

802.11n Wireless PCI Adapter



USER MANUAL 1.0.0

Table of Contents

Chapter I	Introduction	4
1. Welcome		4
2. Product Feature		4
3. Contents of Package		4
4. Before you begin		4
Chapter II	Designing Your PCI Adapter	5
Chapter III	Installation	5
1. Install Your PCI Adapter		5
2. Install Driver and Utility		6
Chapter IV	Utility Config	11
1. WZC		11
1.1 Ralink Wireless Utility (RaUI) or Windows Zero Configuration (WZC)		11
1.2 Use WZC to configure wireless NIC		12
2. RaUI		18
2.1 Start		18
2.1. Start RaUI		18
2.2 Profile		24
2.2. Profile		24
2.2. Add/Edit Profile		26
2.2. Example to Add Profile in Profile		27
2.3 Network		31
2.3. Network		31
2.3. Example on Adding Profile in Network		38
2.4 Advanced		42
2.4. Advanced		42
2.5 Statistics		43
2.5. Statistics		43
2.6 WMM		45
2.6. WMM		45
2.6. Example to Configure to Enable DLS (Direct Link Setup)		46
2.6. Example to Configure to Enable Wi-Fi Multi-Media		51
2.6. Example to Configure to Enable WMM - Power Save		52
2.7 WPS		53
2.7. WPS		53
2.7. WPS Information on AP		56
2.7. Example to Add to Registrar Using PIN Method		57
2.7. Example to Add to Registrar Using PBC Method		63
2.7. Example to Configure a Network/AP Using PIN or PBC Method		68
2.8 About		70
2.8. About		70
2.9 Link Status		71

2.9. Link Status	71
3. Security	73
3.1 Auth. \ Encry. Setting - WEP/TKIP/AES	73
3.2 802.1x Setting	73
3.3 Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is Failed in Profile	
3.4 Example to Configure Connection with WEP on	80
3.5 Example to Configure Connection with WPA-PSK	83
3.6 Example to Configure Connection with WPA	87
Chapter V Trouble Shooting	103

1 Introduction

1.1 Welcome

PCI Adapter connects you with IEEE802.11n(Draft 2.0) networks at receiving rate up to an incredible 600Mbps! 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, IEEE 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, it 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, WPA (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 (Draft 2.0), IEEE 802.11g, IEEE 802.11b standards
- Provides 32-bit PCI interface
- Provides 600Mbps receiving rate and 600Mbps 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 smooth
- Supports Windows® 2000, XP 32/64, Vista 32/64, Windows 7, Windows 8, Windows 10

1.3 Contents of Package

- One PCI Adapter
- One Installation CD w/User Manual
- Two dipole antennas

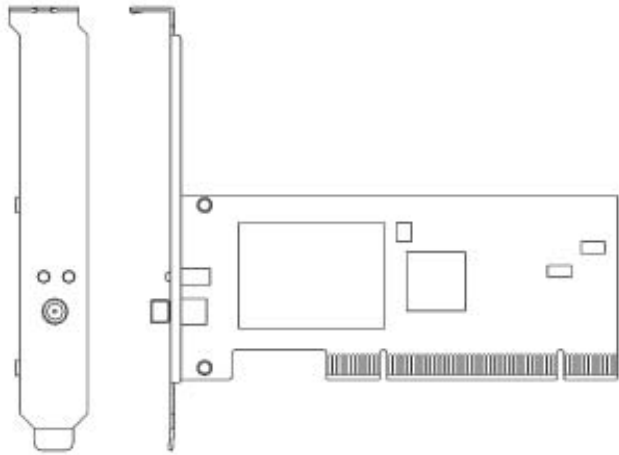
Contact your local authorized reseller or the store purchased from for any items damaged and/or missing.

1.4 Before you begin

- You must have the following:
- A desktop PC with an available 32-bit PCI slot
- Minimum 300MHz processor and 32MB memory
- Windows 2000, XP, 2003, Vista, Windows 7, Windows 8, Windows 10
- A CD-ROM Drive
- PCI controller properly installed and working in the desktop PC
- 802.11n or 802.11b/g Access Point (for infrastructure Mode) or another 802.11n or 802.11b/g wireless adapter (for Ad-Hoc; Peer-to-Peer networking mode.)

2 Designing Your PCI Adapter

PCI Adapter supports up to 100 Mbps connections. It is fully compliant with the specifications defined in 802.11n (Draft 2.0) standard.



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

- Lnk/Act ON (Green): Indicates a valid connection.
- Lnk/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 slot 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 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.

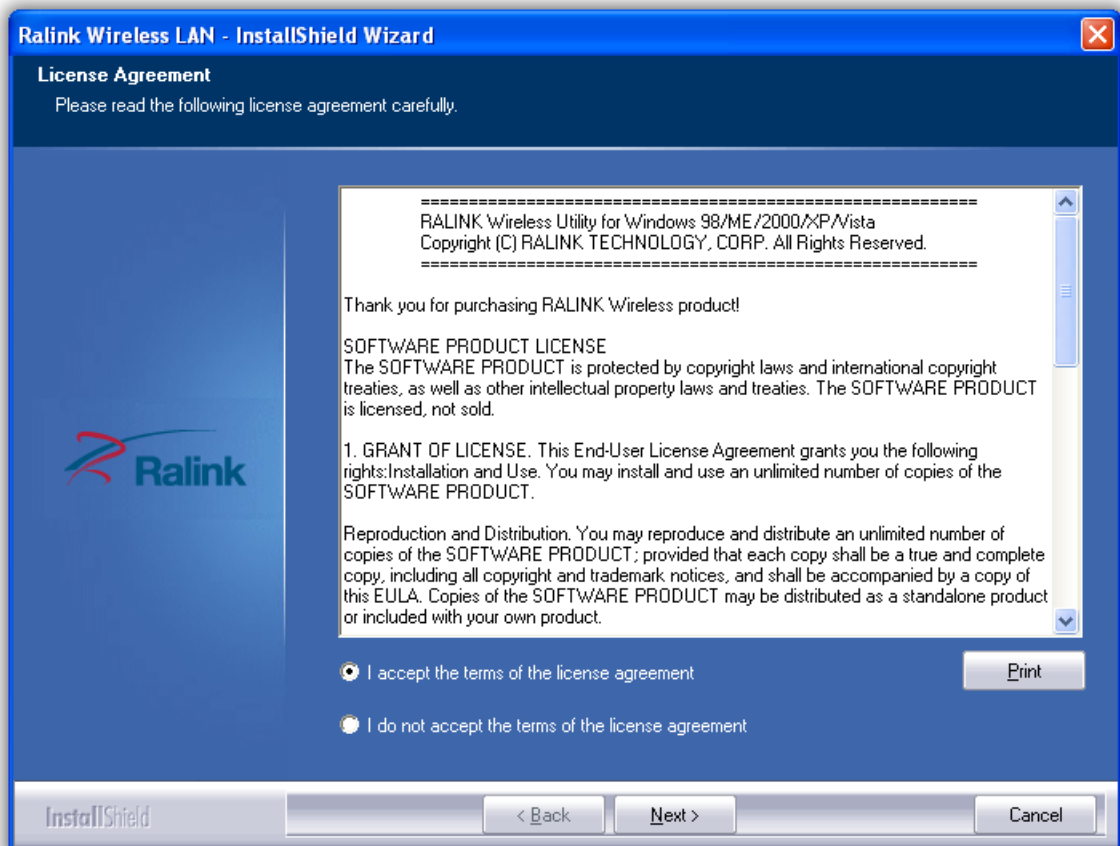
Note: Select **Cancel** when "Found New Hardware" window appears.



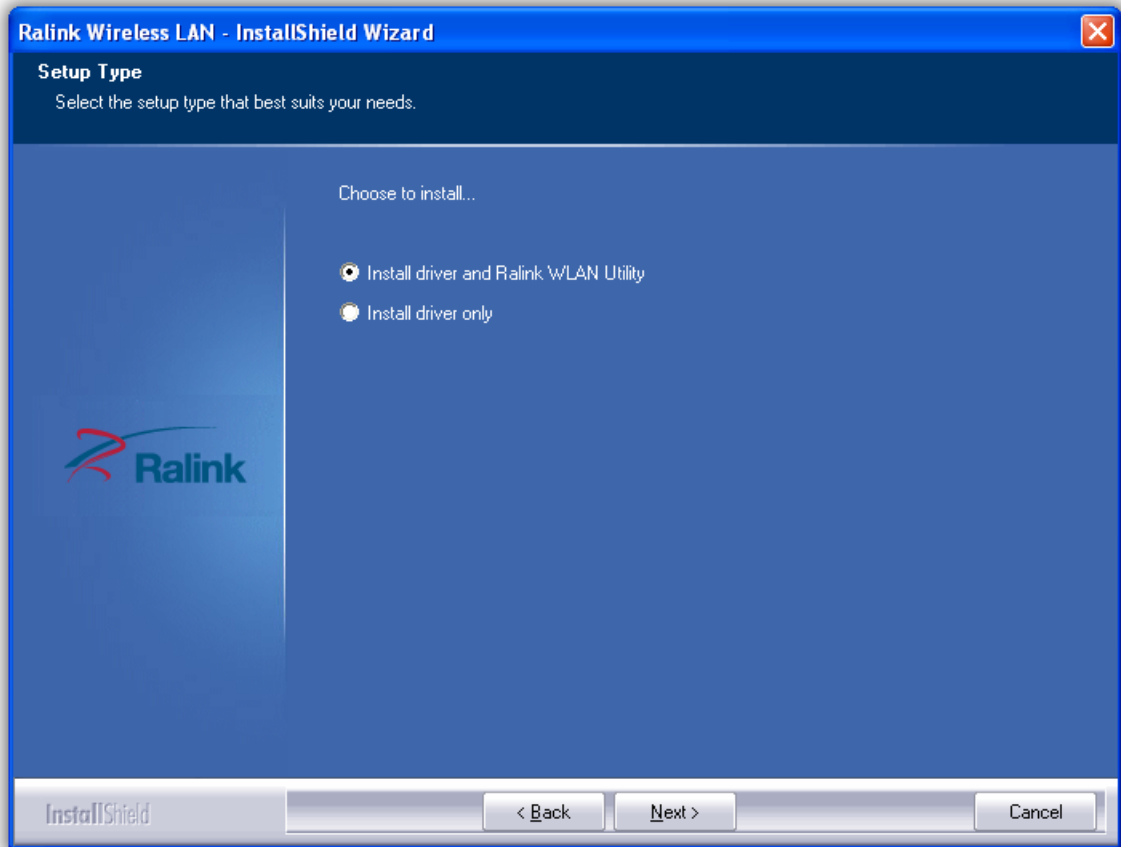
3.2 Install Driver and Utility

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

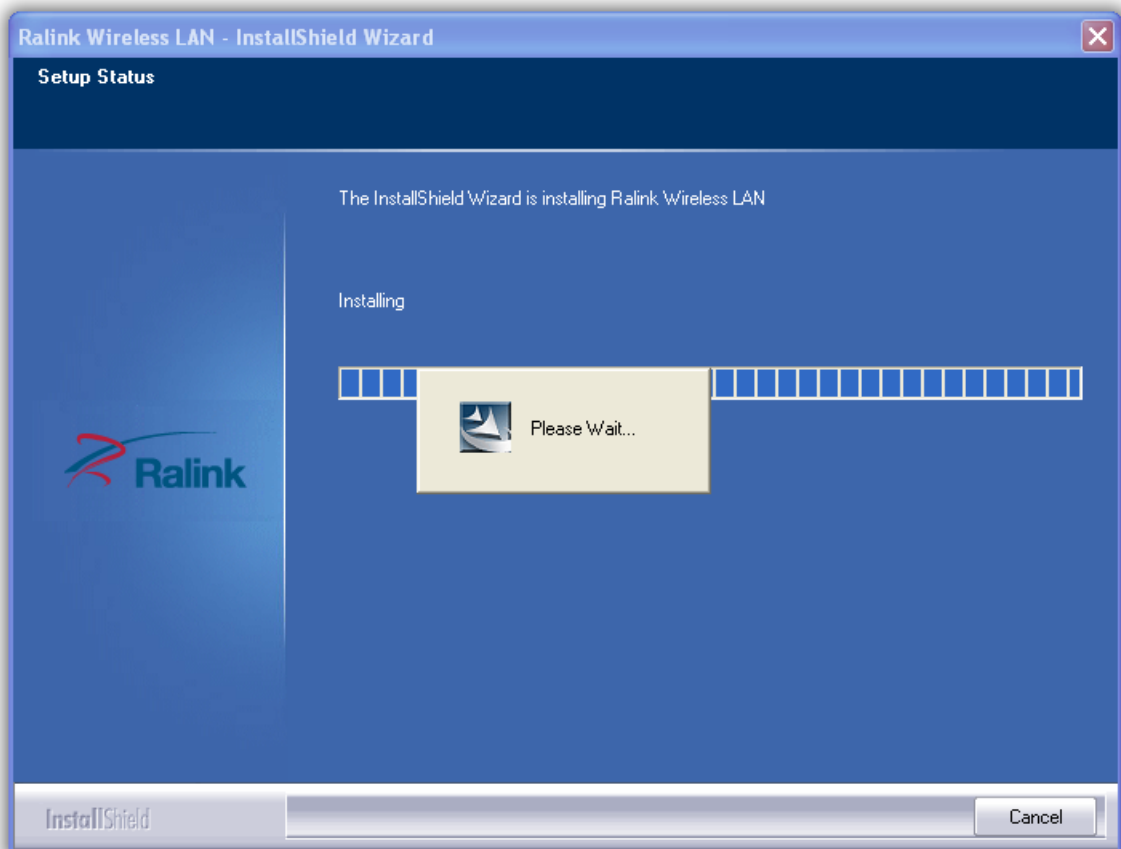
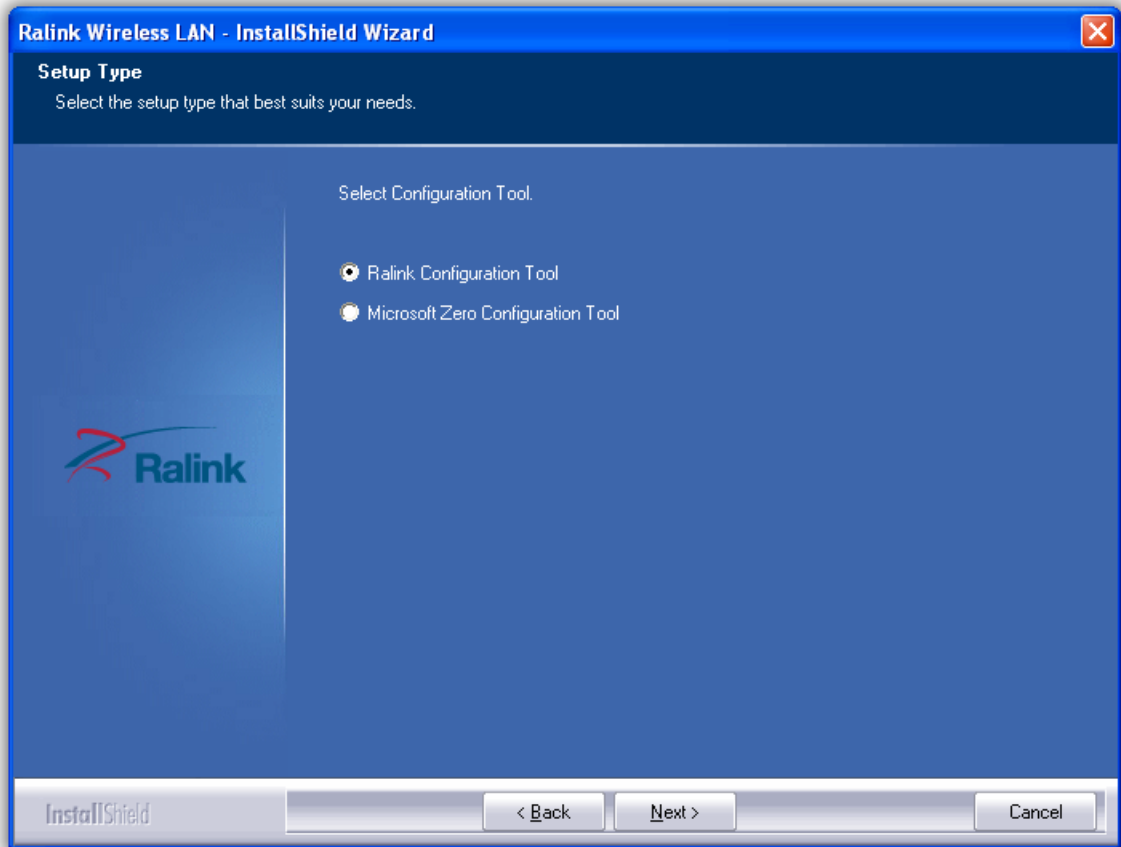
1. Insert Installation CD to your CD-ROM drive. And click **Driver Installation**. The wizard will run and install all necessary files to your computer automatically.
2. Click **Next** to accept the Agreement. Or click **Cancel** to cancel the installation.



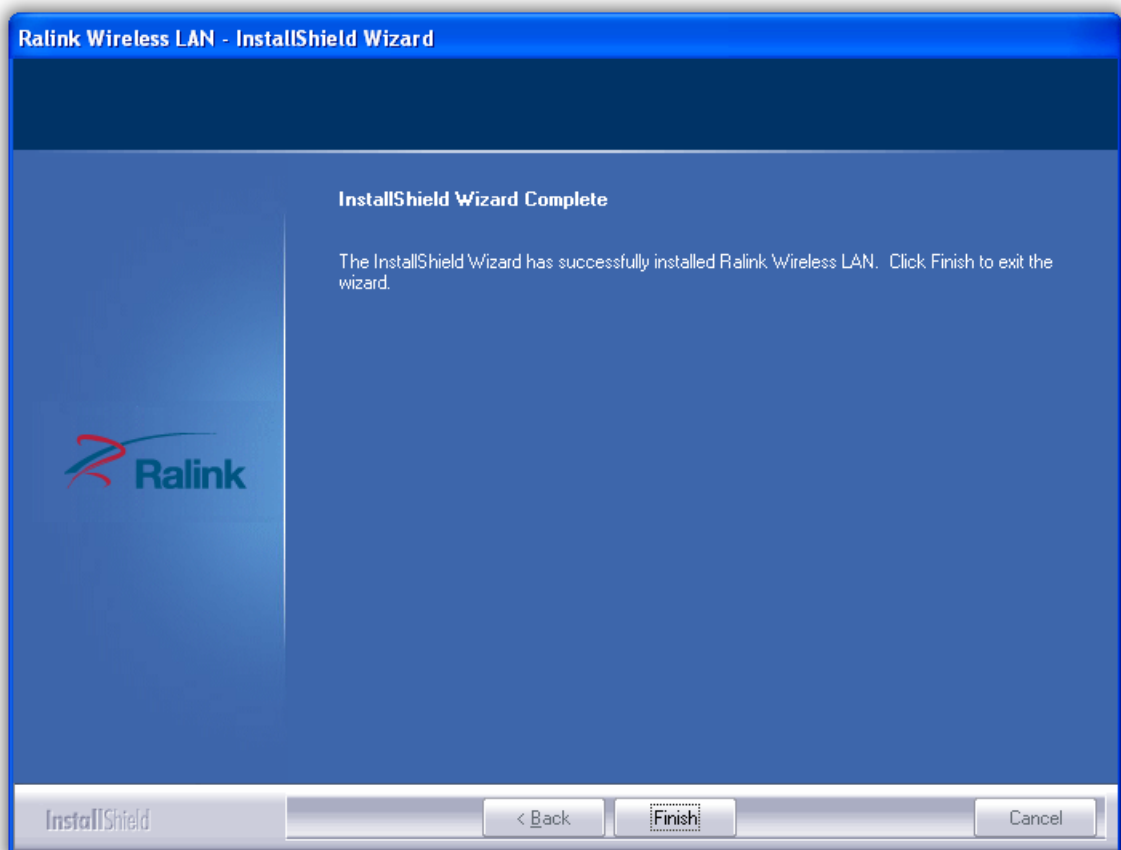
3. Click **Next**.



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 function 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**.



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



4 Utility Config

4.1 WZC

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. To make it 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.



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.

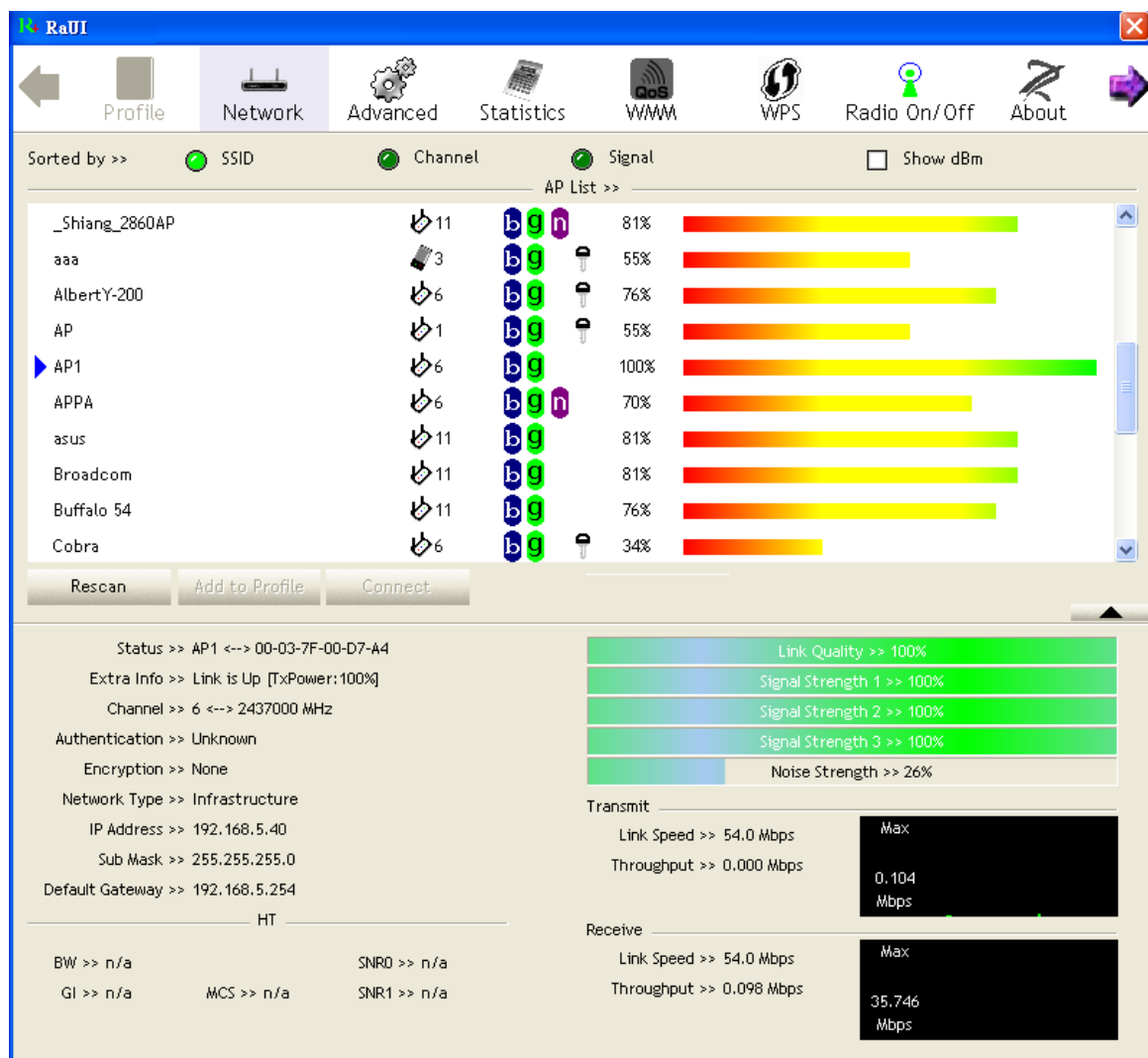


Figure 1-3 RaUI status with WZC active

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 connect 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.

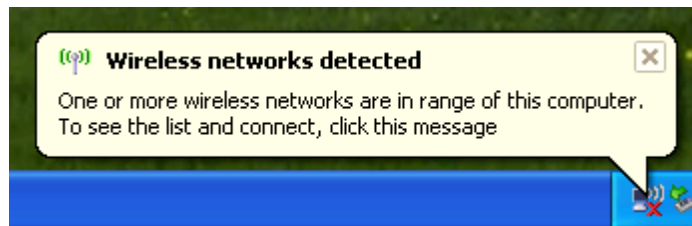


Figure 1-4 status prompt for no connection

- 2 Right-click the network connection icon in taskbar.



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.

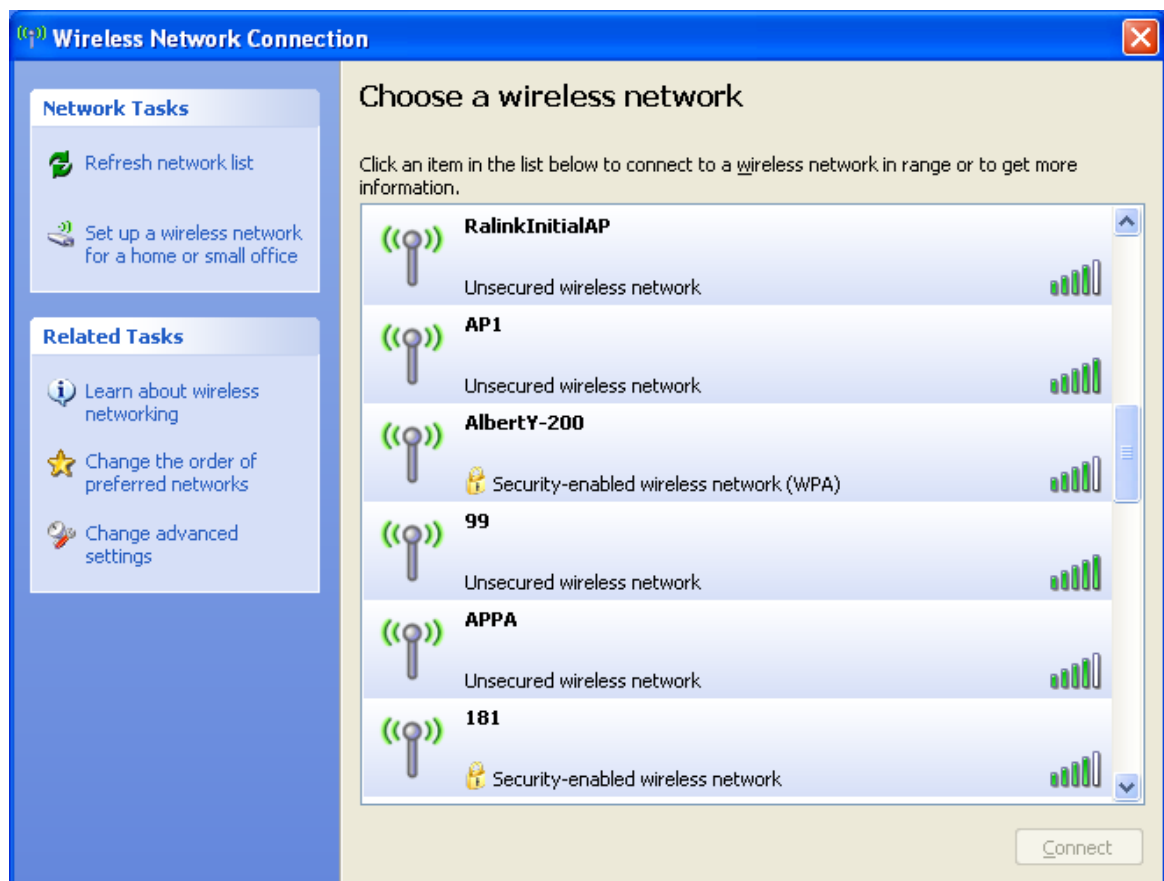


Figure 1-6 Wireless Network Connection

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

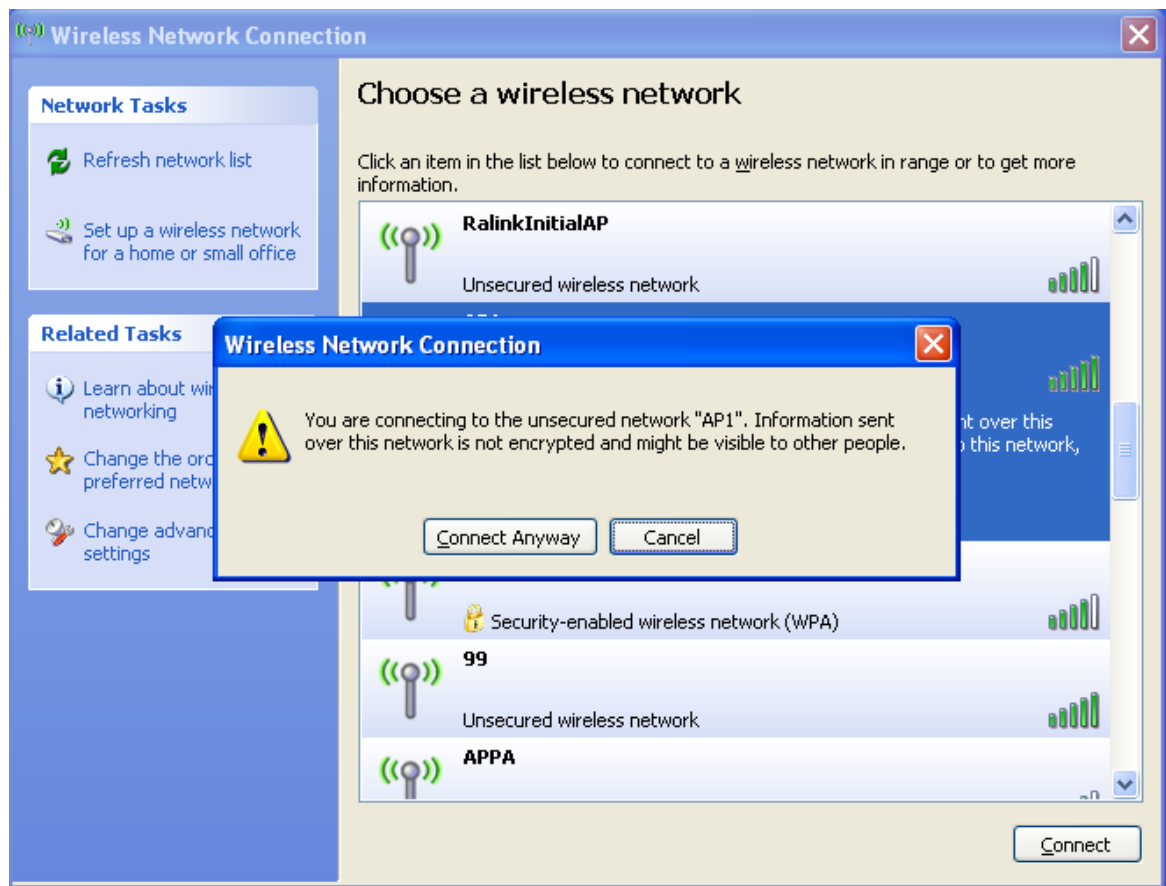


Figure 1-7 Select intended AP : AP1, then click "Connect"

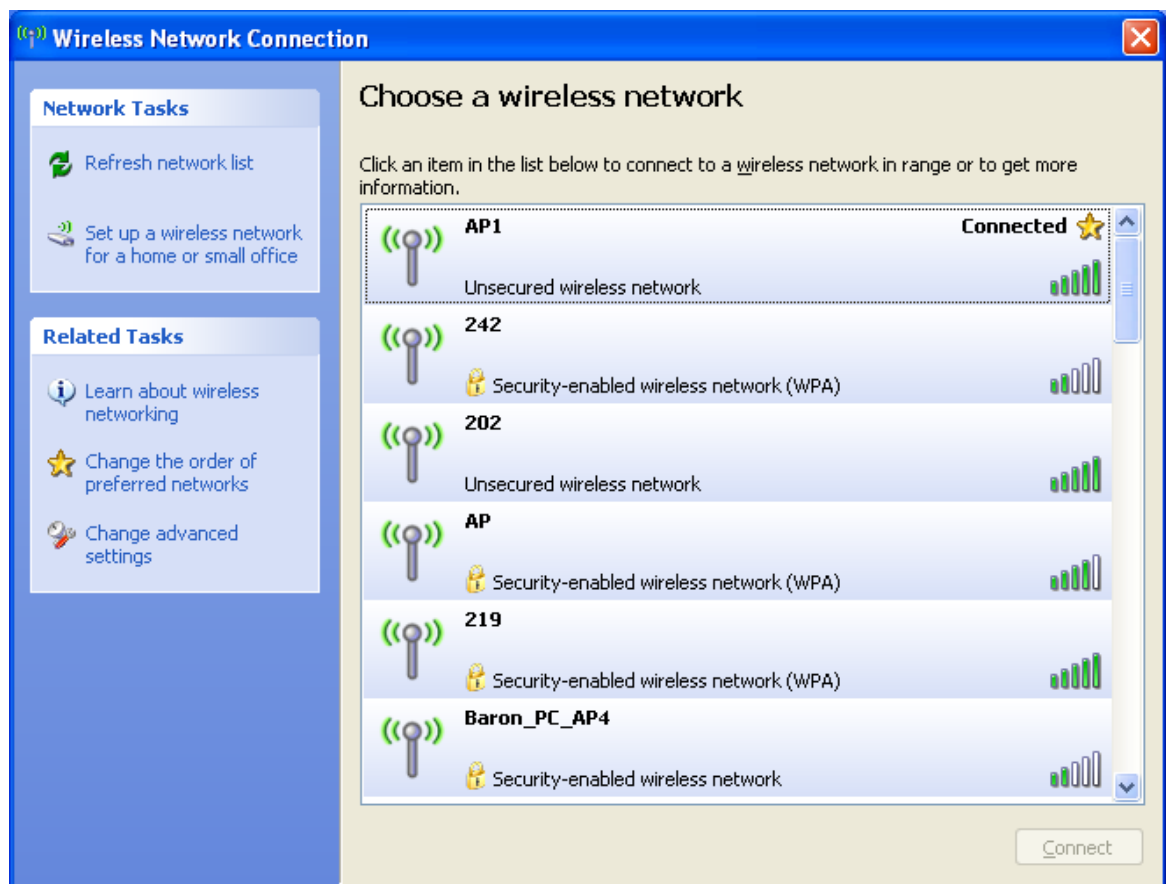


Figure 1-8 Connect AP : AP1 successfully

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.

