



Wireless Adapter RNX-G300EX/LX
User Manual



CONTENT

Introduction	- 2 -
Specifications	- 3 -
Installation	- 4 -
Hardware Installation	- 4 -
Software Installation (for all windows OS)	- 5 -
Software Uninstall	- 9 -
Ralink Wireless Utility (RaUI) or Windows Zero Configuration (WZC)	- 10 -
Use WZC to configure wireless NIC	- 12 -
Start RaUI	- 19 -
Profile	- 26 -
Icons and buttons :	- 27 -
Add/Edit Profile	- 28 -
Example to Add Profile in Profile	- 30 -
Network	- 34 -
Icons and buttons :	- 35 -
Connected network :	- 36 -
Example on Adding Profile in Network	- 42 -
Advanced	- 46 -
Icons and buttons:	- 47 -
Statistics	- 47 -
Icons and buttons:	- 48 -
WMM	- 49 -
Icons and buttons:	- 49 -
Example to Configure to Enable DLS (Direct Link Setup)	- 50 -
Example to Configure to Enable Wi-Fi Multi-Media	- 56 -
Example to Configure to Enable WMM Power Save	- 58 -
WPS	- 59 -
Icons and buttons:	- 60 -
WPS Information on AP	- 61 -
Example to Add to Registrar Using PIN Method	- 63 -
Example to Add to Registrar Using PBC Method	- 69 -
Example to Configure a Network/AP Using PIN or PBC Method	- 74 -
Link Status	- 77 -
Auth. \ Encry. Setting - WEP/TKIP/AES	- 78 -
802.1x Setting	- 79 -
Authentication type :	- 79 -
Authentication :	- 80 -
- ID \ PASSWORD -	- 80 -
- Client Certification -	- 80 -
- EAP Fast -	- 81 -
- Server Certification -	- 81 -
Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is Failed in Profile	- 82 -
Example to Configure Connection with WEP on	- 86 -
Example to Configure Connection with WPA-PSK	- 90 -
Example to Configure Connection with WPA	- 94 -
EAP-FAST :	- 107 -
Acknowledgements	- 110 -

INTRODUCTION

Thank you for purchasing Wireless LAN PCI Card. Wireless card is a perfect combination product of performance and cost-effectiveness. It is sincerely hoped that you can enjoy the wireless world through this solidly profiled wireless card.

It provides a full solution of the IEEE 802.11b/g protocols, this solution passed the

WiFi tests that are compatible with all the wireless products with WiFi logo. If you

have a wireless card on hand, it means you can connect to the wireless world without any difficulty.

It provides all the data rates in the IEEE 802.11b/g standards, which confines the highest data rate as 54Mbps. In addition, it rewards customers with proprietary

“Turbo mode” for a better throughput as well as supports both the short and long preambles to ensure the compatibilities with legacy wireless products and new ones, saving the panic works for finding compatible products.

Since the security has become one of the most important issue in the wireless society,

it provides you with the full security coverage from the naïve 64/128bits Wep encryptions, second generation WPA-PSK and WPA-AES encryption, to the most advanced WPA2-PSK and WPA2-AES encryption. WPA2 is the latest security standard currently approved by WiFi standard.

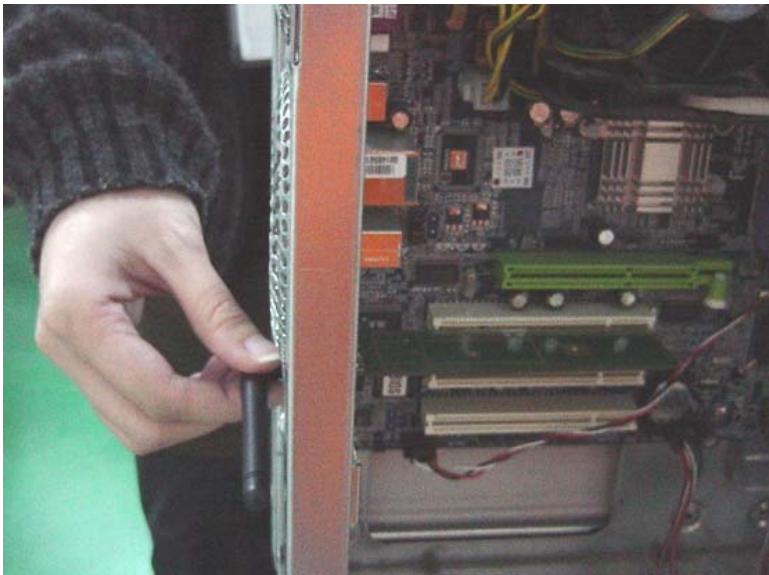
SPECIFICATIONS

Interface	PCI
Standard	802.11b, 802.11g
OS support	98SE, WinME, Win2000, WinXP32, WinXP64, Vista32, Vista64
Data rate	1,2,5.5,11,6,8,12,18,24,36,48,54Mbps, depends on the wireless mode
Frequency band	BG:2.4 ~ 2.497 GHz
Operation Channel	1~11(BG)
Coverage Area	Indoors: 100m (BG) Outdoors: 400m (BG)
Compatibility	Fully compatible with IEEE 802.11 b/g devices
Operation Mode	Infrastructure and AdHoc
Security Capacity	64-bit/128-bit WEP, TKIP,WPA-AES, and WPA2-PSK,WPA2-AES
Antenna	External antenna
LED	LED0: On: link is on. Off: link is off LED1:Blinking: data transition
Turbo mode	Active when there is no other station around
Power Saving mode	Fast wake up and maximum power saving
Other features	Dynamically adjust power for the most stable and best throughput Dynamically adjust receiving ability for the best receiving Compiled with all the main radio regulations

INSTALLATION

HARDWARE INSTALLATION

1. Turn off your PC and remove the cover.
2. Insert the RNX-G300EX/ LX to an available PCI slot firmly.
3. Secure this card to the rear of the computer chassis
4. Put back the cover.
4. Fix the antenna to the antenna connector of the card.
5. Turn on the computer.



SOFTWARE INSTALLATION (FOR ALL WINDOWS OS)

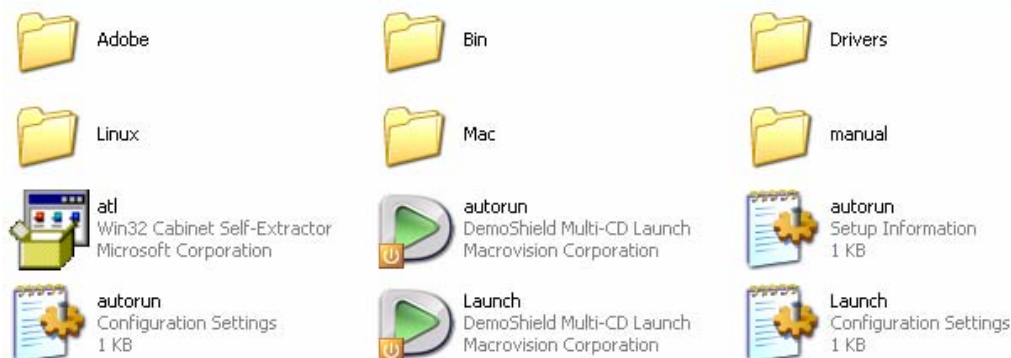
After hardware installation complete, system will detect new hardware automatically as below:

Found New Hardware Wizard window pops up, click **Cancel**.



Insert the driver disk into your DVD-ROM.

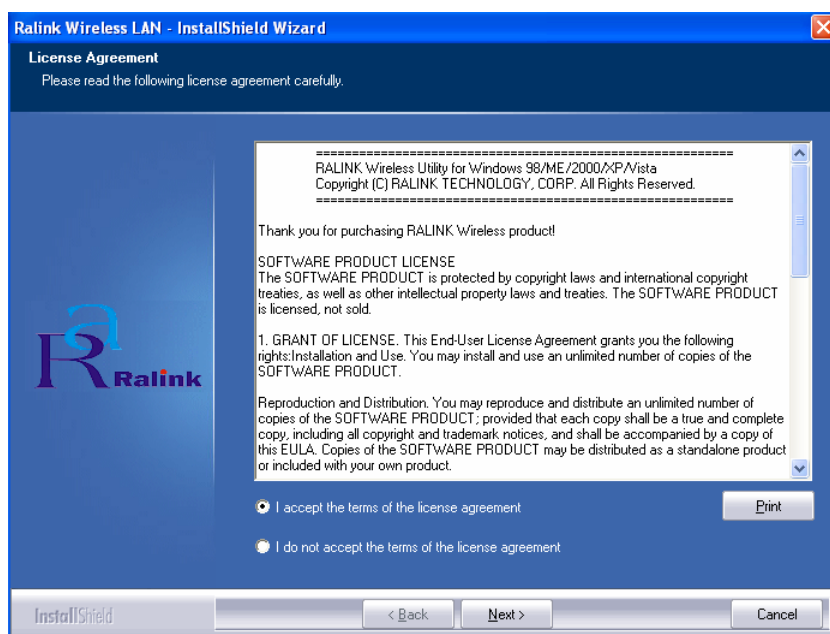
Click My Computer icon, then click DVD-ROM, then click autorun



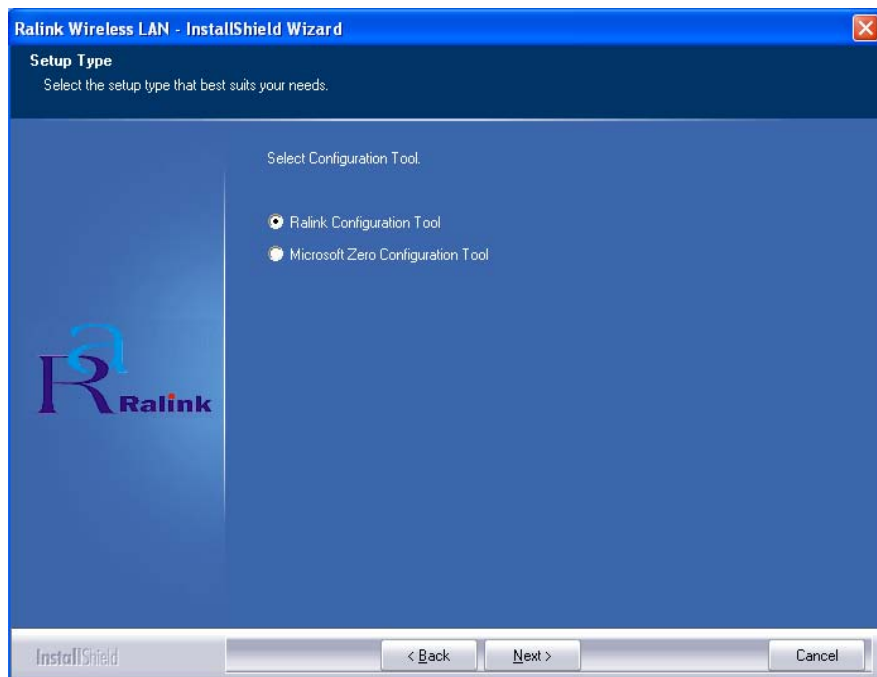
Click Driver Installation



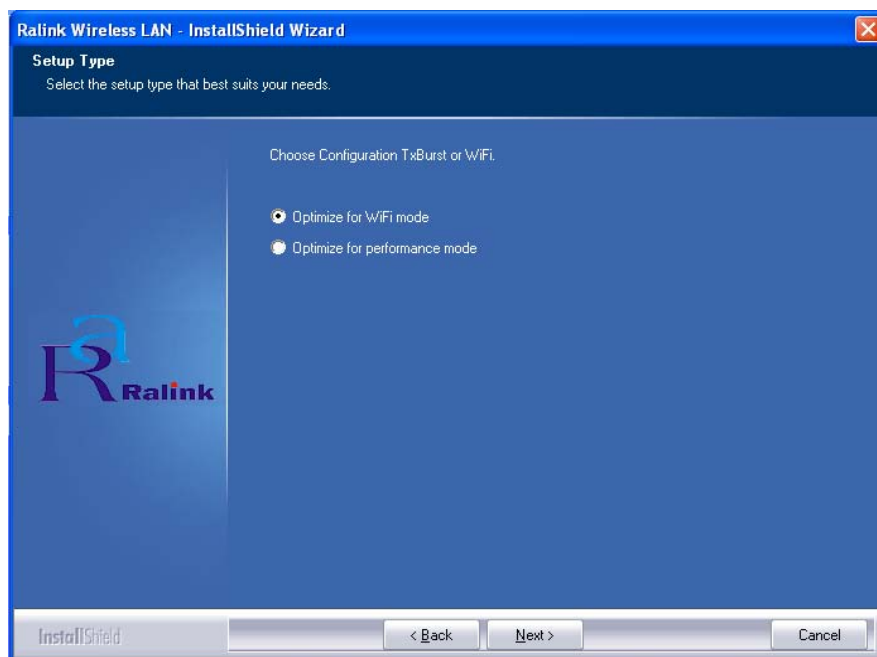
Click I accept the term of the license agreement ,then click Next icon.



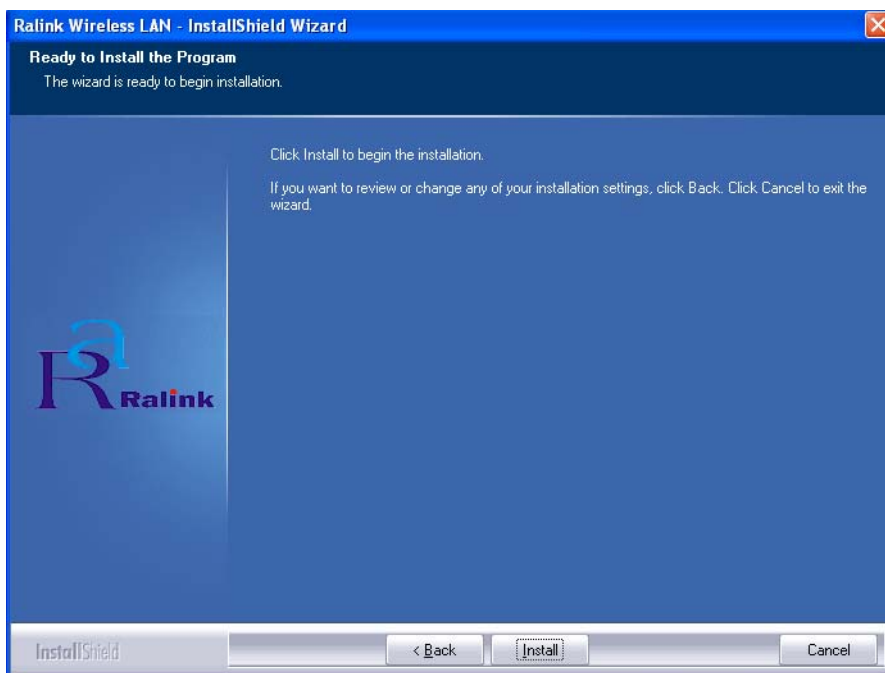
Click Ralink Configuration Tool, then click Next icon.



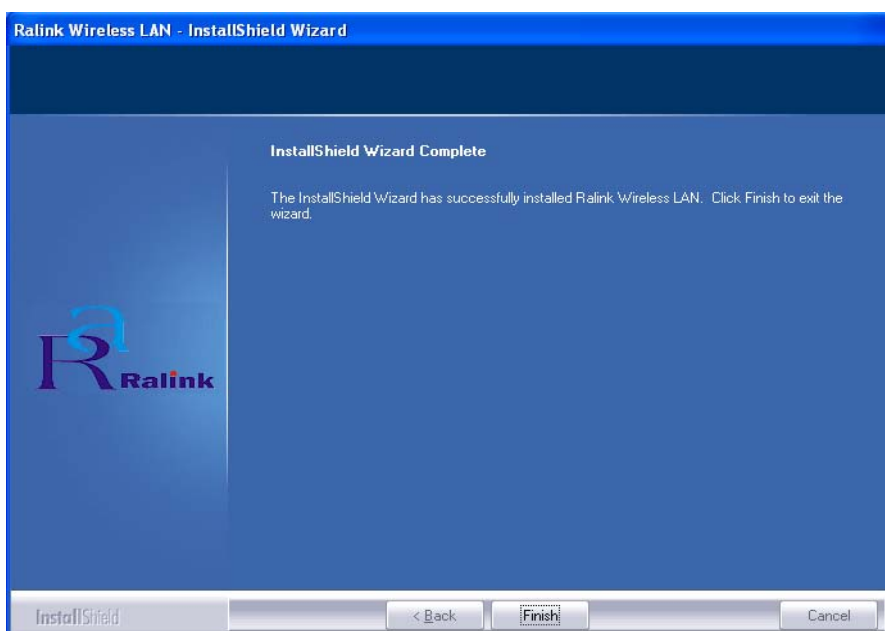
Click Optimize for WiFi modes, then click Next icon.



Click Install icon.

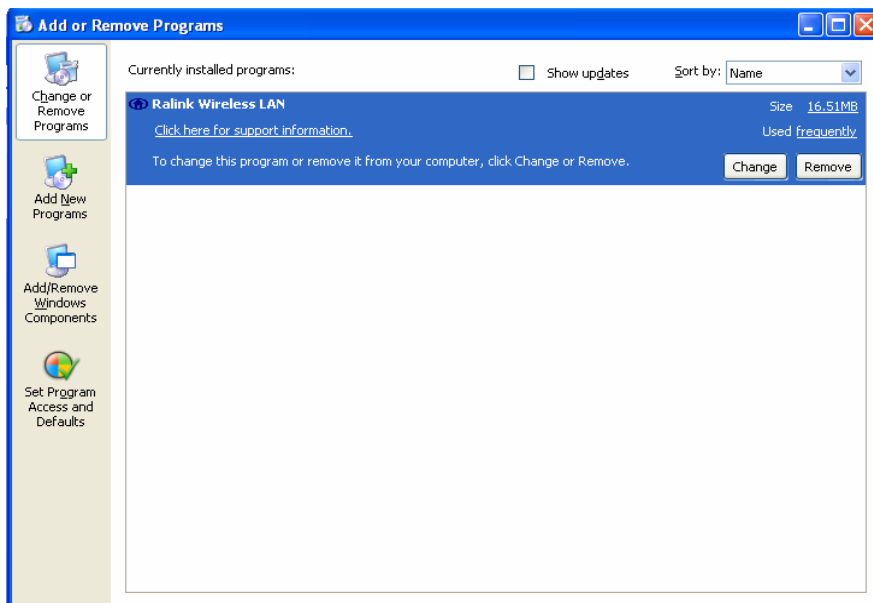


Click Finish icon.

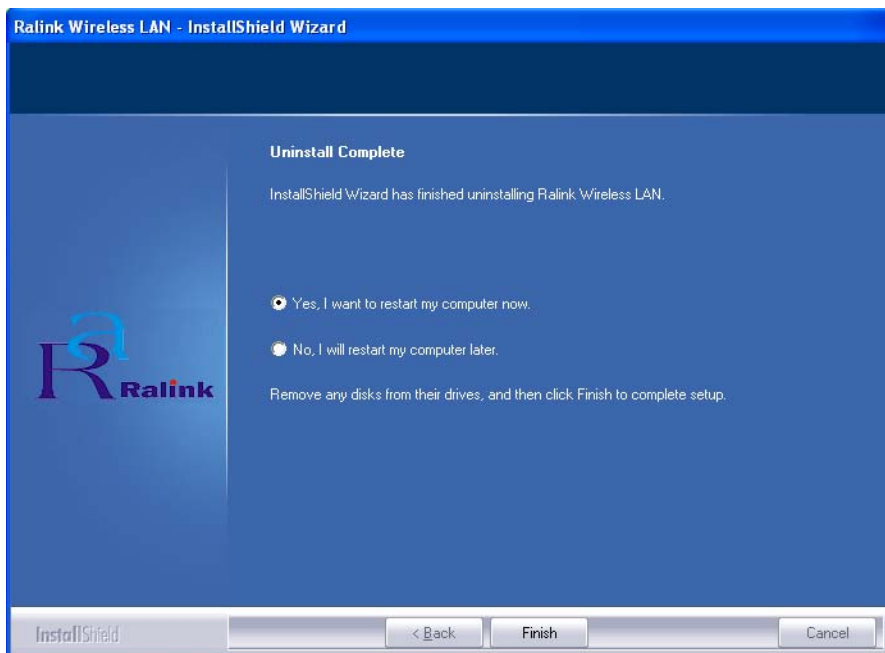


SOFTWARE UNINSTALL

Click My Computer icon, then click Add or Remove Program icon, and then click Ralink Wireless LAN icon and then click Remove icon.



Click Yes, I want to restart my computer now icon, and then Finish icon.



RALINK WIRELESS UTILITY (RAUI) OR WINDOWS ZERO CONFIGURATION (WZC)

In windows XP, it provides wireless configuration utility named "Windows Zero configuration" which provides basic configuration function for Ralink Wireless NIC. Ralink's utility (RaUI) provides WPA supplicant functionality. To make it easier for user to select

the correct utility. RaUI will let user make the selection when it first runs after windows XP boots.

Click Figure 1-1 the icon will bring up the selection window and let user make the selection.



Figure 1-1 RaUI.exe

RaUI can co-exist with WZC. When coexisting with WZC, RaUI only provides monitoring function, such as link status, network status, statistic counters, advance 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 on the section. We will explain the difference between RaUI and WZC. Figure 1-3 shows the RaUI status when WZC is active as main control utility.

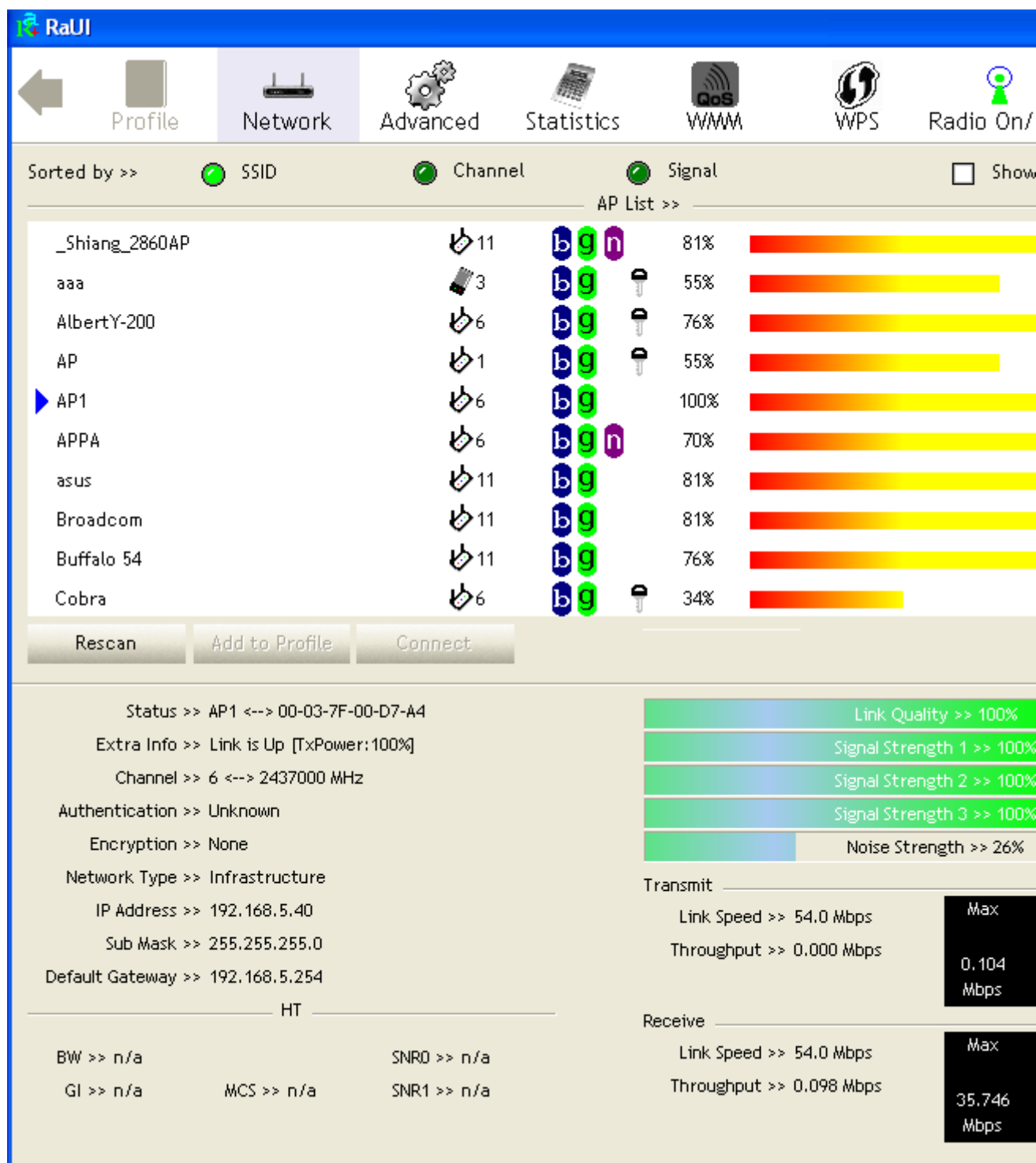


Figure 1-3 RaUI status with WZC active

When activating WZC, there are couple difference on RaUI status compared to that with out WZC running.

- A. Profile button will be gray, profile function is removed since the NIC is controlled by WZC
- B. The connect and add profile function will be gray. The reason is same as the first difference.

For all other functions provided by RaUI, please read through this document for full detail.

USE WZC TO CONFIGURE WIRELESS NIC

A. If connection is lost or not connected, the status prompt as Figure 1-4 will pop up.

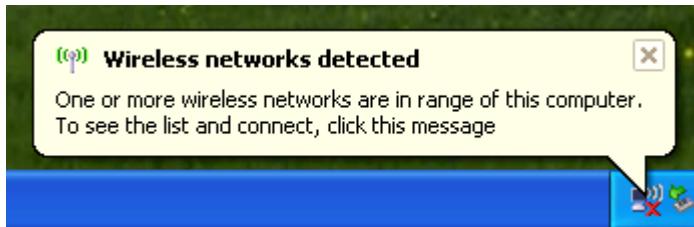


Figure 1-4 status prompt of no connection

B. Right-click the network connection icon in task bar.

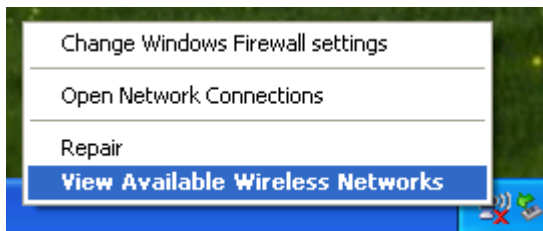


Figure 1-5 Select WZC main status

C. Select "View Available Wireless Networks" will pop up the dialog shown as Figure 1-6.

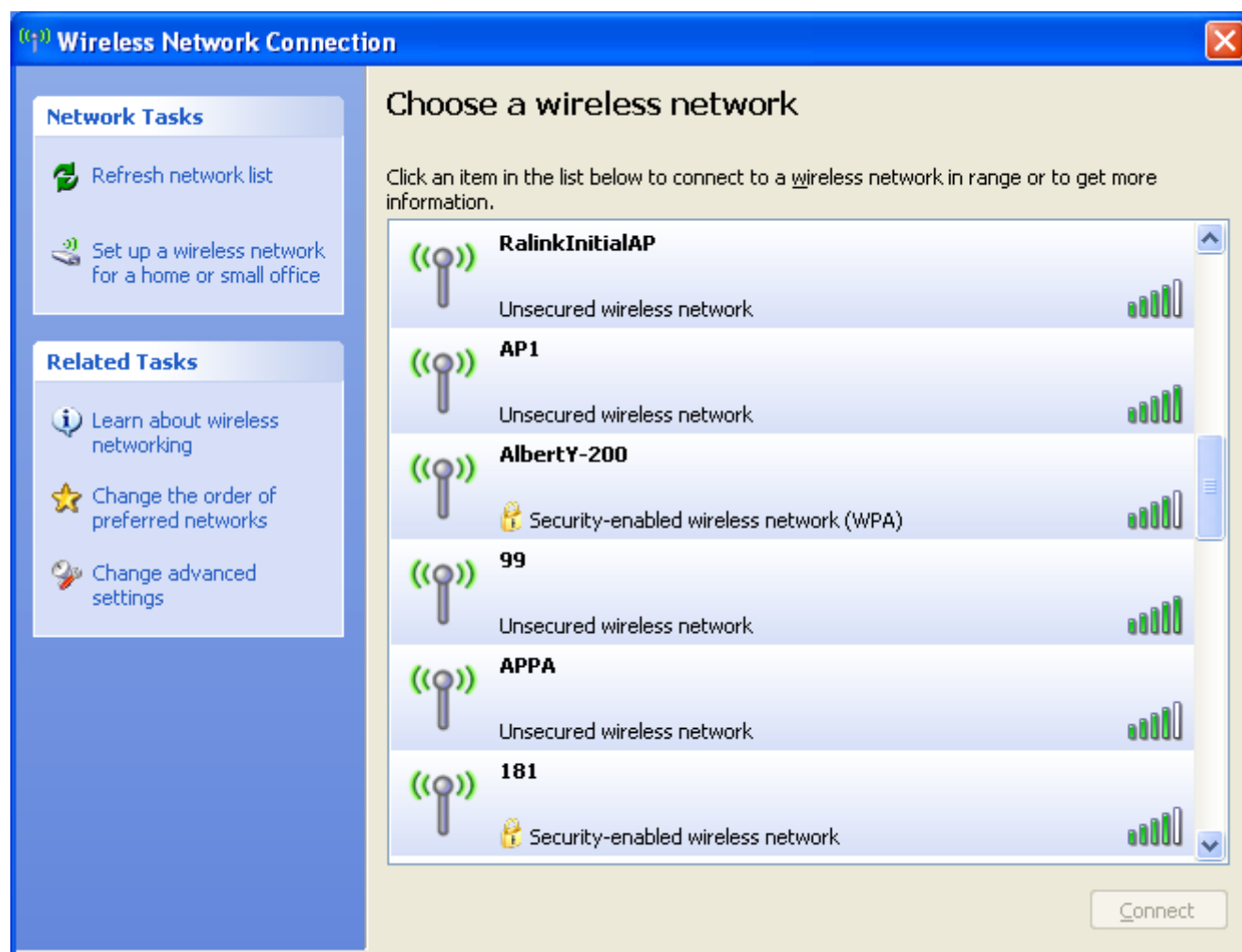


Figure 1-6 Wireless Network Connection

D. Select intended AP and click "Connect" shown as Figure 1-7. Then click "Connect Anyway" shown as Figure 1-8.

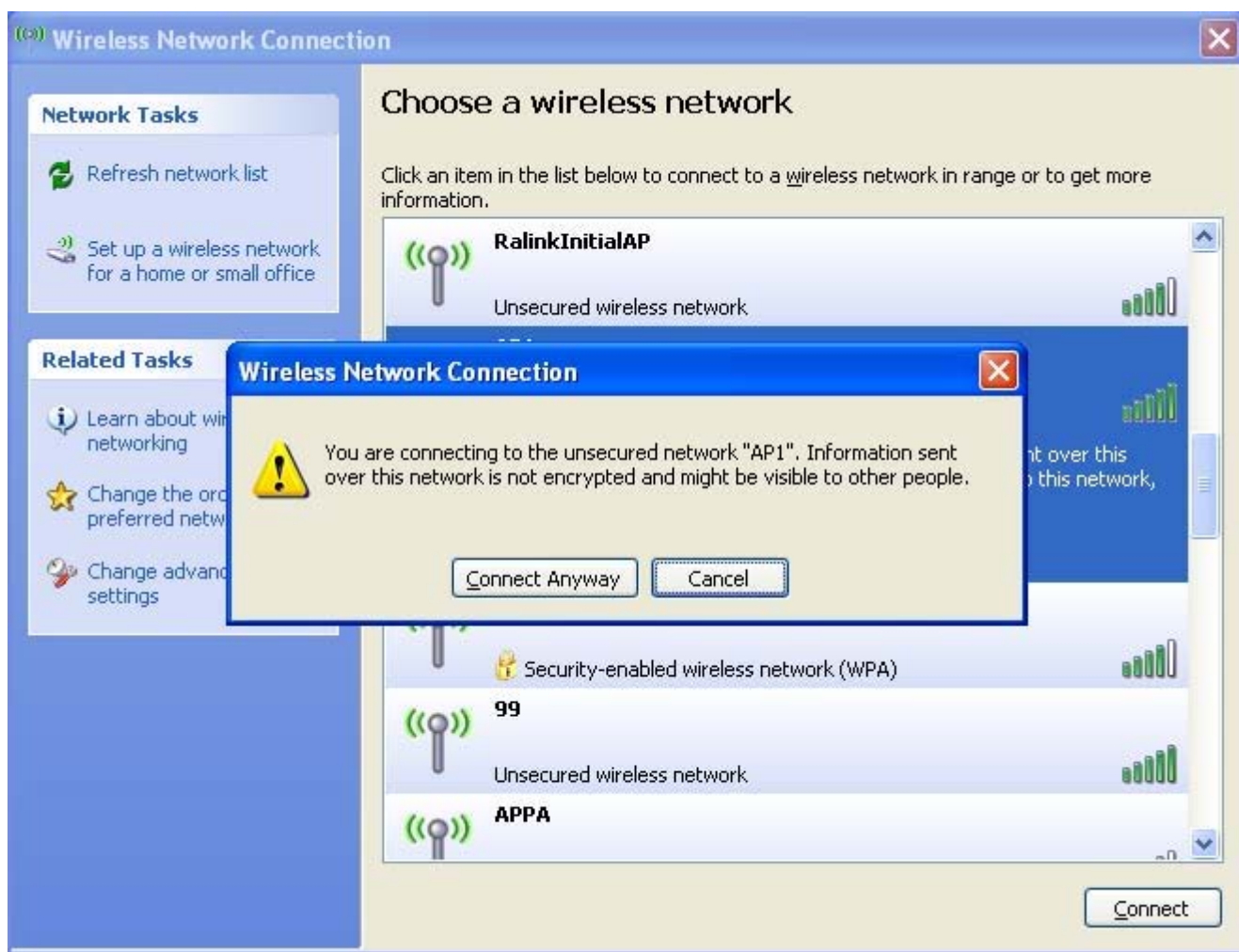


Figure 1-7 Select intended AP : AP1, then click "Connect"

