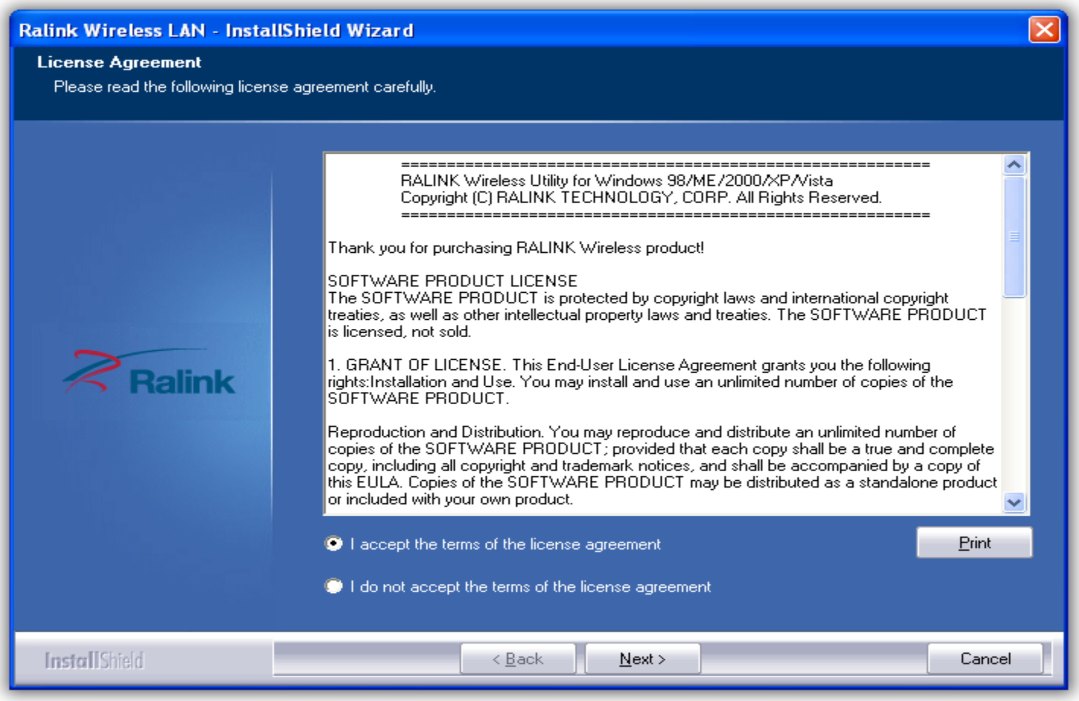
Click Next to continue.

3.2 Install Driver and Utility

NOTE: Snap-shot screens of the following installation procedure are based on Windows XP. installation procedures will be similar for other windows operating systems.

1. Insert Installation CD to your CD-ROM drive. And click **Driver Installation**. The wizard will be run and install all necessary files to your computer automatically.

2. Click **next** to accept the Agreement. Or click **Cancel** to cancel the installation



Ralink Wireless LAN - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

===
RALINK Wireless Utility for Windows 98/ME/2000/XP/Vista
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.
===

Thank you for purchasing RALINK Wireless product!

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

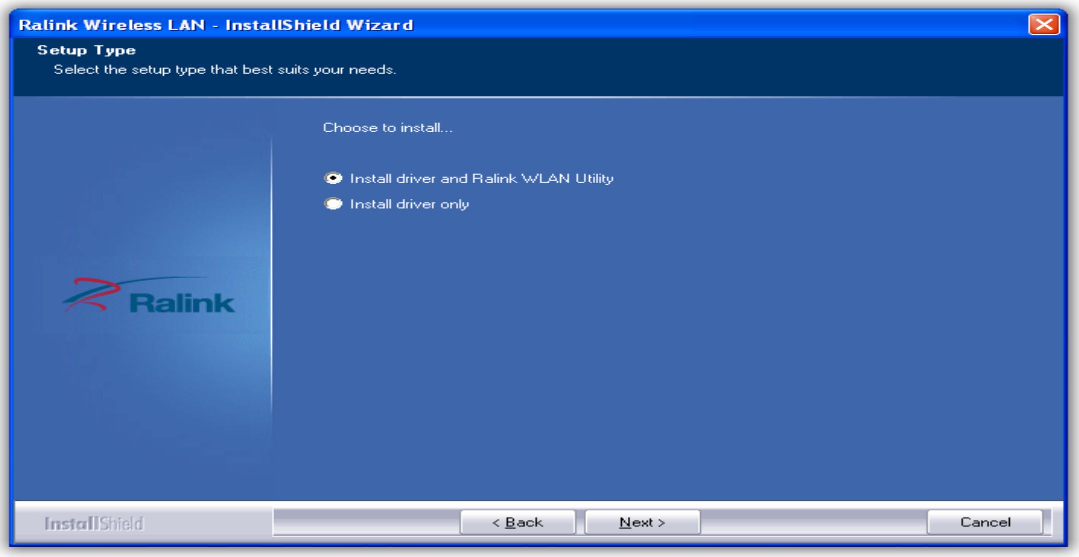
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

3. Click NEXT



Ralink Wireless LAN - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Choose to install...

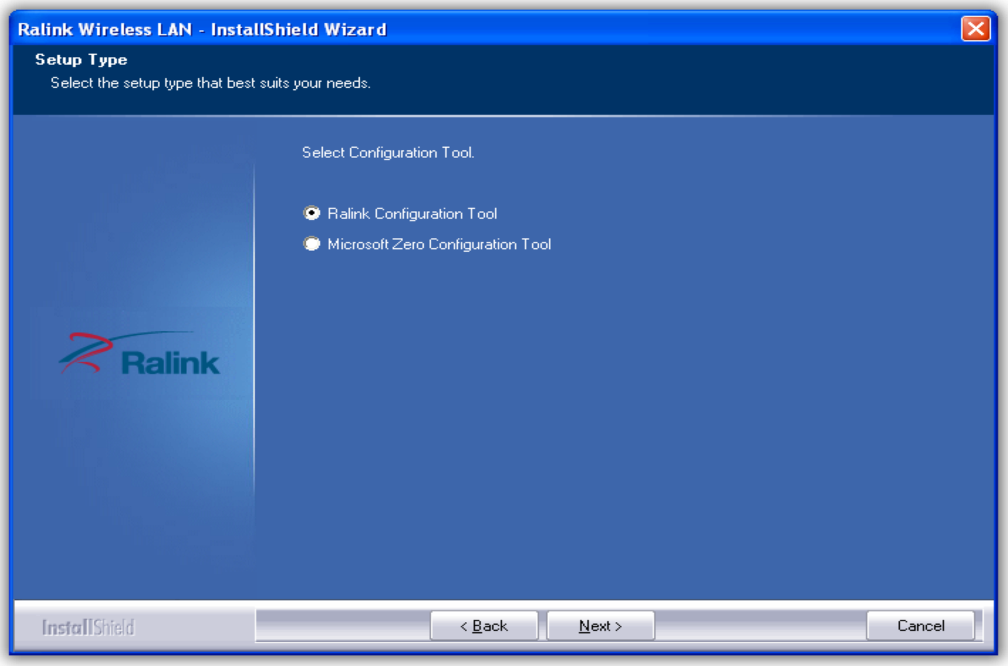
● Install driver and Ralink WLAN Utility

○ Install driver only

4. Select Ralink Configuration Tool or Microsoft Zero Configuration Tool then click Next.

a. It’s recommended to select Ralink Configuration Tool, which provides fully access to all functions of PCI Adapter.

b. If you prefer to use the wireless configuration tool provided by Windows XP or Vista, please select Microsoft Zero Configuration Tool



Ralink Wireless LAN - InstallShield Wizard

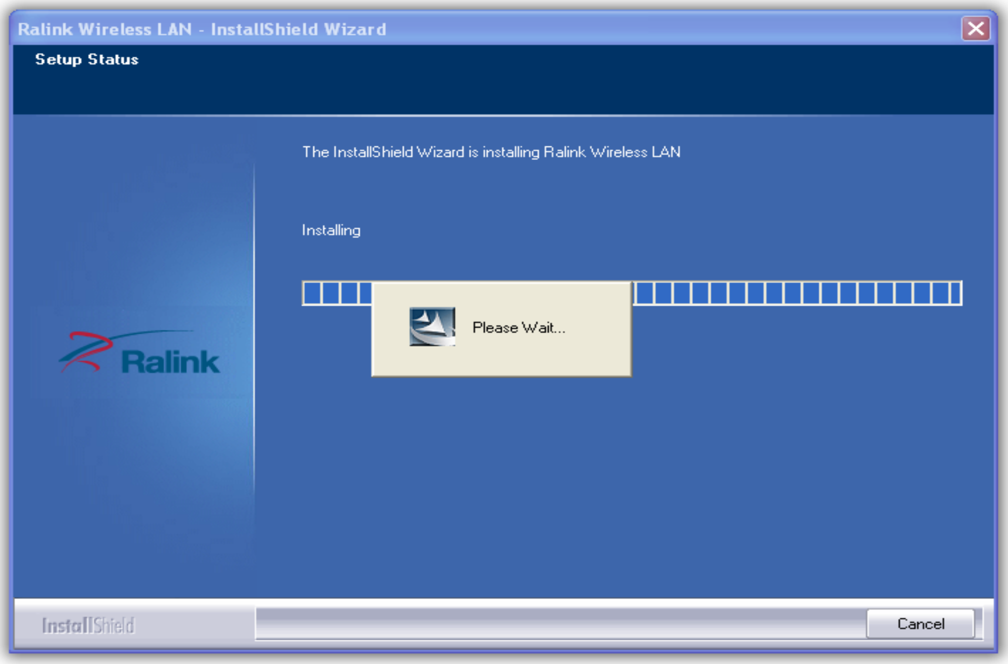
Setup Type

Select the setup type that best suits your needs.

Select Configuration Tool.

● Ralink Configuration Tool

○ Microsoft Zero Configuration Tool



Ralink Wireless LAN - InstallShield Wizard

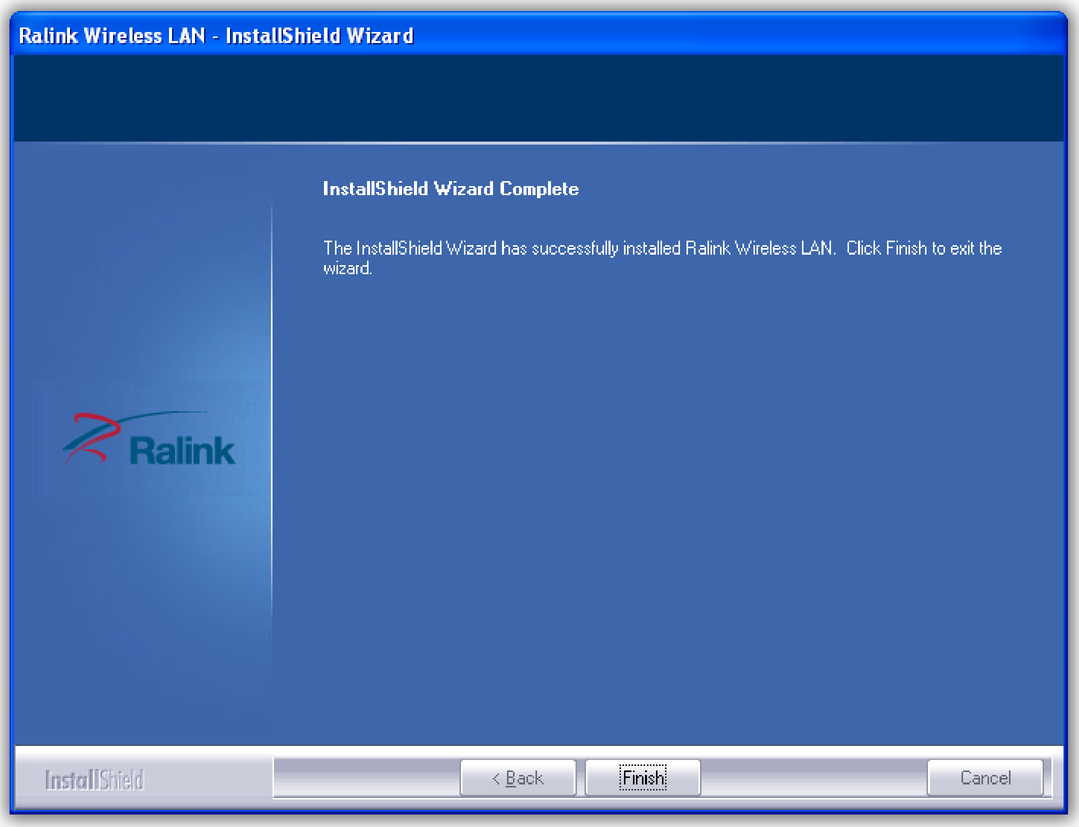
Setup Status

The InstallShield Wizard is installing Ralink Wireless LAN

Installing

Please Wait...

5. Click **Finish** to complete the software installation.



Ralink Wireless LAN - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Ralink Wireless LAN. Click Finish to exit the wizard.

4. Utility Configuration

4.1.1 Ralink Wireless Utility (RaUI) or Windows Zero Configuration (WZC)

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to the Ralink. Wireless NIC. Ralink's utility (RaUI) additionally provides WPA functionality. It’s easier for the user to select the correct utility. RaUI will let users make a selection when it first runs after windows XP boots. Double-clicking the icon will bring up the selection window and allow the user make a selection.

Figure 1-1 RaUI.exe

RaUI can co-exist with WZC. When coexisting with WZC, RaUI only provides monitoring functions, such as surveying the link status, network status, statistic counters, advanced feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-2.

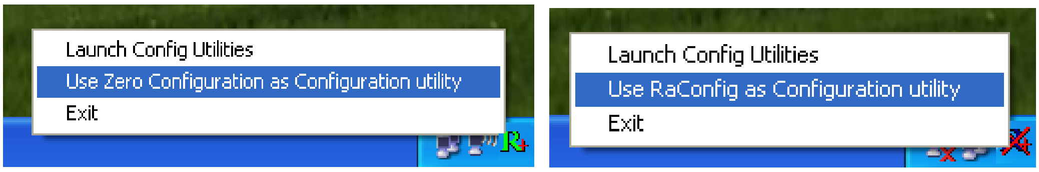
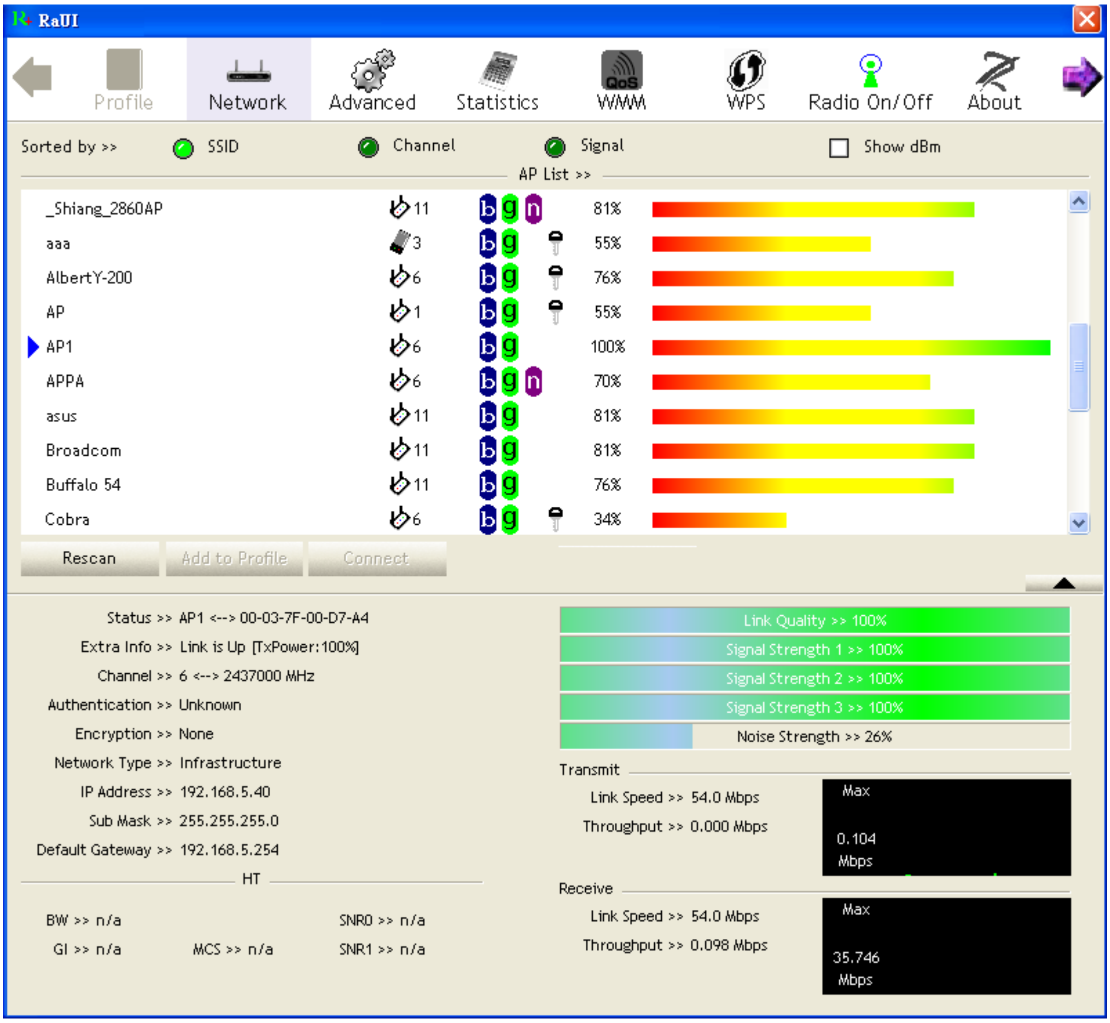

Launch Config Utilities
Use Zero Configuration as Configuration utility
Exit
Launch Config Utilities
Use RaConfig as Configuration utility
Exit

Figure 1-2 Select WZC or RaUI

If "Use RaConfig as Configuration utility" is selected, please jump to Section 2 on running RaUI.

If "Use Zero Configuration as Configuration utility" is selected, please continue.

We will explain the difference between RaUI and WZC. Figure 1-3 shows the RaUI status when WZC is activated as the main control utility.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

SSID	Channel	Mode	Security	Signal
_Shiang_2860AP	11	b g n		81%
aaa	3	b g	🔑	55%
AlbertY-200	6	b g	🔑	76%
AP	1	b g	🔑	55%
AP1	6	b g		100%
APPA	6	b g n		70%
asus	11	b g		81%
Broadcom	11	b g		81%
Buffalo 54	11	b g		76%
Cobra	6	b g	🔑	34%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.40
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 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Max
0.104 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.098 Mbps
Max
35.746 Mbps

Figure 1-3 RaUI status with WZC active

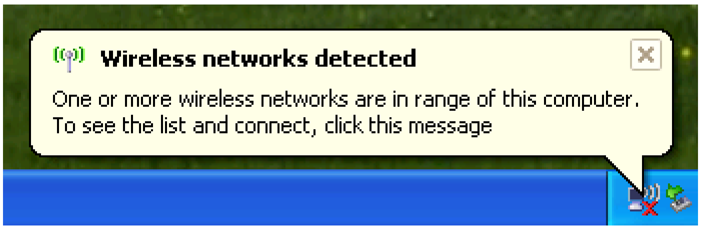
When activating WZC, there are several difference with the RaUI status, compared to the RaUI status without WZC running.

1. The profile button will be gray. Profile functionality is removed since the NIC is controlled by WZC.
2. The connection and add profile function will be gray. Profile functionality is removed since the NIC is controlled by WZC.

Please read through this document for full details on the other functions provided by RaUI.

4.1.2 Use WZC to configure wireless NIC

1. If there is no connection or it is lost, the status prompt will pop up, as shown in Figure 1-4.



Wireless networks detected

One or more wireless networks are in range of this computer.
To see the list and connect, click this message

Figure 1-4 status prompt for no connection

2. Right-click the network connection icon in taskbar

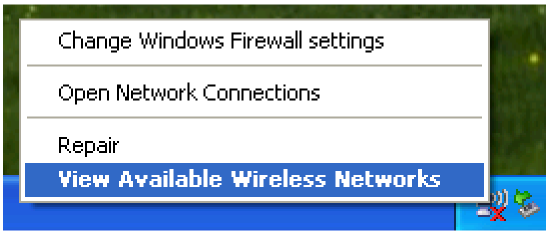
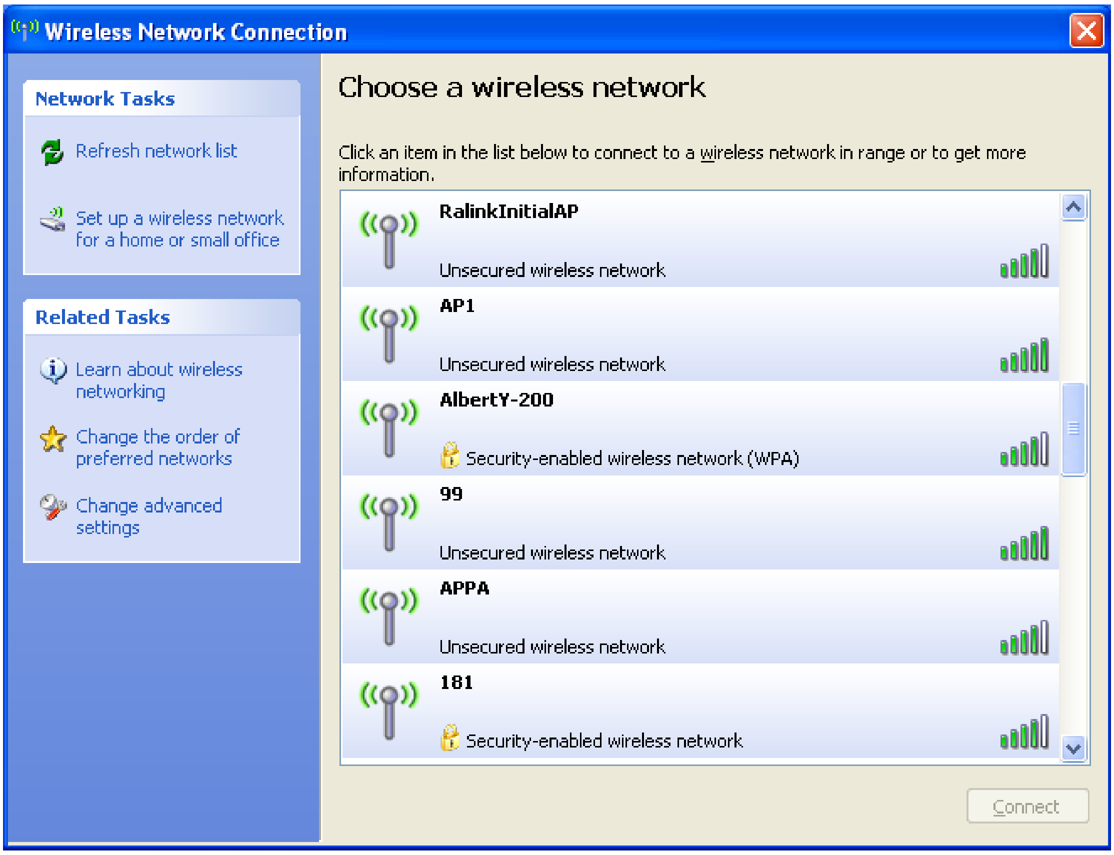

Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

Figure 1-5 Select WZC main status

3. Select "View Available Wireless Networks" and the "Wireless Network Connection" dialog box will pop up, as shown in Figure 1-6.


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
Connect

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

AP1
Unsecured wireless network

AlbertY-200
Security-enabled wireless network (WPA)

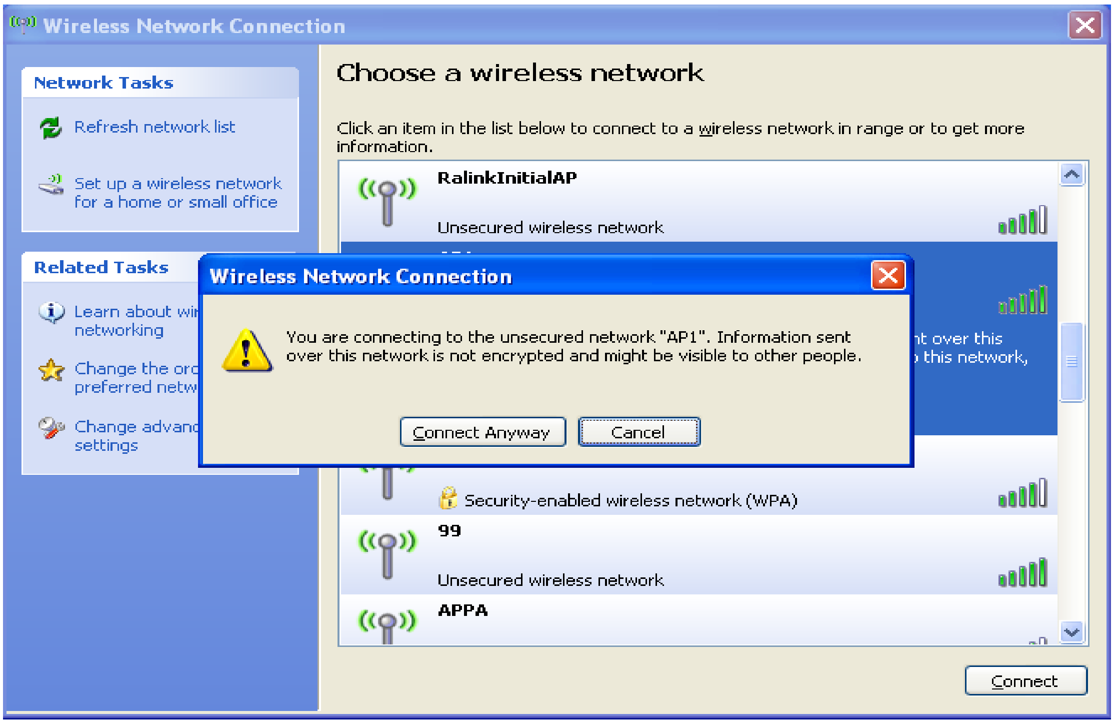
99
Unsecured wireless network

APPA
Unsecured wireless network

181
Security-enabled wireless network

Figure 1-6 Wireless Network Connection

4. Select the intended access point and click "Connect". Then click "Connect Anyway" as shown as Figure 1-7.



Wireless Network Connection

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

Security-enabled wireless network (WPA)

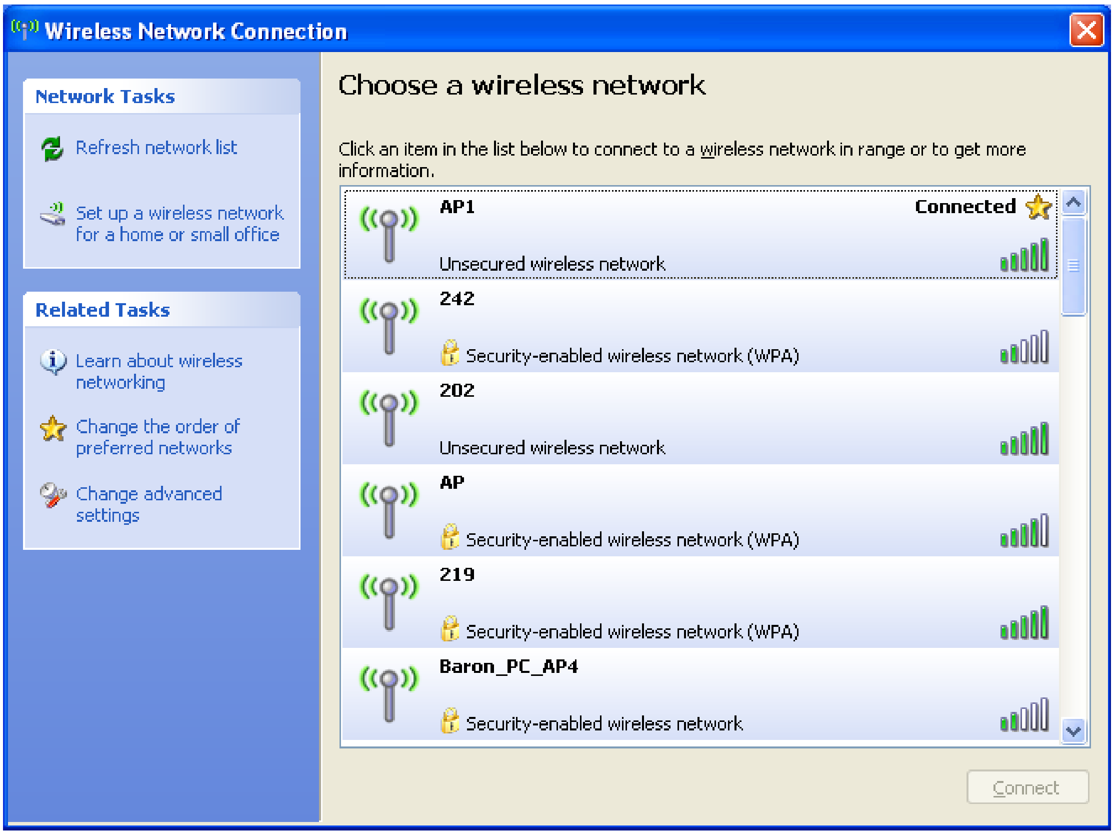
99
Unsecured wireless network

APPA

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.

Figure 1-7 Select intended AP : AP1, then click "Connect"



Wireless Network Connection

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)

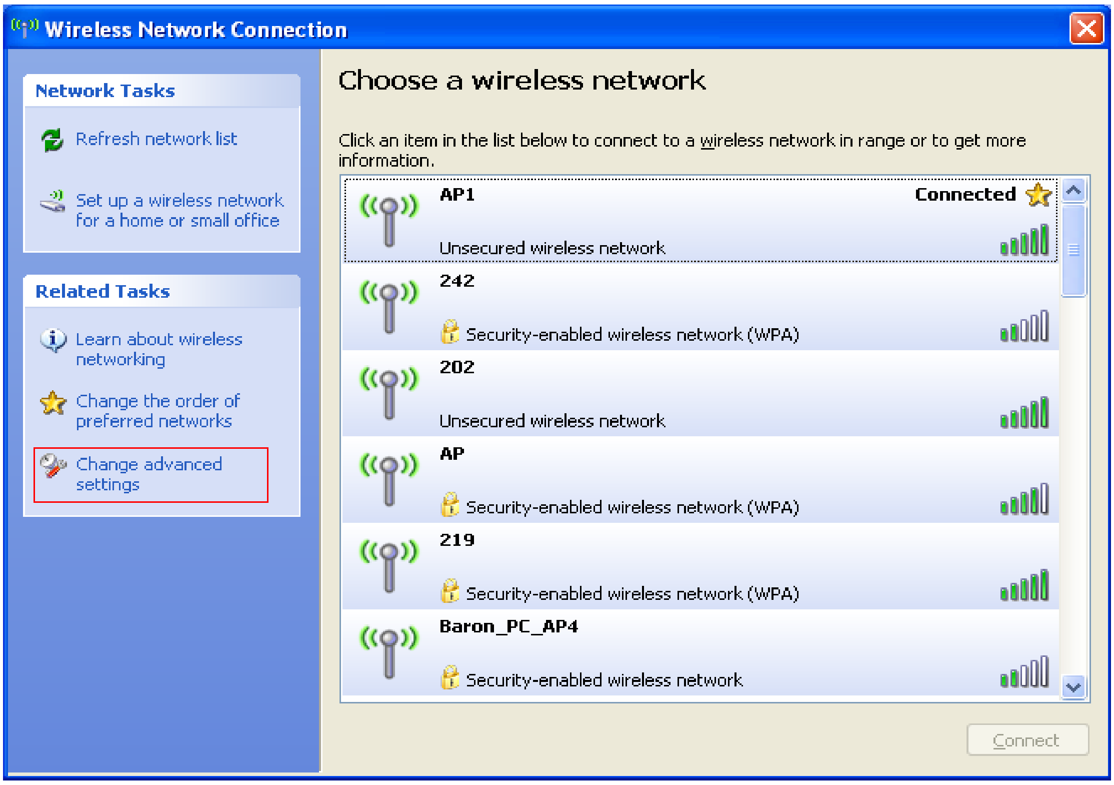
219
Security-enabled wireless network (WPA)

Baron_PC_AP4
Security-enabled wireless network

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
Connect

Figure 1-8 Connect AP: AP1 successfully

5. If you want to modify information about the AP, click "Change advanced settings" as shown in Figure 1-9. Then select the "Wireless Networks" tab shown as Figure 1-10.



Wireless Network Connection

Network Tasks

- Refresh network list
- Set up a wireless network for a home or small office

Related Tasks

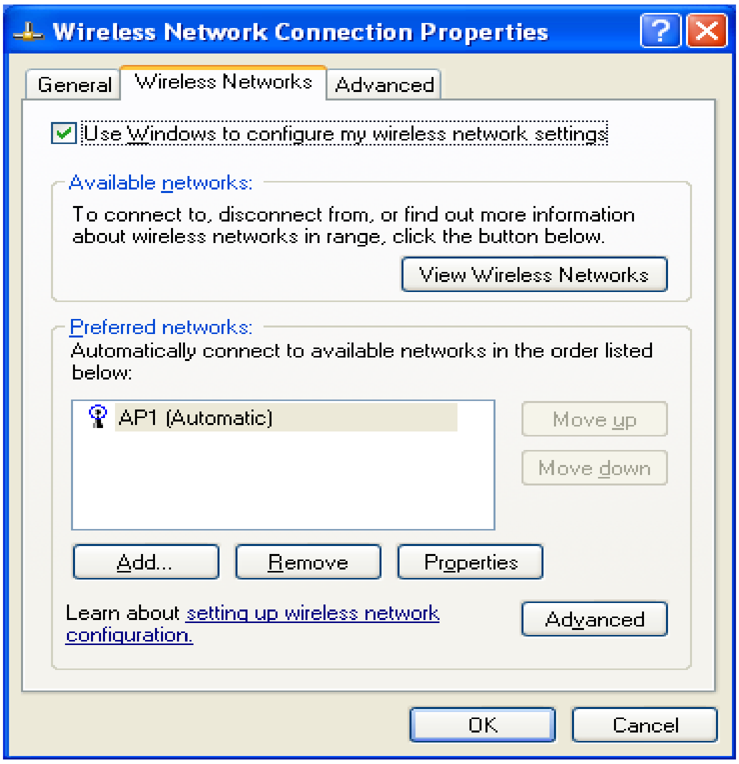
- Learn about wireless networking
- Change the order of preferred networks
- Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Network	Status	Security
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

Figure 1-9 Click "Change advanced settings"



Wireless Network Connection Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

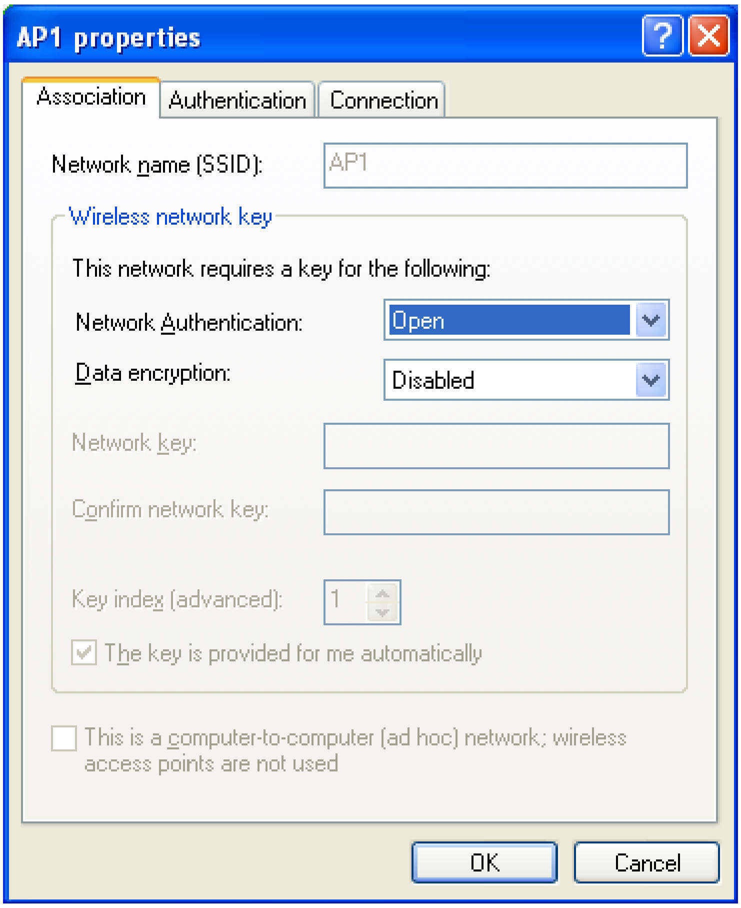
Automatically connect to available networks in the order listed below:

AP1 (Automatic)

Learn about setting up wireless network configuration.

Figure 1-10 Choose the "Wireless Networks" tab

6. Click "Properties" as shown in Figure 1-11. Then click "OK" button.



AP1 properties

Network name (SSID): AP1

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key:

Confirm network key:

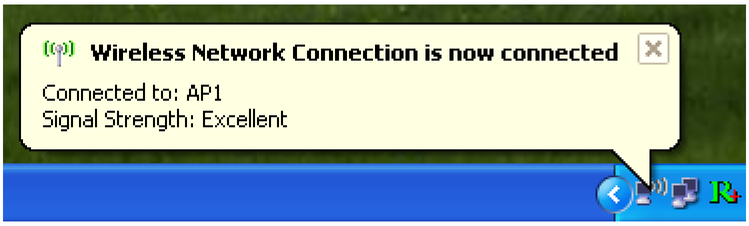
Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 1-11 AP's properties

7. After filling in the appropriate value, click "OK." The pop-up will indicate the status. as shown in Figure 1-12.

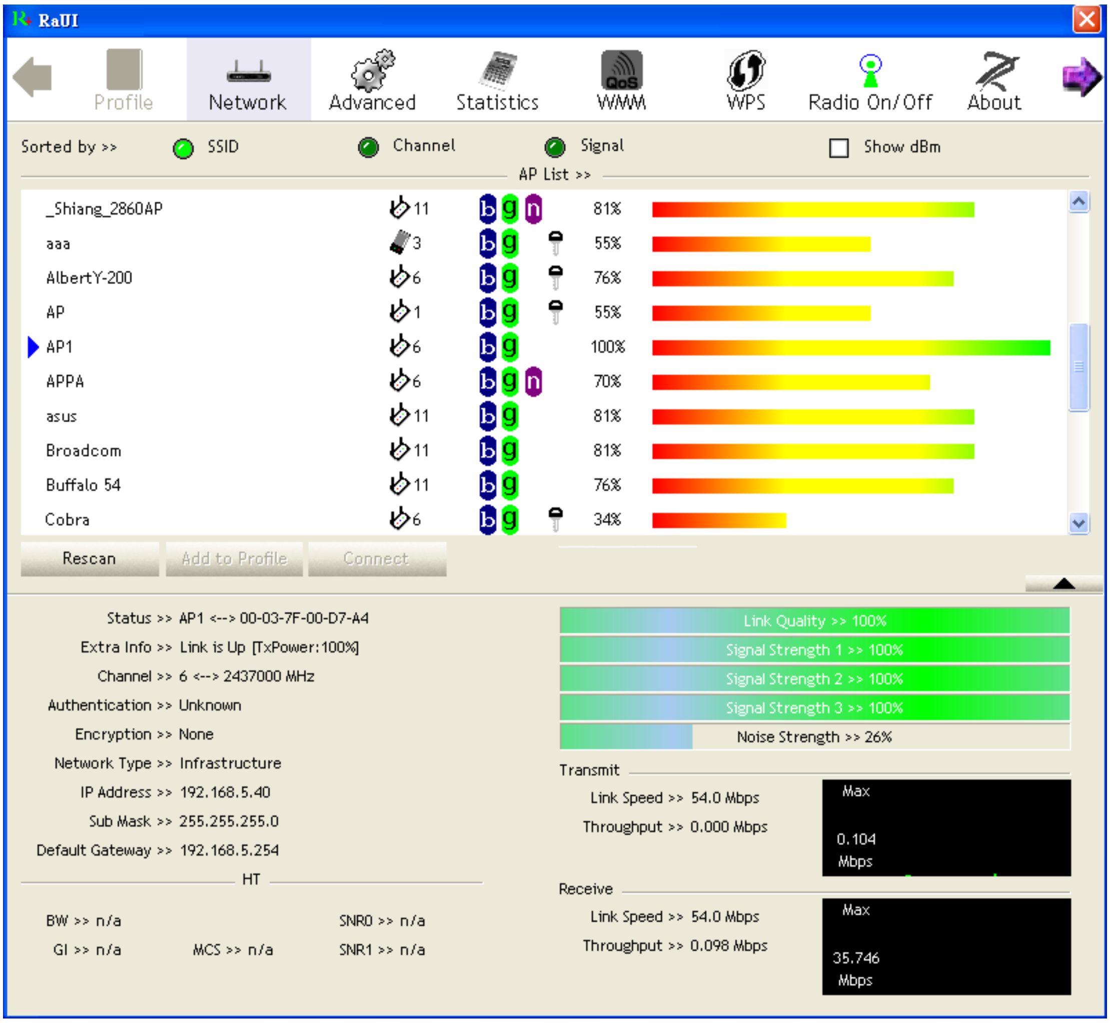


Wireless Network Connection is now connected

Connected to: AP1
Signal Strength: Excellent

Figure 1-12 Network connection status

8. Clicking the Ralink icon will bring up the RaUI main window. Users can find the surrounding APs in the list. The currently connected AP will be shown with a blue icon beside it, as shown in Figure 1-13. Users may use the advanced tab to configure more advanced features provided by Ralink's wireless NIC. For details on configuring the advanced features, please check the Advance setting section.



_Shiang_2860AP	11	b g n		81%
aaa	3	b g	🔑	55%
AlbertY-200	6	b g	🔑	76%
AP	1	b g	🔑	55%
▶ AP1	6	b g		100%
APPA	6	b g n		70%
asus	11	b g		81%
Broadcom	11	b g		81%
Buffalo 54	11	b g		76%
Cobra	6	b g	🔑	34%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.40
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
0.104 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.098 Mbps
35.746 Mbps

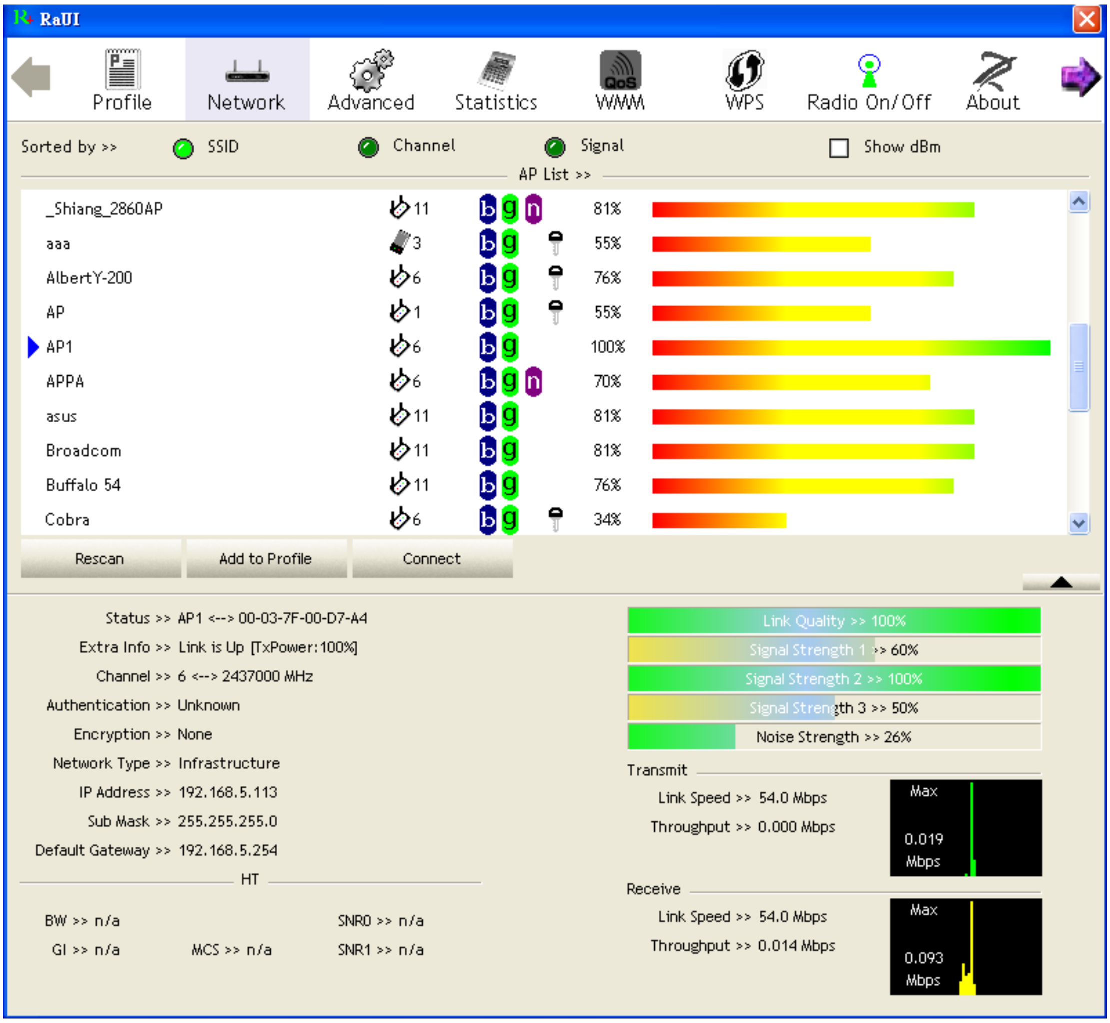
Figure 1-13 Show connection status by using WZC to initiate the connection

B. RaUI

4.2.1 Start

4.2.1.1 Start RaUI

When starting RaUI, the system will connect to the AP with best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 2-1.