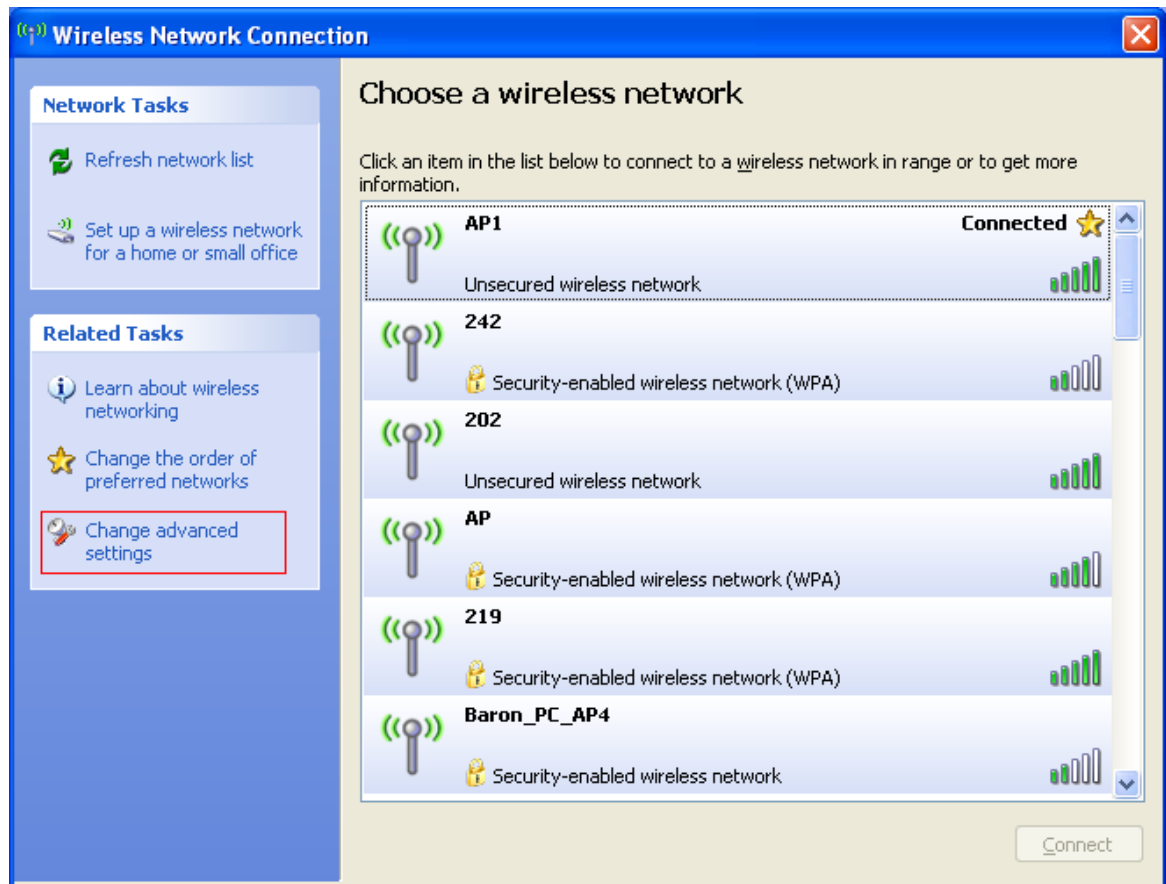


Figure 1-9 Click "Change advanced settings"

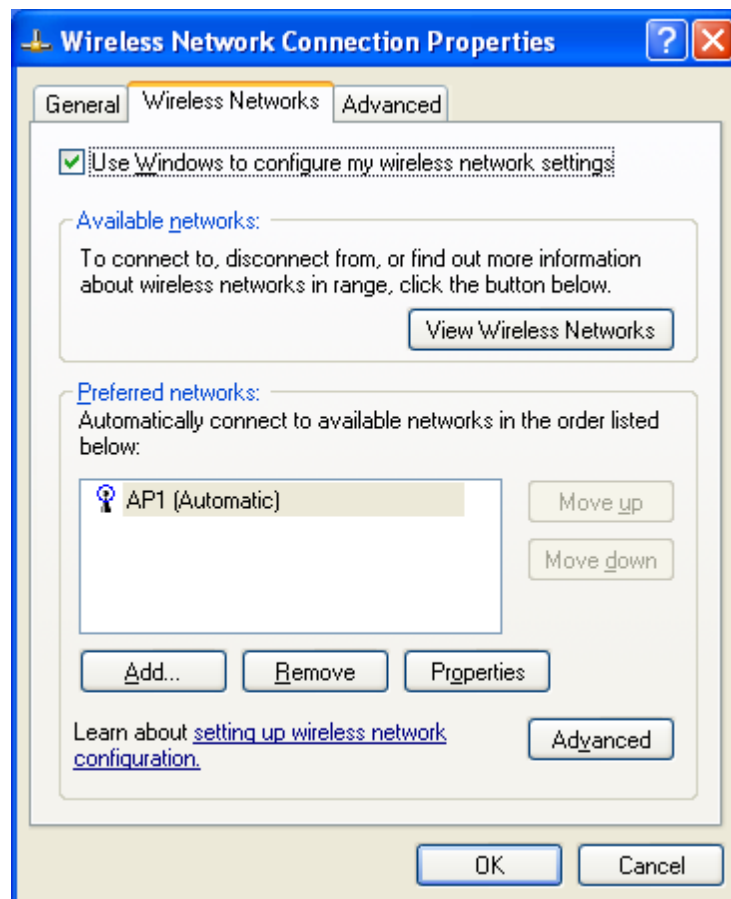


Figure 1-10 Choose the "Wireless Networks" tab

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

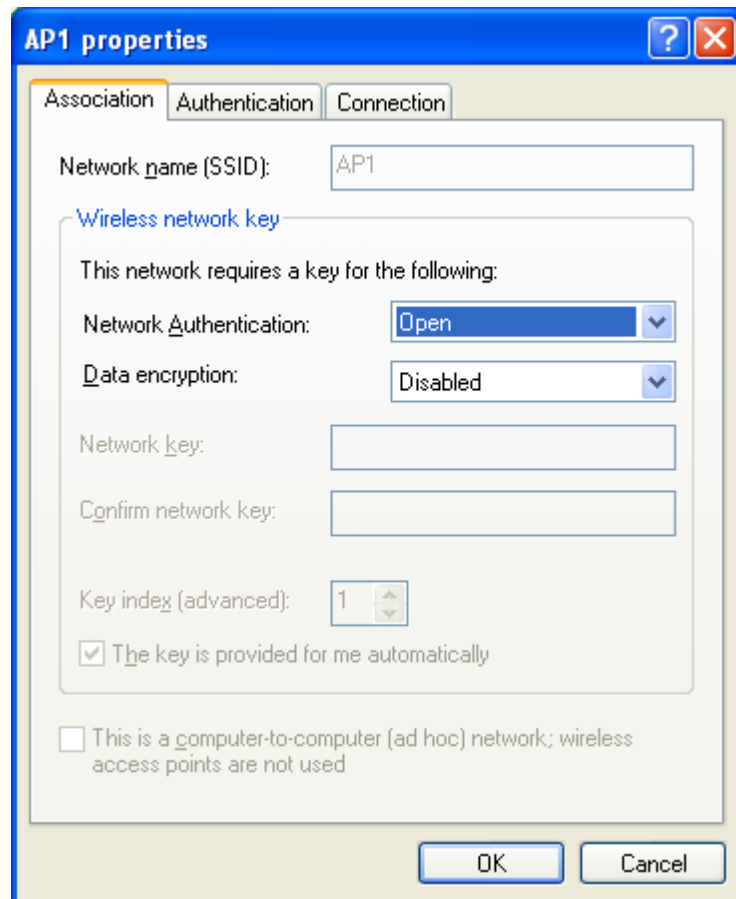


Figure 1-11 AP's properties

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

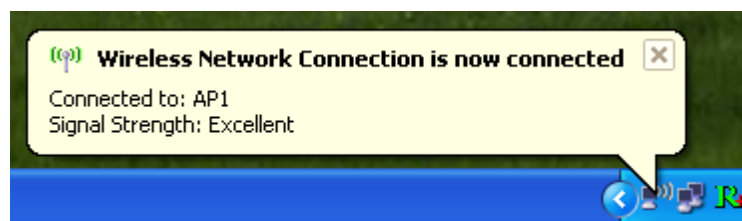


Figure 1-12 Network connection status

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.

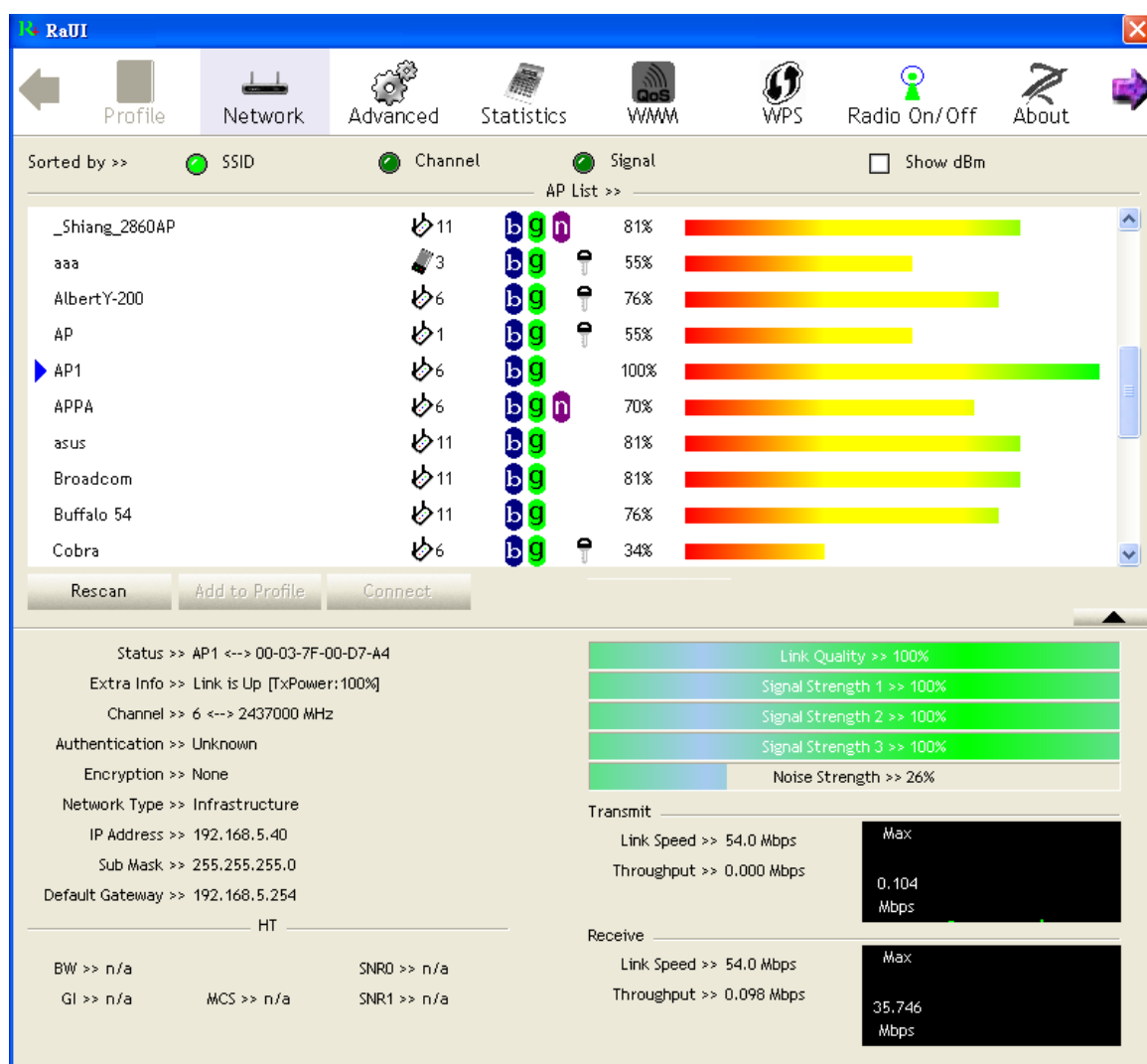


Figure 1-13 Show connection status by using WZC to initiate the connection

4.2 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.

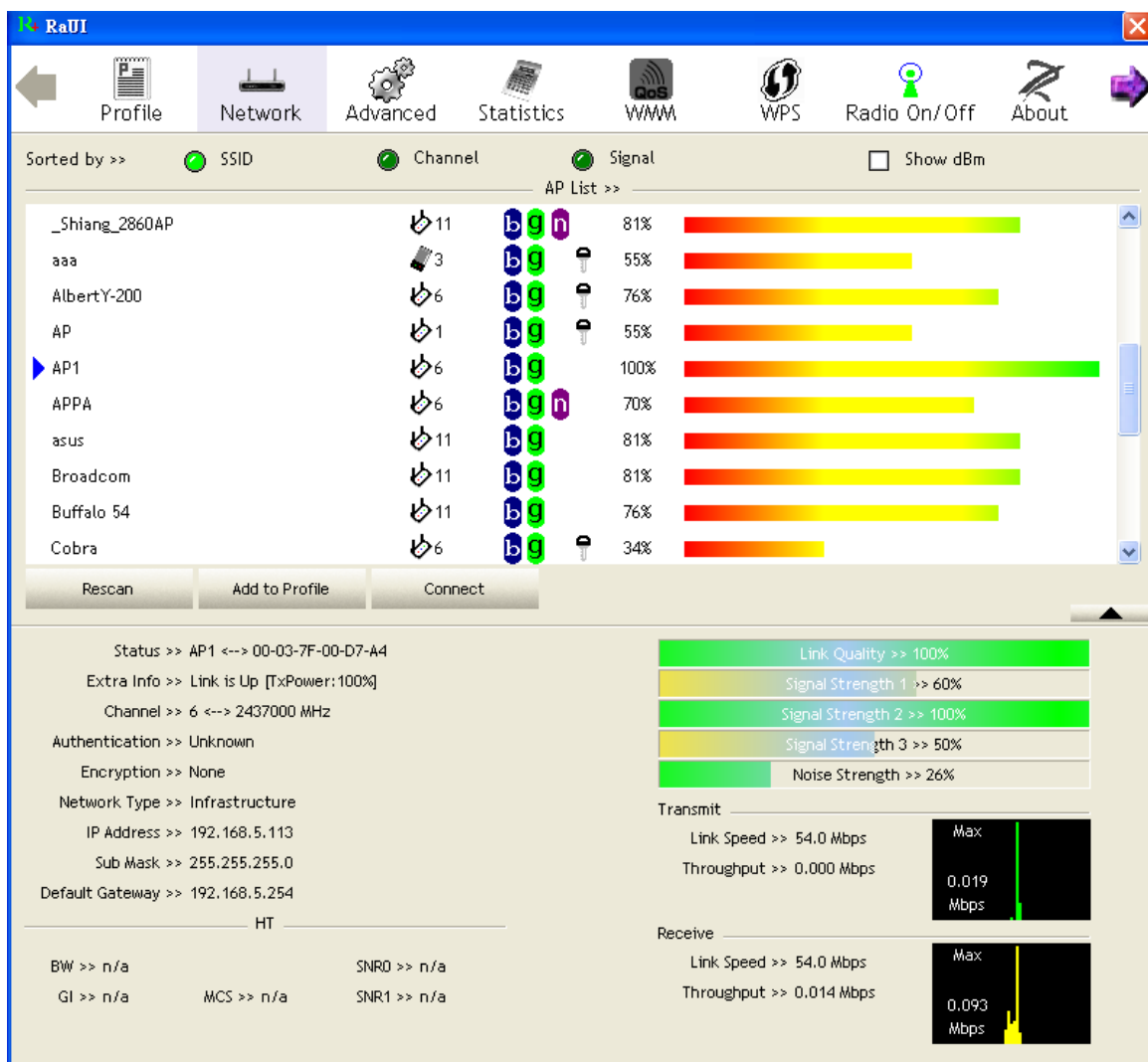


Figure 2-1-1 RaUI section introduction

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.

The screenshot shows a web-based interface for managing network profiles. On the left, there is a large empty box labeled "Profile List". Below this box are four buttons: "Add", "Edit", "Delete", and "Activate". On the right side, there is a list of configuration options, each followed by a double right-pointing arrow (>>): "Profile Name", "SSID", "Network Type", "Authentication", "Encryption", "Use 802.1x", "Channel", "Power Save Mode", "Tx Power", "RTS Threshold", and "Fragment Threshold".

Figure 2-1-5 Profile page

The screenshot displays a network scan results page. At the top, there are sorting options: "Sorted by >>" followed by radio buttons for "SSID", "Channel", and "Signal", and a checkbox for "Show dBm". Below this is a table of detected Access Points (APs). The table has columns for AP Name, Channel, Signal Strength (represented by a signal icon and a percentage), and a visual signal strength bar. The APs listed are: _Shiang_2860AP (Channel 11, 81%), aaa (Channel 3, 55%), AlbertY-200 (Channel 6, 76%), AP (Channel 1, 55%), AP1 (Channel 6, 100%), APPA (Channel 6, 70%), asus (Channel 11, 81%), Broadcom (Channel 11, 81%), Buffalo 54 (Channel 11, 76%), and Cobra (Channel 6, 34%). At the bottom of the table are three buttons: "Rescan", "Add to Profile", and "Connect".

Figure 2-1-6 Network page

The screenshot shows an advanced configuration page for a wireless network. It includes several checkboxes and input fields. At the top, "Wireless mode >>" is set to "2.4+5G". There is a checkbox for "Enable CCX (Cisco Compatible eXtensions)". Below it are checkboxes for "Turn on CCKM" and "Enable Radio Measurements". A checkbox for "Non-Serving Channel Measurements limit" is followed by a text input field containing "250" and the unit "ms (0-2000)". Other checkboxes include "Enable TX Burst", "Enable TCP Window Size", "Fast Roaming at" (with a dropdown set to "-70 dBm"), and "Show Authentication Status Dialog". A section labeled "Select Your Country Region Code" contains two dropdown menus: "11 B/G >>" set to "0: CH1-11" and "11 A >>" set to "7: CH 36,40,44,48,52,56,60,64,100". An "Apply" button is at the bottom left.

Figure 2-1-7 Advance page

Transmit		Receive	
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

Reset Counter

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

Apply

Tear Down

Figure 2-1-9 WMM page

WPS AP List

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

WPS Profile List

--	--

WPS Associate IE ☒ WPS Probe IE ☒ Automatically select the AP ☐

Progress >> 0%

Rescan

Information

Pin Code

64893945 Renew

Config Mode

Enrollee

Detail

Connect

Rotate

Disconnect

Export Profile

Delete

Figure 2-1-10 WPS page

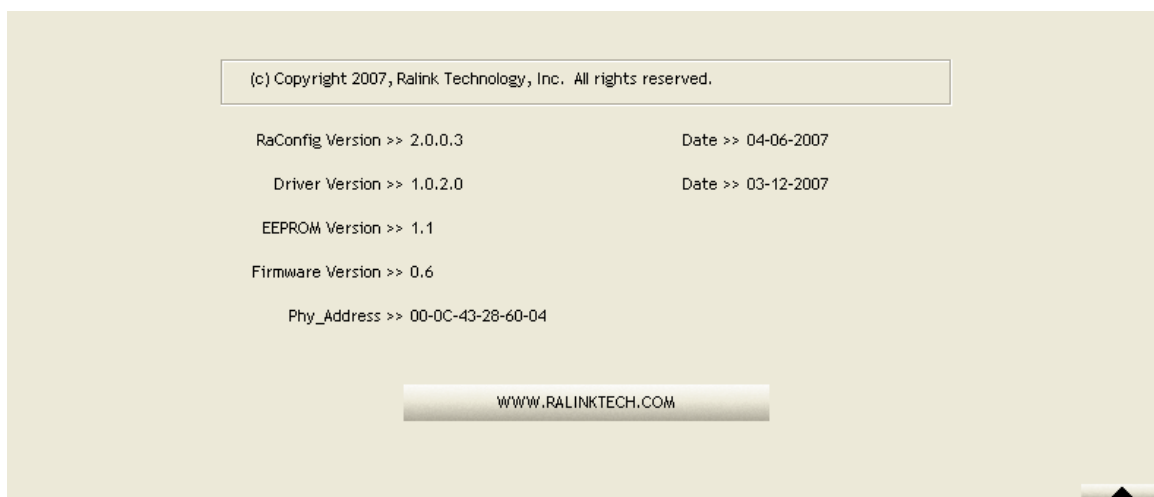


Figure 2-1-11 About page

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.

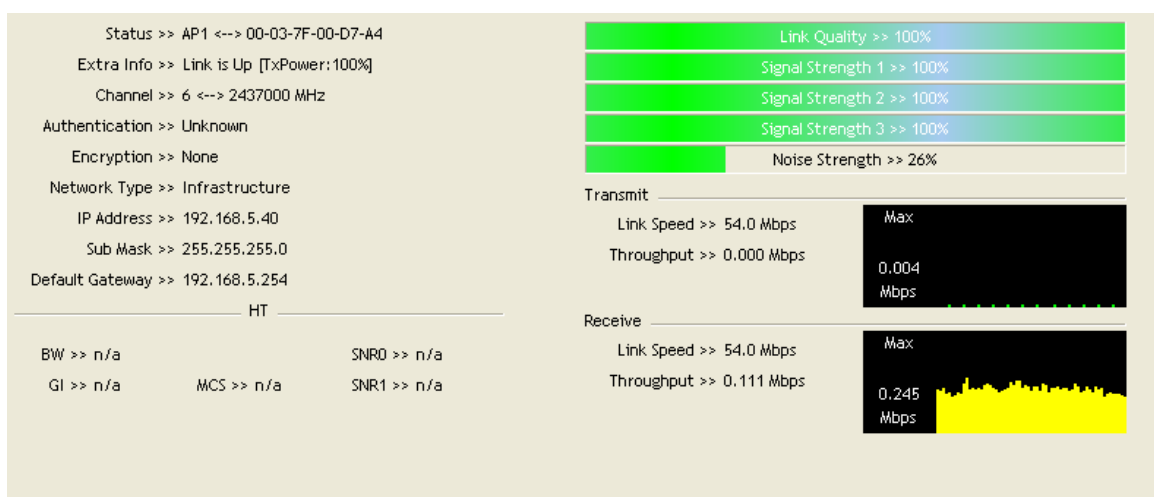


Figure 2-1-12 Link Status



Figure 2-1-13 Authentication Status

General WPS CCX

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

OK

Figure 2-1-14 AP's Information

Card Name >> Ralink 802.11n Wireless LAN Card

Profile Name >> PROF1

Message >> Invalid identity or password

Identity >>

Password >>

OK Cancel

Figure 2-1-15 Retry the connection

System Config Auth. \ Encry. 8021X

Authentication >> WPA Encryption >> TKIP

WPA Preshared Key >>

Wep Key

Key#1	Hexadecimal	<input type="text"/>
Key#2	Hexadecimal	<input type="text"/>
Key#3	Hexadecimal	<input type="text"/>
Key#4	Hexadecimal	<input type="text"/>

☐ Show Password

OK Cancel






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:

-  : Indicates the connected and signal strength is good.
-  : Indicates the connected and signal strength is normal.
-  : Indicates that it is not yet connected.
-  : Indicates that a wireless NIC can not be detected.
-  : 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.

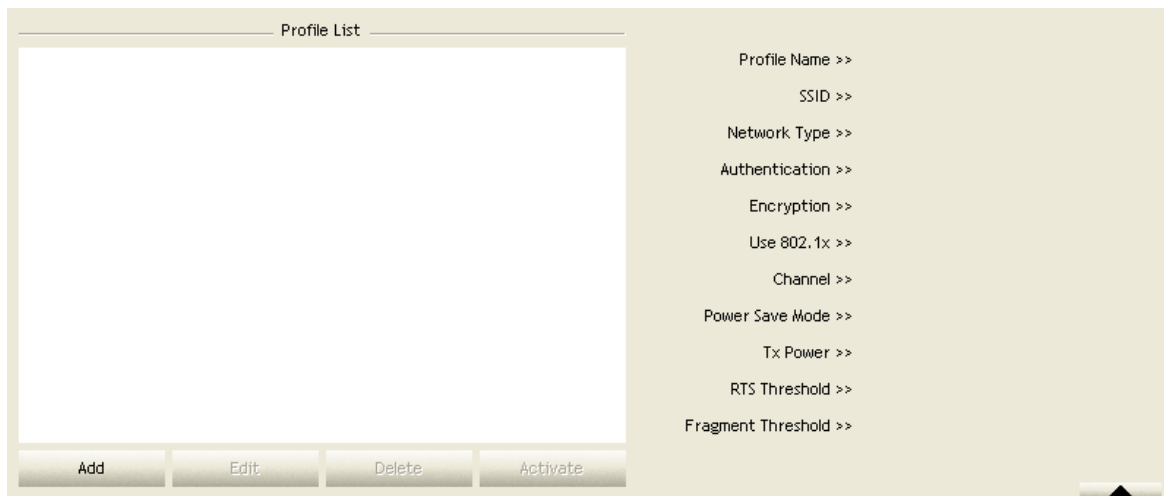








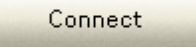
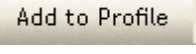
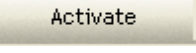


Figure 2-2-1 Profile function

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:

- 1  : Indicates if a connection made from the currently activated profile.
- 2  : Indicates if the connection has failed on a currently activated profile.
- 3  : Indicates the network type is infrastructure mode.
- 4  : Indicates the network type is in Ad-hoc mode.
- 5  : Indicates if the network is security-enabled.
- 6  : Click to add a new profile.
- 7  : Click to edit an existing profile.
- 8  : Deletes an existing profile.
- 9  : Activates the selected profile.
- 10  : Shows information of the related status section.
- 11  : 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.

The figure consists of two screenshots of the Profile Editor dialog box. The top screenshot shows the 'System Config' tab. It has a 'Profile Name' field with 'PROF1', an 'SSID' dropdown with 'AP1', a 'Network Type' dropdown with 'Infrastructure', a 'Tx Power' dropdown with 'Auto', a 'Preamble' dropdown with 'Auto', and 'Power Save Mode' with radio buttons for 'CAM' and 'PSM' (both selected). There are also 'RTS Threshold' and 'Fragment Threshold' fields with sliders and input boxes. The bottom screenshot shows the 'Auth. \ Encry.' tab. It has 'Authentication' and 'Encryption' dropdowns (set to 'Open' and 'None' respectively), a 'WPA Preshared Key' field, a 'Wep Key' field, and four 'Wep Key' entries (Key#1 to Key#4) each with a radio button (all selected) and a 'Hexadecimal' dropdown. There is also a 'Show Password' checkbox. Both screenshots have 'OK' and 'Cancel' buttons at the bottom.