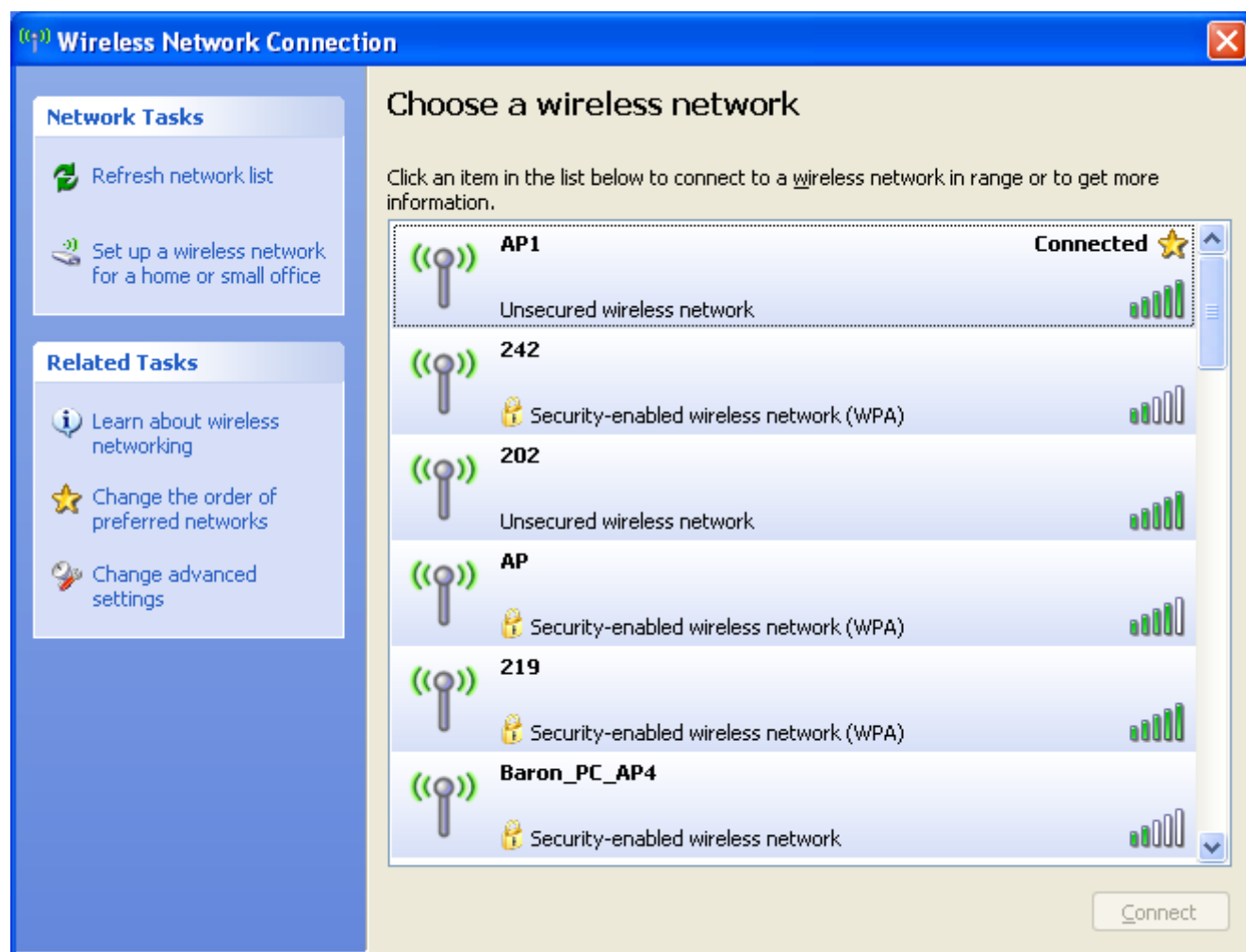


Figure 1-8 Connect AP : AP1 successfully

E. If you want to modify information about AP, click "Change advanced settings" shown as Figure 1-9. Then choose "Wireless Networks" label shown as Figure 1-10.

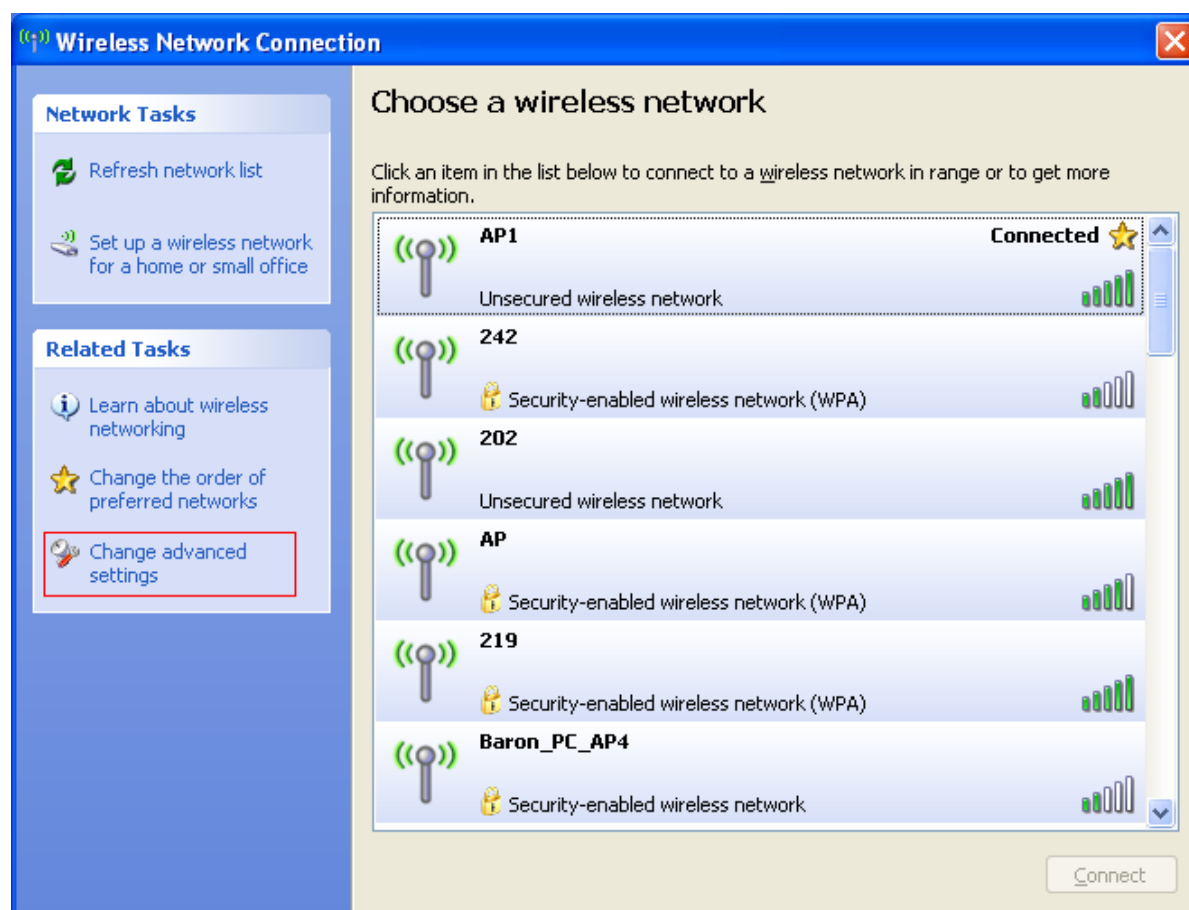


Figure 1-9 Click "Change advanced settings"

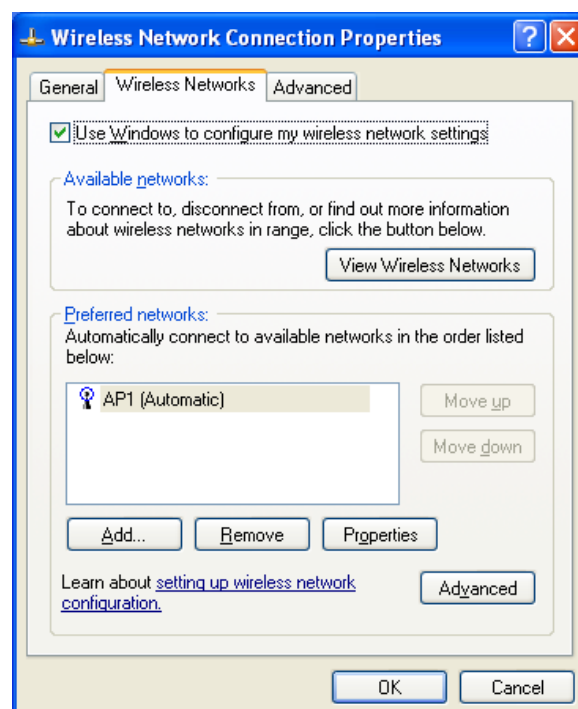


Figure 1-10 Choose "Wireless Networks" label

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

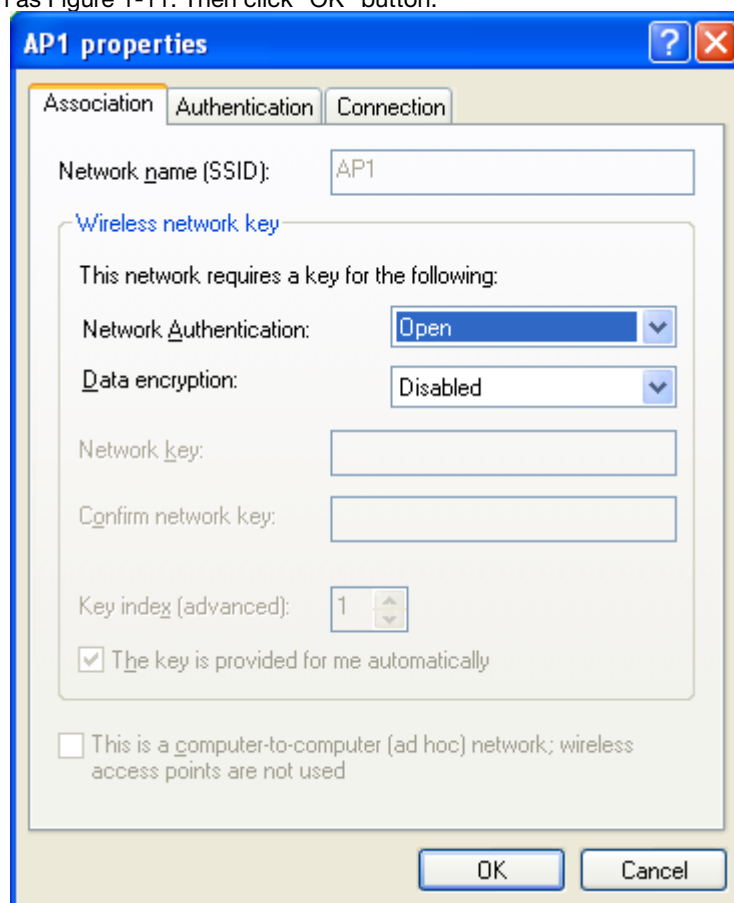


Figure 1-11 AP's properties

G. After filling appropriate value, click "OK" button. And the status will prompt up as Figure 1-12.

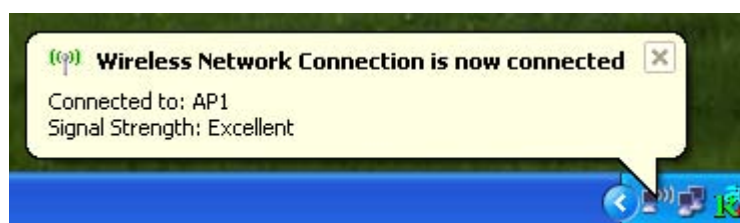


Figure 1-12 Network connection status

H. Click the Ralink's icon will bring up RaUI main window. User can find the surrounding APs in the list. The current connected AP will also shown with the green icon indicated as Figure 1-13. User may use the advance tab to configure more advanced features provided by Ralink's wireless NIC. For the detail on configure the advanced features, please check the Advance setting section for detail.

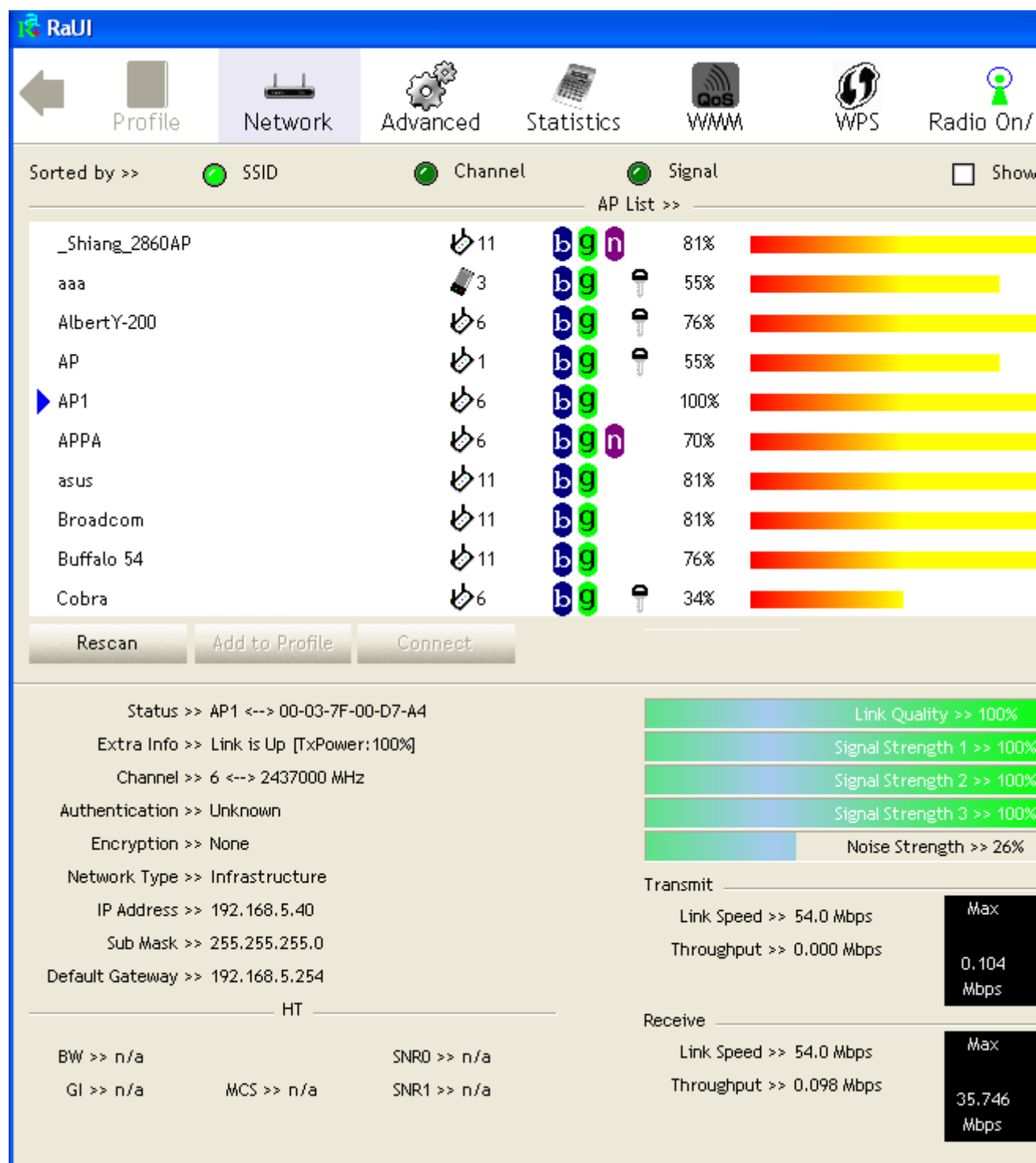


Figure 1-13 Show connection status by using WZC to do connection

START RAUI

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

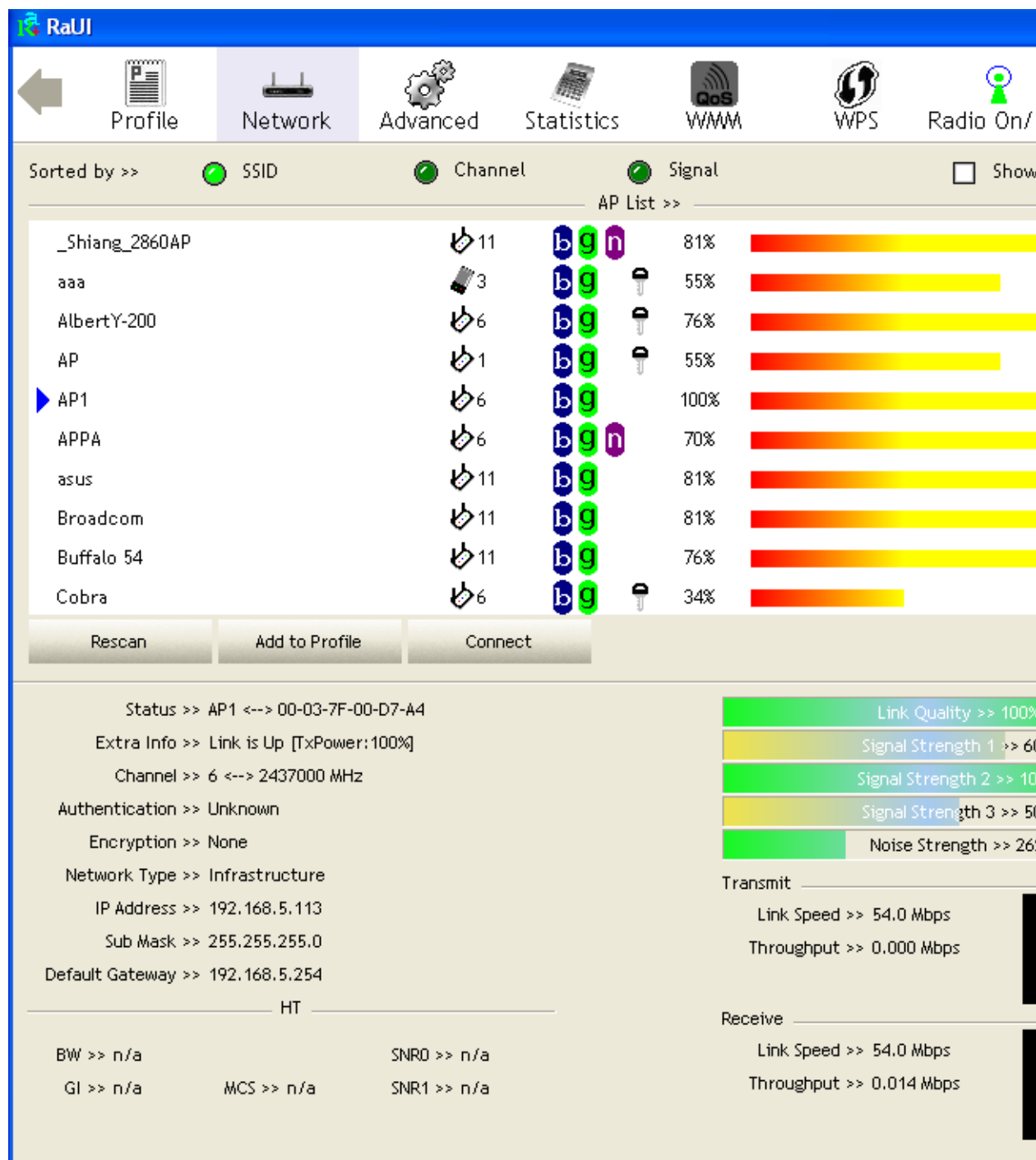


Figure 2-1-1 RaUI section introduction

There are three sections in RaUI. These sections are briefly described as follow.

A. Button Section : Include Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, About button, Radio On/Off button and Help button.



Figure 2-1-2 Button section



Figure 2-1-3 Move to the left



Figure 2-1-4 Move to the right

B. Function Section : Corresponding button.



Figure 2-1-5 Profile page

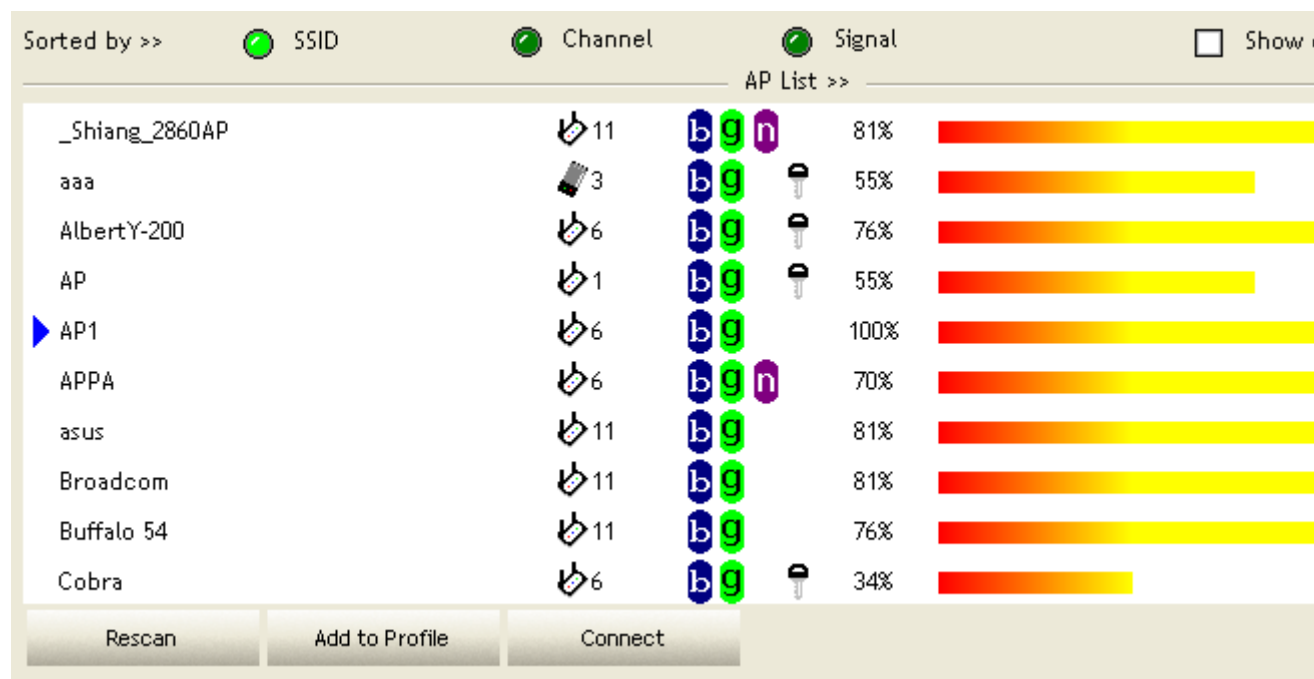


Figure 2-1-6 Network page

Wireless mode >> 802.11 A/B/G/N mix

☐ Enable CCX (Cisco Compatible eXtensions)

☐ Turn on CCKM

☐ Enable Radio Measurements

☐ Non-Serving Channel Measurements limit 250

☐ Enable TX Burst

☐ Enable TCP Window Size

☐ Fast Roaming at -70 dBm

☐ Show Authentication Status Dialog

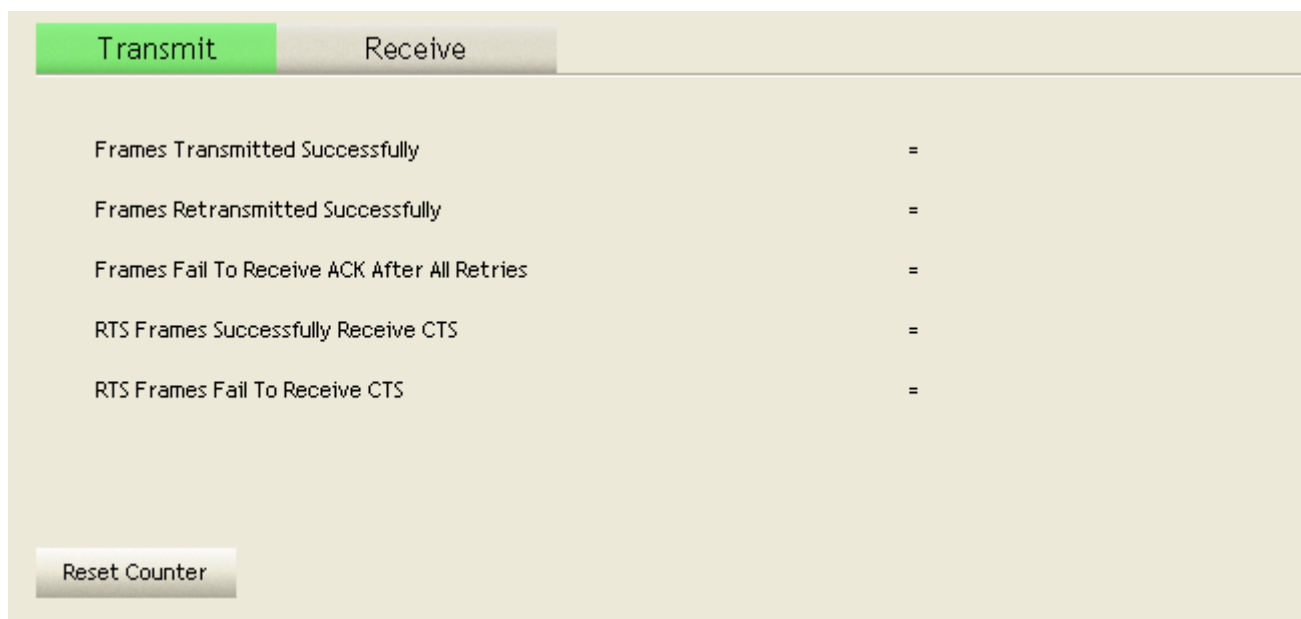
Select Your Country Region Code

11 B/G >> 0: CH1-11

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

Apply

Figure 2-1-7 Advance page

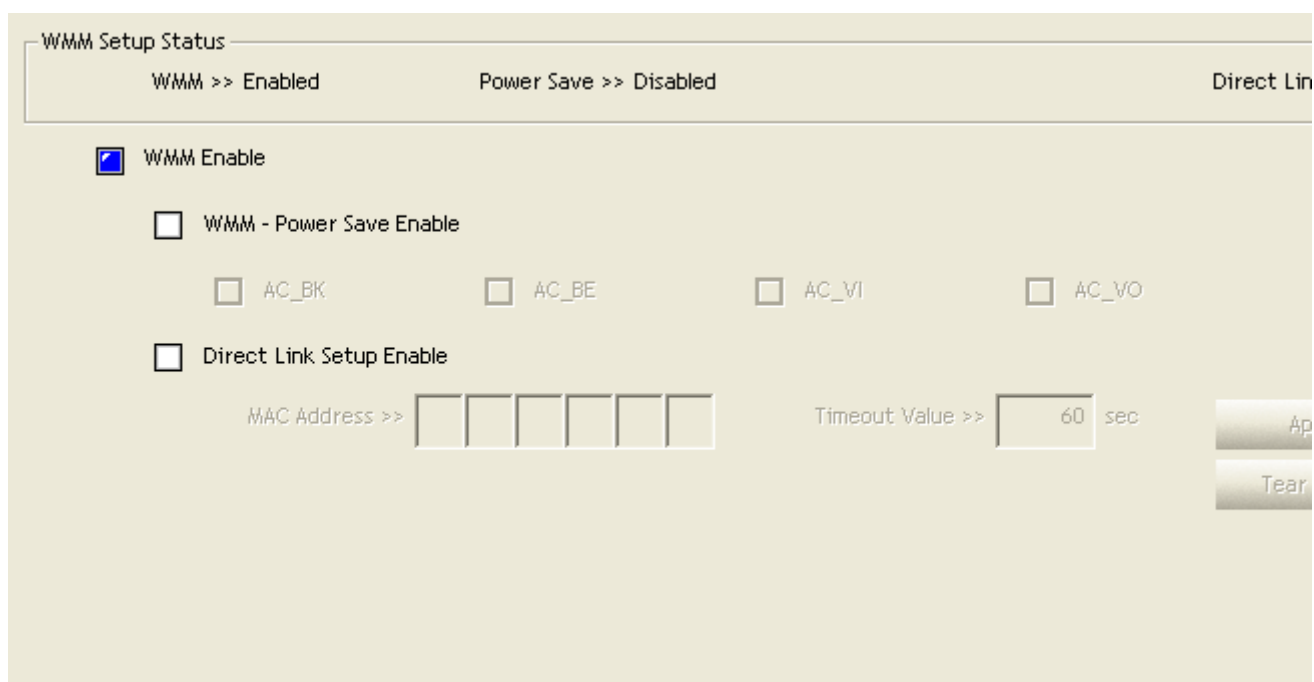


The screenshot shows a web interface with two tabs: 'Transmit' (active) and 'Receive'. Below the tabs is a table of statistics. The table has two columns: the first column lists the statistic names, and the second column shows the values, all of which are currently empty. At the bottom left, there is a 'Reset Counter' button.