	SSID	Channel	Mode	Security	Signal
	_Shiang_2860AP	11	b g n		81%
	aaa	3	b g	🔑	55%
	AlbertY-200	6	b g	🔑	76%
	AP	1	b g	🔑	55%
▶	AP1	6	b g		100%
	APPA	6	b g n		70%
	asus	11	b g		81%
	Broadcom	11	b g		81%
	Buffalo 54	11	b g		76%
	Cobra	6	b g	🔑	34%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.113
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 >> 60%
Signal Strength 2 >> 100%
Signal Strength 3 >> 50%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Max 0.019 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.014 Mbps
Max 0.093 Mbps

Figure 2-1-1 RaUI section introduction

There are three sections to the RaUI dialog box. These sections are briefly described as follow.

1. Button Section: Include buttons for selecting the Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, the About button, Radio On/Off button and Help.

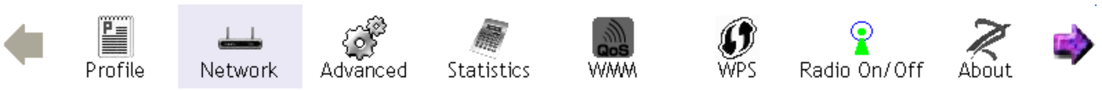


Figure 2-1-2 Button section

Figure 2-1-3 Move to the left

Figure 2-1-4 Move to the right

2. Function Section: Appears to present information and options related to the button.

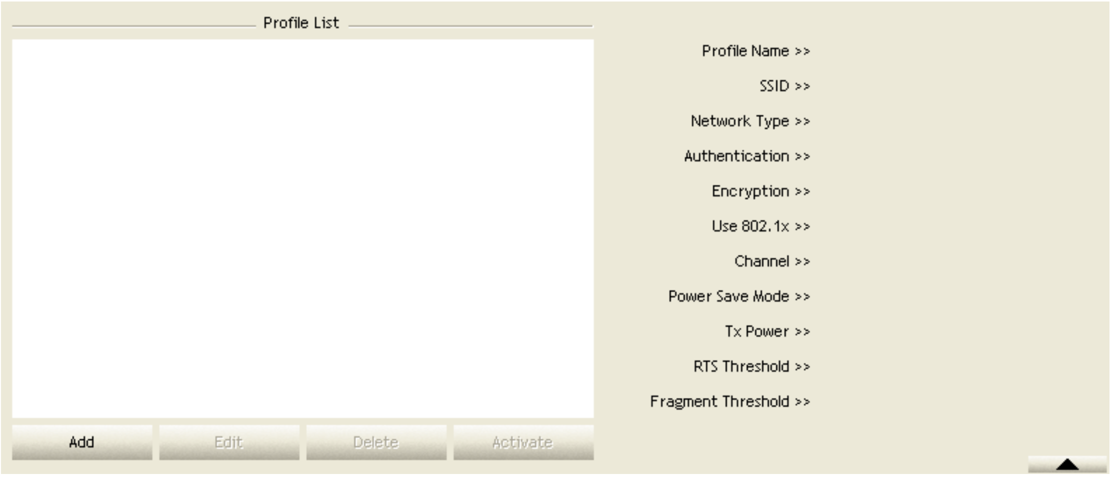
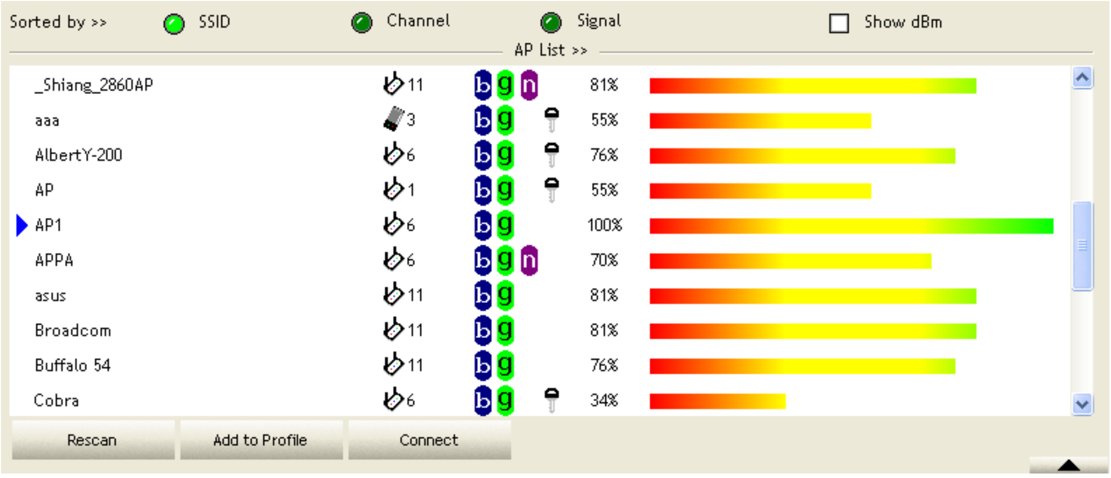
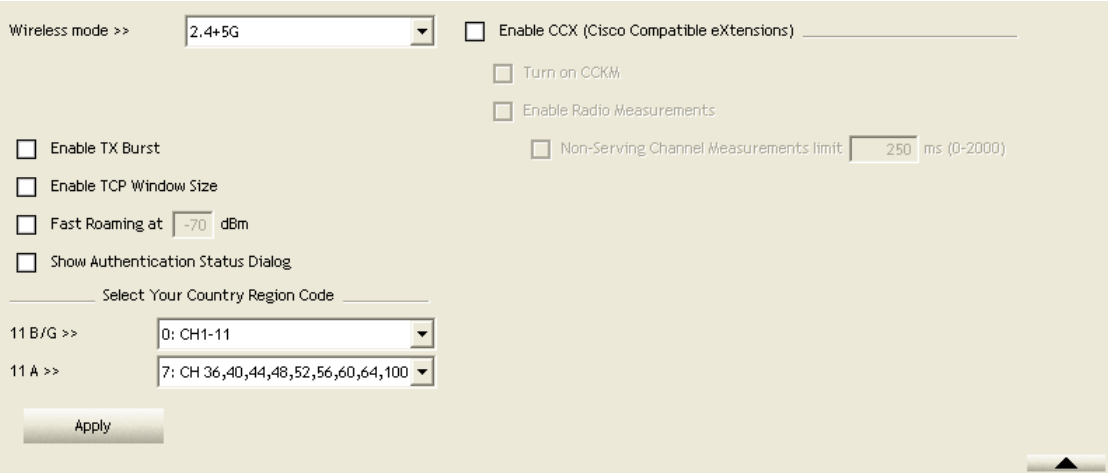


Figure 2-1-5 Profile page



_Shiang_2860AP	11	b g n		81%
aaa	3	b g	🔑	55%
AlbertY-200	6	b g	🔑	76%
AP	1	b g	🔑	55%
▶ AP1	6	b g		100%
APPA	6	b g n		70%
asus	11	b g		81%
Broadcom	11	b g		81%
Buffalo 54	11	b g		76%
Cobra	6	b g	🔑	34%

Figure 2-1-6 Network page



Wireless mode >> 2.4+5G

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements limit 250 ms (0-2000)

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

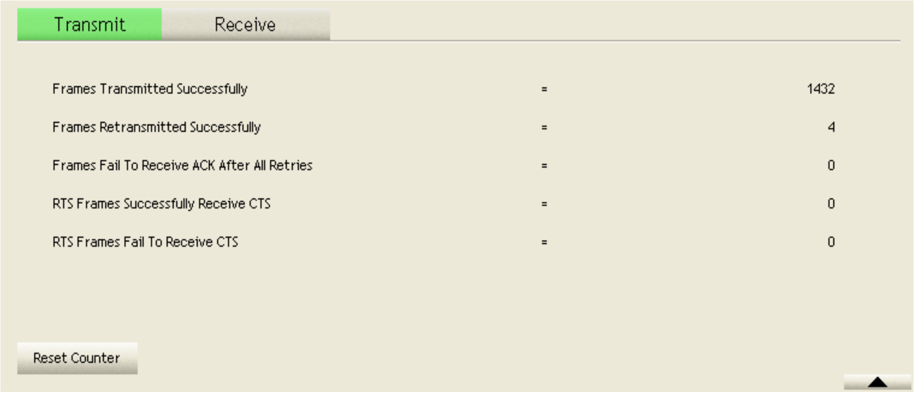
□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

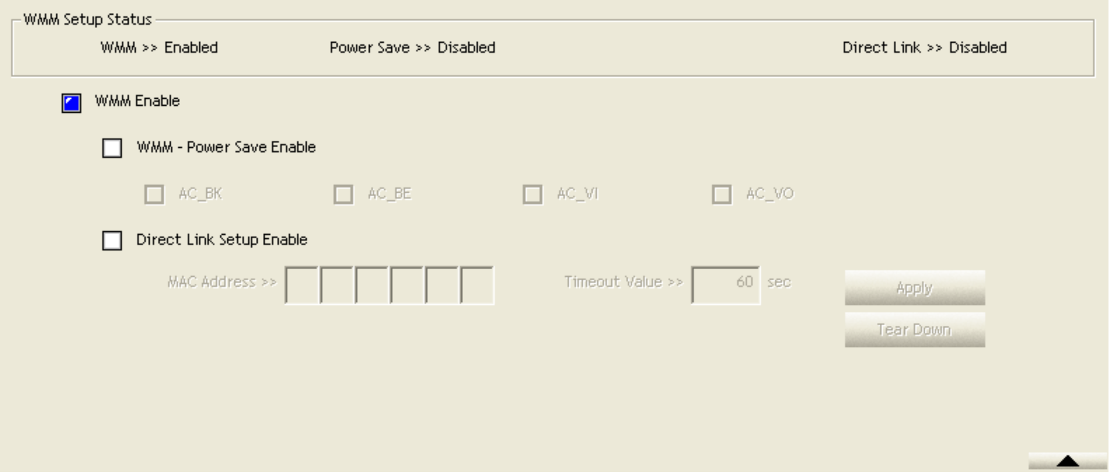
11 A >> 7: CH 36,40,44,48,52,56,60,64,100

Figure 2-1-7 Advance page



Frames Transmitted Successfully	=	1432
Frames Retransmitted Successfully	=	4
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0

Figure 2-1-8 Statistics page



WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link >> Disabled

☑ WMM Enable

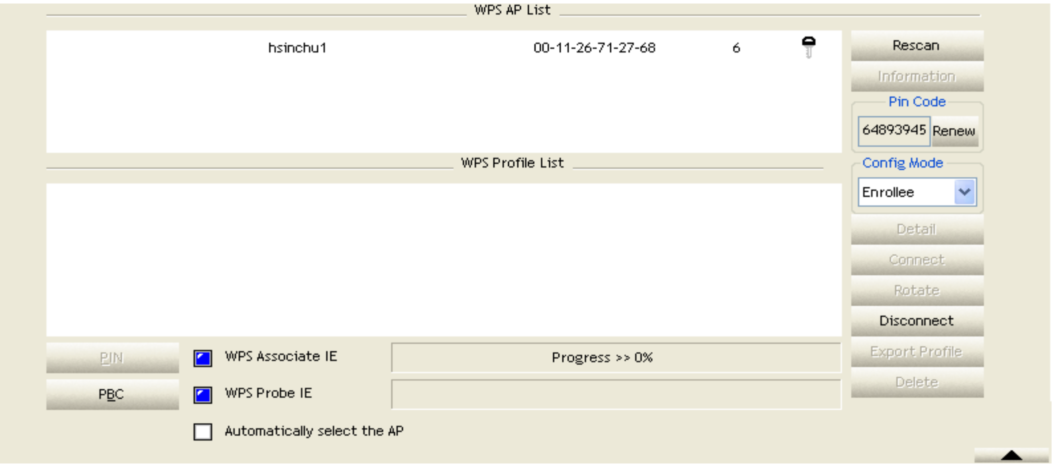
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

Figure 2-1-9 WMM page



hsinchu1 00-11-26-71-27-68 6

Pin Code: 64893945

Config Mode: Enrollee

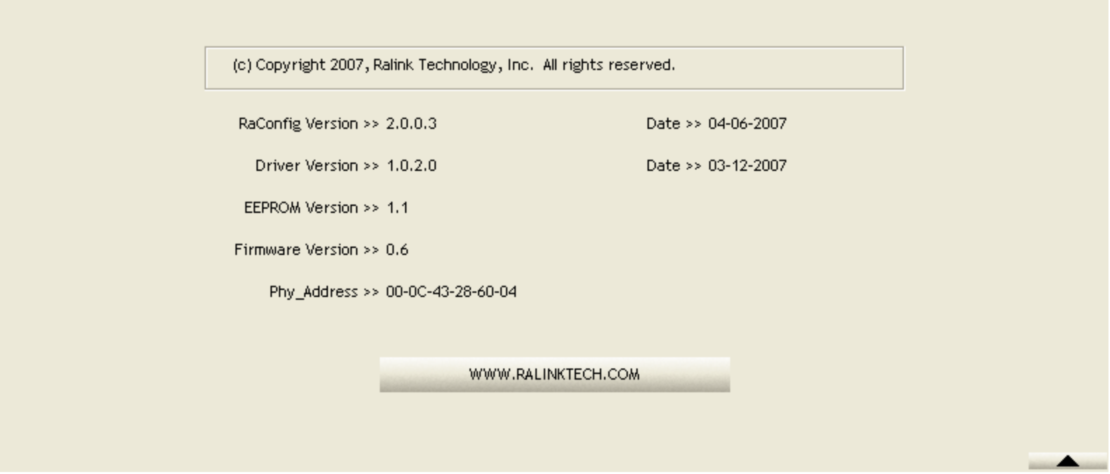
☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

Figure 2-1-10 WPS page



(c) Copyright 2007, Ralink Technology, Inc. All rights reserved.

RaConfig Version >> 2.0.0.3 Date >> 04-06-2007

Driver Version >> 1.0.2.0 Date >> 03-12-2007

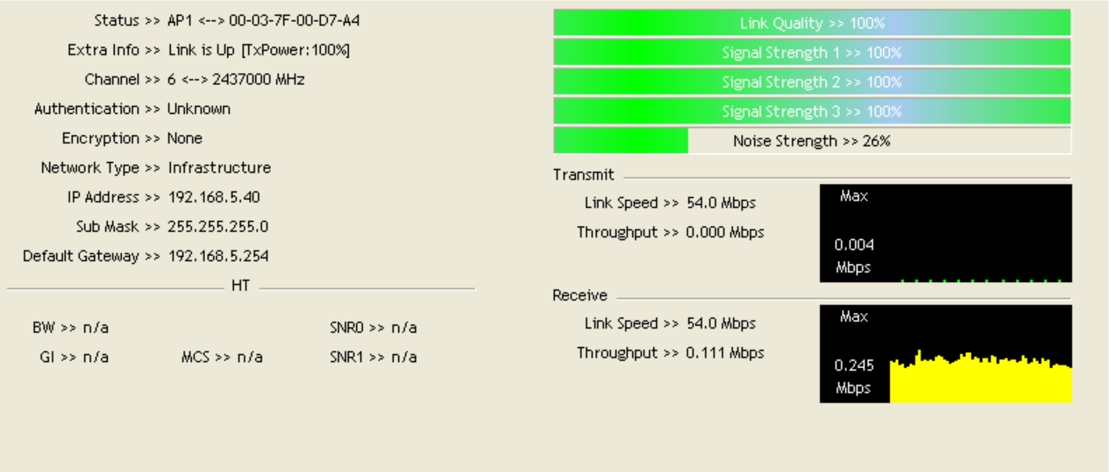
EEPROM Version >> 1.1

Firmware Version >> 0.6

Phy_Address >> 00-0C-43-28-60-04

Figure 2-1-11 About page

3. Status Section: This section includes information about the link status, authentication status, AP's information and configuration, and retrying the connection when authentication is failed.



Status >> AP1 <--> 00-03-7F-00-D7-A4

Extra Info >> Link is Up [TxPower:100%]

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.40

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

0.004 Mbps

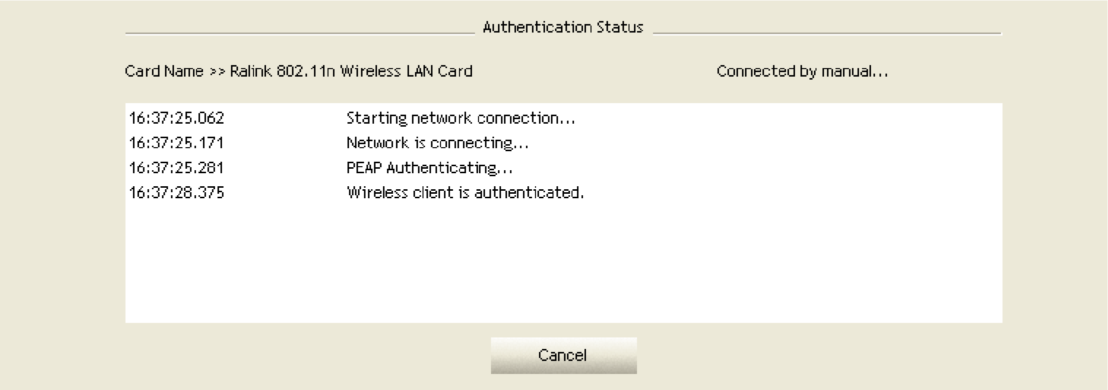
Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.111 Mbps

0.245 Mbps

Figure 2-1-12 Link Status



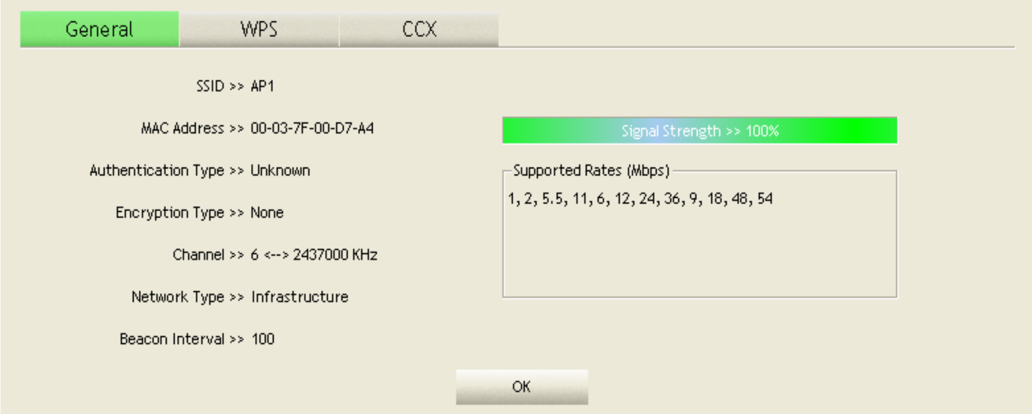
Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card

Connected by manual...

```
16:37:25.062        Starting network connection...
16:37:25.171        Network is connecting...
16:37:25.281        PEAP Authenticating...
16:37:28.375        Wireless client is authenticated.
```

Figure 2-1-13 Authentication Status



SSID >> AP1

MAC Address >> 00-03-7F-00-D7-A4

Signal Strength >> 100%

Authentication Type >> Unknown

Supported Rates (Mbps)

1, 2, 5.5, 11, 6, 12, 24, 36, 9, 18, 48, 54

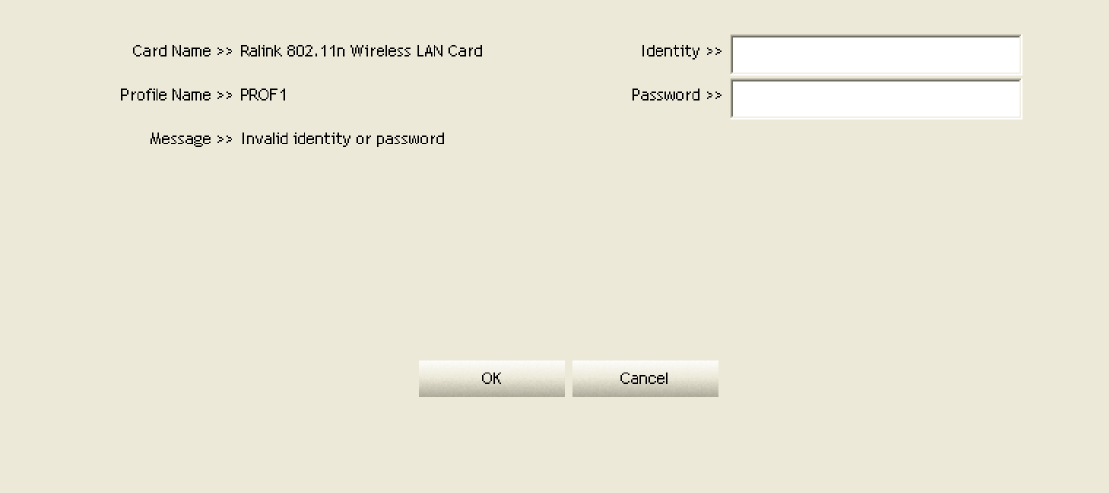
Encryption Type >> None

Channel >> 6 <--> 2437000 KHz

Network Type >> Infrastructure

Beacon Interval >> 100

Figure 2-1-14 AP's Information



Card Name >> Ralink 802.11n Wireless LAN Card

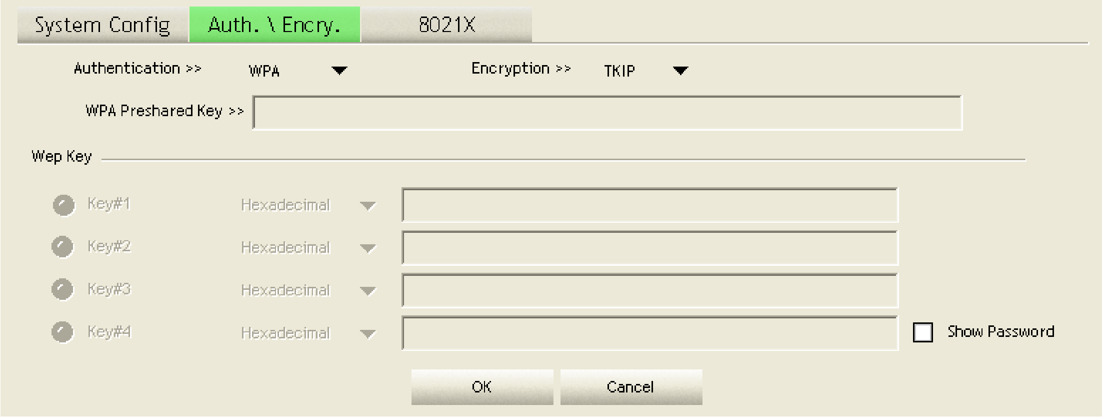
Identity >>

Profile Name >> PROF1

Password >>

Message >> Invalid identity or password

Figure 2-1-15 Retry the connection



Authentication >> WPA

Encryption >> TKIP

WPA Preshared Key >>

Wep Key

○ Key#1	Hexadecimal	
○ Key#2	Hexadecimal	
○ Key#3	Hexadecimal	
○ Key#4	Hexadecimal	

□ Show Password

Figure 2-1-16 Configuration

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close RaUI utility.

Figure 2-1-17 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:

R+ : Indicates the connected and signal strength is good.

R+ : Indicates the connected and signal strength is normal.

R+ : Indicates that it is not yet connected.

R+ : Indicates that a wireless NIC can not be detected.

R+: Indicates that the connection and signal strength is weak.

4.2.2 Profile

4.2.2.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 shows the basic profile section

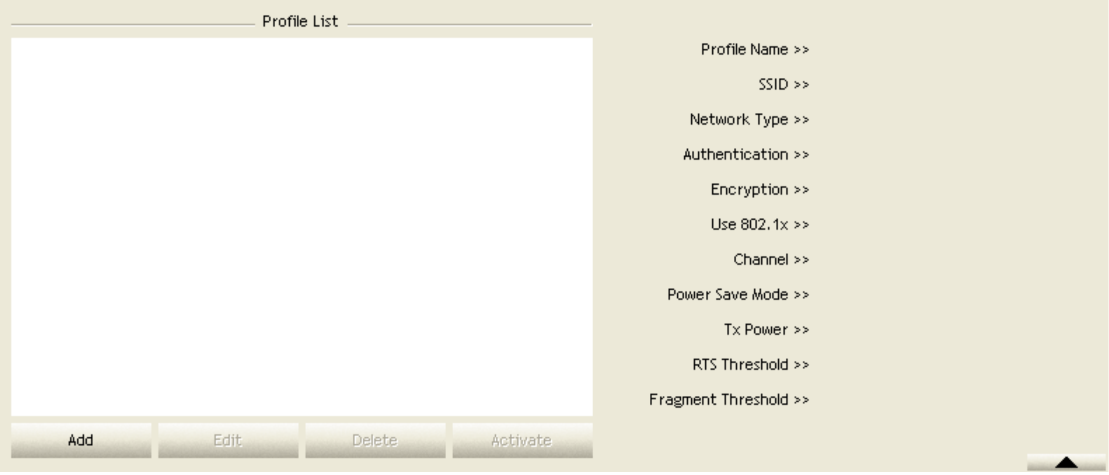


Figure 2-2-1 Profile function.

Definition of each field:

1. Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).

2. SSID: The access point or Ad-hoc name.

3. Network Type: Indicates the networks type, including infrastructure and Ad- Hoc.

4. Authentication: Indicates the authentication mode used.

5. Encryption: Indicates the encryption Type used.

6. Use 802.1x: Shows if the 802.1x feature is used or not.

7. Cannel: Channel in use for Ad-Hoc mode.

8. Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.

9. Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.

10. RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.

11. Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

Icons and buttons:

a : Indicates if a connection made from the currently activated profile.

b : Indicates if the connection has failed on a currently activated profile.

g : Indicates the network type is infrastructure mode.

n : Indicates the network type is in Ad-hoc mode.

: Indicates if the network is security-enabled.

Rescan : Click to add a new profile.

Connect : Click to edit an existing profile.

Add to Profile : Deletes an existing profile.

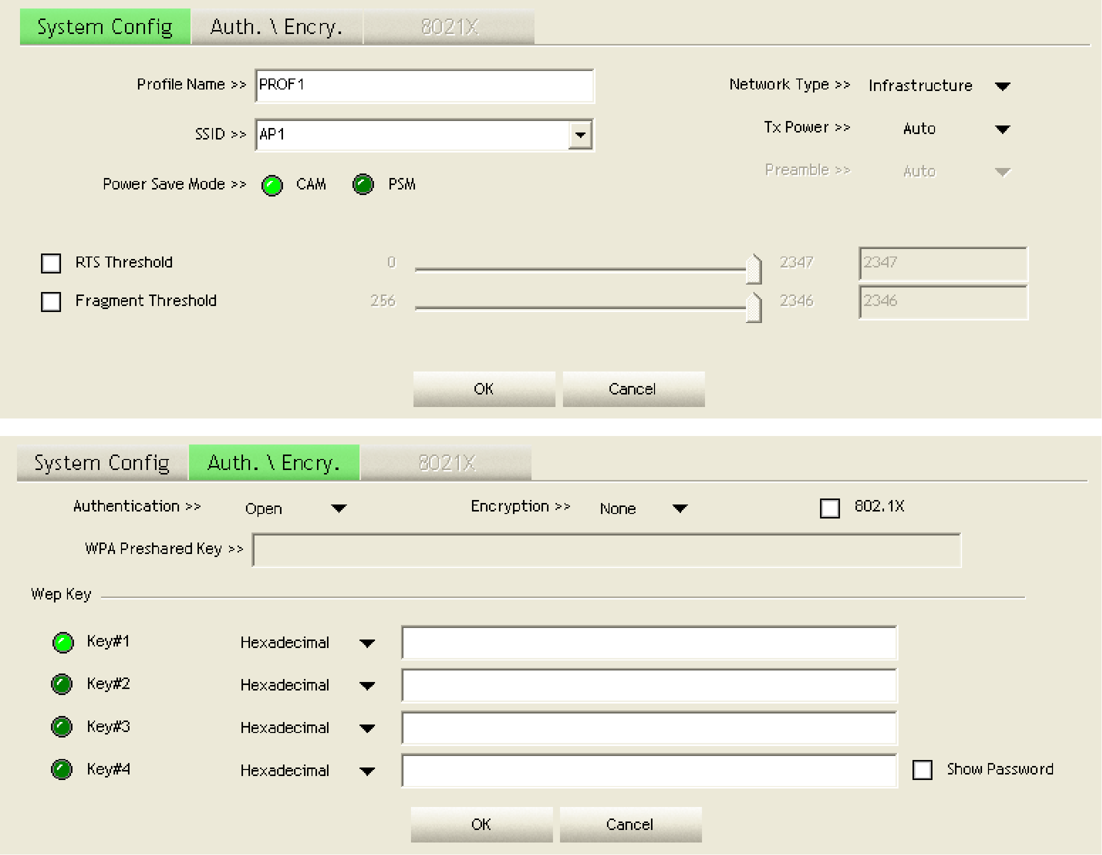
Activate : Activates the selected profile.

▼: Shows information of the related status section.
▲: Hides information of the related status section.

4.2.2.2 Add / Edit Profile

There are three methods to open the Profile Editor dialog box.

1. You can open it by clicking the "Add to Profile" button in the Site Survey tab.
2. You can open it by clicking the "Add" button in the Profile tab.
3. You can open it by clicking the "Edit" button on the Profile tab



Profile Name >> PROF1

SSID >> AP1

Power Save Mode >> ● CAM ● PSM

Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

Authentication >> Open

Encryption >> None

□ 802.1X

WPA Preshared Key >>

Wep Key

● Key#1 Hexadecimal

● Key#2 Hexadecimal

● Key#3 Hexadecimal

● Key#4 Hexadecimal

□ Show Password

Figure 2-2-2 Configuration

1. Profile Name: The user can chose any name for this profile, or use the default name defined by system.
2. SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.
3. Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
4. Network Type: There are two types, infrastructure and 802.11 Ad-hoc modes. Under Ad-hoc mode, user can also choose the preamble type. The available preamble type includes auto and long. In addition, the channel field will be available for setup in Ad-hoc mode.
5. RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or key in the value directly. The default value is 2347.
6. Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.
7. Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-hoc network. Authentication Type: There are 7 type of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

8. Encryption Type: For open and shared authentication mode, the selection of available encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.

9. 802.1x Setting: This is introduced in the topic of "Section 3-2 : 802.1x Setting".

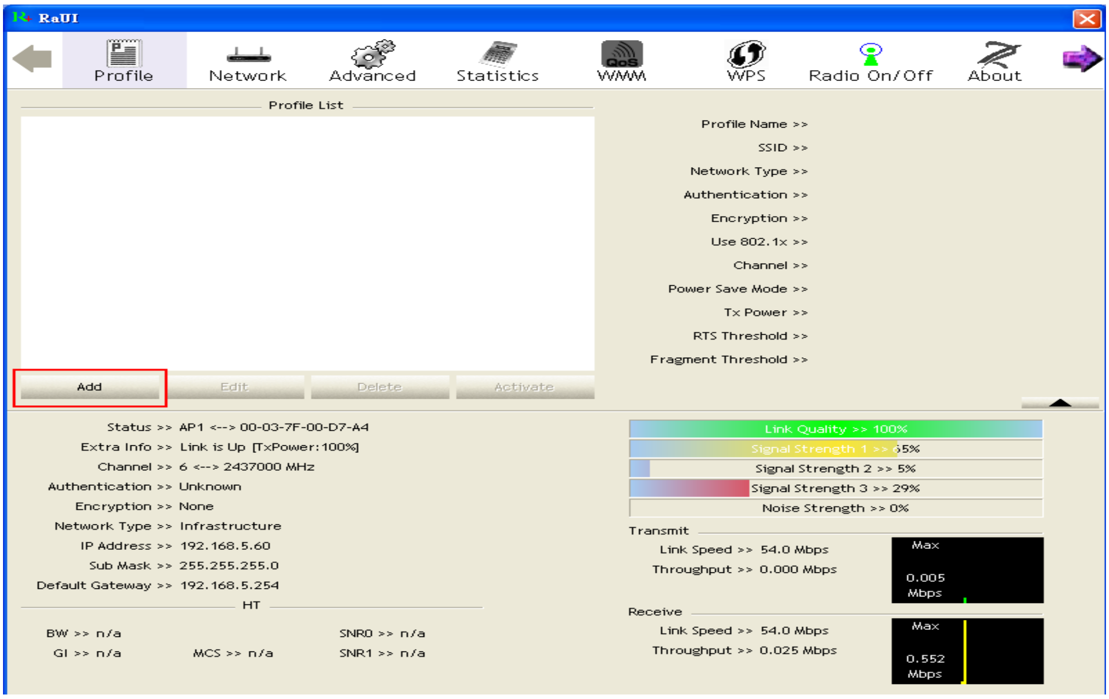
10. WPA Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

11. WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys.

1. Hexadecimal - 40bits : 10 Hex characters.
2. Hexadecimal - 128bits : 26Hex characters.
3. ASCII - 40bits : 5 ASCII characters.
4. ASCII - 128bits : 13 ASCII characters

4.2.2.3 Example on Adding Profile in Network

Click "Add" below the Profile List.



Profile Name >>
SSID >>
Network Type >>
Authentication >>
Encryption >>
Use 802.1x >>
Channel >>
Power Save Mode >>
Tx Power >>
RTS Threshold >>
Fragment Threshold >>

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

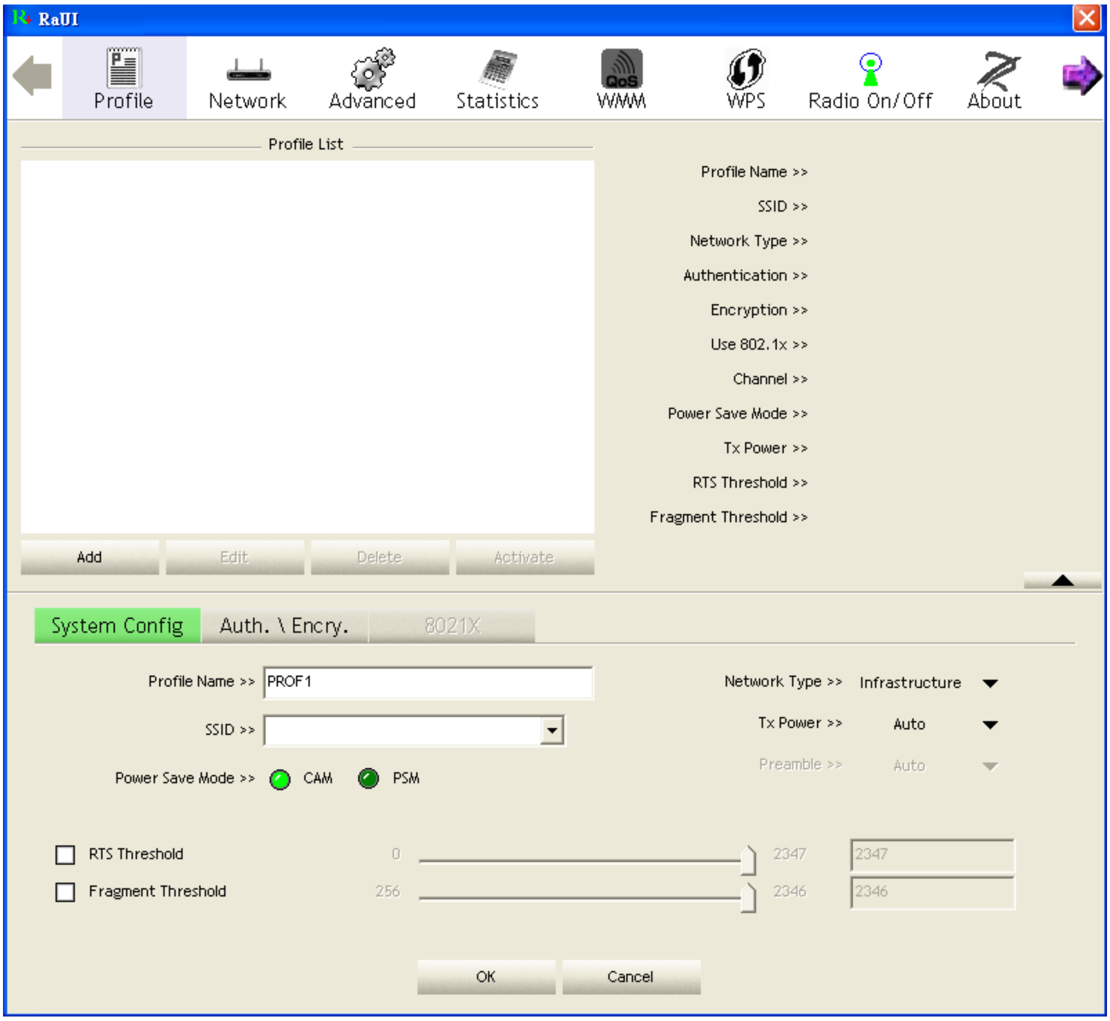
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 65%
Signal Strength 2 >> 5%
Signal Strength 3 >> 29%
Noise Strength >> 0%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
0.005 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.025 Mbps
0.552 Mbps

The "Add Profile" will appear.



Profile Name >> PROF1

SSID >>

Power Save Mode >> ● CAM ● PSM

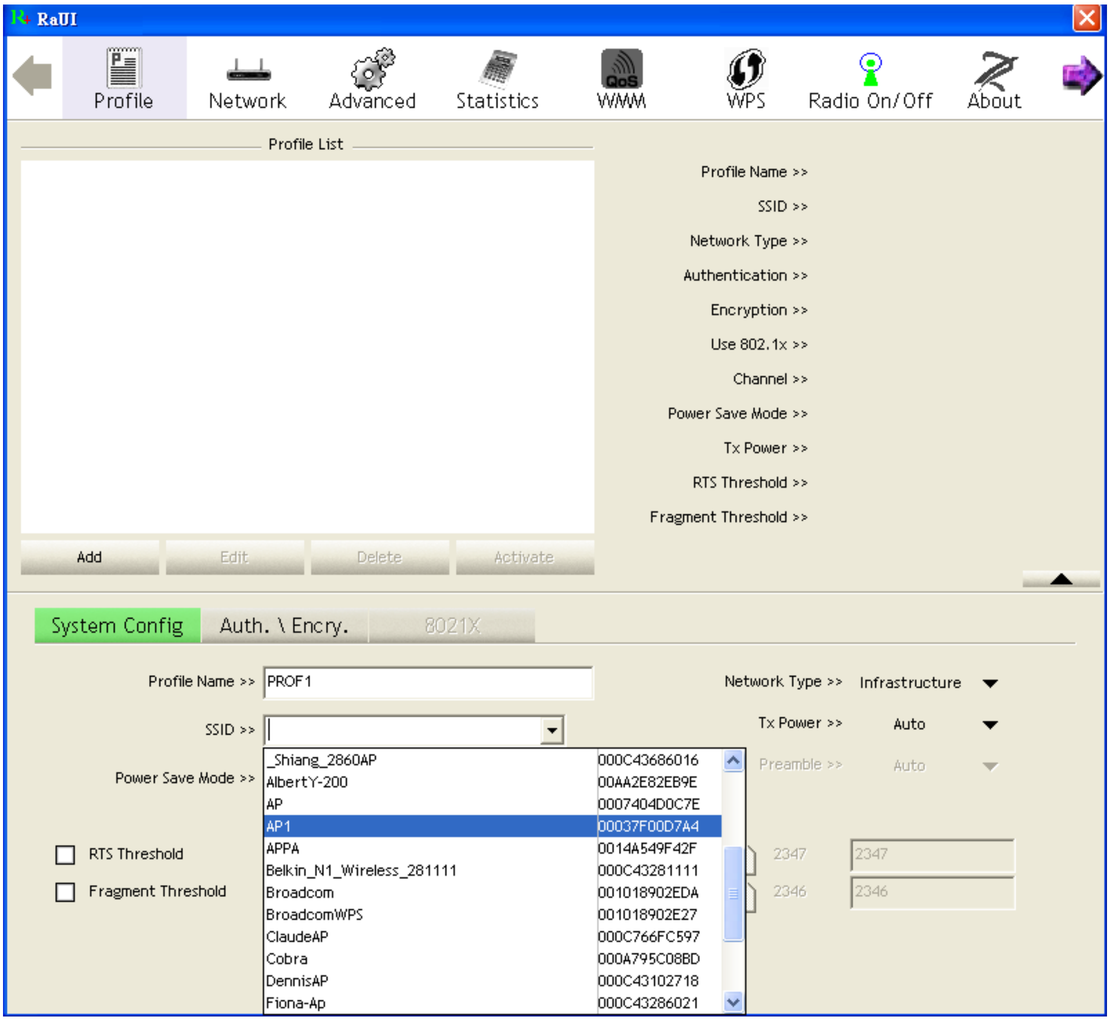
Network Type >> Infrastructure

Tx Power >> Auto

□ RTS Threshold 2347

□ Fragment Threshold 2346

Specify a Profile Name. Select an AP from the SSID drop-down list. The AP list is from the last Network.



Profile Name >>
SSID >>
Network Type >>
Authentication >>
Encryption >>
Use 802.1x >>
Channel >>
Power Save Mode >>
Tx Power >>
RTS Threshold >>
Fragment Threshold >>

Profile Name >> PROF1

SSID >>

Power Save Mode >>

□ RTS Threshold 2347 2347

□ Fragment Threshold 2346 2346

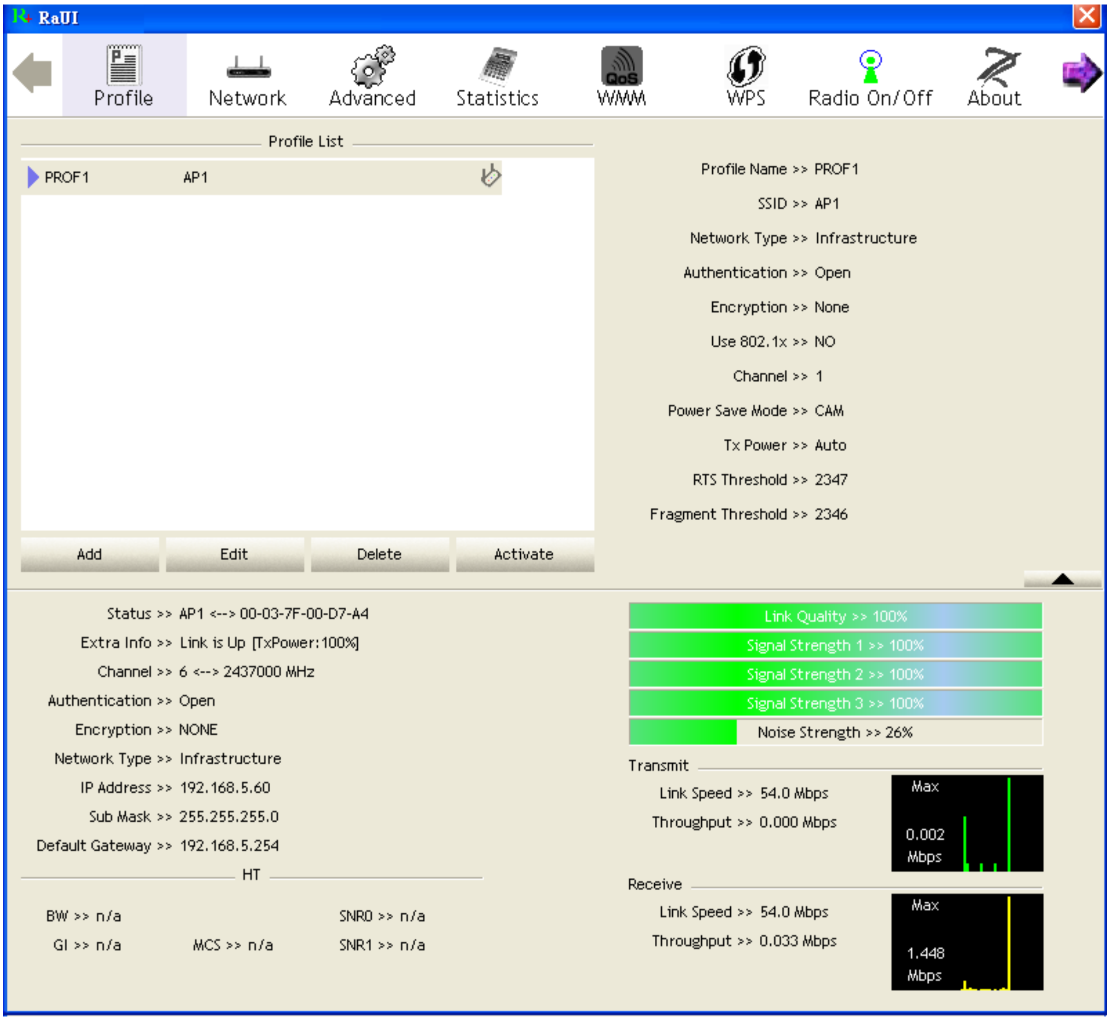
Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

_Shiang_2860AP	000C43686016
AlbertY-200	00AA2E82EB9E
AP	0007404D0C7E
AP1	00037F00D7A4
APPA	0014A549F42F
Belkin_N1_Wireless_281111	000C43281111
Broadcom	001018902EDA
BroadcomWPS	001018902E27
ClaudeAP	000C766FC597
Cobra	000A795C08BD
DennisAP	000C43102718
Fiona-Ap	000C43286021

Now the profile which the user set appears in the profile list. Click "Activate".



PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

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

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

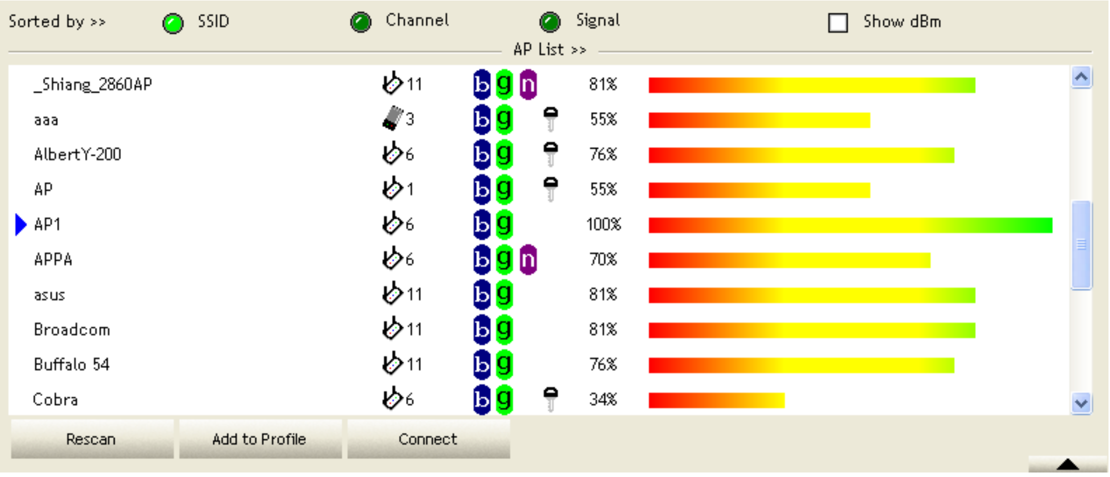
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
0.002 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps
1.448 Mbps

4.2.3 Network

4.2.3.1 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as shown in Figure 2-3-1-1.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

	_Shiang_2860AP	11	b g n		81%
	aaa	3	b g	🔑	55%
	AlbertY-200	6	b g	🔑	76%
	AP	1	b g	🔑	55%
▶	AP1	6	b g		100%
	APPA	6	b g n		70%
	asus	11	b g		81%
	Broadcom	11	b g		81%
	Buffalo 54	11	b g		76%
	Cobra	6	b g	🔑	34%

Figure 2-3-1-1 Network function

1. SSID: Name of BSS or IBSS network.
2. Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
3. Channel: Channel in use.
4. Wireless Mode: AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode.
5. Security-Enable: Indicates if the AP provides a security-enabled wireless network.
6. Signal: Receive signal strength of the specified network.

Icons and buttons:

a : Indicates that the connection is successful.

g : Indicates the network type is in infrastructure mode.

n : Indicates the network type is in Ad-hoc mode.

Sorted by >> ● SSID ● Channel ● Signal :

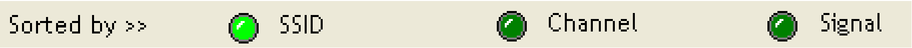
Indicate that the wireless network is security - enabled.

a : Indicates 802.11a wireless mode.

b : Indicates 802.11b wireless mode

g : Indicates 802.11g wireless mode.

n : Indicates 802.11n wireless mode.



Sorted by >> ● SSID ● Channel ● Signal

: Indicates that the AP list is sorted by SSID, Channel or Signal.

Connect

: Button to connect to the selected network.

Rescan

: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

Add to Profile

: Adds the selected AP to the Profile setting. It will bring up a profile page and save the user's setting to a new profile.

▼: Shows the Status Section.

▲: Hides the Status Section.

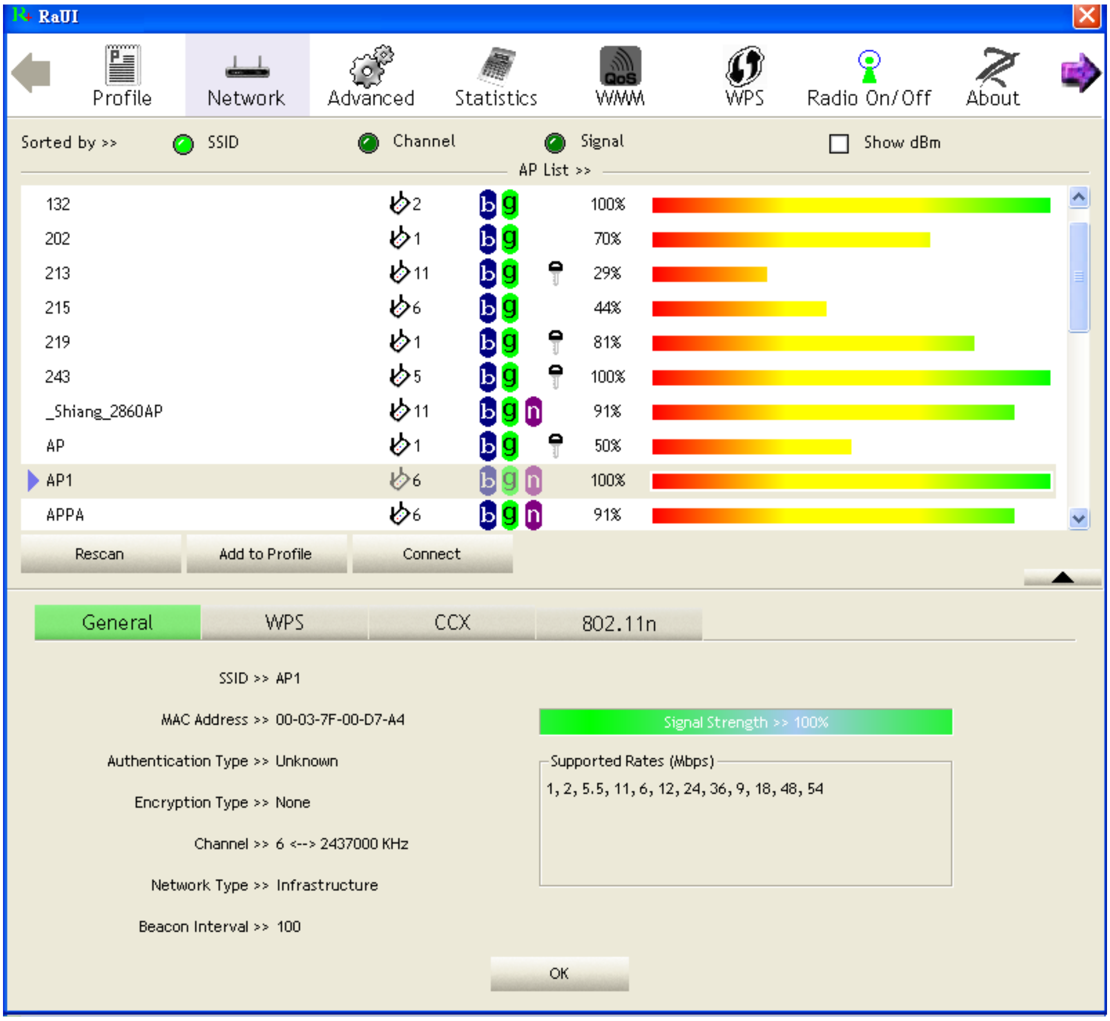
Connected network:

1. When RaUI first runs, it will select the best AP to connect to automatically.
2. If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.
3. If the intended network uses encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to the example on how to fill in the security information

When you double click an AP, you can see detailed information about that AP.

The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode.) The introduction is as follows:

A. General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.



SSID	Channel			Signal
132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

SSID >> AP1

MAC Address >> 00-03-7F-00-D7-A4

Authentication Type >> Unknown

Encryption Type >> None

Channel >> 6 <--> 2437000 KHz

Network Type >> Infrastructure

Beacon Interval >> 100

Signal Strength >> 100%

Supported Rates (Mbps)

1, 2, 5.5, 11, 6, 12, 24, 36, 9, 18, 48, 54

Figure 2-3-1-2 General information about the Access Point

b. WPS information contains the authentication type, encryption type, config. methods, device password ID, selected registrar, state, version, AP setup lock status, UUID-E and RF bands, as shown in Figure 2-3-1-3. The information is further explained as follows :

1. Authentication Type: There are three types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

2. Encryption Type: For open and shared authentication mode, the choices of the encryption type are none and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

3. Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars, (a bitwise OR of values.)

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

4. Device Password ID: Indicates the method or identifies the specific password that the selected Registrar intends to use. The AP in PBC mode must indicate 0x0004 within the two-minute Walk Time.

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	Push Button (PBC)
0x0005	Registrar-specified
0x0006-0x00F	Reserved

5. Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

6. State: The current configuration state of the AP. The values are "Unconfigured" and "Configured".

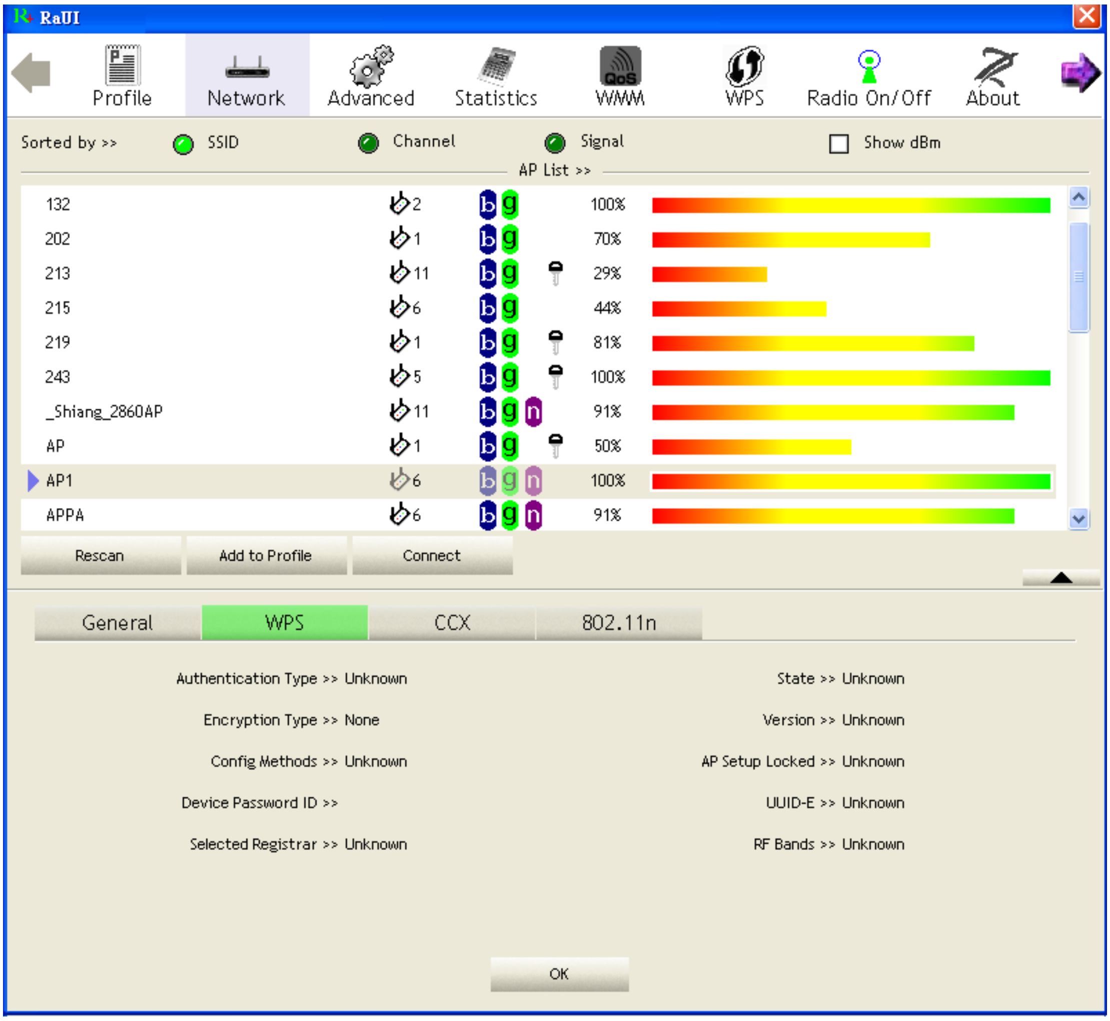
7. Version: The specified WPS version.

8. AP Setup Locked: Indicates if the AP has entered a locked setup state.

9. UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. The value is 16 bytes.

10. RF Bands: Indicates all of the RF bands available to the AP. A dual-band AP must provide it. The values are

"2.4GHz" and "5GHz".



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Unknown

Version >> Unknown

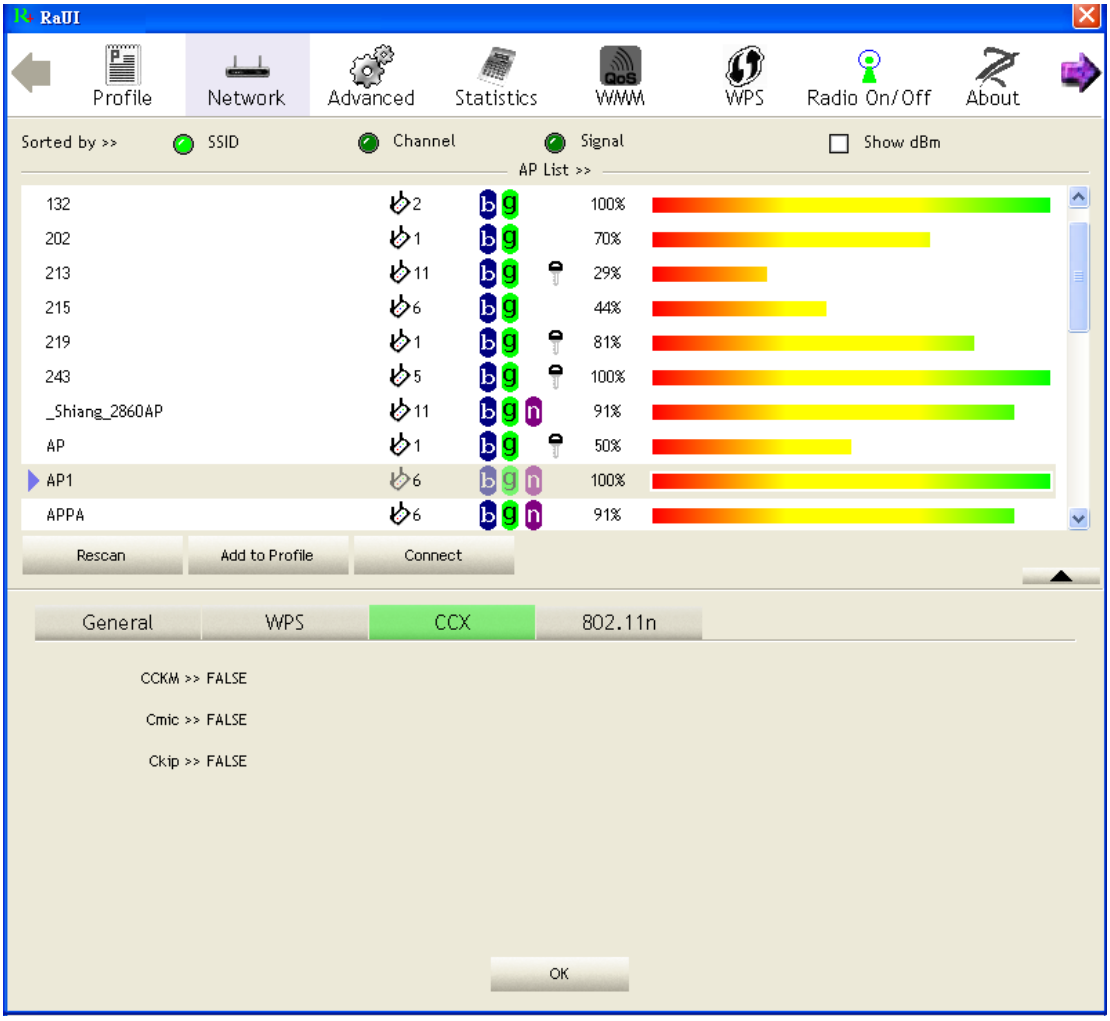
AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

Figure 2-3-1-3 WPS Detailed information about the AP

c. CCX information contains the CCKM, Cmic and Ckip information. It is shown in Figure 2-3-1-4.



SSID	Channel	Mode	Security	Signal
132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

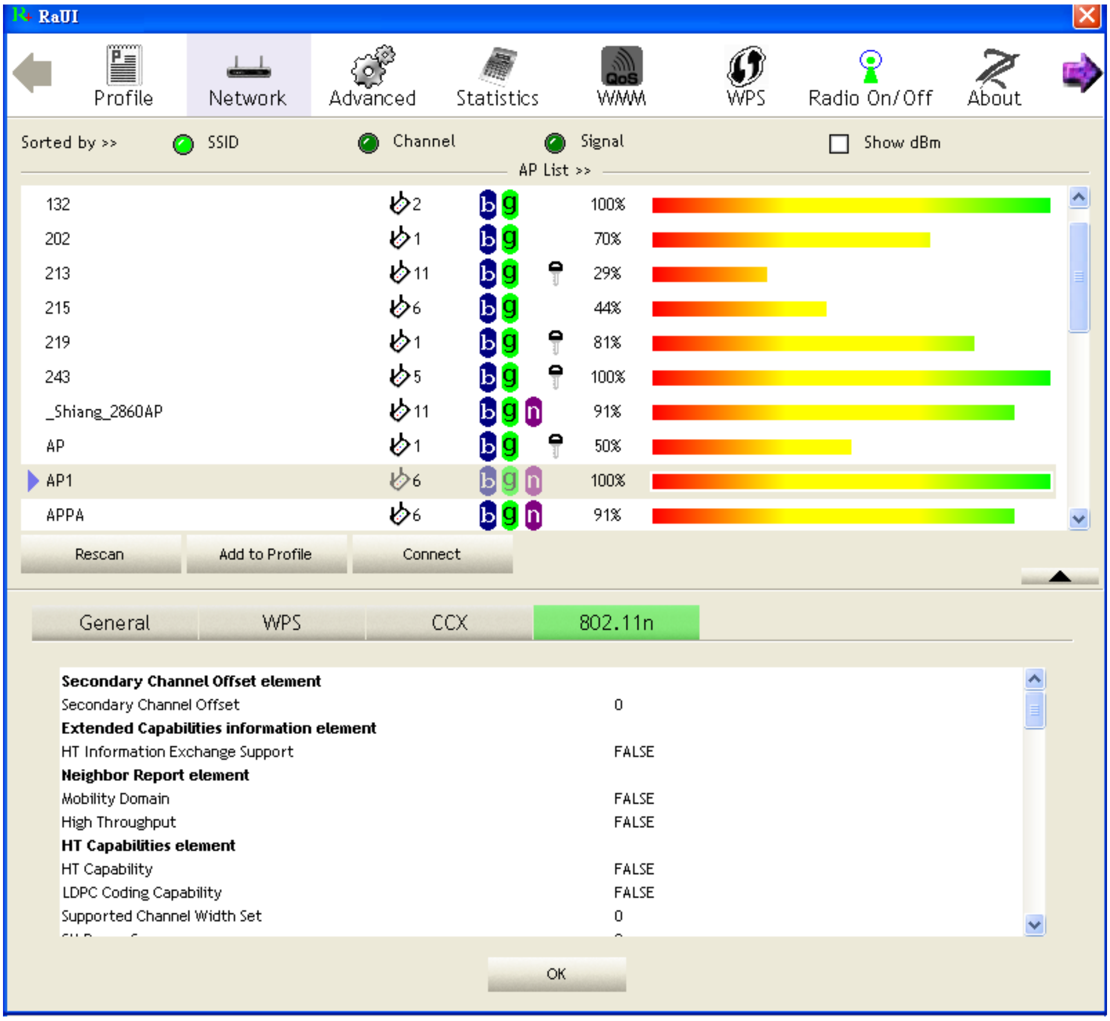
CCKM >> FALSE

Cmic >> FALSE

Ckip >> FALSE

Figure 2-3-1-4 CCX information about AP's detail information

d. 802.11n information contains some related 802.11n information. It is shown in Figure 2-3-1-5.



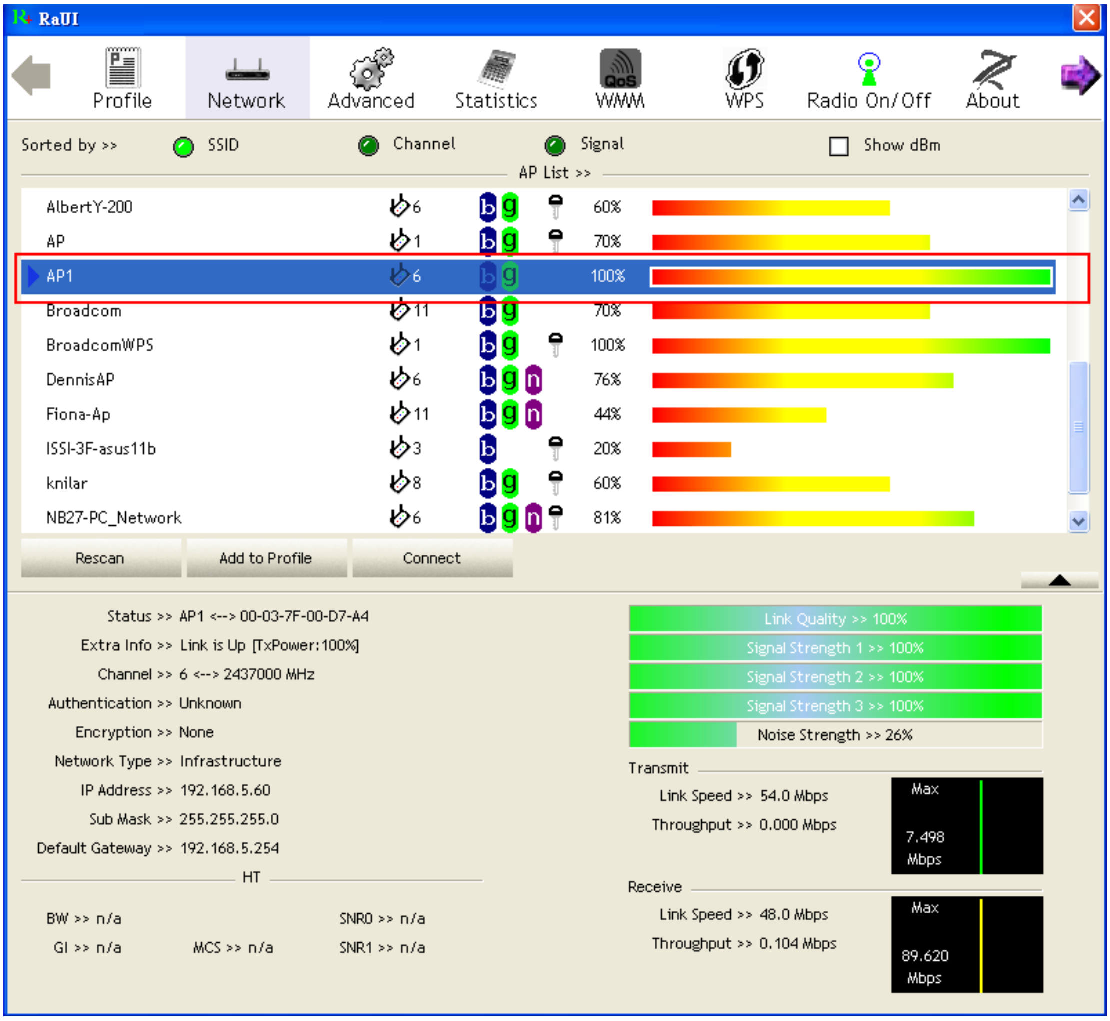
SSID	Channel			Signal
132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

Secondary Channel Offset element
Secondary Channel Offset 0
Extended Capabilities information element
HT Information Exchange Support FALSE
Neighbor Report element
Mobility Domain FALSE
High Throughput FALSE
HT Capabilities element
HT Capability FALSE
LDPC Coding Capability FALSE
Supported Channel Width Set 0

Figure 2-3-1-5 802.11n information

4.2.3.2 Example on Adding Profile in Network

1. Select the AP from the list on the Network tab



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

AlbertY-200	6	b g	🔒	60%
AP	1	b g	🔒	70%
AP1	6	b g		100%
Broadcom	11	b g		70%
BroadcomWPS	1	b g	🔒	100%
DennisAP	6	b g n		76%
Fiona-Ap	11	b g n		44%
ISSI-3F-asus11b	3	b	🔒	20%
knilar	8	b g	🔒	60%
NB27-PC_Network	6	b g n	🔒	81%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

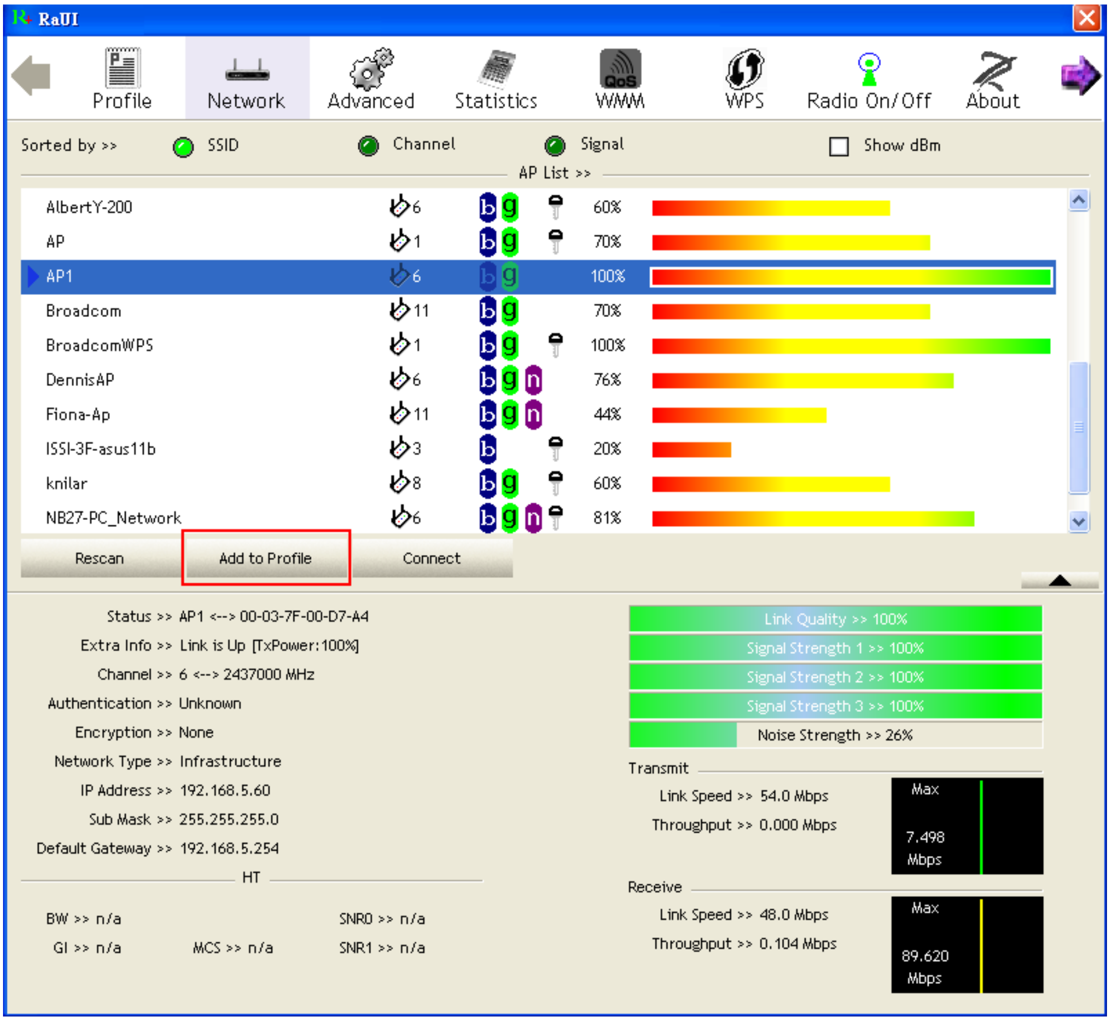
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Max
7.498
Mbps

Receive
Link Speed >> 48.0 Mbps
Throughput >> 0.104 Mbps
Max
89.620
Mbps

2. Click "Add to Profile"



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

AlbertY-200	6	b g	🔒	60%
AP	1	b g	🔒	70%
AP1	6	b g		100%
Broadcom	11	b g		70%
BroadcomWPS	1	b g	🔒	100%
DennisAP	6	b g n		76%
Fiona-Ap	11	b g n		44%
ISSI-3F-asus11b	3	b	🔒	20%
knilar	8	b g	🔒	60%
NB27-PC_Network	6	b g n	🔒	81%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

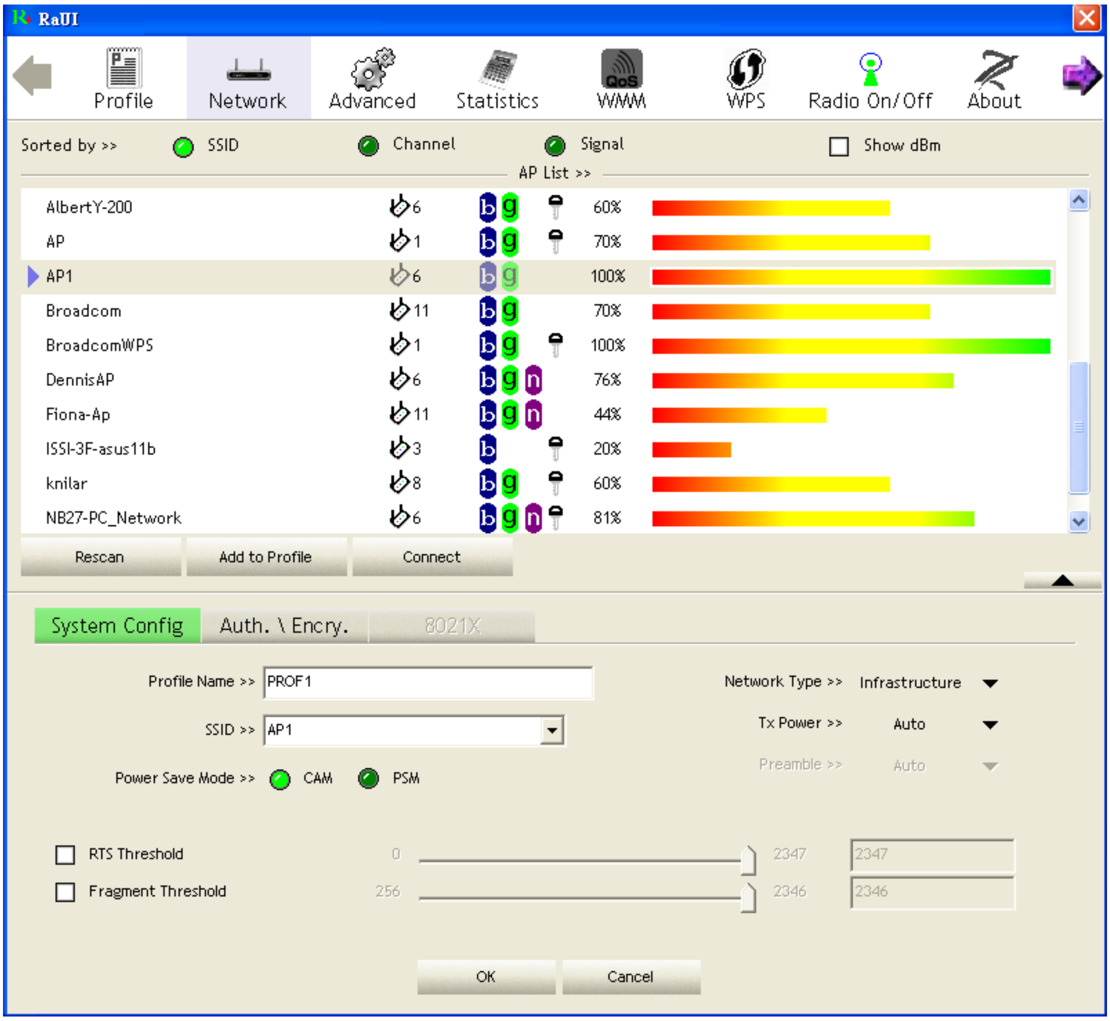
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Max
7.498
Mbps

Receive
Link Speed >> 48.0 Mbps
Throughput >> 0.104 Mbps
Max
89.620
Mbps

3. The System section will appear at the bottom of the Add Profile window. You can specify your own profile name



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

AlbertY-200	6	b g	🔒	60%
AP	1	b g	🔒	70%
AP1	6	b g		100%
Broadcom	11	b g		70%
BroadcomWPS	1	b g	🔒	100%
DennisAP	6	b g n		76%
Fiona-Ap	11	b g n		44%
ISSI-3F-asus11b	3	b	🔒	20%
knilar	8	b g	🔒	60%
NB27-PC_Network	6	b g n	🔒	81%

Profile Name >> PROF1

SSID >> AP1

Power Save Mode >> ● CAM ● PSM

Network Type >> Infrastructure

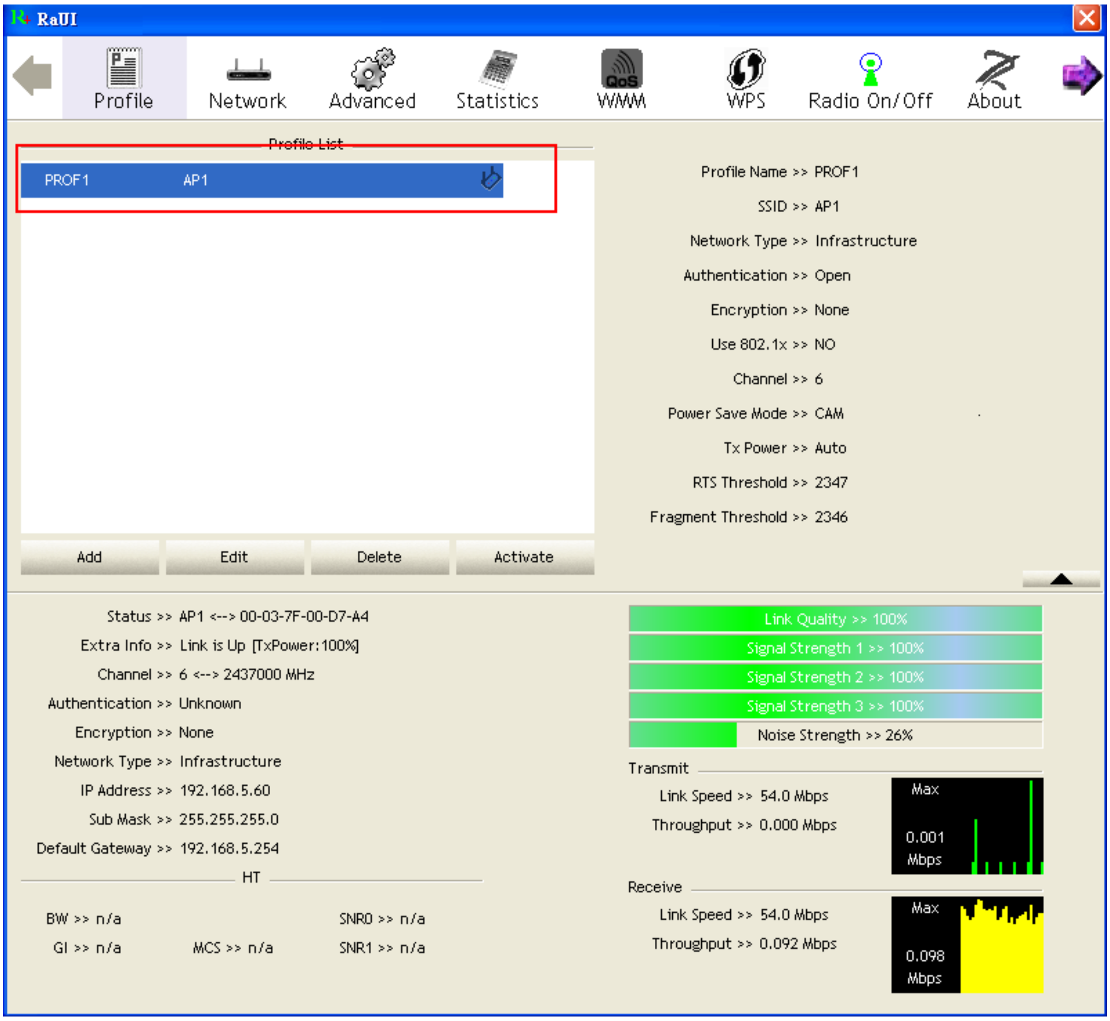
Tx Power >> Auto

Preamble >> Auto

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

4. Next, you will see the new profile in the profile list. Click "Activate"



PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 6
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

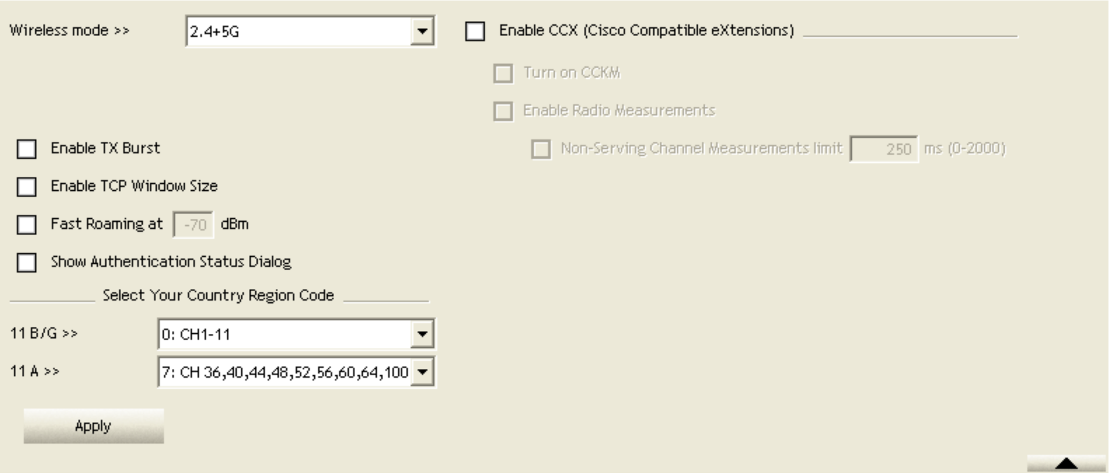
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
Max
0.001 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.092 Mbps
Max
0.098 Mbps

4.2.4 Advanced functions

4.2.4.1 Advanced functions

Figure 2-4 shows the Advance functions of RaUI.



Wireless mode >> 2.4+5G

☐ Enable CCX (Cisco Compatible eXtensions)

☐ Turn on CCKM

☐ Enable Radio Measurements

☐ Non-Serving Channel Measurements limit 250 ms (0-2000)

☐ Enable TX Burst

☐ Enable TCP Window Size

☐ Fast Roaming at -70 dBm

☐ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

11 A >> 7: CH 36,40,44,48,52,56,60,64,100

Figure 2-4 Advance function

1. Wireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported.
2. Wireless Protection: Users can choose from Auto, On, and Off. (This is not supported by 802.11n adapters.)

a. Auto: STA will dynamically change as AP announcement.

b. On: The frames are always sent with protection.

c. Off: The frames are always sent without protection.

3. TX Rate: Manually select the transfer rate. The default setting is auto. (802.11n wireless cards do not allow the user to select the TX Rate.)
4. Enable TX Burst: Ralink's proprietary frame burst mode.
5. Enable TCP Window Size: Optimise the TCP window size to allow for greater throughput.
6. Fast Roaming at-: enables fast roaming, which is set by the transmit power.
7. Select Your Country Region Code: There are eight countries to choose from in the country channel list. (11A ListBox only shows for 5G adapter.)
8. Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.
9. Enable CCX (Cisco Compatible Extensions): Choose whether Cisco Compatible Extensions are supported or not.

a. LEAP turn on CCKM.

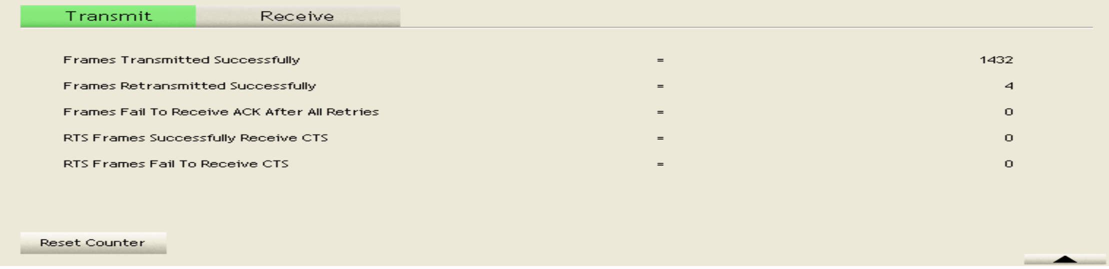
b Enabled Radio Measurement: can measure the channel every 0~2000 milliseconds

10. Apply the above changes

4.2.5 Statistics

4.2.5.1 Statistics

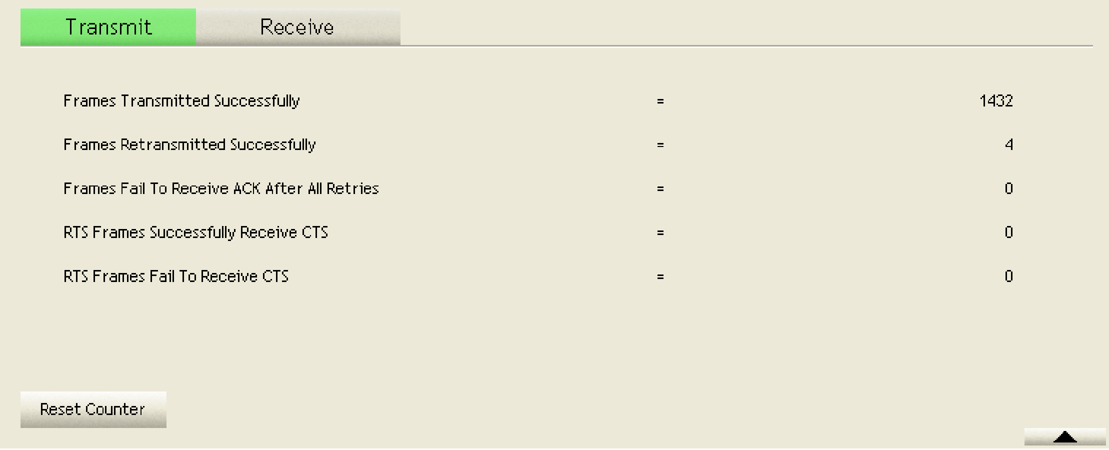
The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to understand. Figure 2-5-1 shows the detailed page layout.



Frames Transmitted Successfully = 1432
Frames Retransmitted Successfully = 4
Frames Fail To Receive ACK After All Retries = 0
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0

Figure 2-5-1 Statistics function

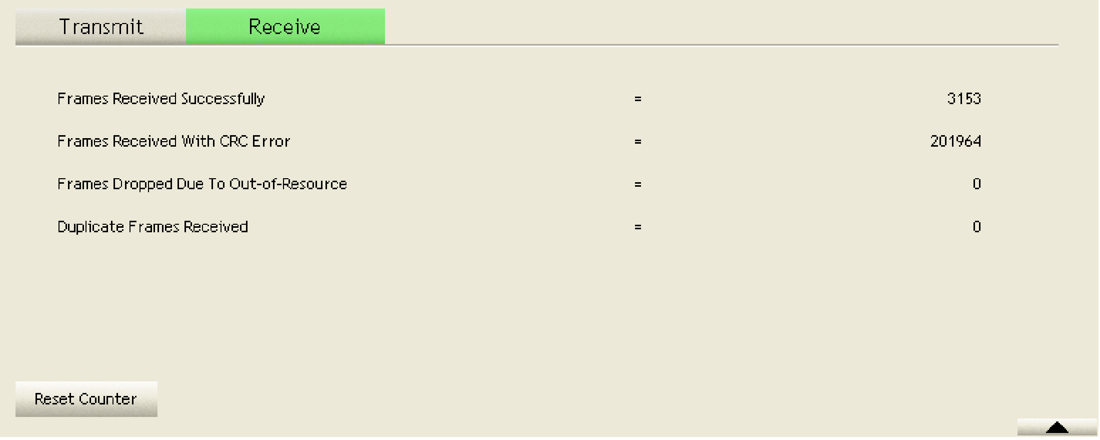
Transmit Statistics:



Frames Transmitted Successfully = 1432
Frames Retransmitted Successfully = 4
Frames Fail To Receive ACK After All Retries = 0
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0

1. Frames Transmitted Successfully: Frames successfully sent.
2. Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
3. RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
4. RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.
5. Frames Retransmitted Successfully: Successfully retransmitted frames numbers.
6. Reset counters to zero.