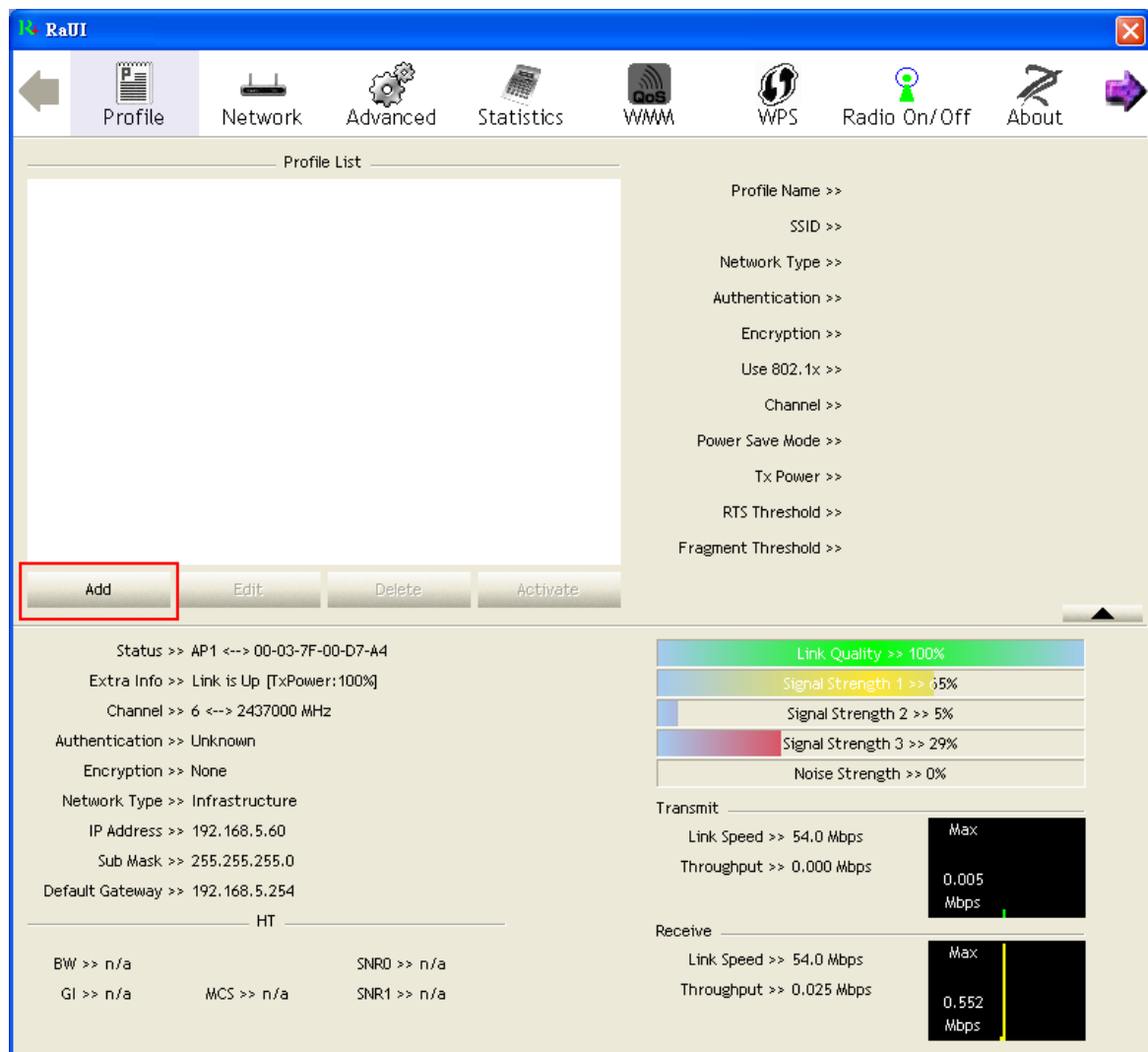
Figure 2-2-2 Configuration

- 1 Profile Name: The user can choose 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 mode. 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.
- ⑧ 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.
- ⑨ 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.
- ⑩ 802.1x Setting: This is introduced in the topic of "Section 3-2 : 802.1x Setting".
- ⑪ 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.
- ⑫ 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 : 26 Hex characters.
 - 3. ASCII - 40bits : 5 ASCII characters.
 - 4. ASCII - 128bits : 13 ASCII characters.

4.2.2.3 Example to Add Profile in Profile

- ① Click "Add" below the Profile List.



2 The "Add Profile" will appear.

Profile List

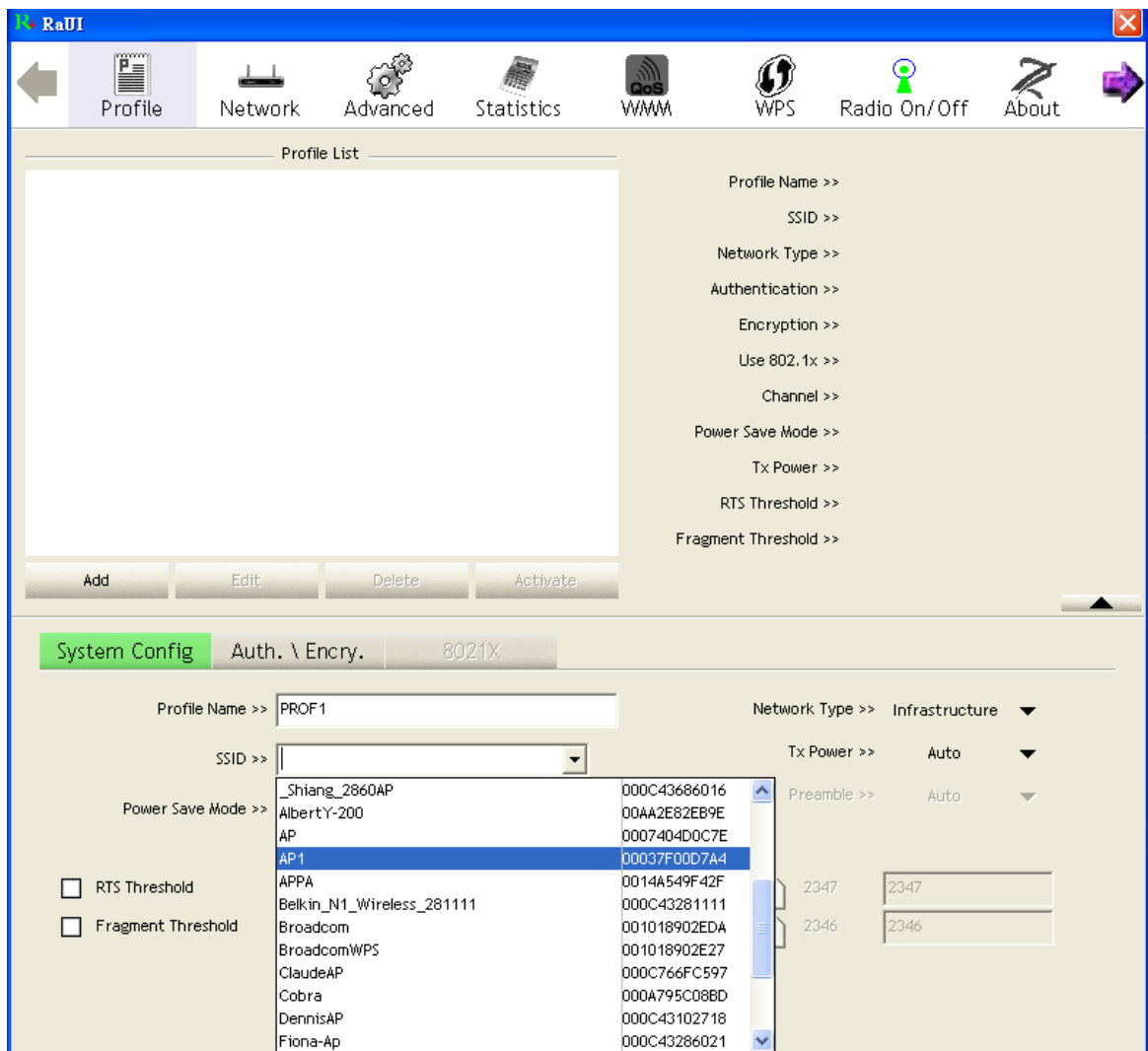
Profile Name >>
SSID >>
Network Type >>
Authentication >>
Encryption >>
Use 802.1x >>
Channel >>
Power Save Mode >>
Tx Power >>
RTS Threshold >>
Fragment Threshold >>

Add Edit Delete Activate

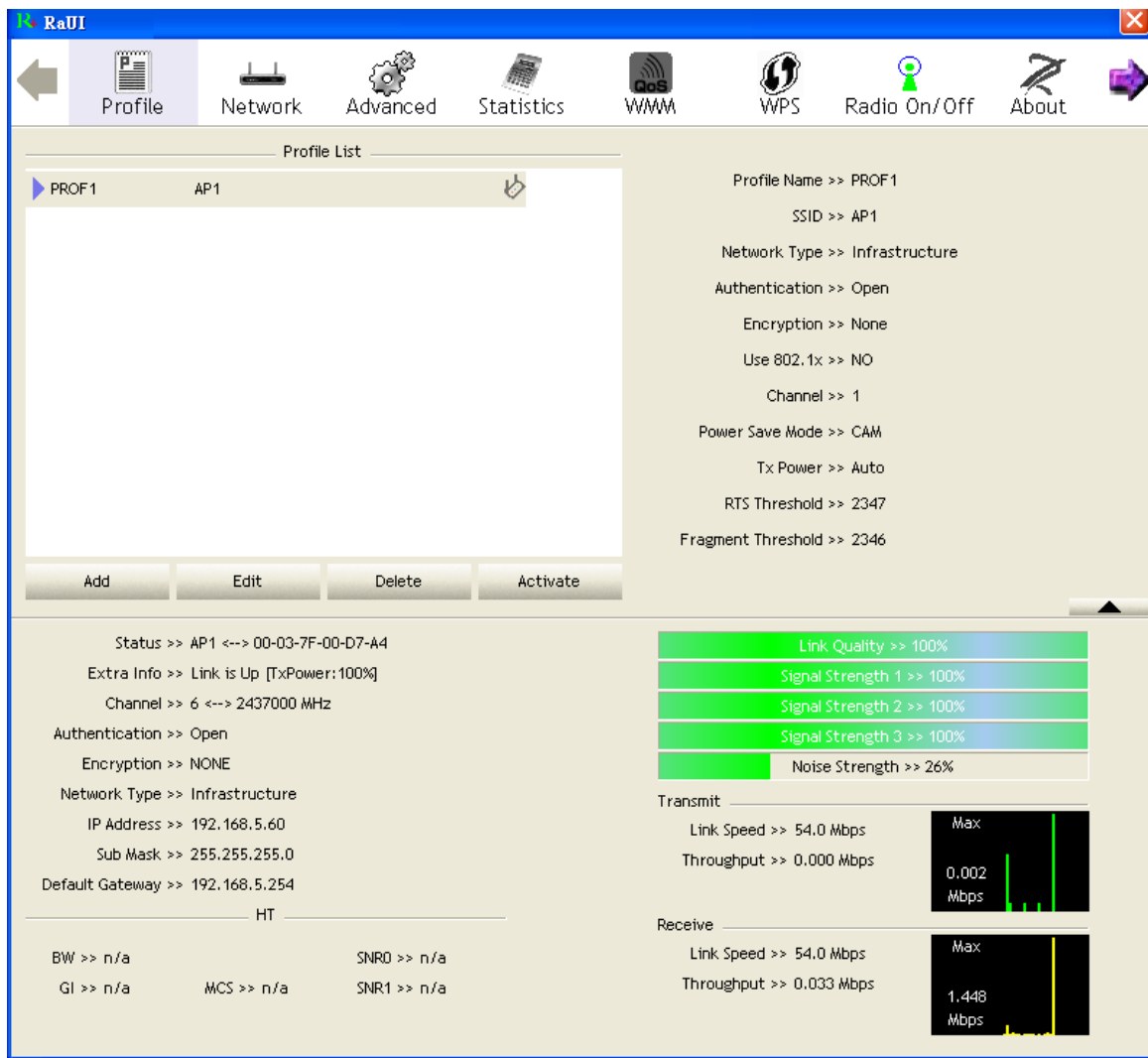
System Config Auth. \ Encry. 802.1X

Profile Name >> PROF1
SSID >>
Power Save Mode >> ☒ CAM ☒ PSM
Network Type >> Infrastructure
Tx Power >> Auto
Preamble >> Auto
☐ RTS Threshold 0 2347 2347
☐ Fragment Threshold 256 2346 2346
OK Cancel

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



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



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.

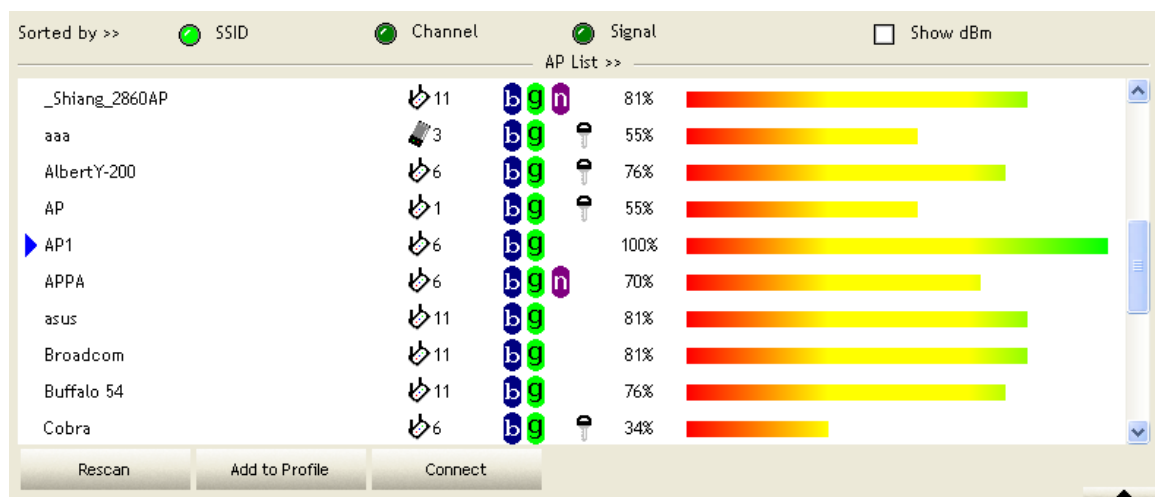



Figure 2-3-1-1 Network function


Definition of each field :

- 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.

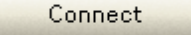
Icons and buttons :

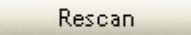
- ① : Indicates that the connection is successful.
- ② : Indicates the network type is in infrastructure mode.
- ③ : Indicates the network type is in Ad-hoc mode.
- ④ : Indicates that the wireless network is security-enabled.
- ⑤ : Indicates 802.11a wireless mode.
- ⑥ : Indicates 802.11b wireless mode.

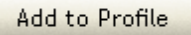
7  : Indicates 802.11g wireless mode.

8  : Indicates 802.11n wireless mode.

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

10  : Button to connect to the selected network.

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

12  : 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.

13  : Shows the Status Section.

14  : 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:

- 1 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.

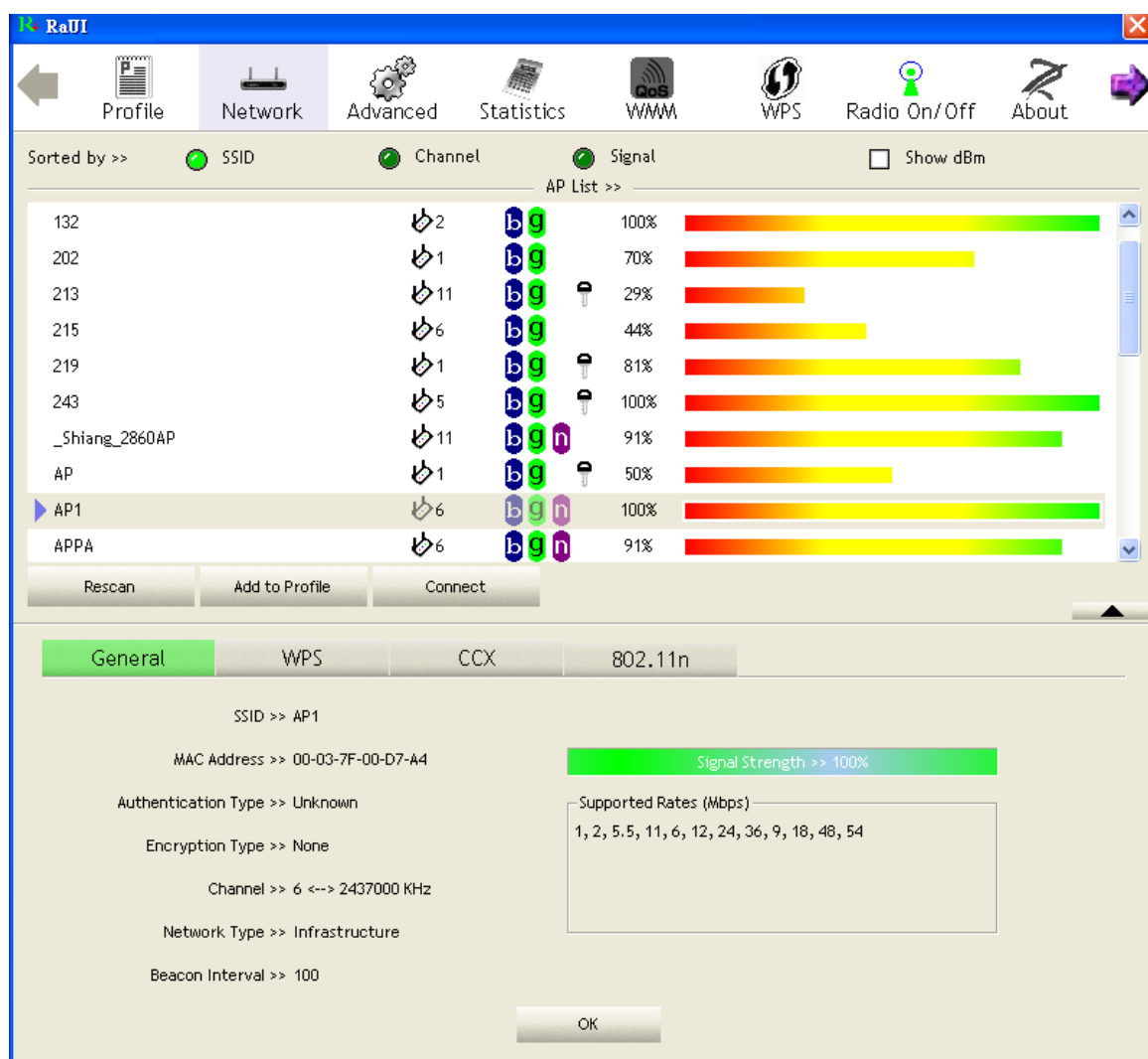


Figure 2-3-1-2 General information about the Access Point

② 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	USB (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	PushButton (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 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".



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

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

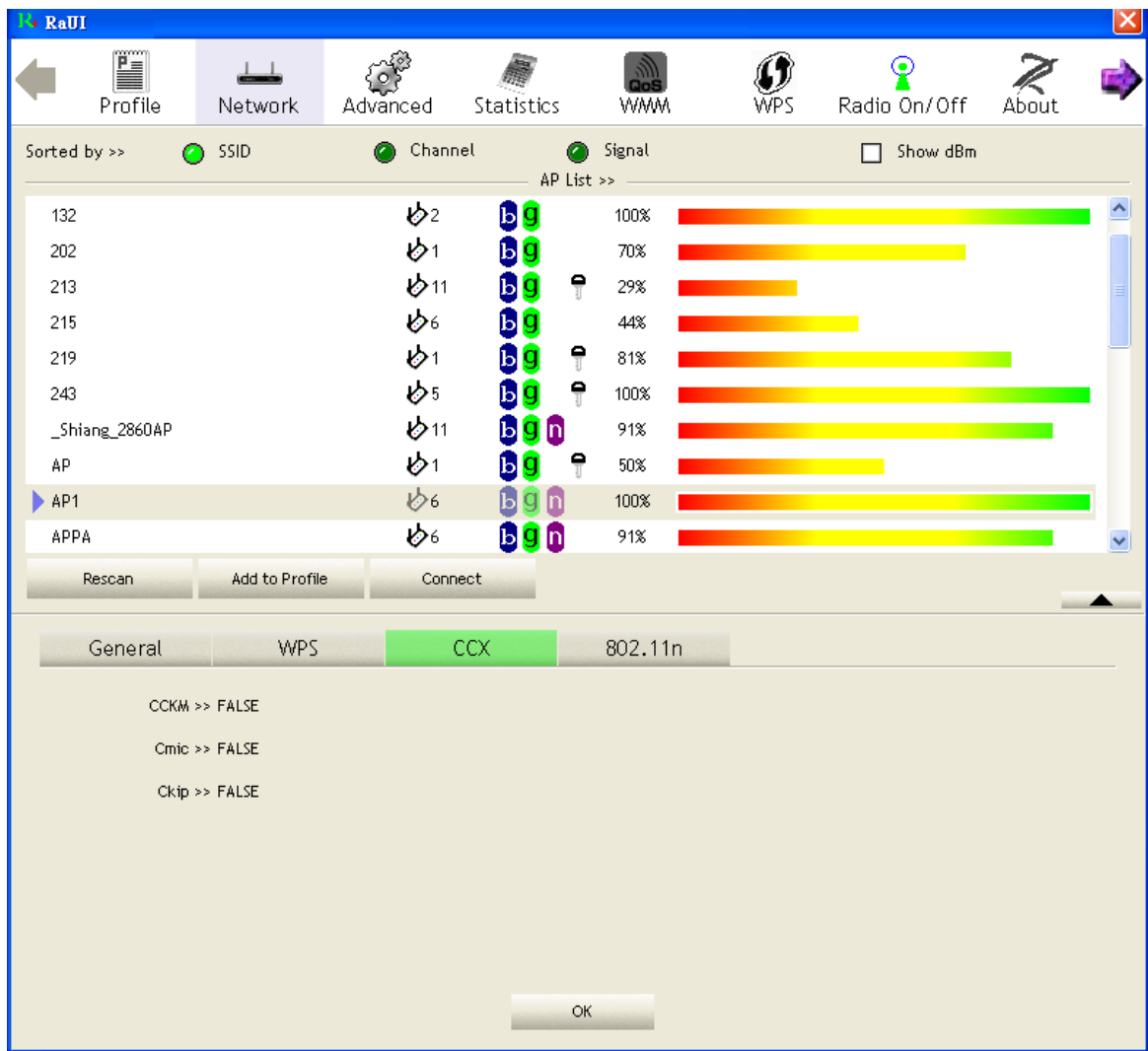


Figure 2-3-1-4 CCX information about AP's detail information

④ 802.11n information contains some related 802.11n information. It is shown in Figure 2-3-1-5.

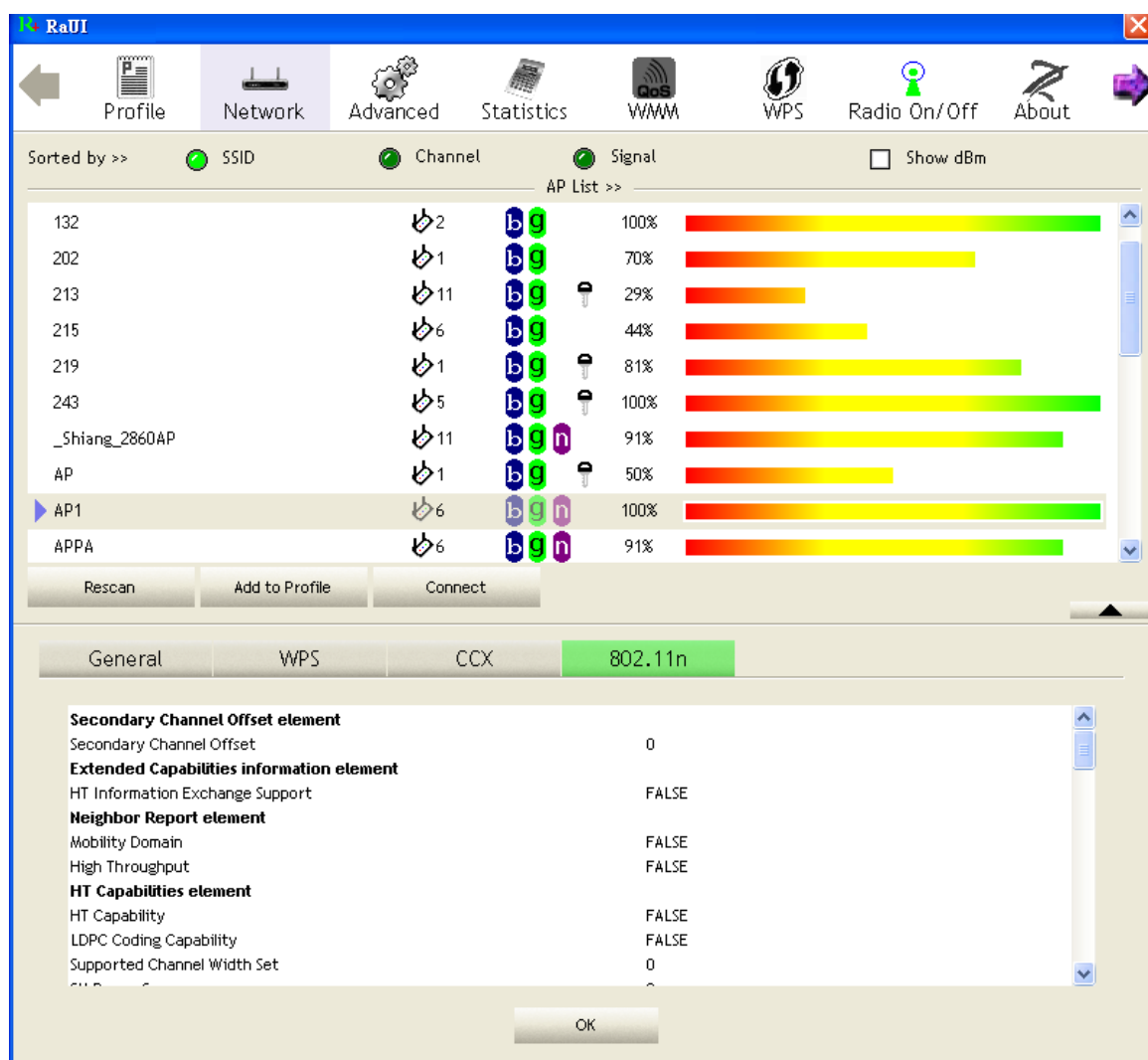


Figure 2-3-1-5 802.11n information

4.2.3.2 Example on Adding Profile in Network

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

RaUI

Profile | **Network** | Advanced | Statistics | WMM | WPS | Radio On/Off | About

Sorted by >> ☒ SSID ☒ Channel ☒ Signal ☐ Show dBm

AP List >>

AP Name	Channel	Signal	Strength
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%

Rescan | Add to Profile | Connect

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 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