Transmit	Receive
Frames Transmitted Successfully	=
Frames Retransmitted Successfully	=
Frames Fail To Receive ACK After All Retries	=
RTS Frames Successfully Receive CTS	=
RTS Frames Fail To Receive CTS	=

Reset Counter

Figure 2-1-8 Statistics page



The screenshot shows the 'WMM Setup Status' page. At the top, it displays 'WMM >> Enabled' and 'Power Save >> Disabled'. On the right, there is a 'Direct Link' button. Below this, there are several checkboxes: 'WMM Enable' (checked), 'WMM - Power Save Enable' (unchecked), and 'Direct Link Setup Enable' (unchecked). Under 'WMM - Power Save Enable', there are four checkboxes: 'AC_BK', 'AC_BE', 'AC_VI', and 'AC_VO', all of which are unchecked. Below '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'. On the right side, there are two buttons: 'Ap' and 'Tear'.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link

☒ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☐ Direct Link Setup Enable

MAC Address >>

Timeout Value >> sec

Ap

Tear

Figure 2-1-9 WMM page

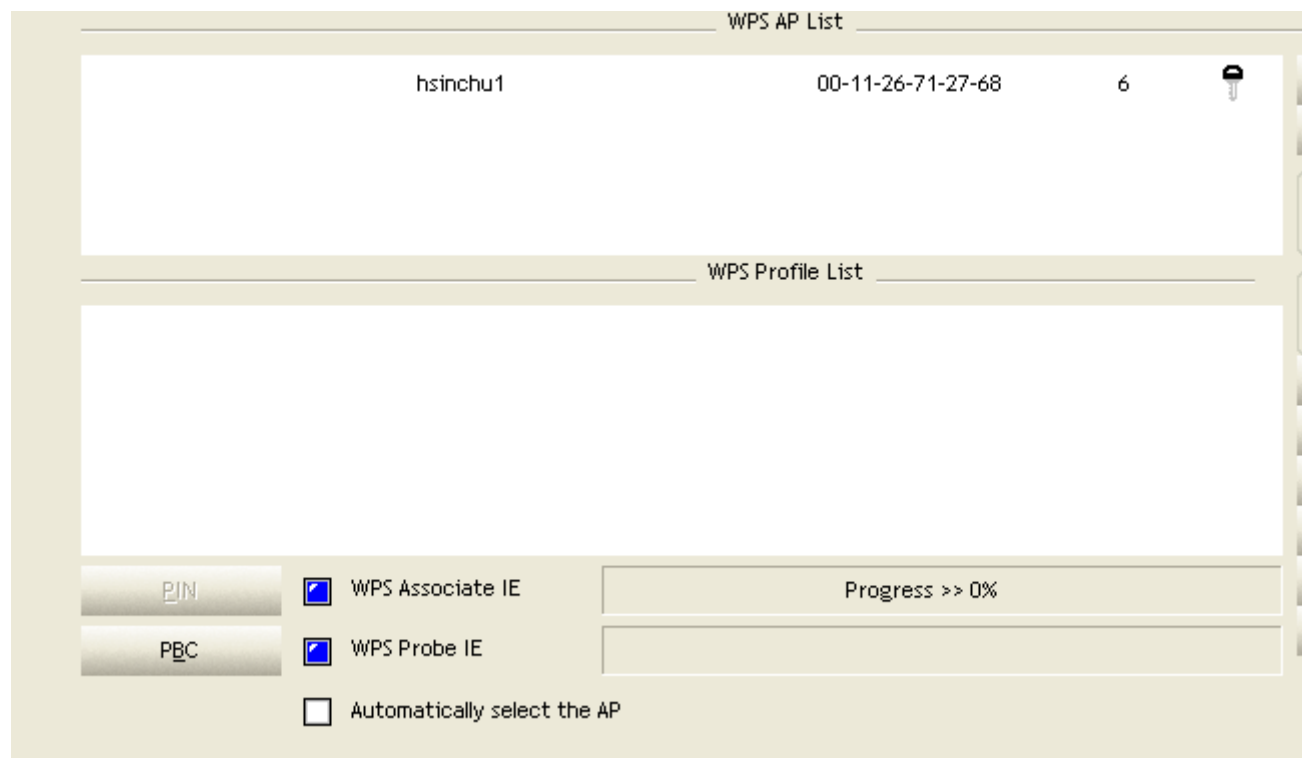


Figure 2-1-10 WPS page



Figure 2-1-11 About page

C. Status Section : Include Link Status, Authentication Status, AP's information, Configuration and retrying the connection when authentication is failed.

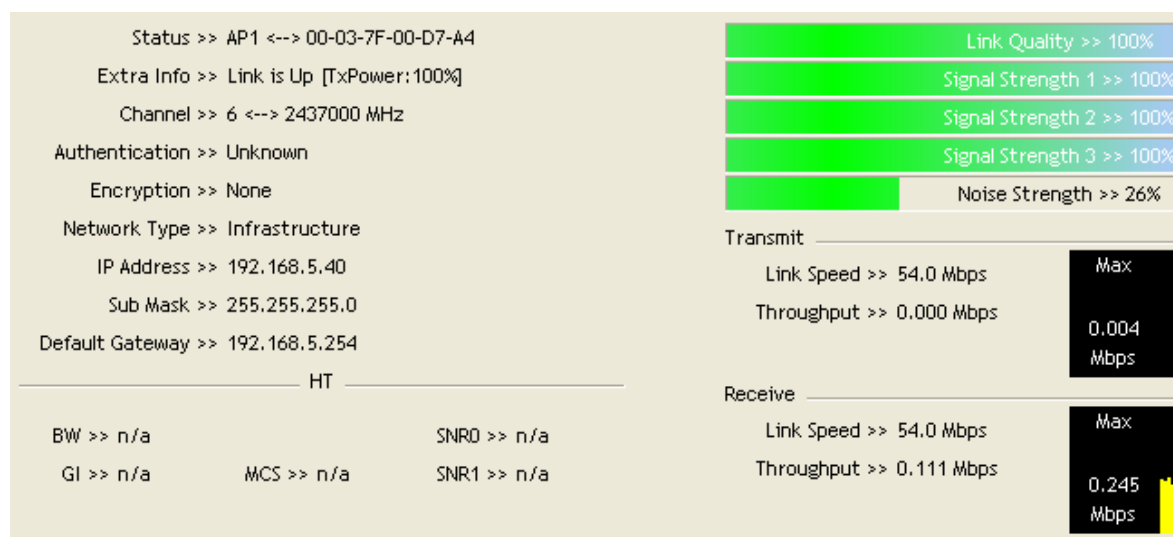


Figure 2-1-12 Link Status

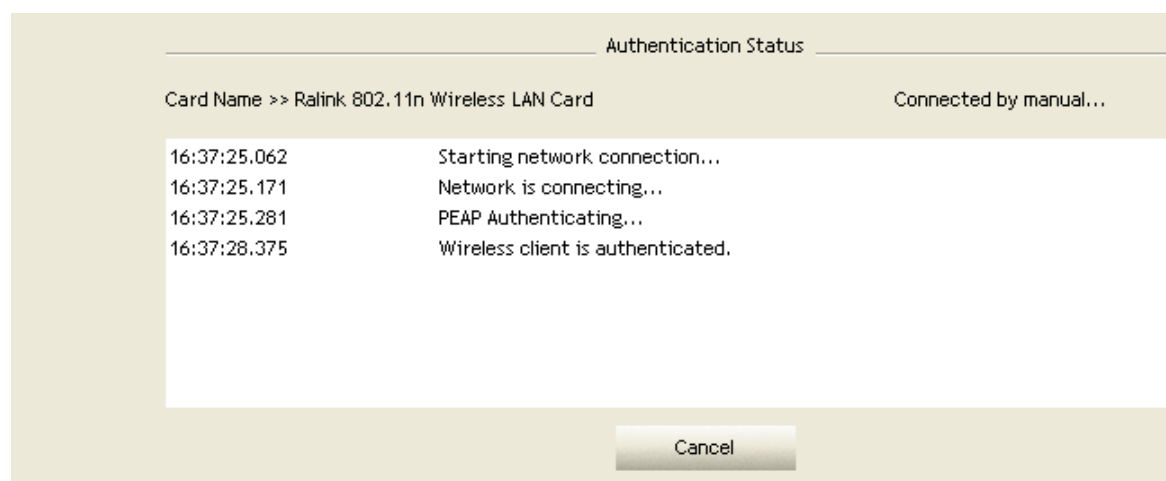


Figure 2-1-13 Authentication Status

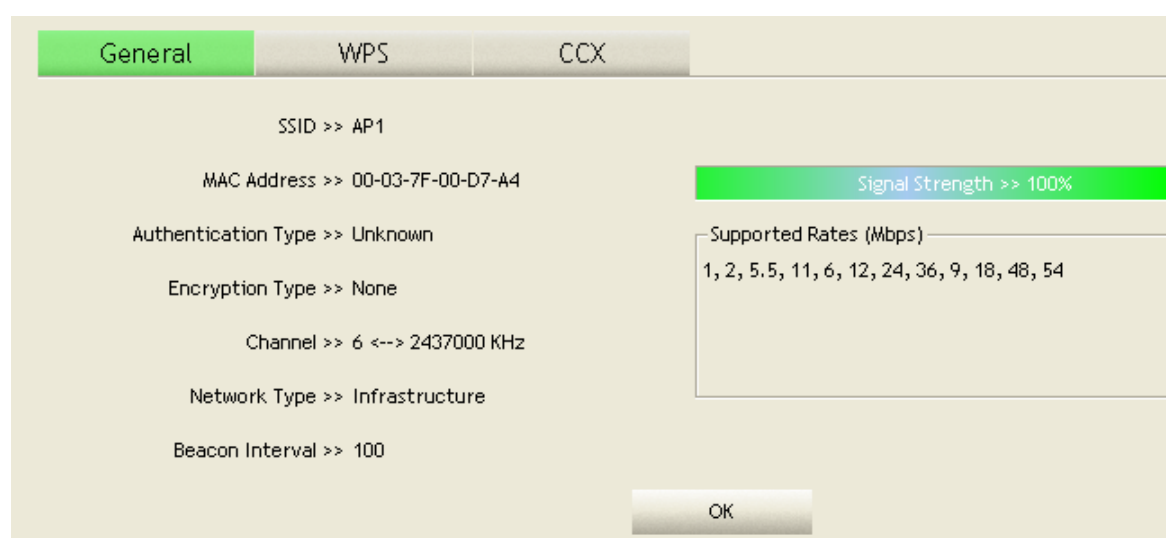


Figure 2-1-14 AP's Information

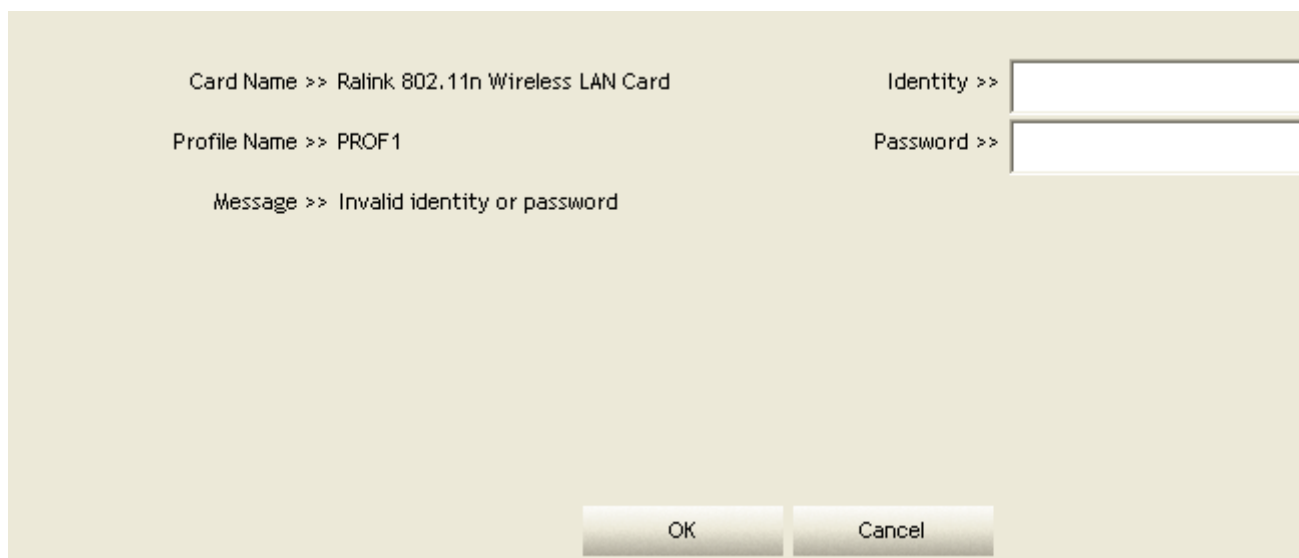


Figure 2-1-15 Retry the connection

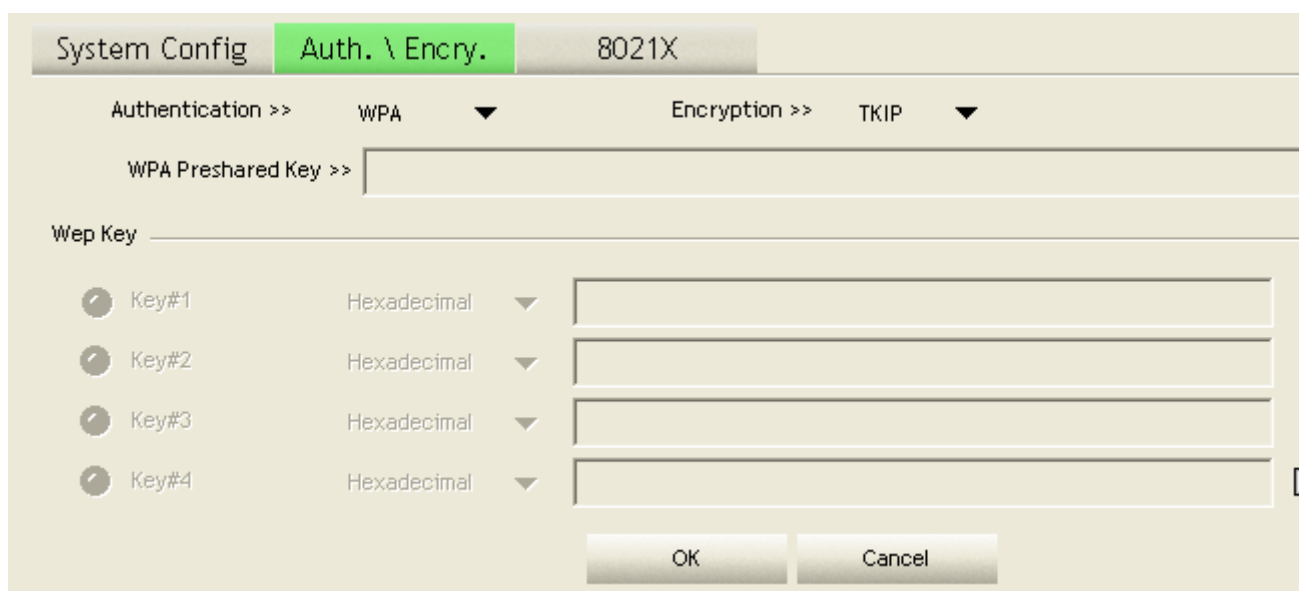


Figure 2-1-16 Configuration


At the mean time of starting RaUI, there is also a small Ralink icon appears within windows taskbar as Figure 2-1-15. You may double click it to bring up the main menu if you selected


to close RaUI menu earlier. You may also use mouse's right button to close RaUI utility.




Figure 2-1-17 Ralink icon in system tray


Besides, the small icon will change color to reflect current wireless network connection status. The status indicates as follow:

 : Indicate Connected and Signal Strength is Good.

 : Indicate Connected and Signal Strength is Normal.

 : Indicated not connected yet.

 : Indicated wireless NIC not detected.

 : Indicate Connected and Signal Strength is Weak.

PROFILE

Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 show the profile function.

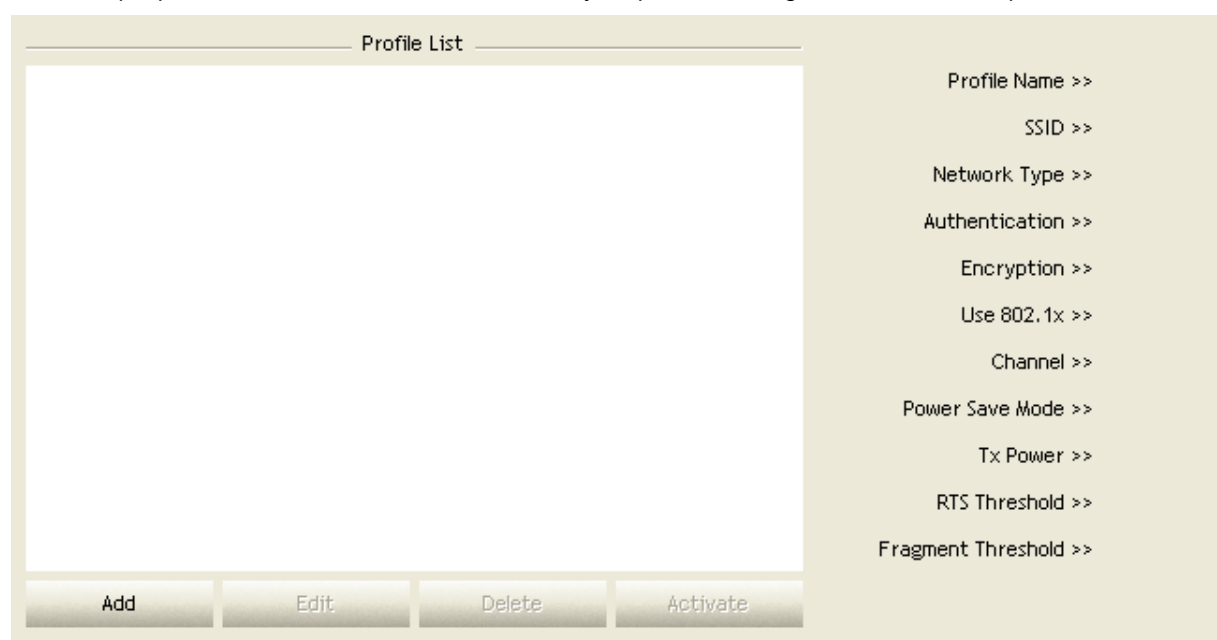


Figure 2-2-1 Profile function

Definition of each field :

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

B. SSID : AP or Ad-hoc name.

C. Network Type : Network's type, including infrastructure and Ad-Hoc.

Authentication : Authentication mode.

D. Encryption : Encryption Type.

E. Use 802.1x : Whether or not use 802.1x feature.

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

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

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

K. RTS Threshold : User can adjust the RTS threshold number by sliding the bar or key in the value directly.

L. Fragment Threshold : User can adjust the Fragment threshold number by sliding the bar or key in the value directly.

ICONS AND BUTTONS :



Indicate connection is successful on currently activated profile.



Indicate connection is failed on currently activated profile.



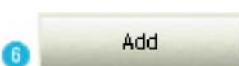
Indicate network type is infrastructure mode.



Indicate network type is Ad-hoc mode.



Indicate security-enabled wireless network.



Add a new profile.



Edit an existing profile.



Delete an existing profile.



Activate selected profile.



Show the information of Status Section.



Hide the information of Status Section.

ADD/EDIT PROFILE

There are three methods to open Profile Editor form.

- A. You can open it from "Add to Profile" button in Site Survey function.
- B. You can open it from "Add" button in Profile function.
- C. You can open it from "Edit" button in Profile function.

The screenshot shows the 'ADD/EDIT PROFILE' dialog box with the 'System Config' tab selected. The 'Auth. \ Encry.' tab is also visible. The '802.1X' checkbox is checked. The 'Profile Name' field contains 'PROF1'. The 'SSID' field contains 'AP1'. The 'Power Save Mode' section has two radio buttons: 'CAM' (selected) and 'PSM'. The 'RTS Threshold' is set to 0 and the 'Fragment Threshold' is set to 256. The 'Network Type' is set to 'Infrastr'. The 'Tx Power' is set to 'Aut' and the 'Preamble' is set to 'Aut'. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'ADD/EDIT PROFILE' dialog box with the 'Auth. \ Encry.' tab selected. The '802.1X' checkbox is checked. The 'Authentication' dropdown is set to 'Open' and the 'Encryption' dropdown is set to 'None'. The 'WPA Preshared Key' field is empty. The 'Wep Key' section has four radio buttons: 'Key#1', 'Key#2', 'Key#3', and 'Key#4', all of which are selected. Each key has a 'Hexadecimal' dropdown and a corresponding text input field. The 'OK' and 'Cancel' buttons are at the bottom.

Figure 2-2-2 Configuration

- A. Profile Name : User can chose name for this profile, or use default name defined by system.
- B. SSID : User can key in the intended SSID name or use pull down menu to select from available APs.
- C. Power Save Mode : Choose from CAM Constantly Awake Mode for Power Saving Mode.

D. 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 to that, the channel field will be available for setup in Ad-hoc mode.

E. RTS Threshold : User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.

F. Fragment Threshold : User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

G. Channel : Only available for setting under Ad-hoc mode. User can choose the channel frequency to start their Ad-hoc network.

H. 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.

I..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.

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

K. WPA Pre-shared Key : This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.

L. WEP Key : Only valid when using WEP encryption algorithm. The key must matched 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.

EXAMPLE TO ADD PROFILE IN PROFILE

A. Click Add in Profile function.

The screenshot displays the RaUI interface with the 'Profile' tab selected. The 'Profile List' area is empty, and the 'Add' button is highlighted with a red box. The right sidebar shows configuration options for a profile, and the bottom section displays detailed status and performance metrics.

Profile List

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

Buttons: Add, Edit, Delete, Activate

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 >> 5
Signal Strength 2 >> 5
Signal Strength 3 >> 2
Noise Strength >> 0%

Transmit

Link Speed >> 54.0 Mbps
 Throughput >> 0.000 Mbps

Receive

Link Speed >> 54.0 Mbps
 Throughput >> 0.025 Mbps

B. Add Profile page will pop up.

RaUI

Profile | Network | Advanced | Statistics | WMM | WPS | Radio On/

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. | 8021X

Profile Name >> PROF1

SSID >> [Dropdown]

Network Type >> Infrast.

Tx Power >> A

Power Save Mode >> ☒ CAM ☒ PSM

Preamble >> A

☐ RTS Threshold 0 [Slider] 2347 [2347]

☐ Fragment Threshold 256 [Slider] 2346 [2346]

OK Cancel

C. Change profile name to what you want to connect. Pull down the ssid and select one intended AP. The AP list is the result of last Network.

The screenshot displays the RaUI interface with the 'Profile' tab selected. The 'Profile List' section is empty, and the 'Add', 'Edit', 'Delete', and 'Activate' buttons are visible at the bottom. The configuration section below shows the 'System Config' tab, with 'Auth. \ Encry.' and '8021X' sub-tabs. The 'Profile Name' is set to 'PROF1'. The 'SSID' dropdown is open, showing a list of available APs. The 'Power Save Mode' is set to 'On'. The 'RTS Threshold' and 'Fragment Threshold' are both unchecked. The 'Network Type' is set to 'Infras'. The 'Tx Power' is set to 'A'. The 'Preamble' is set to 'A'. The 'AP List' table shows the following data:

AP Name	MAC Address
_Shiang_2860AP	000C43686016
AlbertY-200	00AA2E82EB9E
AP	0007404D0C7E
AP 1	00037F00D7A4
APPA	0014A549F42F
Belkin_N1_Wireless_281111	000C43281111
Broadcom	001018902EDA
BroadcomWPS	001018902E27
ClaudeAP	000C766FC597
Cobra	000A795C08BD
DennisAP	000C43102718
Fiona-Ap	000C43286021

D. Then, you can see the profile which you set appear in the profile list. Click "Activate". Activate the profile setting.

The screenshot displays the RaUI interface with the 'Profile' tab selected. The 'Profile List' shows a single profile named 'PROF1' with SSID 'AP1'. To the right, the configuration details for this profile are listed. Below the profile list are buttons for 'Add', 'Edit', 'Delete', and 'Activate'. The bottom section of the interface shows the status and performance metrics for the selected profile.

Profile List

Profile Name	SSID	Actions
PROF1	AP1	[Edit Icon]

Profile Configuration Details:

- 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 & Performance Metrics:

- 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 (High Throughput) Metrics:

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

Link Quality & Signal Strength:

- Link Quality >> 100%
- Signal Strength 1 >> 10
- Signal Strength 2 >> 10
- Signal Strength 3 >> 10
- Noise Strength >> 26

Transmit Performance:

- Link Speed >> 54.0 Mbps
- Throughput >> 0.000 Mbps

Receive Performance:

- Link Speed >> 54.0 Mbps
- Throughput >> 0.033 Mbps

NETWORK

Under the Network function, system will display the information of surrounding APs from last scan result. List informations include SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as Figure 2-3-1-1 shown.

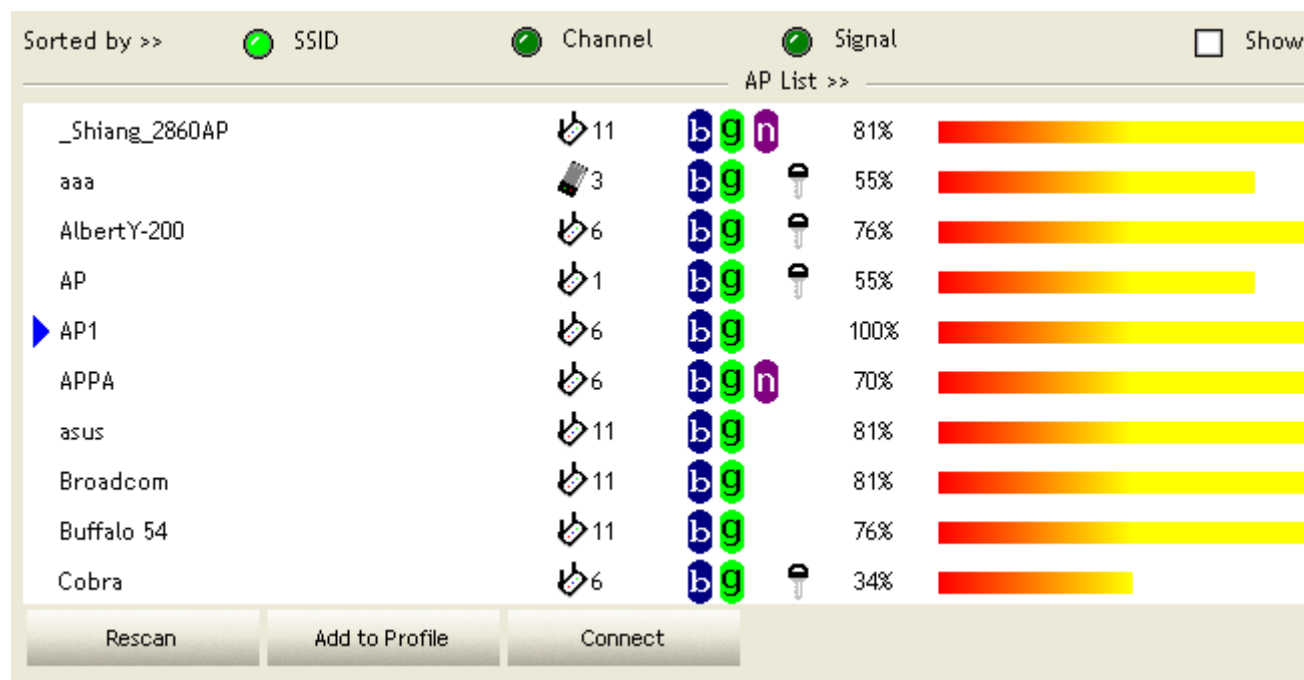


Figure 2-3-1-1 Network function

Definition of each field :

- A. SSID : Name of BSS or IBSS network.
- B. Network Type : Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
- C. Channel : Channel in use.
- D. Wireless Mode : AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode.
- E. Security-Enable : Whether AP provides security-enabled wireless network.
- F. Signal : Receive signal strength of specified network.

ICONS AND BUTTONS :



Indicate connection is successful.



Indicate network type is infrastructure mode.



Indicate network type is Ad-hoc mode.



Indicate security-enabled wireless network.



Indicate 802.11a wireless mode.



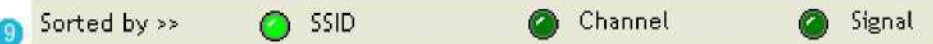
Indicate 802.11b wireless.



Indicate 802.11g wireless mode.



Indicate 802.11n wireless mode



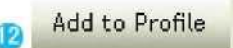
Indicate that AP list are sorted by SSID, Channel or Signal.



Command to connect to the selected network.



Issue an rescan command to wireless NIC to update information on surrounding wireless network.



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



Show the information of Status Section.



Hide the information of Status Section.

CONNECTED NETWORK :

A. When RaUI first ran, it will select the best AP to connect automatically.

B. If user wants to connect to other AP. He can click "Connect" button for the intended AP to make connection.

C. If the intended network has encryption other than "Not Use", RaUI will bring up the security page and let user input the appropriate information to make the connection. Please refer to example on how to fill the security information.

When you double click on the intended AP, you can see AP's detail information.

AP's detail information divide into three parts. They are General, WPS, CCX information and 802.11n (802.11n button only exists for the AP supported N mode). The introduction is as follow :

A-1. General information contain AP's ssid, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It shows as Figure 2-3-1-2.

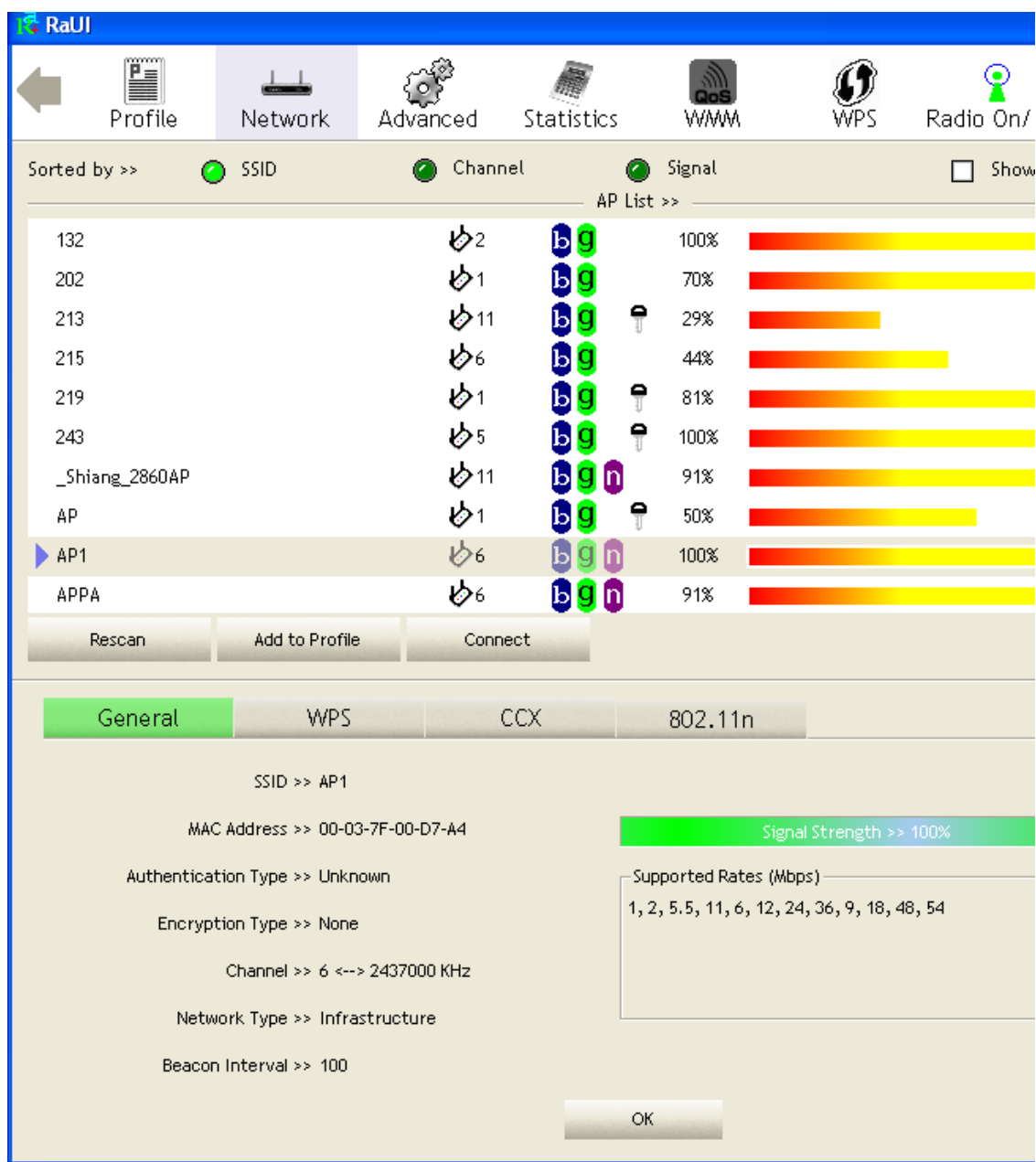


Figure 2-3-1-2 General informaion about AP's detal information

A-2. WPS information contain authentication type, encryption type, config methods, device password id, selected registrar, state, version, AP setup locked, UUID-E and RF bands as Figure 2-3-1-3. The introduction indicates as follow :

A-2-1. Authentication Type : There are three type of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

A-2-2. 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.

