

# **Wireless LAN PCI Card**

## **User Manual V1.1**

# Content

<b>Introduction</b> .....	<b>3</b>
<b>Specifications</b> .....	<b>4</b>
<b>Installation/ Uninstallation</b> .....	<b>5</b>
<b>Ralink Wireless Utility ( RaUI ) or Windows Zero Configuration ( WZC )</b> .....	<b>10</b>
<b>Use WZC to configure wireless NIC</b> .....	<b>12</b>
<b>Start RaUI</b> .....	<b>19</b>
<b>Profile</b> .....	<b>26</b>
<b>Add/Edit Profile</b> .....	<b>28</b>
<b>Example to Add Profile in Profile</b> .....	<b>30</b>
<b>Network</b> .....	<b>34</b>
<b>Example on Adding Profile in Network</b> .....	<b>42</b>
<b>Advanced</b> .....	<b>46</b>
<b>Statistics</b> .....	<b>47</b>
<b>WMM</b> .....	<b>49</b>
<b>Example to Configure to Enable DLS (Direct Link Setup)</b> .....	<b>50</b>
<b>Example to Configure to Enable Wi-Fi Multi-Media</b> .....	<b>56</b>
<b>Example to Configure to Enable WMM Power Save</b> .....	<b>58</b>
<b>WPS</b> .....	<b>59</b>
<b>WPS Information on AP</b> .....	<b>61</b>
<b>Example to Add to Registrar Using PIN Method</b> .....	<b>63</b>
<b>Example to Add to Registrar Using PBC Method</b> .....	<b>69</b>
<b>Example to Configure a Network/AP Using PIN or PBC Method</b> .....	<b>74</b>
<b>Link Status</b> .....	<b>77</b>
<b>Auth. \ Encry. Setting - WEP/TKIP/AES</b> .....	<b>78</b>
<b>802.1x Setting</b> .....	<b>79</b>
<b>Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is Failed in Profile</b> .....	<b>82</b>
<b>Example to Configure Connection with WEP on</b> .....	<b>86</b>
<b>Example to Configure Connection with WPA-PSK</b> .....	<b>90</b>
<b>Example to Configure Connection with WPA</b> .....	<b>94</b>
<b>Country Channel List</b> .....	<b>110</b>
<b>Acknowledgements</b> .....	<b>112</b>

## 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.

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

**IMPORTANT NOTE:** To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user’s authority to operate the device. This device should be installed and operated with a minimum distance of 20centimeters between the radiator and your body.

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

•The equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on , the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval Form Loopcomm Technology, Inc..Modification could void authority to use this equipment.

## 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

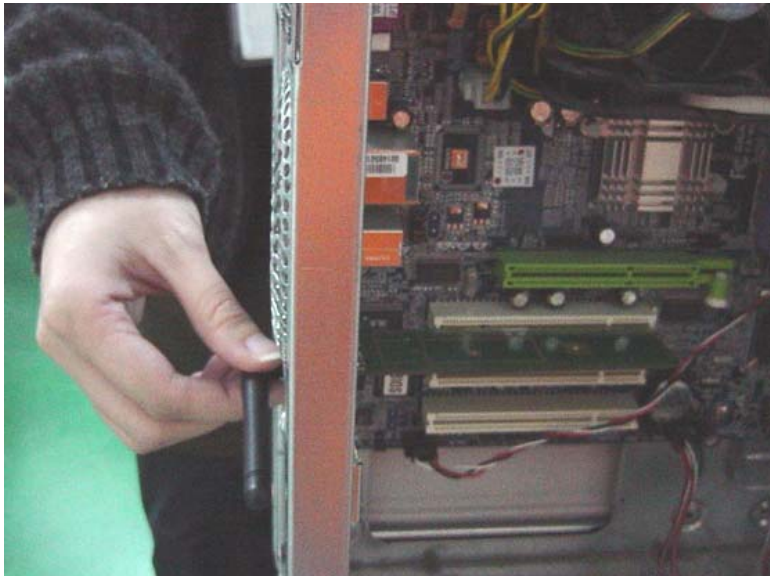
## Installation

### Hardware Installation

Install Wireless LAN PCI Card (card only) into your computer PCI slot as below.