7.498 Mbps

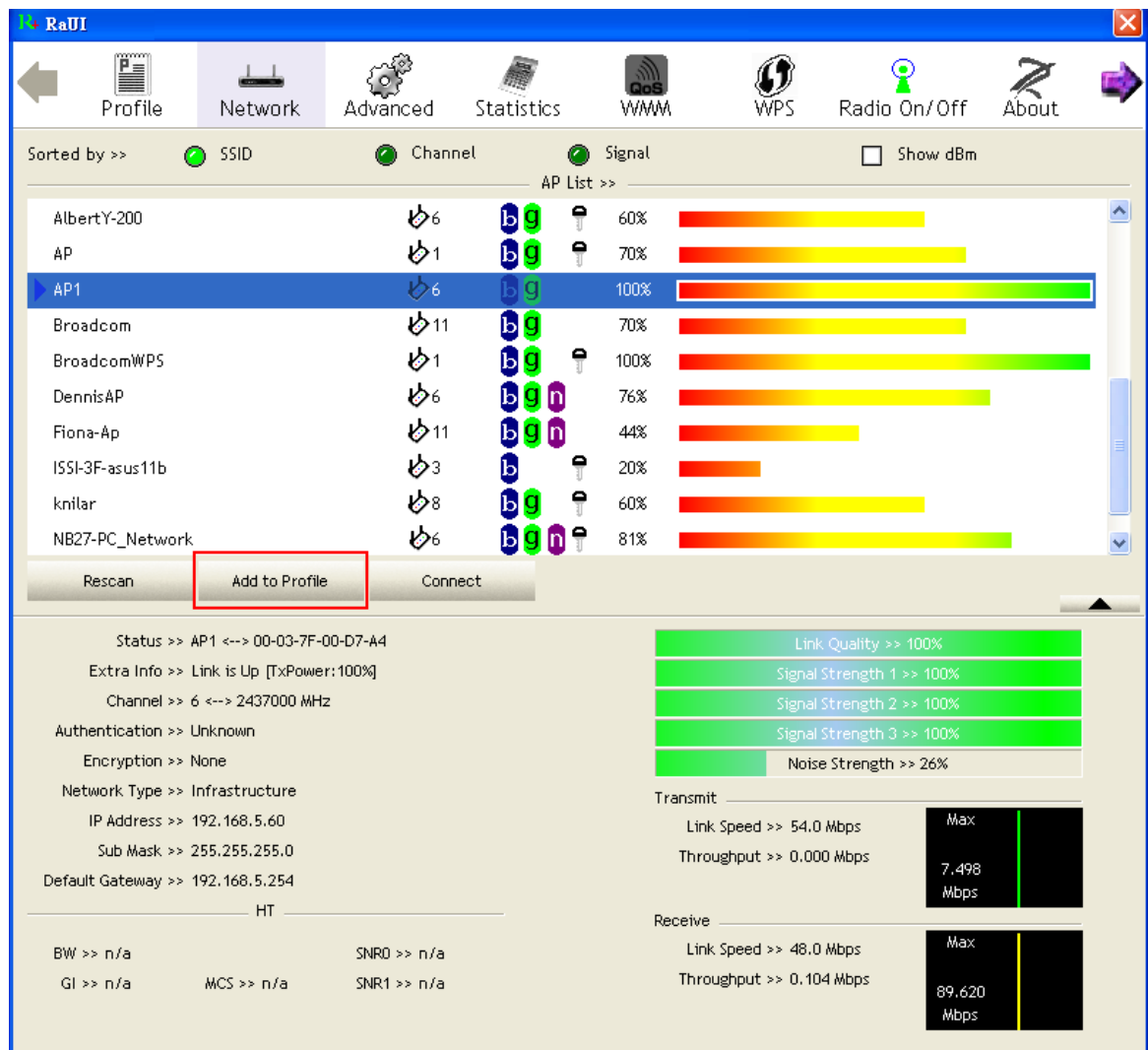
Receive

Link Speed >> 48.0 Mbps

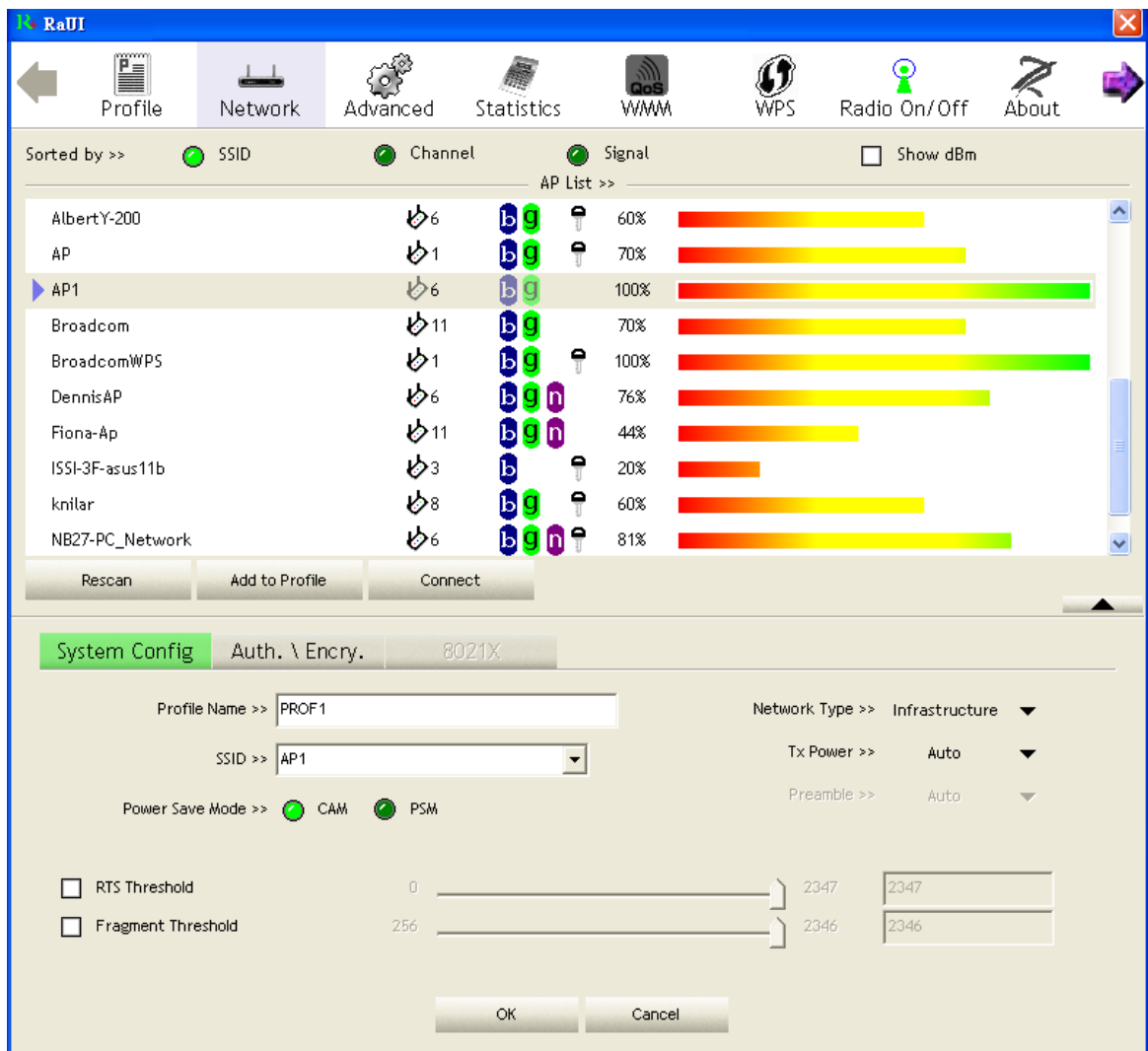
Throughput >> 0.104 Mbps

89.620 Mbps

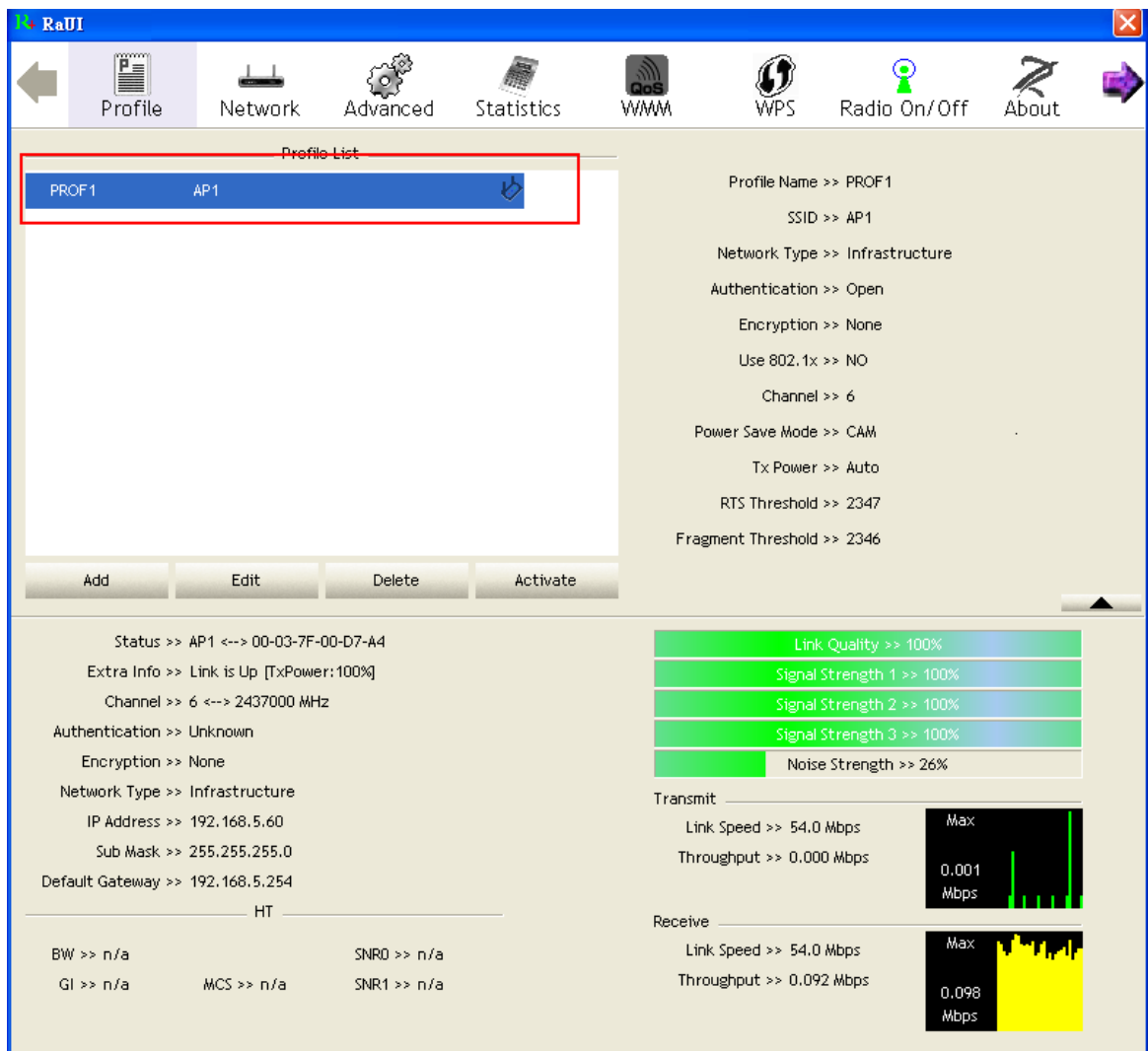
2 Click "Add to Profile"



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



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



4.2.4 Advanced

4.2.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

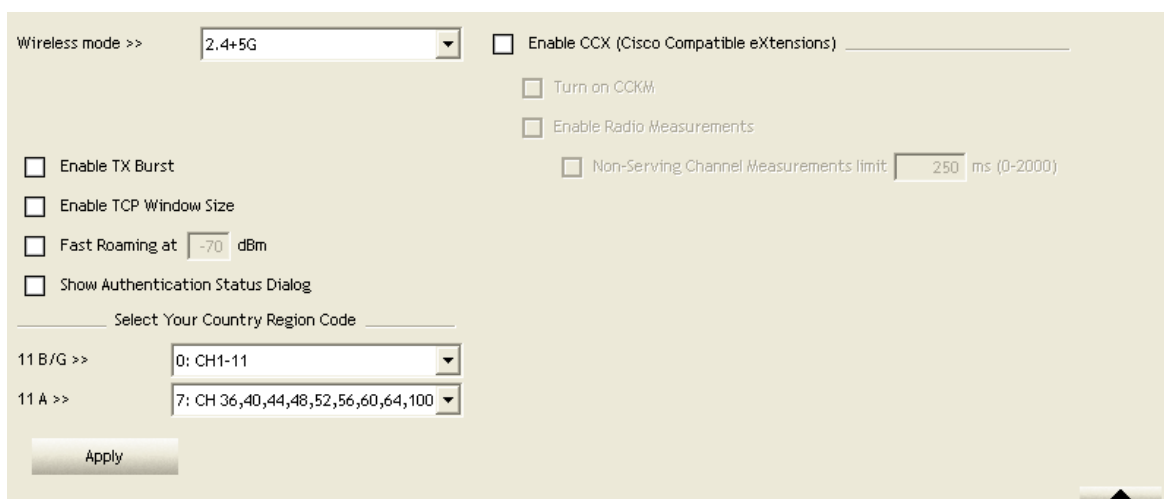




Figure 2-4 Advance function

- 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.)
 - ① Auto: STA will dynamically change as AP announcement.
 - ② On: The frames are always sent with protection.
 - ③ 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.
 - ① LEAP turn on CCKM.
 - ② Enable Radio Measurement: can measure the channel every 0~2000 milliseconds.
- ⑩ Apply the above changes.

Icons and buttons:

- ①  : Show the Status Section information.
- ②  : Hide the Status Section information.

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.



Transmit		
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
<button>Reset Counter</button>		

Figure 2-5-1 Statistics function

Transmit Statistics:



Transmit		
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
<button>Reset Counter</button>		

- 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:

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

Reset Counter

- 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.

Icons and buttons:

- ① : Show the Status Section information.
- ② : Hide the Status Section information.

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 :

Figure 2-6-1 WMM function

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

Icons and buttons:



Show the information of Status Section.



Hide the information of Status Section.

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

- ❶ 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 >> 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.

RaUI

Profile Network Advanced Statistics WMM WPS Radio On/Off About

Profile List

PROF1 AP1

Add Edit Delete Activate

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:

1. Connect with an AP that support DLS features.
2. 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

Apply

Tear Down

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

Apply

Tear Down

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

Apply Tear Down

Describe "DLS Status" as follow :

① 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 users local MAC address and Timeout Value are displayed.

② 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

Apply Tear Down

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

Apply Tear Down

3 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

Apply Tear Down

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

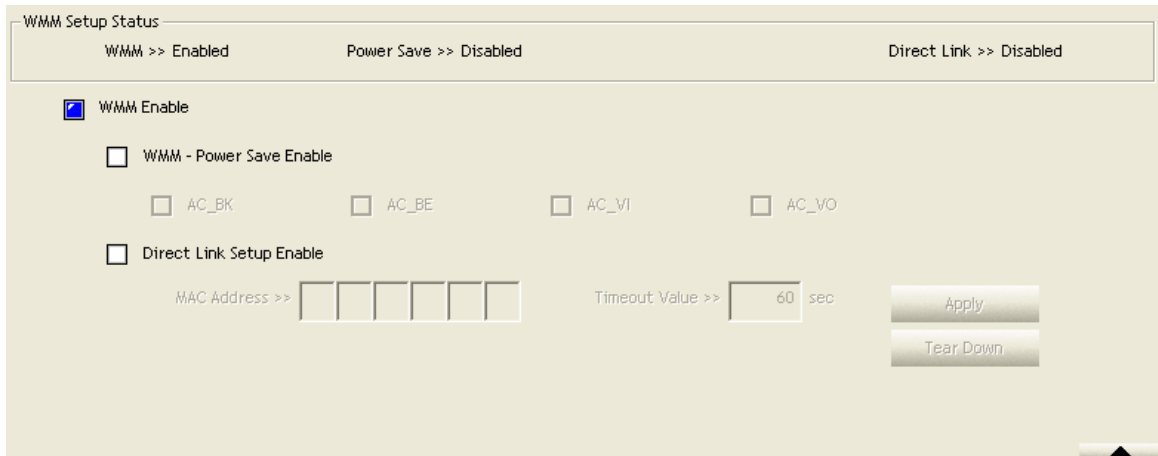
MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec

Apply Tear Down

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

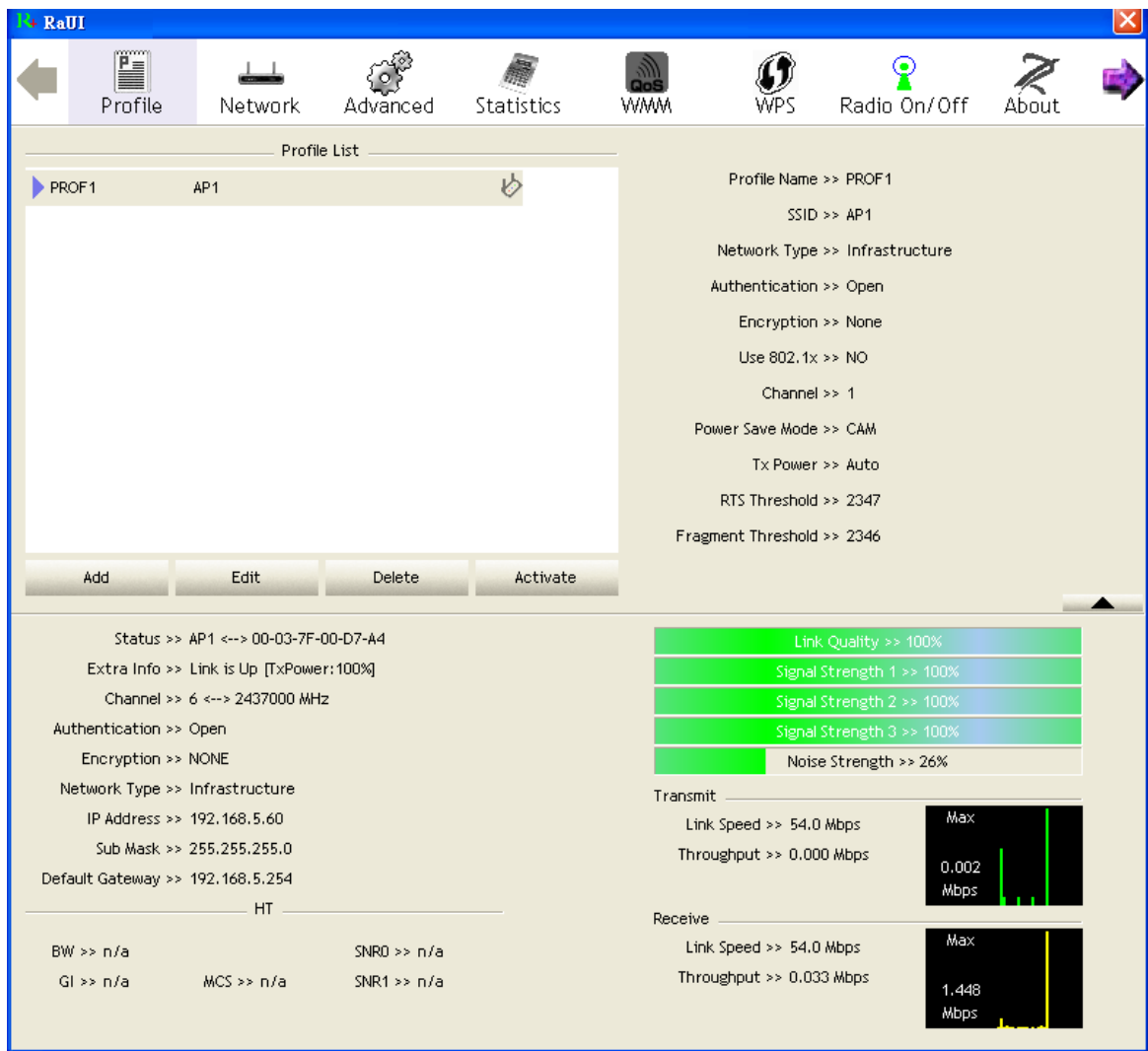
If you want to use "WMM-Power Save" or "Direct Link" you must enable WMM. The setting method of enabling WMM indicates as follows:

- 1 Click "WMM Enable".



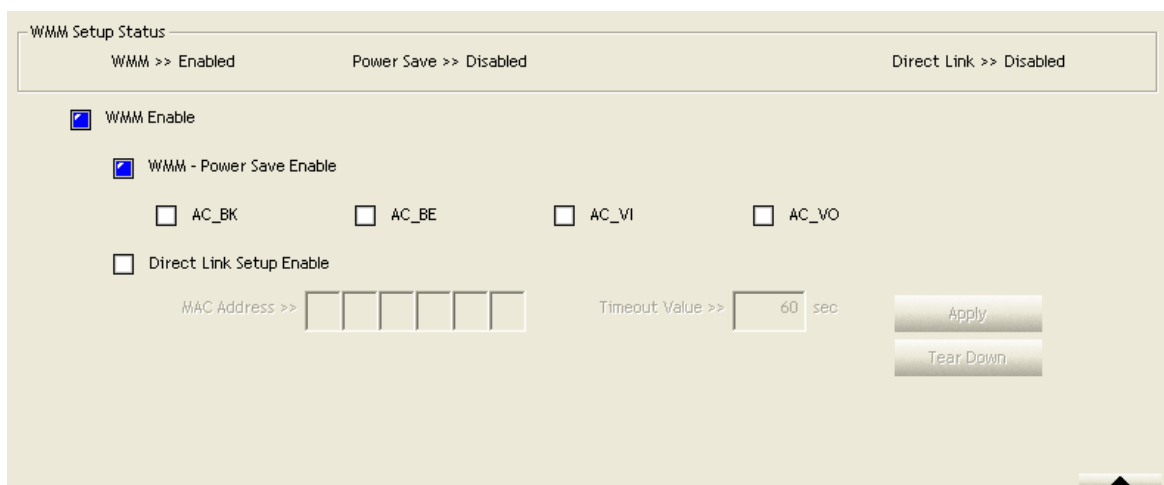
The image shows a "WMM Setup Status" configuration window. At the top, there are three status indicators: "WMM >> Enabled", "Power Save >> Disabled", and "Direct Link >> Disabled". Below these, there are several checkboxes and input fields. The "WMM Enable" checkbox is checked. Below it, the "WMM - Power Save Enable" checkbox is unchecked. Under "WMM - Power Save Enable", there are four unchecked checkboxes: "AC_BK", "AC_BE", "AC_VI", and "AC_VO". Below these, the "Direct Link Setup Enable" checkbox is unchecked. Under "Direct Link Setup Enable", there is a "MAC Address >>" field with six empty boxes, and a "Timeout Value >>" field with the value "60" and the unit "sec". At the bottom right, there are two buttons: "Apply" and "Tear Down".

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

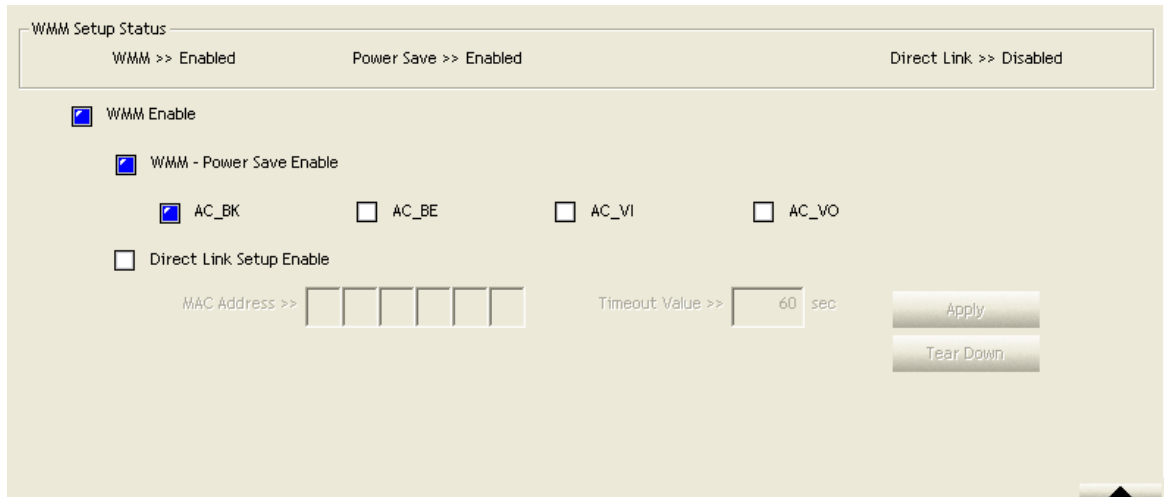


4.2.6.4 Example to Configure to Enable WMM - Power Save

1 Click "WMM-Power Save Enable".



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 >> sec

Apply

Tear Down

4.2.7 WPS

4.2.7.1 WPS

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



Figure 2-7-1 WPS function

- ❶ **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.
- ❷ **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.
- ❸ **Rescan:** Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.
- ❹ **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.
- ❺ **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.

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

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

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

4. 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.

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

6. 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)

Icons and buttons:

1  : Show the information of Status Section.

2  : Hide the information of Status Section.

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.



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-PSK

authentication mode, the encryption type supports both TKIP and AES.

④ 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	PushButton (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.

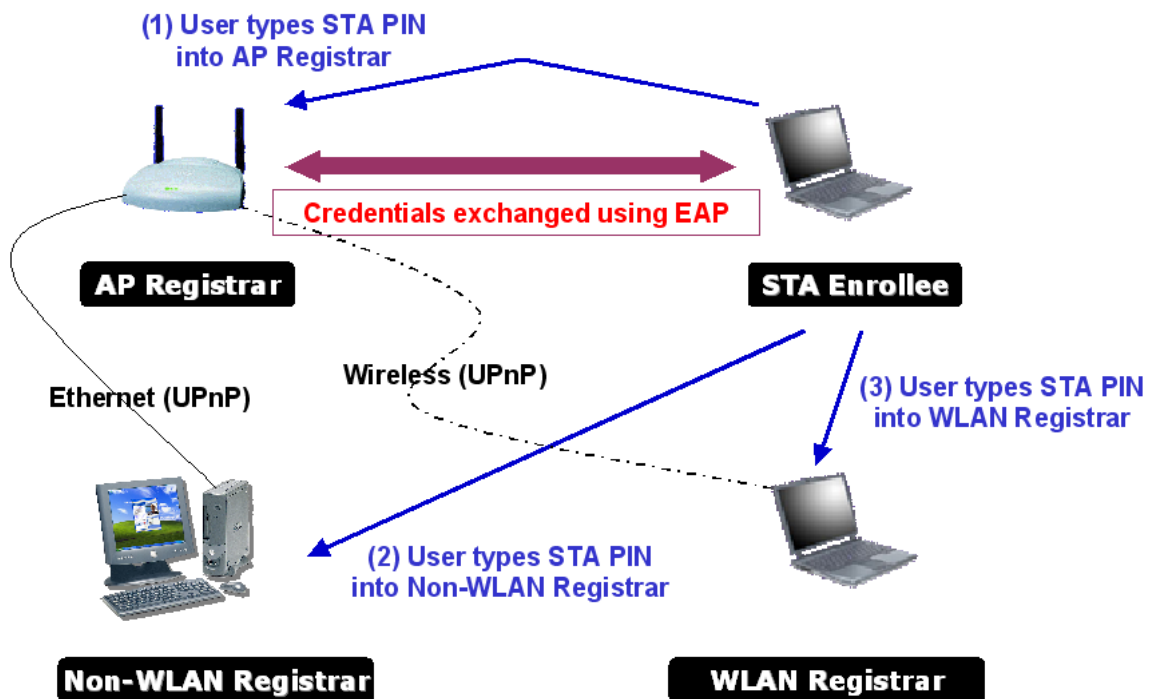
⑧ AP Setup Locked: Indicates if the AP has entered a setup locked state.

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

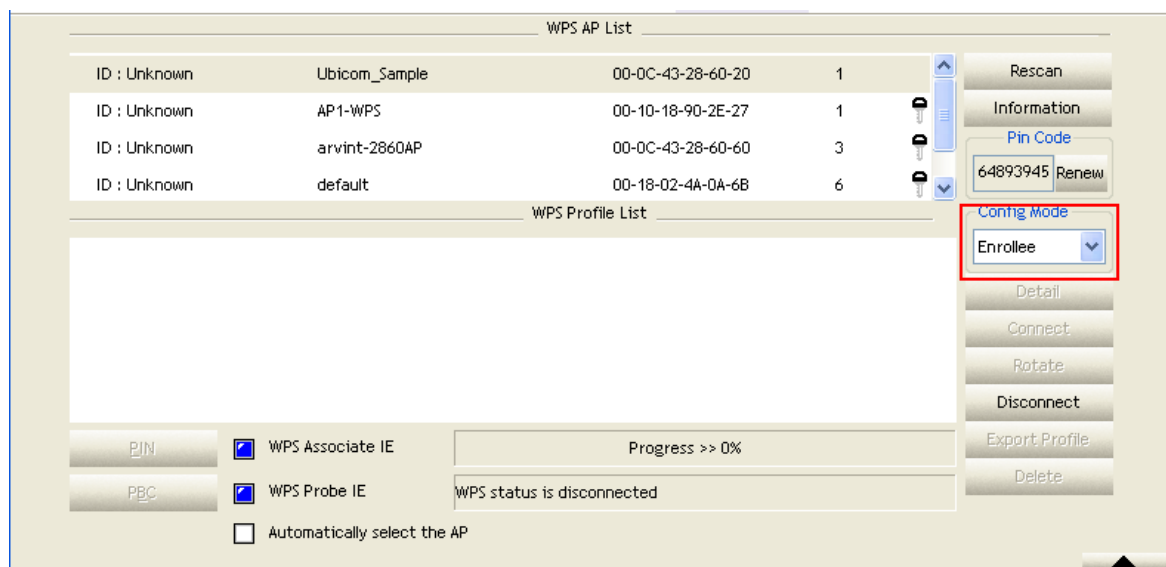
⑩ RF Bands: Indicates all the RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

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



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

WPS AP List

ID	SSID	BSSID	Count	Icon
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 ☒ WPS Associate IE Progress >> 0%

PBC ☒ WPS Probe IE WPS status is disconnected

☐ Automatically select the AP

Buttons: Rescan, Information, Pin Code, 64893945 Renew, Config Mode, Enrollee, Detail, Connect, Rotate, Disconnect, Export Profile, Delete.

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

WPS AP List

ID	SSID	BSSID	Count	Icon
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 ☒ WPS Associate IE Progress >> 0%

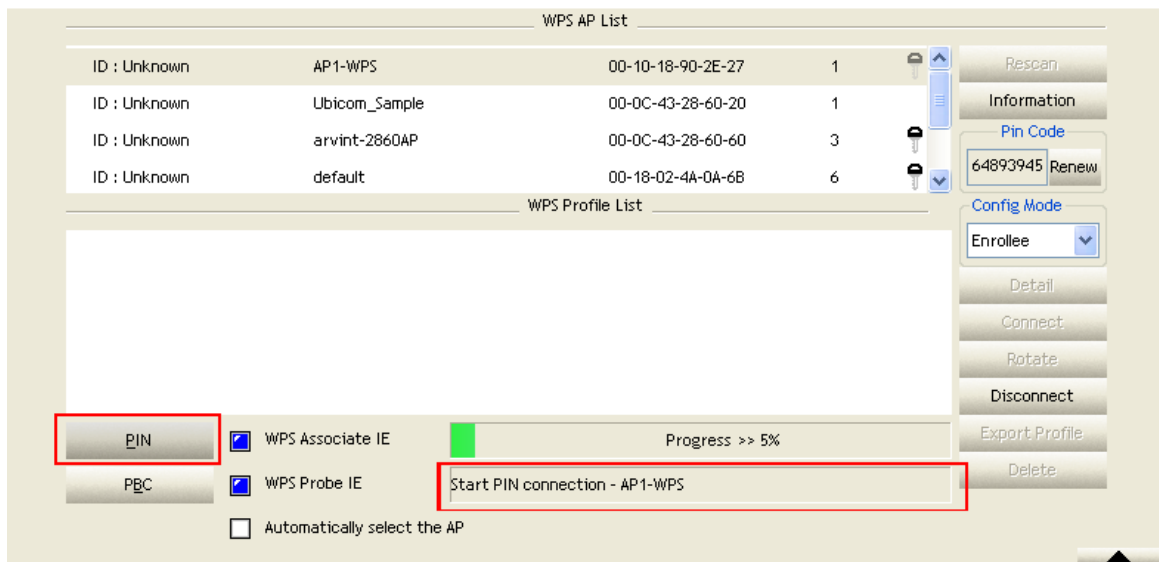
PBC ☒ WPS Probe IE WPS status is disconnected

☐ Automatically select the AP

Buttons: Rescan, Information, Pin Code, 64893945 Renew, Config Mode, Enrollee, Detail, Connect, Rotate, Disconnect, Export Profile, Delete.

- 4 Click "PIN" to enter the PIN

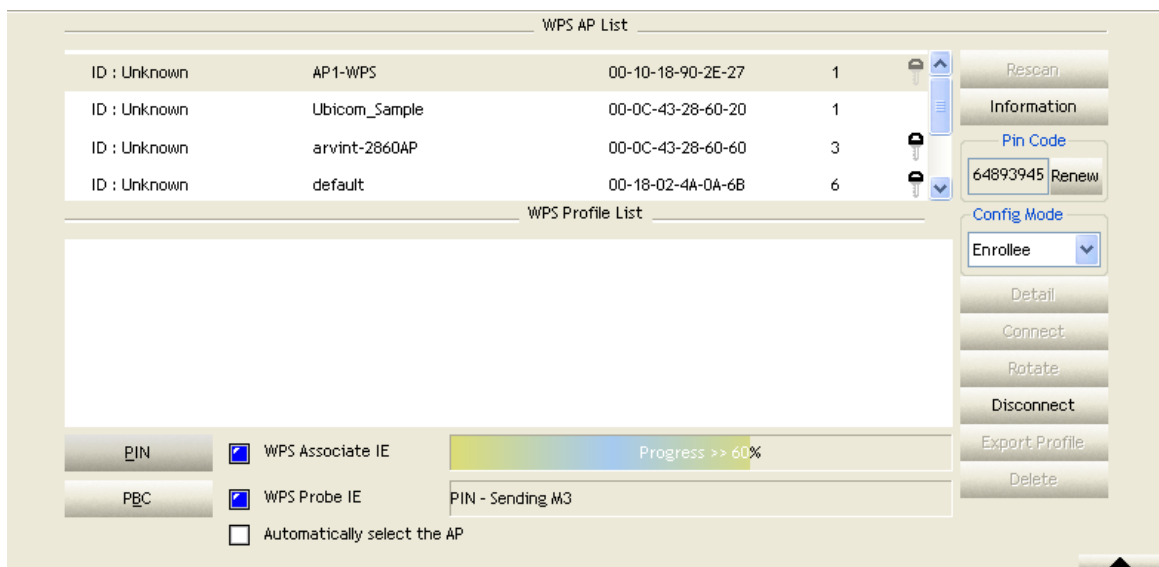
- 5 Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.