Receive Statistics:



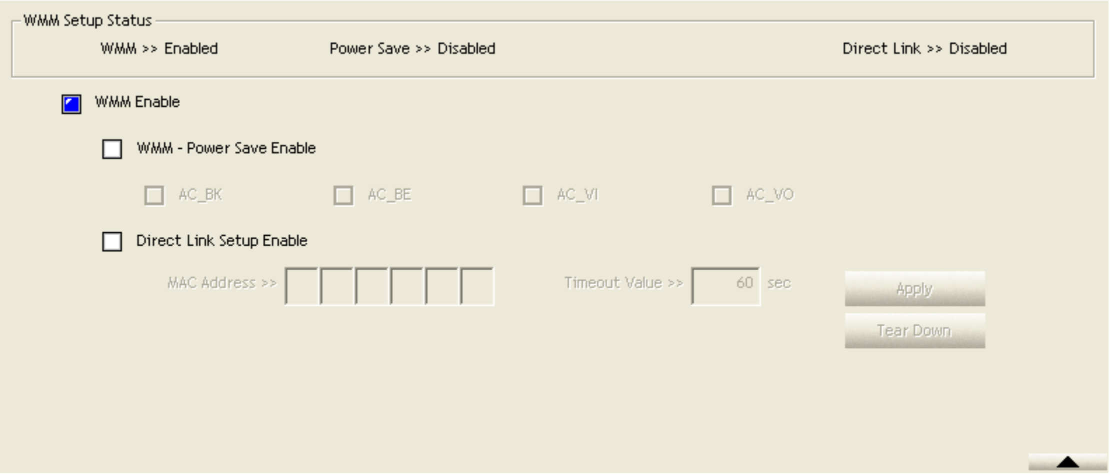
Frames Received Successfully = 3153
Frames Received With CRC Error = 201964
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0

1. Frames Received Successfully: The number of frames successfully received.
2. Frames Received With CRC Error: The number of frames received with a CRC error.
3. Frames Dropped Due To Out-of-Resource: The number of frames dropped due to a resource issue.
4. Duplicate Frames Received: The number of duplicate frames received.
5. Reset all the counters to zero.

4.2.6 WMM

4.2.6.1 WMM

Figure 2-6-1 shows WMM function of RaUI. It involves "WMM Enable", "WMM -Power Save Enable" and DLS setup. The introduction indicates as follow :



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Disabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

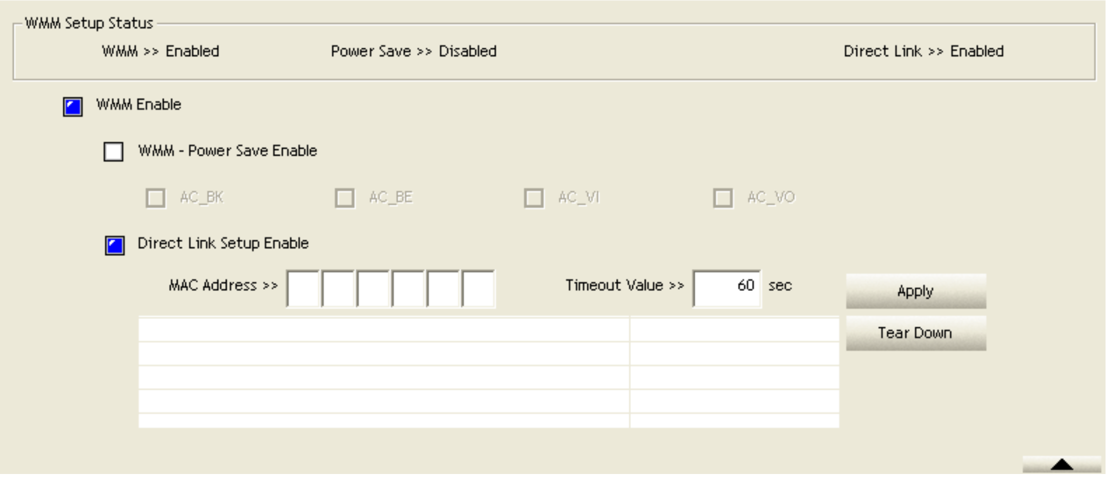
MAC Address >>   Timeout Value >> 60 sec

Figure 2-6-1 WMM function

1. WMM Enable: Enable Wi-Fi Multi-Media. The setting method follows Section 2-6-2.
2. WMM - Power Save Enable: Enable WMM Power Save. The setting method follows Section 2-6-3.
3. Direct Link Setup Enable: Enable DLS (Direct Link Setup). The setting method follows Section 2-6-4.

4.2.6.2 Example to Configure to Enable DLS (Direct Link Setup)

1. Click the "Direct Link Setup Enable" checkbox



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

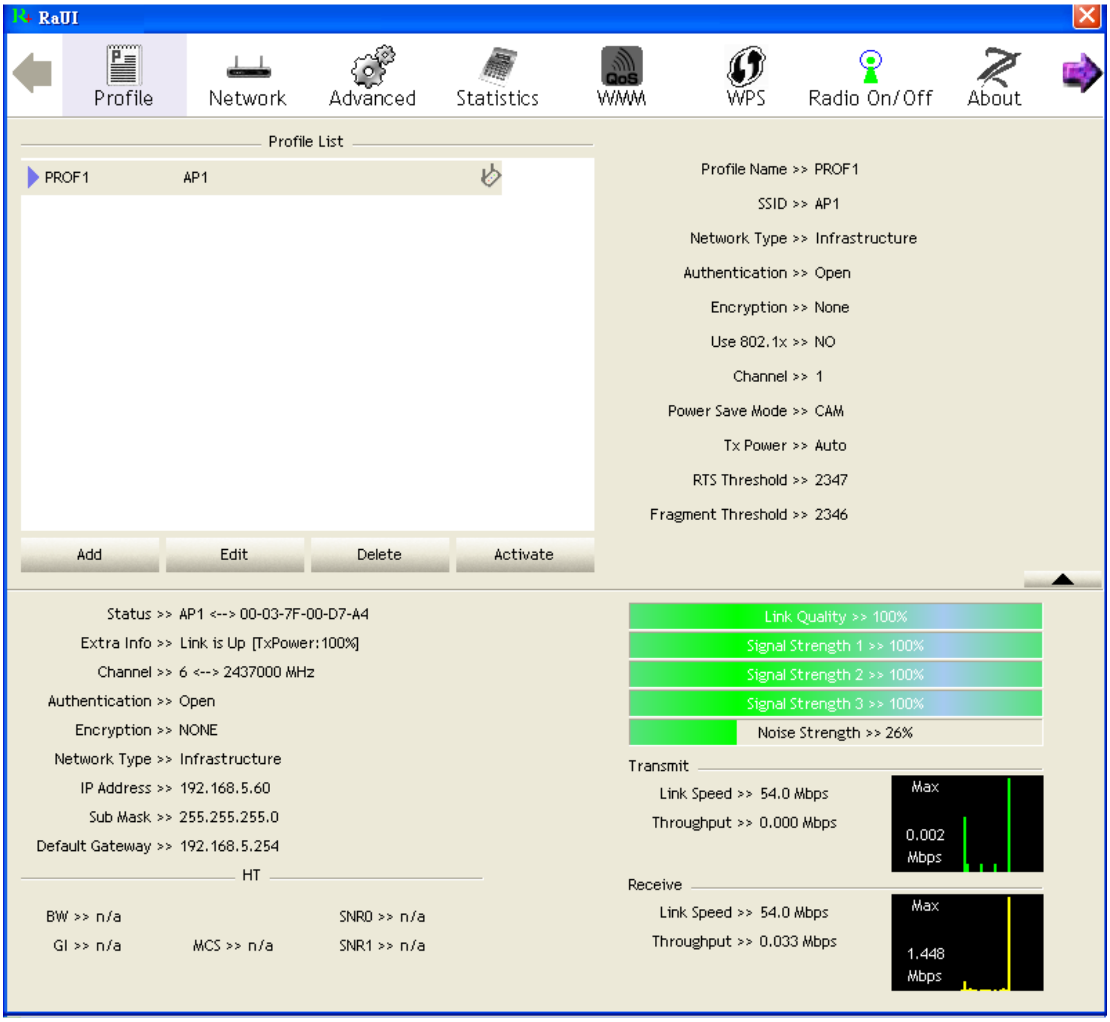
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

2. Change to "Network" function. Add an AP that supports DLS features to the profile. The result will look like the Profile Page in the figure below.



PROF1   AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

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   SNR0 >> n/a
GI >> n/a   MCS >> n/a   SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

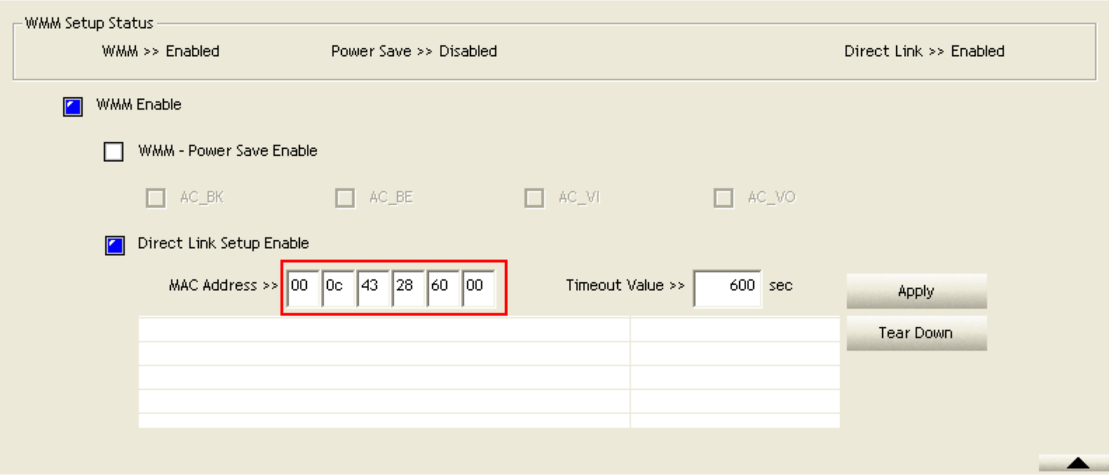
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps

The DLS settings are explained as follows:

1. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to these two conditions.

a. Connect with an AP that supports DLS features.

b. Ensure that DLS is enabled.



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

□ WMM - Power Save Enable

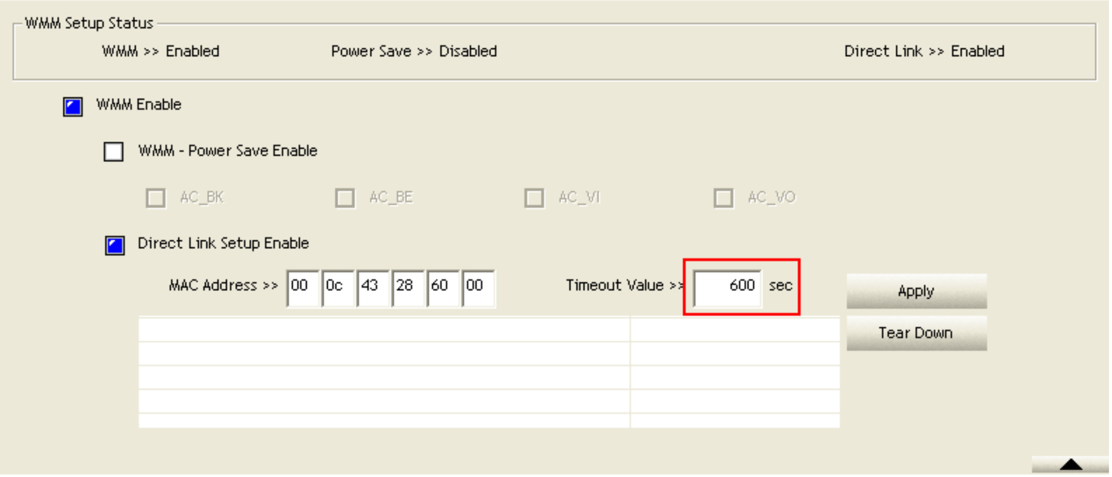
□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

2. The Timeout Value indicates the time in seconds before it disconnects automatically.

The value is an integer. The integer must be between 0~65535. A zero value specifies that it stays connected. The default Timeout Value is 60 seconds.



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

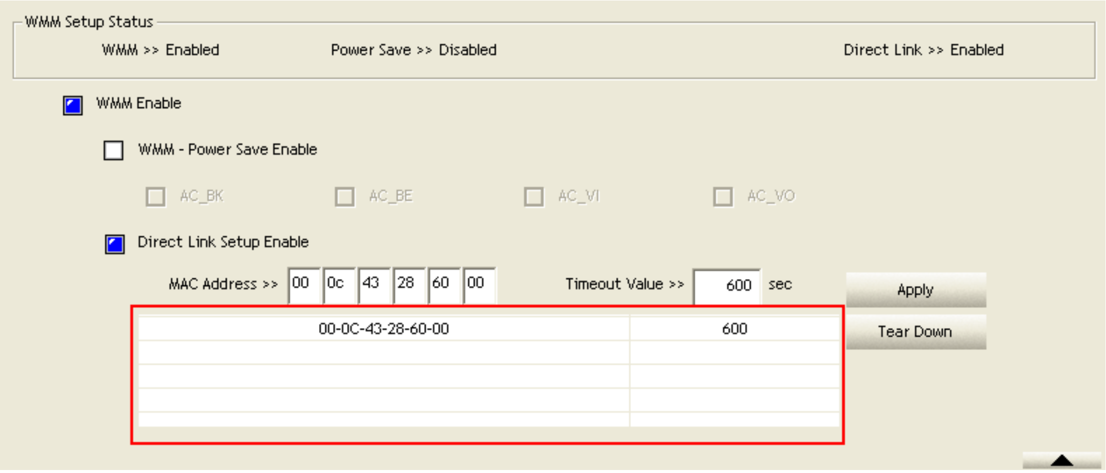
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

3. Click "Apply"



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

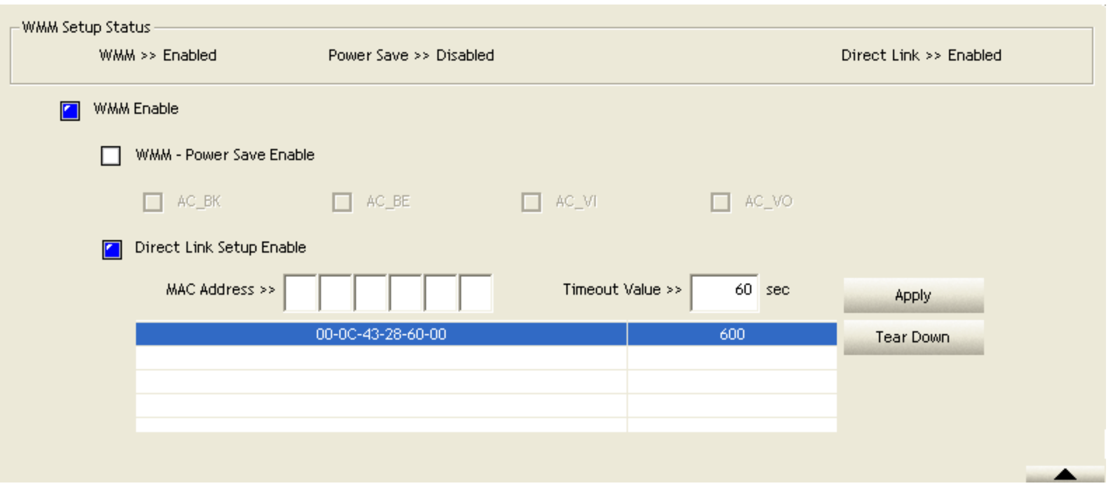
00-0C-43-28-60-00	600

Describe "DLS Status" as follow :

a. After configuring the DLS successfully, the MAC address and Timeout Value are displayed in the "DLS Status". In "DLS Status" on the opposite side, the user’s local MAC address and Timeout Value are displayed.

b. Display the values of "DLS Status" to "Direct Link Setup" as follow:

1. In "DLS Status" select a direct link STA what you want to show it's values in "Direct Link Setup".



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

☐ WMM - Power Save Enable

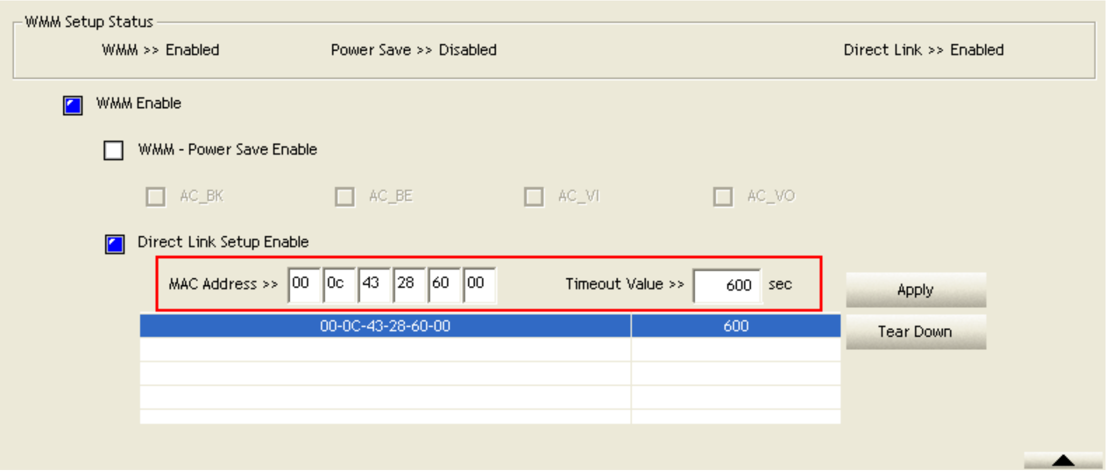
☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☑ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

00-0C-43-28-60-00	600

2. Double click. And the result will look like the below figure.



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

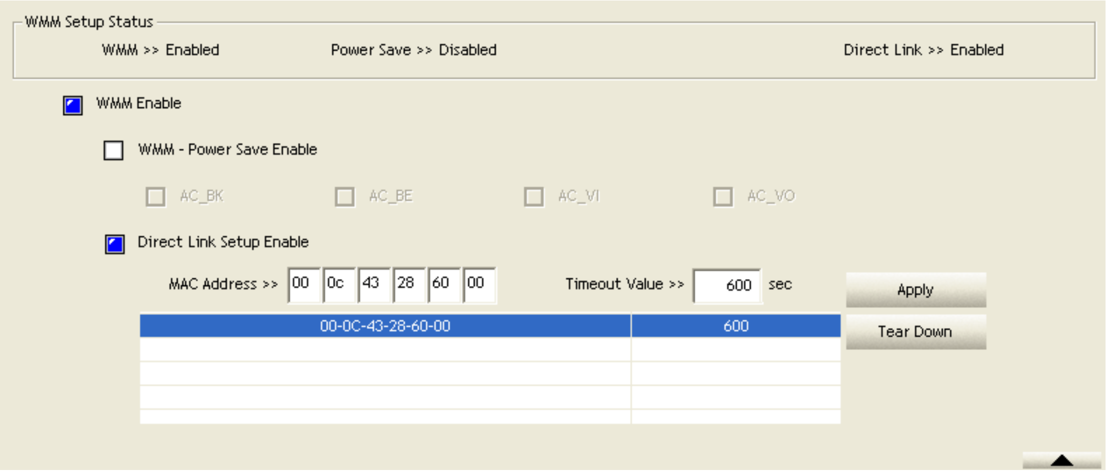
☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

00-0C-43-28-60-00	600

c. Disconnect Direct Link Setup as follow:

1. Select a direct link STA.



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

□ WMM - Power Save Enable

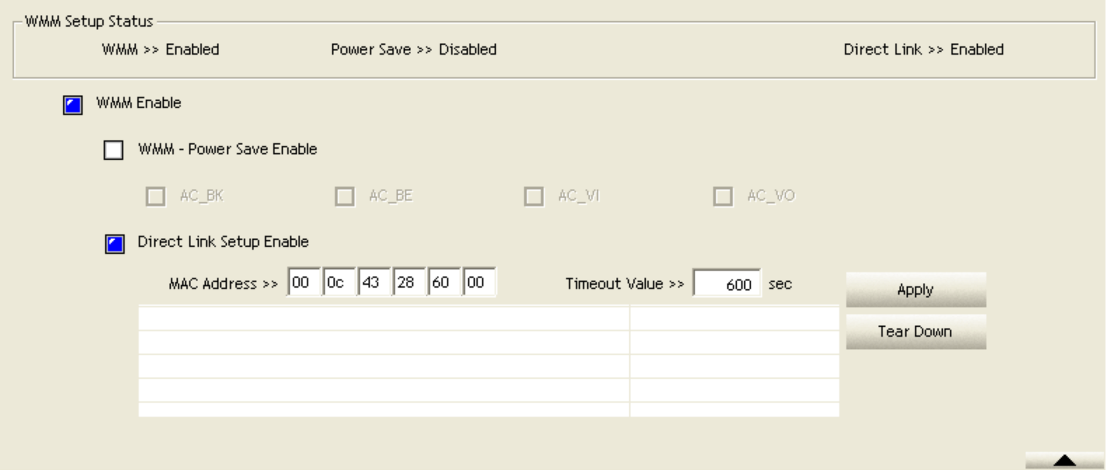
□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

00-0C-43-28-60-00	600

2. Click "Tear Down" button. The result will look like the below figure.



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

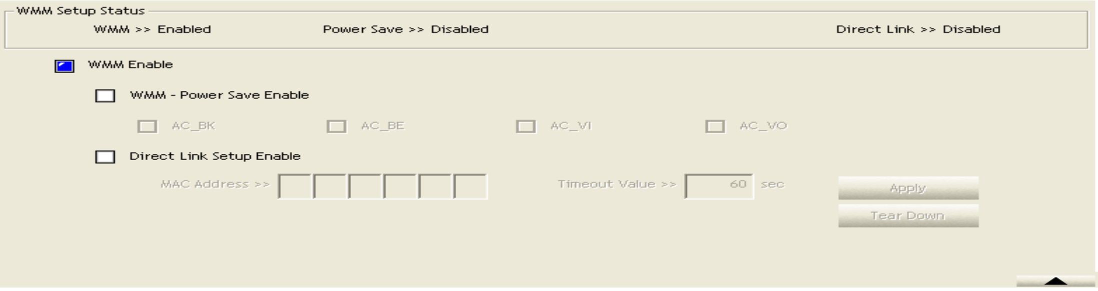
☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

4.2.6.3 Example to Configure TO Enable Wi-Fi Multi-Media

If you want to use "WMM-Power Save" or "Direct Link" you must enable WMM. The setting method of enabling WMM indicates as follows:

1. Click "WMM Enable".



WMM Setup Status
WMM >> Enabled   Power Save >> Disabled   Direct Link >> Disabled

☑ WMM Enable

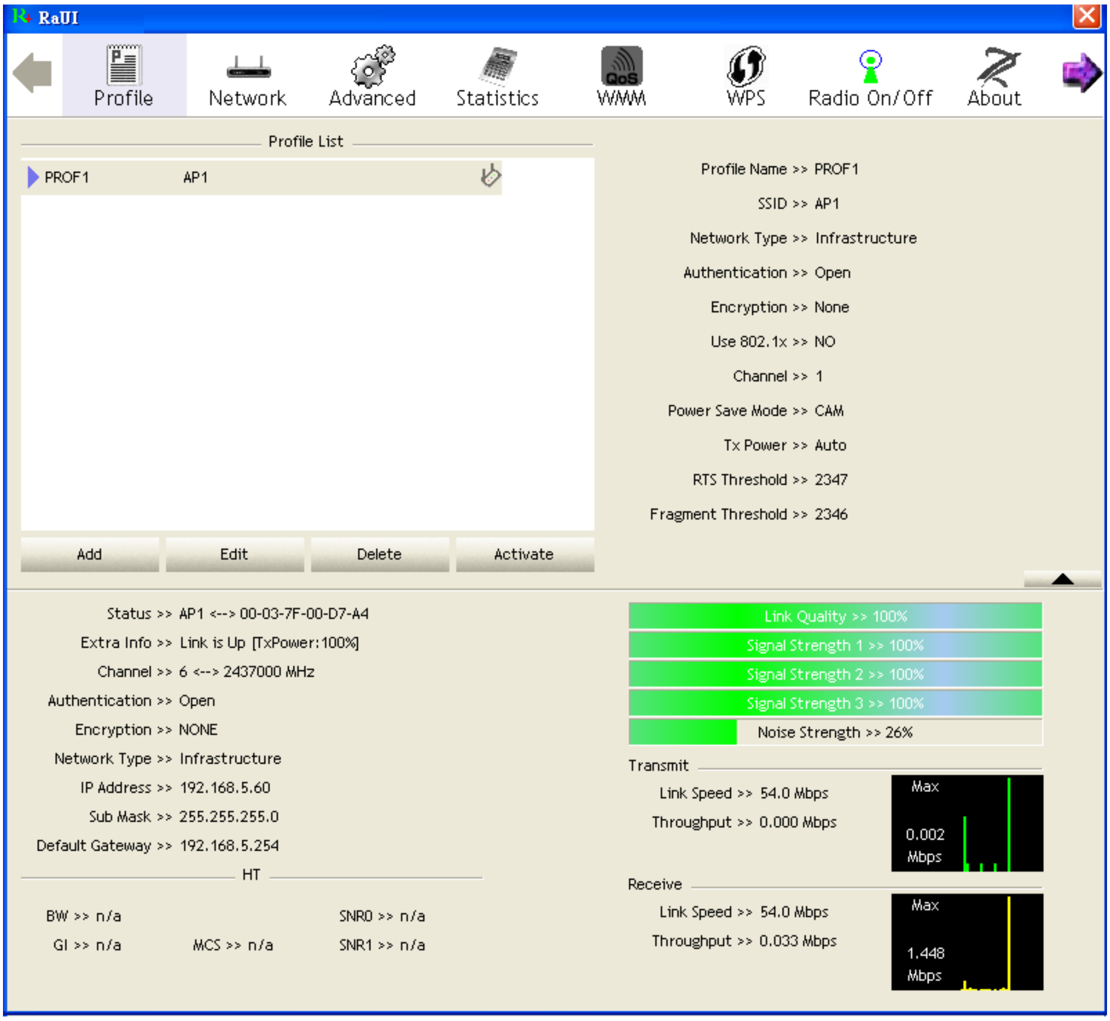
□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

2. Change to "Network" function. And add an AP that supports WMM features to a Profile. The result will look like the below figure in Profile page.



Profile List

PROF1   AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

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   SNR0 >> n/a
GI >> n/a   MCS >> n/a   SNR1 >> n/a

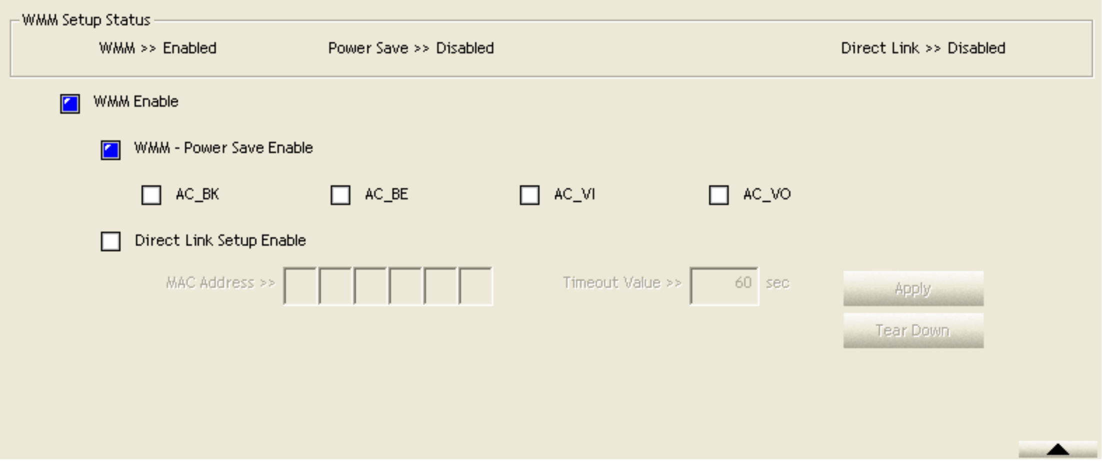
Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps

4.2.6.4 Example to Configure TO Enable WMM-Power Save

1. Click "WMM-Power Save Enable".



WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link >> Disabled

☑ WMM Enable

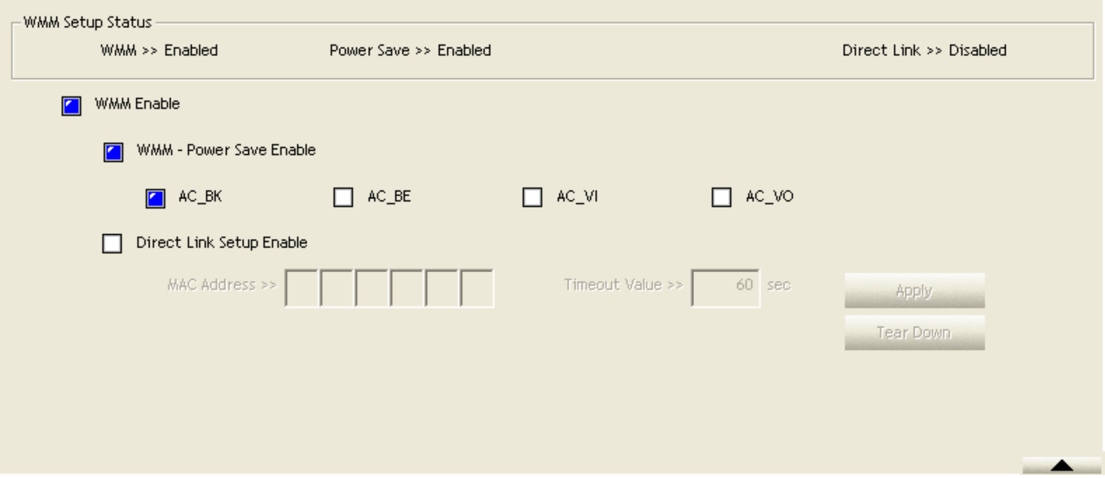
☑ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

2. Please select which ACs you want to enable. The setting of enabling WMM Power Save is successfully.



WMM Setup Status

WMM >> Enabled Power Save >> Enabled Direct Link >> Disabled

☑ WMM Enable

☑ WMM - Power Save Enable

☑ AC_BK □ AC_BE □ AC_VI □ AC_VO

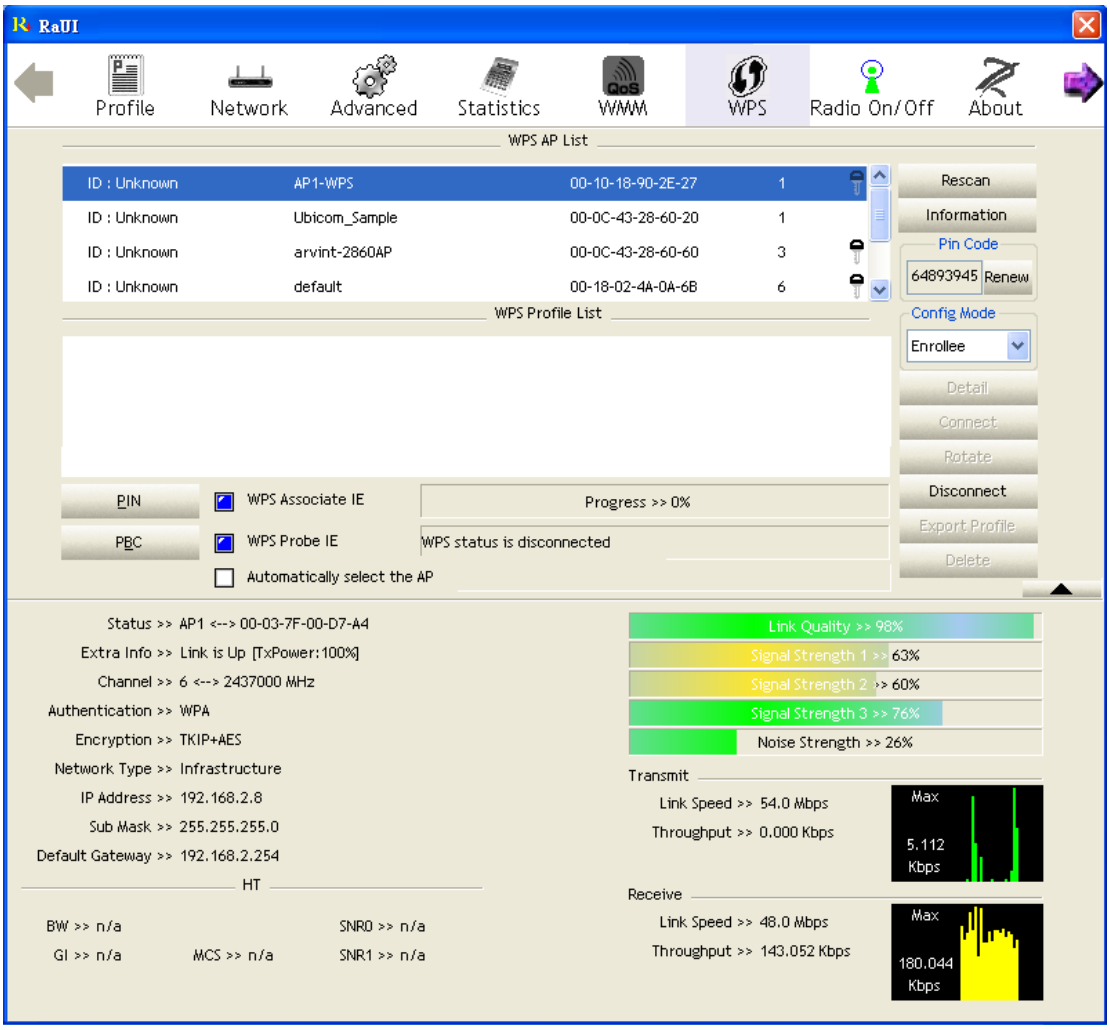
□ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

4.2.7 WPS

4.2.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> TKIP+AES
Network Type >> Infrastructure
IP Address >> 192.168.2.8
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.2.254

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 98%
Signal Strength 1 >> 63%
Signal Strength 2 >> 60%
Signal Strength 3 >> 76%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps
5.112 Kbps

Receive
Link Speed >> 48.0 Mbps
Throughput >> 143.052 Kbps
180.044 Kbps

Figure 2-7-1 WPS function

1. WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks.

Ralink STA supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.

2. WPS AP List: Displays the information of the surrounding APs with WPS IE from the last scan result. The detailed information includes the SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.

3. Rescan: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

4. Information: Displays the information about WPS IE on the selected network. The detailed list includes the Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. Further details are available here: WPS Information on AP.

5. PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to re-generate a new PIN Code.

6. Config Mode: The station serving as an Enrollee or an external Registrar.

7. Table of Credentials: Displays all credentials obtained by the Registrar. The detailed list includes information about the SSID, MAC Address, Authentication and Encryption Type. If STA is the Enrollee, the credentials are created immediately with each WPS success. If STA is the Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change this until switching to STA Registrar.

8. Control items for credentials.

a. Detail: Command to obtain Information about Security and the Key in the credential.

b. Connect: Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.

c. Rotate: Command to rotate to connect to the next network inside credentials.

d. Disconnect: Stops the WPS action and disconnects the active link. It then selects the most recent profile on the Profile Page of RaUI. If there are no profiles, the driver will select any non-security AP.

e. Export Profile: Exports all credentials to a Profile.

f. Delete: Deletes an existing credential. And then selects the next credential. If there is not another credential, the driver will select any non-security AP.

9. 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.

10. PBC: Start to add to AP using PBC configuration method.

After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

11. WPS associate IE: Sends the association request with WPS IE during the WPS setup. It is optional for STA.

12. WPS probe IE: Sends the probe request with WPS IE during WPS setup. It is optional for STA.

13. Progress Bar: Displays the rate of progress from Start to Connected.

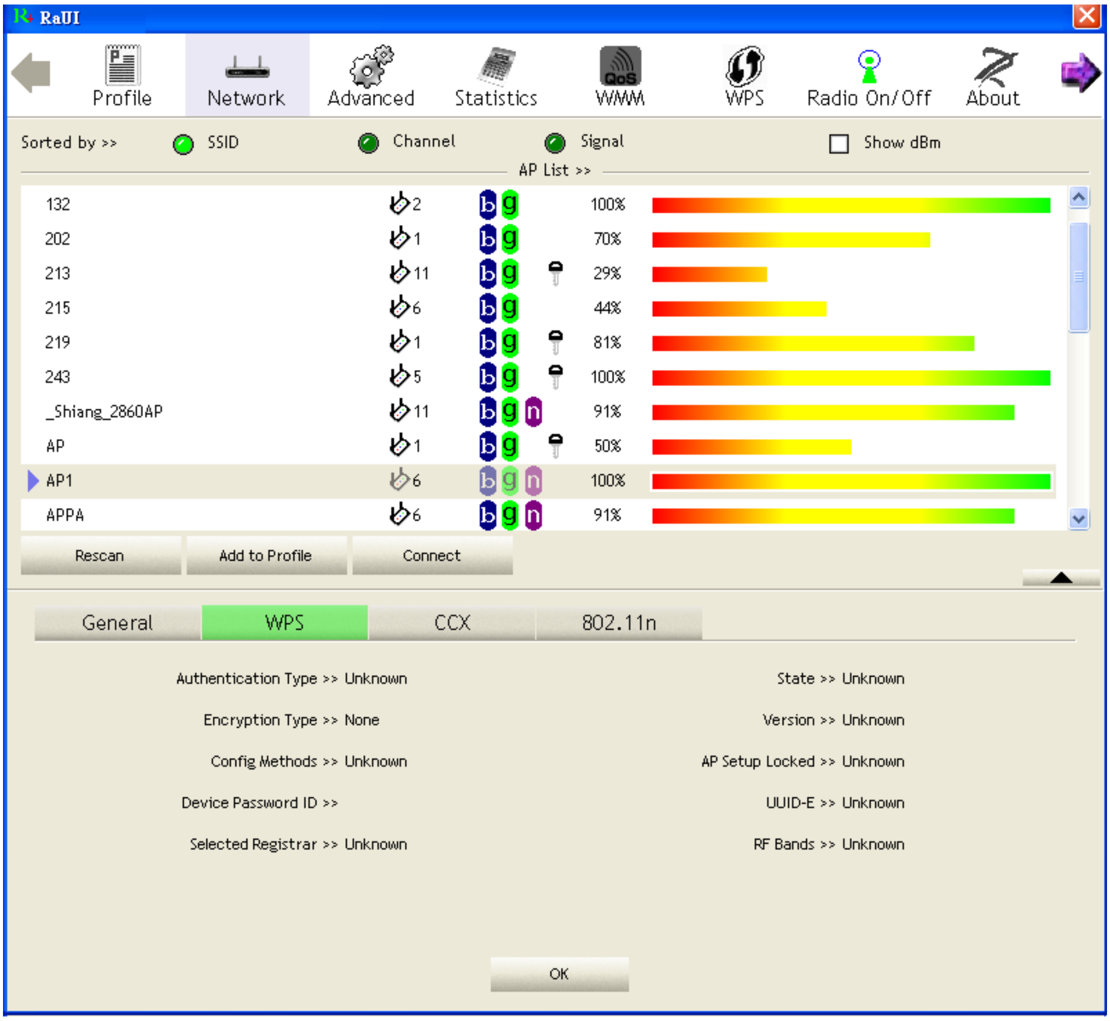
14. Status Bar: Displays the current WPS Status.

15. Automatically select the AP: Starts to add to AP by using to select the AP automatically in PIN method.

**There are examples in section 2-7-3 (PIN Enrollee Setup), section 2-7-4(PBC Enrollee Setup) and section 2-7-5 (Registrar Configures and AP) **

4.2.7.2 WPS Information on AP

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



132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Unknown

Version >> Unknown

AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

1. Authentication Type: There are three authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

2. Encryption Type: For open and shared authentication mode, the selection of encryption type are none and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSKauthentication mode, the encryption type supports both TKIP and AES.

3. Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (A bitwise OR of values)

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

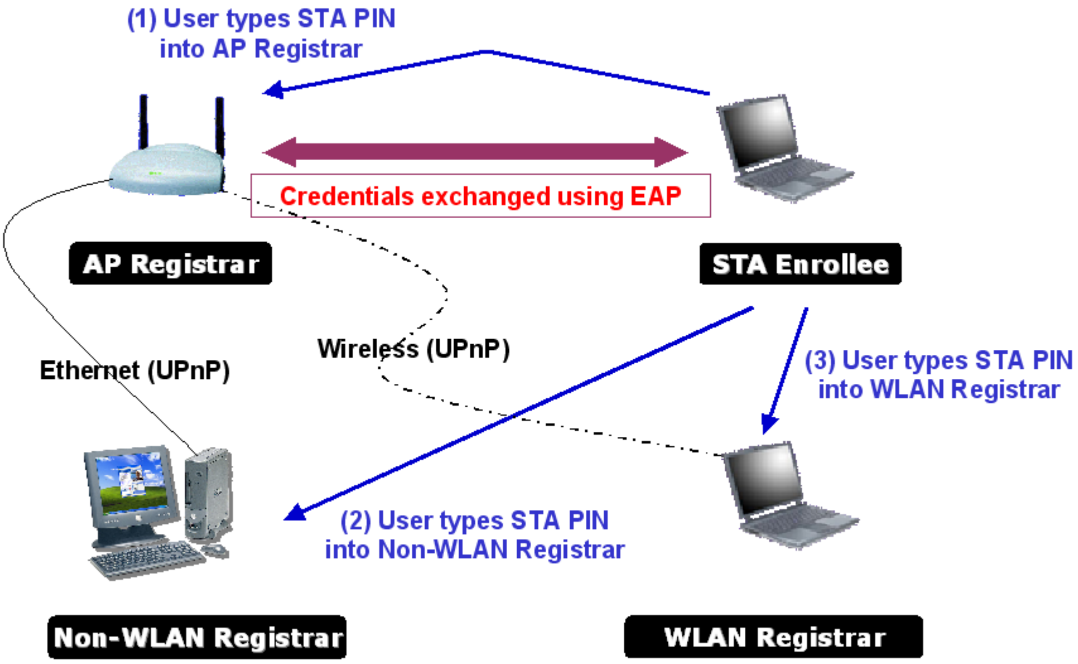
4. Device Password ID: Indicates the method or identifies the specific password that the selected Registrar intends to use. APs in PBC mode must indicate 0x0004 within two-minute Walk Time.

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

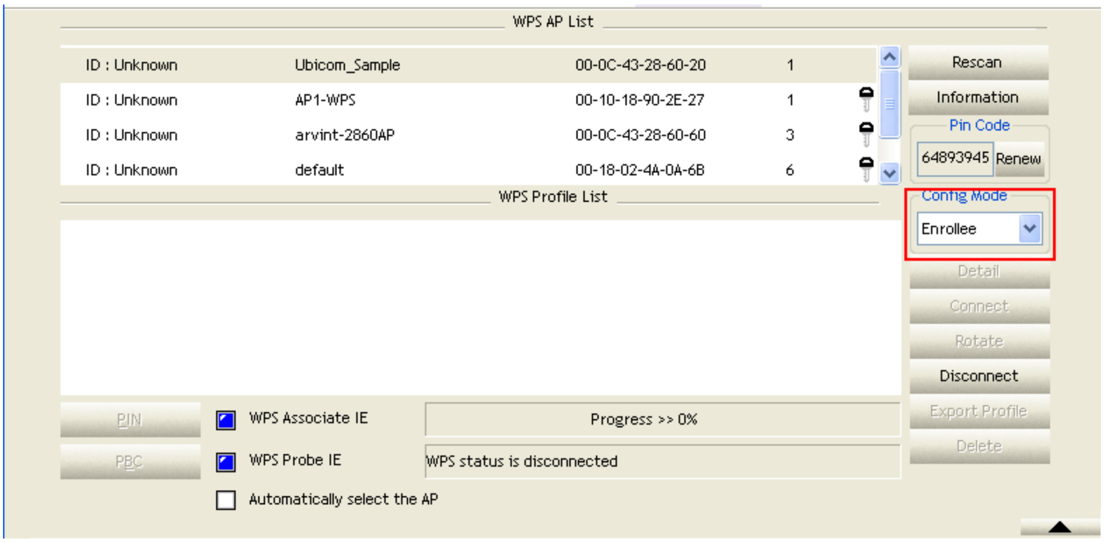
5. Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
6. State: The current configuration state on AP. The values are "Unconfigured" and "Configured".
7. Version: WPS specified version. AP Setup Locked: Indicates if the AP has entered a setup locked state.
8. UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. This is a 16 byte value.
9. RF Bands: Indicates all the RF bands available on the AP. A dual-band AP must
10. Provide it. The values are "2.4GHz" and "5GHz".