A-2-3. 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

A-2-4. Device Password ID : Indicate the method or identifies the specific password that the selected Registrar intends to use. AP 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

A-2-5. Selected Registrar : Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

A-2-6. State : The current configuration state on AP. The values are "Unconfigured" and "Configured".

A-2-7. Version : WPS specified version.

A-2-8. AP Setup Locked : Indicate if AP has entered a setup locked state.

A-2-9. UUID-E : The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.

A-2-10. RF Bands : Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

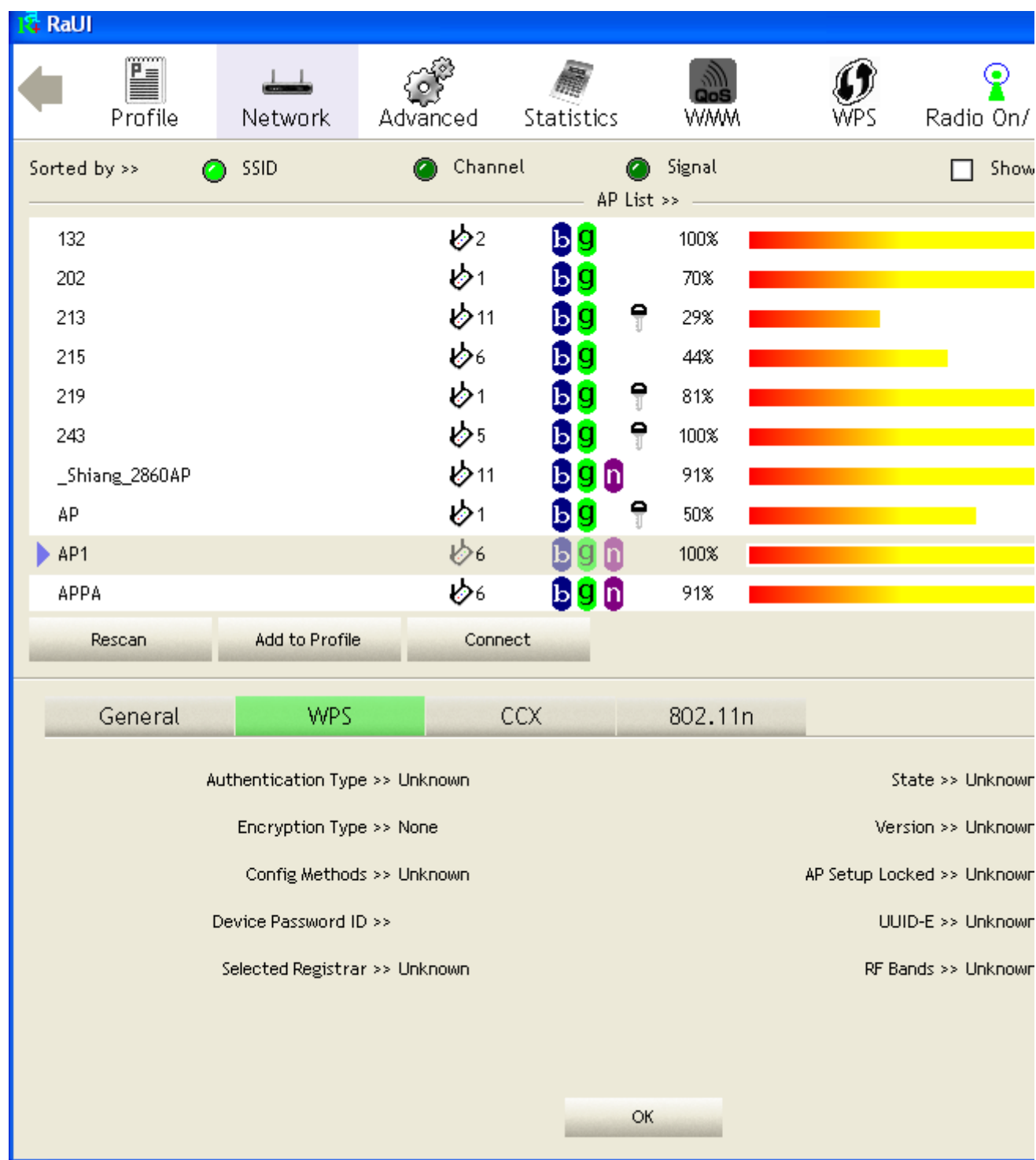


Figure 2-3-1-3 WPS information about AP's detail information

A-3. CCX information contains CCKM, Cmic and Ckip information. It shows as Figure 2-3-1-4.

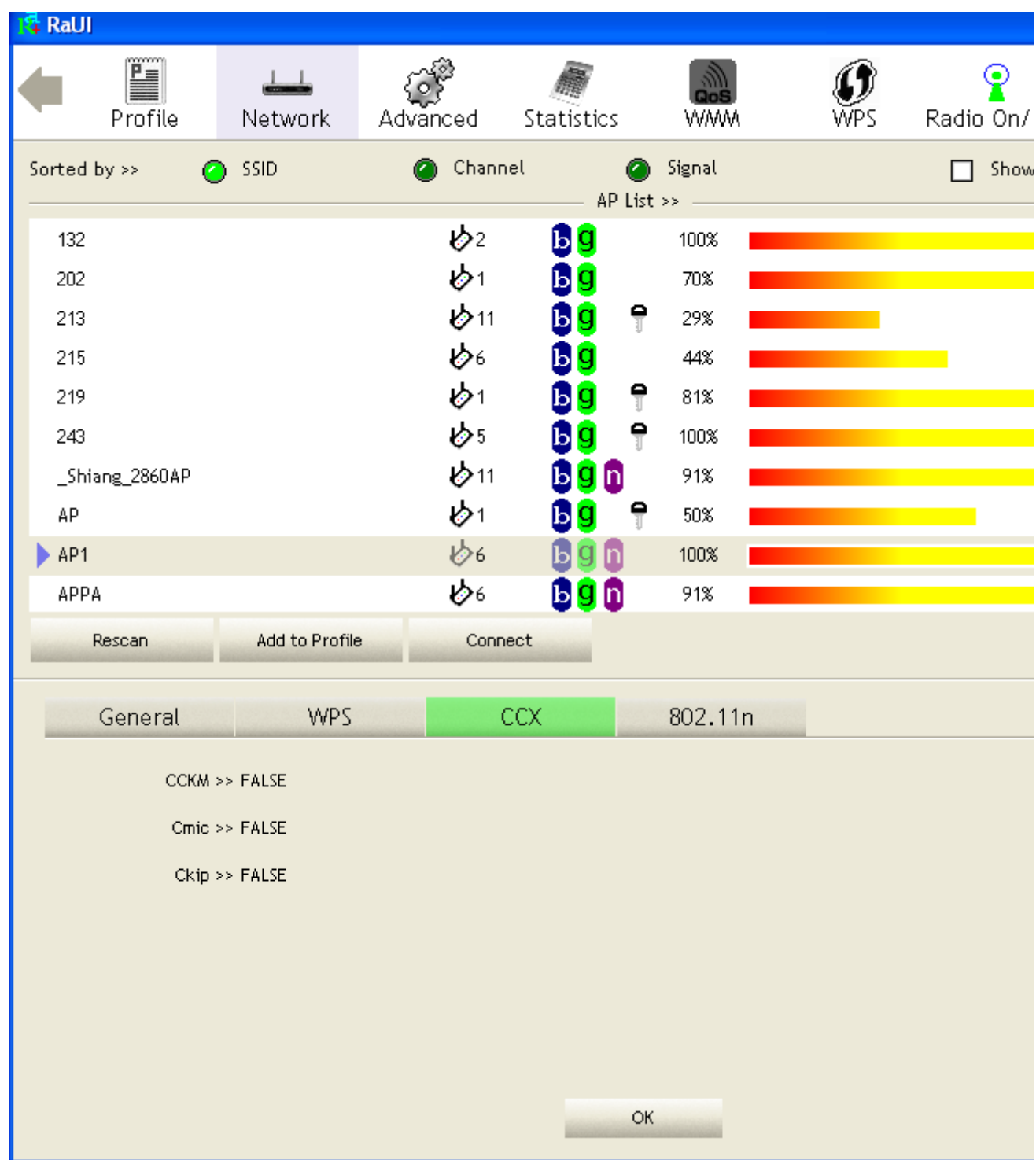


Figure 2-3-1-4 CCX information about AP's detail information

A-4. 802.11n information contains some related 802.11n information. It shows as Figure 2-3-1-5.

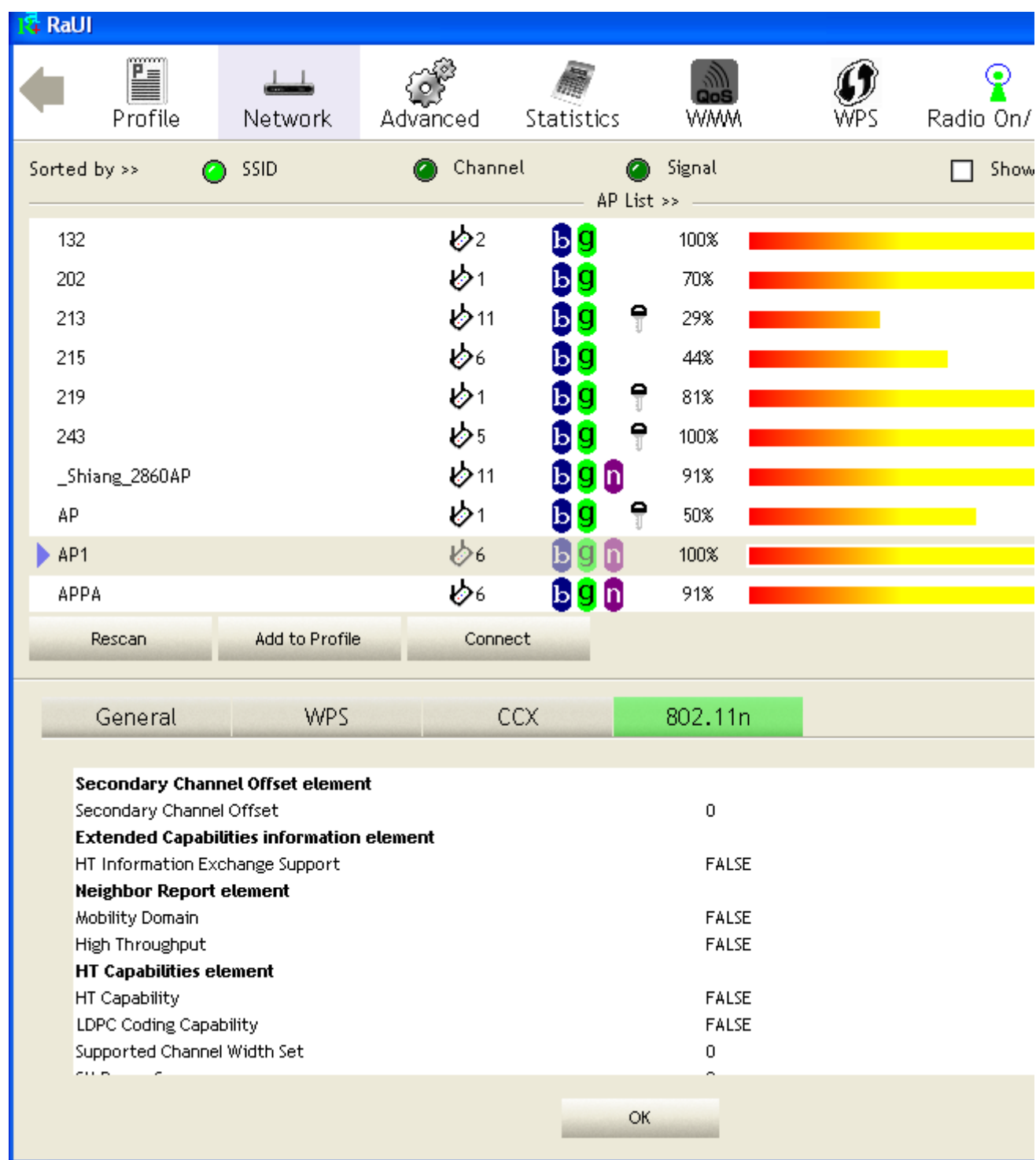


Figure 2-3-1-5 802.11n information

EXAMPLE ON ADDING PROFILE IN NETWORK

A. Select the intended network from AP list in Network function.

The screenshot displays the RaUI Network function interface. The top navigation bar includes icons for Profile, Network (selected), Advanced, Statistics, WMM, WPS, and Radio On/Off. Below the navigation bar, the 'AP List' is shown, sorted by SSID, Channel, and Signal. The 'AP1' entry is highlighted with a red box. Below the AP list, there are buttons for Rescan, Add to Profile, and Connect. The bottom section displays network status and details for the selected AP1.

AP Name	Channel	Signal
AlbertY-200	6	60%
AP	1	70%
AP1	6	100%
Broadcom	11	70%
BroadcomWPS	1	100%
DennisAP	6	76%
Fiona-Ap	11	44%
I55I-3F-asus11b	3	20%
knilar	8	60%
NB27-PC_Network	6	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 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Receive

Link Speed >> 48.0 Mbps

Throughput >> 0.104 Mbps

B. Click "Add to Profile".

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays various wireless networks. The 'AP1' entry is highlighted, and the 'Add to Profile' button is circled in red. Below the table, the status and configuration details for AP1 are shown, including link quality, signal strength, and network type.

AP Name	Channel	Signal	Link Quality
AlbertY-200	6	60%	100%
AP	1	70%	100%
AP1	6	100%	100%
Broadcom	11	70%	100%
BroadcomWPS	1	100%	100%
DennisAP	6	76%	100%
Fiona-Ap	11	44%	100%
ISSI-3F-asus11b	3	20%	100%
knilar	8	60%	100%
NB27-PC_Network	6	81%	100%

AP1 Details:

- 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 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

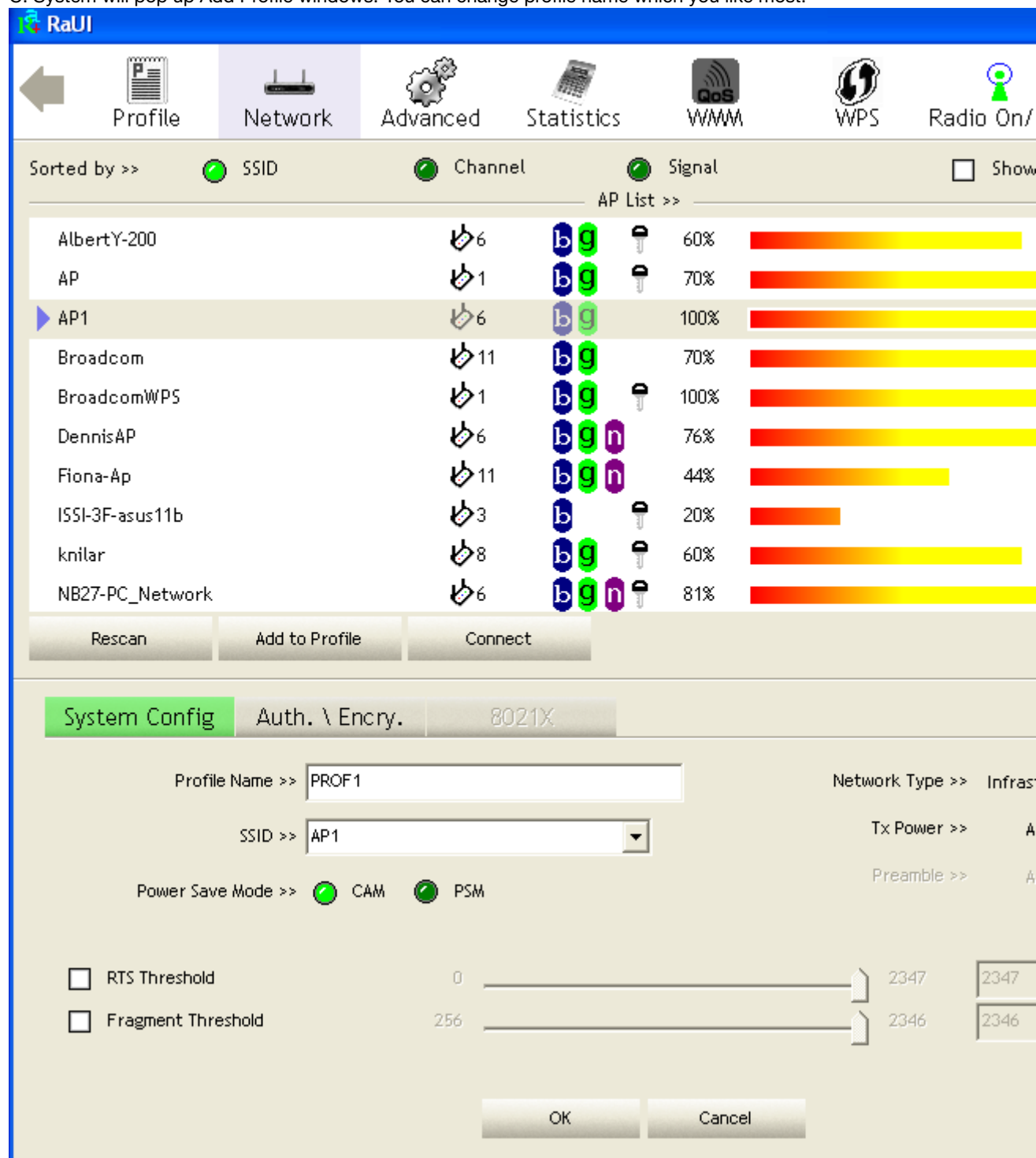
Transmit

- Link Speed >> 54.0 Mbps
- Throughput >> 0.000 Mbps

Receive

- Link Speed >> 48.0 Mbps
- Throughput >> 0.104 Mbps

C. System will pop up Add Profile windows. You can change profile name which you like most.



D. Then, you can see the profile which you set appear in the profile list. Click "Activate". Activate the profile setting.

The screenshot displays the RaUI interface with a blue header bar containing the RaUI logo and a navigation menu with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The 'Profile' tab is selected.

Profile List

Profile Name	AP Name	Action
PROF1	AP1	

Buttons: Add, Edit, Delete, Activate

Profile Configuration Details:

- 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 & Link Information:

- 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 (High Throughput) Section:

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

Link Quality & Signal Strength:

- Link Quality >> 100%
- Signal Strength 1 >> 10
- Signal Strength 2 >> 10
- Signal Strength 3 >> 10
- Noise Strength >> 26

Transmit Section:

- Link Speed >> 54.0 Mbps
- Throughput >> 0.000 Mbps

Receive Section:

- Link Speed >> 54.0 Mbps
- Throughput >> 0.092 Mbps

ADVANCED

Figure 2-4 shows Advance function of RaUI.

Figure 2-4 Advance function

A. Wireless mode : Select wireless mode. 802.11 B only, 802.11 A only, 802.11 B/G mix, 802.11 B/G/N mix, 802.11 A/B/G mix, and 802.11 A/B/G/N mix modes are supported.

(802.11 A/B/G mix selection item only exists for A/B/G adapter ; 802.11 B/G/N mix selection item only exists for B/G/N adapter ; 802.11 A/B/G/N mix selection item only exists for A/B/G/N adapter)

B. Wireless Protection : User can choose from Auto, On, and Off.
(only 802.11n adapter don't support.)

B-1. Auto : STA will dynamically change as AP announcement.

B-2. On : Always send frame with protection.

B-3. Off : Always send frame without protection.

C. TX Rate : Manually force the Transmit using selected rate. Default is auto.
(802.11n wireless card don't support TX Rate now)

D. Enable TX Burst : Ralink's proprietary frame burst mode.

E. Enable TCP Window Size : Enhance throughput.

F. Fast Roaming at : fast to roaming, setup by transmit power.

G. Select Your Country Region Code : eight countries to choose. Country channel list : Country channel list. (11A ListBox only shows for A/B/G adapter.)

H. Show Authentication Status Dialog : When you connect AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog display the process about 802.1x authentication.

I. Enable CCX (Cisco Compatible eXtensions) : support Cisco Compatible Extensions function.

I-1. LEAP turn on CCKM.

I-2. Enable Radio Measurement : can channel measurement every 0~2000 milliseconds.

J. Apply the above changes.

ICONS AND BUTTONS:



Show the information of Status Section.



Hide the information of Status Section.

STATISTICS

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

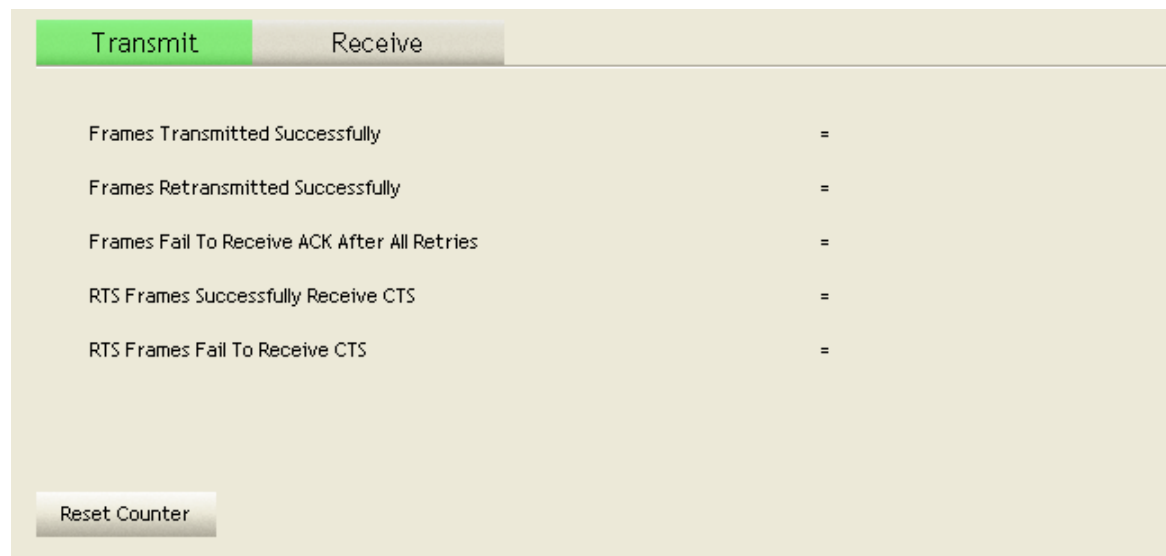
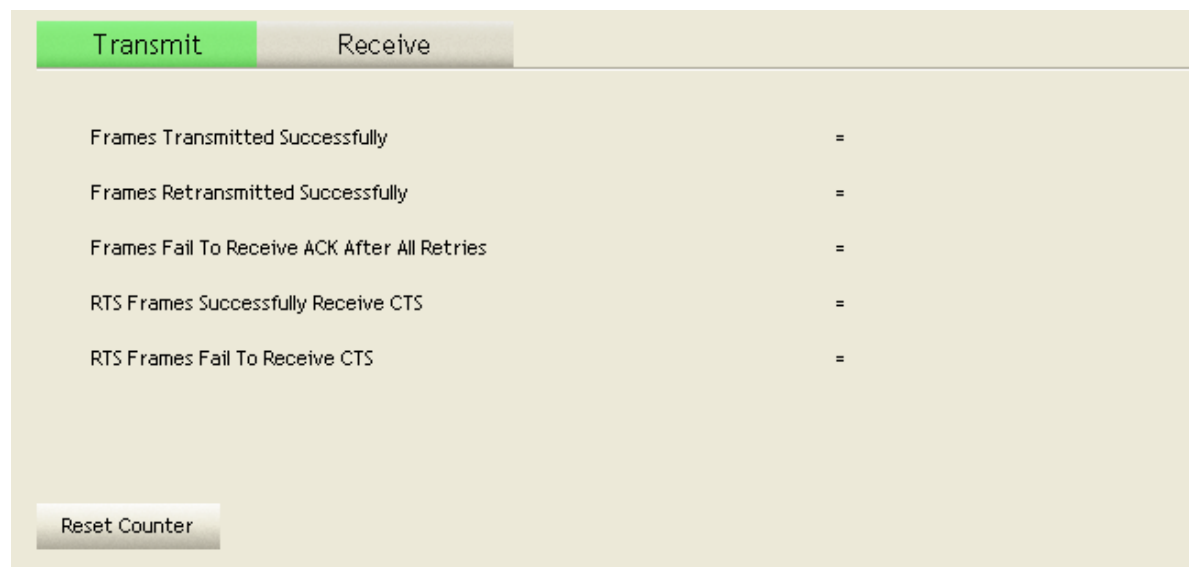


Figure 2-5-1 Statistics function

Transmit Statistics :



A. Frames Transmitted Successfully : Frames successfully sent.

B. Frames Fail To Receive ACK After All Retries : Frames failed transmit after hitting retry limit.

- C. RTS Frames Successfully Receive CTS : Successfully receive CTS after sending RTS frame.
- D. RTS Frames Fail To Receive CTS : Failed to receive CTS after sending RTS.
- E. Frames Retransmitted Successfully : Successfully retransmitted frames numbers.
- F. Reset counters to zero.

Receive Statistics :

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

Reset Counter

- A. Frames Received Successfully : Frames received successfully.
- B. Frames Received With CRC Error : Frames received with CRC error.
- C. Frames Dropped Due To Out-of-Resource : Frames dropped due to resource issue.
- D. Duplicate Frames Received : Duplicate received frames.
- E. Reset counters to zero.

ICONS AND BUTTONS:



Show the information of Status Section.



Hide the information of Status Section.

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 :

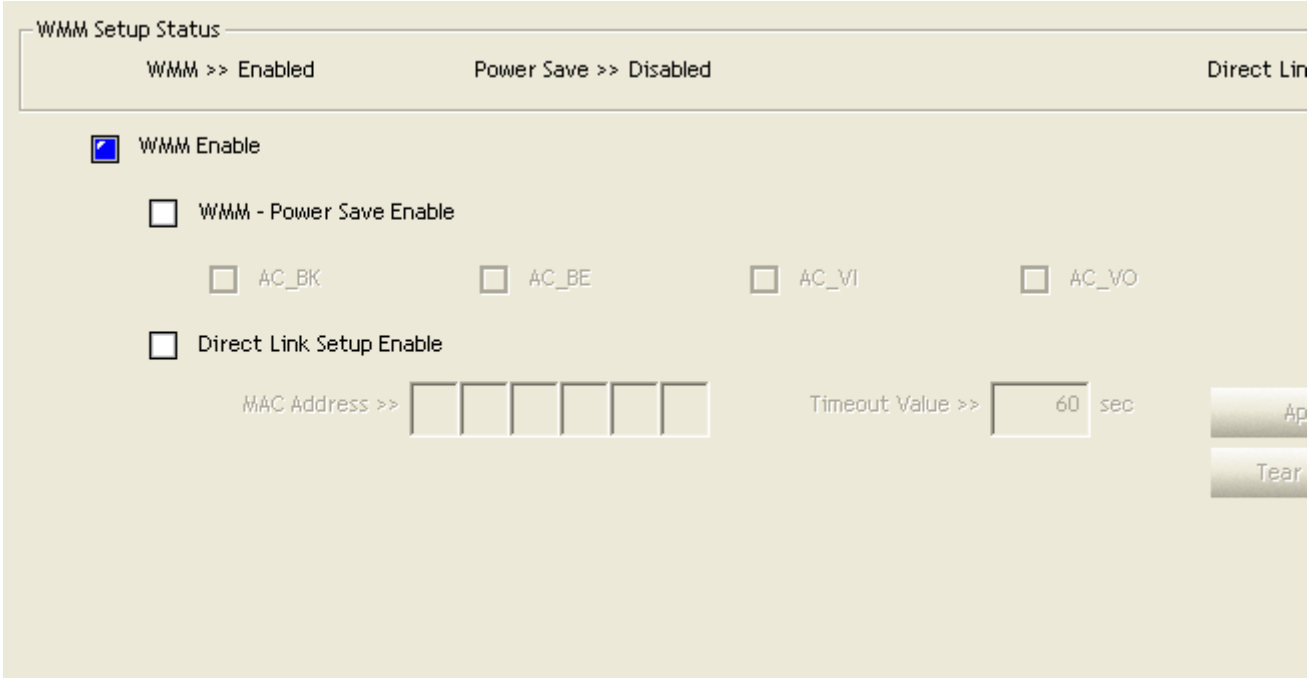


Figure 2-6-1 WMM function

- A. WMM Enable : Enable Wi-Fi Multi-Media. The setting method follows Section 2-6-2. WMM –
- B. Power Save Enable : Enable WMM Power Save. The setting method follows Section 2-6-3.
- C. 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.

EXAMPLE TO CONFIGURE TO ENABLE DLS (DIRECT LINK SETUP)

A. Click "Direct Link Setup Enable"

WMM Setup Status

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

☒ WMM Enable

☐ WMM - Power Save Enable

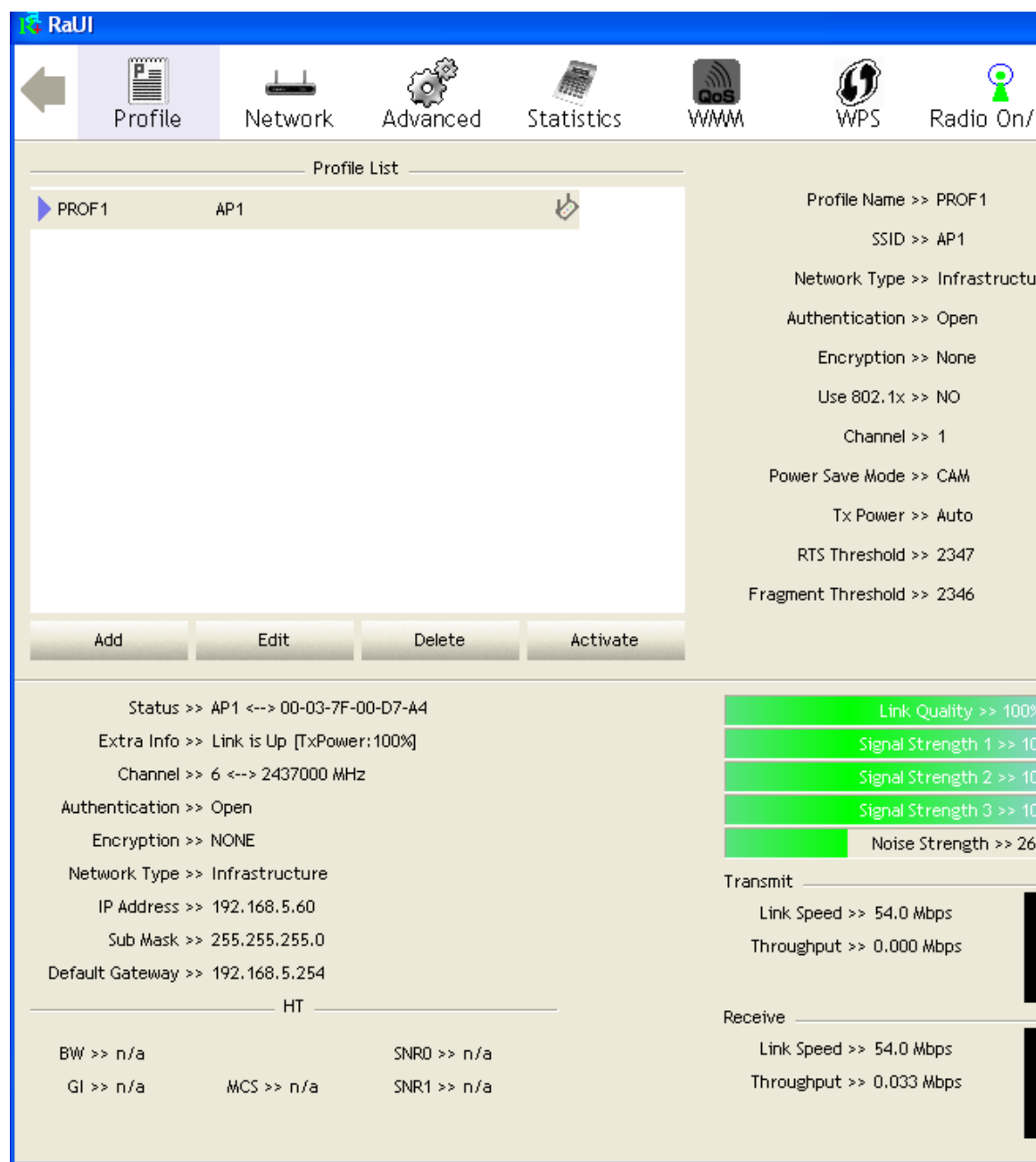
☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☒ Direct Link Setup Enable

MAC Address >> Timeout Value >> sec

Ap
Tear

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



The setting of DLS indicates as follow :

A. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to two conditions as follow :

1. Connect with the same AP that support DLS features.
2. Have to enable DLS.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ 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

Ap
Tear

B. Timeout Value represents that it disconnect automatically after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ 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

Ap
Tear

C. Click "Apply" button. The result will look like the below figure.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ 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

Ap
Tear

Describe "DLS Status" as follow :

A. As the up figure, after configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in "DLS Status". In "DLS Status" of the opposite side, it shows MAC address of myself and Timeout Value of setting.