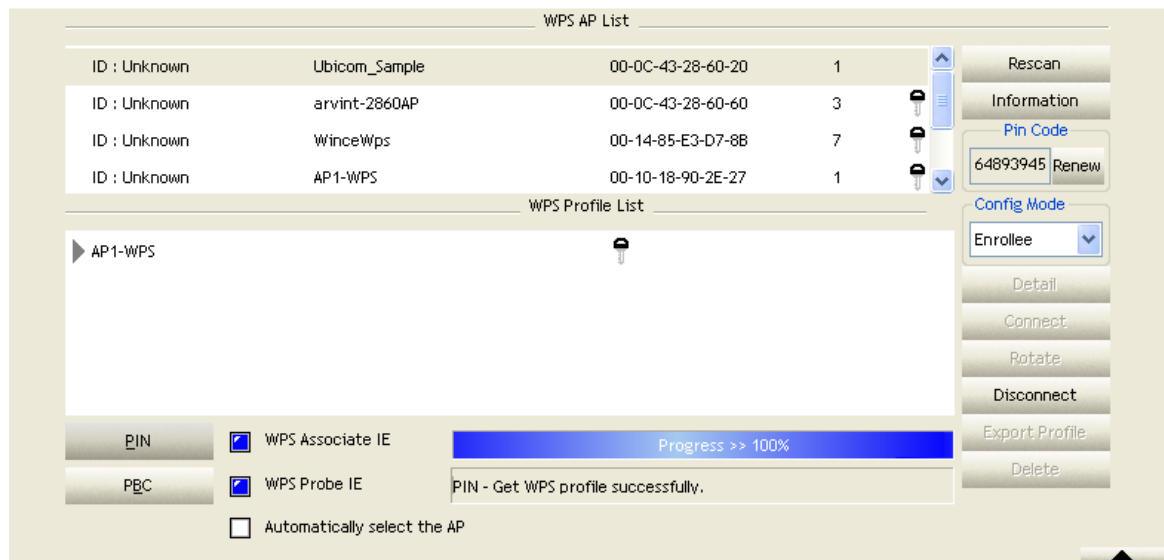
Allow of an exchange between Step 4 and Step 5.

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.

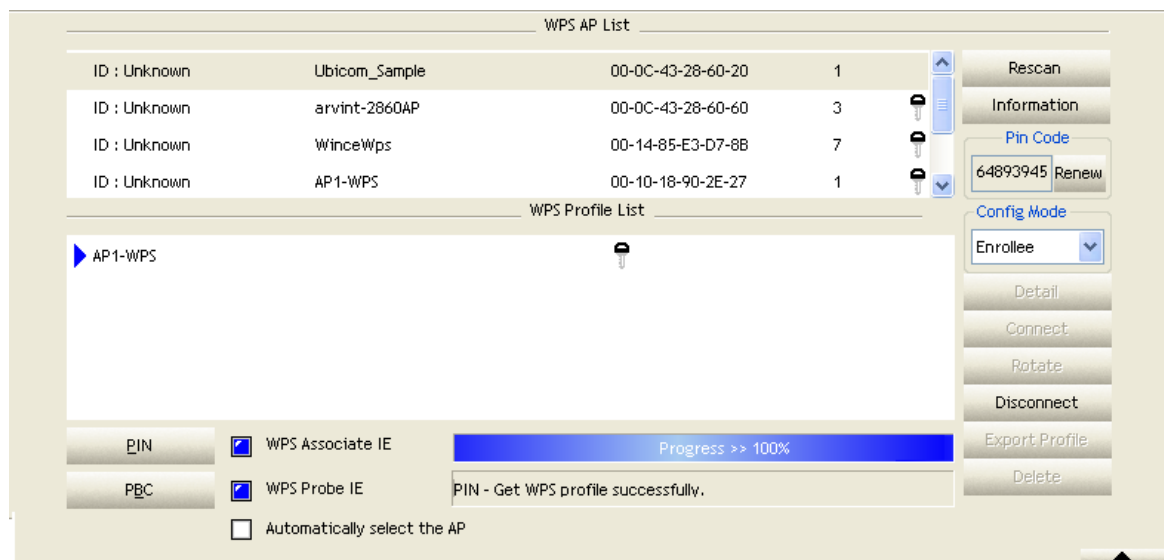
6 The result should appear as the image below.



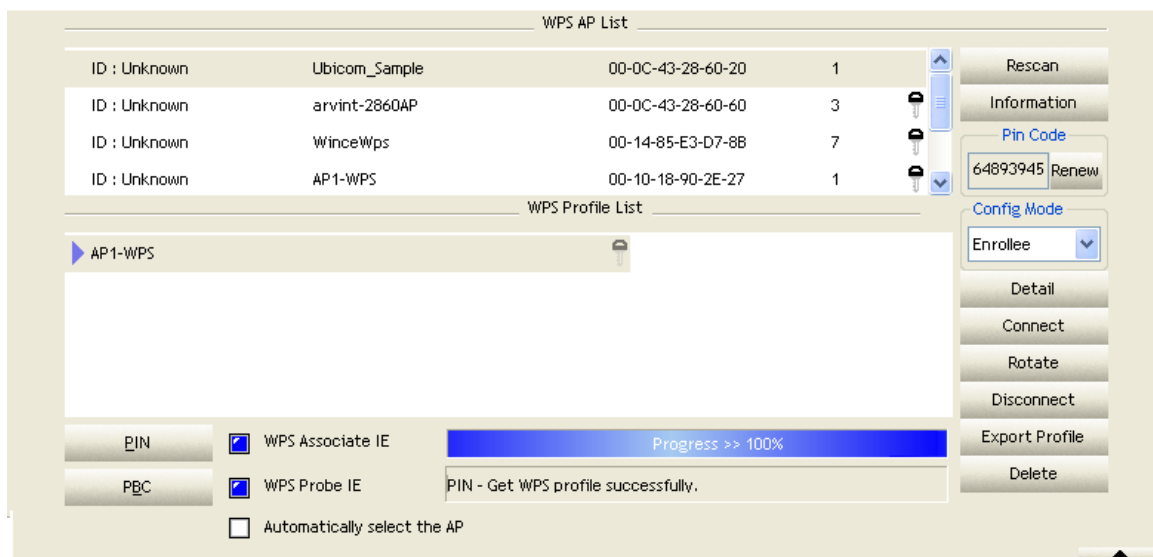
7 Configure one or more credentials



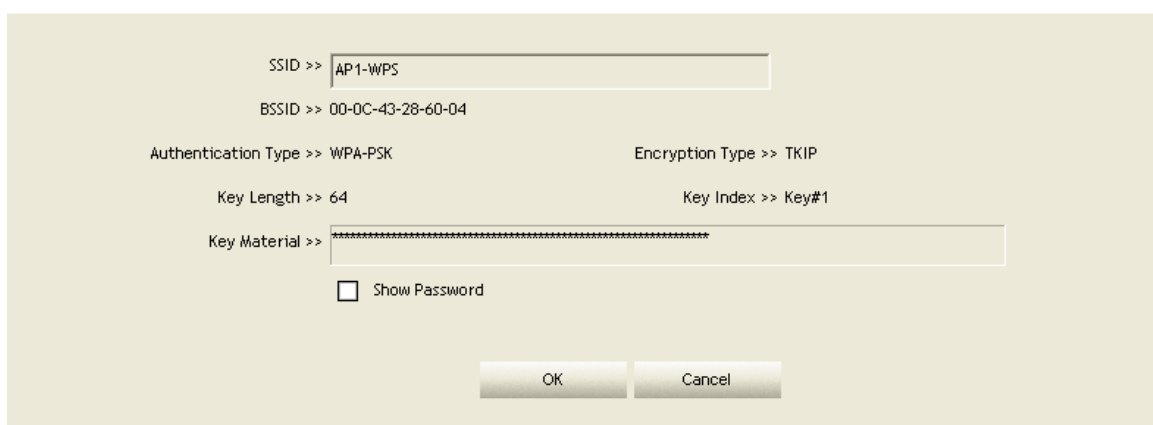
8 Then connect successfully. The result appear as the following image.



9 Click "Detail"



10 You will look like the below figure.



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:

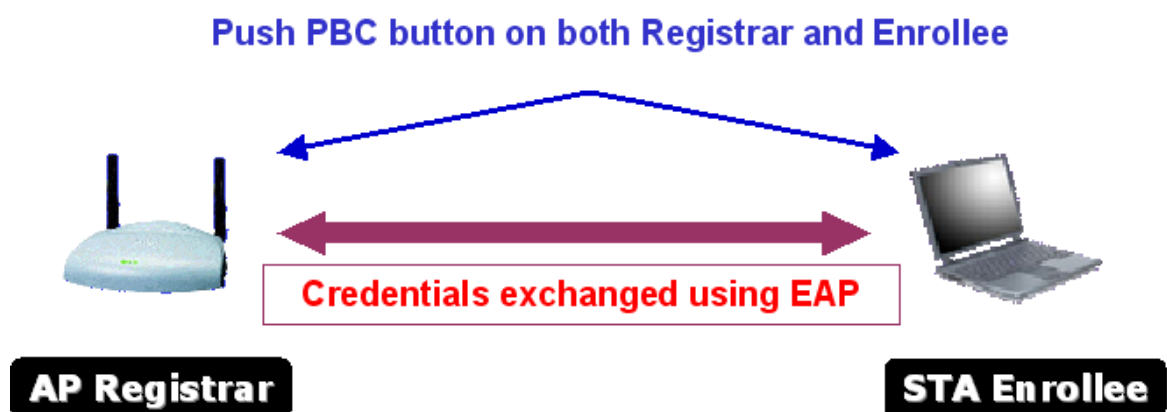
1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. Error PIN Code.
4. An inappropriate EAP-FAIL received.

4.2.7.4 Example to Add to Registrar Using PBC Method

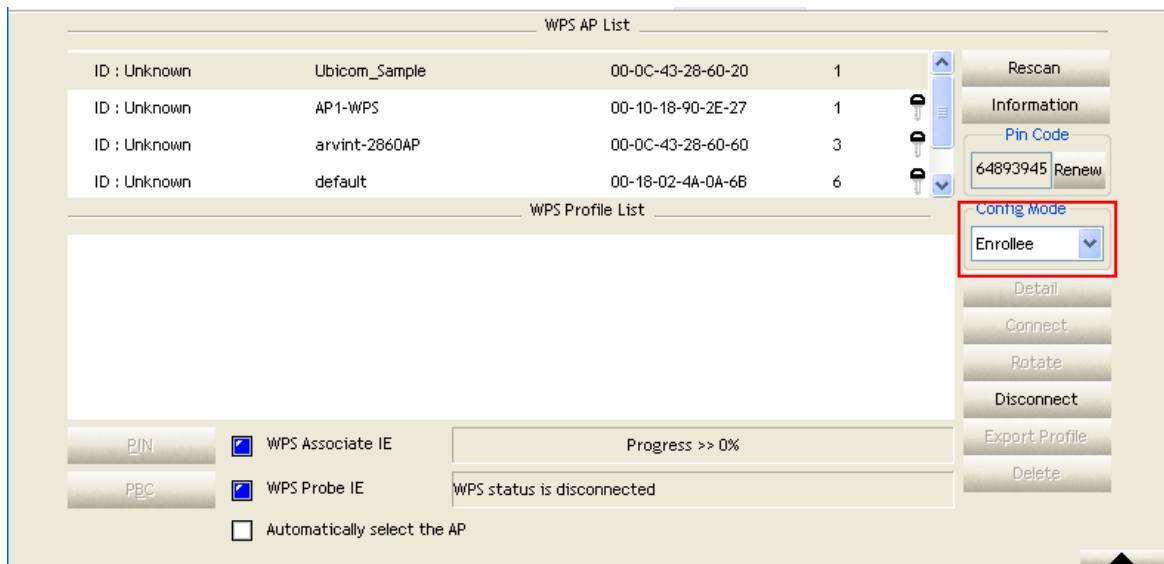
The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately 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.**

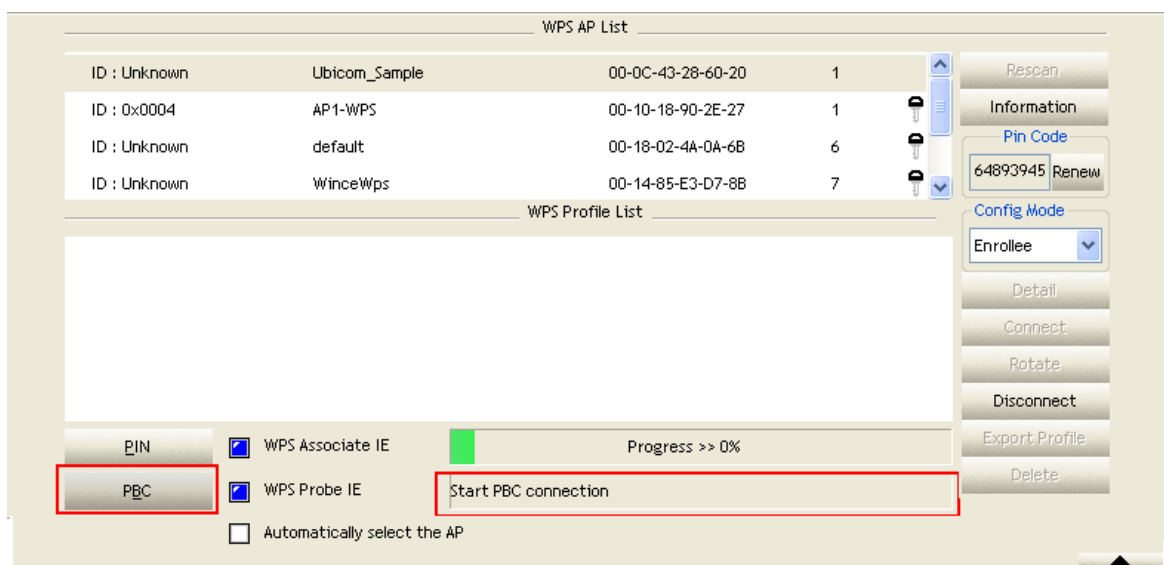


① Select "Enrollee" from the Config Mode drop-down list.



2 Click PBC to start the PBC connection.

3 Push the PBC on AP.



*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

☒ WPS Associate IE

☒ WPS Probe IE

PBC - Scanning AP

☐ Automatically select the AP

Progress >> 10%

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

☒ WPS Associate IE

☒ WPS Probe IE

PBC - Begin associating to WPS AP

☐ Automatically select the AP

Progress >> 15%

6 Check WPS Information on the available WPS APs

General WPS CCX

Authentication Type >> WPA-PSK
 State >> Configured

Encryption Type >> TKIP
 Version >> 1.0

Config Methods >> 0x0088
 AP Setup Locked >> Unknown

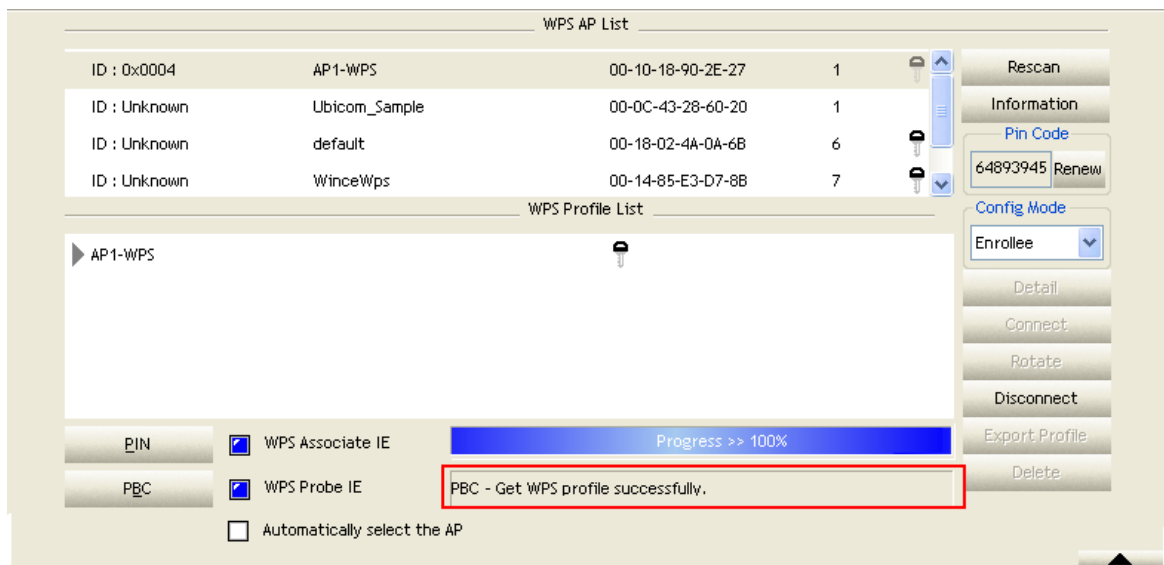
Device Password ID >>

0x0004

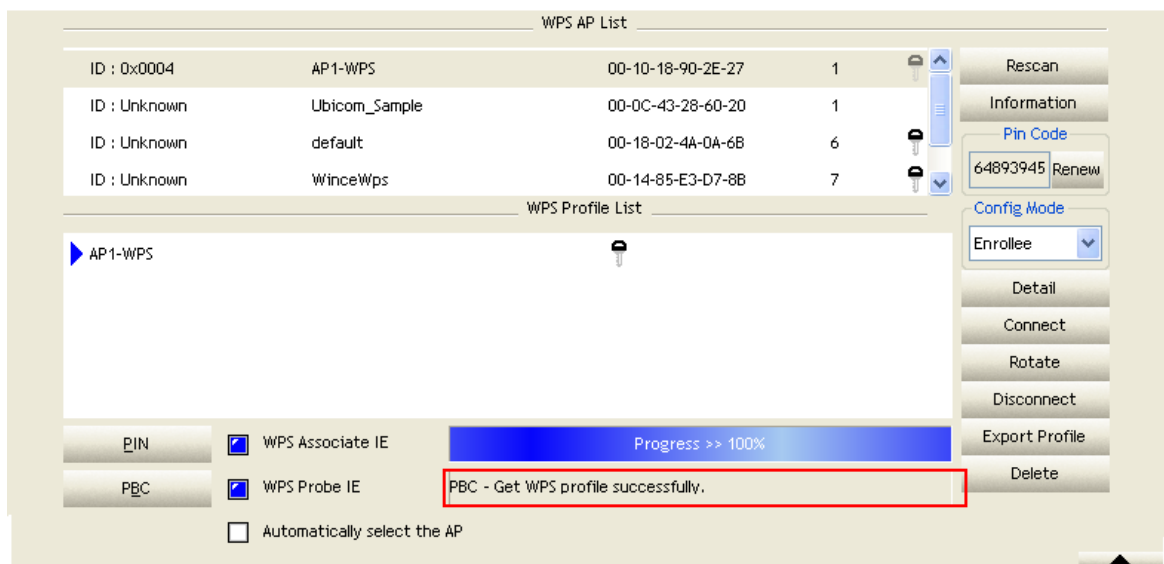
 UUID-E >> Unknown

Selected Registrar >> TRUE
 RF Bands >> Unknown

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



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



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 :

① 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.

② Different UUID-E :

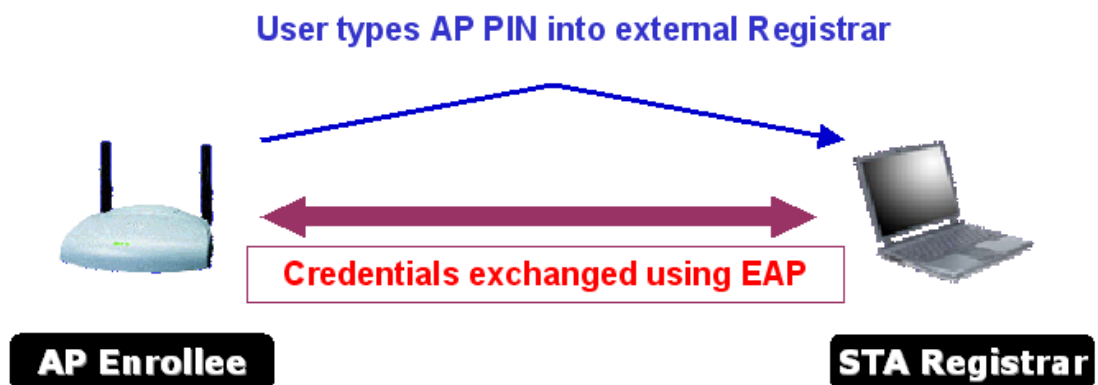
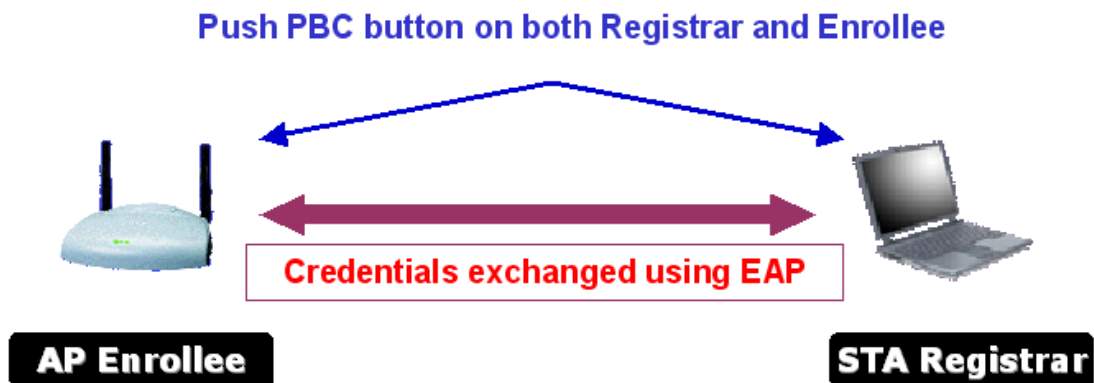
AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

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

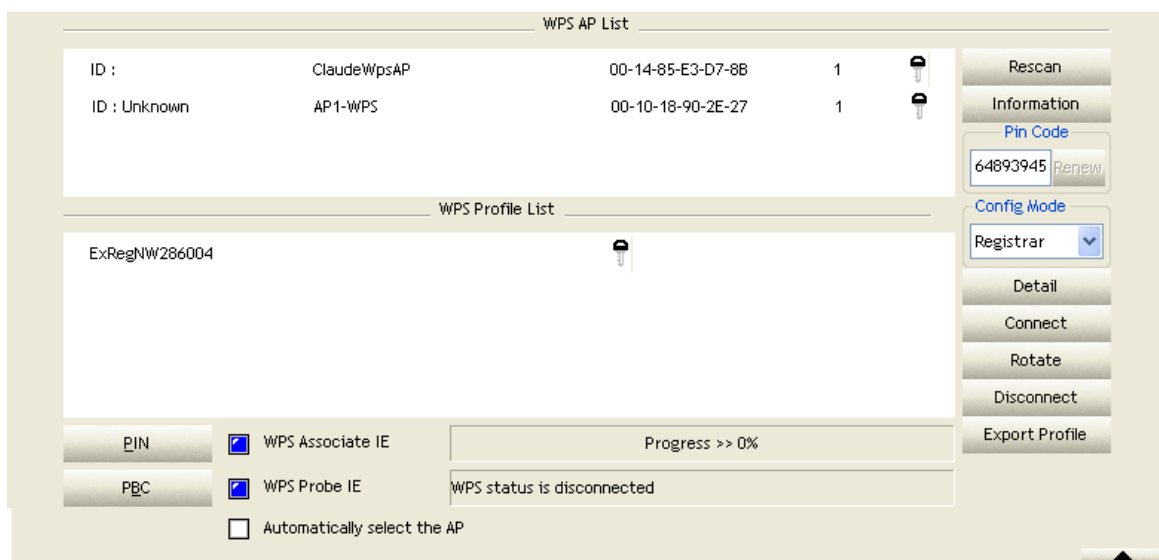
They have the different UUID-E.

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



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



- 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

OK Cancel

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

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	
---------------	--

Config Mode
Registrar

Rescan
Information
Pin Code
64893945 Renew
Detail
Connect
Rotate
Disconnect
Export Profile

PIN PBC

☒ WPS Associate IE

☒ WPS Probe IE

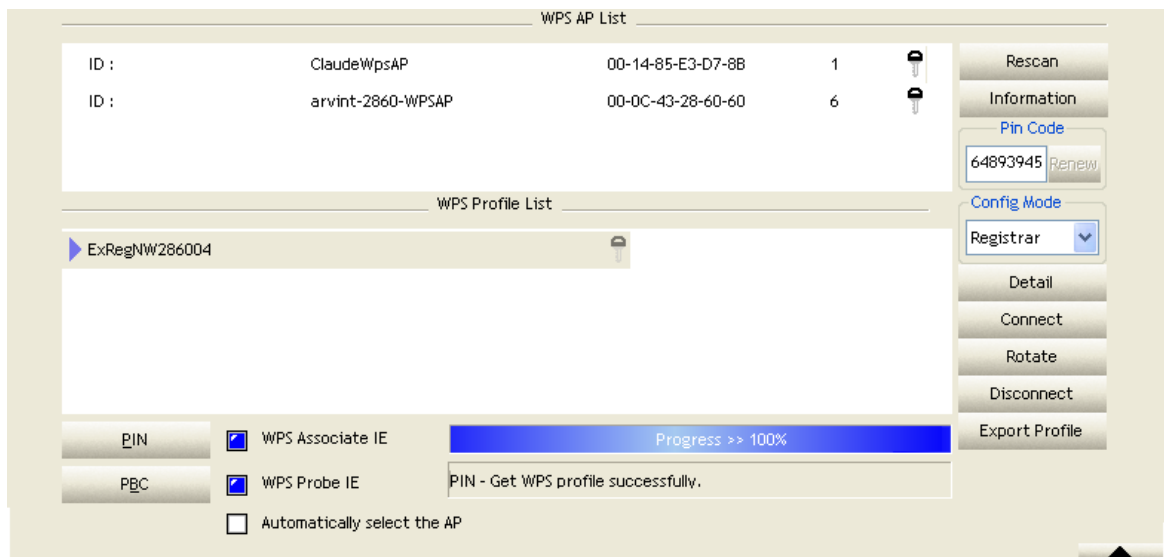
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

- 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.



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 status is connected successfully-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.

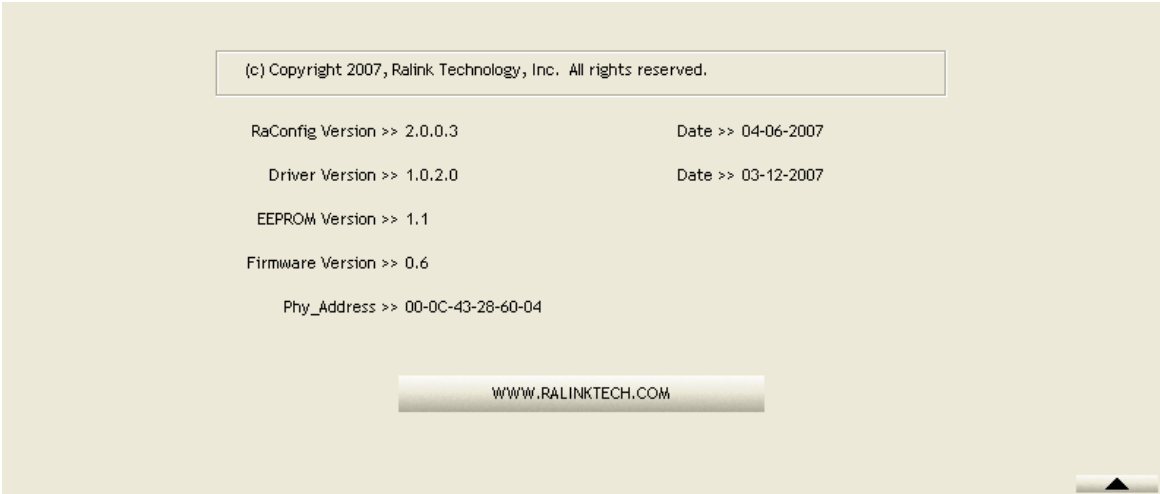


Figure 2-8 About function

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

Icons and buttons:

- 1 : Show the information of Status Section.
- 2 : Hide the information of Status Section.

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.

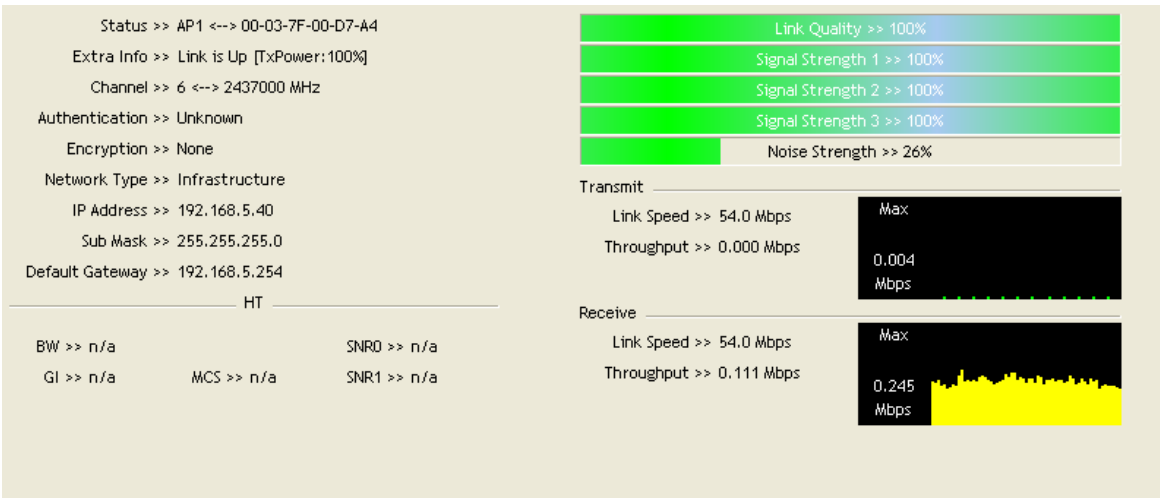


Figure 2-9 Link Status function

-
- 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.
 - ⑧ 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 Throughput : 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 : Receive signal strength 1, user can choose to display as percentage or dBm format.
 - ⑭ Signal Strength 2 : Receive signal strength 2, user can choose to display as percentage or dBm format.
 - ⑮ Signal Strength 3 : Receive signal strength 3, user can choose to display as percentage or dBm format.
 - ⑯ Noise Strength : Display noise signal strength.
 - ⑰ 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

Figure 3-1 Auth.\Encry. Settings

- ❶ Authentication Type: There are 7 authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.
- ❷ 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.
- ❸ 8021X: This is introduced in the topic of Section 3-2.
- ❹ 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.
- ❺ 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.
 - ❶ Hexadecimal - 40bits: 10 Hex characters.
 - ❷ Hexadecimal - 128bits: 32Hex characters.
 - ❸ ASCII - 40bits: 5 ASCII characters.
 - ❹ ASCII - 128bits: 13 ASCII characters.