4.2.7.3 Example to Add to Registrar Using PIN Method

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The following image outlines the process.


(1) User types STA PIN into AP Registrar
Credentials exchanged using EAP
AP Registrar
STA Enrollee
Wireless (UPnP)
Ethernet (UPnP)
(3) User types STA PIN into WLAN Registrar
(2) User types STA PIN into Non-WLAN Registrar
Non-WLAN Registrar
WLAN Registrar

1. Select "Enrollee" from the Config Mode drop-down list.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

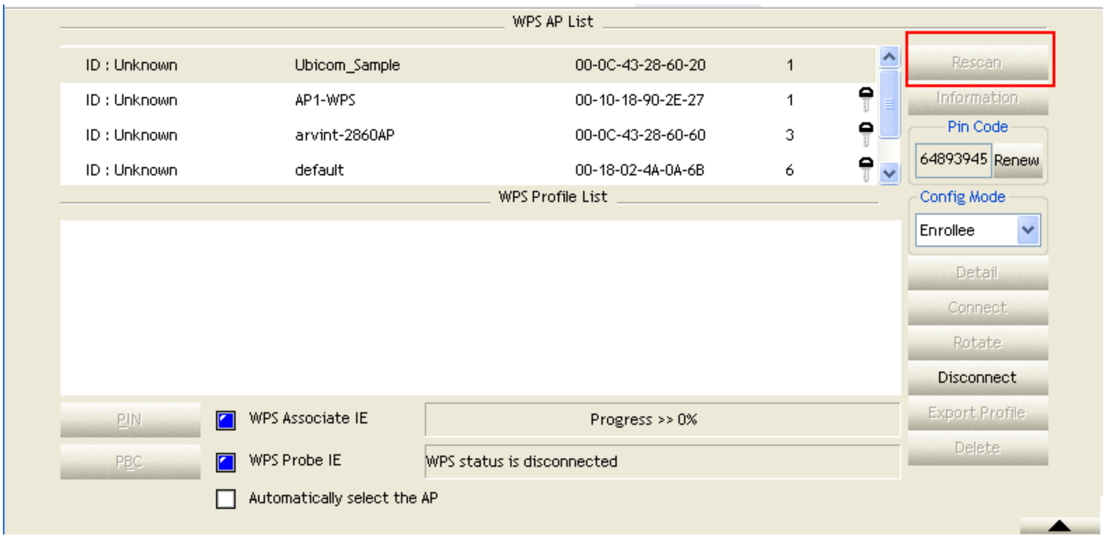
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

2. Click "Rescan" to update available WPS APs.



ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

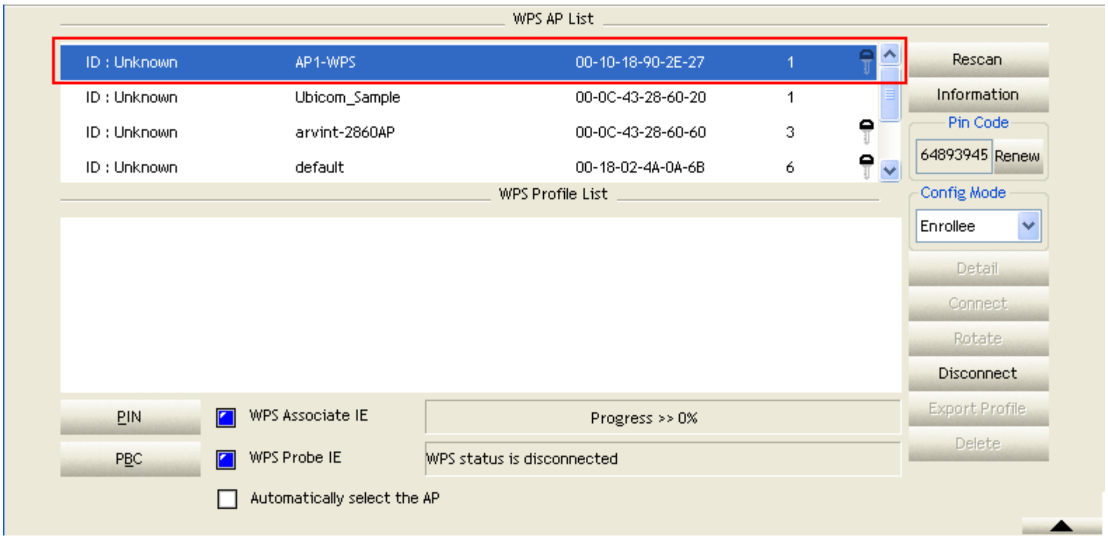
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

3. Select an AP (SSID/BSSID) that STA will join to.



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

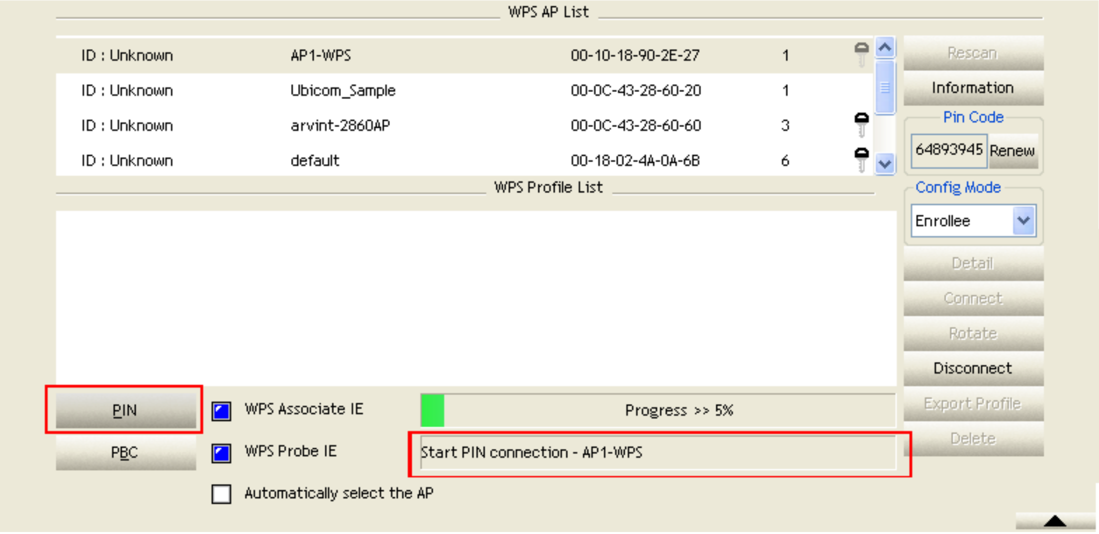
□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

4. Click "PIN" to enter the PIN

5. Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

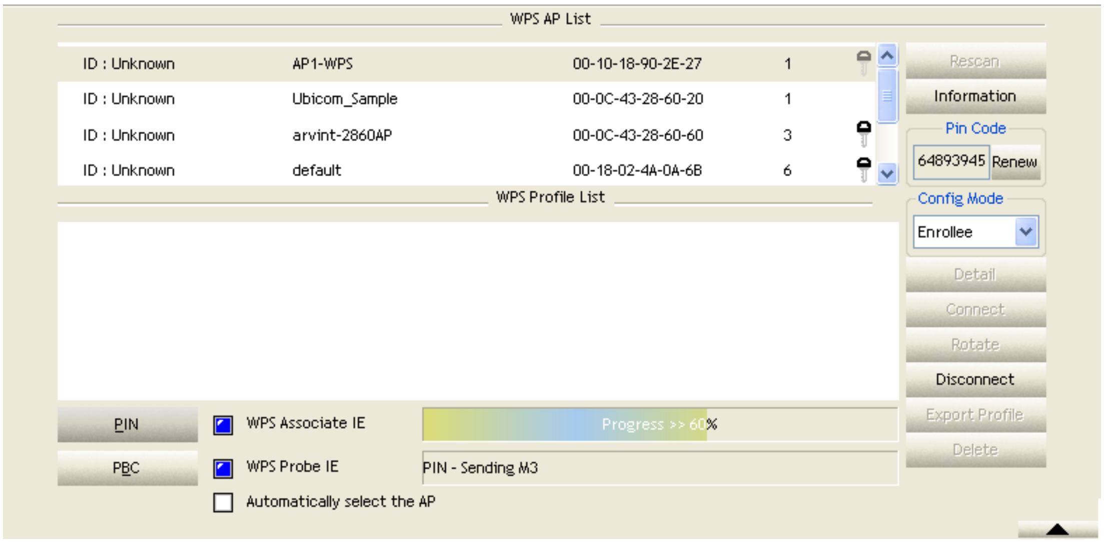
Progress >> 5%

Start PIN connection - AP1-WPS

Allow of an exchange between Step 4 and Step 5.

If you use Microsoft Window Connection Now as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

6. The result should appear as the image below.



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

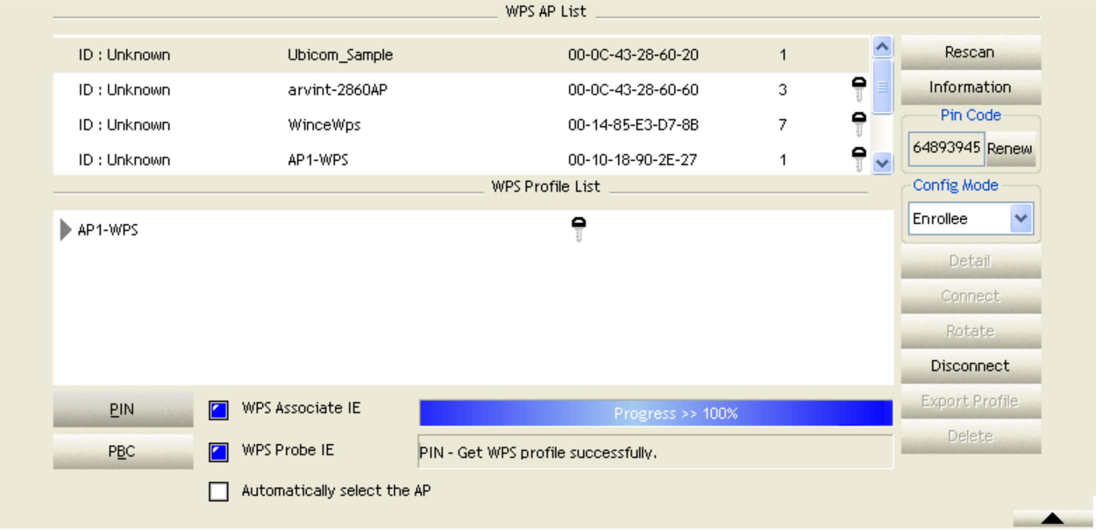
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 60%

PIN - Sending M3

7. Configure one or more credentials



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

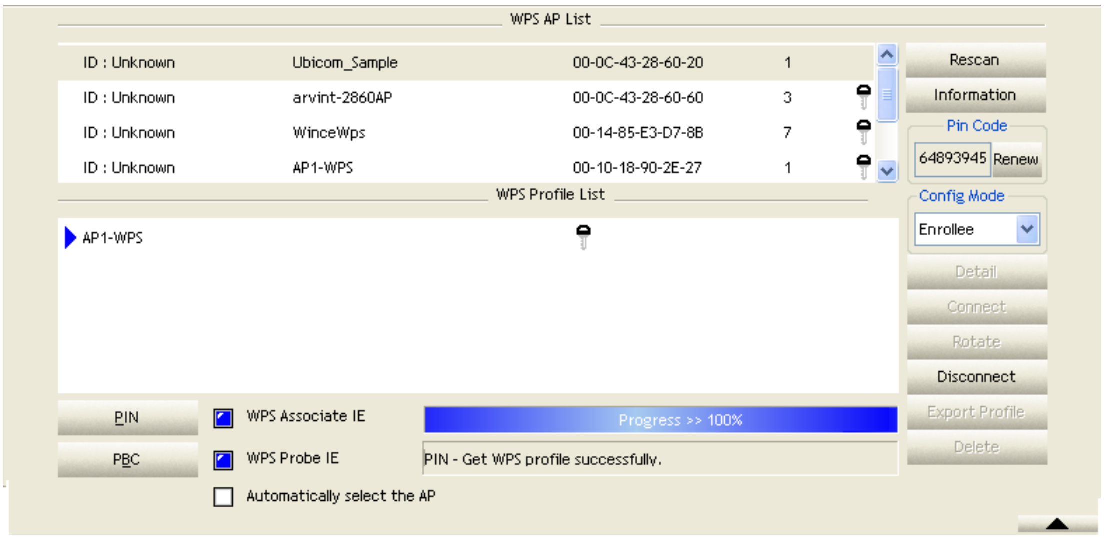
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

8. Then connect successfully. The result appears as the following image.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

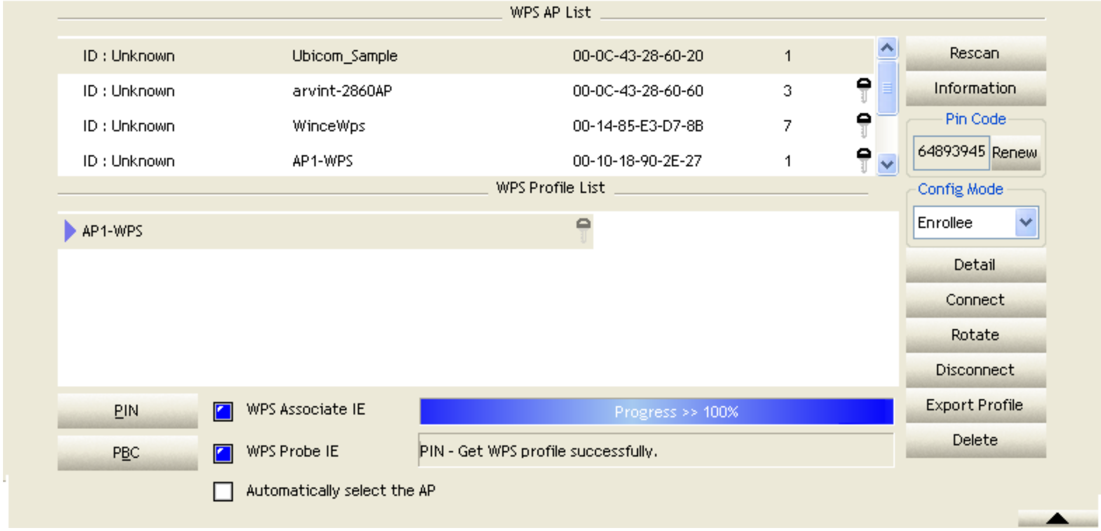
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

9. Click "Detail"



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

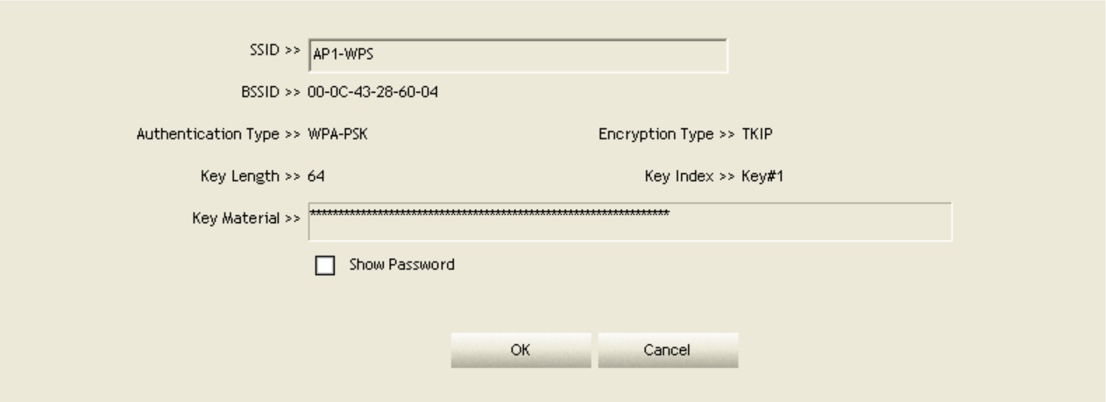
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

10. You will look like the below figure.



SSID >> AP1-WPS

BSSID >> 00-0C-43-28-60-04

Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Key Length >> 64

Key Index >> Key#1

Key Material >> **

□ Show Password

If Credential#1 is reliable and present, the system will connect with Credential#1.
If not, the system will automatically rotate to the next existing credential. The user can also click "Rotate" to rotate to the next credential usable credential

Describe "WPS Status Bar" - "PIN - xxx" as follow:

1. Acceptable PIN Configurations:

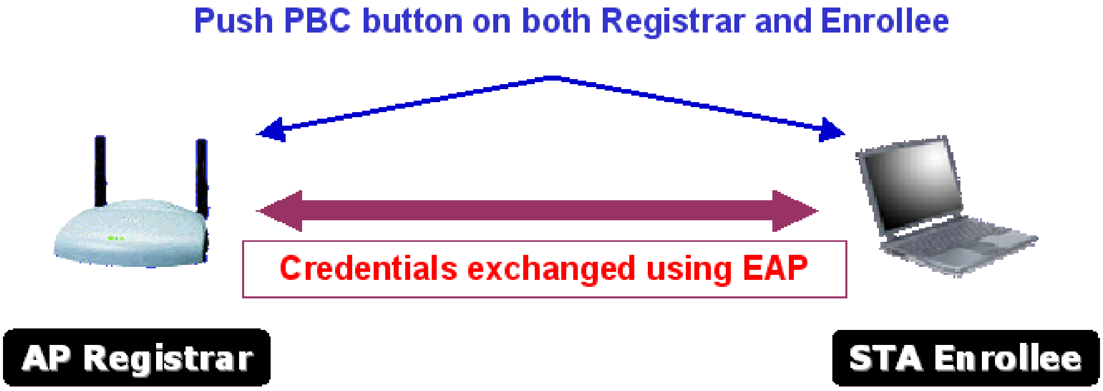
Start PIN connection - SSID -> Begin associating to WPS AP
-> Associated to WPS AP -> Sending EAPOL-Start
-> Sending EAP-Rsp (ID) -> Receive EAP-Req (Start) -> Sending M1
-> Received M2 -> (Received M2D -> Sending EAP-Rsp (ACK))
-> Sending M3 -> Received M4 -> Sending M5 -> Received M6
-> Sending M7 -> Received M8 -> Sending EAP-Rsp(Done)
-> Configured -> WPS status is disconnected
-> WPS status is connected successfully-SSID

2. WPS configuration doesn't complete after a two-minute connection:
WPS EAP process failed.
3. When errors occur within **two minutes of connecting**, the WPS status bar might
report "WPS Eap process failed".

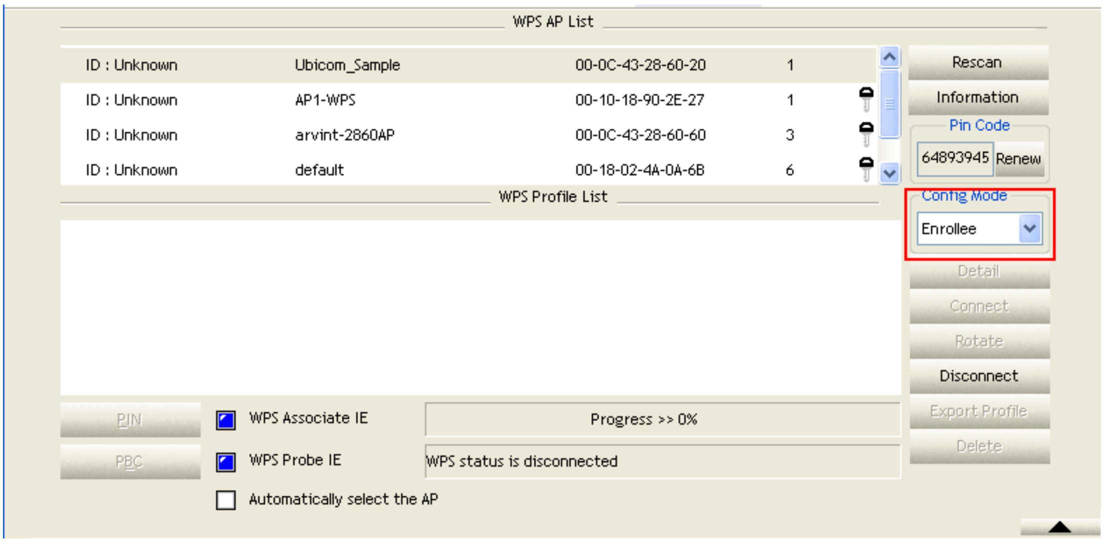
Error messages might be:
1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. Error PIN Code.
4. An inappropriate EAP-FAIL received.

4.2.7.4 Example to Add to Registrar Using PBC Method

The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately begin running the Registration Protocol.
If the Enrollee discovers more than one Registrar in PBC mode, it MUST abort its connection attempt at this scan and continue searching until the two-minute timeout.
*Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC
Mode or APs using PBC mode have left their Walk Time.


Push PBC button on both Registrar and Enrollee
Credentials exchanged using EAP
AP Registrar
STA Enrollee

1. Select "Enrollee" from the Config Mode drop-down list.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

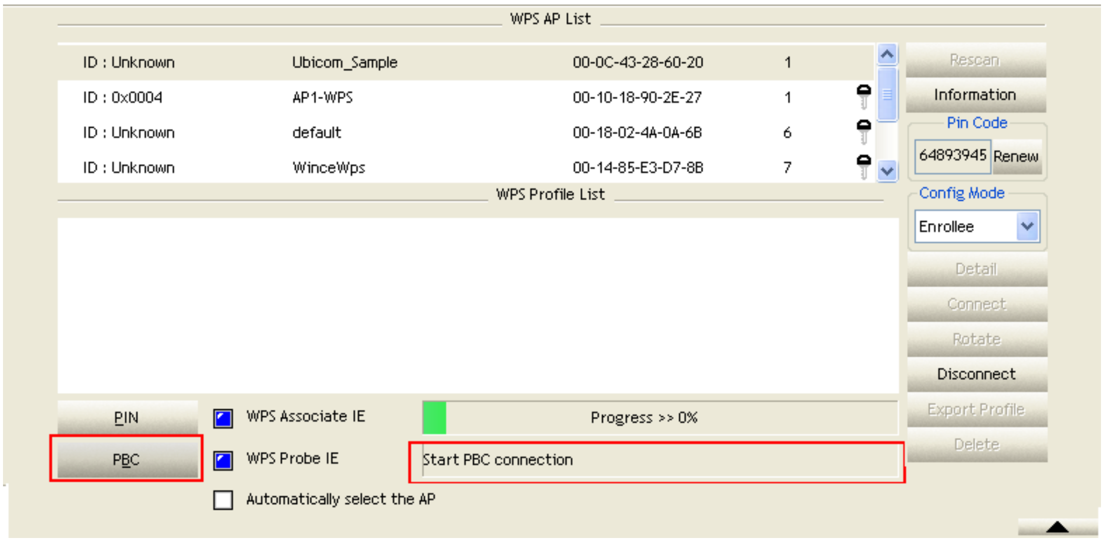
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

2. Click PBC to start the PBC connection.

3. Push the PBC on AP.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

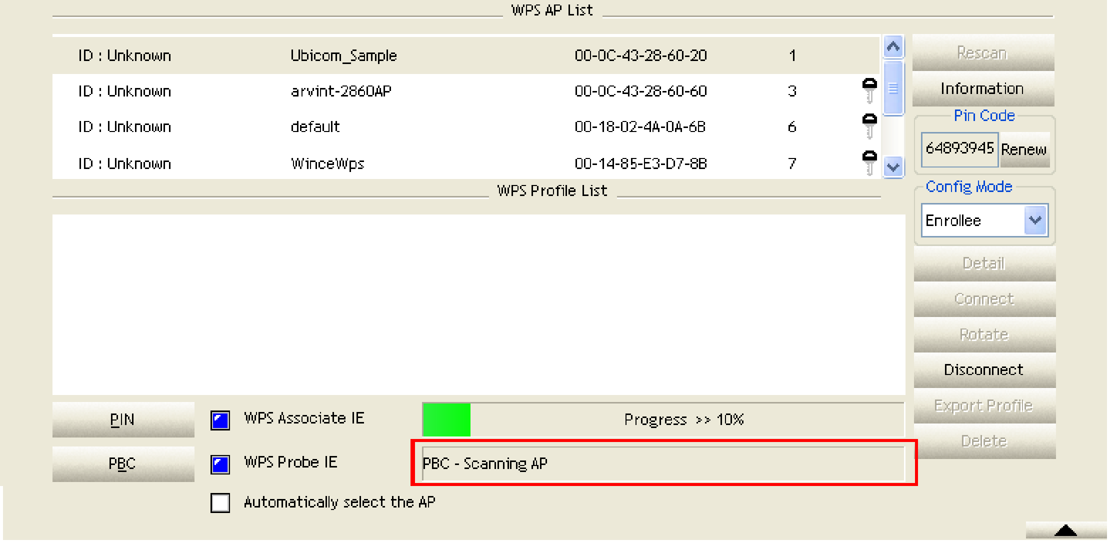
☐ Automatically select the AP

Progress >> 0%

Start PBC connection

*Allow time for an exchange between Step 2 and Step 3.

4. The progress bar as shown in the figure below indicates that scanning progress



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

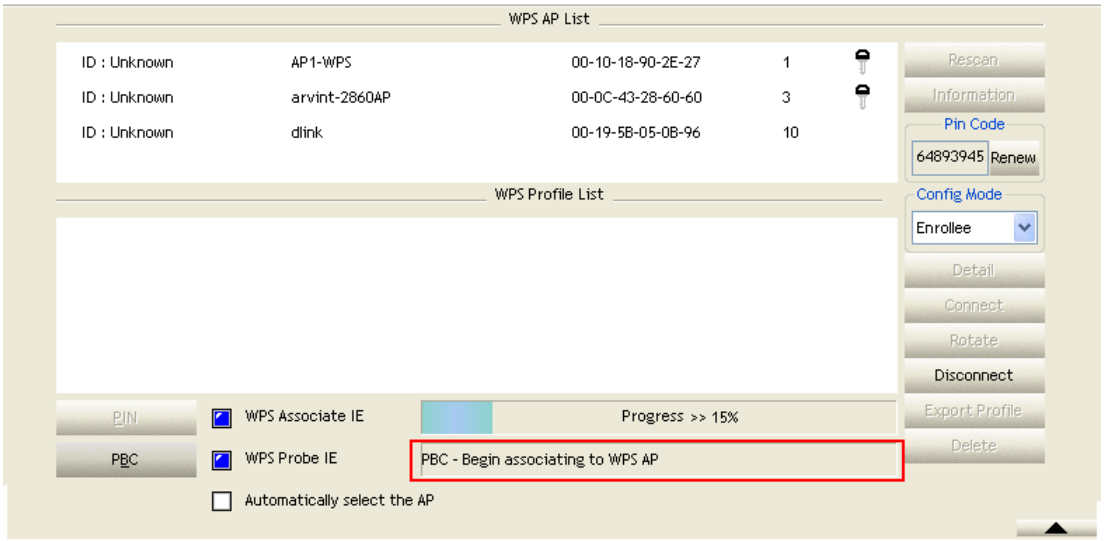
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 10%

PBC - Scanning AP

5. When one AP is found, join it.



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	🔑
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3	🔑
ID : Unknown	dlink	00-19-5B-05-0B-96	10	

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

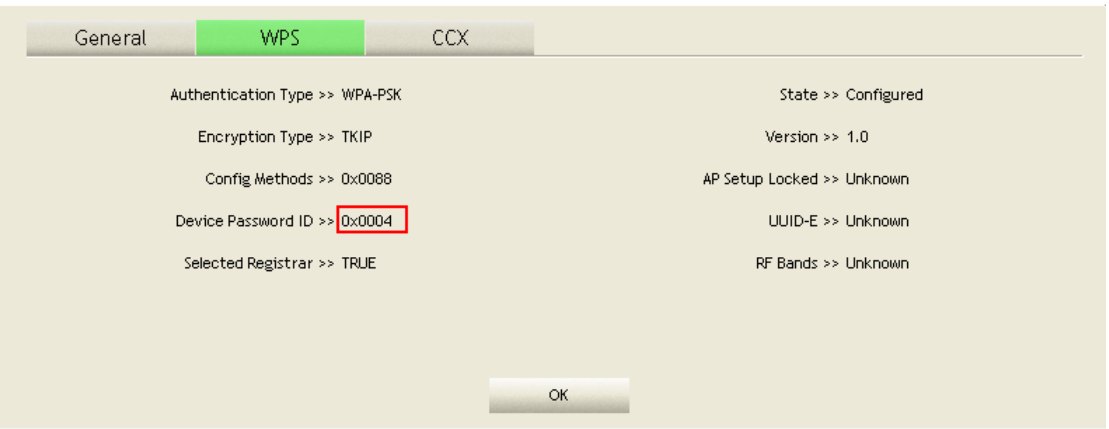
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 15%

PBC - Begin associating to WPS AP

6. Check WPS Information on the available WPS APs.



Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Config Methods >> 0x0088

Device Password ID >> 0x0004

Selected Registrar >> TRUE

State >> Configured

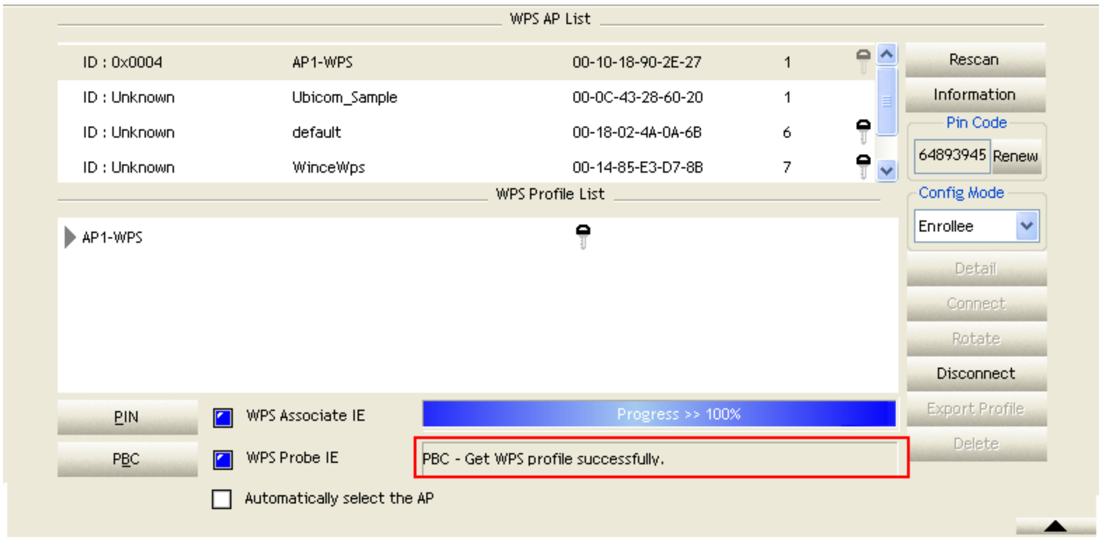
Version >> 1.0

AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

7. Configure and receive one or more credential(s).



WPS AP List

ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1	🔑
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1	
ID : Unknown	default	00-18-02-4A-0A-6B	6	🔑
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7	🔑

WPS Profile List

AP1-WPS 🔑

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

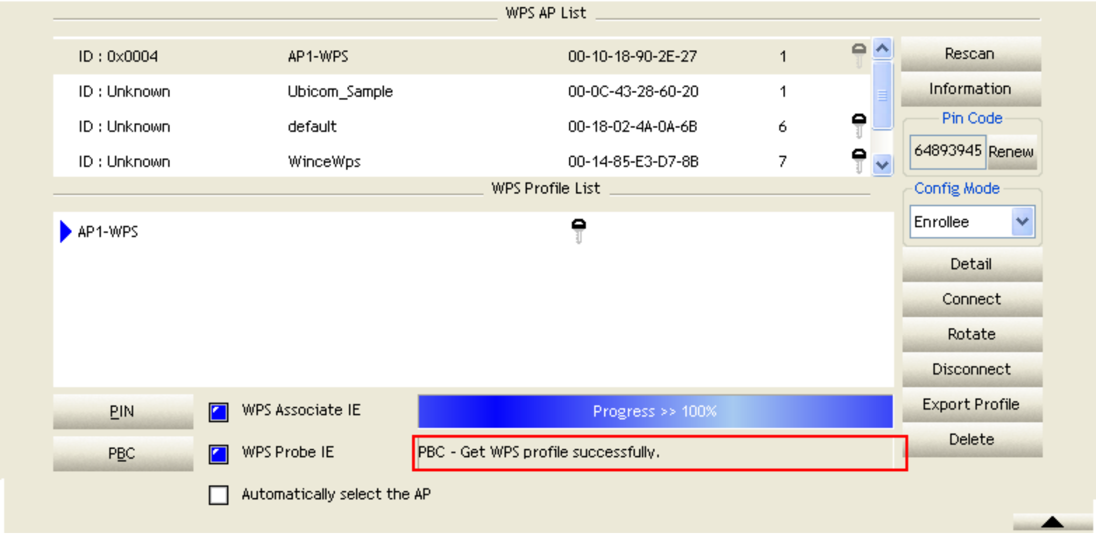
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PBC - Get WPS profile successfully.

8. Then connect successfully. The result will be displayed as it is in the figure below.



WPS AP List

ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

WPS Profile List

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PBC - Get WPS profile successfully.

Describe "WPS Status Bar" - "PBC - xxx" as follow:

1. A successful PBC Configuration:

Start PBC connection -> Scanning AP
-> Begin associating to WPS AP ->Associated to WPS AP
-> Sending EAPOL-Start -> Sending EAP-Rsp (ID)
->Receive EAP-Rsp (Start) -> Sending M1 -> Received M2
-> Sending M3 ->Received M4 -> Sending M5 -> Received M6
-> Sending M7 -> Received M8 ->Sending EAP-Rsp (Done)
-> Configured -> WPS status is disconnected
-> WPS status is connected successfully-SSID

2. No PBC AP available :

Scanning AP -> No PBC AP available -> Scanning AP -> No PBC AP available….

3. Too Many PBC AP available :

Scanning AP -> Too Many PBC AP available -> Scanning AP -> Too Many PBC AP available ->

4. WPS configuration doesn't complete after **two-minute connection**

WPS Eap process failed.

5. When Errors occur within **two-minutes of establishing a connection**, the WPS status bar might report "WPS Eap process failed".

Error messages might be:

1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. An inappropriate EAP-FAIL received.

Describe "Multiple PBC session overlaps" as follow:

a. Dual bands:

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a A-Band AP using PBC mode. (ID = 0x0004)

They have the same UUID-E.

STA would regard these two APs as a dual-radio AP and select one band to connect.

b. Different UUID-E :

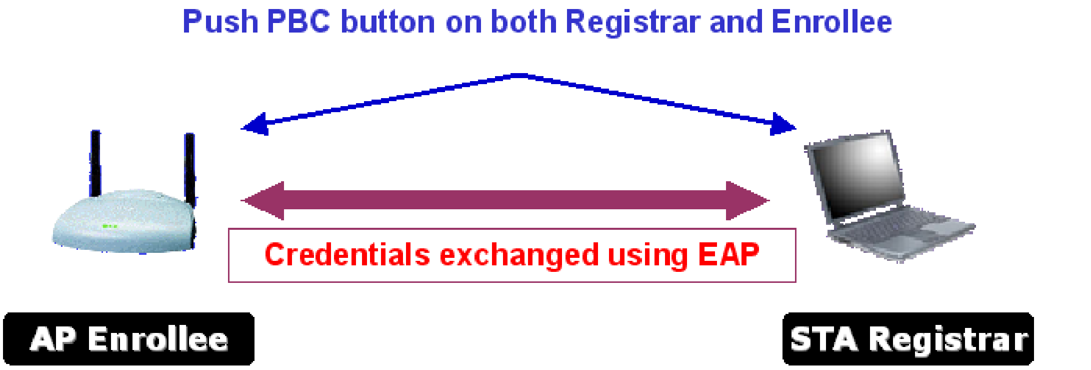
AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

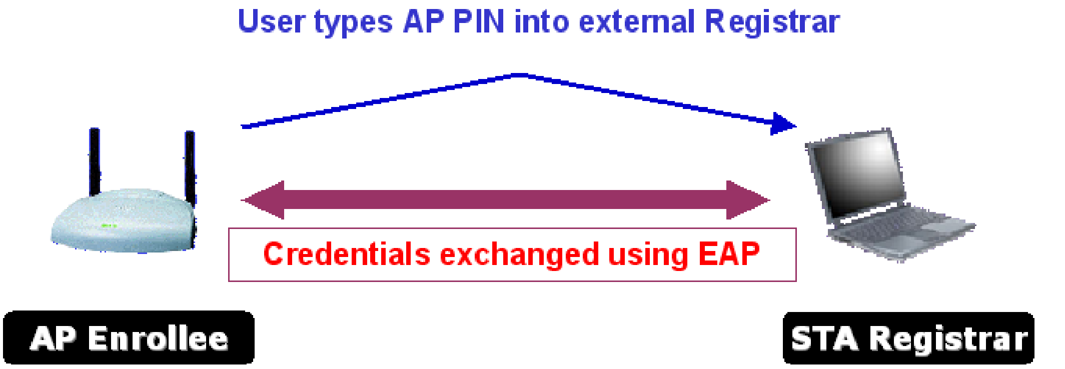
AP2 is a G-Band AP using PBC mode. (ID = 0x0004)

They have the different UUID-E.

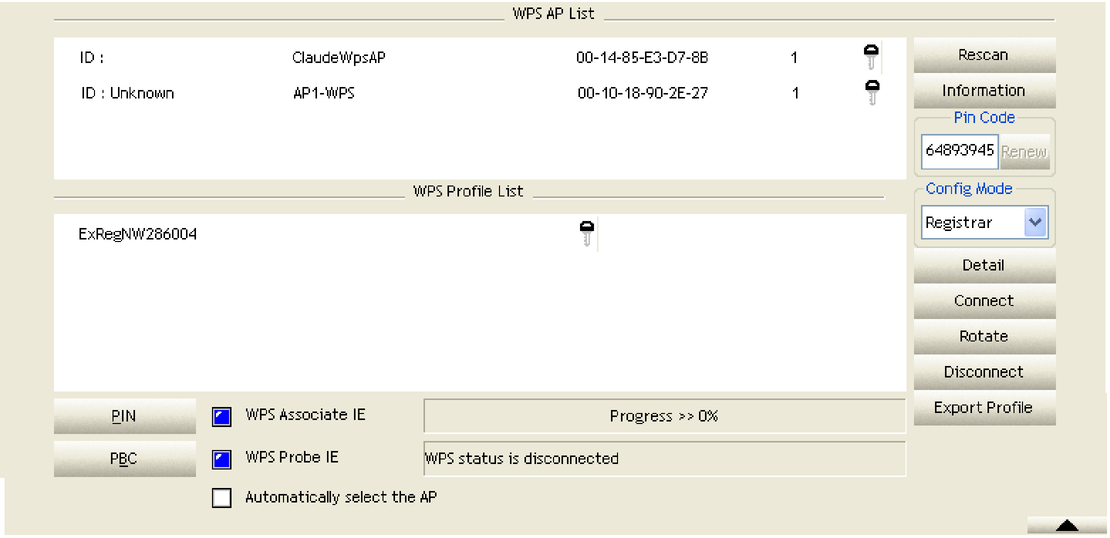
STA would regard these two APs as two different APs and wait until only one PBC AP is available.

4.2.7.5 Example to Configure a Network/AP using PIN or PBC Method


Push PBC button on both Registrar and Enrollee
Credentials exchanged using EAP
AP Enrollee
STA Registrar


User types AP PIN into external Registrar
Credentials exchanged using EAP
AP Enrollee
STA Registrar

1. Select Registrar from the Config Mode drop-down list.



WPS AP List

ID :	ClaudeWpsAP	00-14-85-E3-D7-8B	1	
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	

WPS Profile List

ExRegNW286004

Pin Code: 64893945

Config Mode: Registrar

☑ WPS Associate IE

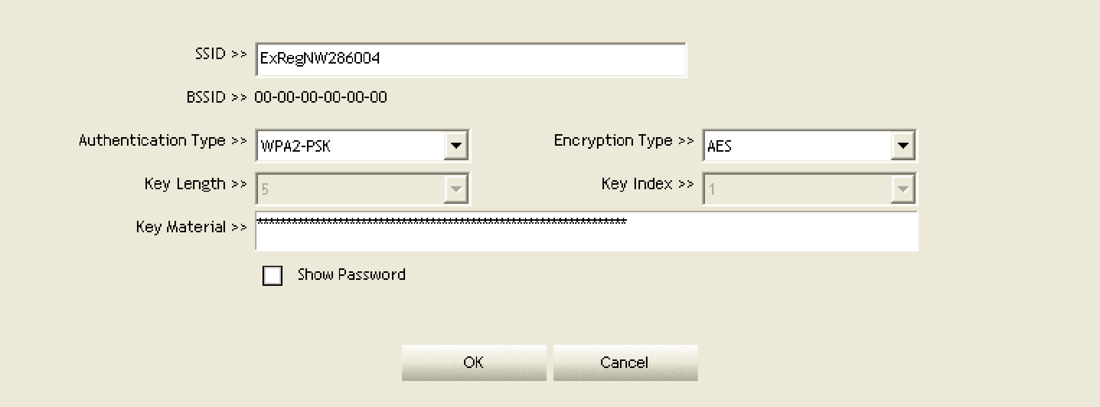
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

2. Enter the details of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if needed.



SSID >> ExRegNW286004

BSSID >> 00-00-00-00-00-00

Authentication Type >> WPA2-PSK

Encryption Type >> AES

Key Length >> 5

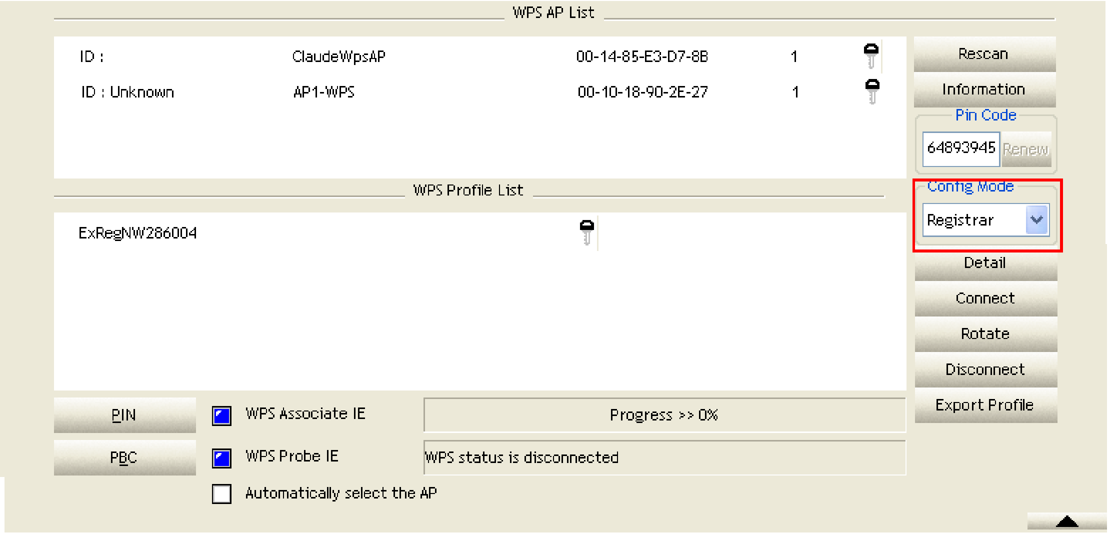
Key Index >> 1

Key Material >> **

□ Show Password

3. If the PIN configuration is setup, enter the PIN sent from the Enrollee.

Start



WPS AP List

ID :	ClaudeWpsAP	00-14-85-E3-D7-8B	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

ExRegNW286004

Pin Code: 64893945

Config Mode: Registrar

☑ WPS Associate IE

☑ WPS Probe IE

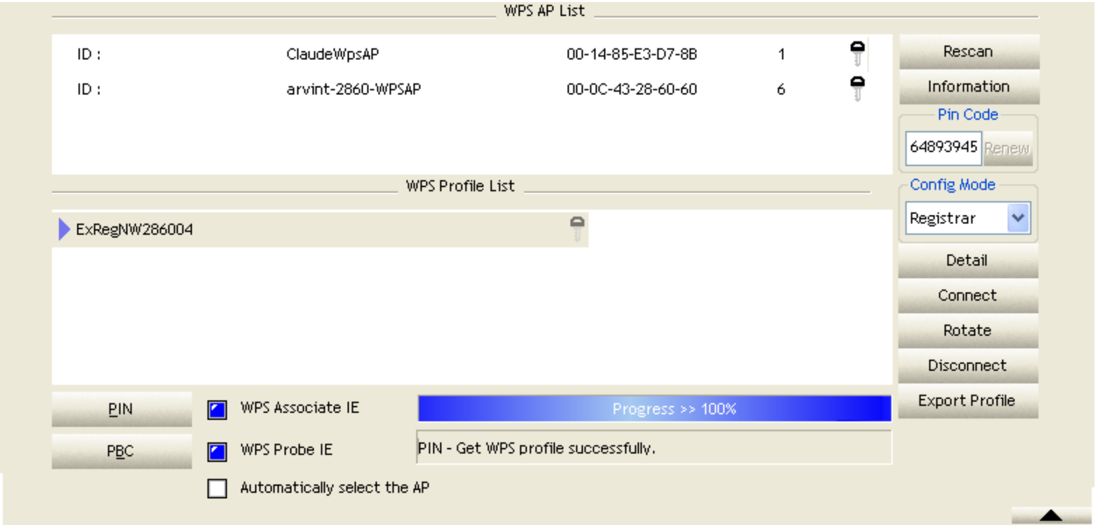
Progress >> 0%

WPS status is disconnected

□ Automatically select the AP

4. Start PIN or PBC. The following procedures are as similar as section 2-7-3 (PIN Enrollee Setup) or section 2-7-4(PBC Enrollee Setup),

5. If your AP Enrollee has been configured before the WPS process, the credential you set in advance will be updated to the AP itself. Otherwise, after a successful registration, the AP Enrollee will be re-configured with the new parameters, and the STA Registrar will connect to the AP Enrollee with these new parameters.