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

B-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 Lin

☒ 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

Ap
Tear

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

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ 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

Ap
Tear

C. Disconnect Direct Link Setup as follow :

C-1. Select a direct link STA.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ 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

Ap
Tear

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

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☒ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☒ Direct Link Setup Enable

MAC Address >> Timeout Value >> sec

Ap
Tear

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:

A. Click "WMM Enable".

The screenshot shows the "WMM Setup Status" window. At the top, there are three status indicators: "WMM >> Enabled", "Power Save >> Disabled", and "Direct Link". Below these, the "WMM Enable" checkbox is checked. Underneath, the "WMM - Power Save Enable" checkbox is unchecked. Further down, four checkboxes are displayed: "AC_BK", "AC_BE", "AC_VI", and "AC_VO", all of which are unchecked. Below these, the "Direct Link Setup Enable" checkbox is also unchecked. At the bottom, there are two input fields: "MAC Address >>" followed by six empty boxes, and "Timeout Value >>" followed by a box containing "60" and the text "sec". On the right side of the window, there are two buttons: "Apply" and "Tear D".

B. 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.

RaUI

Profile Network Advanced Statistics WMM WPS Radio On/Off

Profile List

Profile Name	AP
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 >> 10
 Signal Strength 2 >> 10
 Signal Strength 3 >> 10
 Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps
 Throughput >> 0.000 Mbps

Receive

Link Speed >> 54.0 Mbps
 Throughput >> 0.033 Mbps

EXAMPLE TO CONFIGURE TO ENABLE WMM POWER SAVE

A. Click "WMM-Power Save Enable".

The screenshot shows the 'WMM Setup Status' page. At the top, there are two status indicators: 'WMM >> Enabled' and 'Power Save >> Disabled'. Below these, there are several checkboxes: 'WMM Enable' (checked), 'WMM - Power Save Enable' (checked), 'AC_BK' (unchecked), 'AC_BE' (unchecked), 'AC_VI' (unchecked), 'AC_VO' (unchecked), and 'Direct Link Setup Enable' (unchecked). There is a 'MAC Address >>' field with six empty boxes and a 'Timeout Value >>' field with '60' and 'sec'. On the right side, there are two buttons: 'Ap' and 'Tear'.

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

The screenshot shows the 'WMM Setup Status' page after the configuration changes. The status indicators now show 'WMM >> Enabled' and 'Power Save >> Enabled'. The checkboxes are: 'WMM Enable' (checked), 'WMM - Power Save Enable' (checked), 'AC_BK' (checked), 'AC_BE' (unchecked), 'AC_VI' (unchecked), 'AC_VO' (unchecked), and 'Direct Link Setup Enable' (unchecked). The 'MAC Address >>' field and 'Timeout Value >>' field remain the same. The 'Ap' and 'Tear' buttons are still present on the right.

WPS

Figure 2-7-1 shows WPS function of RaUI. The introduction indicates as follow:

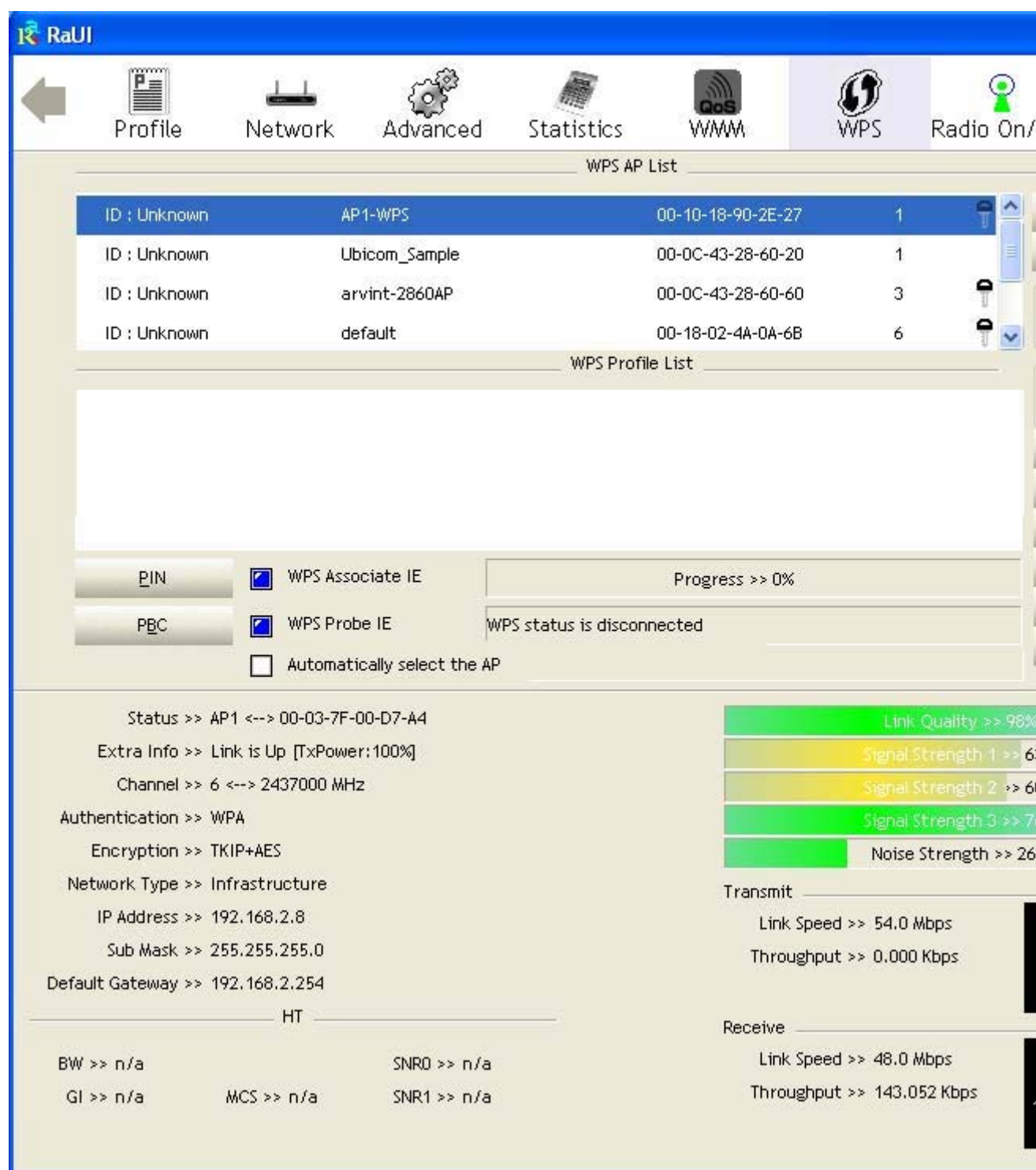


Figure 2-7-1 WPS function

A. 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 as an Enrollee or external Registrar supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

B. WPS AP List : Display the information of surrounding APs with WPS IE from last scan result. List information include SSID, BSSID, Channel, ID (Device Password ID), Security- Enabled.

C. Rescan : Issue a rescan command to wireless NIC to update information on surrounding wireless network.

D. Information : Display the information about WPS IE on the selected network. List information include Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.

It's detail follows WPS Information on AP.

E. PIN Code : 8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.

F. Config Mode : Our station role-playing as an Enrollee or an external Registrar.

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

H. Control items on credentials

H-1. Detail : Information about Security and Key in the credential.

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

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

H-4. Disconnect : Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.

H-5. Export Profile: Export all credentials to Profile.

H-6. Delete : Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.

I. 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.

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

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

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

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

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

N. Status Bar: Display currently WPS Status.

O. Automatically select the AP: Start 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:



Show the information of Status Section.



Hide the information of Status Section.

WPS INFORMATION ON AP

WPS information contain authentication type, encryption type, config methods, device password id, selected registrar, state, version, AP setup locked, UUID-E and RF bands. The introduction indicates as follow :

AP List

AP ID	Channel	Signal	Signal Strength (%)
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%

Buttons: Rescan, Add to Profile, Connect

WPS Information:

- 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

OK

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

B. 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.

C. 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

D. Device Password ID : Indicate the method or identifies the specific password that the selected Registrar intends to use. AP 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

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

F. State : The current configuration state on AP. The values are "Unconfigured" and "Configured".

G. Version : WPS specified version.

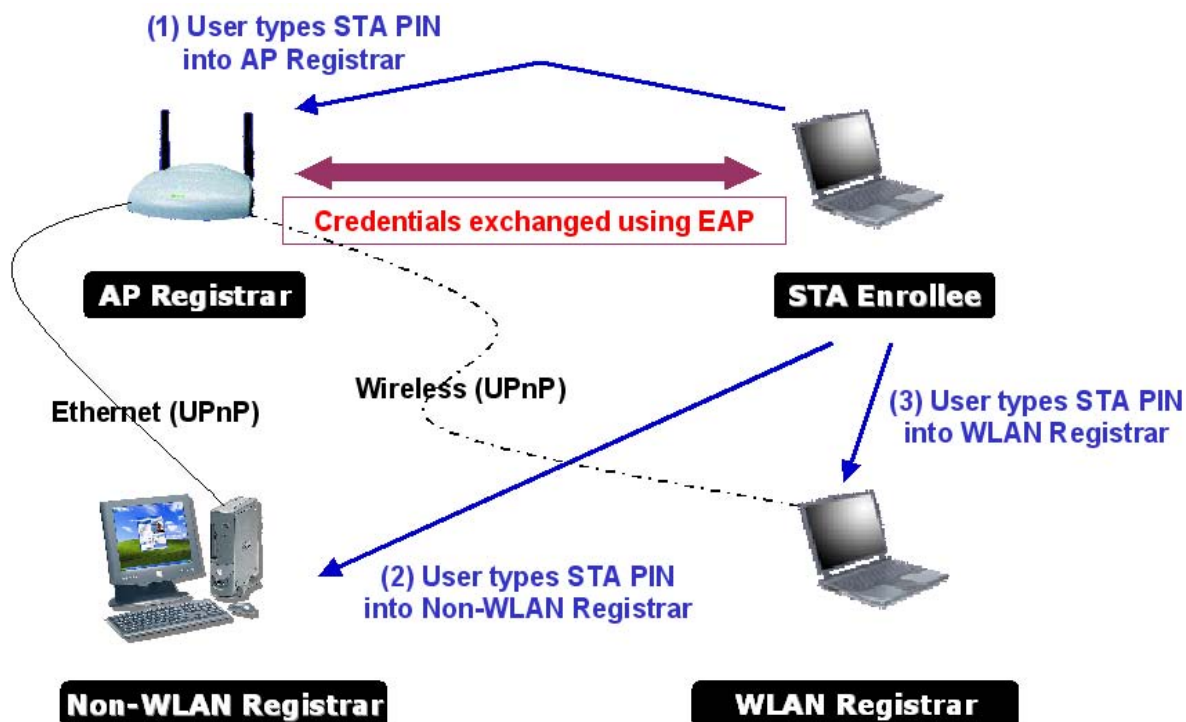
H. AP Setup Locked : Indicate if AP has entered a setup locked state.

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

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

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 detail indicates as follows.



A. Go to the box of Config Mode and select Enrollee.

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

PBC

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

Progress >> 0%

WPS status is disconnected

B. Click "Rescan" button to update available WPS APs.

WPS AP List

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

WPS Profile List

PIN ☒ WPS Associate IE Progress >> 0%

PBC ☒ WPS Probe IE WPS status is disconnected

☐ Automatically select the AP

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

WPS AP List

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

WPS Profile List

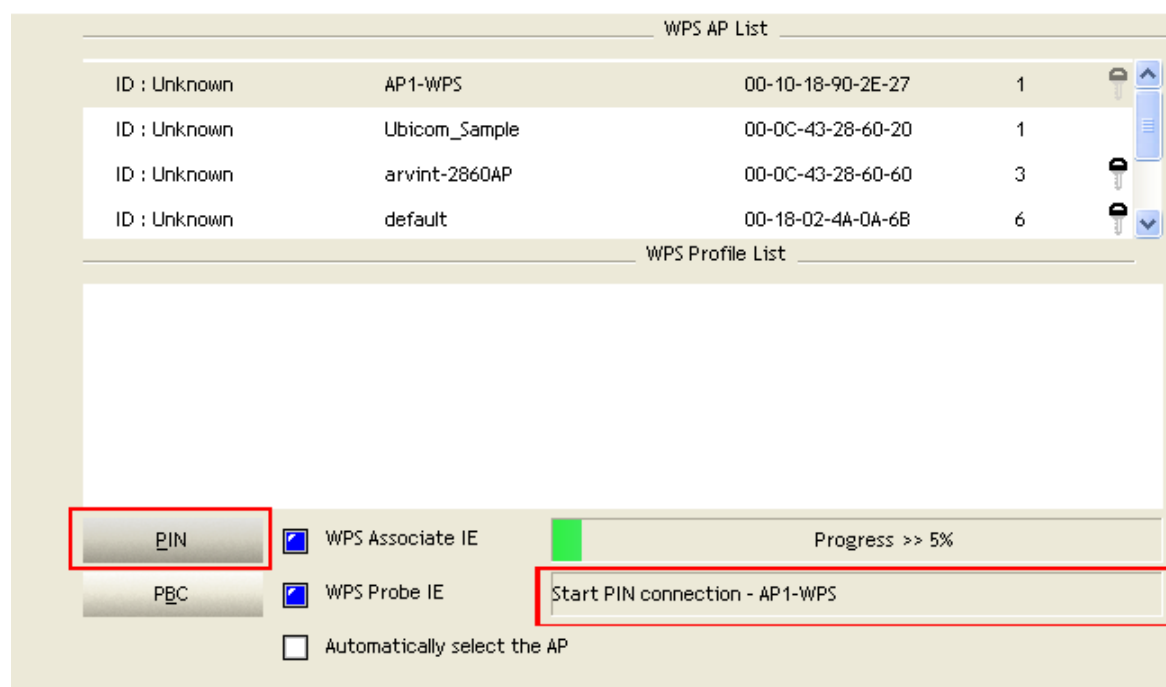
PIN ☒ WPS Associate IE Progress >> 0%

PBC ☒ WPS Probe IE WPS status is disconnected

☐ Automatically select the AP

D. Click "PIN" button to start PIN connection.

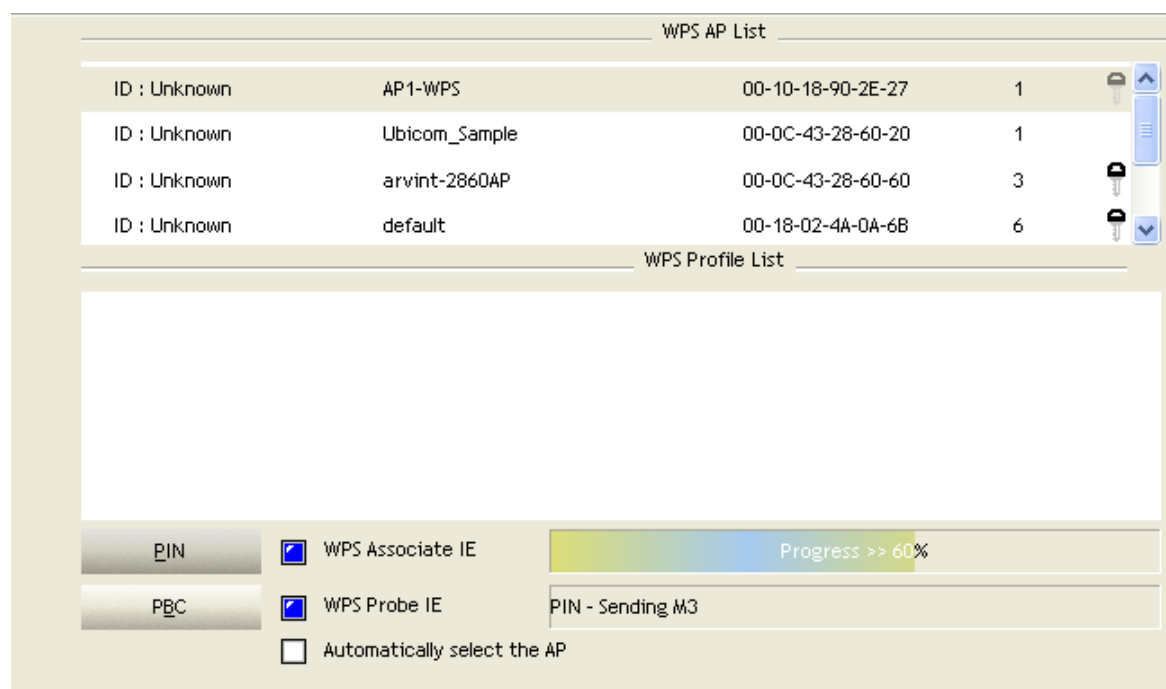
F. Enter PIN Code of STA into the Registrar when prompted by the Registrar.



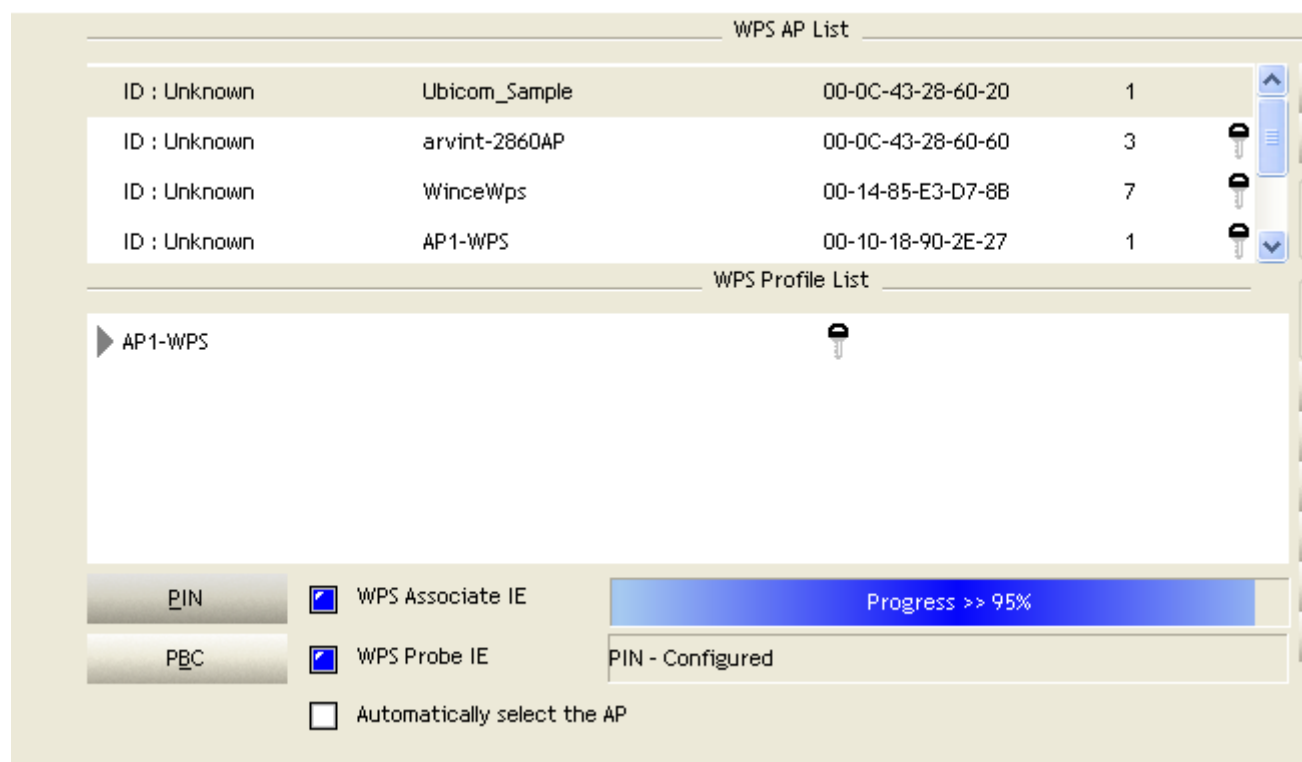
*Allow of an exchange between Step 4 and Step 5.

*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.

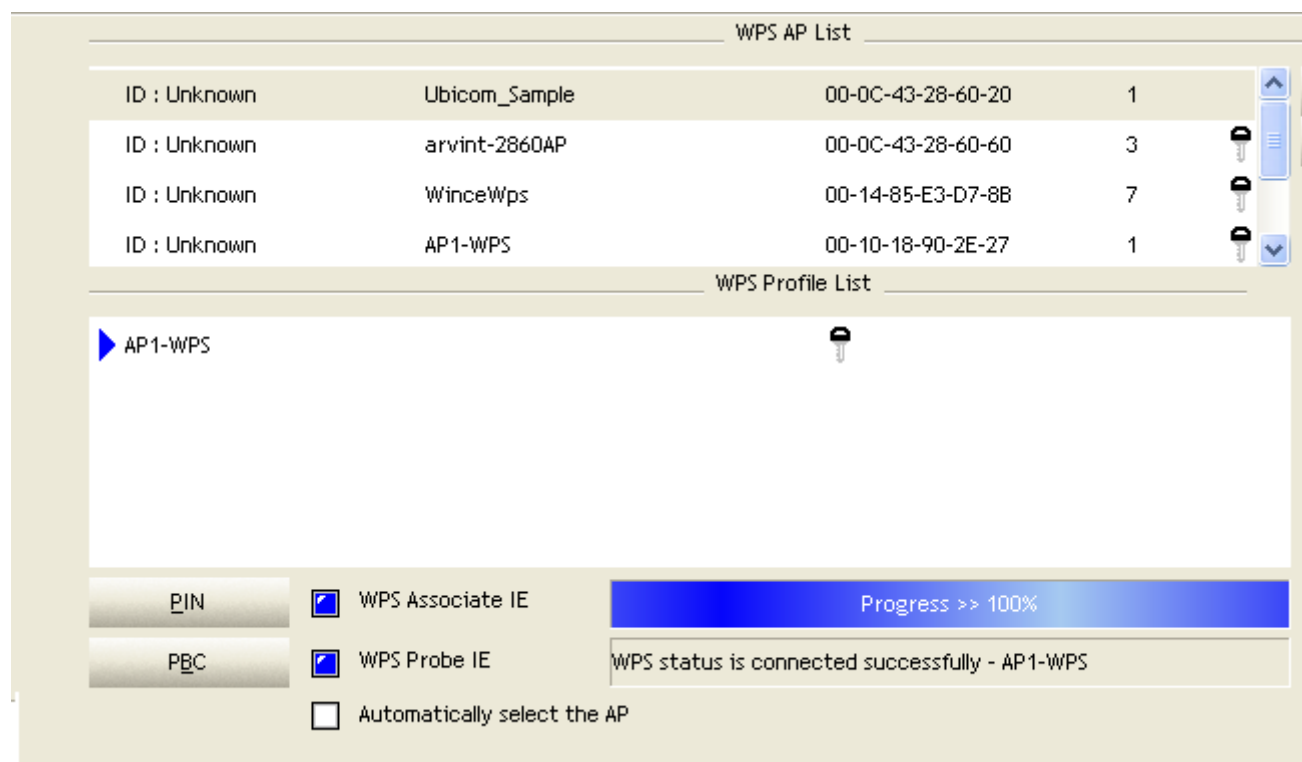
G. The result will look like the below figure.



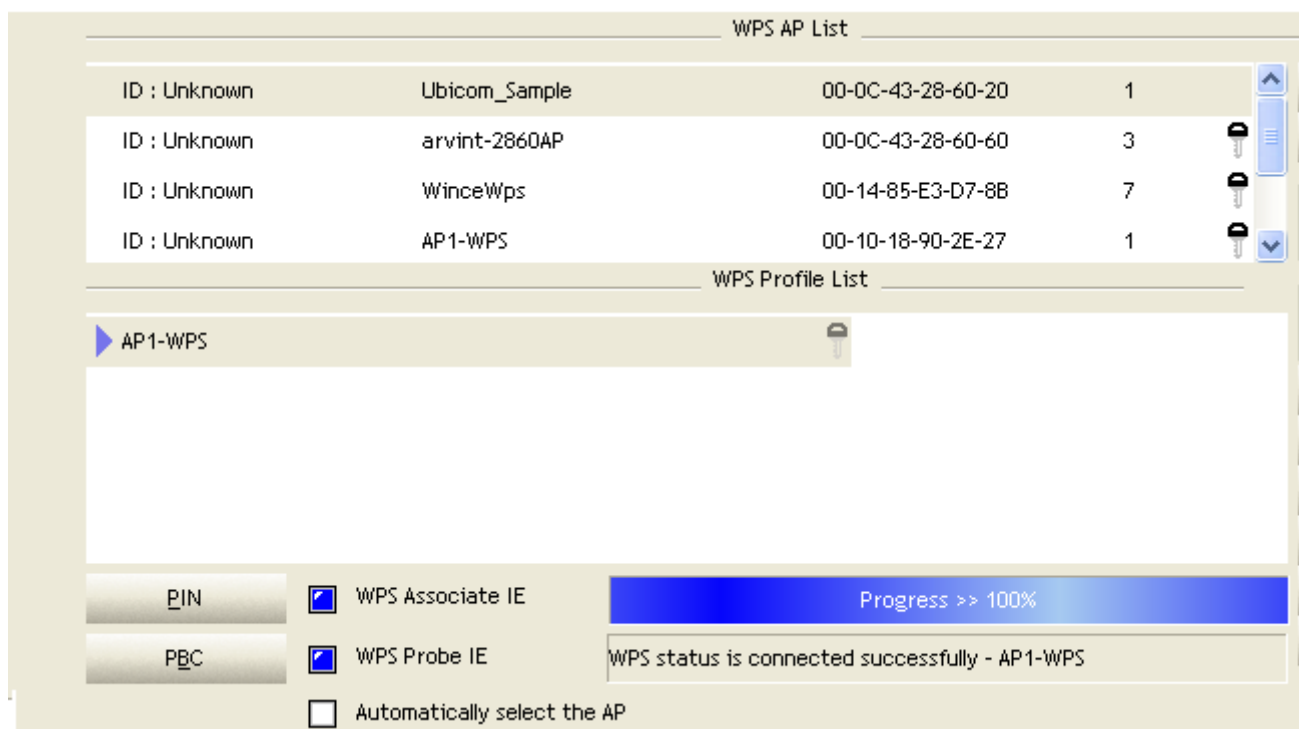
H. Configured and got one or multiple credential(s).



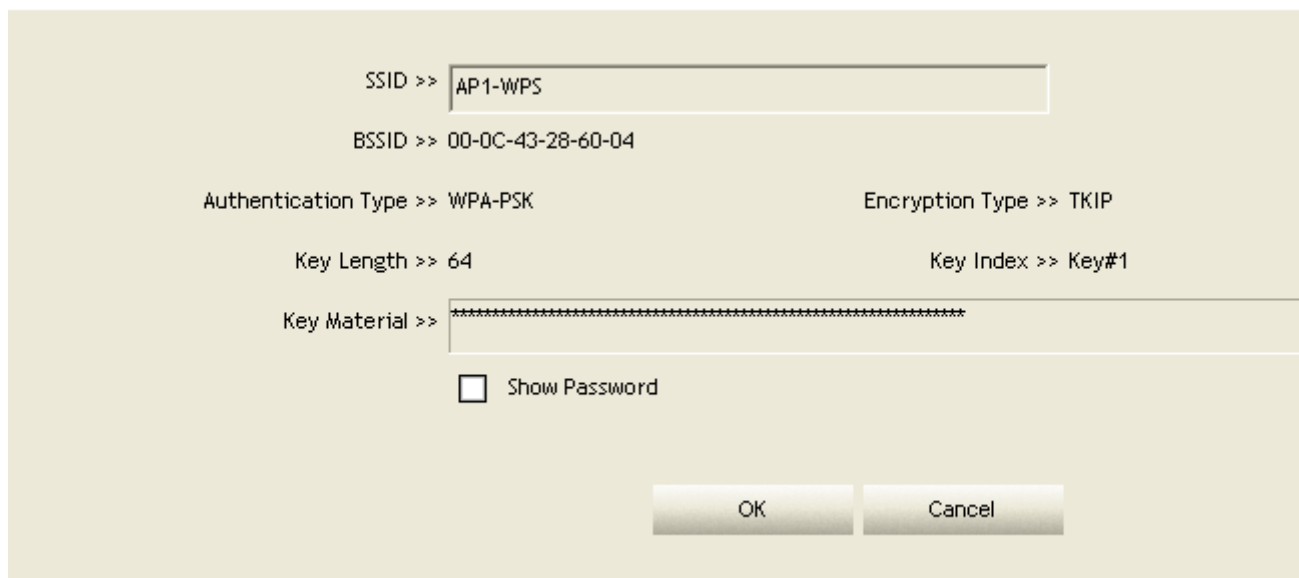
I. Then connect successfully. The result will look like the below figure.



J. Click "Detail" button.



K. You will look like the below figure.



*If Credential#1 is reliable and present, system will connect with Credential#1. On the contrary, system will auto rotate to the next existed credential.

*Also you can click "Rotate" button. Command to rotate to the next credential you want to use.

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

A. Asuccessful PIN Configuration :

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

B. WPS configuration doesn't complete after two-minute connection : WPS Eap process failed.

C. When Errors occur within two-minute connection, the WPS status bar might report on "WPS Eap process failed".

Error messages might be :

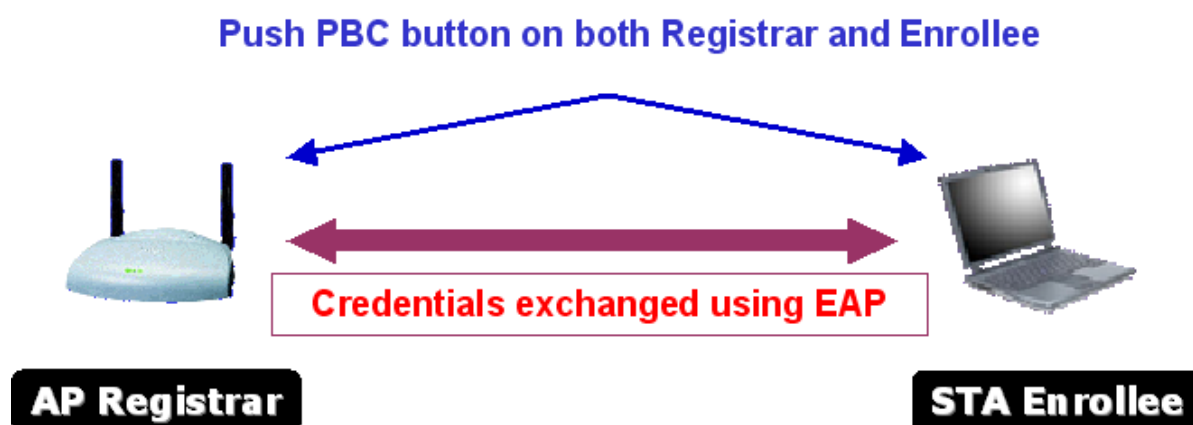
1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. Error PIN Code.
4. An inappropriate EAP-FAIL received.