****Powered by Meetinghouse.**

4.3.2 802.1x Setting

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

Authentication type:

- ❶ 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.
- ❷ 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.
- ❸ 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.
- ❹ 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.**
- ❺ 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.
- ❻ 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:

- ① Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".
- ② Tunnel Identity: Identity for tunnel.
- ③ 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

- ① Use Client certificate: Client certificate for server authentication.

EAP Fast

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

The screenshot shows a network configuration window with the following details:

- Top bar: Auth. \ Encry. 8021X
- EAP Method >>: PEAP
- Tunnel Authentication >>: EAP-MSCHAP v2
- Session Resumption: ☐
- Tabbed interface: ID \ PASSWORD, Client Certification, **Server Certification**
- Server Certification options:
 - ☐ Use certificate chain
 - ☐ Allow intermediate certificates
 - Server name >>: [Text field]
 - ☒ Server name must match exactly
 - ☒ Domain name must end in specified name
- Buttons: OK, Cancel

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.

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

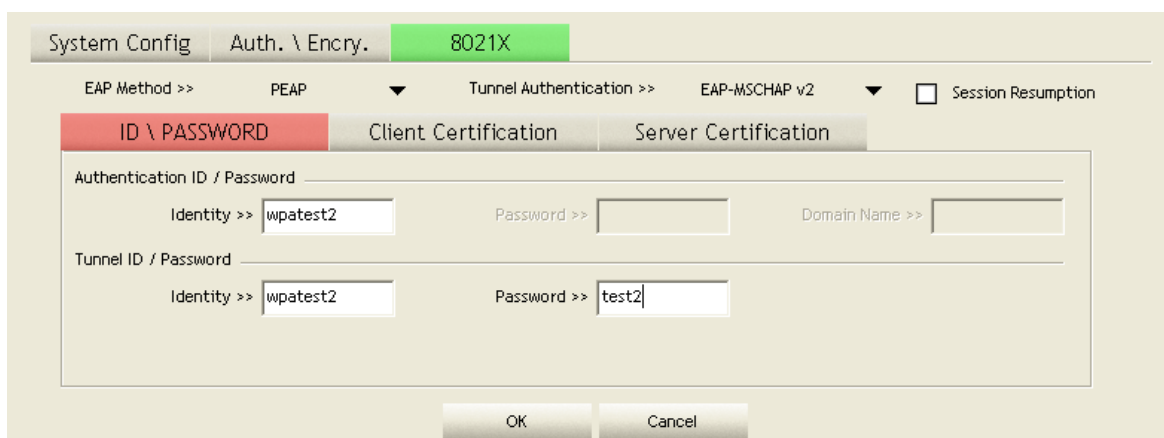
③ If you want to disconnect, click "Cancel" on the Authentication Failure dialog box. If you want to reconnect, key the identity into wpatest2. The tunnel identity is wpatest2 and the tunnel password is test2. Those setting are the same as our intended AP's setting.

④ Click "OK". If it has connected successfully. The result will appear as the image below.

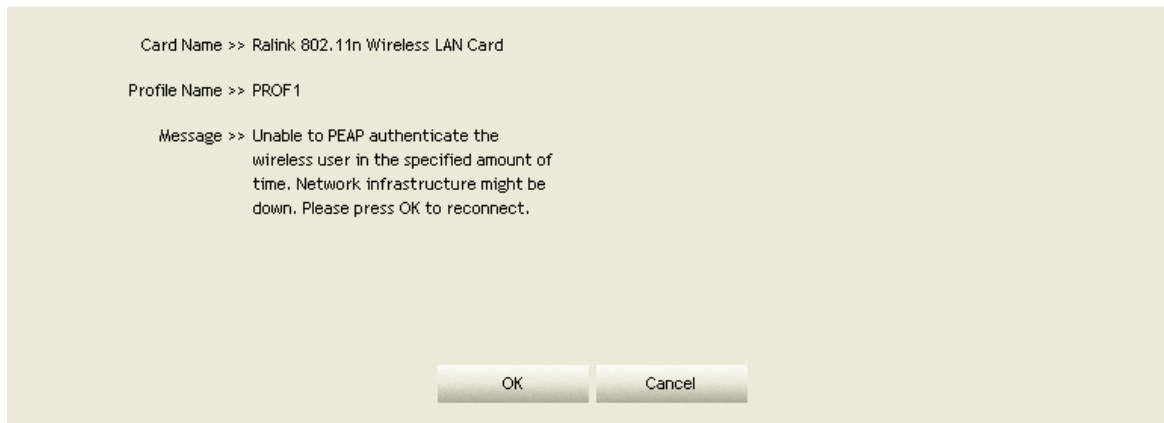


When a "Timeout" occurs;

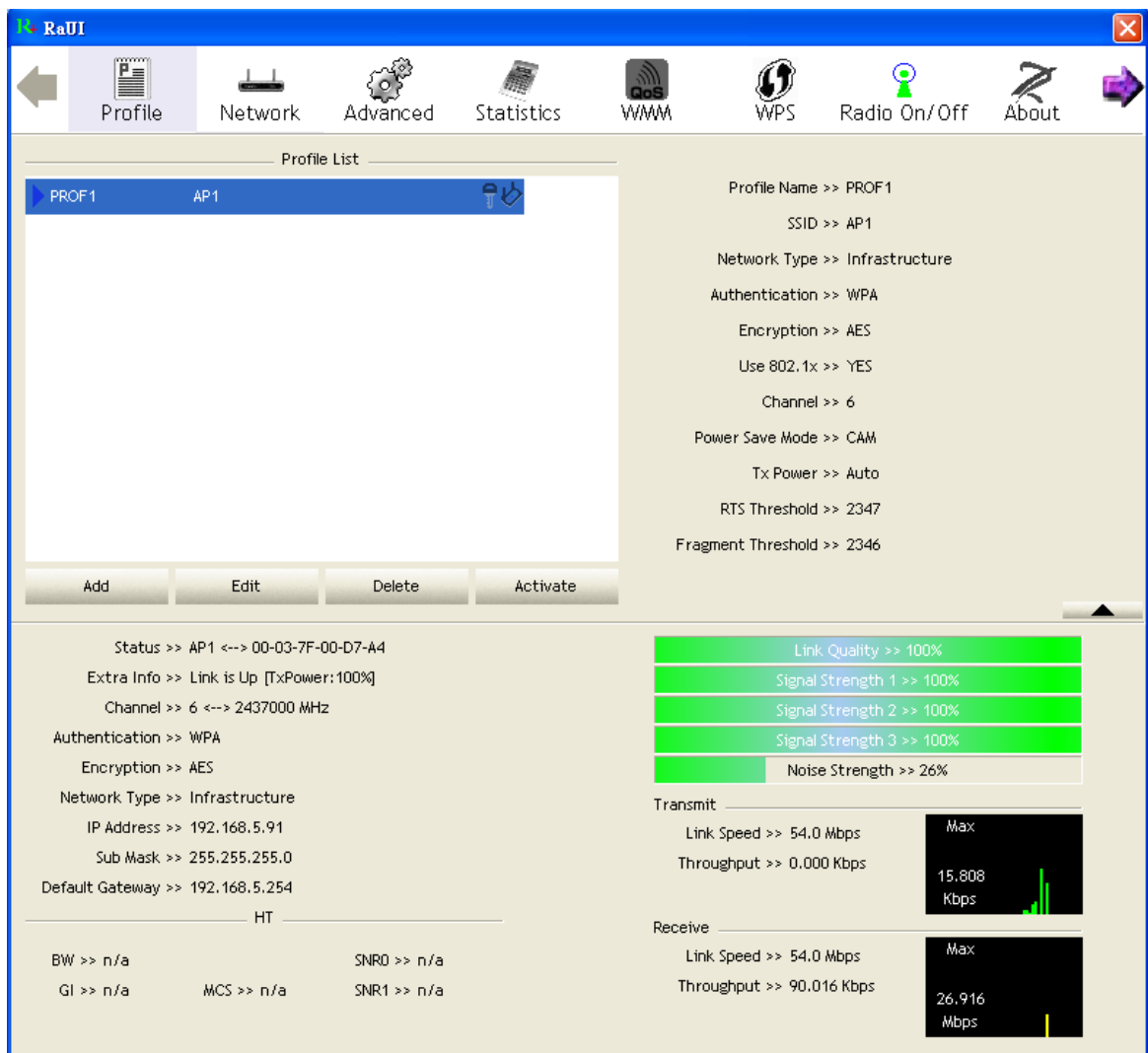
❶ Choose "PEAP" as the Authentication type and key-in "wpatest2" as the identity . Tunnel Protocol is "EAP-MSCHAP-v2, and the tunnel identity is "wpatest2". The tunnel password is "test2". These settings are the same as our intended AP's setting.



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



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



4.3.4 Example to Configure Connection with WEP on

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

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays several access points, with 'ariscadre' selected. Below the table, the 'Status' and 'Extra Info' sections provide details about the selected AP, including its MAC address, channel, and encryption status. The 'Transmit' and 'Receive' sections show link speed and throughput metrics.

AP ID	Channel	Encryption	Signal	Link Quality
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%	
ariscadre	1	b g n	100%	
Broadcom	11	b g	60%	
BroadcomWPS	1	b g	60%	
BUFFALO_A	44	a n	29%	

Status >> ariscadre <--> 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

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

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

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

The screenshot shows the RaUI Utility Config window with the 'Network' tab selected. The 'AP List' table displays various wireless networks. Below the table, the 'Auth. \ Encry.' section is active, showing '802.1X' authentication and 'WEP' encryption. The 'Wep Key' section has four keys, all set to 'Hexadecimal'.

AP List	Channel	Signal	dBm
202	1	60%	
219	1	65%	
230	2	50%	
243	5	81%	
99	6	81%	
AP1	6	100%	
arcsadre	1	100%	
Broadcom	11	60%	
BroadcomWPS	1	60%	
BUFFALO_A	44	29%	

Auth. \ Encry. 802.1X

Authentication >> Open Encryption >> WEP ☐ 802.1X

WPA Preshared Key >>

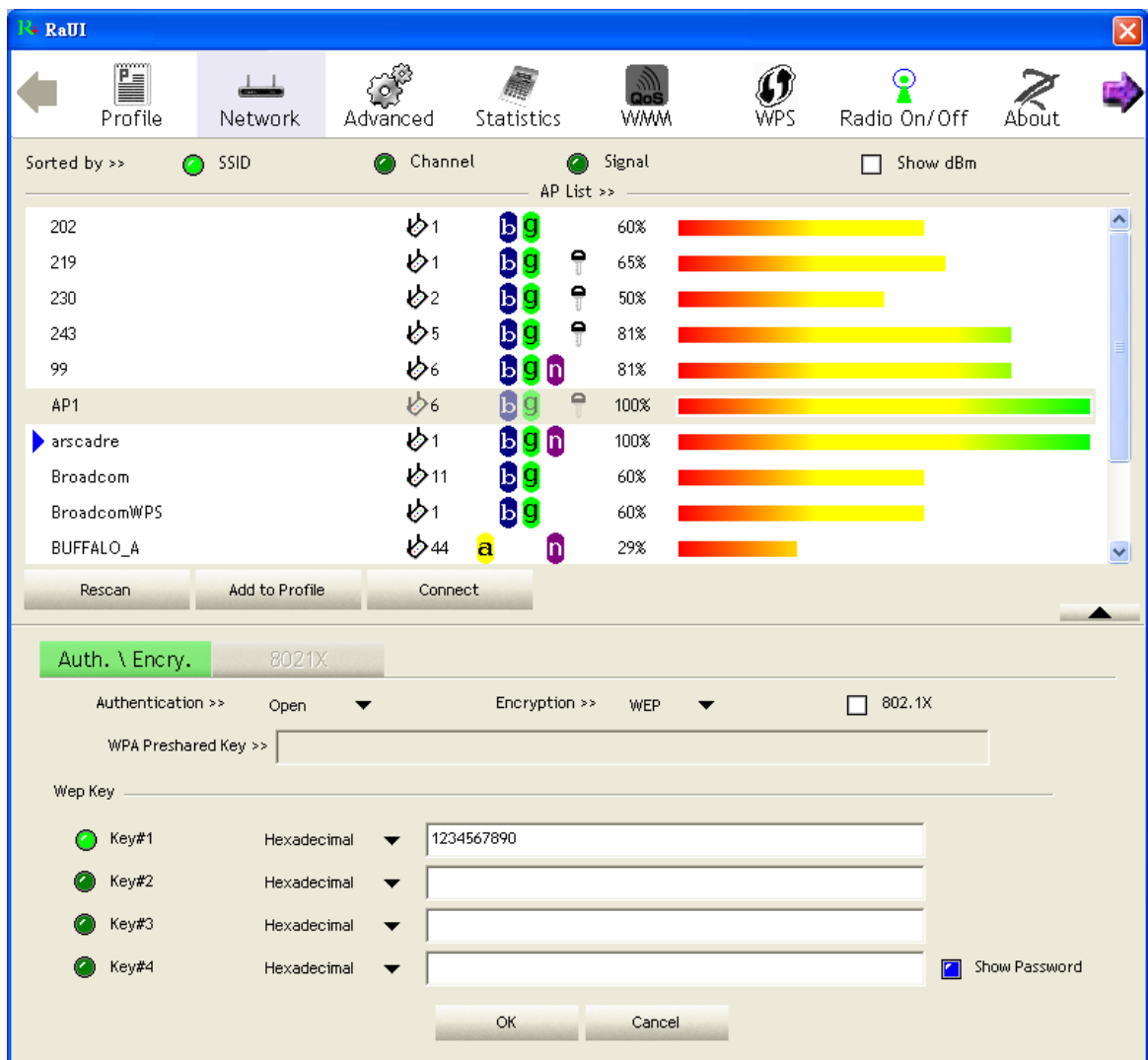
Wep Key

- ☒ Key#1 Hexadecimal
- ☒ Key#2 Hexadecimal
- ☒ Key#3 Hexadecimal
- ☒ Key#4 Hexadecimal

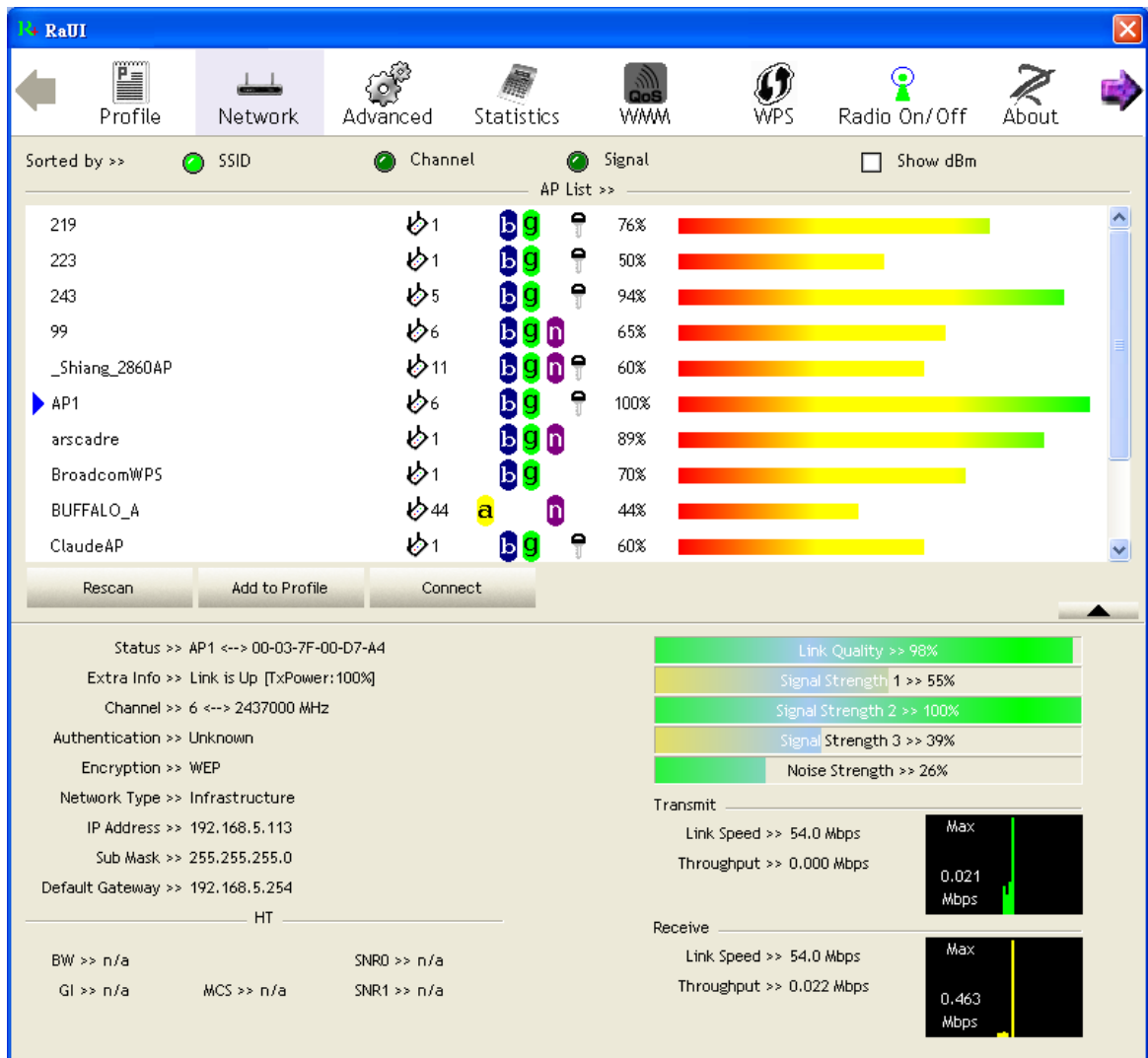
☐ Show Password

OK Cancel

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

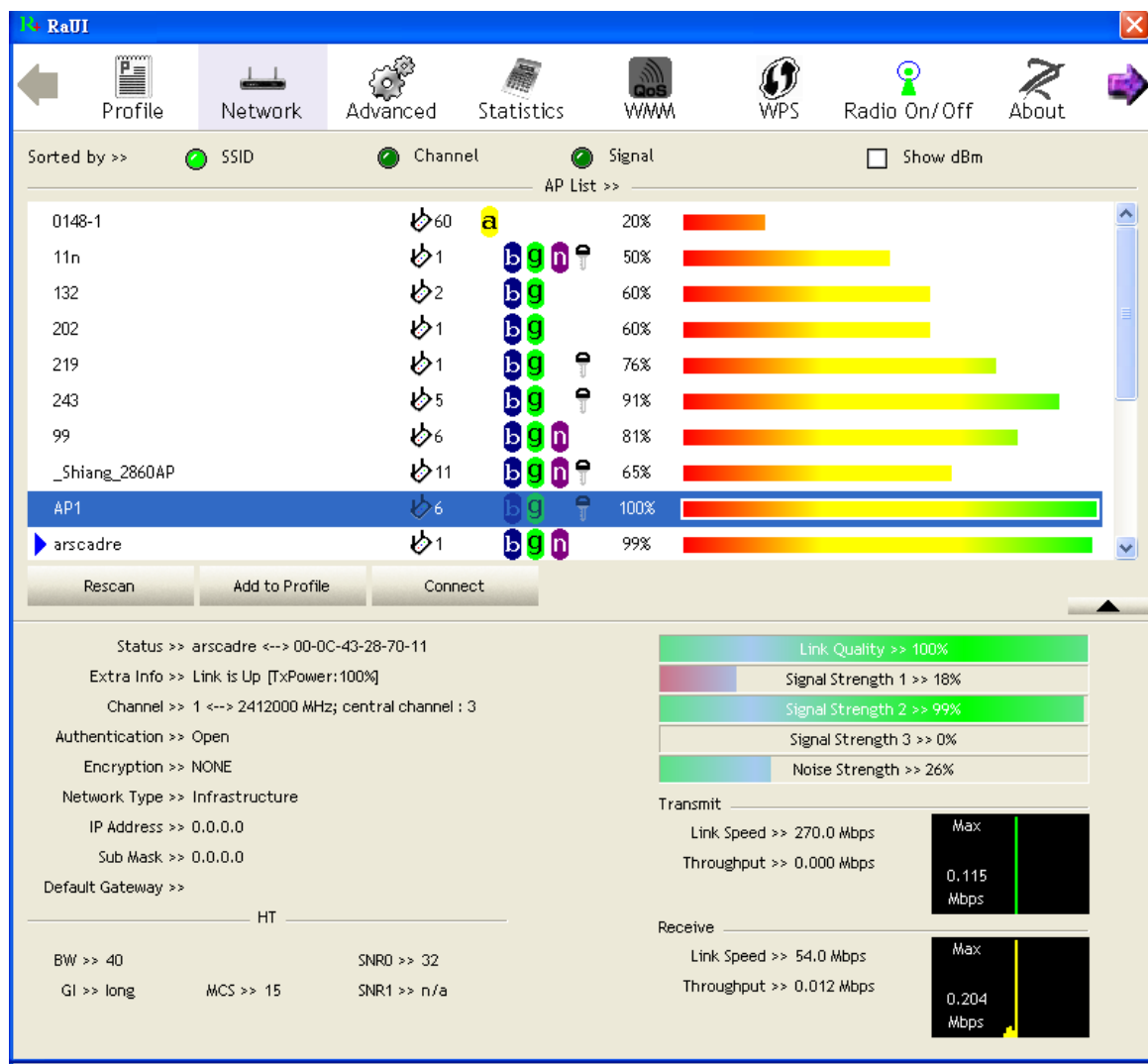


- 4 Click "OK". The dialog box will appear as below;

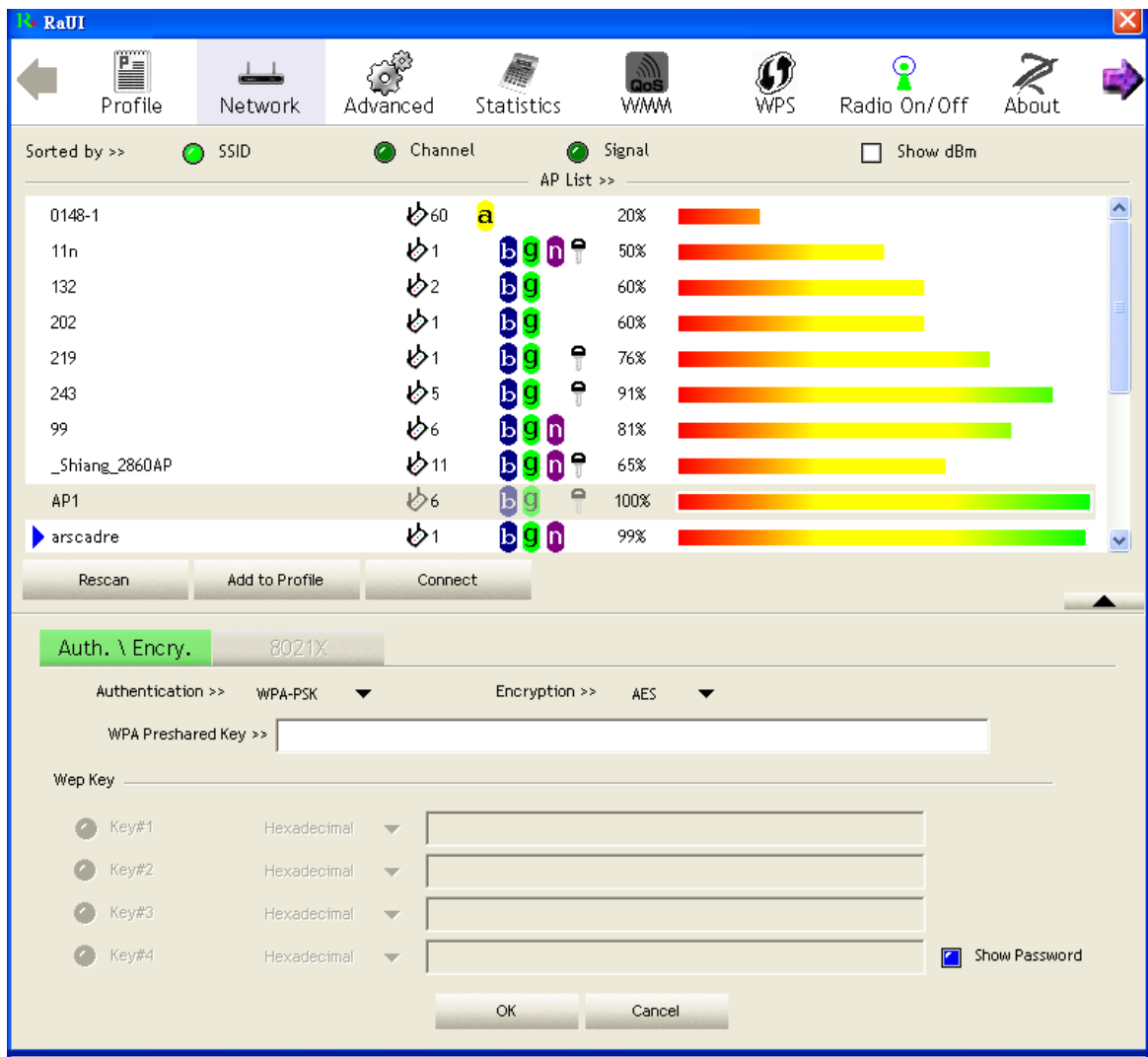


4.3.5 Example to Configure Connection with WPA-PSK

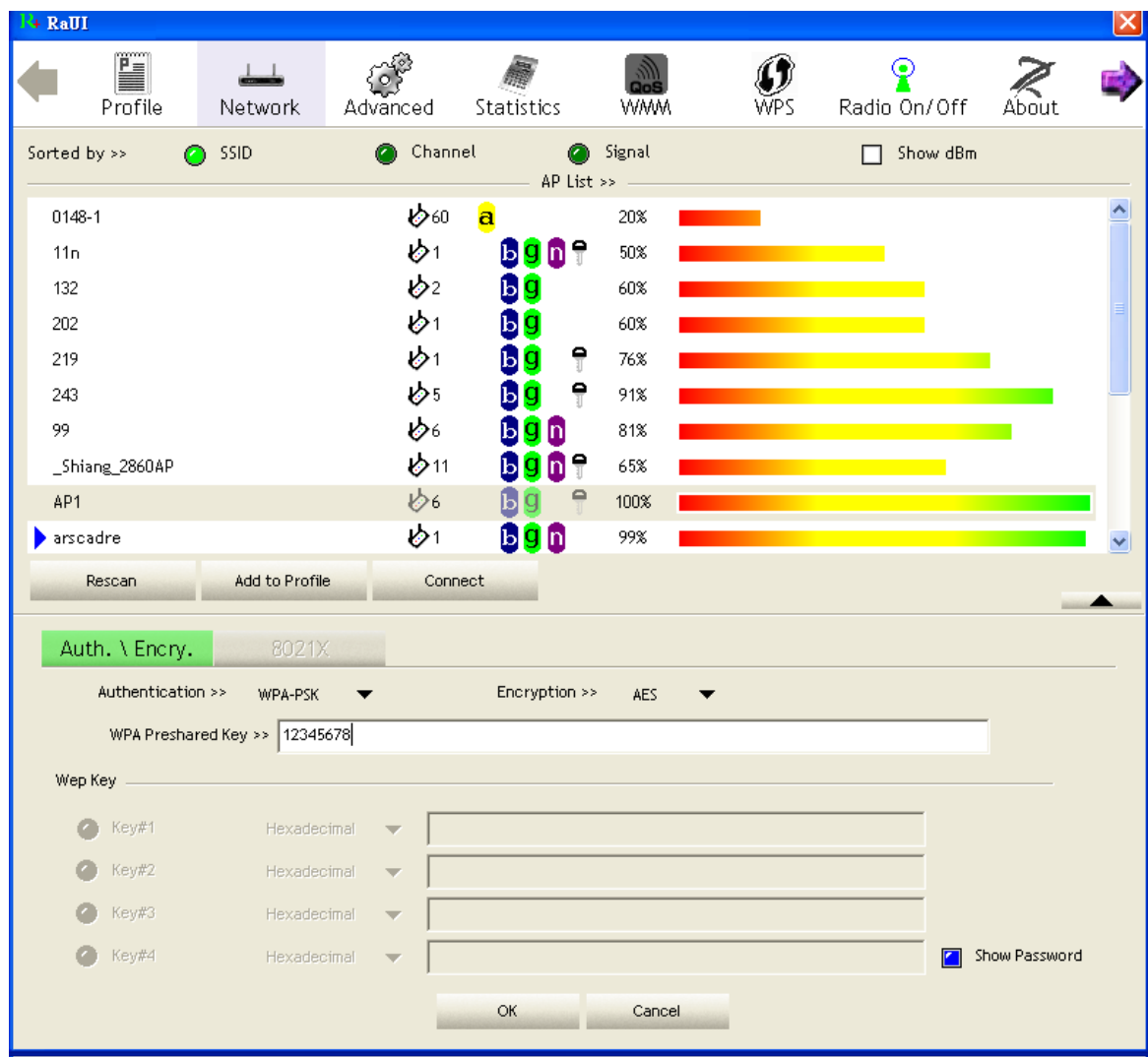
- Select the AP with a WPA-PSK authentication mode and click "Connect".