WPS AP List

ID :	ClaudeWpsAP	00-14-85-E3-D7-8B	1
ID :	arvint-2860-WPSAP	00-0C-43-28-60-60	6

Pin Code: 64893945

Config Mode: Registrar

WPS Profile List

ExRegNW286004

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

Describe "WPS Status Bar" - "PIN - xxx" as follow:

A successful PIN Configuration:

Start PIN connection - SSID -> Begin associating to WPS AP
-> Associated to WPS AP -> Sending EAPOL-Start
-> Sending EAP-Rsp (ID) -> Receive M1 ->Sending M2
-> Receive M3 -> Sending M4 -> Receive M5 -> Sending M6
->Receive M7 -> Sending M8 -> Receive EAP Rsp (Done)
-> Sending EAP Rsp(ACK) -> Configured
-> WPS status is disconnected
-> WPS status is connected successfully-SSID

Describe "WPS Status Bar" - "PBC - xxx" as follow:

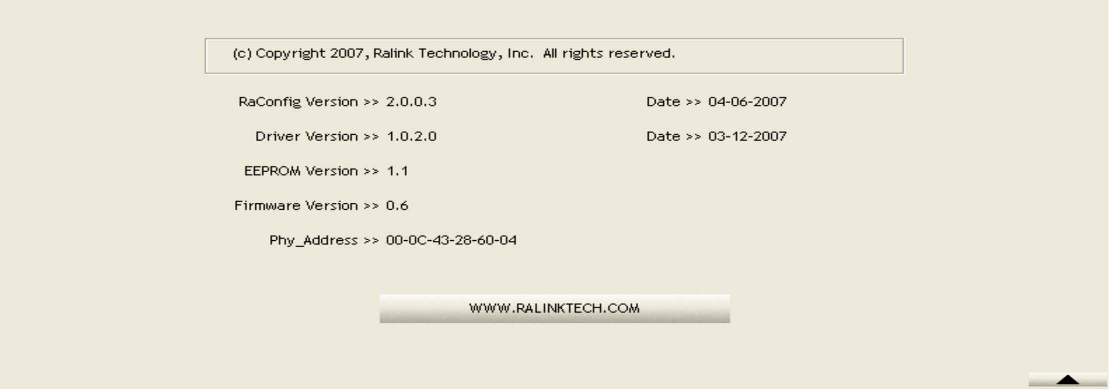
A successful PBC Configuration:

Start PBC connection -> Scanning AP ->
Begin associating to WPS AP ->Associated to WPS AP
-> Sending EAPOL-Start -> Sending EAP-Rsp (ID) ->Receive M1
-> Sending M2 -> Receive M3 -> Sending M4 -> Receive M5
->Sending M6 -> Receive M7 -> Sending M8 ->
Receive EAP Rsp (Done) ->Sending EAP Rsp (ACK) -> Configured -> WPS status is disconnected -> WPS tatus is connected uccessfully-SSID

4.2.8 About

4.2.8.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-8.



(c) Copyright 2007, Ralink Technology, Inc. All rights reserved.

```
RaConfig Version >> 2.0.0.3          Date >> 04-06-2007
  Driver Version >> 1.0.2.0          Date >> 03-12-2007
  EEPROM Version >> 1.1
Firmware Version >> 0.6
     Phy_Address >> 00-0C-43-28-60-04
```

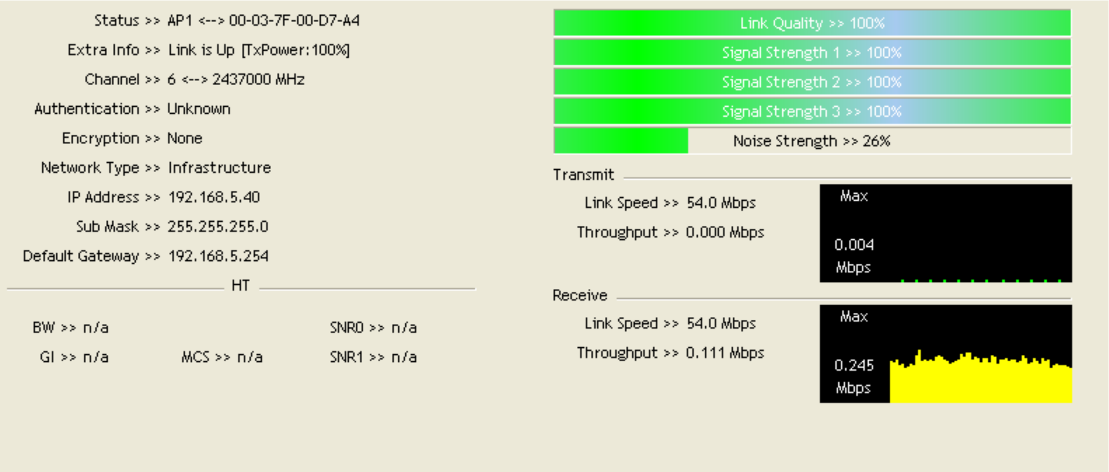
Figure 2-8 about function

1. Connect to Ralink's website: Ralink Technology, Corp.
2. Display Configuration Utility, Driver, and EEPROM version information.
3. Display Wireless NIC MAC address.

4.2.9 Link Status

4.2.9.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-9.



Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.40
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 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

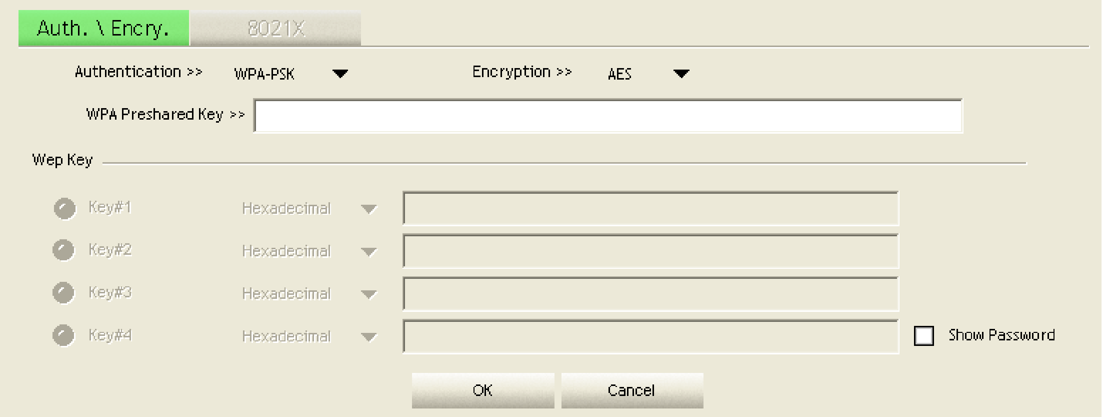
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.111 Mbps

Figure 2-9 Link Status function.

1. Status: Current connection status. If no connection, it will show Disconnected. Otherwise, the SSID and BSSID will show here.
2. Extra Info: Display link status in use.
3. Channel: Display current channel in use.
4. Authentication: Authentication mode in use.
5. Encryption: Encryption type in use.
6. Network Type: Network type in use.
7. IP Address: IP address about current connection.
5. Sub Mask: Sub mask about current connection.
9. Default Gateway: Default gateway about current connection.
10. Link Speed: Show current transmit rate and receive rate.
11. Throughout: Display transmits and receive throughput in unit of Mbps.
12. Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.
13. Signal Strength 1~3: Receive signal strength 1~3, user can choose to display as percentage or dBm format.
14. Noise Strength: Display noise signal strength.
15. HT: Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value. (Show the information only for 802.11n wireless card.)

4.3 Security

4.3.1 Auth / Encry.Setting-WEP/TKIP/AES



Auth. \ Encry. | 8021X

Authentication >> WPA-PSK

Encryption >> AES

WPA Preshared Key >>

Wep Key

○ Key#1 Hexadecimal

○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

□ Show Password

OK | Cancel

Figure 3-1 Auth.\Encry. Settings

1. Authentication Type: There are 7 authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

2. Encryption Type: For open and shared authentication mode, the available encryption types are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

3. 8021X: This is introduced in the topic of Section 3-2.

4. WPA Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

5. WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.

a. Hexadecimal - 40bits: 10 Hex characters.

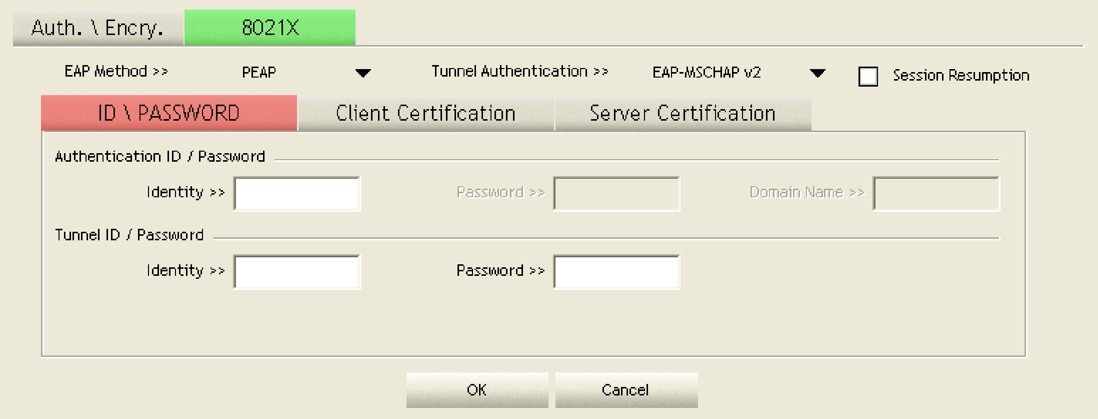
b. Hexadecimal - 128bits: 32Hex characters.

c. ASCII - 40bits: 5 ASCII characters.

d. ASCII - 128bits: 13 ASCII characters

4.3.2 802.1x Setting

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

Authentication type:

1. PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
2. TLS/Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
3. TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
4. EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.
5. LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
6. MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

Session Resumption: The user can choose "Disable" and "Enable".

Tunnel Authentication:

a. Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAPTLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2","PAP" and "EAP-MD5".

b. Tunnel Identity: Identity for tunnel.

c. Tunnel Password: Password for tunnel.

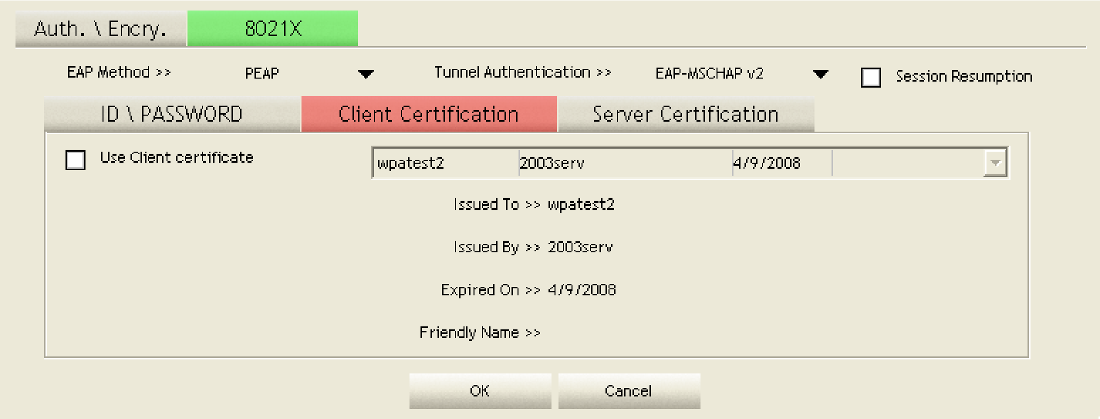
ID \ PASSWORD

1. Authentication ID/Password: The identity, password and domain name for server.

Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.

2. Tunnel ID/Password: Identity and Password for the server

Client Certification



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

□ Use Client certificate

wpatest2 2003serv 4/9/2008

Issued To >> wpatest2

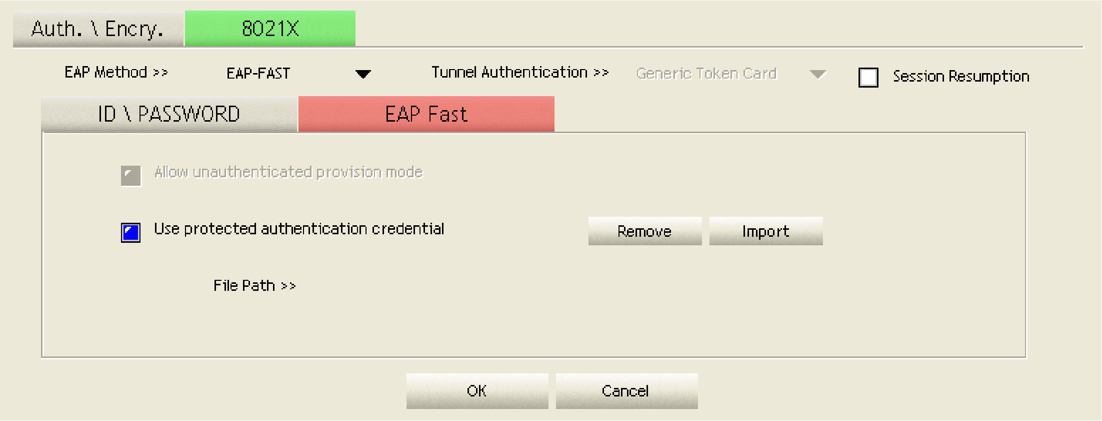
Issued By >> 2003serv

Expired On >> 4/9/2008

Friendly Name >>

Use Client certificate: Client certificate for server authentication.

EAP Fast



Auth. \ Encry. | 8021X

EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card

□ Session Resumption

ID \ PASSWORD | EAP Fast

☑ Allow unauthenticated provision mode

☑ Use protected authentication credential

File Path >>

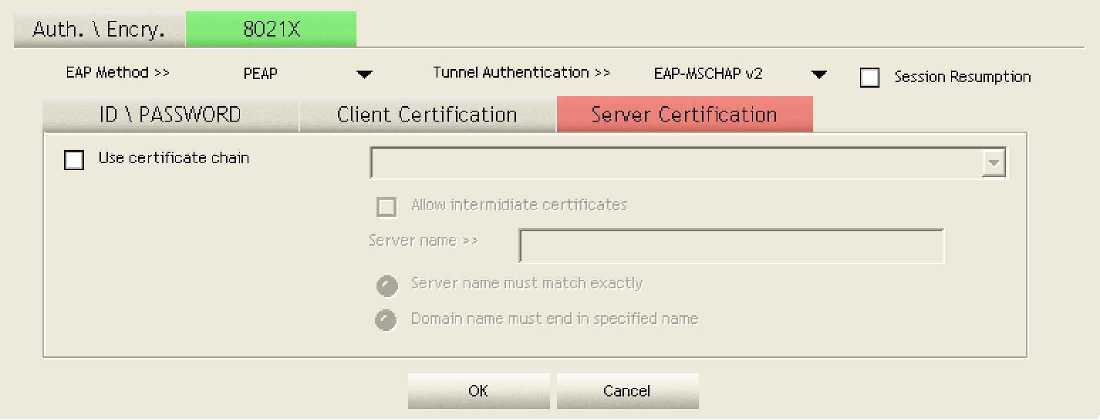
1. Allow unauthenticated provision mode: During the PAC can be provisioned (distributed one time) to the client automatically.

It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now.

It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.

2. Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method

Server Certification



Auth. \ Encry. | 8021X

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

ID \ PASSWORD | Client Certification | Server Certification

□ Use certificate chain

□ Allow intermidiate certificates

Server name >>

○ Server name must match exactly

○ Domain name must end in specified name

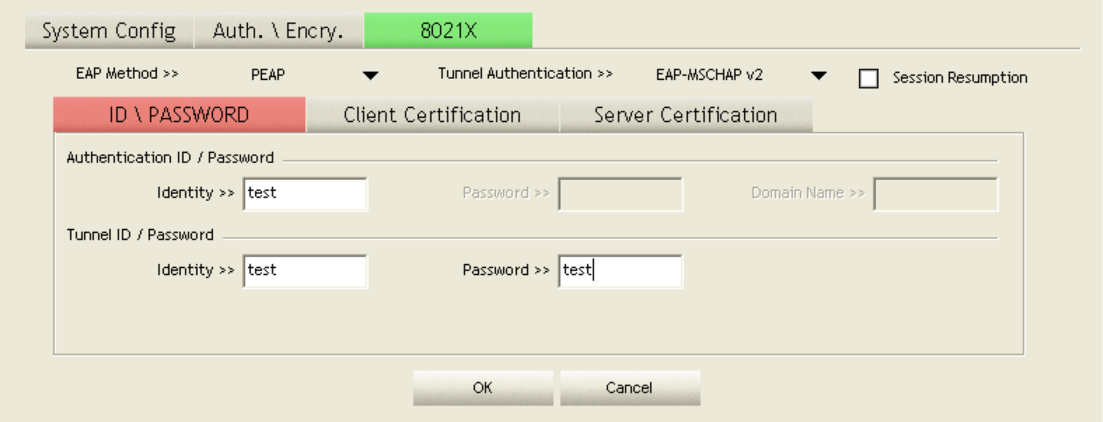
1. Certificate issuer: Select the server that issues the certificate.
2. Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.
3. Server name: Enter an authentication sever root.

4.3.3 Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection is failed in Profile

There are two situations where a user is able to reconnect an 802.1x authenticated connection and authenticate successfully after an 802.1x authenticated connection has failed on the profile page. They are as follows:

When keying in an identity, password or domain name error:

1. Authentication type chooses "PEAP", key identity into test. Tunnel Protocol is "EAP-MSCHAP-v2, the tunnel identity and tunnel password are tested. Those settings are the same as our intended AP's setting.

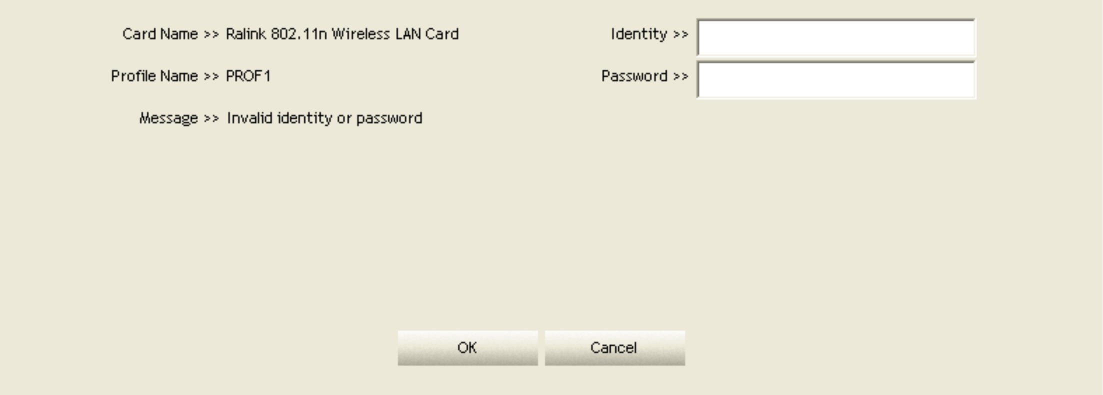


EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
□ Session Resumption

Authentication ID / Password
Identity >> test
Password >>
Domain Name >>

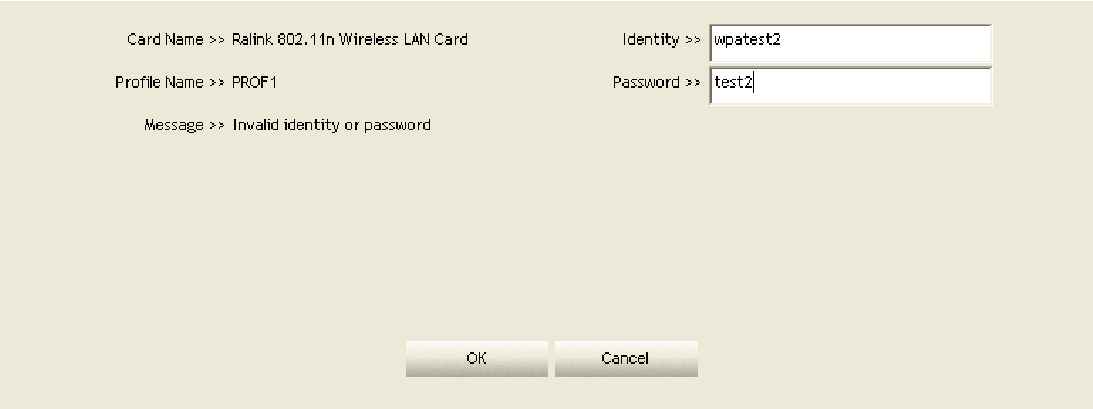
Tunnel ID / Password
Identity >> test
Password >> test

2. Because of keying identity and password errors, the result will appear as in the image below.



Card Name >> Ralink 802.11n Wireless LAN Card
Profile Name >> PROF1
Message >> Invalid identity or password
Identity >>
Password >>

3. If you want to disconnect, click "Cancel" on the Authentication Failure dialog box. If you want to reconnect, key the identity into wpatest2. The tunnel identity is wpatest2 and the tunnel password is test2. Those setting are the same as our intended AP's setting.



Card Name >> Ralink 802.11n Wireless LAN Card

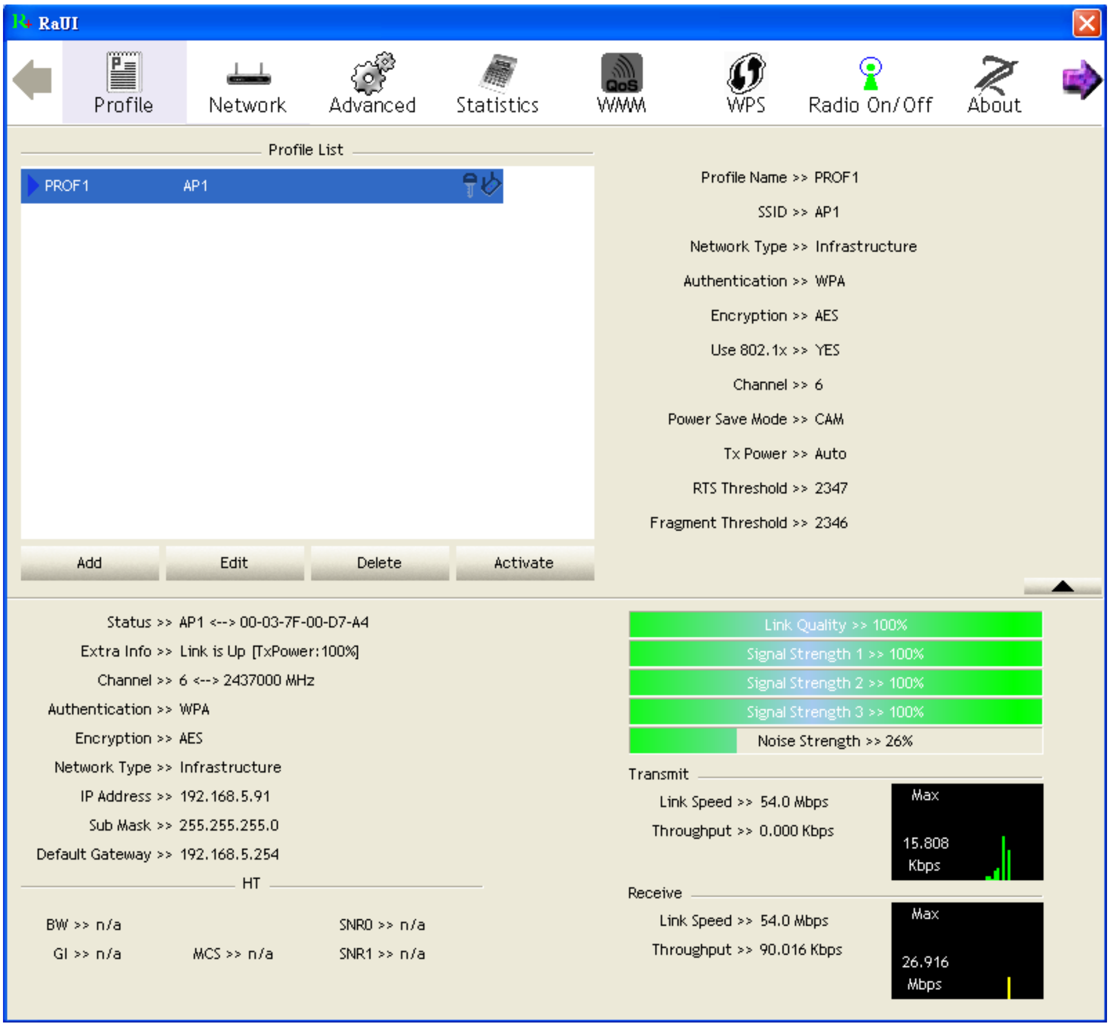
Profile Name >> PROF1

Message >> Invalid identity or password

Identity >> wpatest2

Password >> test2

4. Click "OK". If it worked perfectly and the result will appear as the image below.



PROF1 AP1

Profile Name >> PROF1

SSID >> AP1

Network Type >> Infrastructure

Authentication >> WPA

Encryption >> AES

Use 802.1x >> YES

Channel >> 6

Power Save Mode >> CAM

Tx Power >> Auto

RTS Threshold >> 2347

Fragment Threshold >> 2346

Status >> AP1 <--> 00-03-7F-00-D7-A4

Extra Info >> Link is Up [TxPower:100%]

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.5.91

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

15.808 Kbps

Receive

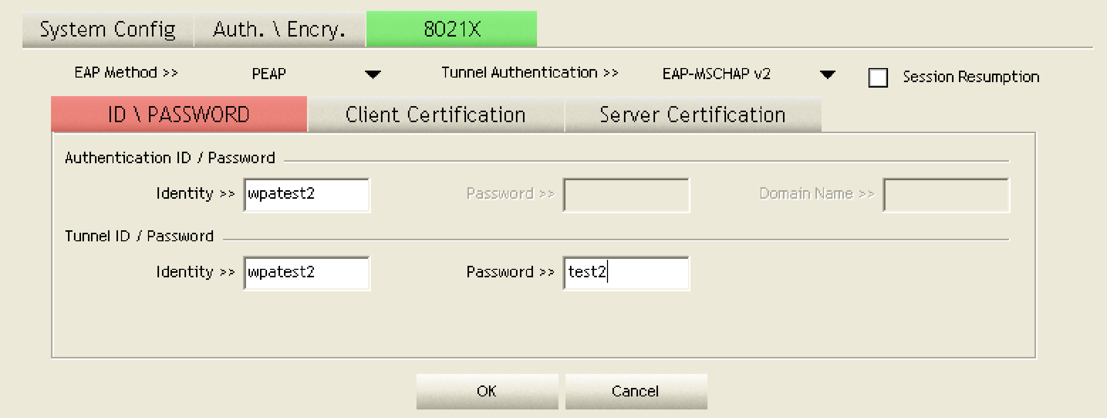
Link Speed >> 54.0 Mbps

Throughput >> 90.016 Kbps

26.916 Mbps

When a "Timeout" occurs;

1. Choose "PEAP" as the Authentication type and key-in "wpatest2" as the identity .Tunnel Protocol is "EAP-MSCHAP-v2, and the tunnel identity is "wpatest2". The tunnel password is "test2". These settings are the same as our intended AP's setting.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

Authentication ID / Password

Identity >> wpatest2

Password >>

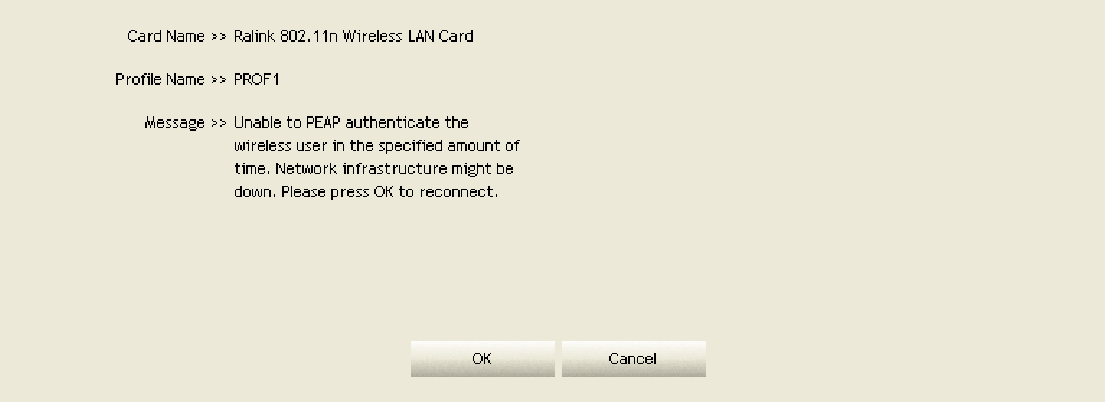
Domain Name >>

Tunnel ID / Password

Identity >> wpatest2

Password >> test2

2. When a "Timeout" occurs, The following dialog box will be displayed;

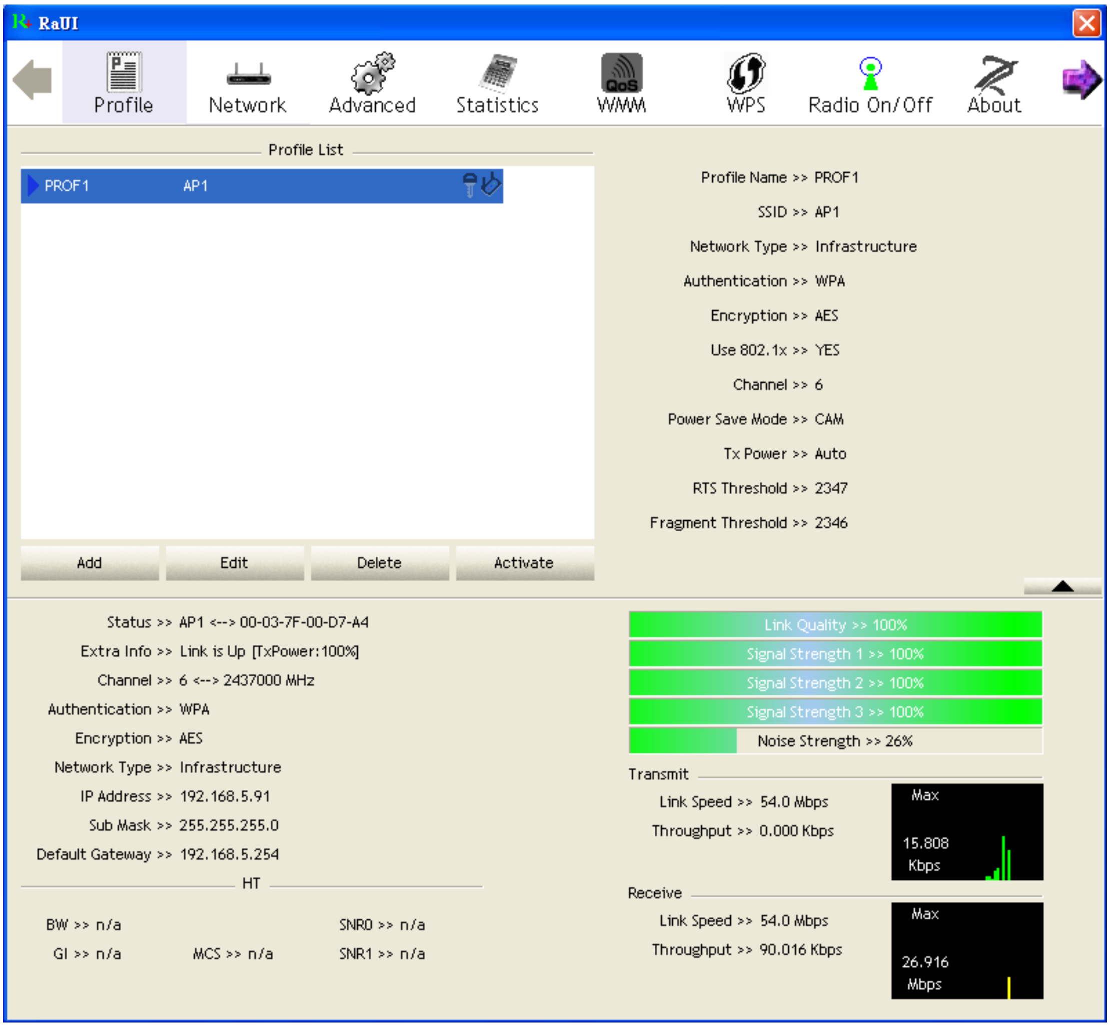


Card Name >> Ralink 802.11n Wireless LAN Card

Profile Name >> PROF1

Message >> Unable to PEAP authenticate the wireless user in the specified amount of time. Network infrastructure might be down. Please press OK to reconnect.

3. If it has connected successfully, the dialog box will appear as follows;



PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> WPA
Encryption >> AES
Use 802.1x >> YES
Channel >> 6
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.5.91
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

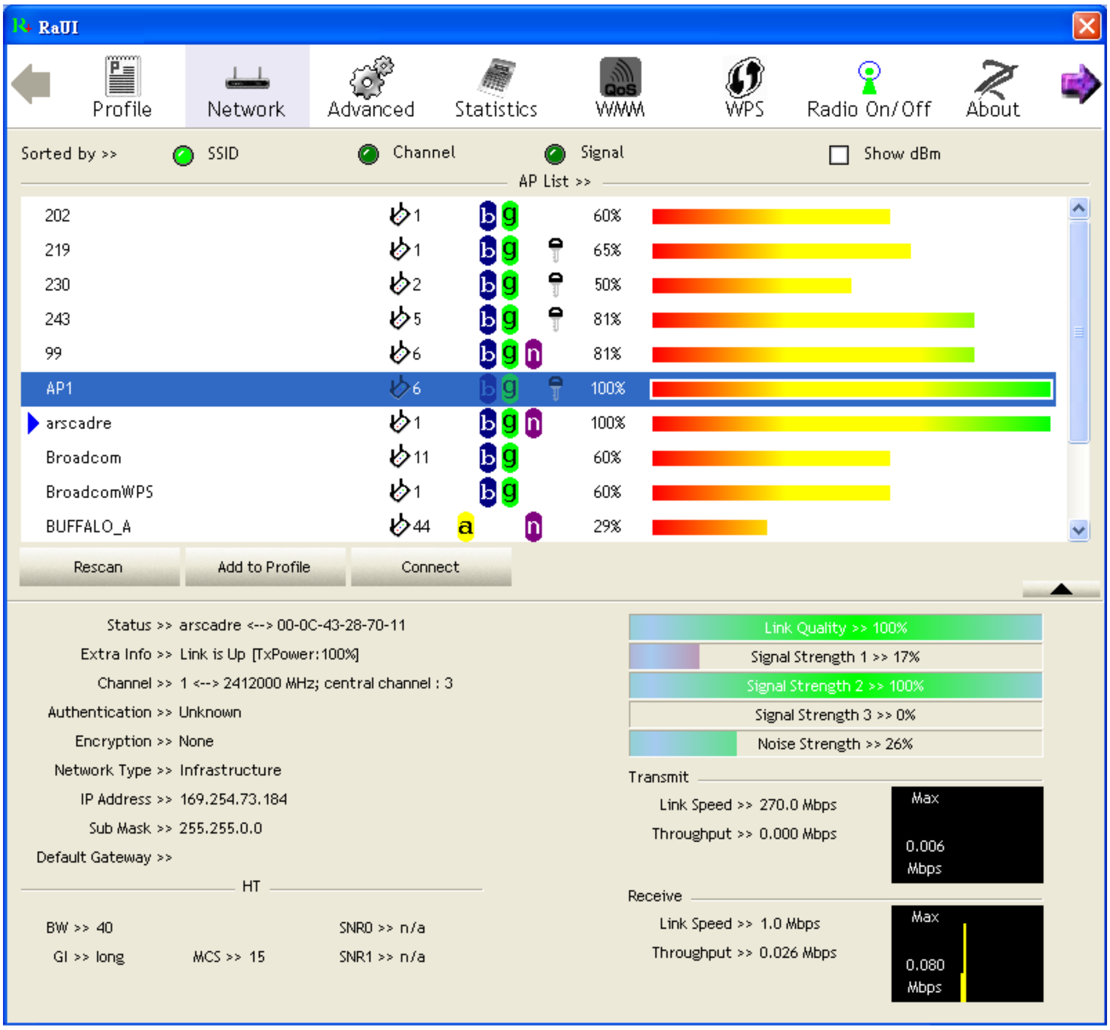
Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps
Max 15.808 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 90.016 Kbps
Max 26.916 Mbps

4.3.4 Example to Configure with WEP on

1. Select an AP with WEP encryption and click "Connect".



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

SSID	Channel			Signal
202	1	b g		60%
219	1	b g	🔑	65%
230	2	b g	🔑	50%
243	5	b g	🔑	81%
99	6	b g n		81%
AP1	6	b g	🔑	100%
arscadre	1	b g n		100%
Broadcom	11	b g		60%
BroadcomWPS	1	b g		60%
BUFFALO_A	44	a n		29%

Status >> arscadre <--> 00-0C-43-28-70-11
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412000 MHz; central channel : 3
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 169.254.73.184
Sub Mask >> 255.255.0.0
Default Gateway >>

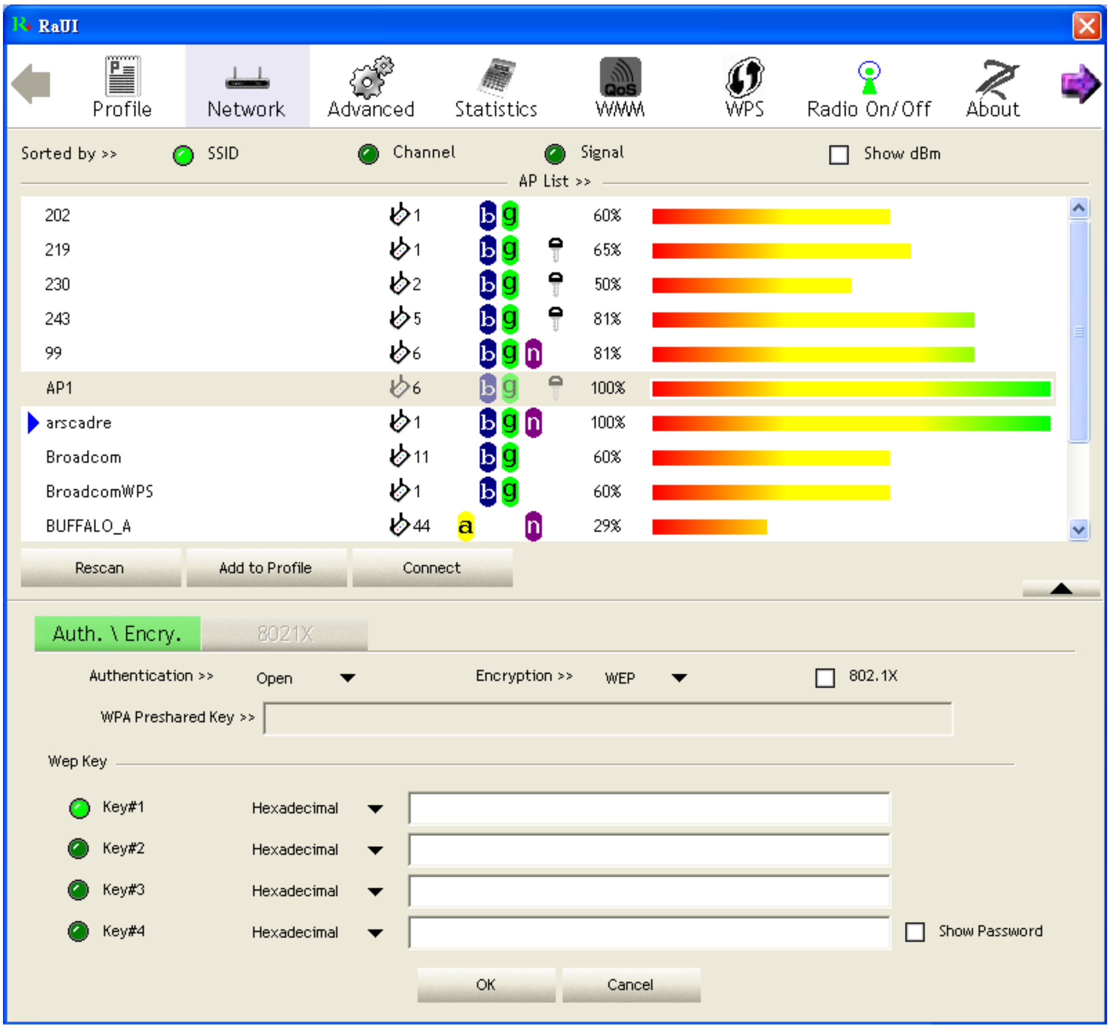
HT
BW >> 40
GI >> long MCS >> 15
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 17%
Signal Strength 2 >> 100%
Signal Strength 3 >> 0%
Noise Strength >> 26%

Transmit
Link Speed >> 270.0 Mbps
Throughput >> 0.000 Mbps
Max
0.006 Mbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 0.026 Mbps
Max
0.080 Mbps

2. The Auth.\Encry. function will appear as below



SSID	Channel		Signal
202	1	b g	60%
219	1	b g	65%
230	2	b g	50%
243	5	b g	81%
99	6	b g n	81%
AP1	6	b g	100%
arscadre	1	b g n	100%
Broadcom	11	b g	60%
BroadcomWPS	1	b g	60%
BUFFALO_A	44	a n	29%

Authentication >> Open

Encryption >> WEP

□ 802.1X

WPA Preshared Key >>

Wep Key

● Key#1 Hexadecimal

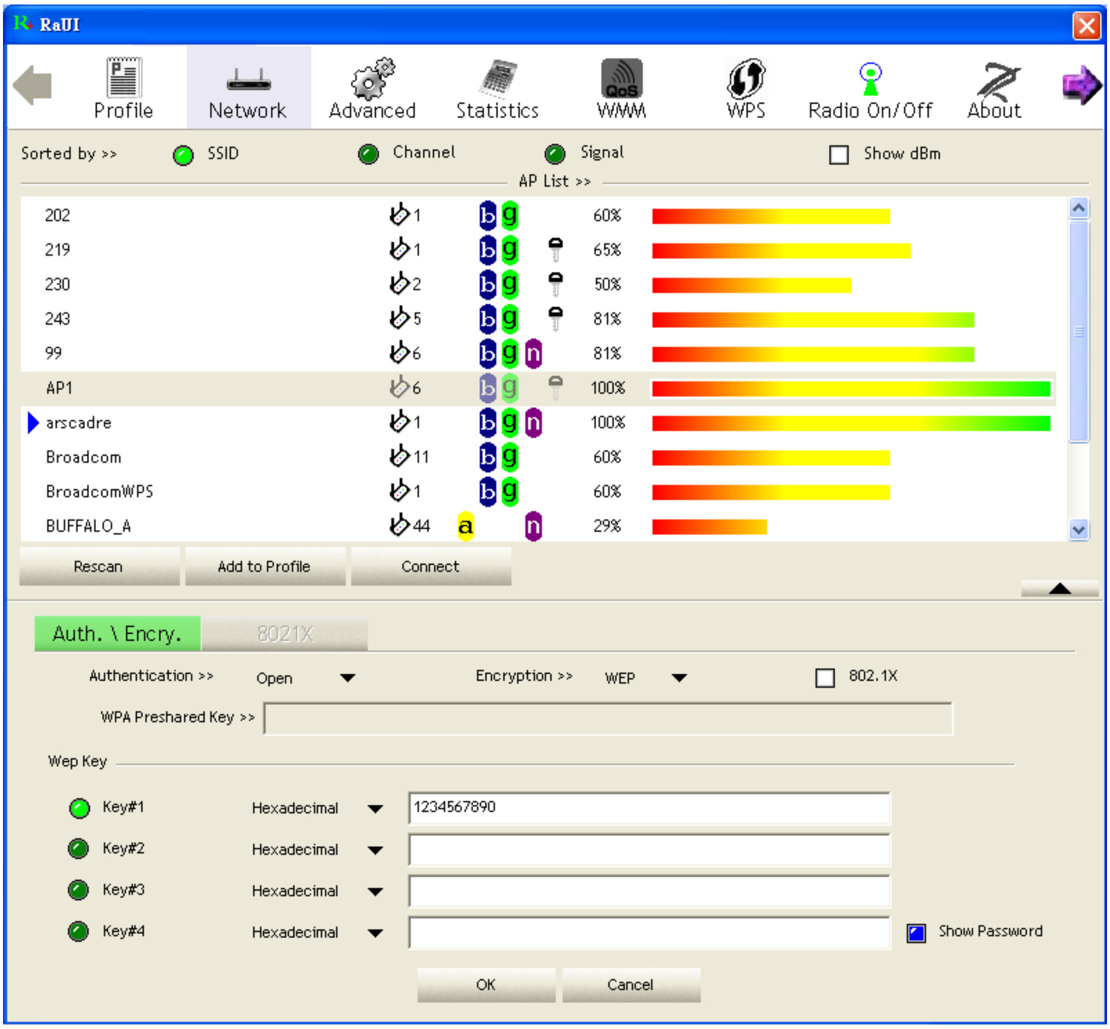
○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