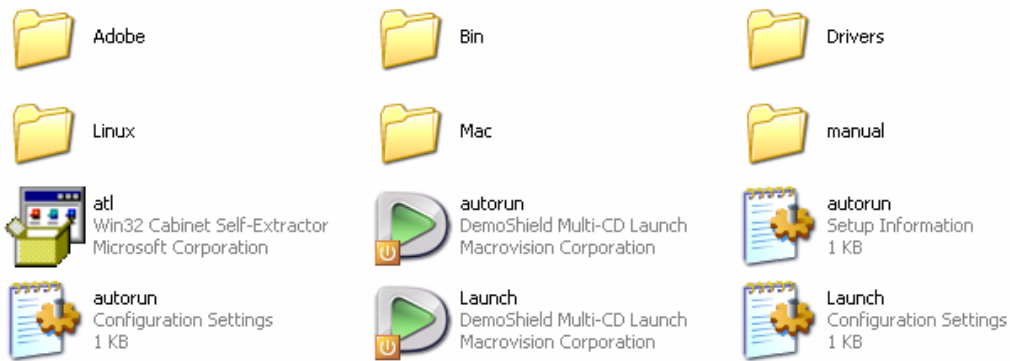


Install antenna to your Wireless LAN PCI Card as picture below.



## Software Installation

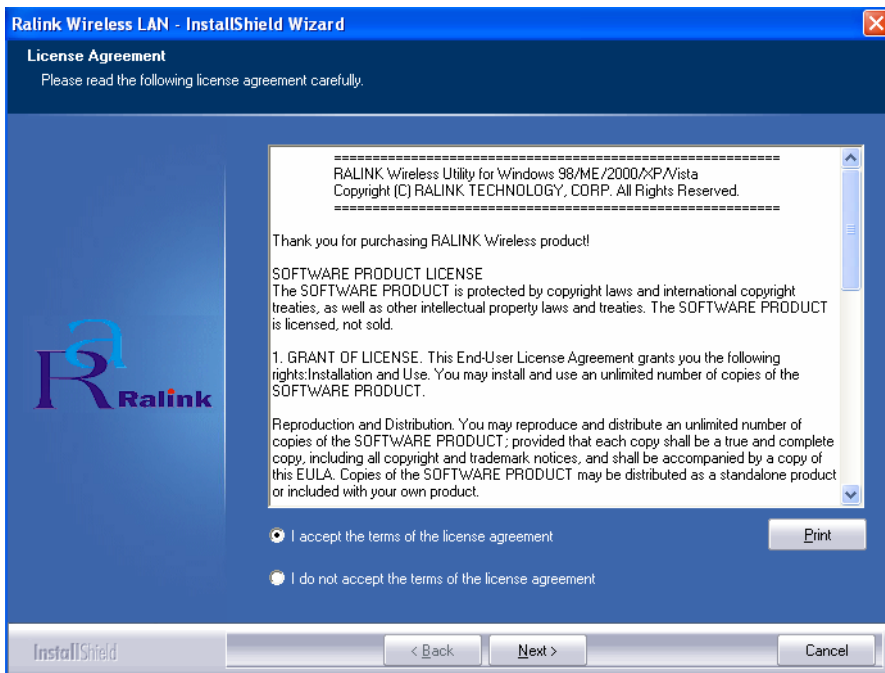
Click My Computer icon, then click DVD, then click autorun