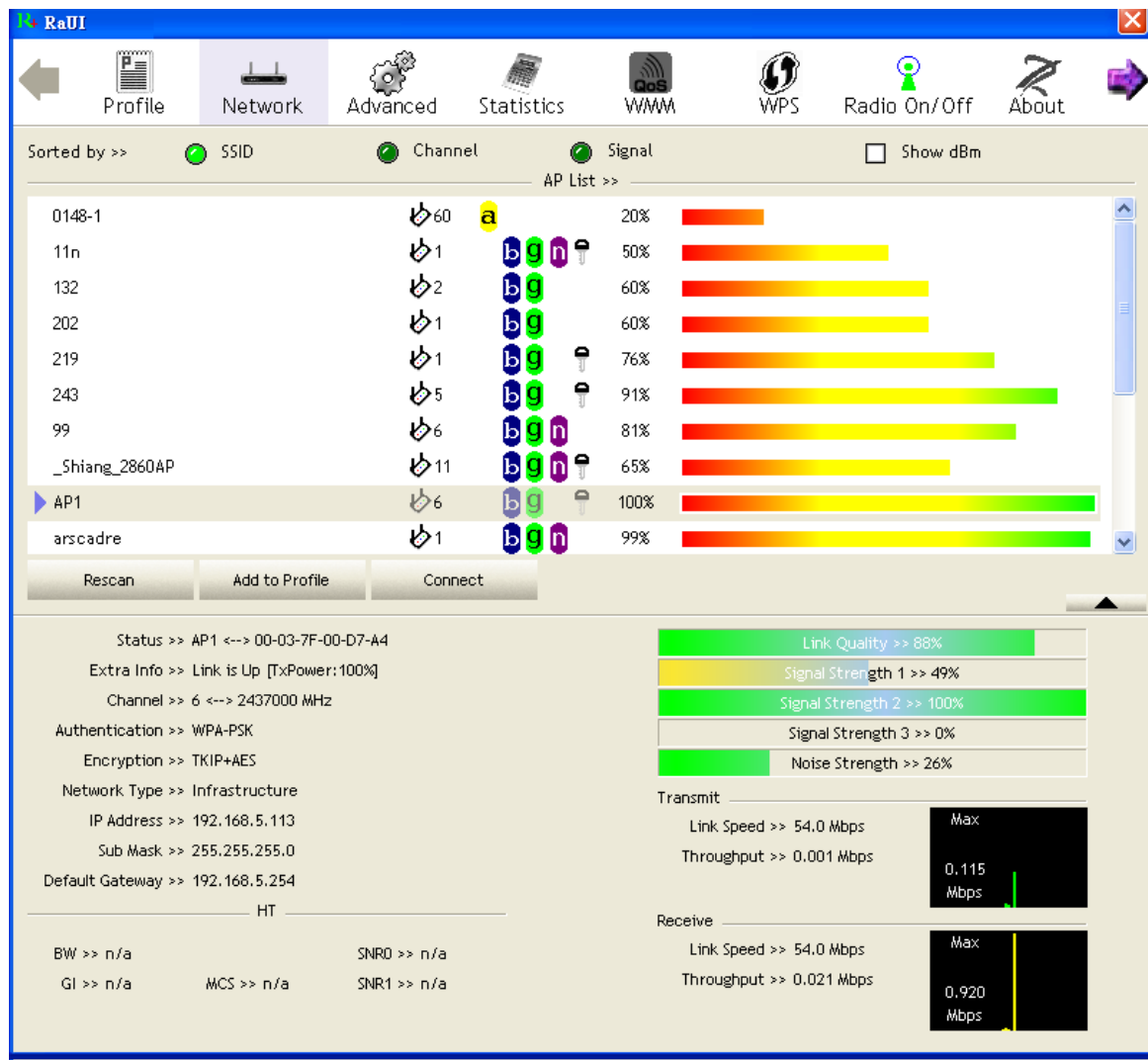
2 Auth.\Encry. function appears.



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

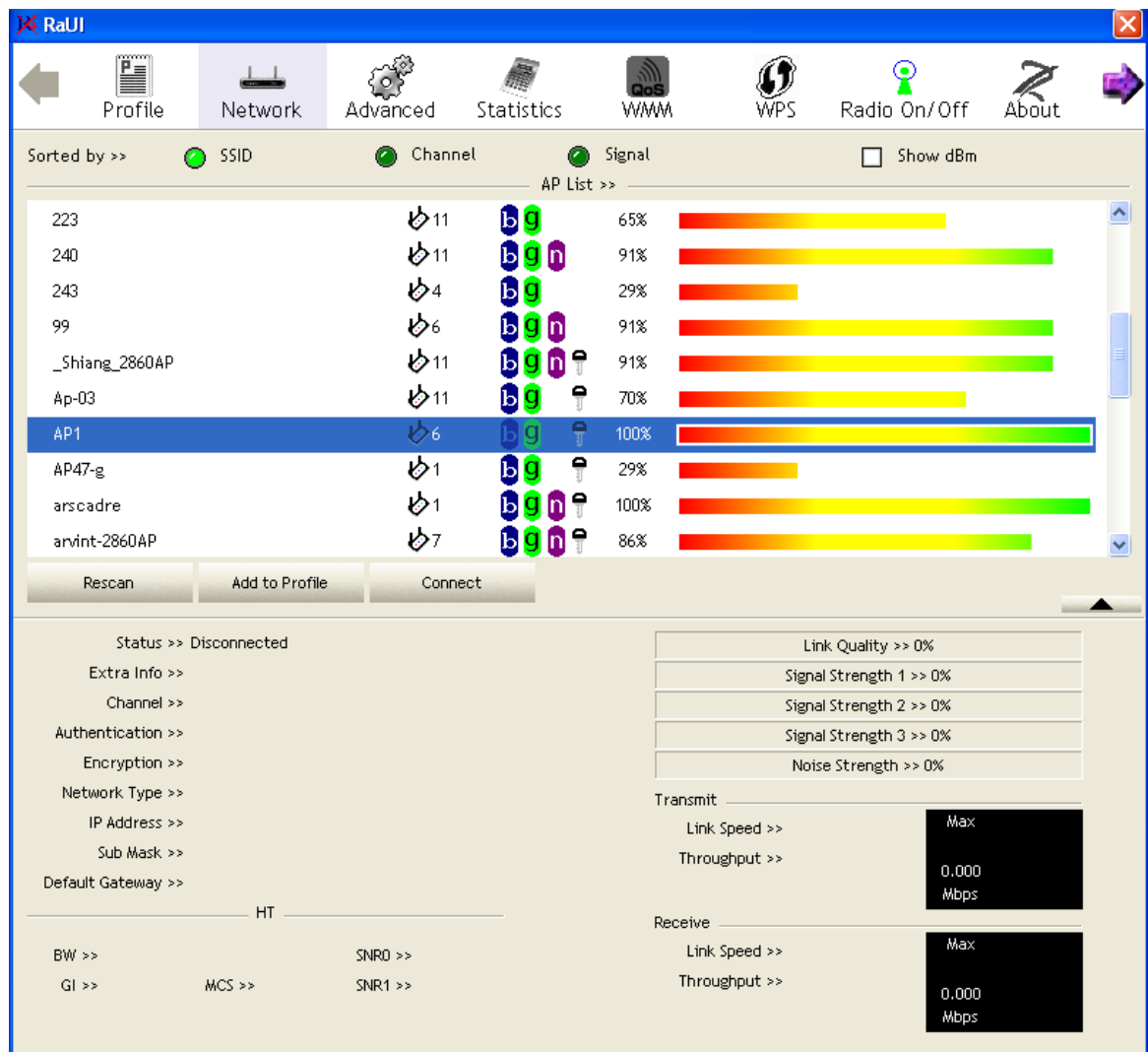


4 Click "OK". Be careful, if the WPA Pre-Shared Key entered is not correct, you won't be able to exchange any data frames, even though the AP can be connected.

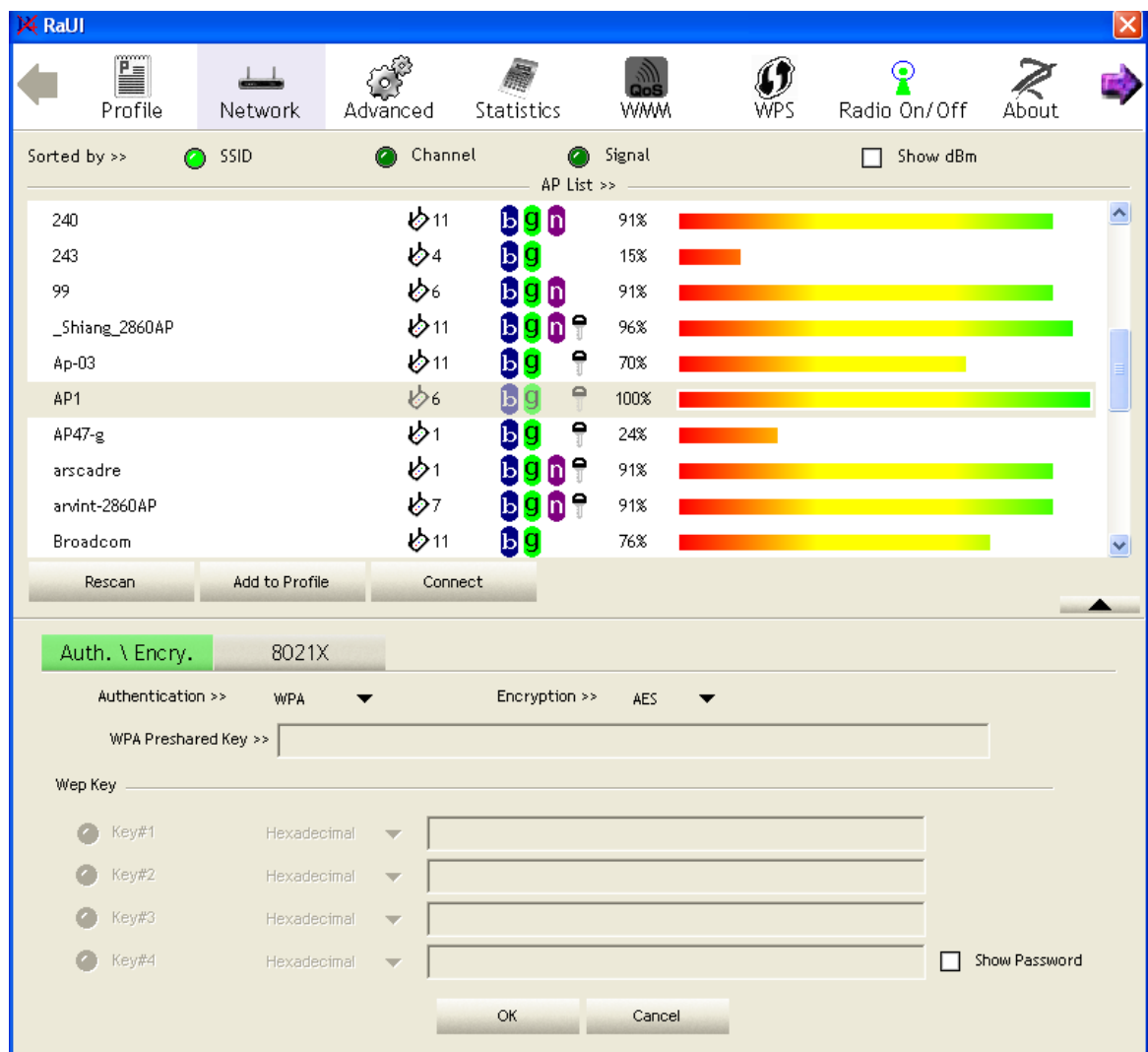


4.3.6 Example to Configure Connection with WPA

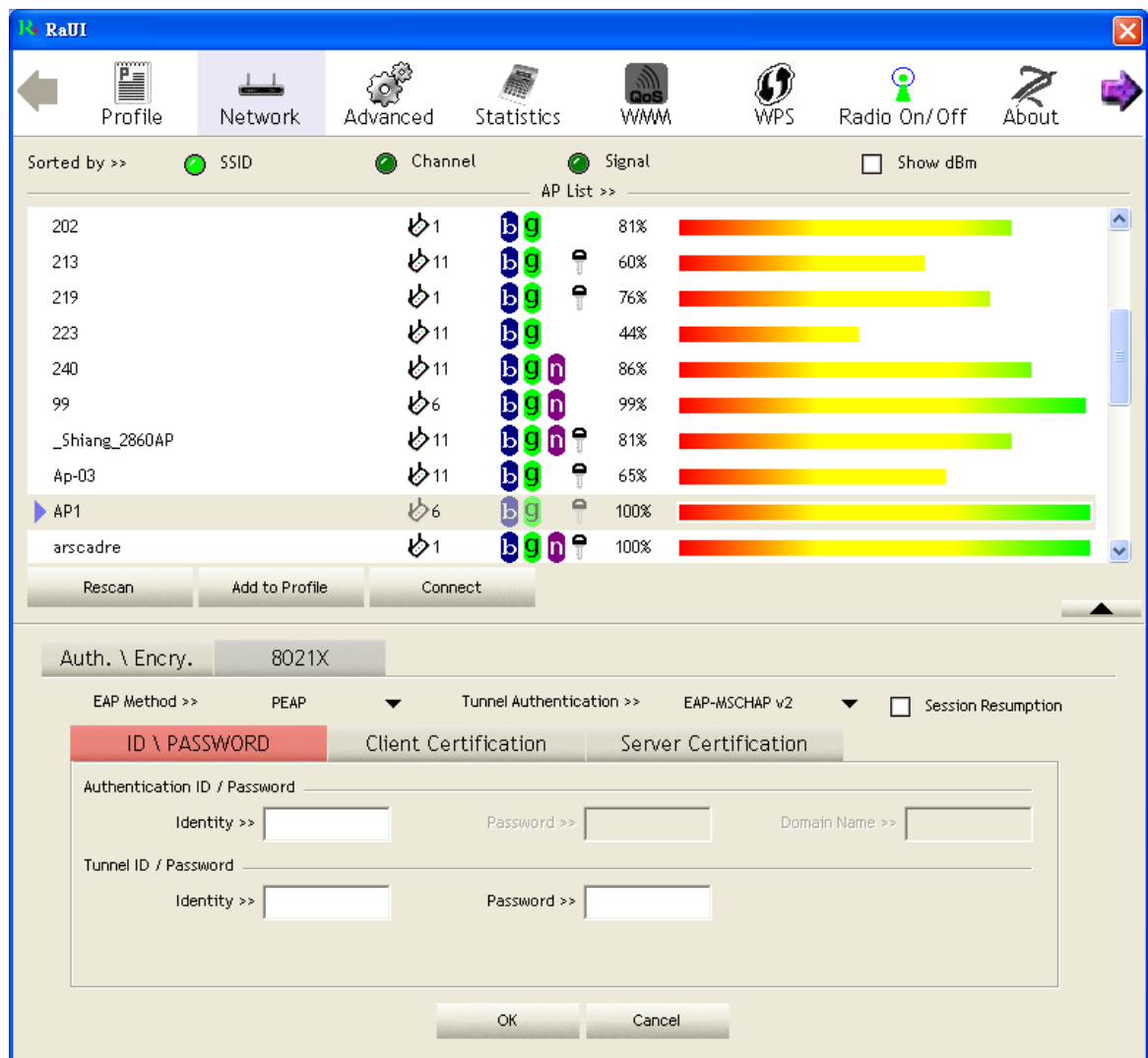
- Select an AP with WPA authentication mode and click "Connect".



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



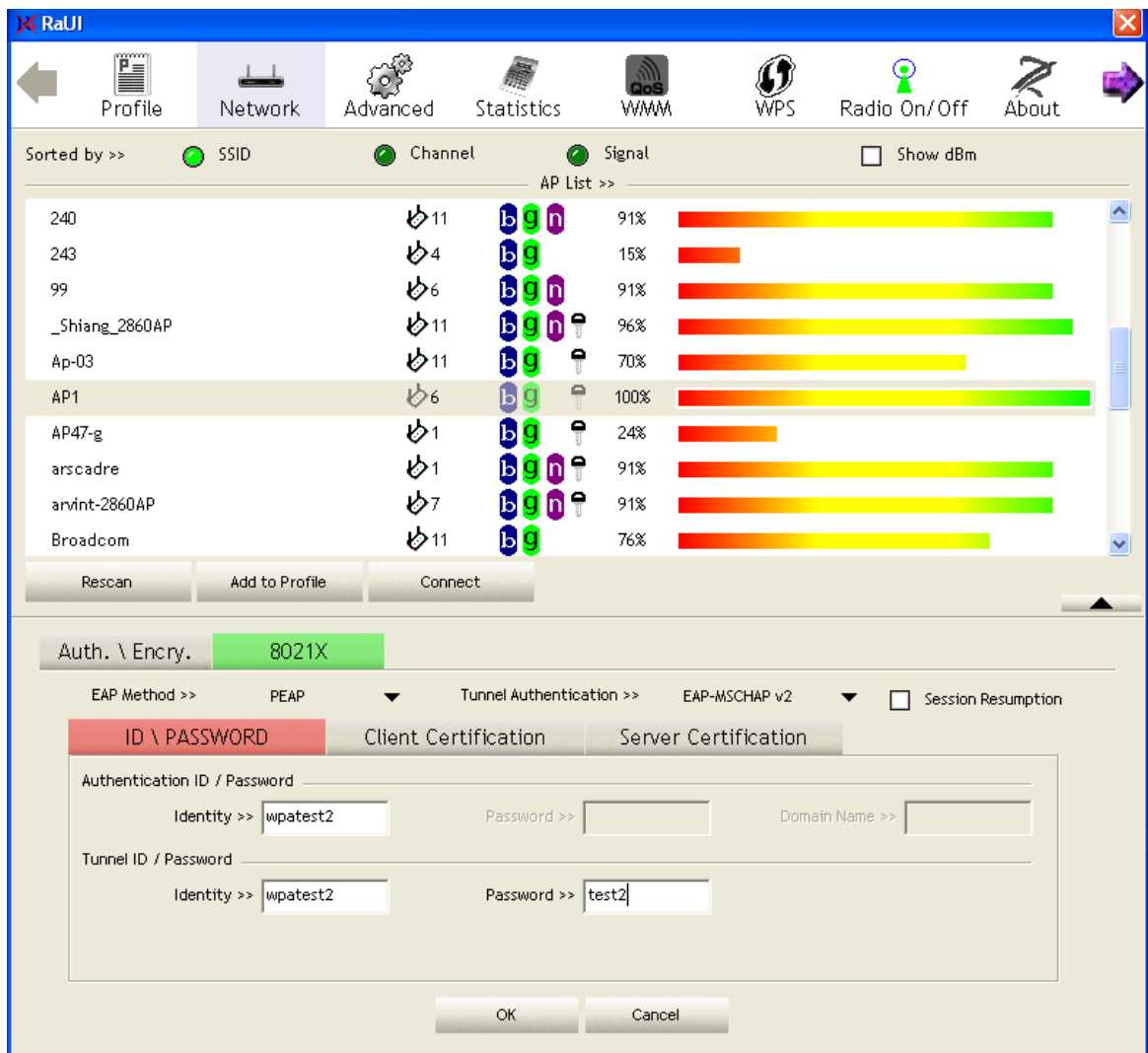
- 3 Click "8021X" and the setting page will appear.



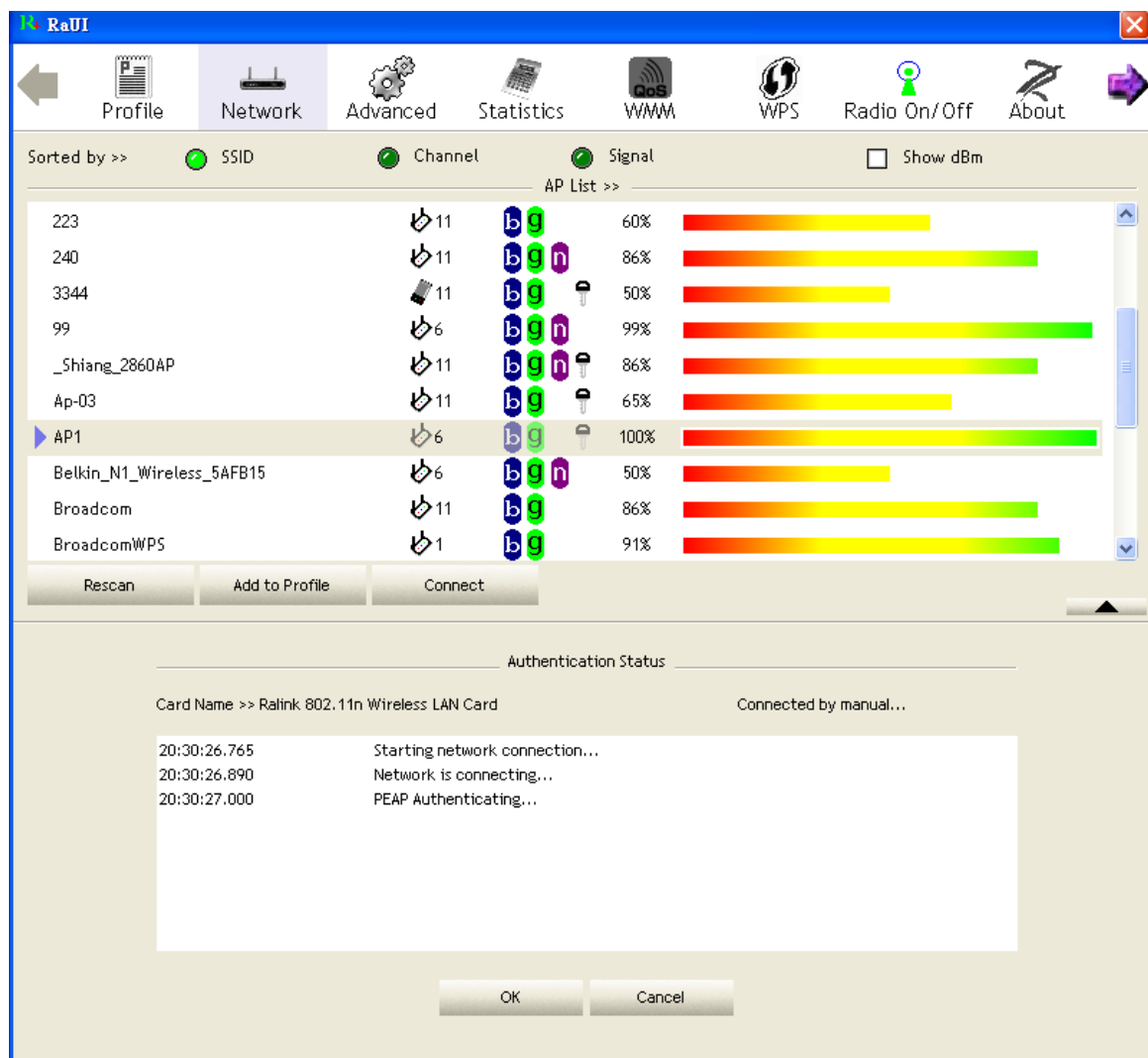
4 Authentication type and setting method :

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.



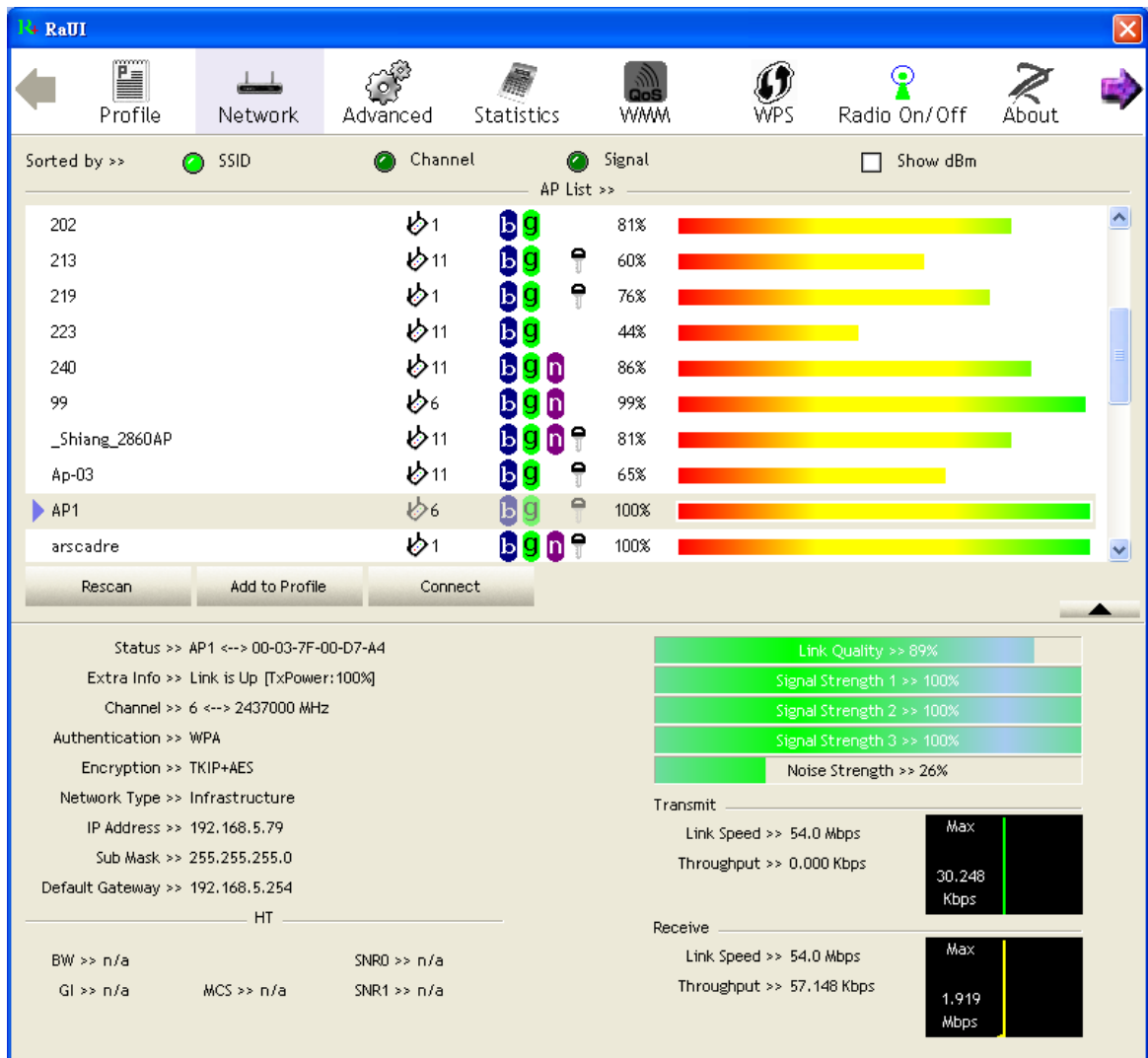
2. Click OK. The dialog box should appear as below.



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

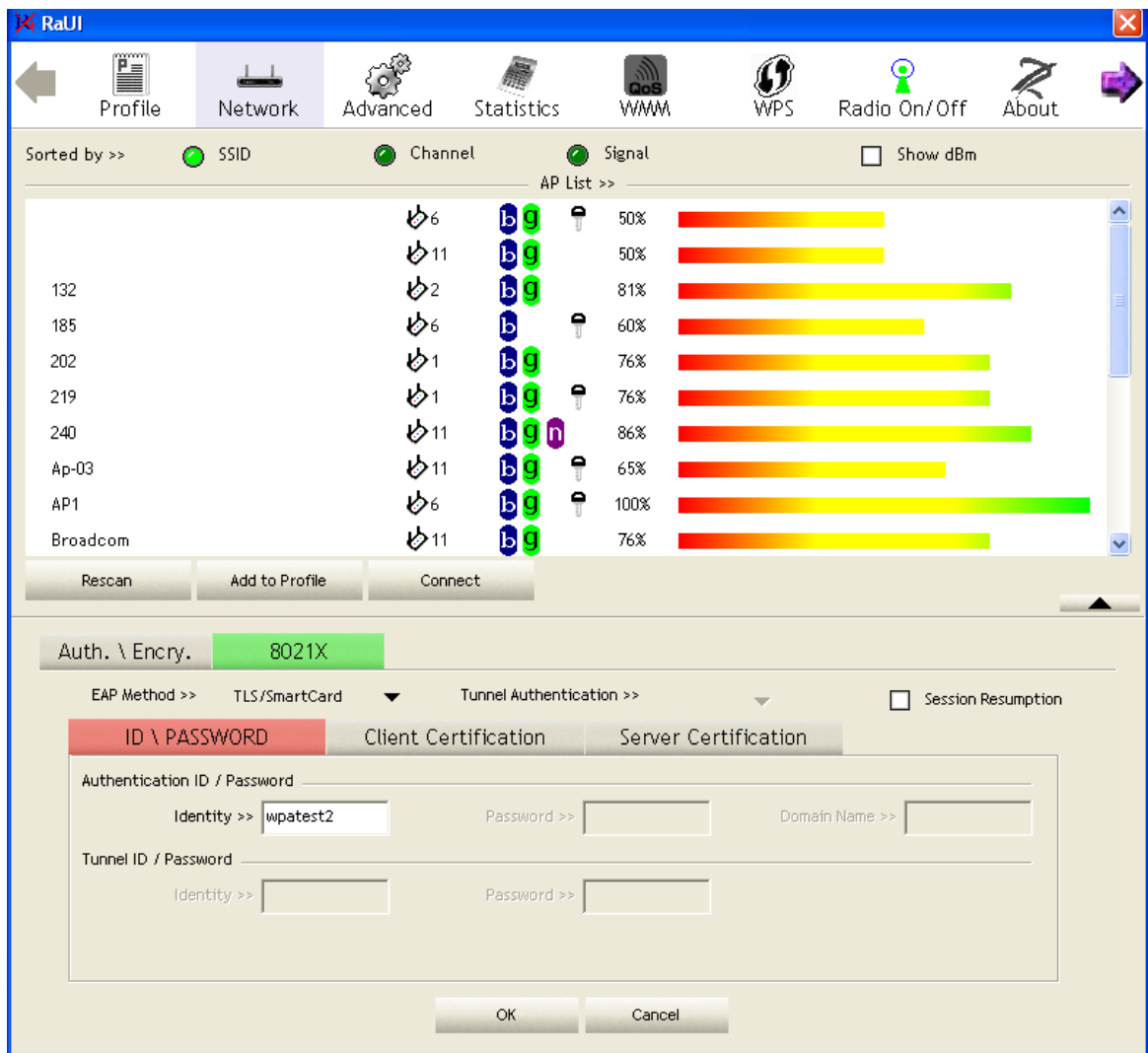
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