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 only one Registrar in PBC mode, which PBC mode is obtained from ID 0x0004, is found after a complete scan, the Enrollee can 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 two-minute timeout.

*Before you press PBC on STA and candidate AP. Make sure all of APs aren't PBC mode or APs using PBC mode have left their Walk Time.



A. Go to the box of Config Mode and select Enrollee.

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

PBC

☒ WPS Associate IE

☒ WPS Probe IE

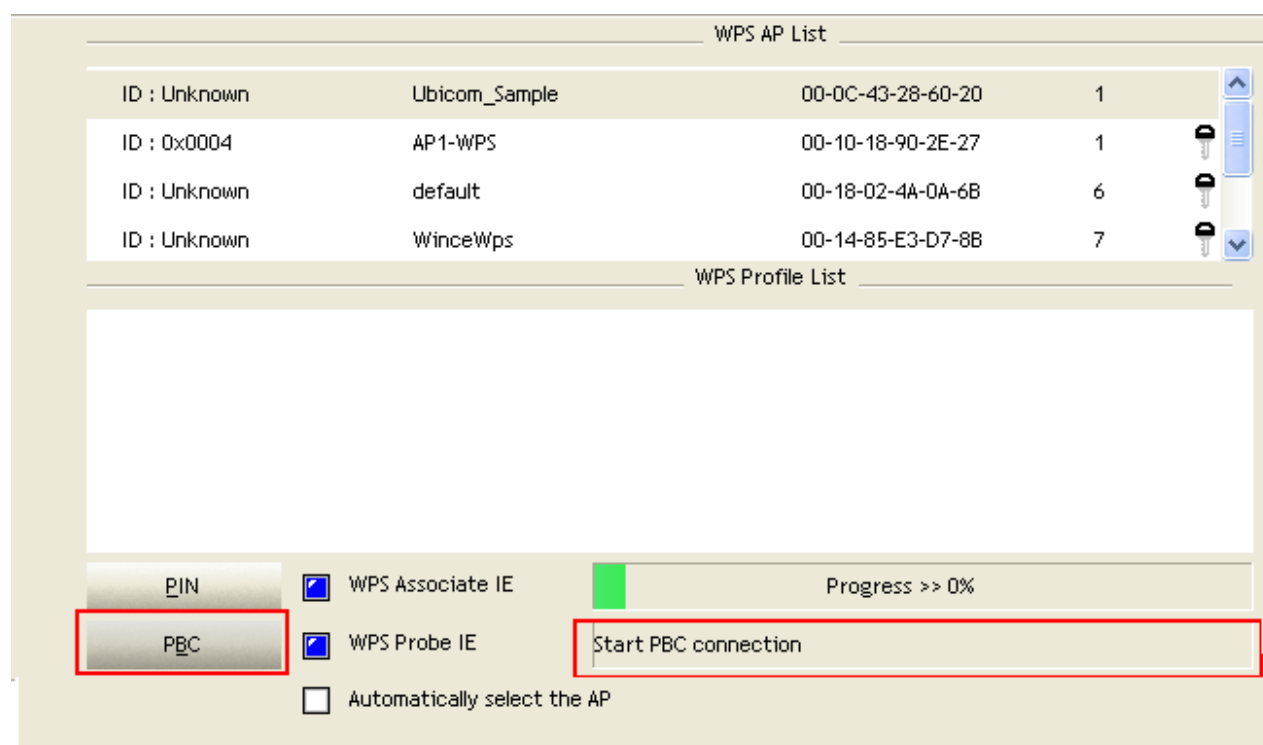
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

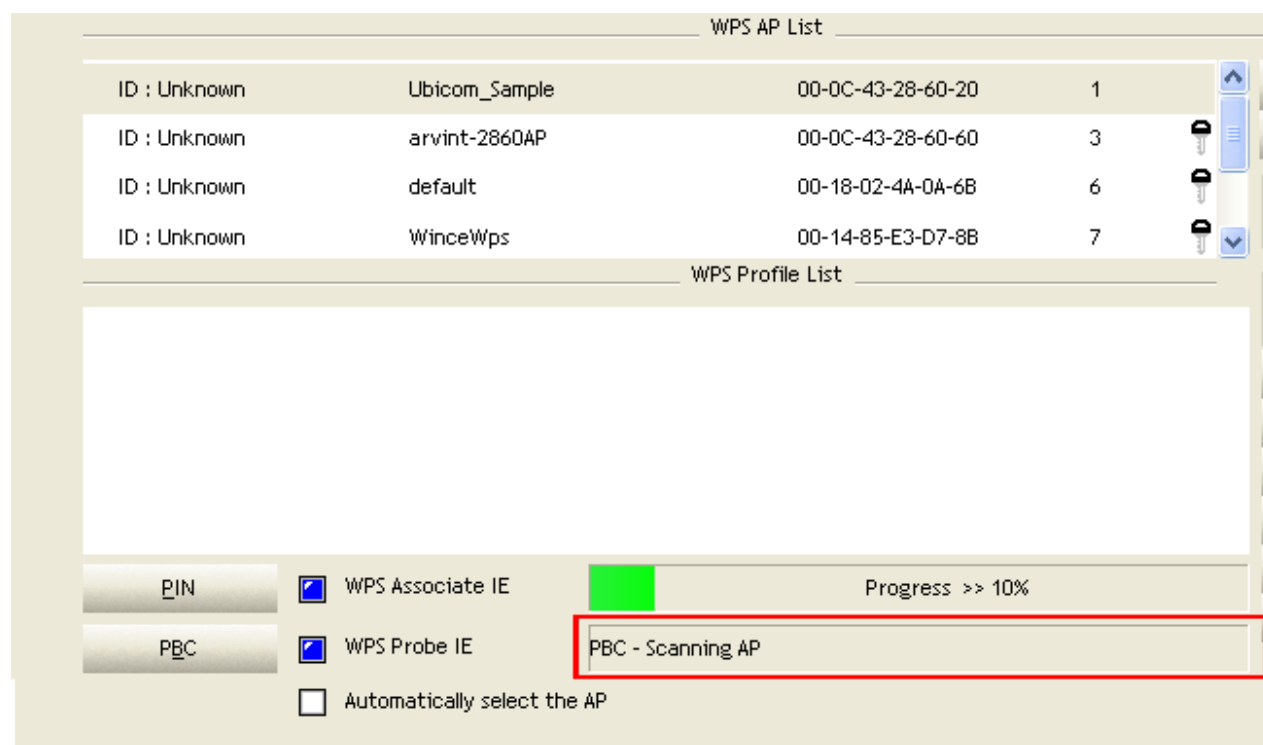
B. Click PBC to start PBC connection.

C. Push PBC on AP.

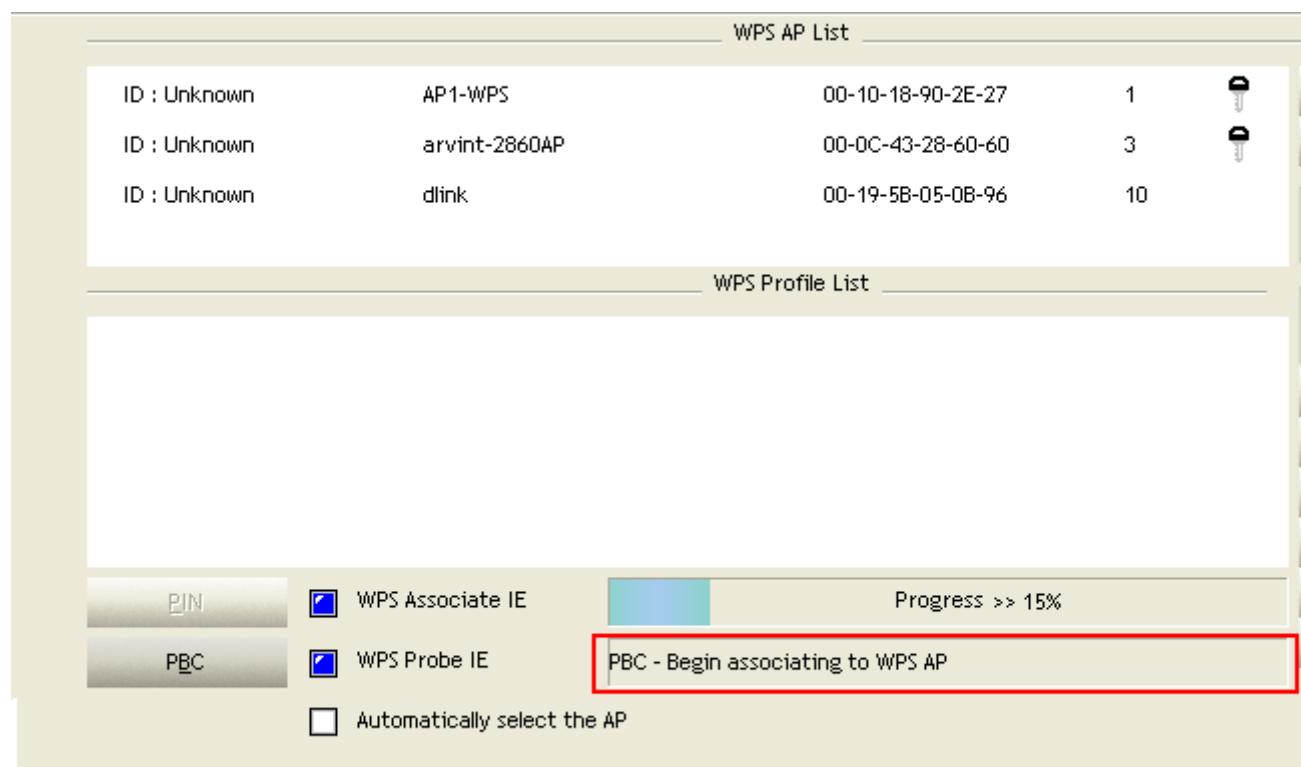


*Allow of an exchange between Step 2 and Step 3.

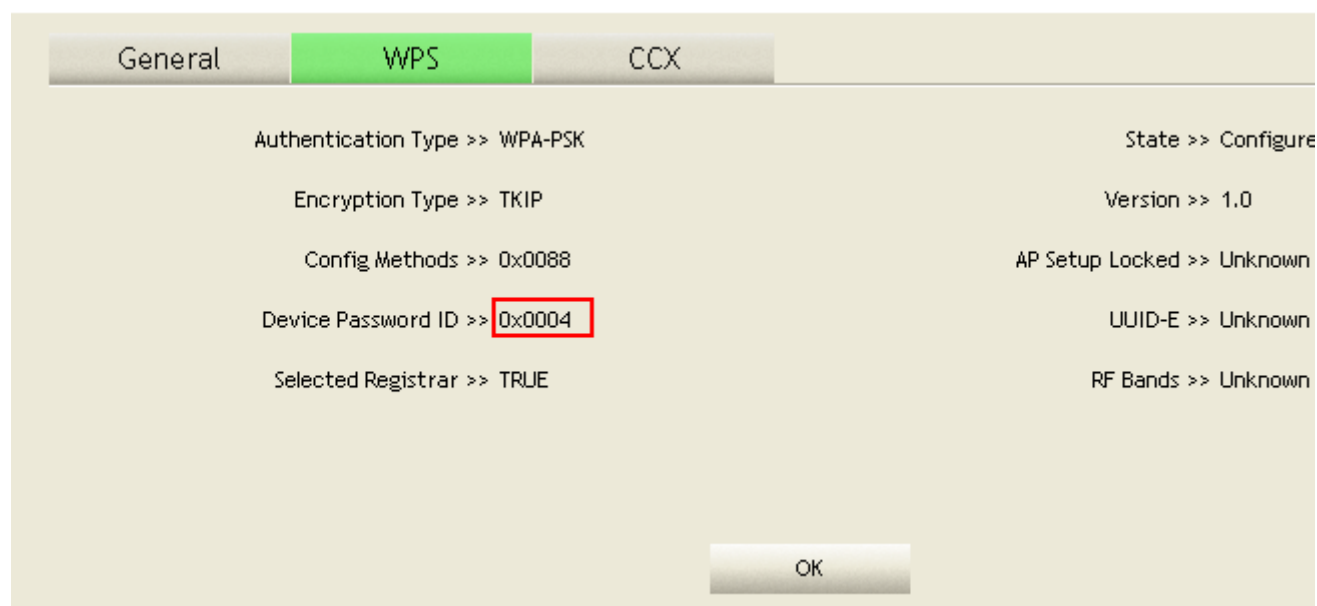
D. Then it can be shown "Scanning AP" as the below figure.



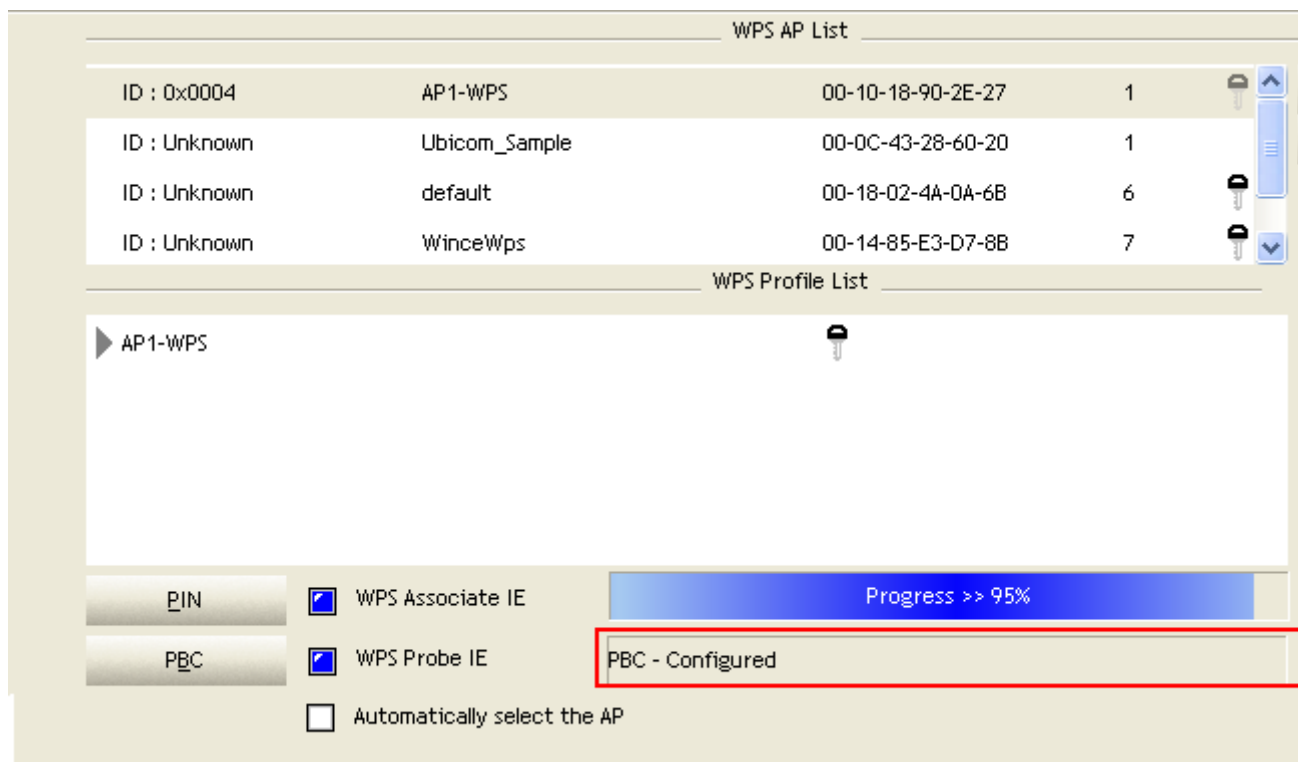
E. When finding only one AP, join it.



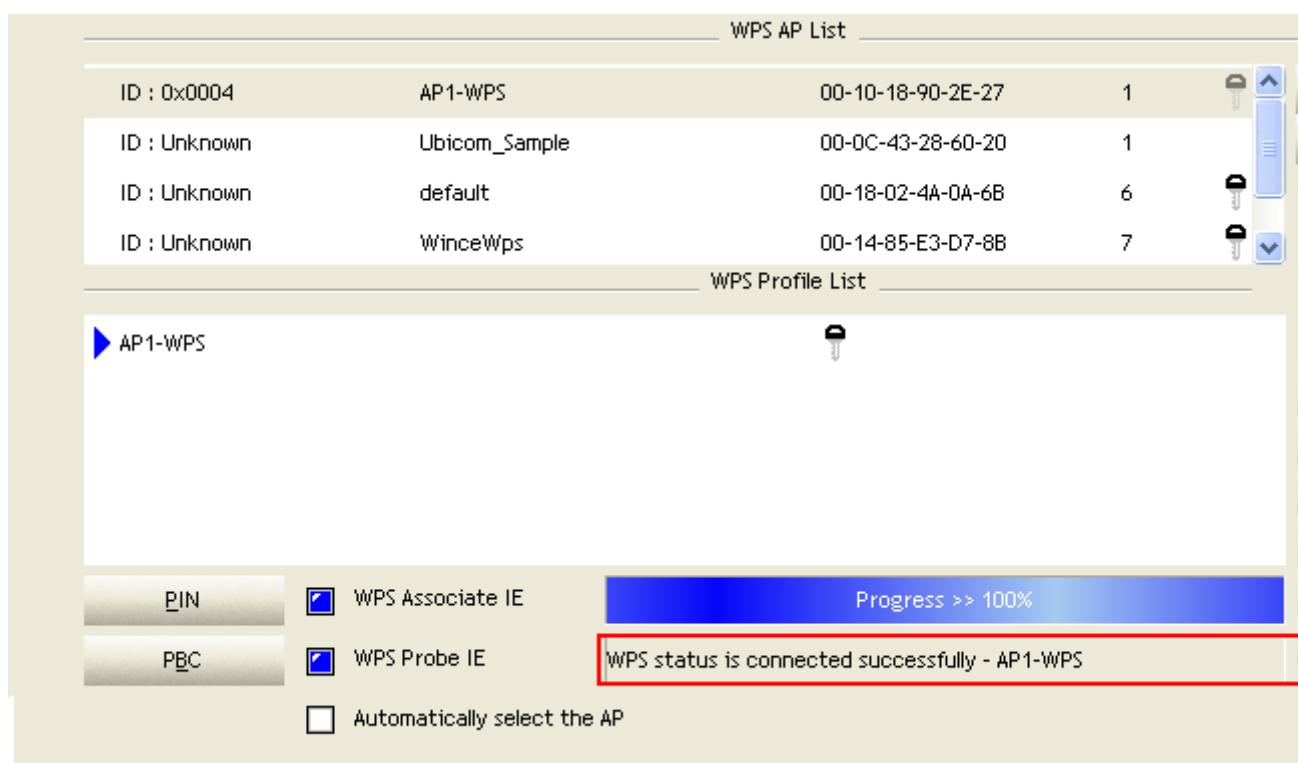
F. Check WPS Information on available WPS APs



G. Configured and got one or multiple credential(s).



H. Then connect successfully. The result will look like the below figure.



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

A. 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

B. No PBC AP available :

Scanning AP ~> No PBC AP available ~> Scanning AP ~> No PBC AP available ~>...

C. Too Many PBC AP available :

Scanning AP ~> Too Many PBC AP available ~> Scanning AP ~> Too Many PBC AP available ~>...

D. WPS configuration doesn't complete after two-minute connection : WPS Eap process failed.

E. When Errors occur within two-minute connection, the WPS status bar might report on " 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.

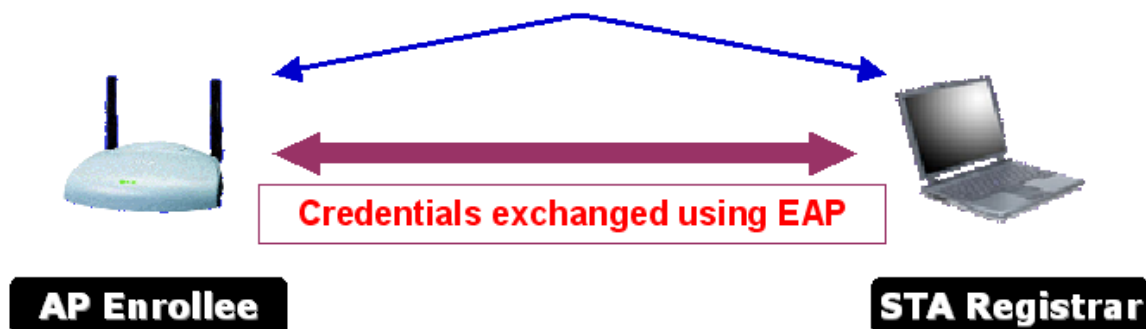
B. Different UUID-E :

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.

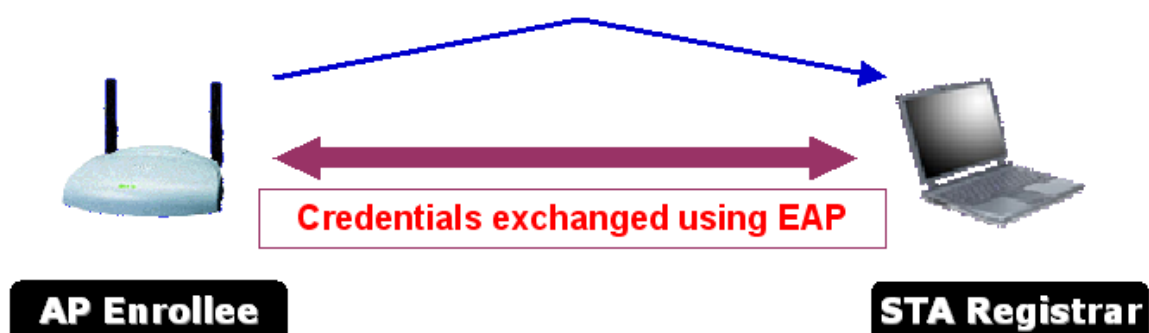
STA would regard these two APs as two different APs and wait until only one PBC AP is available.

EXAMPLE TO CONFIGURE A NETWORK/AP USING PIN OR PBC METHOD

Push PBC button on both Registrar and Enrollee



User types AP PIN into external Registrar



Go to the box of Config Mode and select Registrar.

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	<input checked="" type="checkbox"/> WPS Associate IE	Progress >> 0%
PBC	<input checked="" type="checkbox"/> WPS Probe IE	WPS status is disconnected
<input type="checkbox"/> Automatically select the AP		

B. Enter "Detail" of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if need.

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

C. If PIN configuration setup, enter Pin Code read from your 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

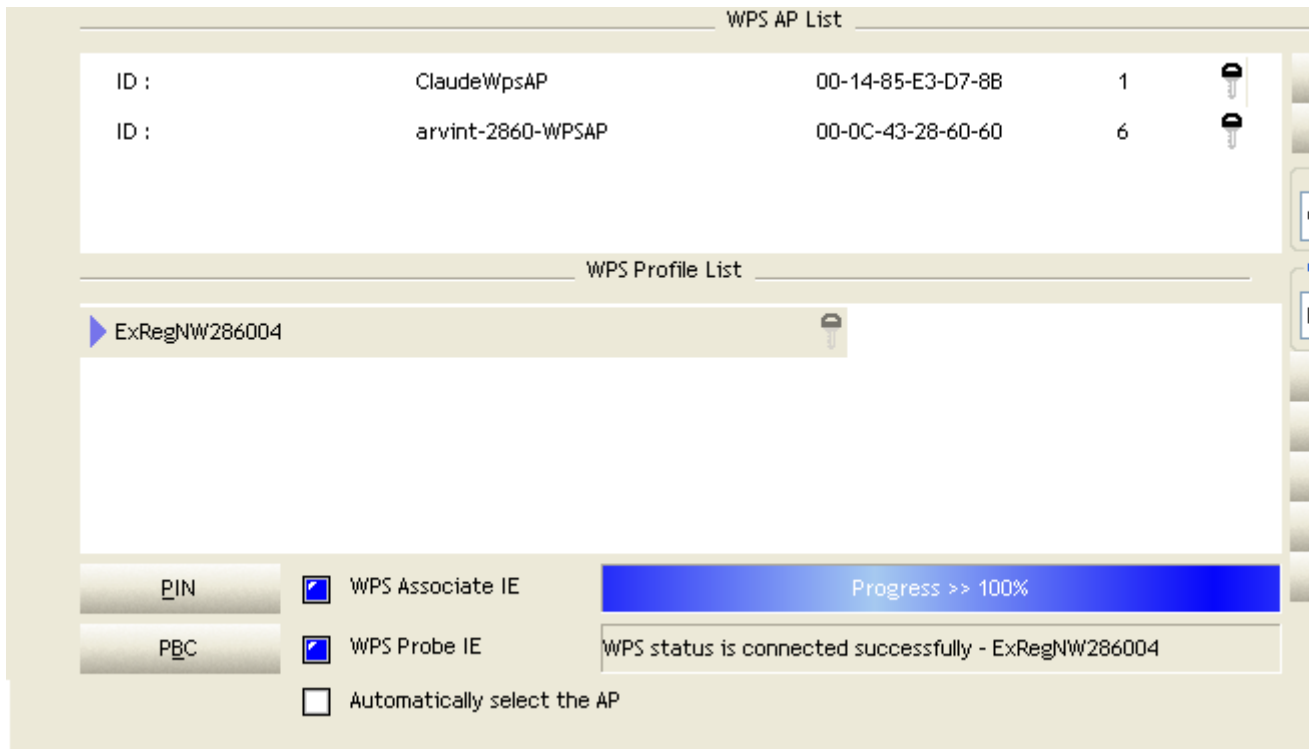
PIN ☒ WPS Associate IE Progress >> 0%

PBC ☒ WPS Probe IE WPS status is disconnected

☐ Automatically select the AP

D. 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),

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

LINK STATUS

Figure 2-9 is the link status page, it displays the detail information current connection.

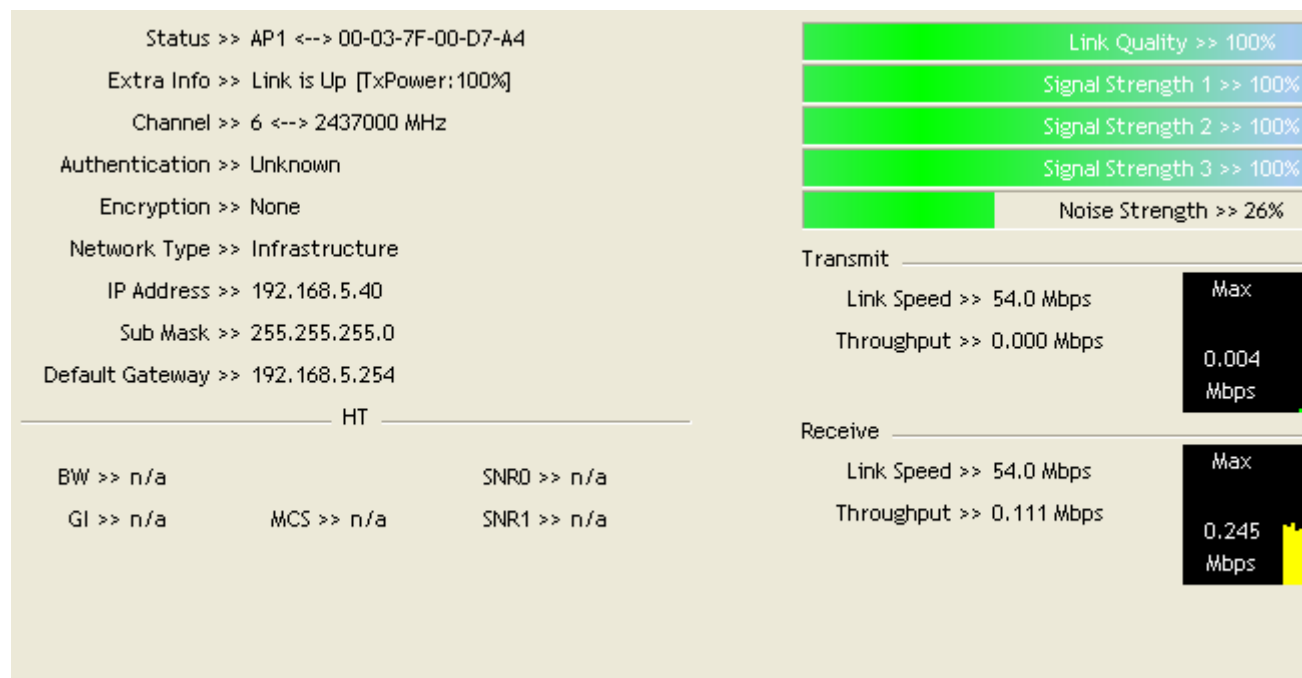


Figure 2-9 Link Status function

A. Status : Current connection status. If no connection, it will show Disconnected. Otherwise, the SSID and BSSID will show here.

B. Extra Info : Display link status in use.

C. Channel : Display current channel in use.

Authentication : Authentication mode in use.

D. Encryption : Encryption type in use.

E. Network Type : Network type in use.

IP Address : IP address about current connection.

F. Sub Mask : Sub mask about current connection.

G. Default Gateway : Default gateway about current connection.

H. Link Speed : Show current transmit rate and receive rate.

I. Throughput : Display transmits and receive throughput in unit of Mbps.

J. Link Quality : Display connection quality based on signal strength and TX/RX packet error rate.

K. Signal Strength 1 : Receive signal strength 1, user can choose to display as percentage or dBm format.

L. Signal Strength 2 : Receive signal strength 2, user can choose to display as percentage or dBm format.

M. Signal Strength 3 : Receive signal strength 3, user can choose to display as percentage or dBm format.

N. Noise Strength : Display noise signal strength.

O. HT : Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value.

(Show the information only for 802.11n wireless card.)

AUTH. \ ENCRY. SETTING - WEP/TKIP/AES

Auth. \ Encry. Setting, shown as Figure 3-1.

Figure 3-1 Auth. \ Encry. Setting

A. 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.

B. 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.

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

D. WPA Pre-shared Key : This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.

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

E-1. Hexadecimal - 40bits : 10 Hex characters.

E-2. Hexadecimal - 128bits : 32Hex characters.

E-3. ASCII - 40bits : 5 ASCII characters.

E-4. ASCII - 128bits : 13 ASCII characters.

**Powered by Meetinghouse.

802.1X SETTING

802.1x is a authentication for "WPA" and "WPA2" certificate to server.

AUTHENTICATION TYPE :

A. PEAP : Protect Extensible Authentication Protocol. PEAP transport securely authentication 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.

B. 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.

C. 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.

D. 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 provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now.

E. LEAP : Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.

F. 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 : user can choose "Disable" and "Enable". Tunnel

AUTHENTICATION :

A. 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".

B. Tunnel Identity : Identity for tunnel.

C. Tunnel Password : Password for tunnel.

- ID \ PASSWORD -

A. Authentication ID / Password : Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.

B. Tunnel ID / Password : Identity and Password for server.

- CLIENT CERTIFICATION -

The screenshot shows a configuration window for wireless authentication. At the top, there's a tab labeled 'Auth. \ Encry.' with a green bar containing '8021X'. Below this, there are dropdown menus for 'EAP Method >>' (set to PEAP) and 'Tunnel Authentication >>' (set to EAP-MSCHAP v2). A checkbox labeled 'Sess' is also present. The main area has three tabs: 'ID \ PASSWORD', 'Client Certification' (which is highlighted in red), and 'Server Certification'. Under the 'Client Certification' tab, there is a checkbox labeled 'Use Client certificate'. To its right, there are three text boxes containing 'wpatest2', '2003serv', and '4/9/2008'. Below these, there are four lines of text: 'Issued To >> wpatest2', 'Issued By >> 2003serv', 'Expired On >> 4/9/2008', and 'Friendly Name >>'. At the bottom, there are 'OK' and 'Cancel' buttons.