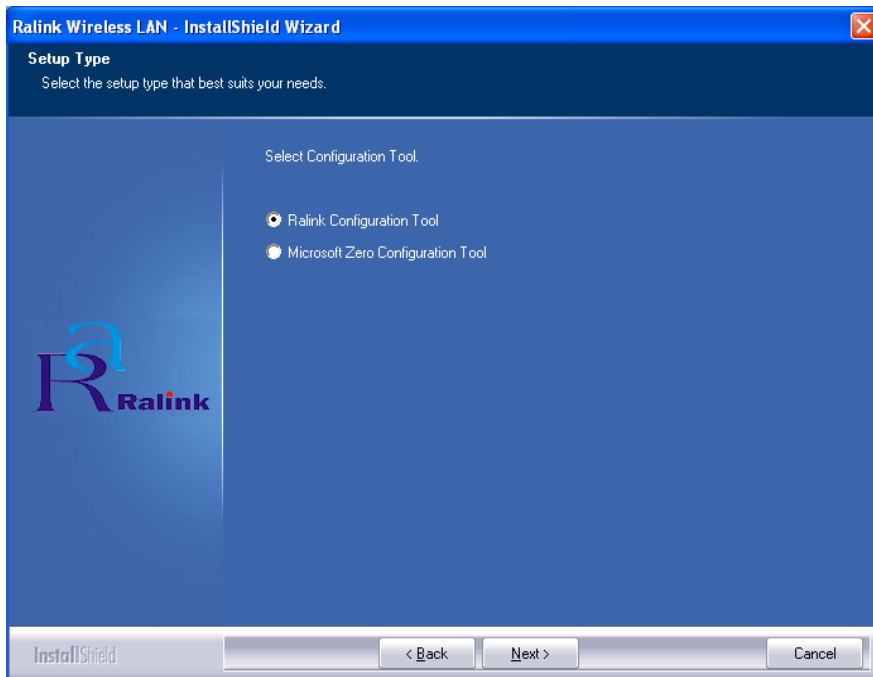
Click Driver Installation



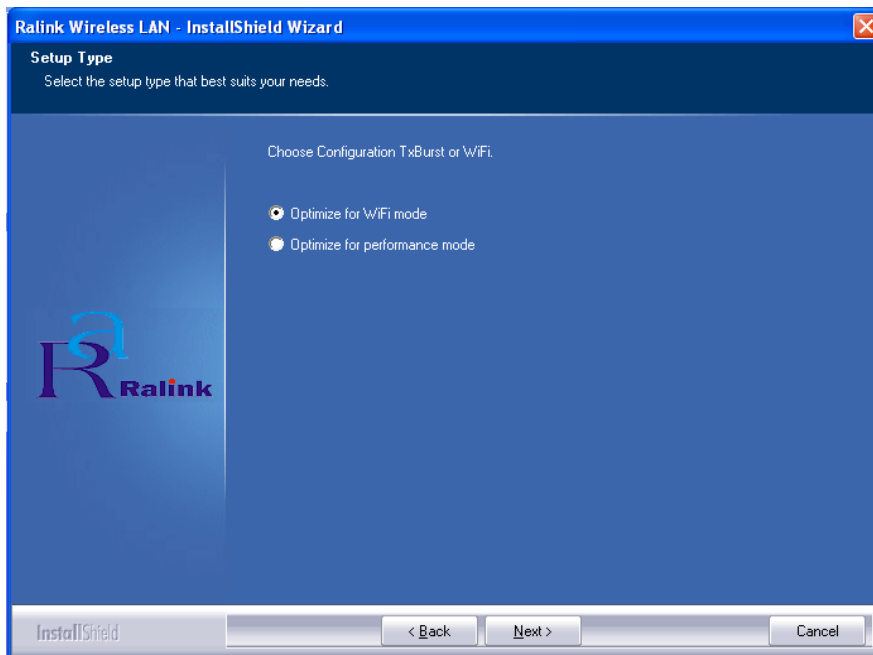
Click I accept the term of the license agreement ,then click Next icon.



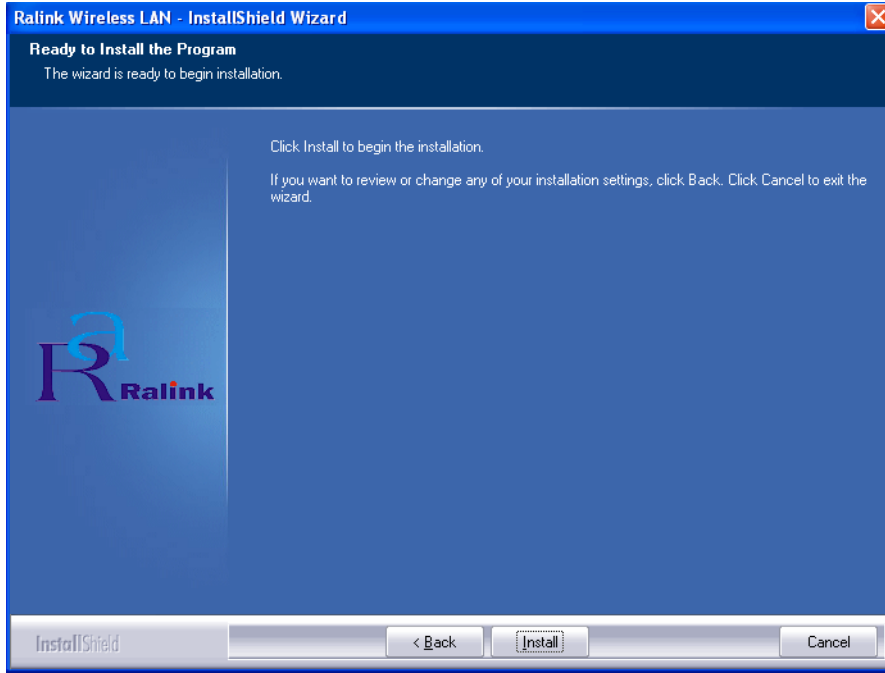
Click Ralink Configuration Tool, then click Next icon.