□ Show Password

3. Enter 1234567890 in the Key#1 Hexadecimal field. This value is same as our intended AP's setting.

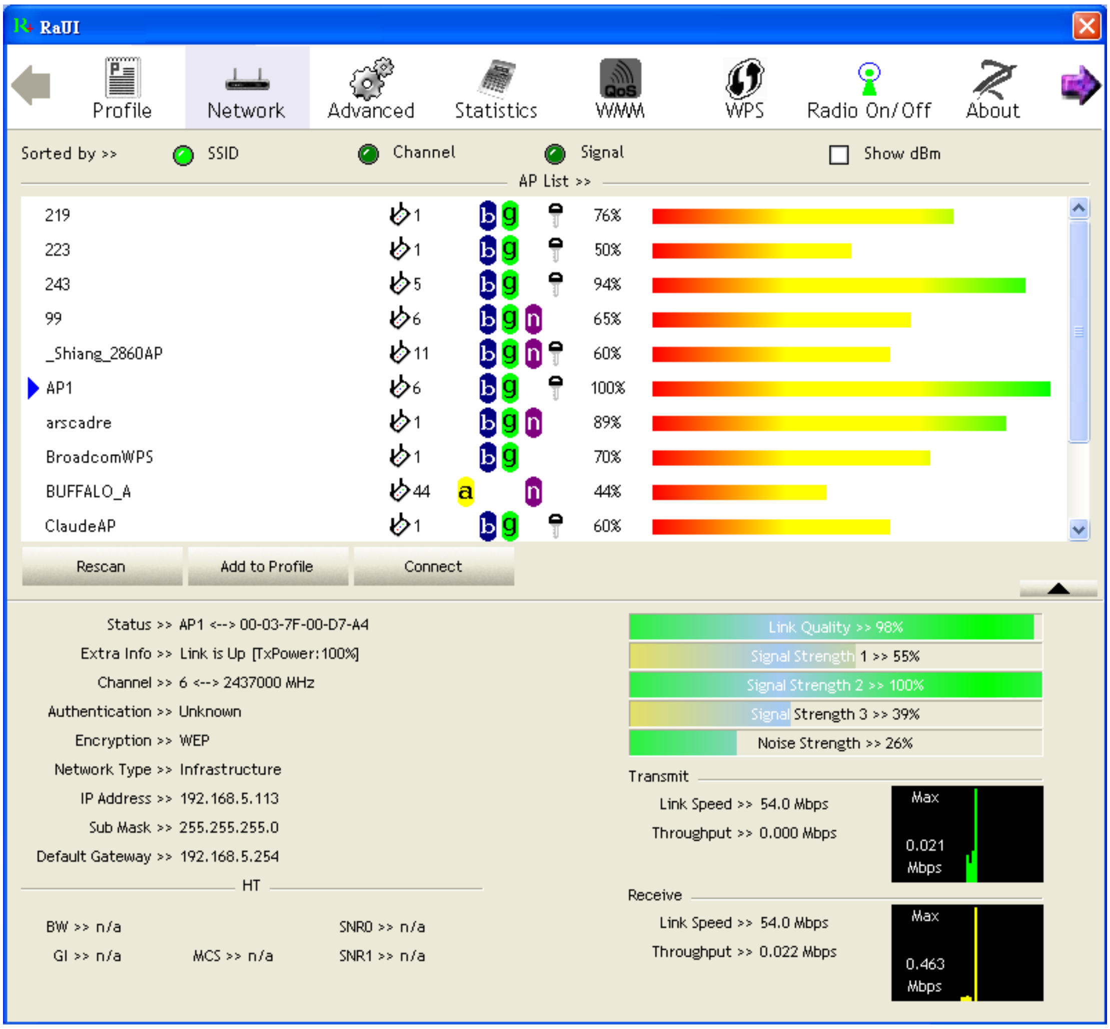


202	1	b g		60%
219	1	b g	🔑	65%
230	2	b g	🔑	50%
243	5	b g	🔑	81%
99	6	b g n		81%
AP1	6	b g	🔑	100%
arscadre	1	b g n		100%
Broadcom	11	b g		60%
BroadcomWPS	1	b g		60%
BUFFALO_A	44	a n		29%

Authentication >> Open
Encryption >> WEP
□ 802.1X
WPA Preshared Key >>

Wep Key
● Key#1 Hexadecimal 1234567890
○ Key#2 Hexadecimal
○ Key#3 Hexadecimal
○ Key#4 Hexadecimal
☑ Show Password

4. Click "OK". The dialog box will appear as below;



219	1	b g	🔑	76%
223	1	b g	🔑	50%
243	5	b g	🔑	94%
99	6	b g n		65%
_Shiang_2860AP	11	b g n	🔑	60%
AP1	6	b g	🔑	100%
arscadre	1	b g n		89%
BroadcomWPS	1	b g		70%
BUFFALO_A	44	a n		44%
ClaudeAP	1	b g	🔑	60%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> WEP
Network Type >> Infrastructure
IP Address >> 192.168.5.113
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 >> 98%
Signal Strength 1 >> 55%
Signal Strength 2 >> 100%
Signal Strength 3 >> 39%
Noise Strength >> 26%

Transmit

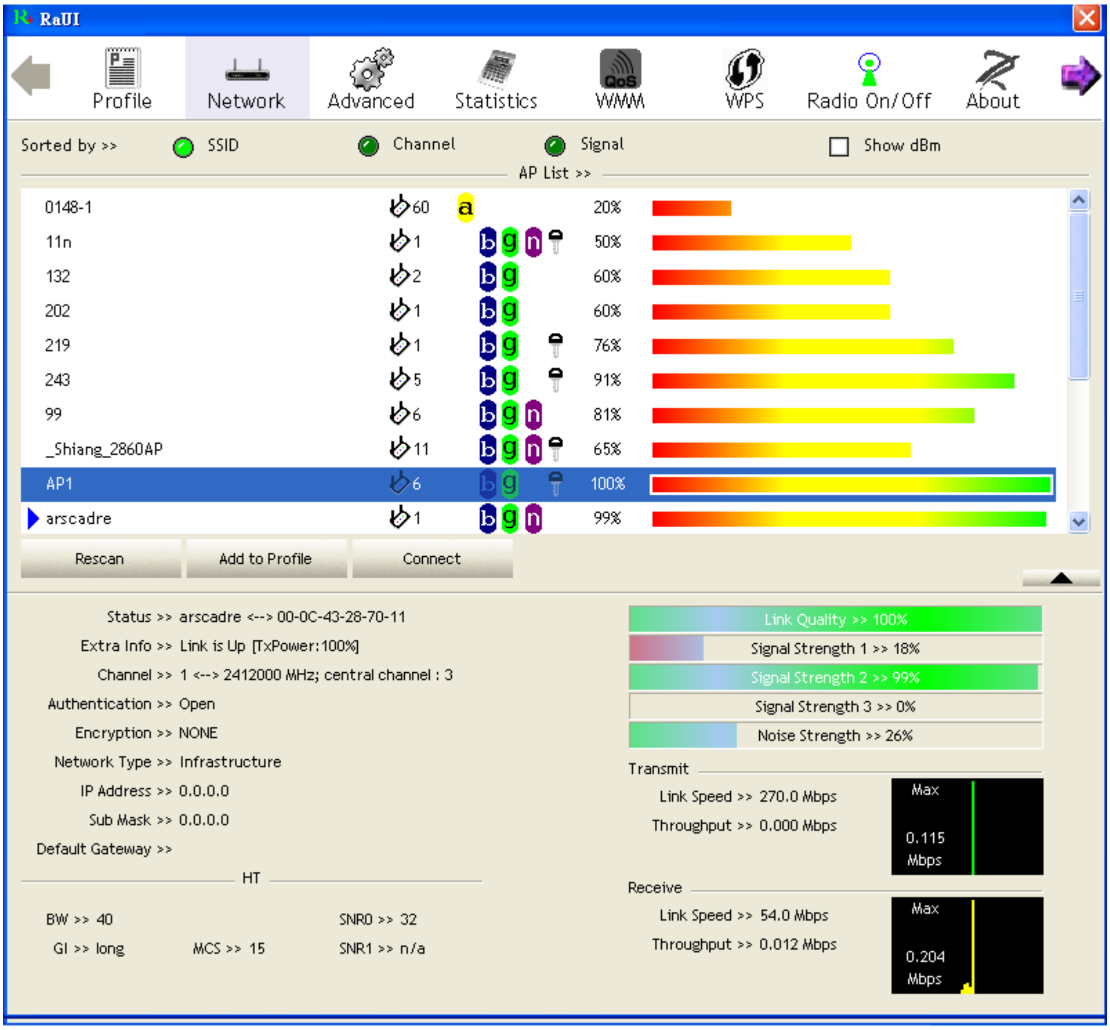
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps
0.021 Mbps

Receive

Link Speed >> 54.0 Mbps
Throughput >> 0.022 Mbps
0.463 Mbps

4.3.5 Example to Configure with WPA-PSK

1. Select the AP with a WPA-PSK authentication mode and click "Connect".



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

0148-1	60	a		20%
11n	1	b g n	🔑	50%
132	2	b g		60%
202	1	b g		60%
219	1	b g	🔑	76%
243	5	b g	🔑	91%
99	6	b g n		81%
_Shiang_2860AP	11	b g n	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n		99%

Status >> arscadre <--> 00-0C-43-28-70-11
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412000 MHz; central channel : 3
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 0.0.0.0
Sub Mask >> 0.0.0.0
Default Gateway >>

HT

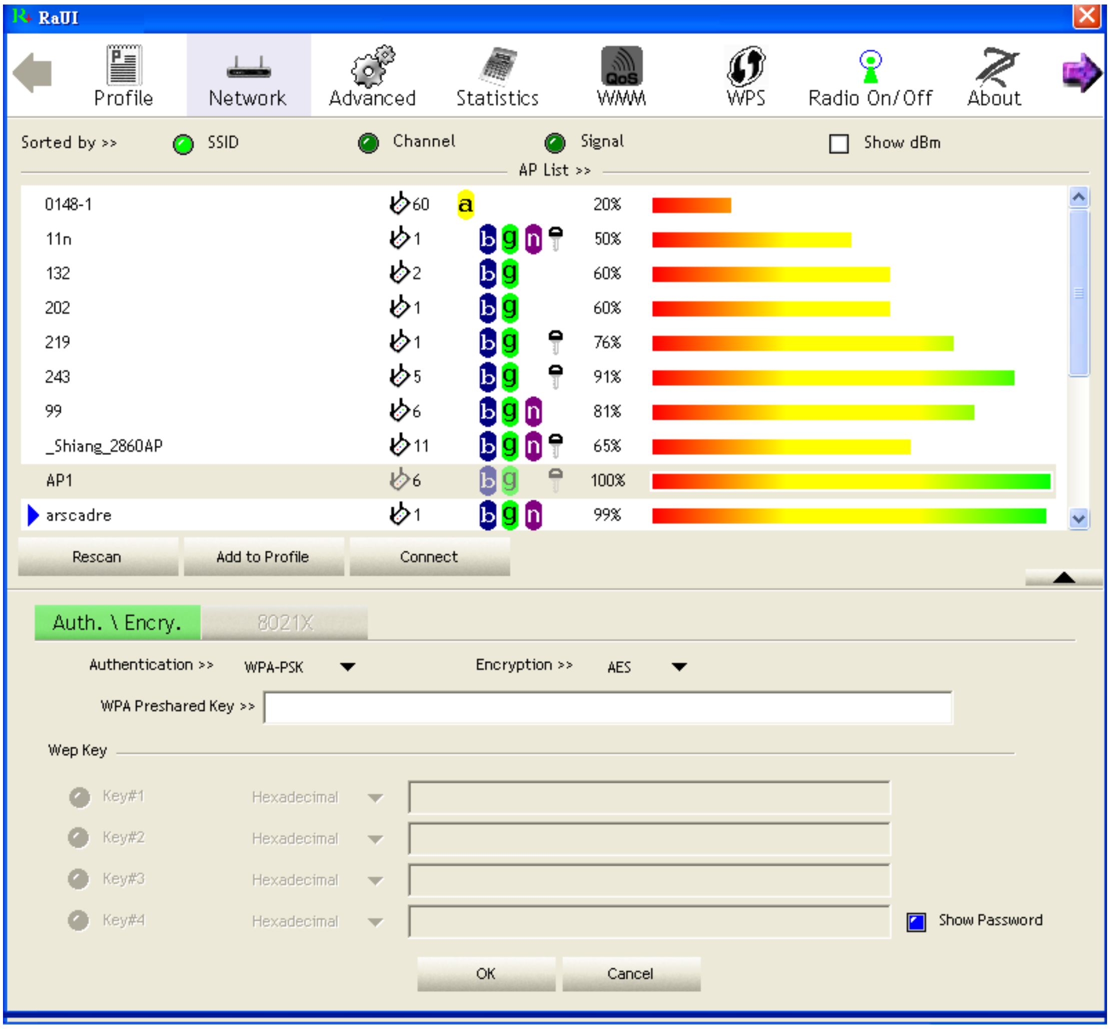
BW >> 40 SNR0 >> 32
GI >> long MCS >> 15 SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 18%
Signal Strength 2 >> 99%
Signal Strength 3 >> 0%
Noise Strength >> 26%

Transmit
Link Speed >> 270.0 Mbps
Throughput >> 0.000 Mbps
Max 0.115 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.012 Mbps
Max 0.204 Mbps

2. Auth.\ Encry. function appears.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

0148-1	60	a		20%
11n	1	b g n	🔑	50%
132	2	b g		60%
202	1	b g		60%
219	1	b g	🔑	76%
243	5	b g	🔑	91%
99	6	b g n		81%
_Shiang_2860AP	11	b g n	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n		99%

Auth. \ Encry. | 8021X

Authentication >> WPA-PSK

Encryption >> AES

WPA Preshared Key >>

Wep Key

○ Key#1 Hexadecimal

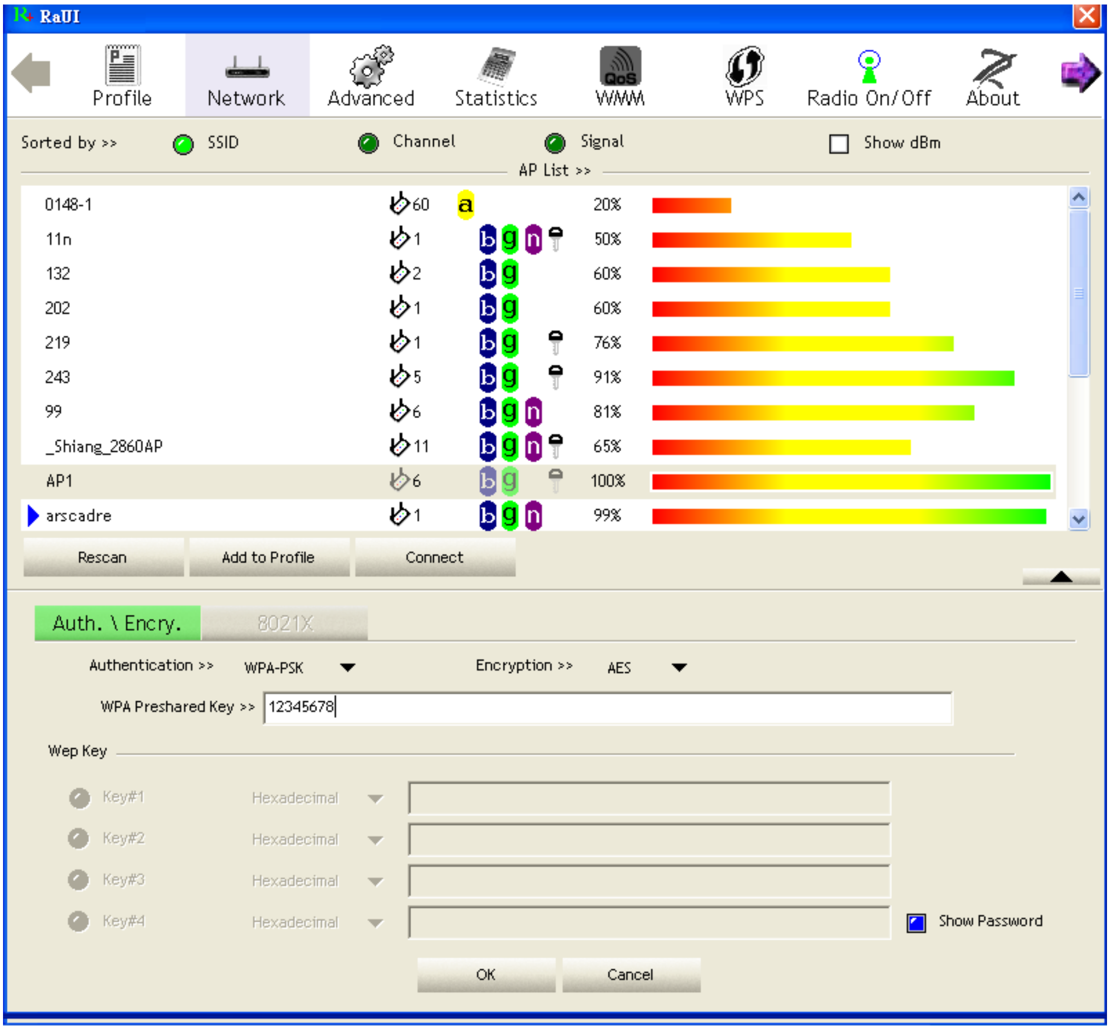
○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

☑ Show Password

3. Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption. Enter the WPA Pre-Shared Key as "12345678".



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

0148-1	60	a	20%
11n	1	b g n 🔑	50%
132	2	b g	60%
202	1	b g	60%
219	1	b g 🔑	76%
243	5	b g 🔑	91%
99	6	b g n	81%
_Shiang_2860AP	11	b g n 🔑	65%
AP1	6	b g 🔑	100%
arscadre	1	b g n	99%

Authentication >> WPA-PSK Encryption >> AES

WPA Preshared Key >> 12345678

Wep Key

○ Key#1 Hexadecimal

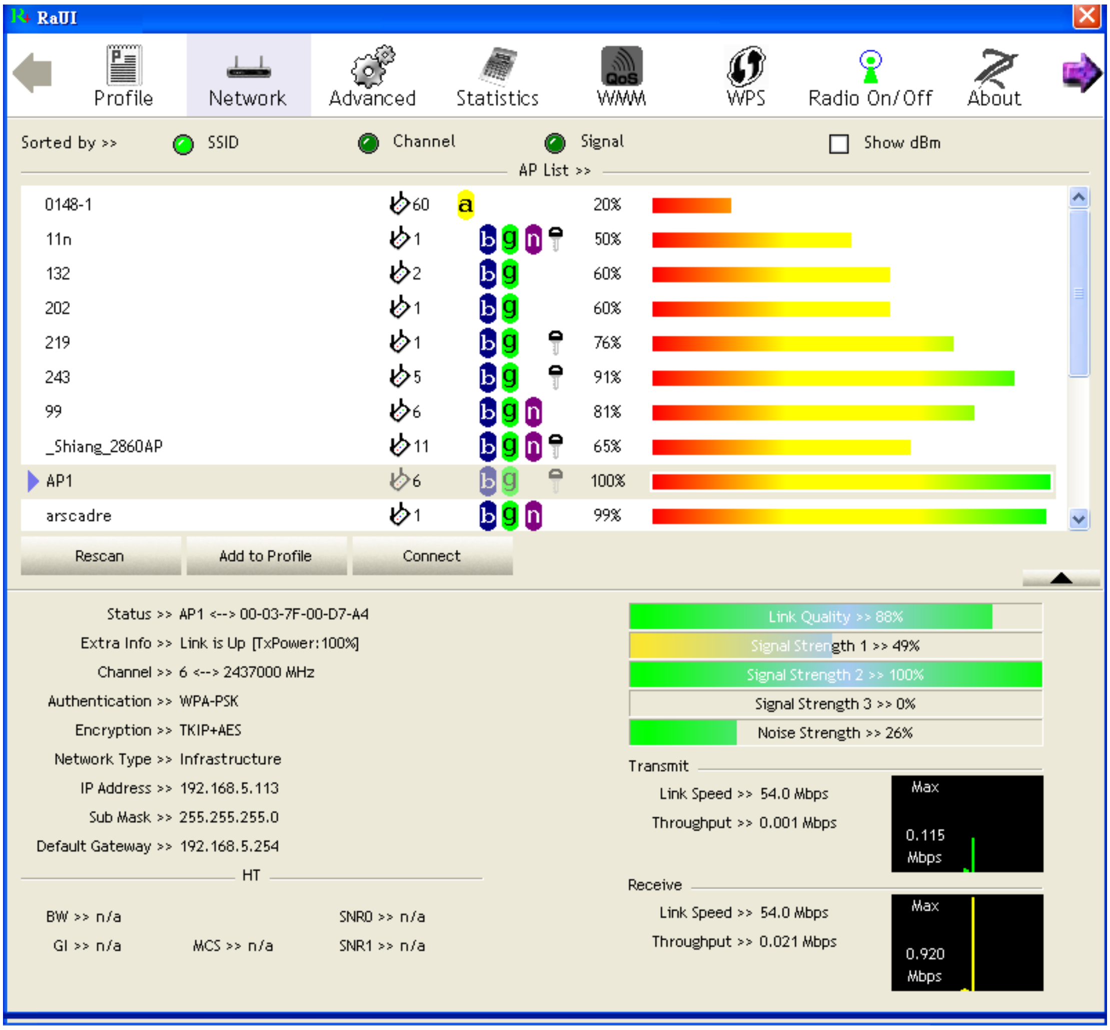
○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

☑ Show Password

4. Click "OK". Be careful, if the WPA Pre-Shared Key entered is not correct, you won’t be able to exchange any data frames, even though the AP can be connected.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

SSID	Channel	Mode		Signal
0148-1	60	a		20%
11n	1	b g n	🔑	50%
132	2	b g		60%
202	1	b g		60%
219	1	b g	🔑	76%
243	5	b g	🔑	91%
99	6	b g n		81%
_Shiang_2860AP	11	b g n	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n		99%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA-PSK
Encryption >> TKIP+AES
Network Type >> Infrastructure
IP Address >> 192.168.5.113
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

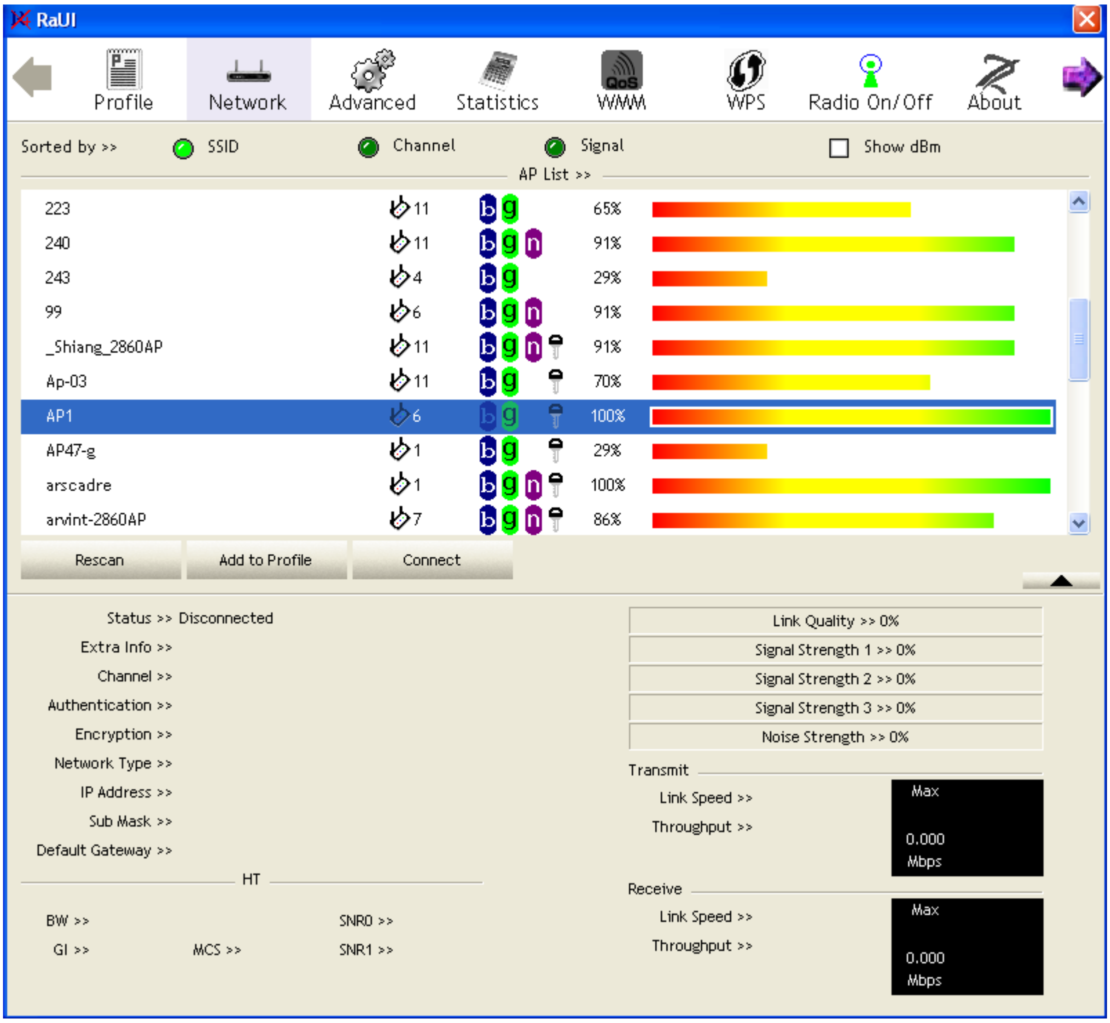
Link Quality >> 88%
Signal Strength 1 >> 49%
Signal Strength 2 >> 100%
Signal Strength 3 >> 0%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.001 Mbps
Max
0.115 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.021 Mbps
Max
0.920 Mbps

4.3.6 Example to Configure with WPA

1. Select an AP with WPA authentication mode and click "Connect".



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

SSID	Channel	Mode	Security	Signal
223	11	b g		65%
240	11	b g n		91%
243	4	b g		29%
99	6	b g n		91%
_Shiang_2860AP	11	b g n	🔑	91%
Ap-03	11	b g	🔑	70%
AP1	6	b g	🔑	100%
AP47-g	1	b g	🔑	29%
arscadre	1	b g n	🔑	100%
arvint-2860AP	7	b g n	🔑	86%

Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

HT

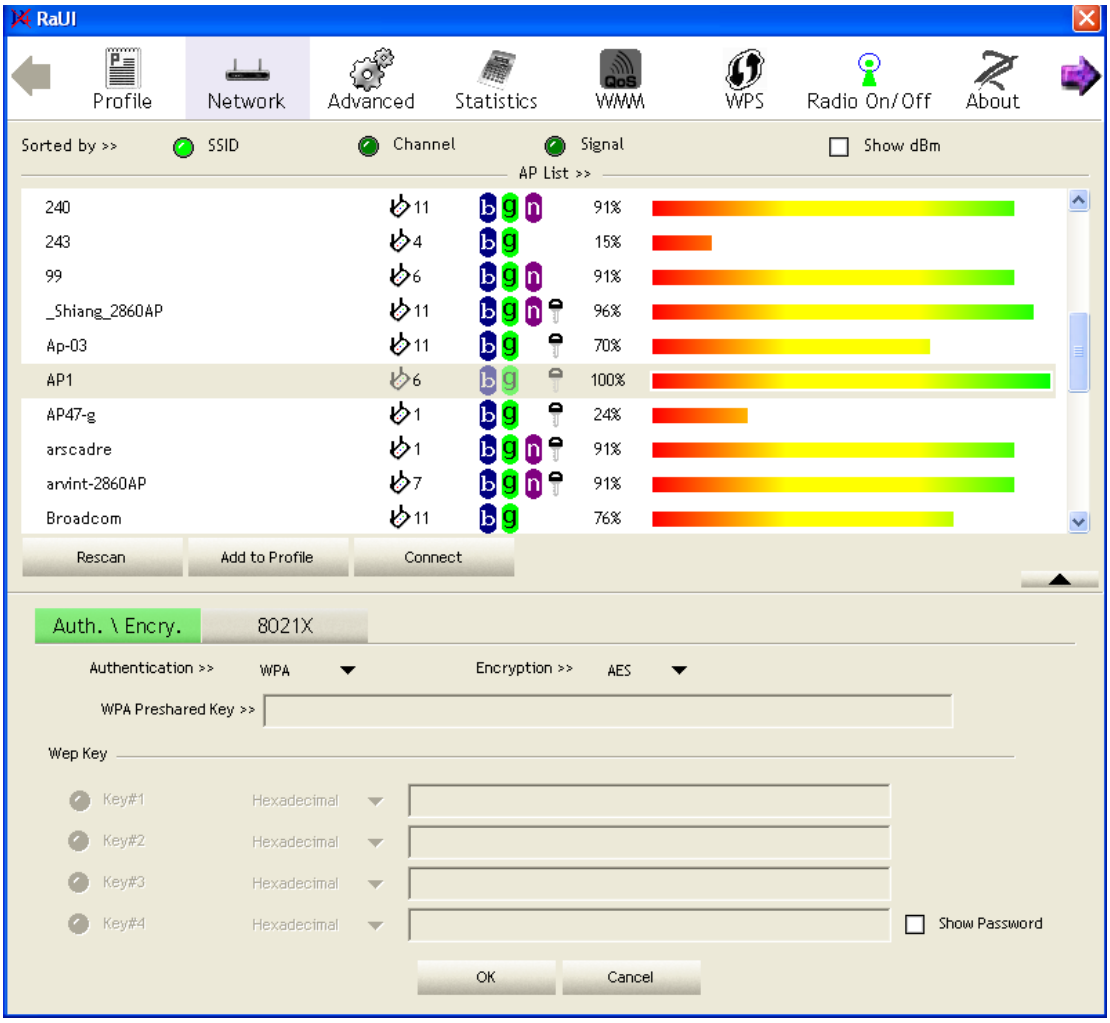
BW >> SNR0 >>
GI >> MCS >> SNR1 >>

Link Quality >> 0%
Signal Strength 1 >> 0%
Signal Strength 2 >> 0%
Signal Strength 3 >> 0%
Noise Strength >> 0%

Transmit
Link Speed >>
Throughput >>
Max
0.000
Mbps

Receive
Link Speed >>
Throughput >>
Max
0.000
Mbps

2. The Auth.\ Encry. Function pop up. (If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)



240	11	b g n		91%
243	4	b g		15%
99	6	b g n		91%
_Shiang_2860AP	11	b g n	🔑	96%
Ap-03	11	b g	🔑	70%
AP1	6	b g	🔑	100%
AP47-g	1	b g	🔑	24%
arscadre	1	b g n	🔑	91%
arvint-2860AP	7	b g n	🔑	91%
Broadcom	11	b g		76%

Auth. \ Encry. | 8021X

Authentication >> WPA

Encryption >> AES

WPA Preshared Key >>

Wep Key

○ Key#1 Hexadecimal

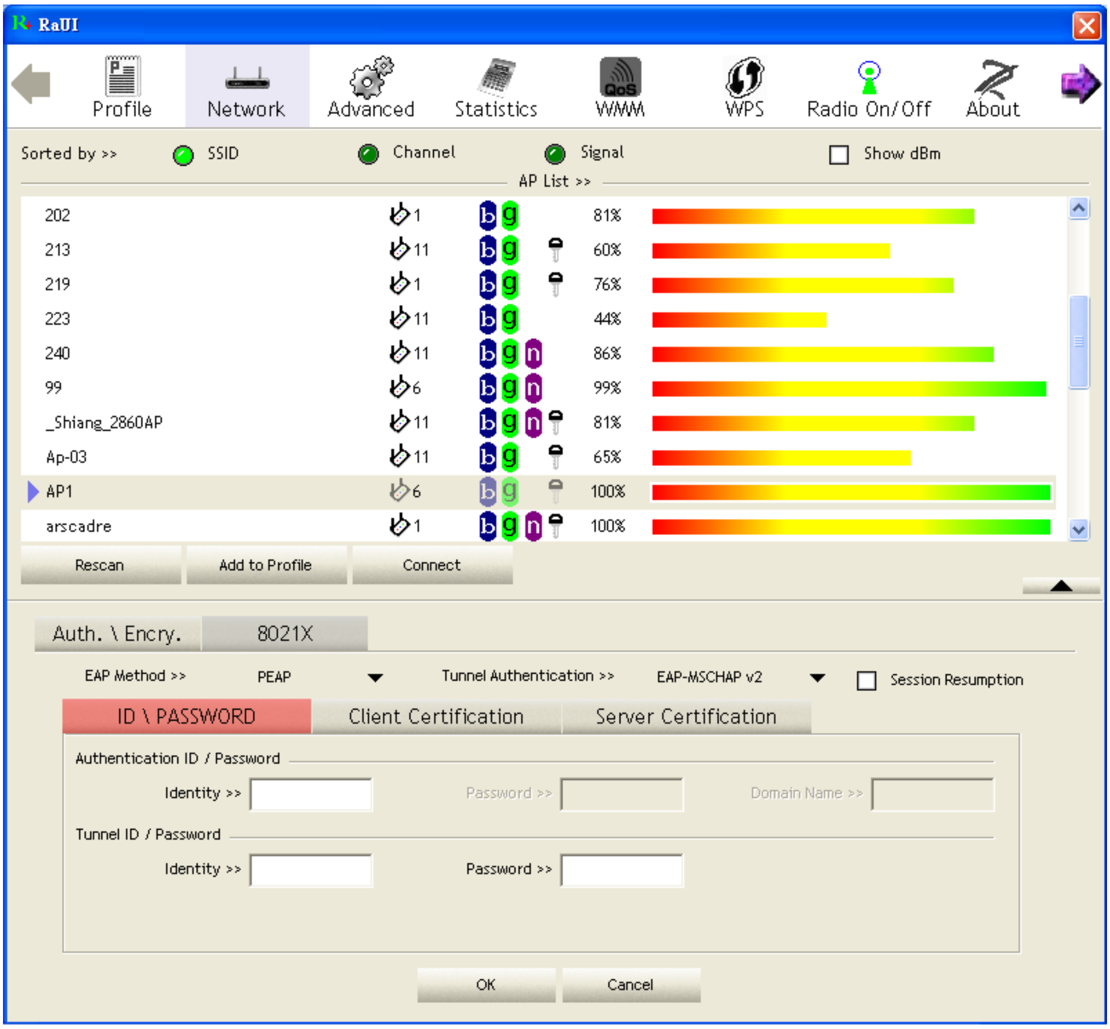
○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

□ Show Password

3. Click "8021X" and the setting page will appear.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

202	1	b g			81%
213	11	b g		🔑	60%
219	1	b g		🔑	76%
223	11	b g			44%
240	11	b g	n		86%
99	6	b g	n		99%
_Shiang_2860AP	11	b g	n	🔑	81%
Ap-03	11	b g		🔑	65%
AP1	6	b g		🔑	100%
arscadre	1	b g	n	🔑	100%

Auth. \ Encry. | 8021X

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

ID \ PASSWORD | Client Certification | Server Certification

Authentication ID / Password

Identity >>

Password >>

Domain Name >>

Tunnel ID / Password

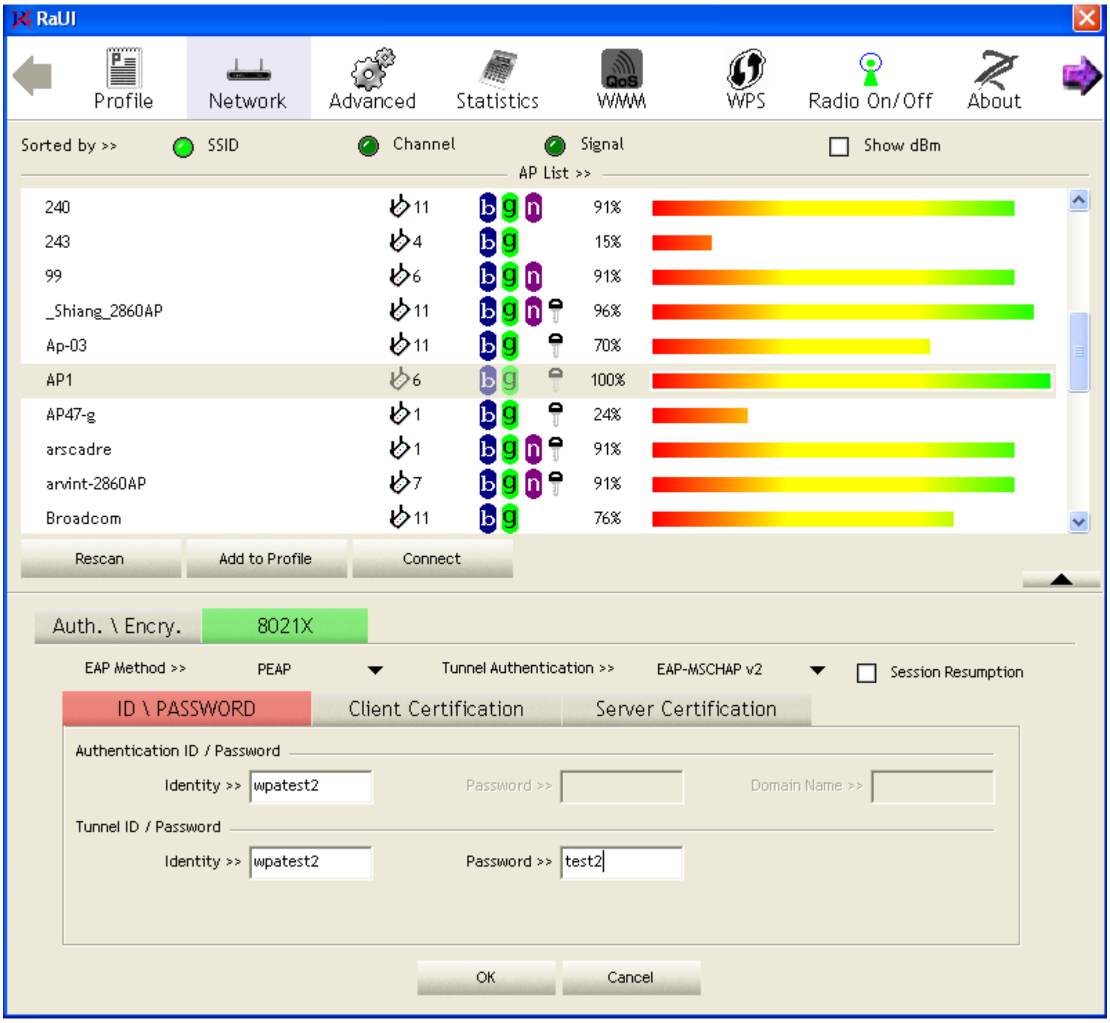
Identity >>

Password >>

4. Authentication type and setting method :

PEAP:

1. Select "PEAP" as the Authentication type from the drop-down list. Key-in "wpatest2" for the identity. "Select "EAP-MSCHAP v2" from the drop-down list for tunnel authentication and key-in the tunnel identity as "wpatest2" and the tunnel password as "test2". These settings are the same as our intended AP's setting.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

240	11	b g n		91%
243	4	b g		15%
99	6	b g n		91%
_Shiang_2860AP	11	b g n	🔑	96%
Ap-03	11	b g	🔑	70%
AP1	6	b g	🔑	100%
AP47-g	1	b g	🔑	24%
arscadre	1	b g n	🔑	91%
arvint-2860AP	7	b g n	🔑	91%
Broadcom	11	b g		76%

Auth. \ Encry. 8021X

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

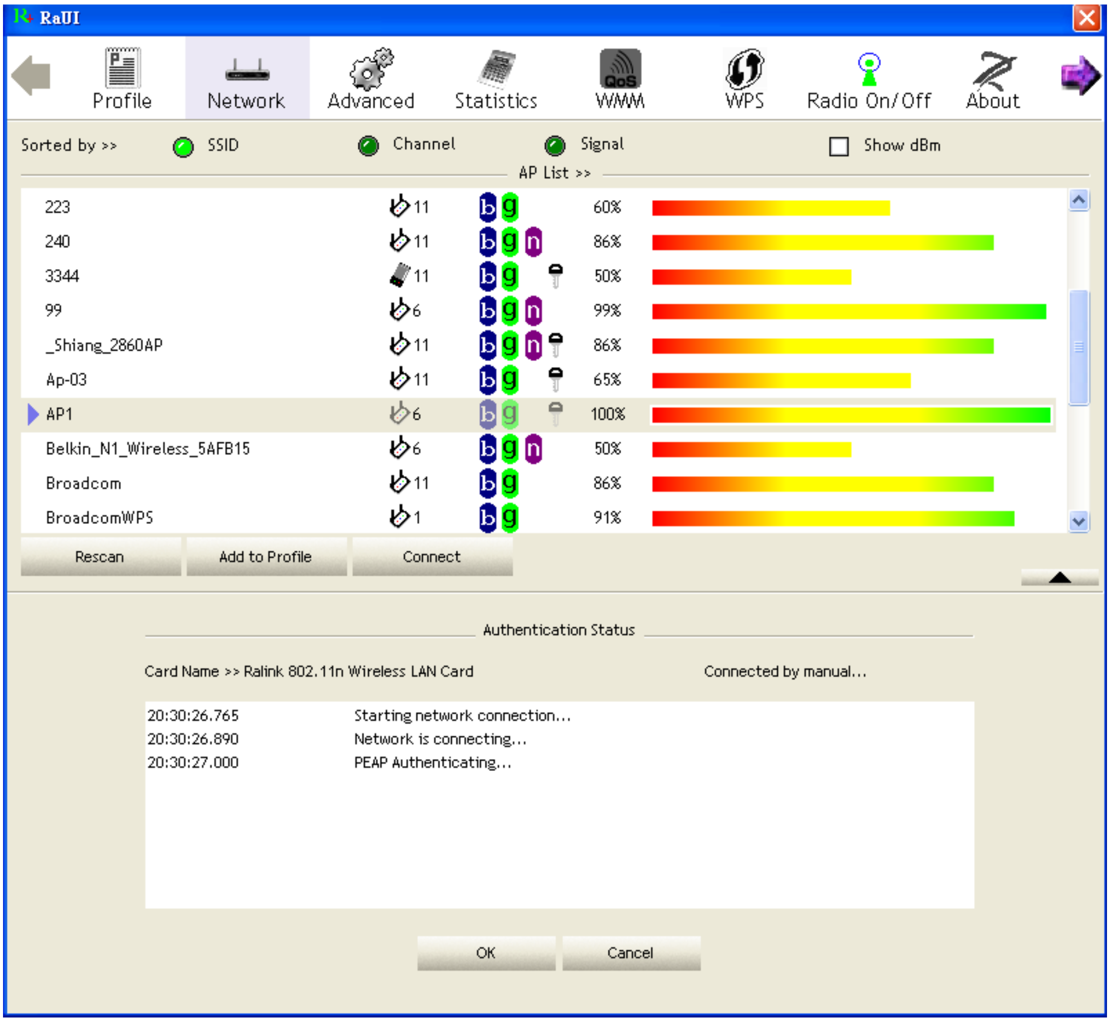
Authentication ID / Password

Identity >> wpatest2 Password >> Domain Name >>

Tunnel ID / Password

Identity >> wpatest2 Password >> test2

2. Click OK. The dialog box should appear as below.



223	11	b g			60%
240	11	b g n			86%
3344	11	b g		🔑	50%
99	6	b g n			99%
_Shiang_2860AP	11	b g n	🔑		86%
Ap-03	11	b g		🔑	65%
▶ AP1	6	b g		🔑	100%
Belkin_N1_Wireless_5AFB15	6	b g n			50%
Broadcom	11	b g			86%
BroadcomWPS	1	b g			91%

Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card

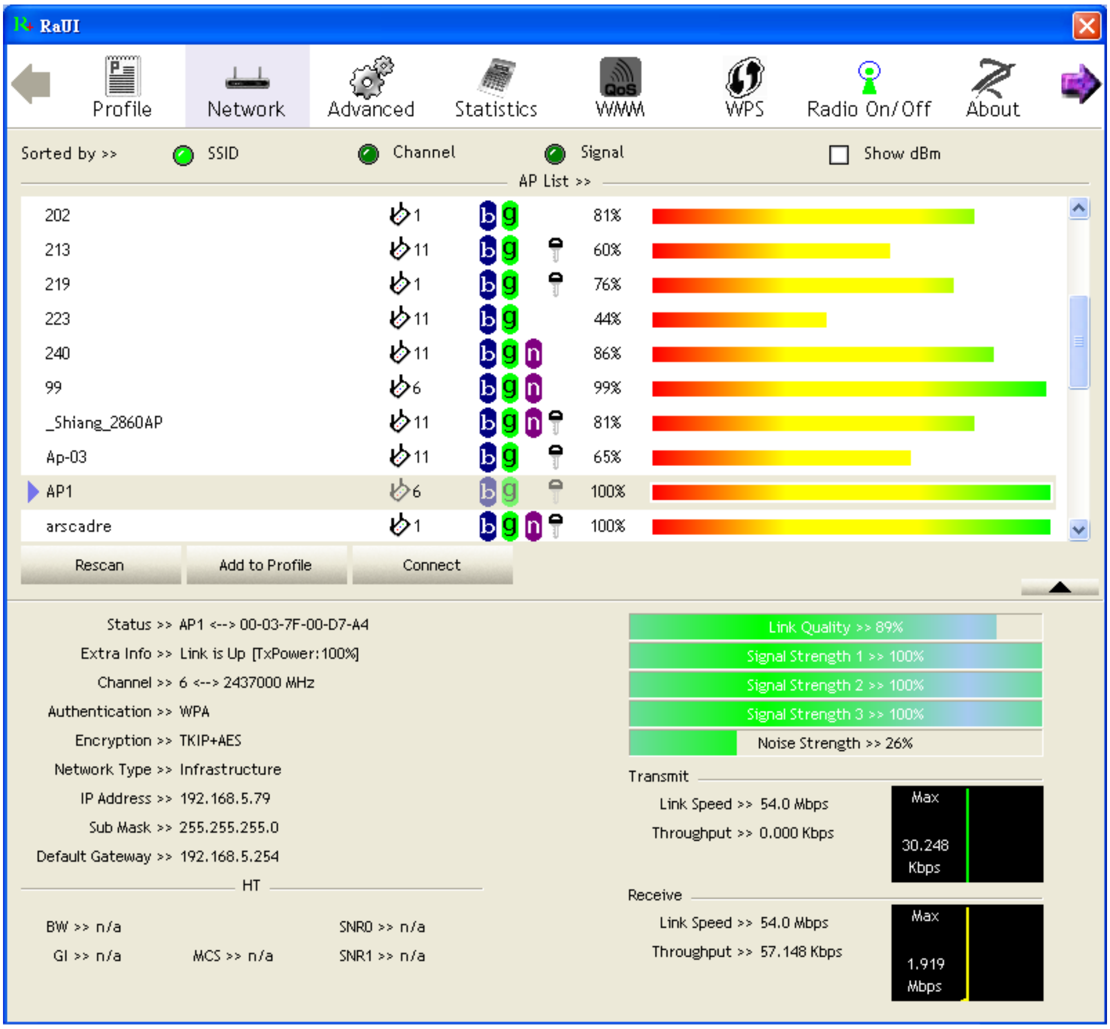
Connected by manual...

```
20:30:26.765          Starting network connection...
20:30:26.890          Network is connecting...
20:30:27.000          PEAP Authenticating...
```

*If you want to disconnect, please click cancel button in Authentication Status function.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

3. If the connection is successful, the dialog will appear as below.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

202	1	b g		81%
213	11	b g	🔑	60%
219	1	b g	🔑	76%
223	11	b g		44%
240	11	b g n		86%
99	6	b g n		99%
_Shiang_2860AP	11	b g n	🔑	81%
Ap-03	11	b g	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n	🔑	100%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> TKIP+AES
Network Type >> Infrastructure
IP Address >> 192.168.5.79
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 >> 89%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit

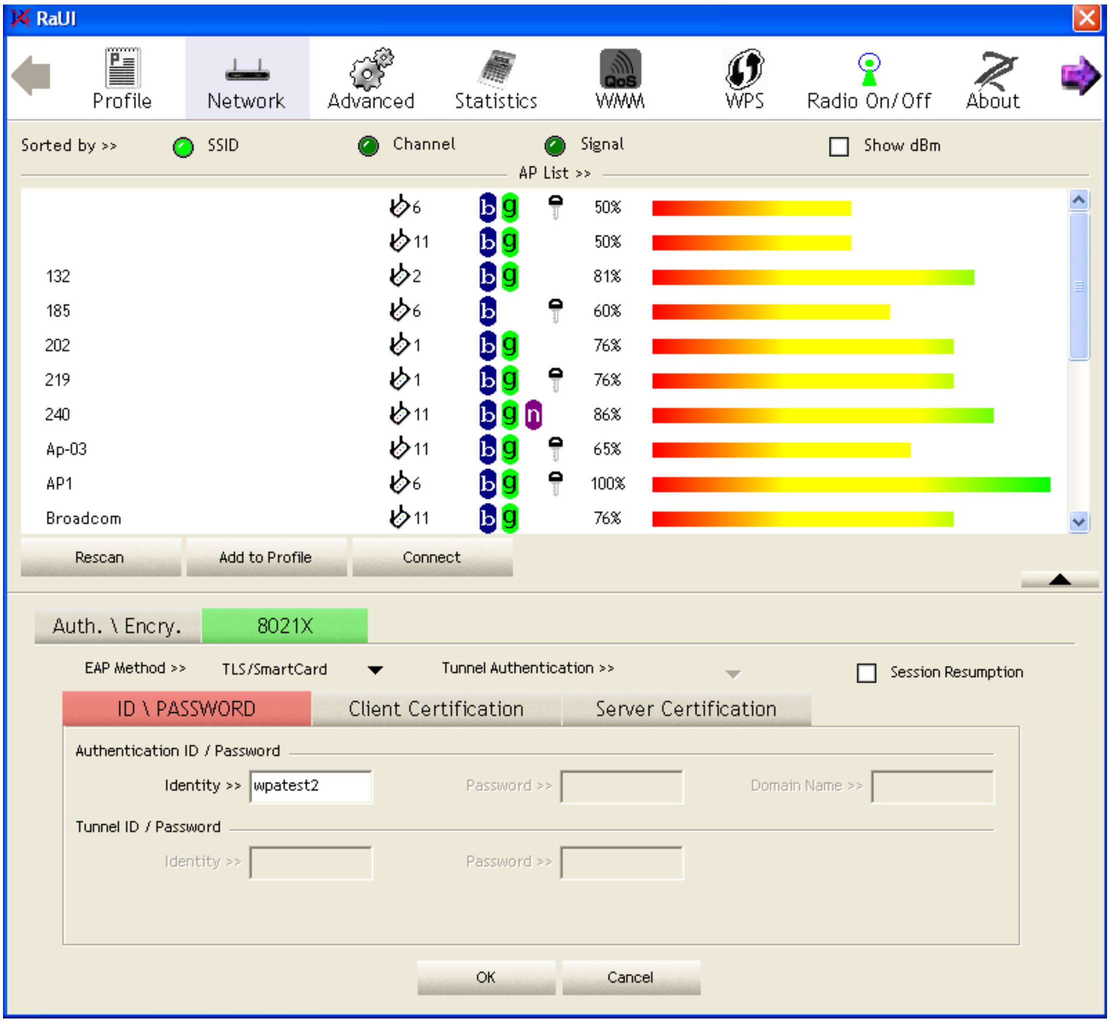
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps

Receive

Link Speed >> 54.0 Mbps
Throughput >> 57.148 Kbps

TLS / Smart Card :

1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server uthentication.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

	6	b g	🔒	50%
	11	b g		50%
132	2	b g		81%
185	6	b	🔒	60%
202	1	b g		76%
219	1	b g	🔒	76%
240	11	b g n		86%
Ap-03	11	b g	🔒	65%
AP1	6	b g	🔒	100%
Broadcom	11	b g		76%

Auth. \ Encry. 8021X

EAP Method >> TLS/SmartCard

Tunnel Authentication >>

□ Session Resumption

ID \ PASSWORD | Client Certification | Server Certification

Authentication ID / Password

Identity >> wpatest2

Password >>

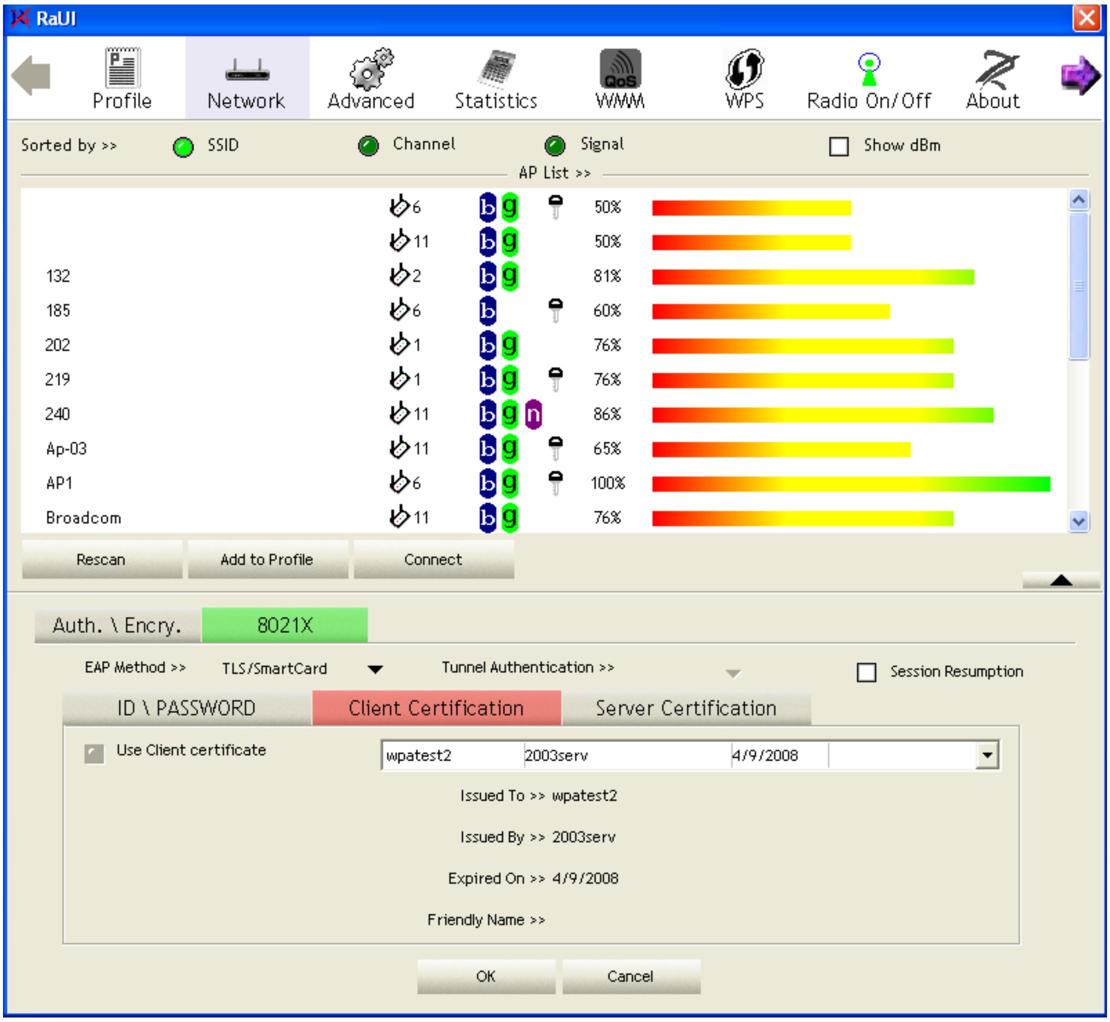
Domain Name >>

Tunnel ID / Password

Identity >>

Password >>

2. TLS must use client certification. Click "Client Certification" and select a certification for server authentication.



SSID	Channel	Mode	Signal
	6	b g	50%
	11	b g	50%
132	2	b g	81%
185	6	b	60%
202	1	b g	76%
219	1	b g	76%
240	11	b g n	86%
Ap-03	11	b g	65%
AP1	6	b g	100%
Broadcom	11	b g	76%

Auth. \ Encry. : 8021X

EAP Method >> TLS/SmartCard

Tunnel Authentication >>

□ Session Resumption

ID \ PASSWORD | Client Certification | Server Certification

☑ Use Client certificate — wpatest2 2003serv 4/9/2008

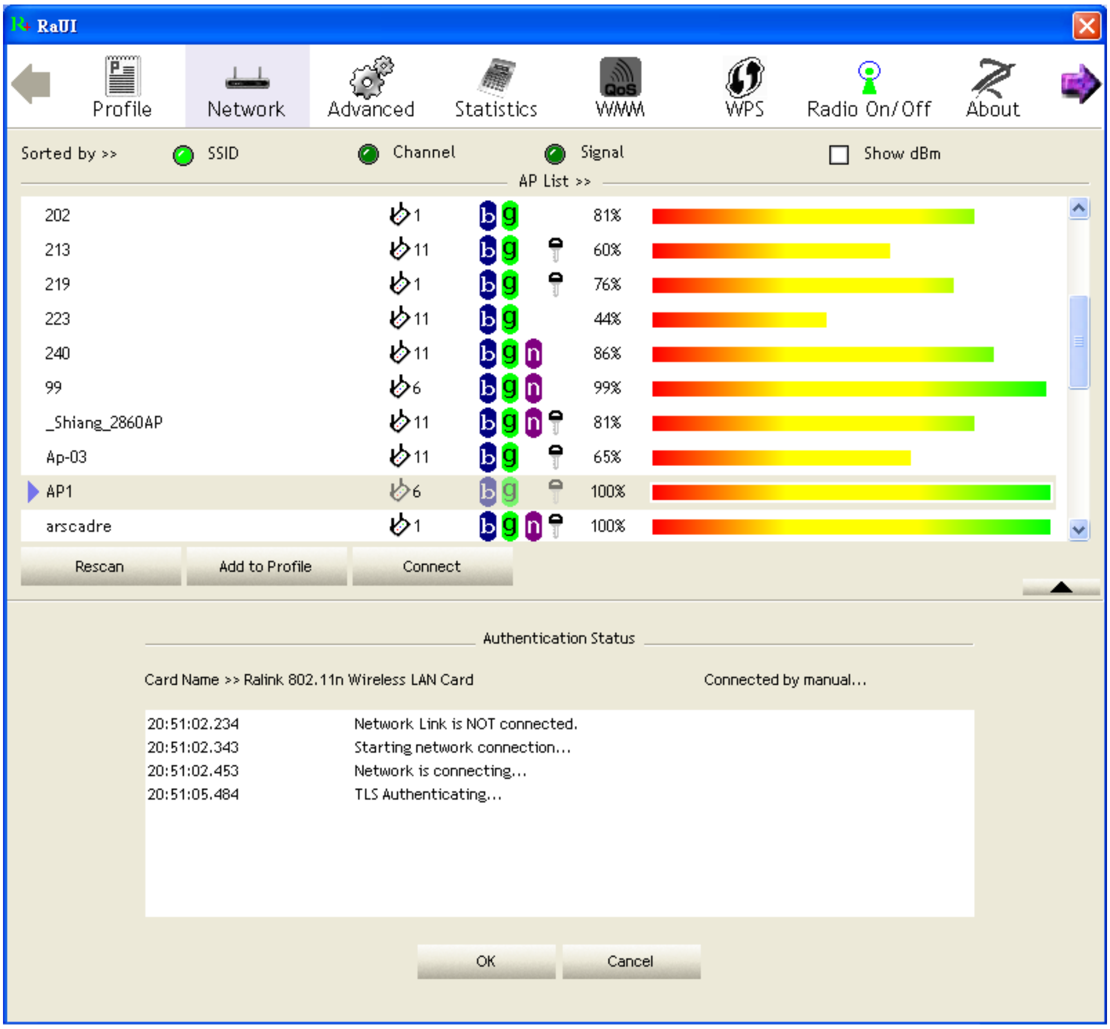
Issued To >> wpatest2

Issued By >> 2003serv

Expired On >> 4/9/2008

Friendly Name >>

3. Click "OK". The dialog box should appear as the image below.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

202	1	b g		81%
213	11	b g	🔑	60%
219	1	b g	🔑	76%
223	11	b g		44%
240	11	b g n		86%
99	6	b g n		99%
_Shiang_2860AP	11	b g n	🔑	81%
Ap-03	11	b g	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n	🔑	100%

Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card

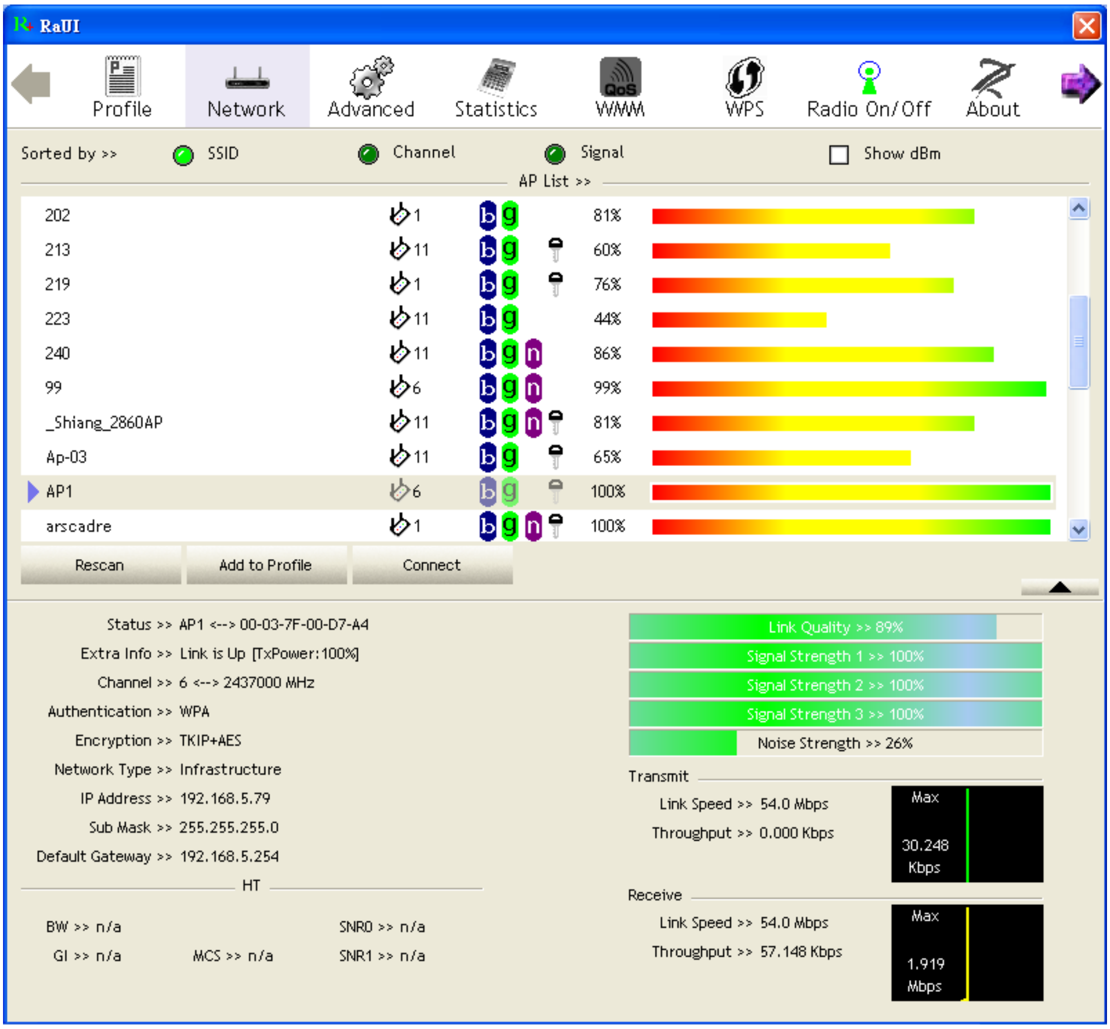
Connected by manual...

```
20:51:02.234        Network Link is NOT connected.
20:51:02.343        Starting network connection...
20:51:02.453        Network is connecting...
20:51:05.484        TLS Authenticating...
```

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. If it connected successfully, the result will appear as in the image below.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

202	1	b g		81%
213	11	b g	🔑	60%
219	1	b g	🔑	76%
223	11	b g		44%
240	11	b g n		86%
99	6	b g n		99%
_Shiang_2860AP	11	b g n	🔑	81%
Ap-03	11	b g	🔑	65%
AP1	6	b g	🔑	100%
arscadre	1	b g n	🔑	100%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> TKIP+AES
Network Type >> Infrastructure
IP Address >> 192.168.5.79
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

BW >> n/a SNR0 >> n/a
GI >> n/a MCS >> n/a SNR1 >> n/a

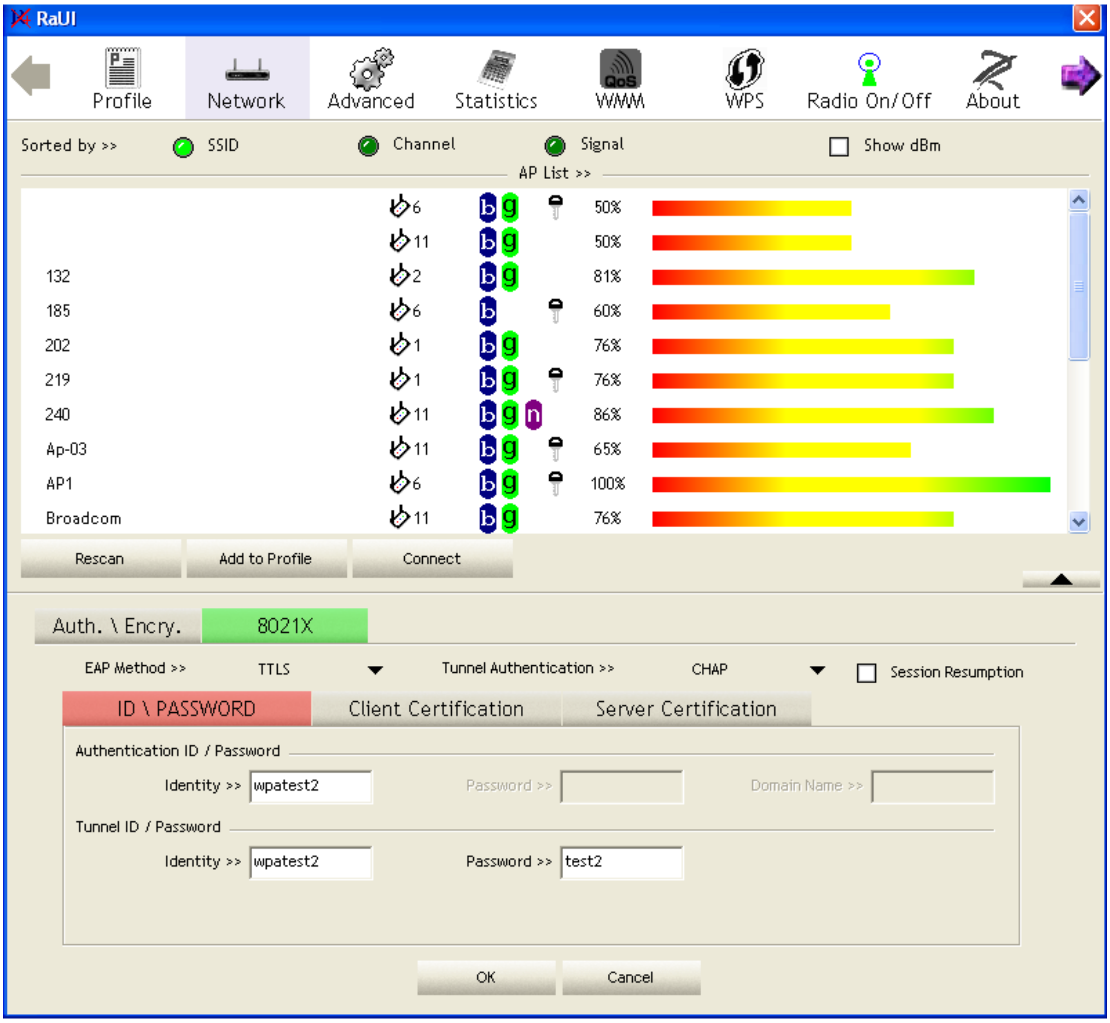
Link Quality >> 89%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps
Max
30.248 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 57.148 Kbps
Max
1.919 Mbps

TTLS :

1. Select TTLS from the Authentication type drop-down list. Key-in the identity as "wpatest2". Select CHAP for tunnel authentication, and key-in the identity as "wpatest2" and tunnel password as "test2". These settings are the same as our intended AP's setting.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

	6	b g	🔑	50%	
	11	b g		50%	
132	2	b g		81%	
185	6	b	🔑	60%	
202	1	b g		76%	
219	1	b g	🔑	76%	
240	11	b g n		86%	
Ap-03	11	b g	🔑	65%	
AP1	6	b g	🔑	100%	
Broadcom	11	b g		76%	

Auth. \ Encry. 8021X

EAP Method >> TTLS

Tunnel Authentication >> CHAP

□ Session Resumption

ID \ PASSWORD | Client Certification | Server Certification

Authentication ID / Password

Identity >> wpatest2

Password >>

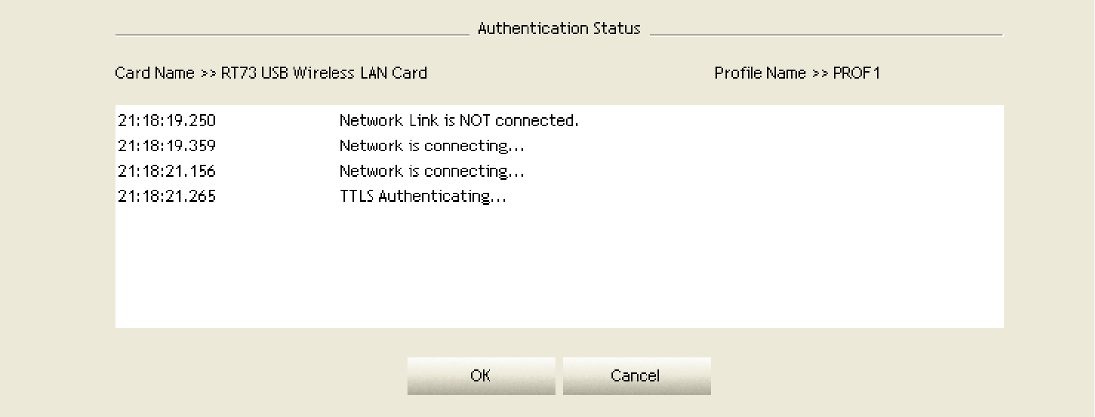
Domain Name >>

Tunnel ID / Password

Identity >> wpatest2

Password >> test2

2. Click "OK". The dialog box should appear as the image below.



Card Name >> RT73 USB Wireless LAN Card

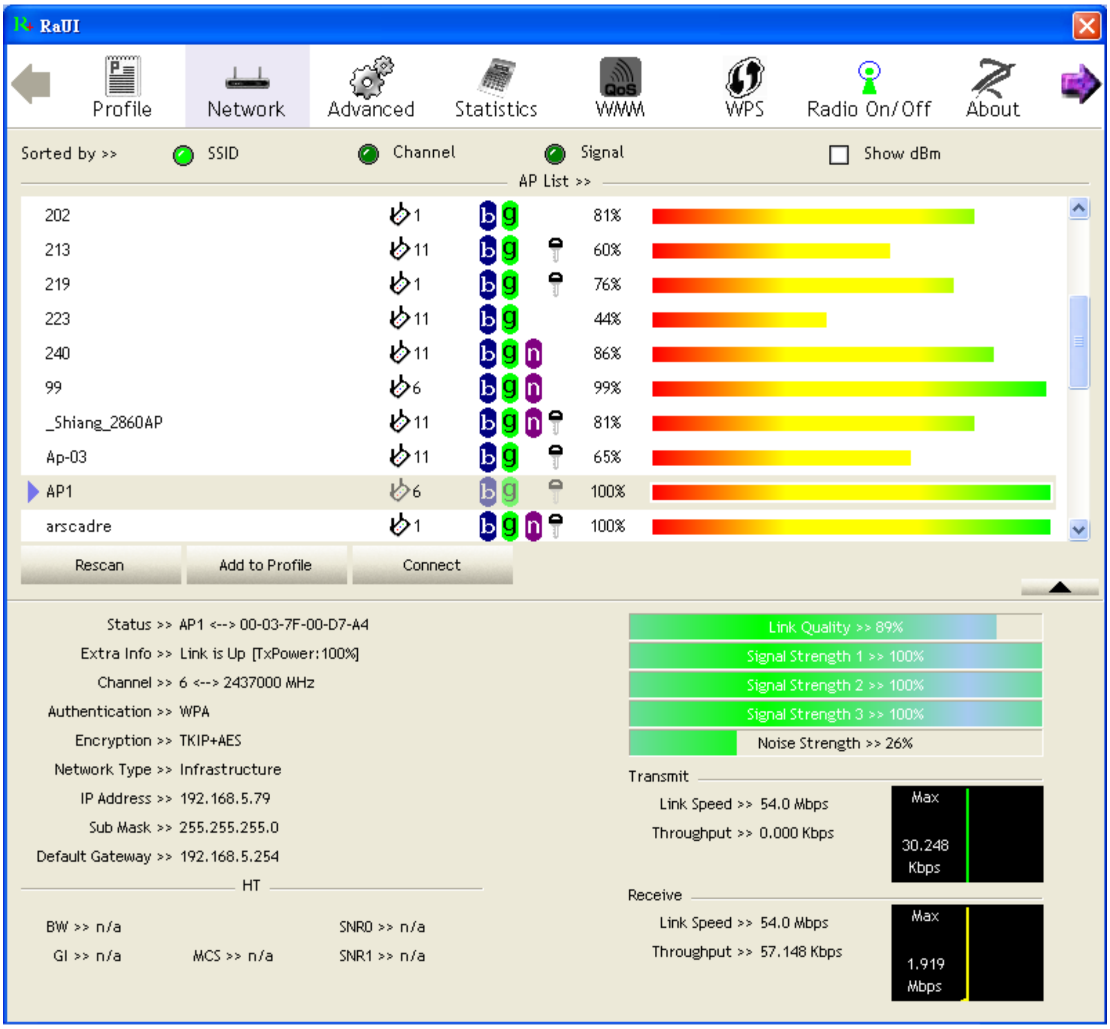
Profile Name >> PROF1

```
21:18:19.250    Network Link is NOT connected.
21:18:19.359    Network is connecting...
21:18:21.156    Network is connecting...
21:18:21.265    TTLS Authenticating...
```

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

3. If the connection is successful, the dialog box will appear as the image below.



202	1	b g		81%
213	11	b g	🔒	60%
219	1	b g	🔒	76%
223	11	b g		44%
240	11	b g n		86%
99	6	b g n		99%
_Shiang_2860AP	11	b g n	🔒	81%
Ap-03	11	b g	🔒	65%
AP1	6	b g	🔒	100%
arscadre	1	b g n	🔒	100%

Status >> AP1 <--> 00-03-7F-00-D7-A4

Extra Info >> Link is Up [TxPower:100%]

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.5.79

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 89%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

30.248 Kbps

Receive

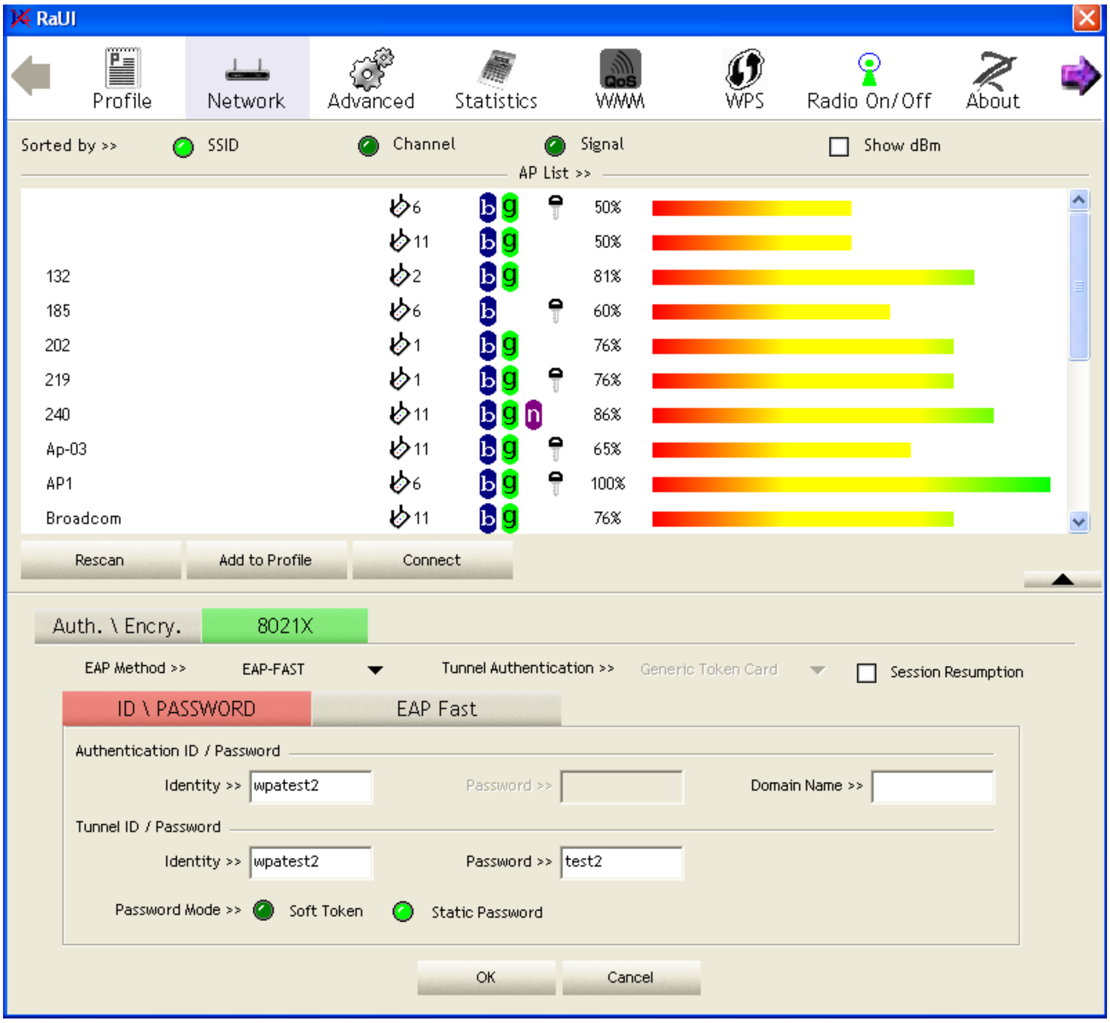
Link Speed >> 54.0 Mbps

Throughput >> 57.148 Kbps

1.919 Mbps

EAP-FAST :

1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. Tunnel Protocol only supports "Generic Token Card" now. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's setting.



SSID	Channel	Mode	Encryption	Signal
	6	b g	🔑	50%
	11	b g		50%
132	2	b g		81%
185	6	b	🔑	60%
202	1	b g		76%
219	1	b g	🔑	76%
240	11	b g n		86%
Ap-03	11	b g	🔑	65%
AP1	6	b g	🔑	100%
Broadcom	11	b g		76%

Auth. \ Encry. 8021X

EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card

□ Session Resumption

ID \ PASSWORD | EAP Fast

Authentication ID / Password

Identity >> wpatest2

Password >>

Domain Name >>

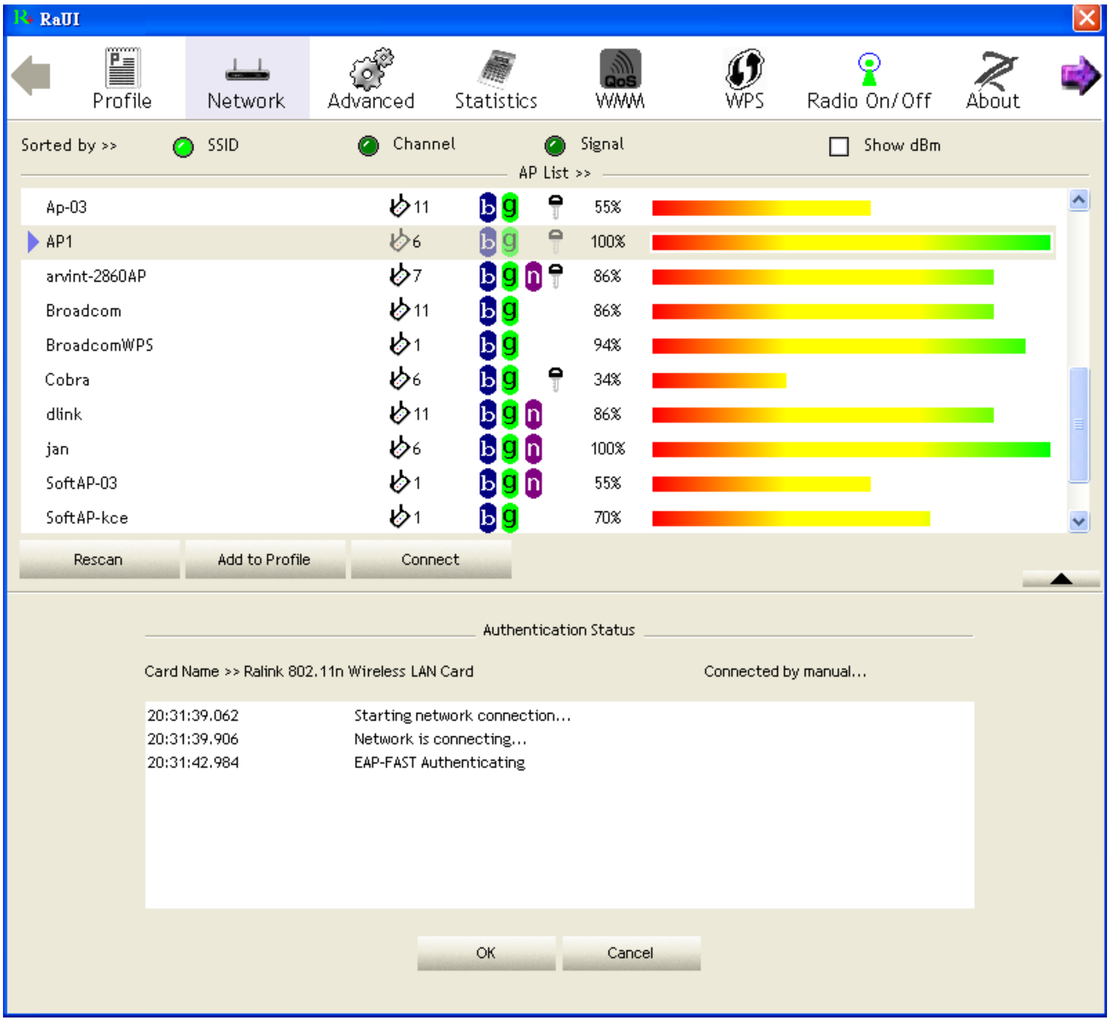
Tunnel ID / Password

Identity >> wpatest2

Password >> test2

Password Mode >> ● Soft Token ● Static Password

2. Click "OK". The dialog box should appear as the image below



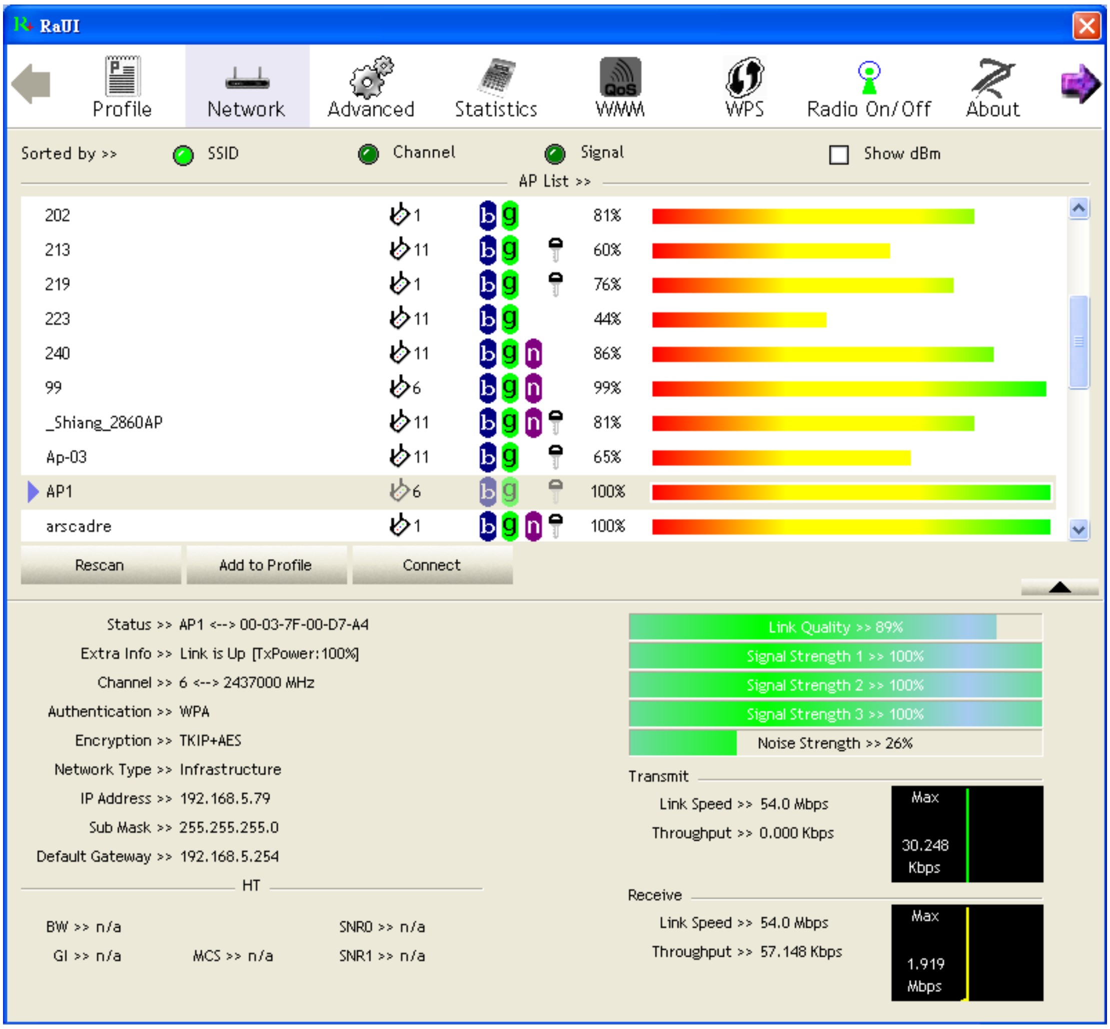
Ap-03	11	b g	🔑	55%
▶ AP1	6	b g	🔑	100%
arvint-2860AP	7	b g n	🔑	86%
Broadcom	11	b g		86%
BroadcomWPS	1	b g		94%
Cobra	6	b g	🔑	34%
dlink	11	b g n		86%
jan	6	b g n		100%
SoftAP-03	1	b g n		55%
SoftAP-kce	1	b g		70%

Card Name >> Ralink 802.11n Wireless LAN Card

Connected by manual...

```
20:31:39.062        Starting network connection...
20:31:39.906        Network is connecting...
20:31:42.984        EAP-FAST Authenticating
```

3. If the connection is successful, the dialog box will appear as the image below.



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

202	1	b g		81%
213	11	b g		60%
219	1	b g		76%
223	11	b g		44%
240	11	b g n		86%
99	6	b g n		99%
_Shiang_2860AP	11	b g n		81%
Ap-03	11	b g		65%
AP1	6	b g		100%
arscadre	1	b g n		100%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> TKIP+AES
Network Type >> Infrastructure
IP Address >> 192.168.5.79
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

BW >> n/a SNR0 >> n/a
GI >> n/a MCS >> n/a SNR1 >> n/a

Link Quality >> 89%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps
Max
30.248
Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 57.148 Kbps
Max
1.919
Mbps

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

5. Trouble Shooting

This chapter provides solutions to problems that may occur during the installation and operation of PCI Adapter. Read the descriptions below to solve your problems.

1. **The PCI Adapter does not work properly.**

Reinsert PCI Adapter into your PC's PCI slot. Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find PCI Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of PCI Adapter. If there is a yellow question mark, please check the following: Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.) Make sure that you have inserted the right adapter and installed the proper driver. If PCI Adapter does not function after attempting the above steps, remove it and do the following: Uninstall the driver software from your PC. Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2. **I can't communicate with the other computers linked via Ethernet in the Infrastructure configuration.**

Make sure that the PC to which PCI Adapter is associated is powered on. Make sure that PCI Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

3. **What should I do when the computer with PCI Adapter installed is unable to connect to the wireless network and/or the Internet?**

Check that the LED indicators for the broadband modem are indicating normal activity. If not, there may be a problem with the broadband connection. Check that the LED indicators on the wireless router are functioning properly. If not, check that the AC power and Ethernet cables are firmly connected. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points. In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it might be necessary to set up one client to establish a BSS (Basic Service Set) and wait briefly before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it. Check that the Network Connection for the wireless client is configured properly. If Security is enabled, make sure that the correct encryption keys are entered on both PCI Adapter and the access point.