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

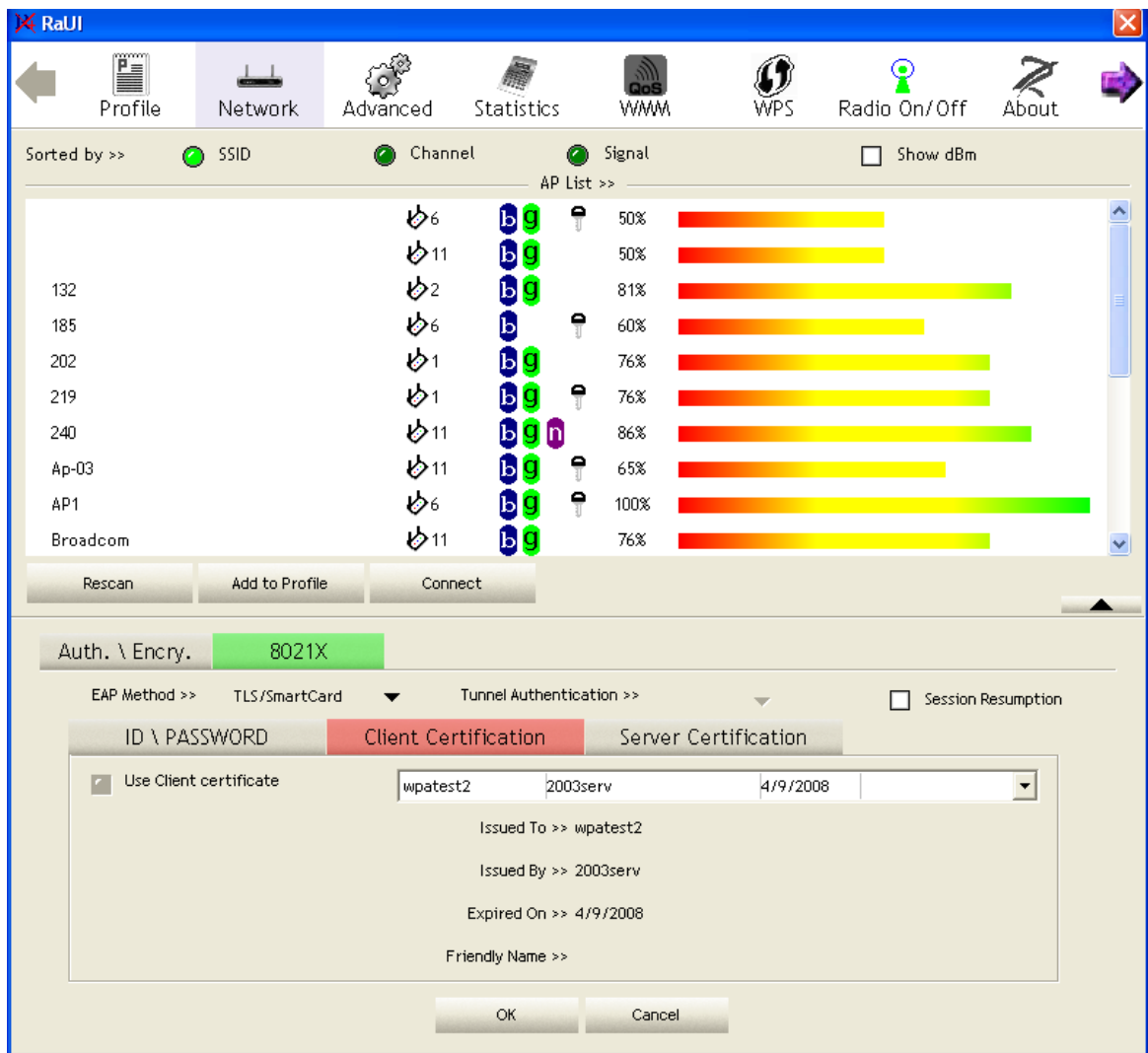


TLS / Smart Card :

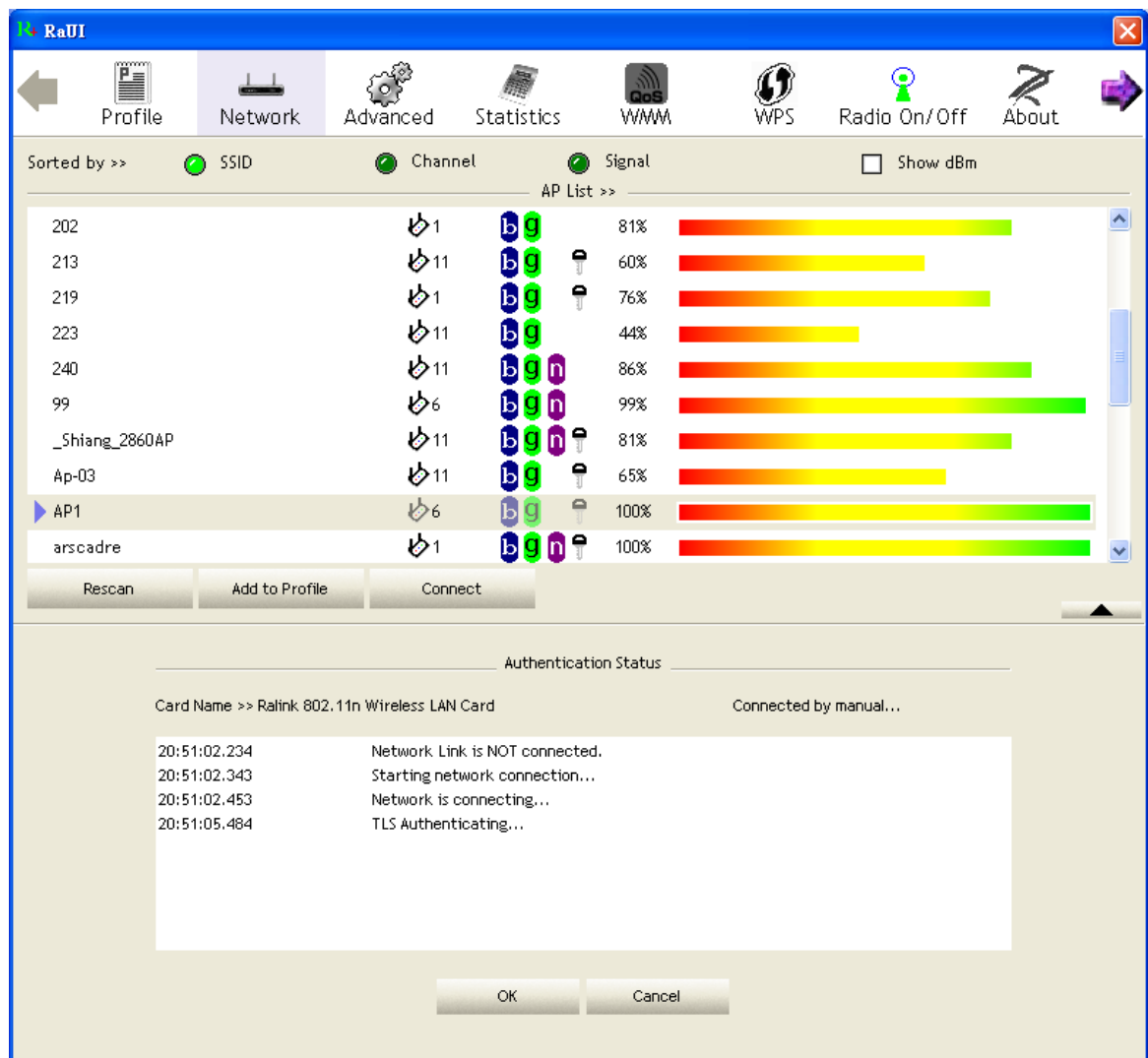
1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server authentication.



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



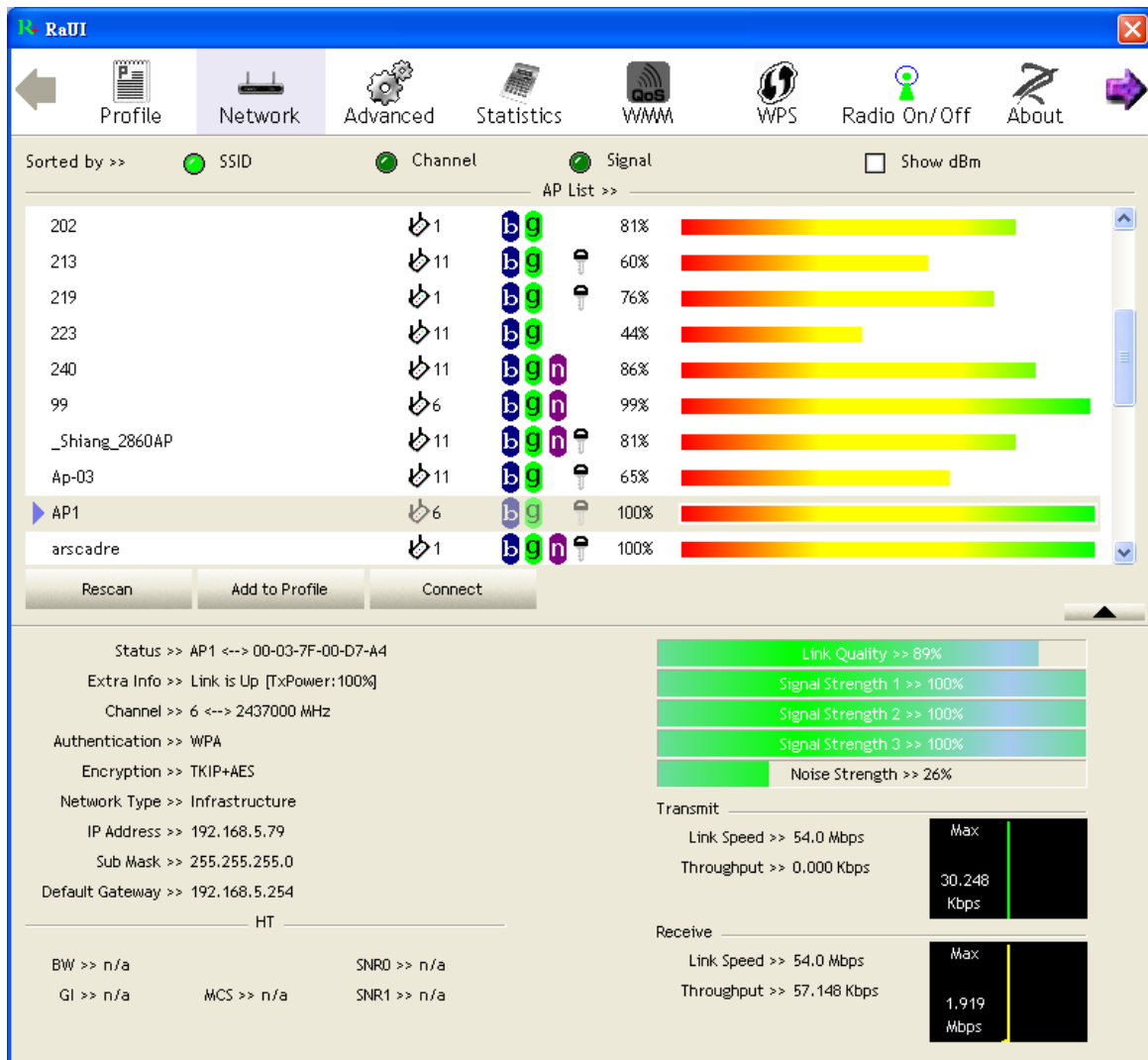
3. Click "OK". The dialog box should appear as the image below.



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

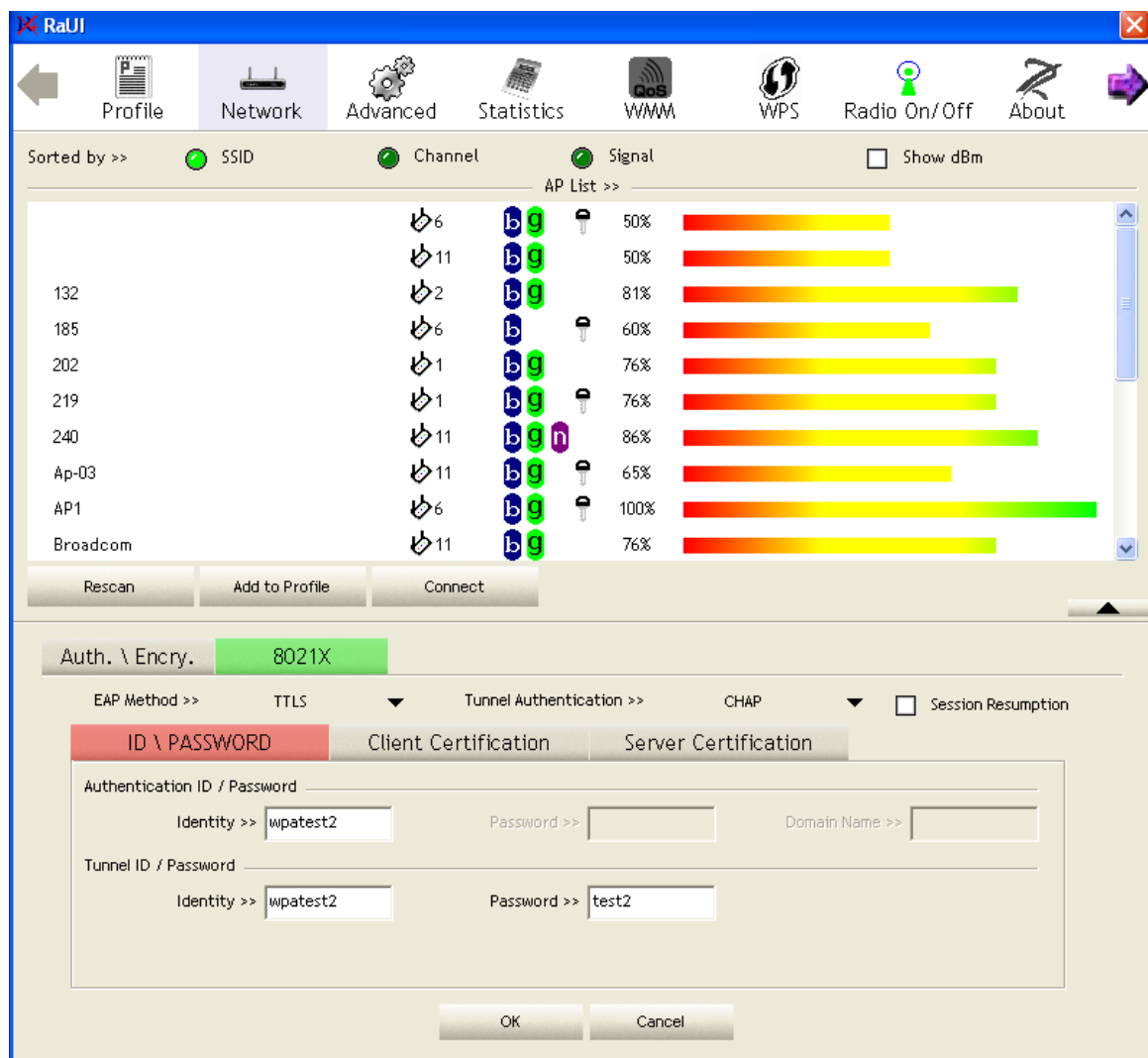
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

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

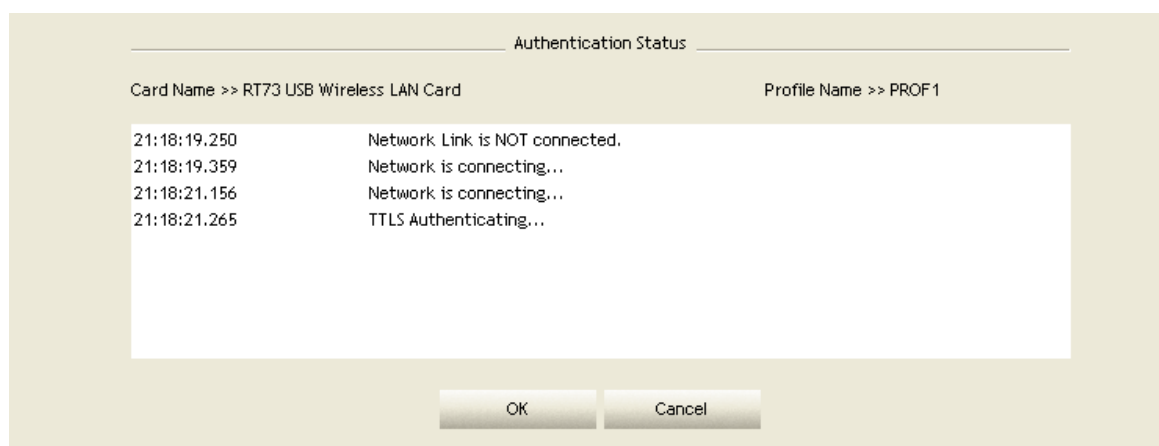


TTLS:

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.



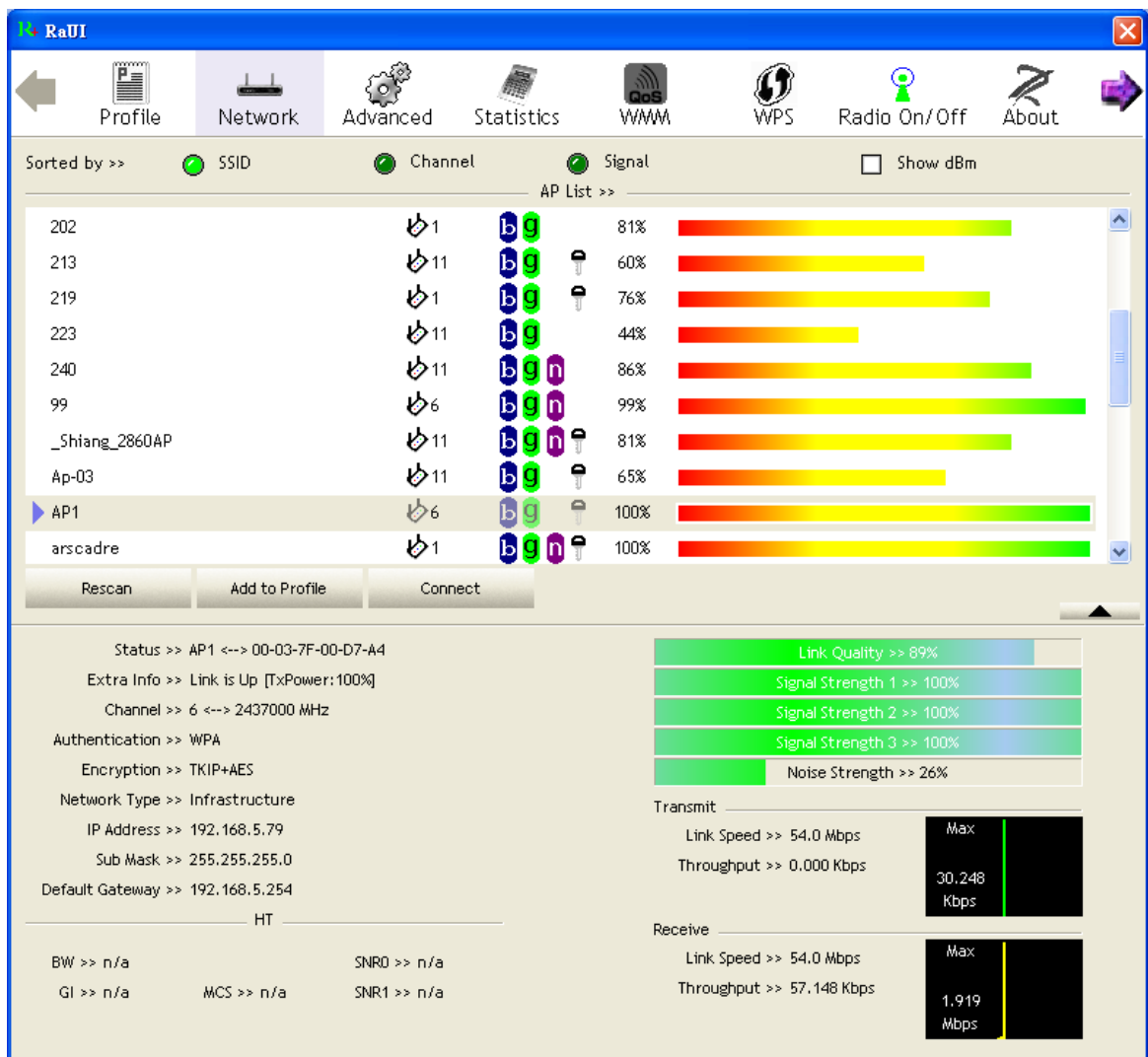
2. Click "OK". The dialog box should appear as the image below.



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

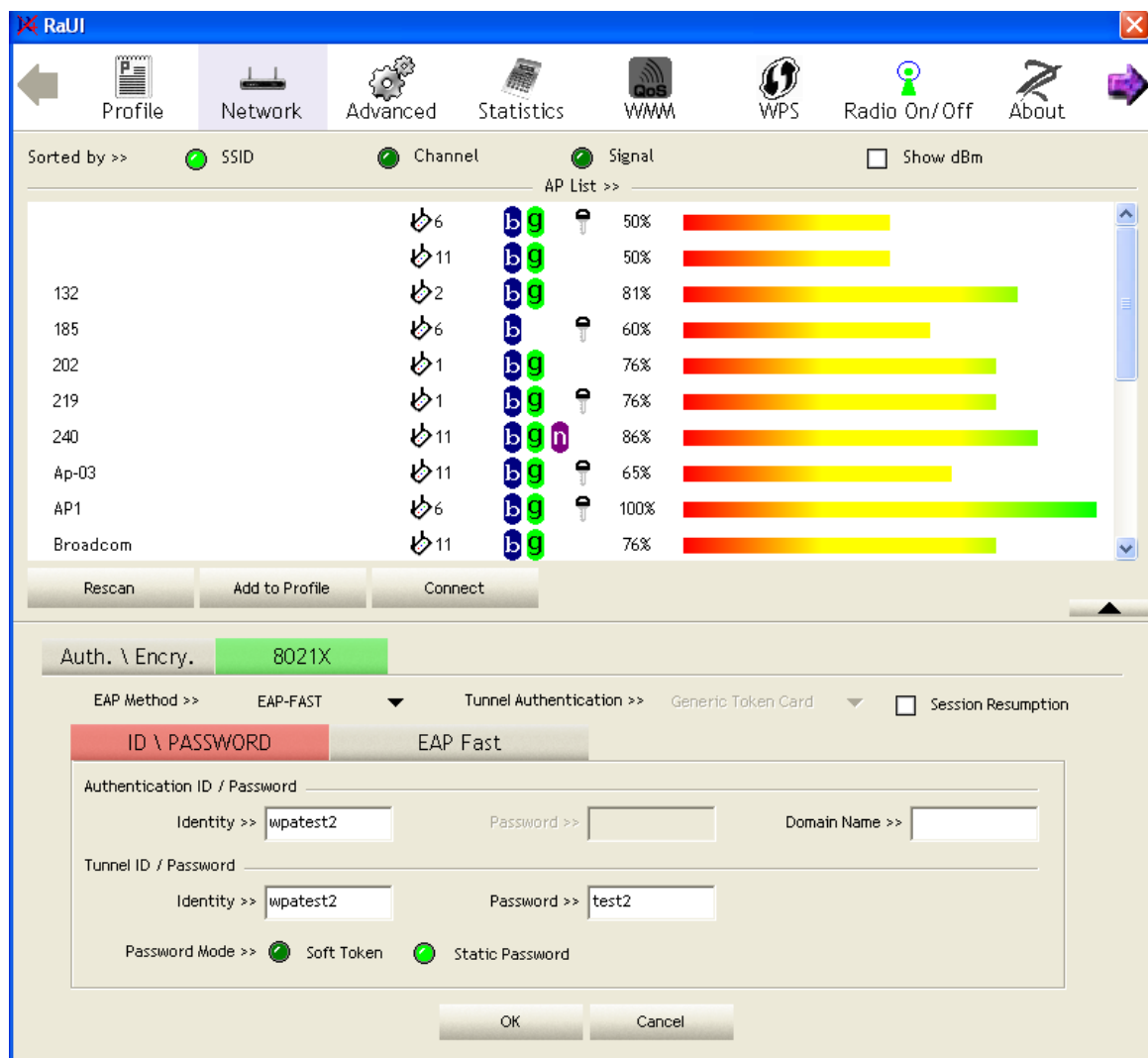
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

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

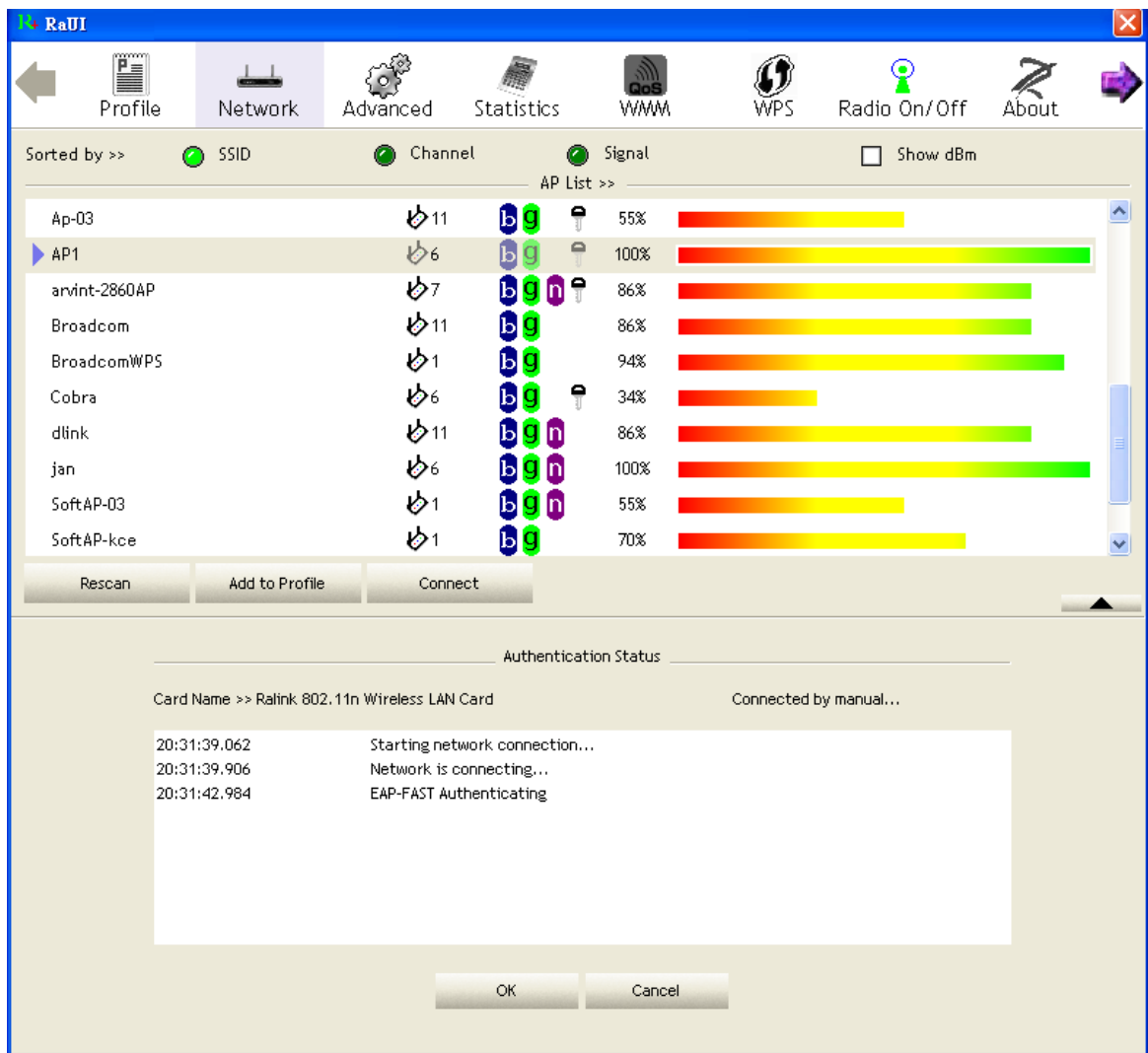


EAP-FAST :

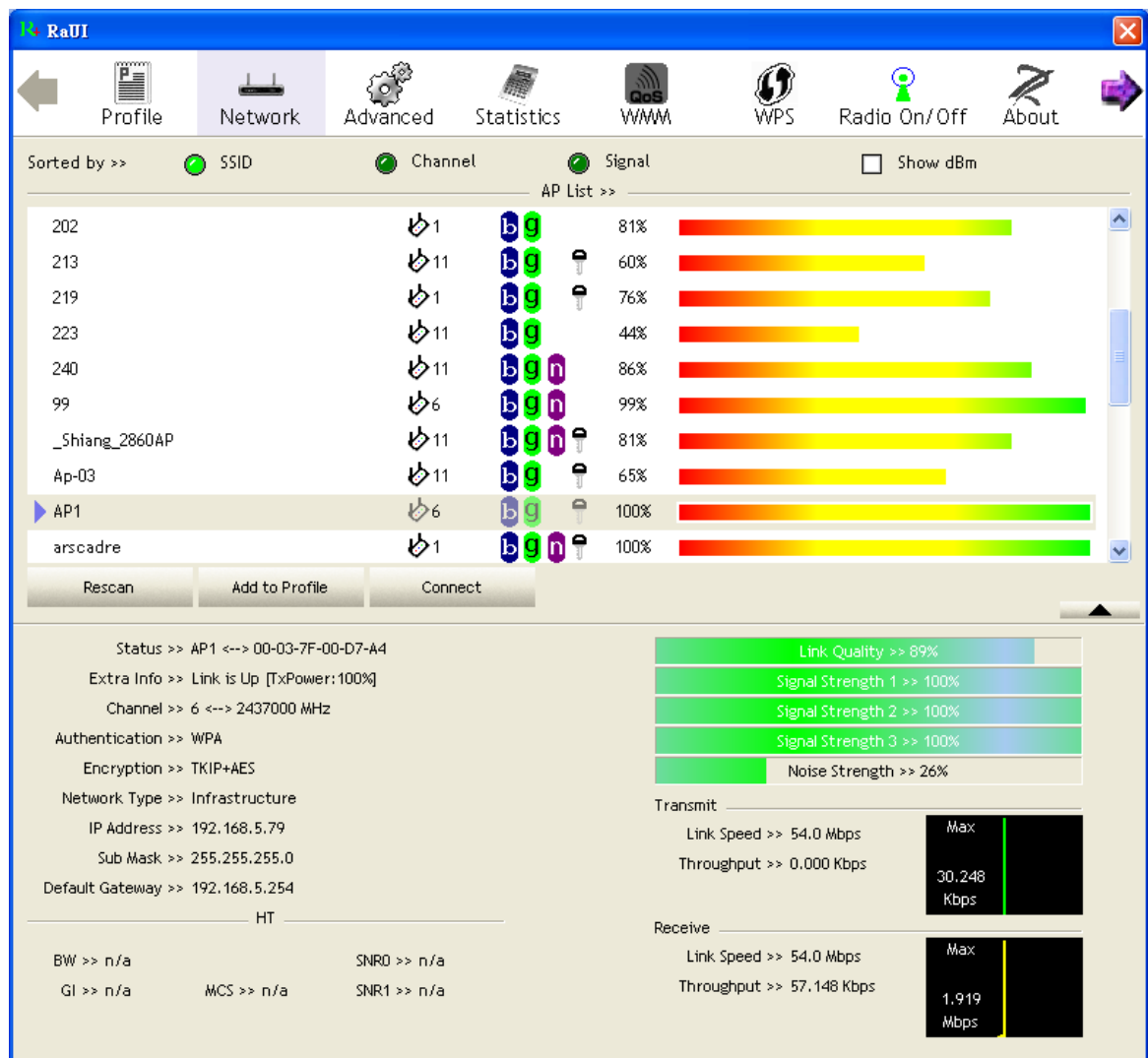
1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. Tunnel Protocol only supports "Generic Token Card" now. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's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



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



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



*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 cannot 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.