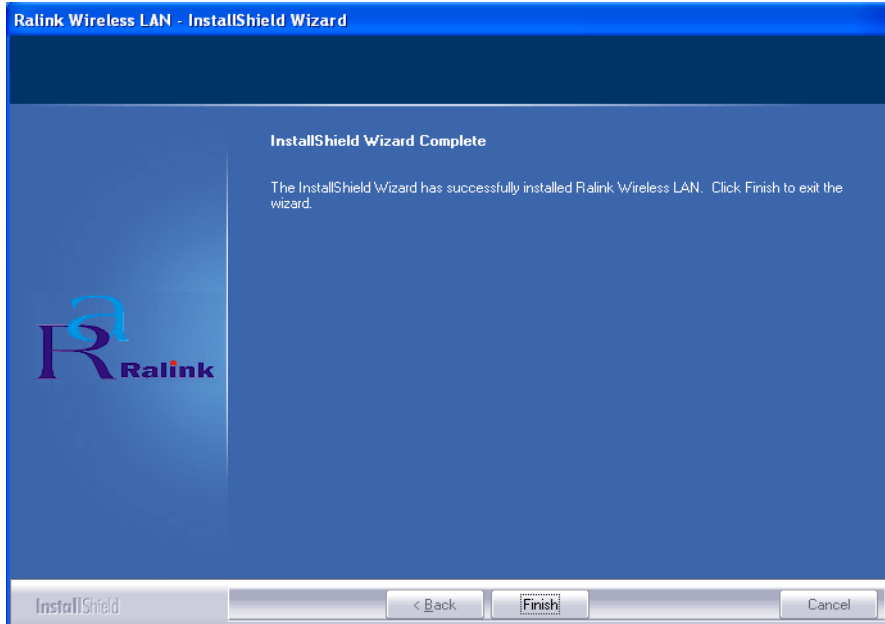
Click Optimize for WiFi modes, then click Next icon.



Click Install icon.



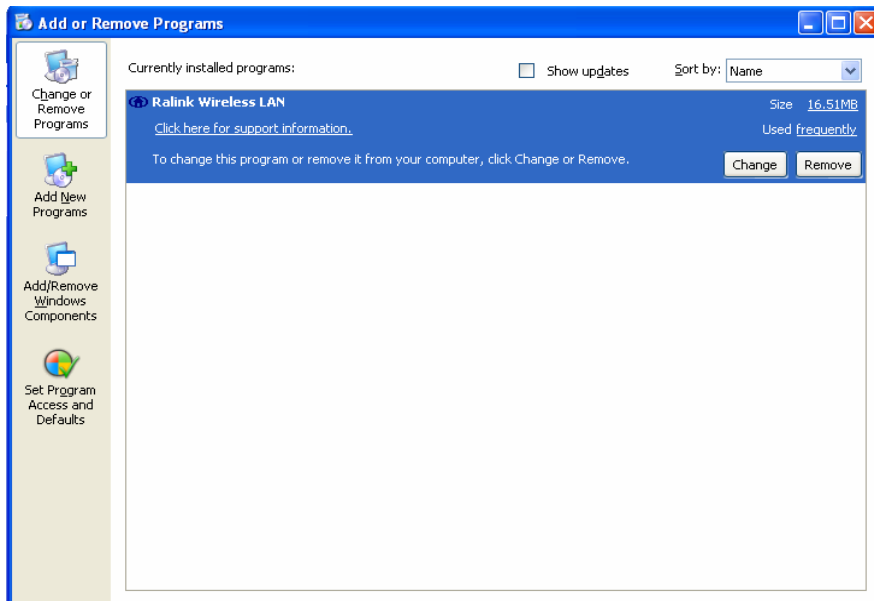
Click Finish icon.