A. Use Client certificate : Client certificate for server authentication.

- EAP FAST -

A. 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.

B. Use protected authentication credential : During the PAC can be provisioned to the client manually via disk or a secured network distribution method.

- SERVER CERTIFICATION -

A. Certificate issuer : Choose use server that issuer of certificates.

B. Allow intimate certificates : It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.

C. Server name : Enter an authentication sever root.

EXAMPLE TO RECONNECT 802.1X AUTHENTICATED CONNECTION AFTER 802.1X AUTHENTICATED CONNECTION IS FAILED IN PROFILE

There are two situations to be able to reconnect 802.1x authenticated connection and authenticate successfully after 802.1x authenticated connection is failed in profile page. Two examples about this case are as follows:

When keying in error identity, password or domain name :

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

The screenshot shows the '8021X' configuration window. The 'Auth. \ Encry.' tab is selected. Under 'EAP Method >>', 'PEAP' is chosen. Under 'Tunnel Authentication >>', 'EAP-MSCHAP v2' is chosen. The 'ID \ PASSWORD' tab is active. The 'Authentication ID / Password' section has 'Identity >>' set to 'test', 'Password >>' set to 'test', and 'Domain Name >>' is empty. The 'Tunnel ID / Password' section has 'Identity >>' set to 'test' and 'Password >>' set to 'test'. 'OK' and 'Cancel' buttons are at the bottom.

B. Because keying error identity and error password, the result will look like the below figure.

The screenshot shows an 'Authentication Failure' dialog box. It displays 'Card Name >> Ralink 802.11n Wireless LAN Card', 'Profile Name >> PROF1', and 'Message >> Invalid identity or password'. There are empty input fields for 'Identity >>' and 'Password >>'. 'OK' and 'Cancel' buttons are at the bottom.

C. If you want to disconnect, click cancel button in Authentication Failure dialog. If you want to reconnect, key identity into wpatest2. And tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

Card Name >> Ralink 802.11n Wireless LAN Card	Identity >> wpatest2
Profile Name >> PROF1	Password >> test2
Message >> Invalid identity or password	
<div style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div>	

D. Click "OK" button. If it connected successfully, the result will look like the below figure.

The RaUI window displays the 'Network' tab. The 'Profile List' on the left shows 'PROF1' with 'AP1' as the selected profile. The right pane shows configuration details for this profile, including SSID, Network Type, Authentication, Encryption, and various thresholds. The bottom section shows the connection status for 'AP1', including link quality, signal strength, and network parameters.

Profile List 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
Add Edit Delete Activate		
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 HT		Link Quality >> 100% Signal Strength 1 >> 10 Signal Strength 2 >> 10 Signal Strength 3 >> 10 Noise Strength >> 26 Transmit Link Speed >> 54.0 Mbps Throughput >> 0.000 Kbps Receive Link Speed >> 54.0 Mbps Throughput >> 90.016 Kbps
BW >> n/a SNR0 >> n/a GI >> n/a MCS >> n/a SNR1 >> n/a		

When occurring "Timeout" :

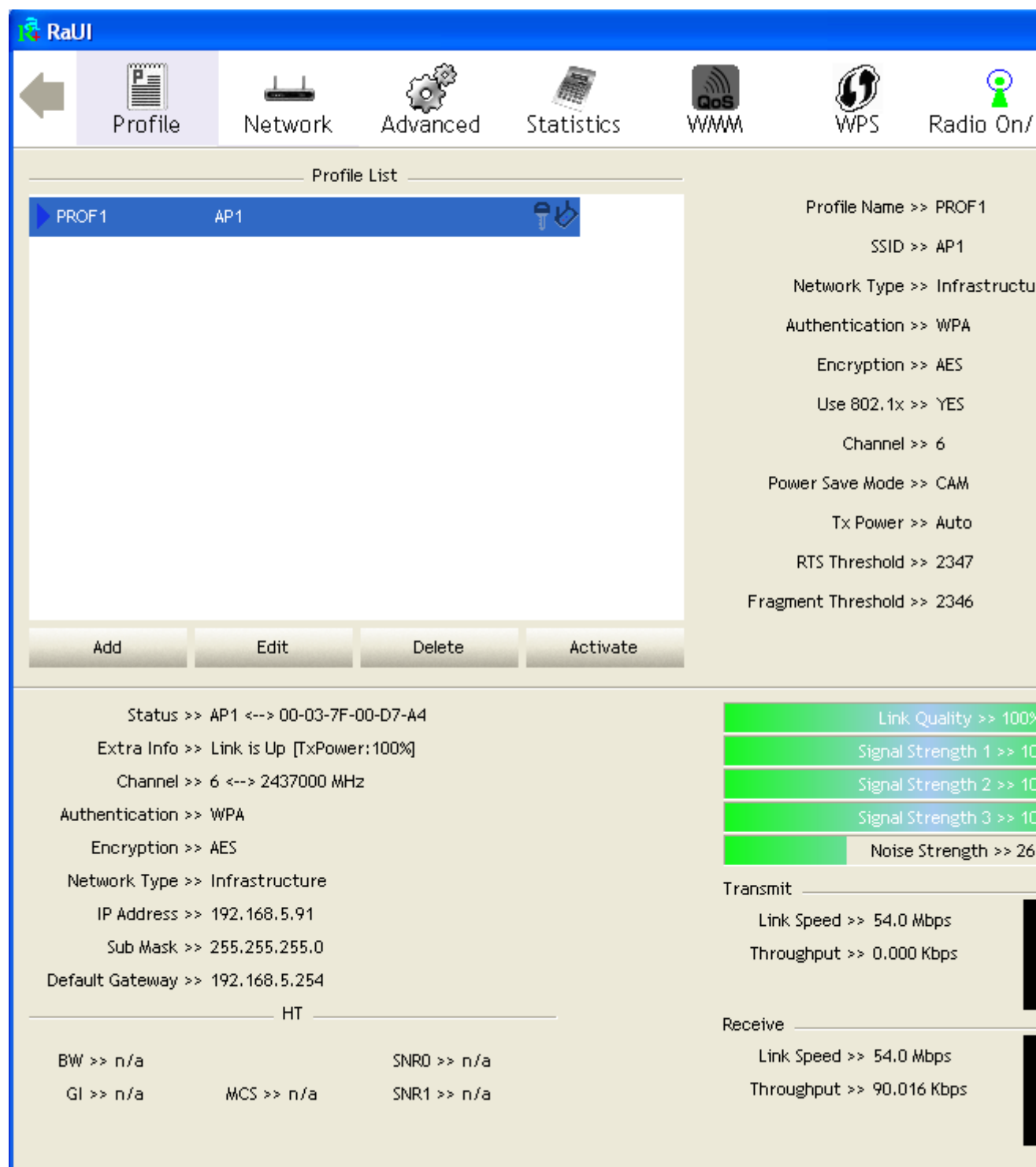
A. Authentication type chooses "PEAP", key identity into wpatest2. Tunnel Protocol is "EAP-MSCHAP-v2, and tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

The screenshot shows the configuration window for the wireless adapter. The 'Auth. \ Encry.' tab is selected, and the '8021X' button is highlighted. The 'EAP Method >>' is set to 'PEAP' and 'Tunnel Authentication >>' is set to 'EAP-MSCHAP v2'. The 'ID \ PASSWORD' tab is active, showing the 'Authentication ID / Password' section with 'Identity >>' set to 'wpatest2' and 'Password >>' set to 'test2'. The 'Tunnel ID / Password' section also has 'Identity >>' set to 'wpatest2' and 'Password >>' set to 'test2'. The 'OK' and 'Cancel' buttons are at the bottom.

B. Because occurring "Timeout", the result will look like the below figure.

The screenshot shows an error message dialog box. The 'Card Name >>' is 'Ralink 802.11n Wireless LAN Card' and the 'Profile Name >>' is 'PROF1'. The 'Message >>' text reads: 'Unable to PEAP authenticate the wireless user in the specified amount of time. Network infrastructure might be down. Please press OK to reconnect.' The 'OK' and 'Cancel' buttons are at the bottom.

c. If it connected successfully, the result will look like the below figure.



EXAMPLE TO CONFIGURE CONNECTION WITH WEP ON

A. Select AP with WEP encryption and click "Connect" button.

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays several available access points. The 'ariscadre' AP is selected, and its connection details are shown below the table.

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

Buttons: Rescan, Add to Profile, Connect

Connection Details for ariscadre:

- 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 Statistics:

- Link Quality >> 100%
- Signal Strength 1 >> 1
- Signal Strength 2 >> 10
- Signal Strength 3 >> C
- Noise Strength >> 26
- Link Speed >> 270.0 Mbps
- Throughput >> 0.000 Mbps

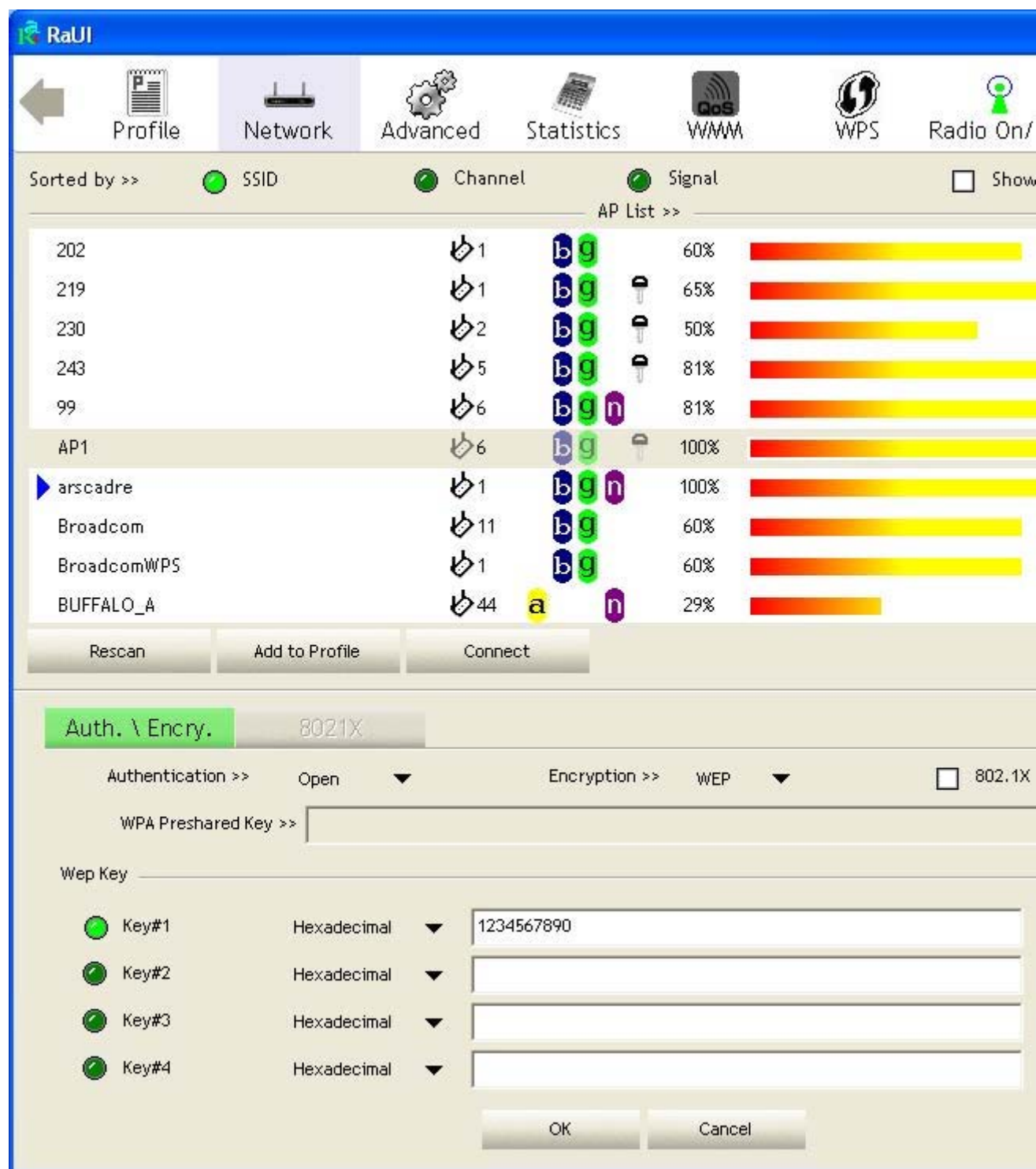
Receive Statistics:

- Link Speed >> 1.0 Mbps
- Throughput >> 0.026 Mbps

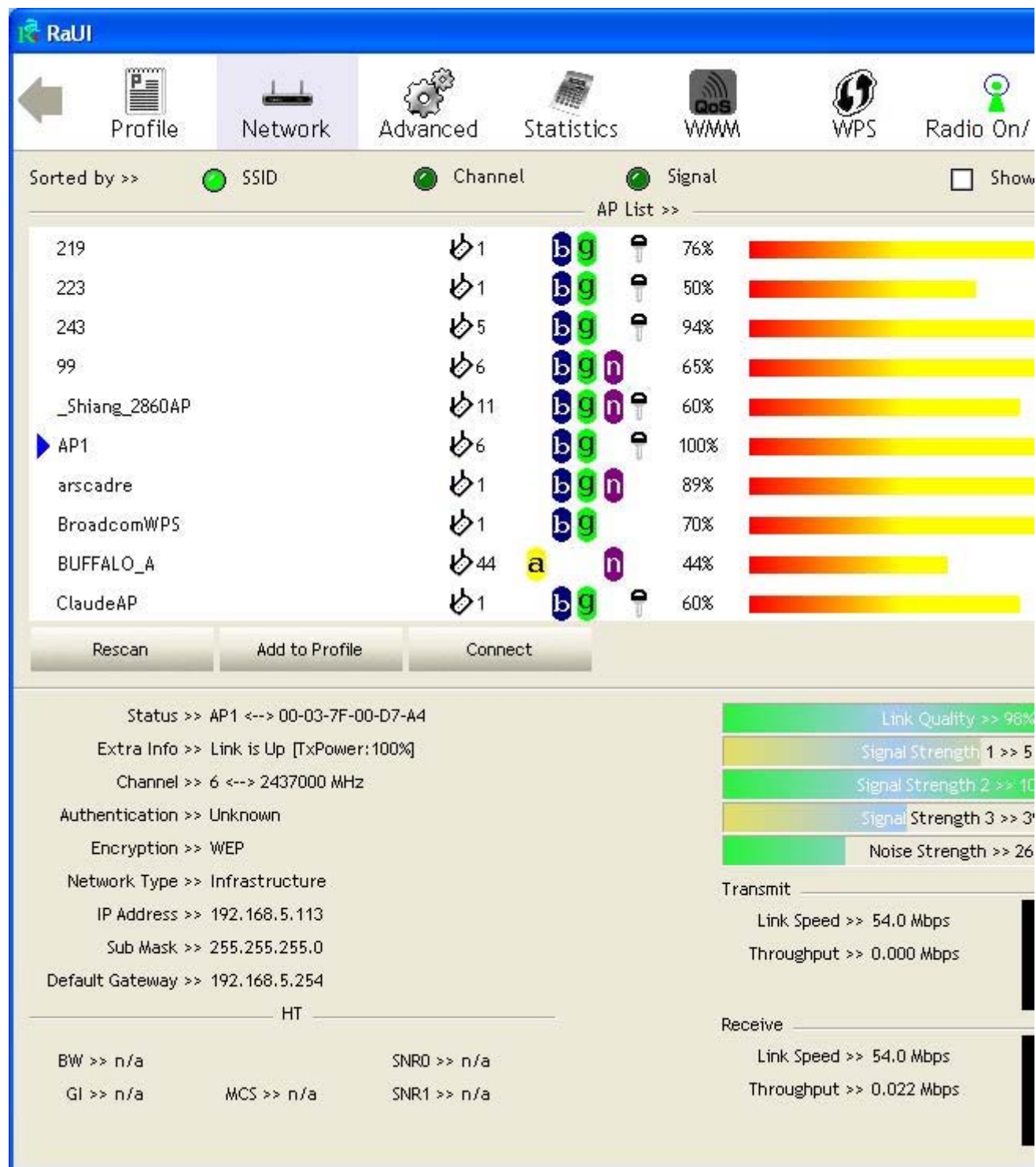
B. Auth. \ Encry. function pop up.



C. Enter 1234567890 at Key#1 which is same as our intended AP's setting.



D. Click "OK" button. The result will look like the below figure.



EXAMPLE TO CONFIGURE CONNECTION WITH WPA-PSK

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

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays various access points, with 'arscadre' selected. Below the table, the 'Connect' button is visible. The bottom section shows the connection status and details for 'arscadre'.

AP Name	Channel	Signal	Link Quality
0148-1	60	20%	
11n	1	50%	
132	2	60%	
202	1	60%	
219	1	76%	
243	5	91%	
99	6	81%	
_Shiang_2860AP	11	65%	
AP1	6	100%	
arscadre	1	99%	

Buttons: Rescan, Add to Profile, Connect

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 >> 1

Signal Strength 2 >> 9

Signal Strength 3 >> 0

Noise Strength >> 26

Transmit

Link Speed >> 270.0 Mbps

Throughput >> 0.000 Mbps

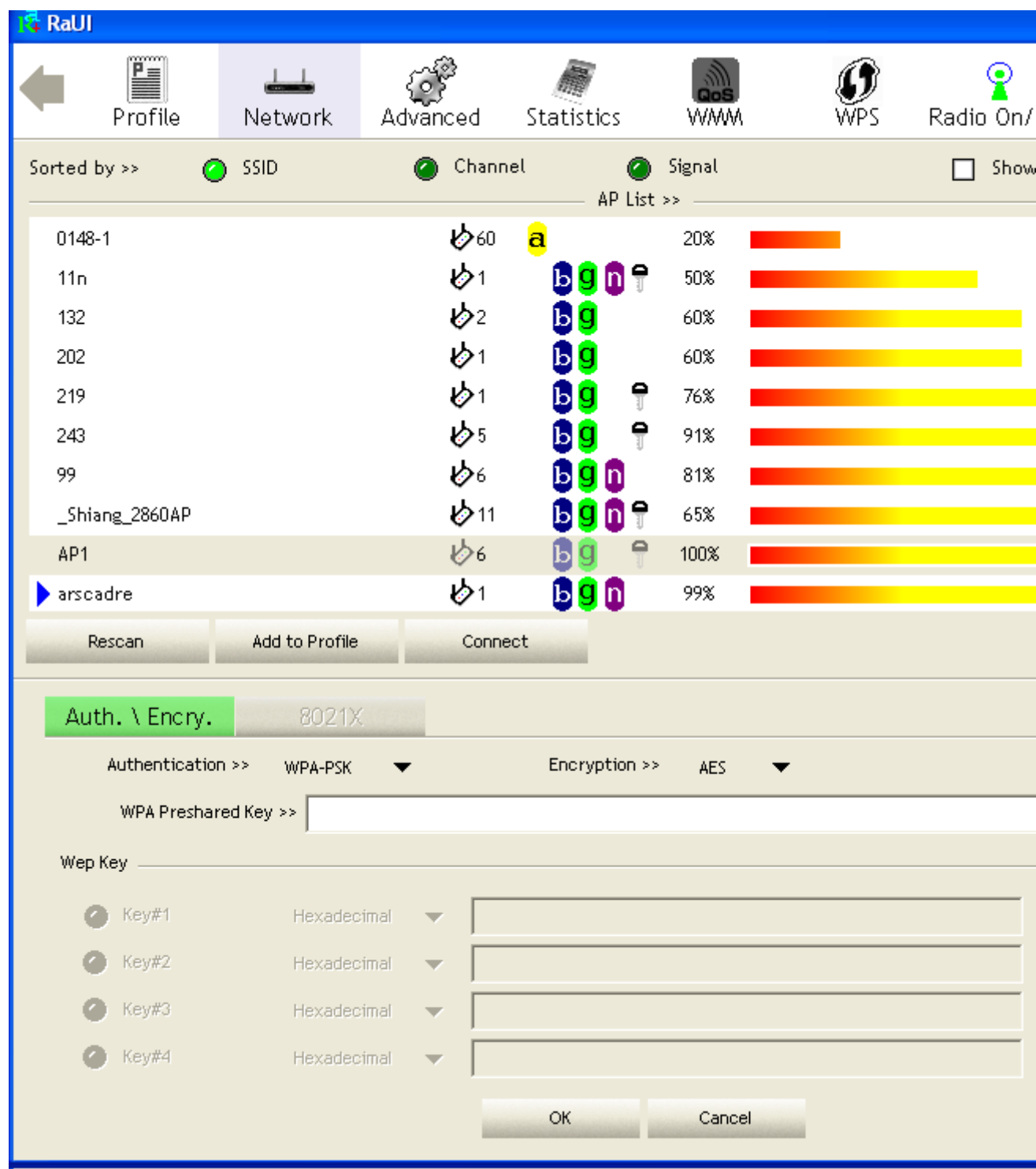
Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.012 Mbps

B. Auth. \ Encry. function pop up.

(If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)



C. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Key secret as 12345678.

The screenshot shows the RaUI Network configuration window. The 'Network' tab is selected. The 'AP List' table displays various wireless networks with their SSIDs, channels, security types, and signal strengths. The 'ariscadre' network is highlighted. Below the table, the 'Auth. \ Encry.' section is set to 'WPA-PSK' and 'AES'. The 'WPA Preshared Key' is entered as '12345678'. The 'Wep Key' section shows four keys, all set to 'Hexadecimal'.

SSID	Channel	Security	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%
ariscadre	1	b g n	99%

Auth. \ Encry. 8021X

Authentication >> WPA-PSK Encryption >> AES

WPA Preshared Key >> 12345678

Wep Key

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

OK Cancel

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

RaUI

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

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

AP List >>

SSID	Channel	Signal	Strength
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%

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 >> 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 SNR0 >> n/a

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

Link Quality >> 88%

Signal Strength 1 >> 4

Signal Strength 2 >> 10

Signal Strength 3 >> 0

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.001 Mbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.021 Mbps

EXAMPLE TO CONFIGURE CONNECTION WITH WPA

A. Select AP with WPA authentication mode and click "Connect" button.

RaUI

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

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

AP List >>

AP Name	Channel	Auth Mode	Signal	Link Quality
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%	

Rescan | Add to Profile | Connect

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 >>

Receive

Link Speed >>

Throughput >>

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

The image shows the RaUI Network tab with an AP list and a security configuration dialog.

AP List >>

AP Name	Channel	Security	Signal
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%

Buttons: Rescan, Add to Profile, Connect

Auth. \ Encry. 8021X

Authentication >> WPA Encryption >> AES

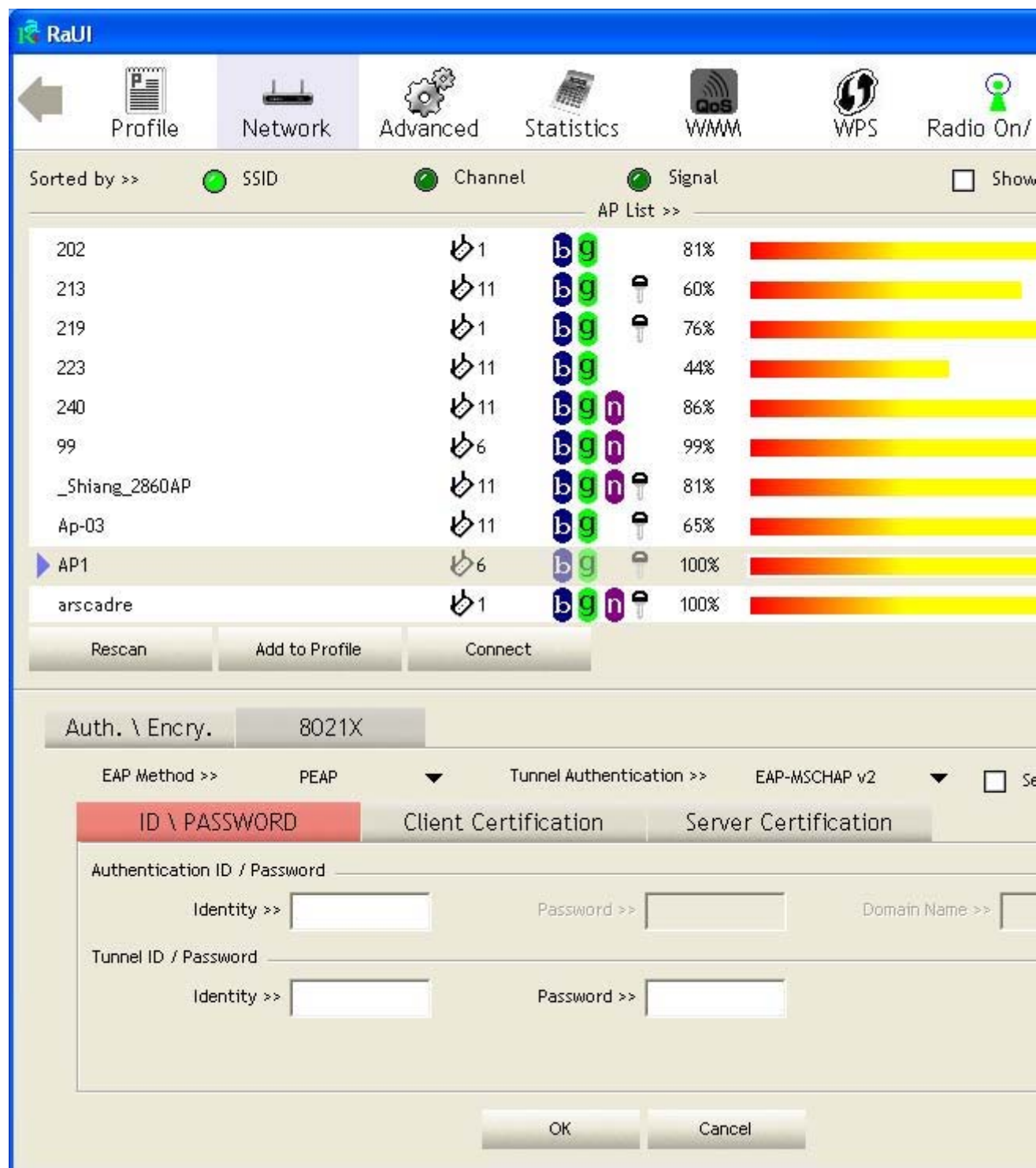
WPA Preshared Key >>

Wep Key

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

Buttons: OK, Cancel

C. Click "8021X" button and 802.1x setting page will pop up.



D. Authentication type and setting method :

PEAP :

A. Authentication type chooses PEAP, key identity into wpatest2. Protocol chooses EAP- MSCHAP v2 for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

The screenshot shows the RaUI interface with the Network tab selected. The AP List table displays various wireless networks with their SSIDs, channels, security types, and signal strengths. Below the table are buttons for Rescan, Add to Profile, and Connect. The authentication settings are configured for PEAP with EAP-MSCHAP v2 protocol. The ID \ PASSWORD tab is active, showing fields for Identity and Password for both Authentication and Tunnel, both set to wpatest2 and test2 respectively.

Sorted by >>	SSID	Channel	Signal	AP List >>
	240	11	91%	b g n
	243	4	15%	b g
	99	6	91%	b g n
	_Shiang_2860AP	11	96%	b g n
	Ap-03	11	70%	b g
	AP1	6	100%	b g
	AP47-g	1	24%	b g
	arscadre	1	91%	b g n
	arvint-2860AP	7	91%	b g n
	Broadcom	11	76%	b g

Buttons: Rescan, Add to Profile, Connect

Auth. \ Encry. 8021X

EAP Method >> PEAP Tunnel Authentication >> EAP-MSCHAP v2

ID \ PASSWORD Client Certification Server Certification

Authentication ID / Password

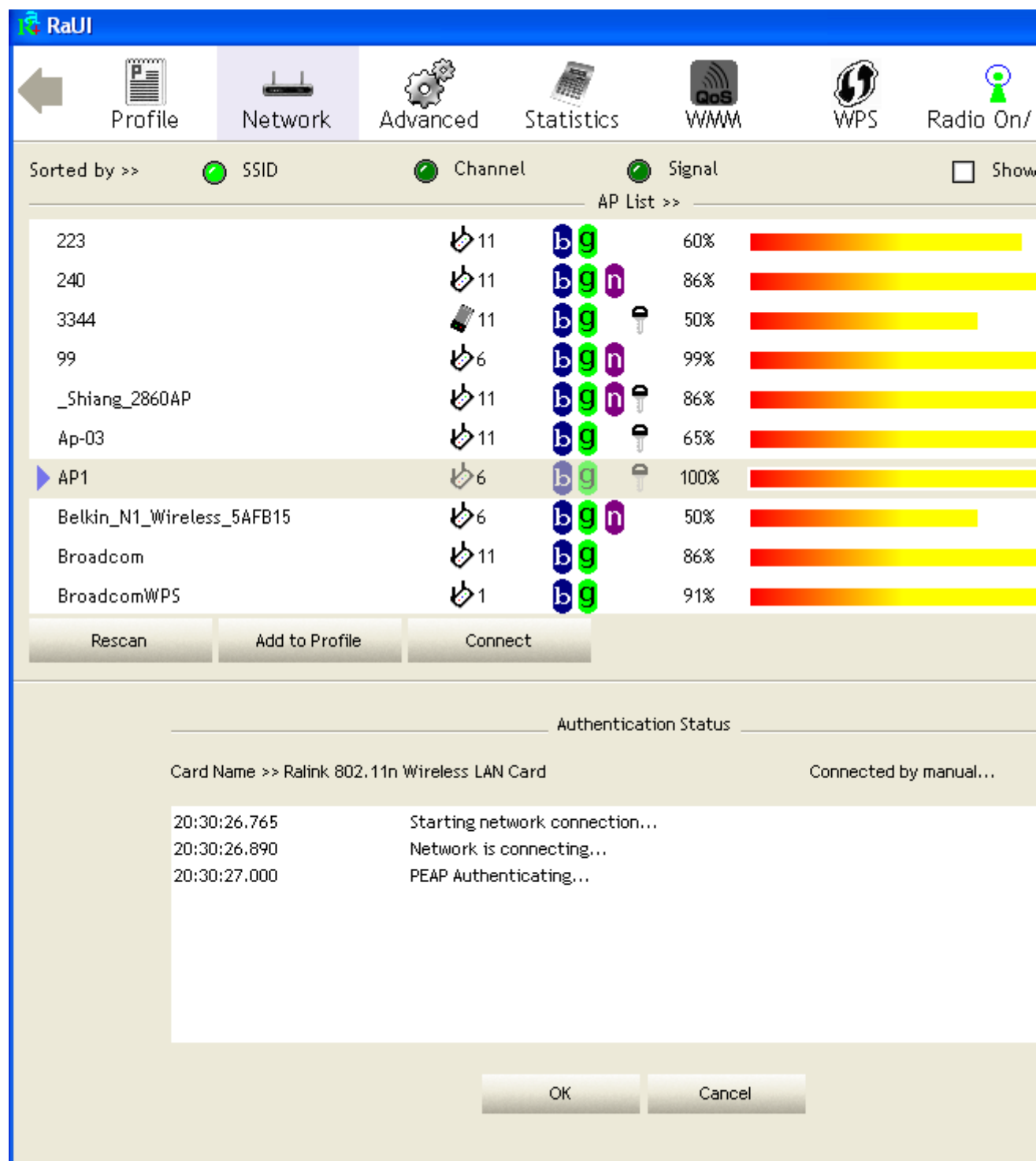
Identity >> wpatest2 Password >> Domain Name >>

Tunnel ID / Password

Identity >> wpatest2 Password >> test2

Buttons: OK, Cancel

B. Click OK. The result will look like the below figure.



*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.

C. If it connected successfully, the result will look like the below figure.

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays various wireless networks. The 'AP1' network is selected, and its connection details are shown below the table. The 'Transmit' and 'Receive' sections show link speed and throughput.