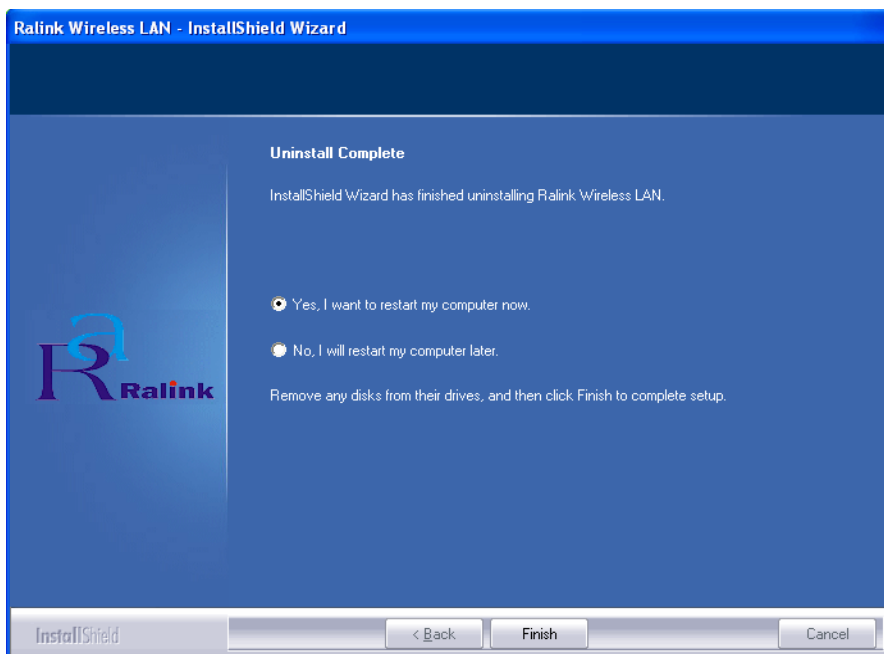


## Software Uninstall

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.

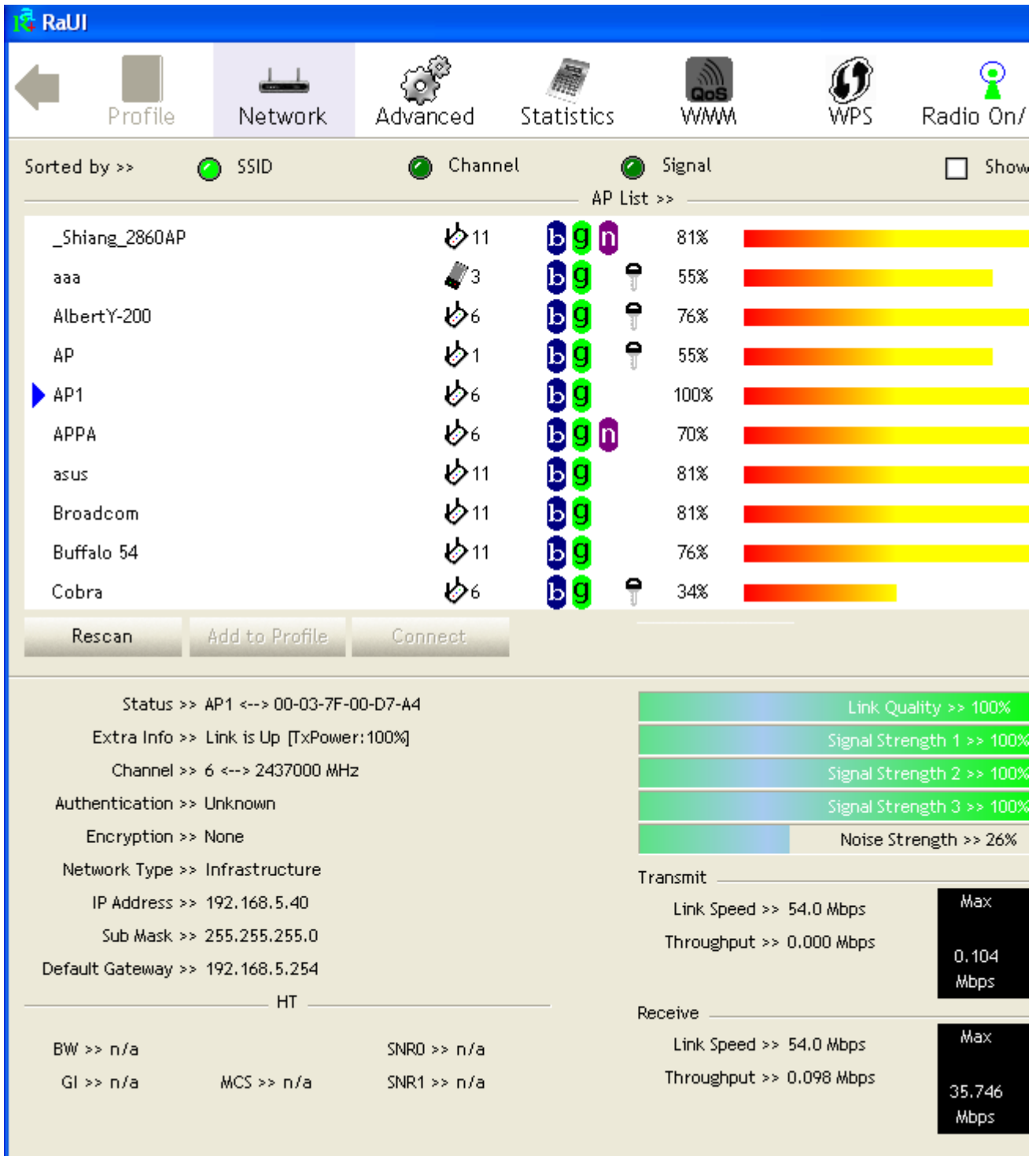


Figure 1-3 RaUI status with WZC active

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

- ① Profile button will be gray, profile function is removed since the NIC is controlled by WZC
- ② 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