Sorted by >>	SSID	Channel	Signal	AP List >>
	202	1	81%	
	213	11	60%	
	219	1	76%	
	223	11	44%	
	240	11	86%	
	99	6	99%	
	_Shiang_2860AP	11	81%	
	Ap-03	11	65%	
	AP1	6	100%	
	arscadre	1	100%	

Buttons: 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 >> 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

Transmit

Link Quality >> 89%
 Signal Strength 1 >> 10
 Signal Strength 2 >> 10
 Signal Strength 3 >> 10
 Noise Strength >> 26

Link Speed >> 54.0 Mbps
 Throughput >> 0.000 Kbps

Receive

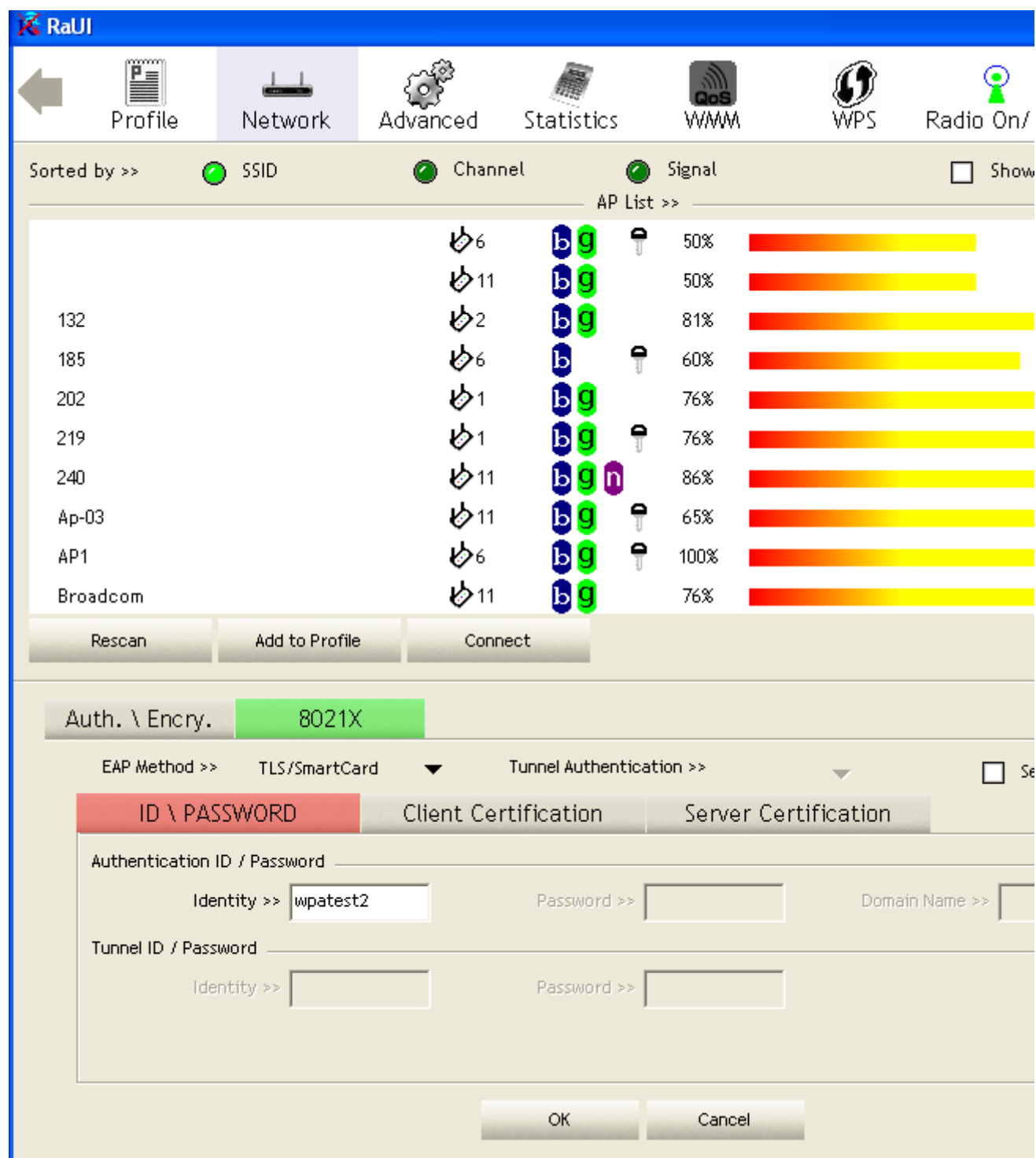
Link Speed >> 54.0 Mbps
 Throughput >> 57.148 Kbps

HT

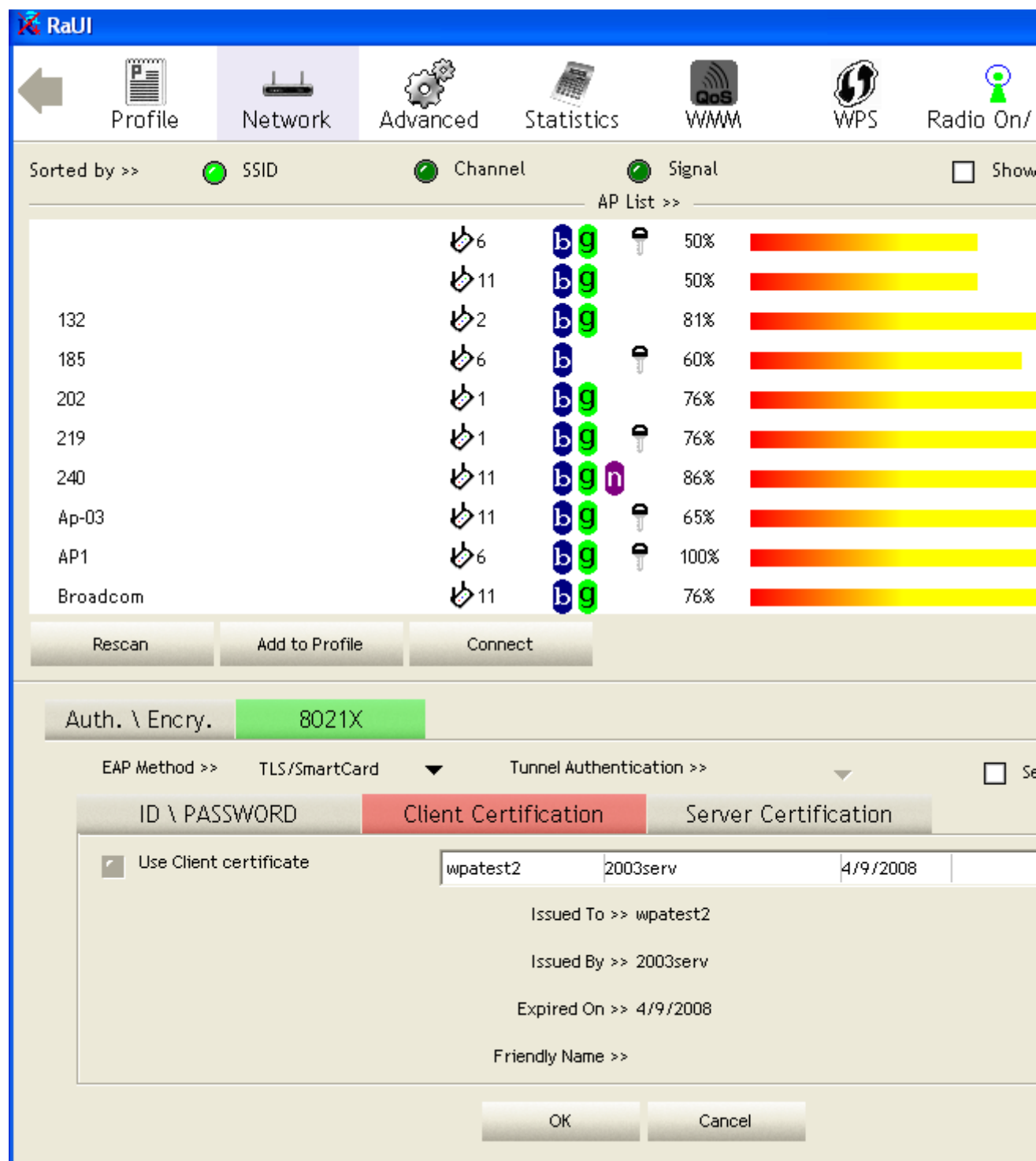
BW >> n/a
 GI >> n/a
 MCS >> n/a
 SNR0 >> n/a
 SNR1 >> n/a

TLS / Smart Card :

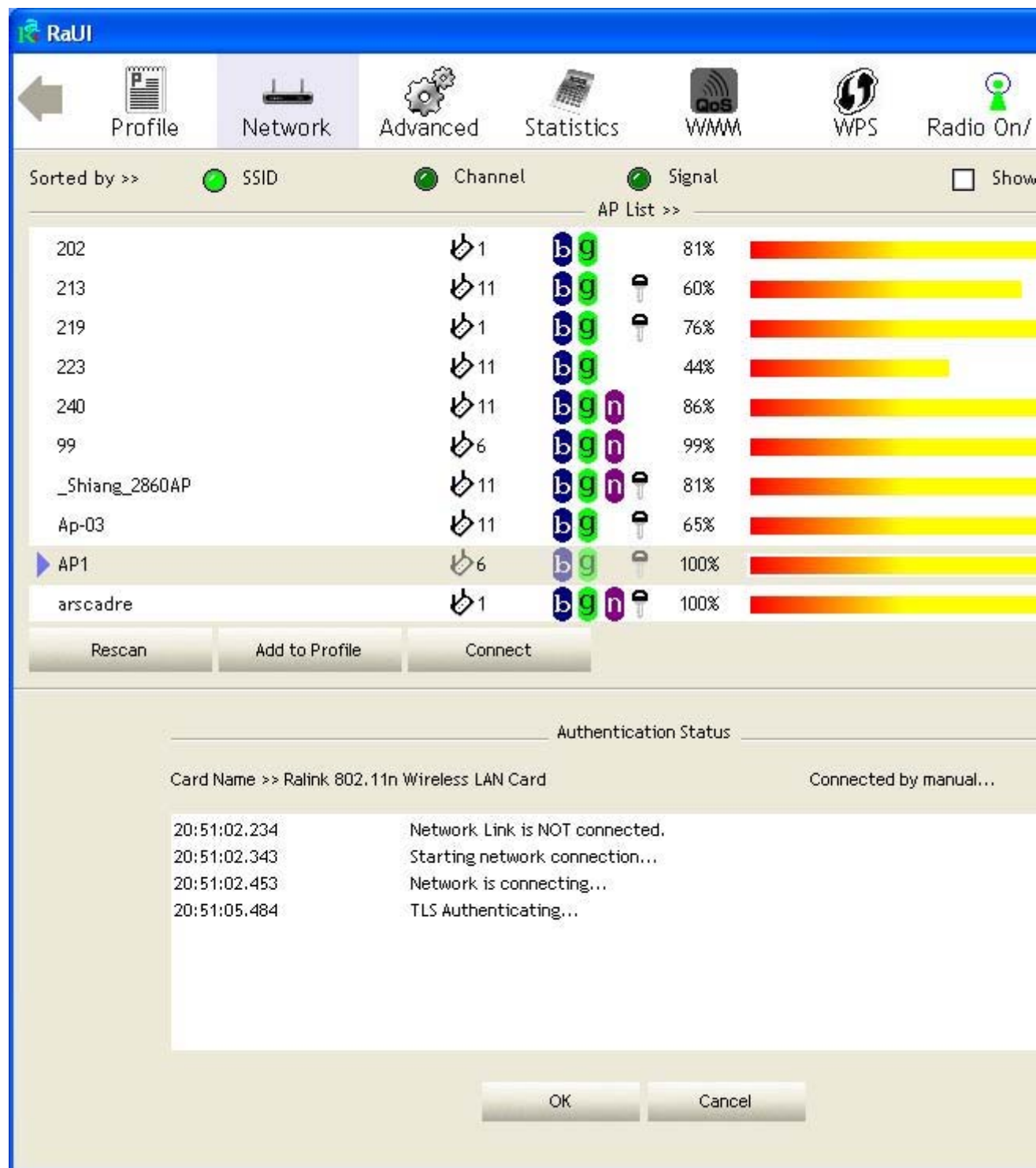
A. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.



B. TLS must use client certification. Click "Client Certification" button and choose a certification for server authentication.



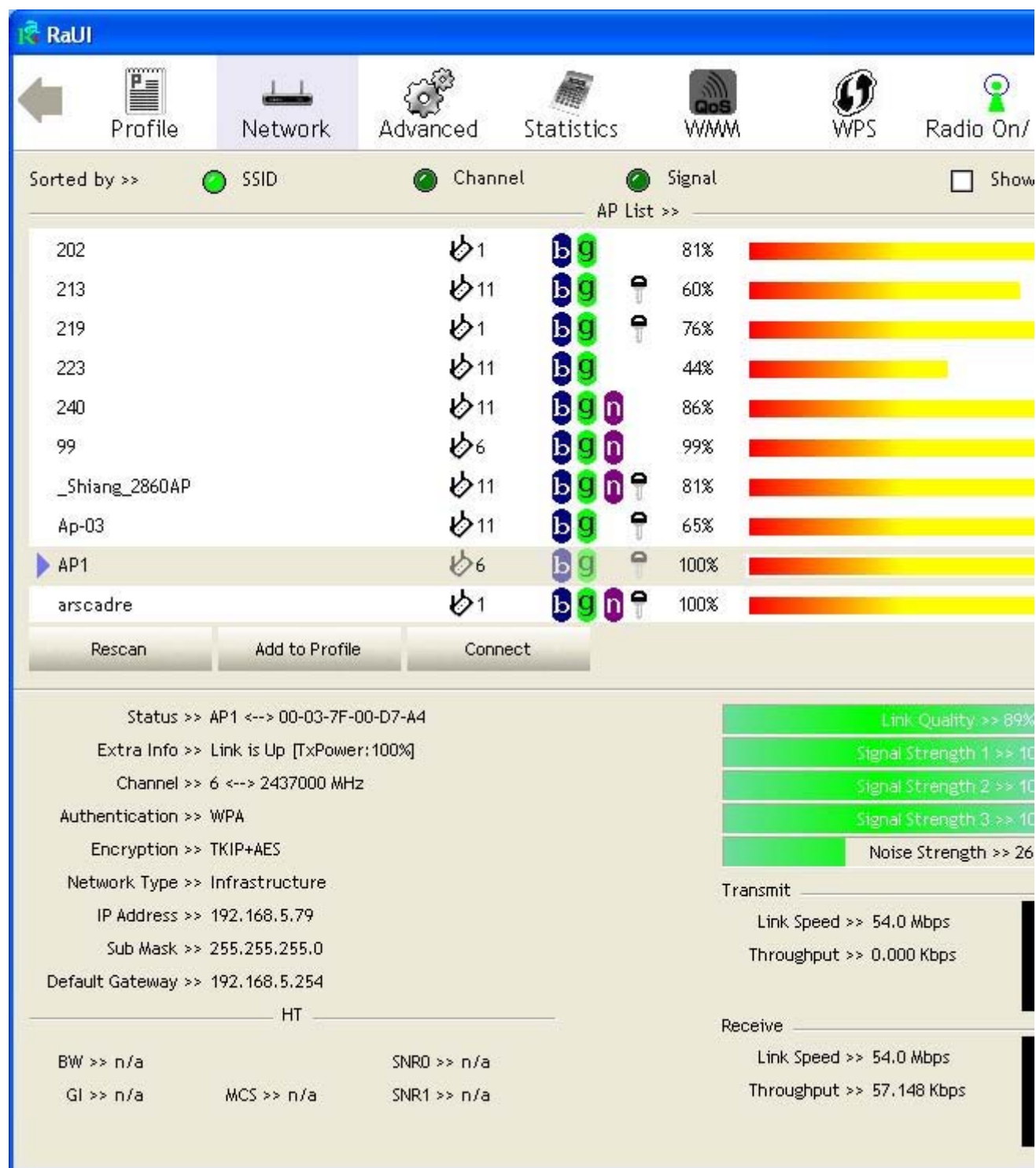
C. Click "OK" button. The result will look like the below figure.



*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.

D. If it connected successfully, the result will look like the below figure.



TTLS :

A. Authentication type chooses TTLS, identity is wpatest2. Protocol chooses CHAP for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by Signal strength. Below the list, the authentication configuration is shown with the following settings:

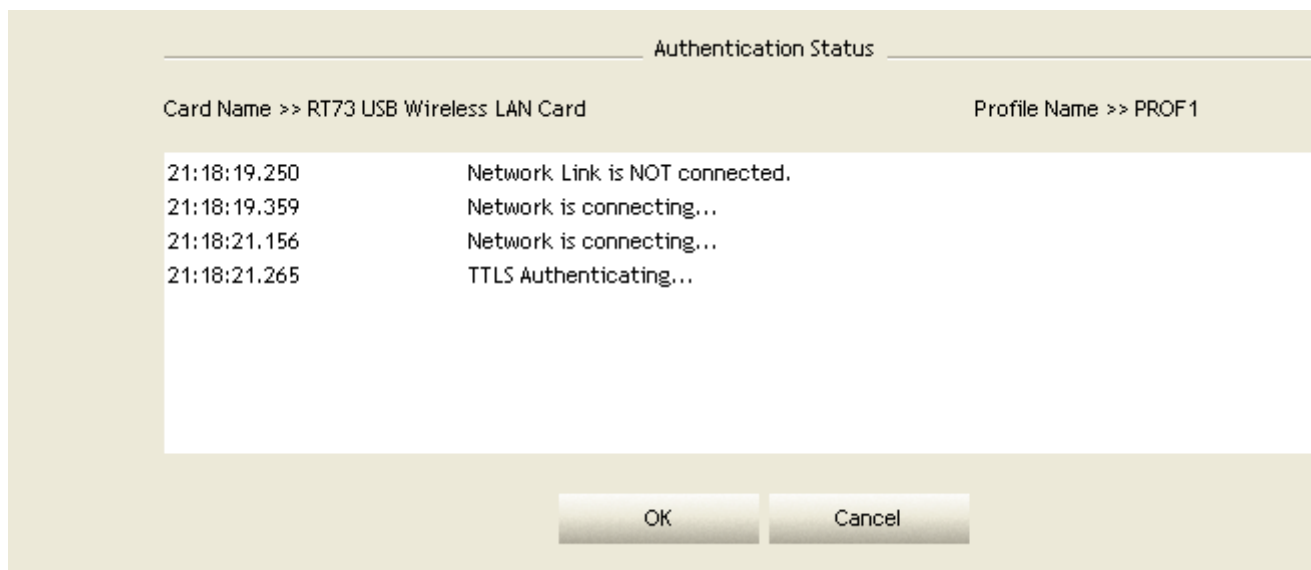
AP Name	Channel	Signal
132	6	50%
185	11	50%
202	2	81%
219	6	60%
240	1	76%
Ap-03	1	76%
AP1	11	86%
Broadcom	11	65%
	6	100%
	11	76%

Below the AP list, the authentication configuration is shown with the following settings:

- Auth. \ Encry.: 8021X
- EAP Method >>: TTLS
- Tunnel Authentication >>: CHAP
- ID \ PASSWORD: Client Certification
- Authentication ID / Password:
 - Identity >>: wpatest2
 - Password >>:
 - Domain Name >>:
- Tunnel ID / Password:
 - Identity >>: wpatest2
 - Password >>: test2

Buttons: Rescan, Add to Profile, Connect, OK, Cancel.

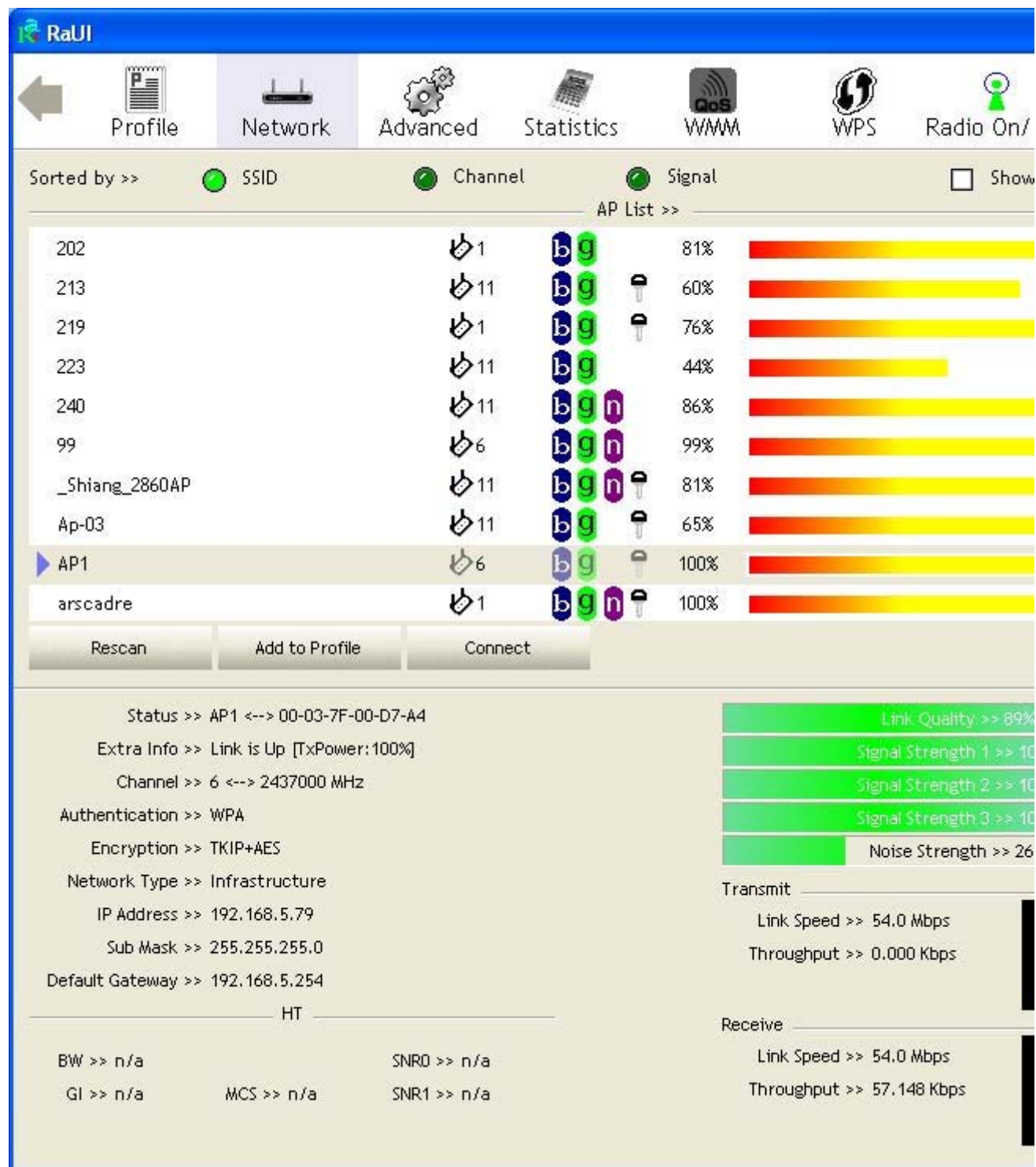
B. Click "OK" button. The result will look like the below figure.



*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.

C. If it connected successfully, the result will look like the below figure.



EAP-FAST :

A. Authentication type chooses EAP-FAST, key identity into wpatest2; key domain name into blank space. Tunnel Protocol only supported "Generic Token Card" now, and tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

The screenshot shows the RaUI Network configuration window. The 'Network' tab is selected. The 'AP List' table displays the following data:

AP Name	Channel	SSID	Signal
132	6	b g	50%
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%

Below the AP List, the 'Auth. \ Encry.' section is set to '8021X'. The 'EAP Method' is 'EAP-FAST' and 'Tunnel Authentication' is 'Generic Token Card'. The 'EAP Fast' tab is selected, showing the following settings:

Authentication ID / Password:

- Identity >> wpatest2
- Password >>
- Domain Name >>

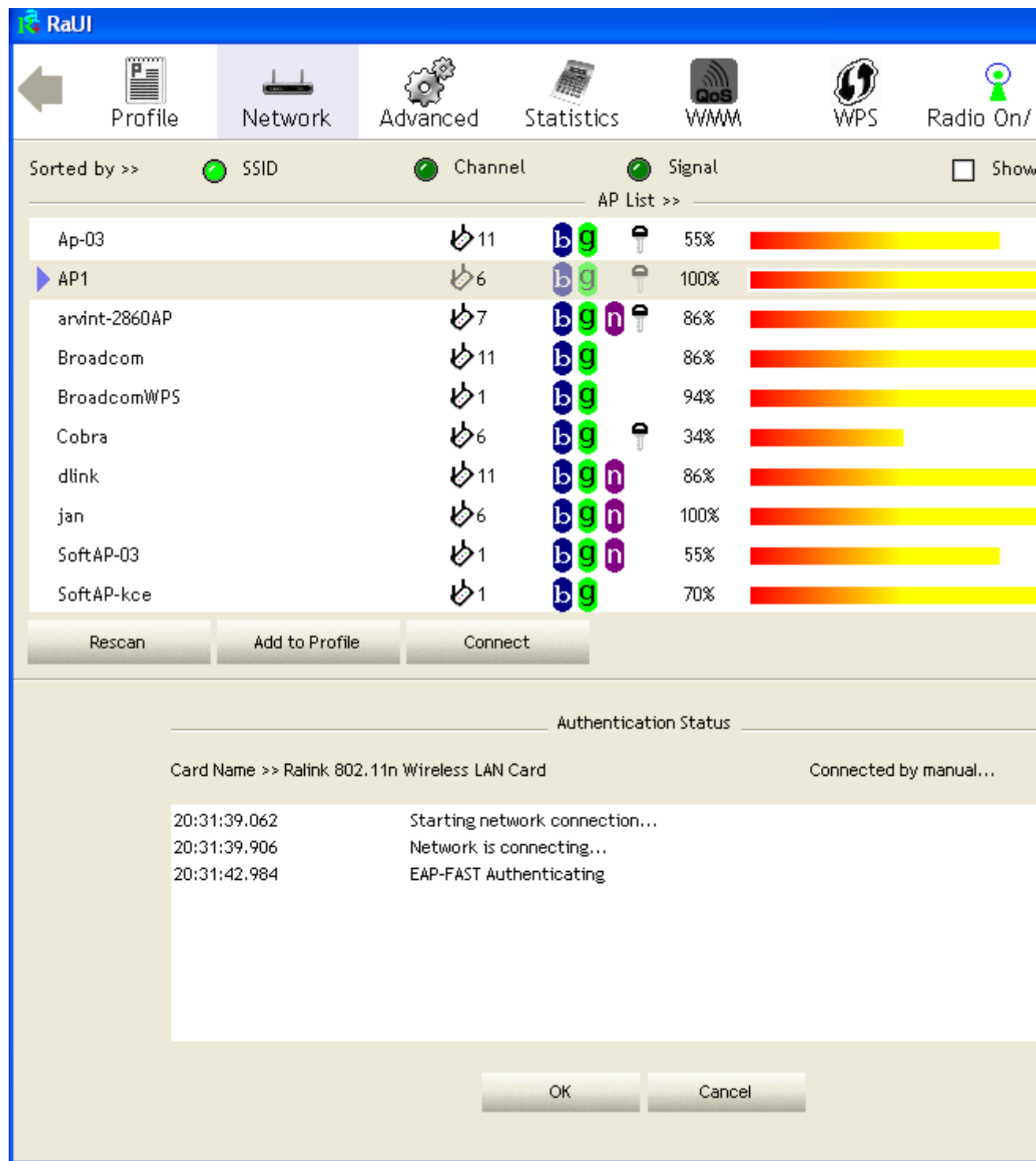
Tunnel ID / Password:

- Identity >> wpatest2
- Password >> test2

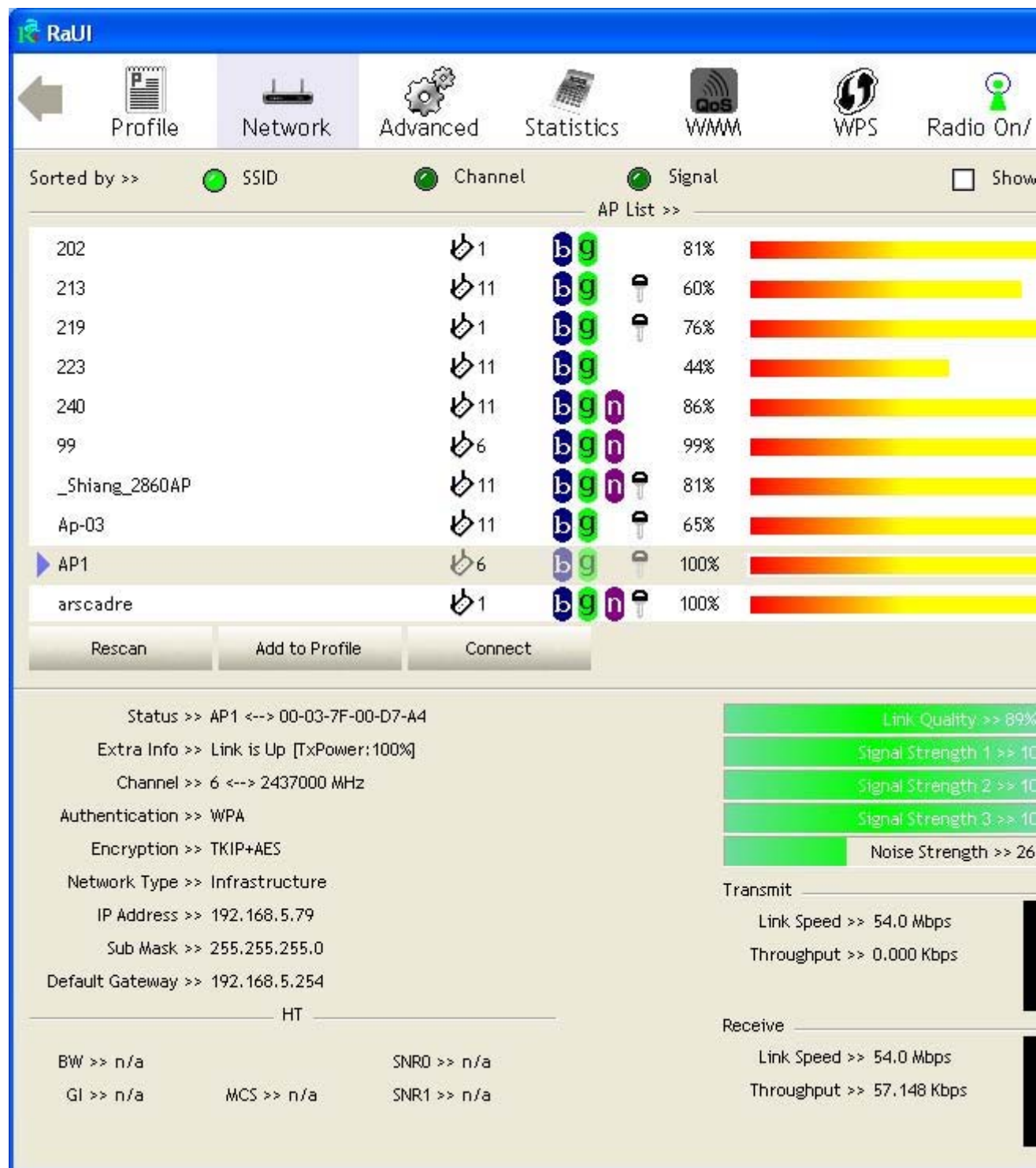
Password Mode >> ☒ Soft Token ☒ Static Password

Buttons: OK, Cancel

B. Click "OK" button. The result will look like the below figure.



C. If it connected successfully, the result will look like the below figure.



*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.

ACKNOWLEDGEMENTS

The above setting is test platform by RaLink technology corp. User can set the function in accordance with A.P.

Acknowledgements:

"This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)". This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Thank you for purchasing a quality Rosewill Product.

Please register your product at : www.rosewill.com for complete warranty information and future support for your product.