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

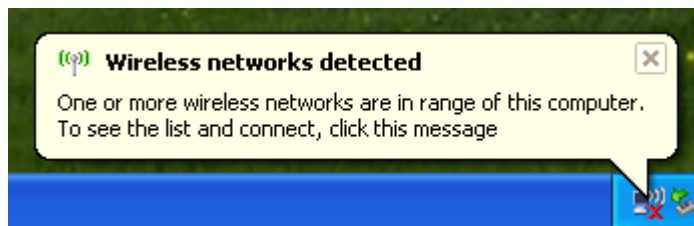


Figure 1-4 status prompt of no connection

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



Figure 1-5 Select WZC main status

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

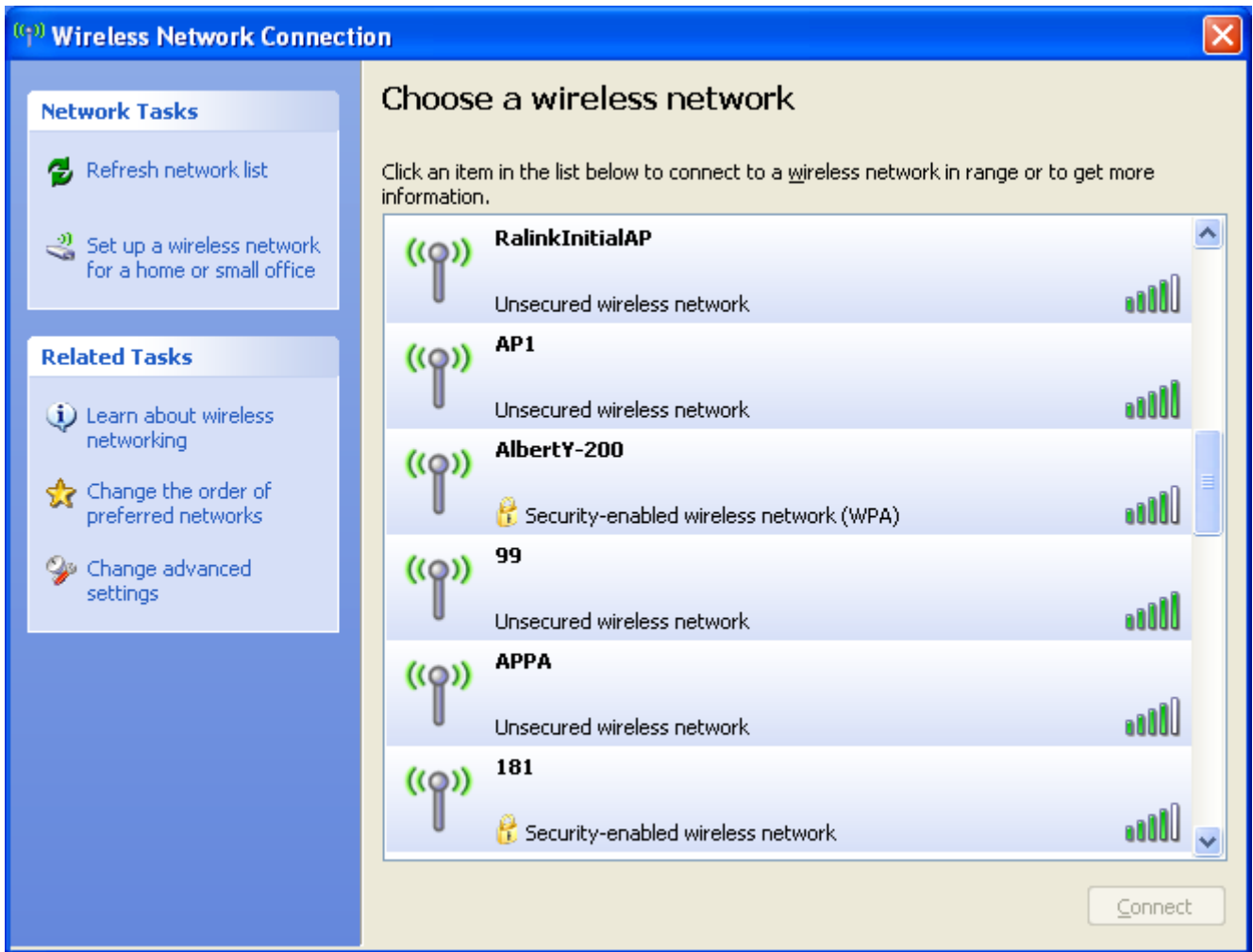


Figure 1-6 Wireless Network Connection

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

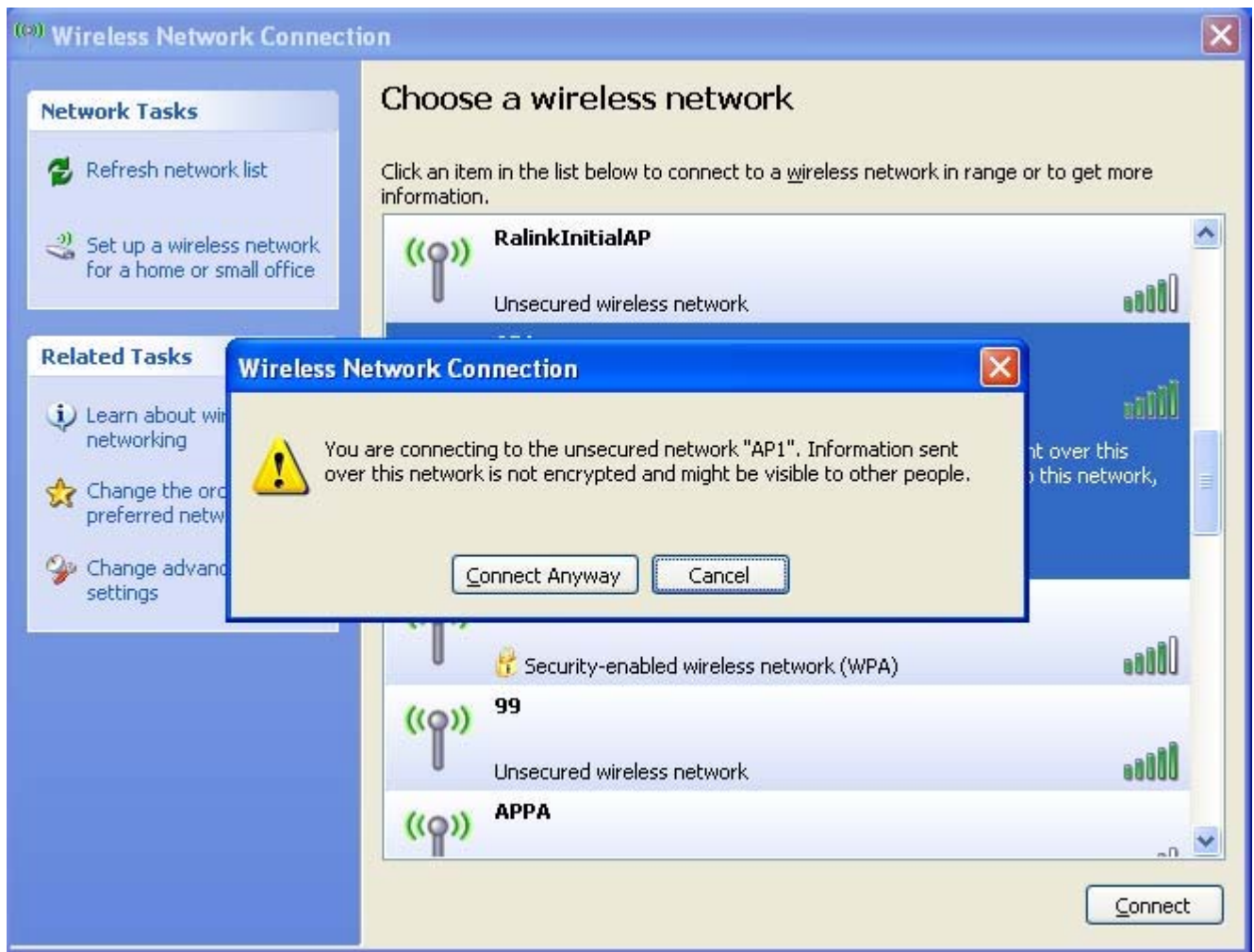


Figure 1-7 Select intended AP : AP1, then click "Connect"

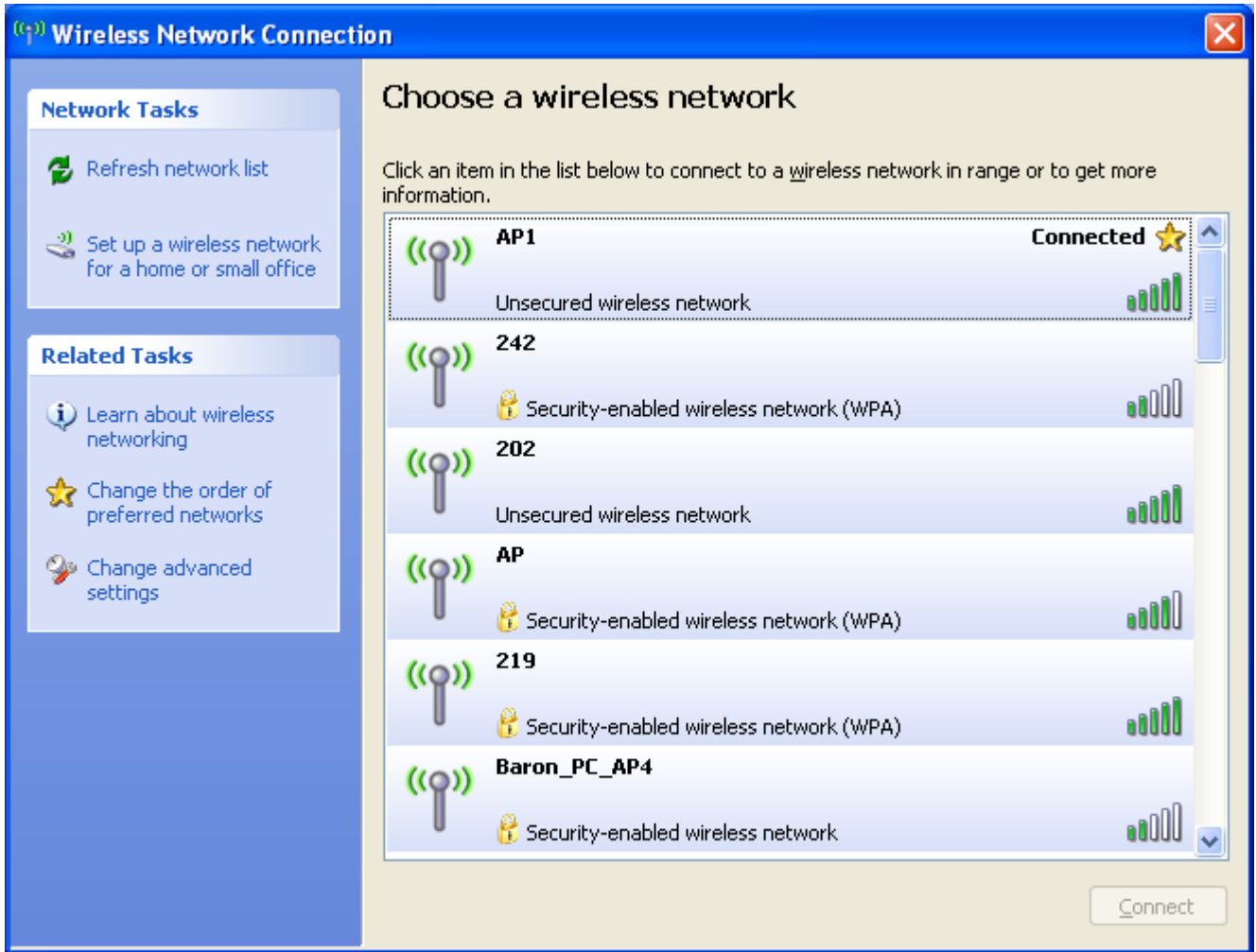


Figure 1-8 Connect AP : AP1 successfully

- 5 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.

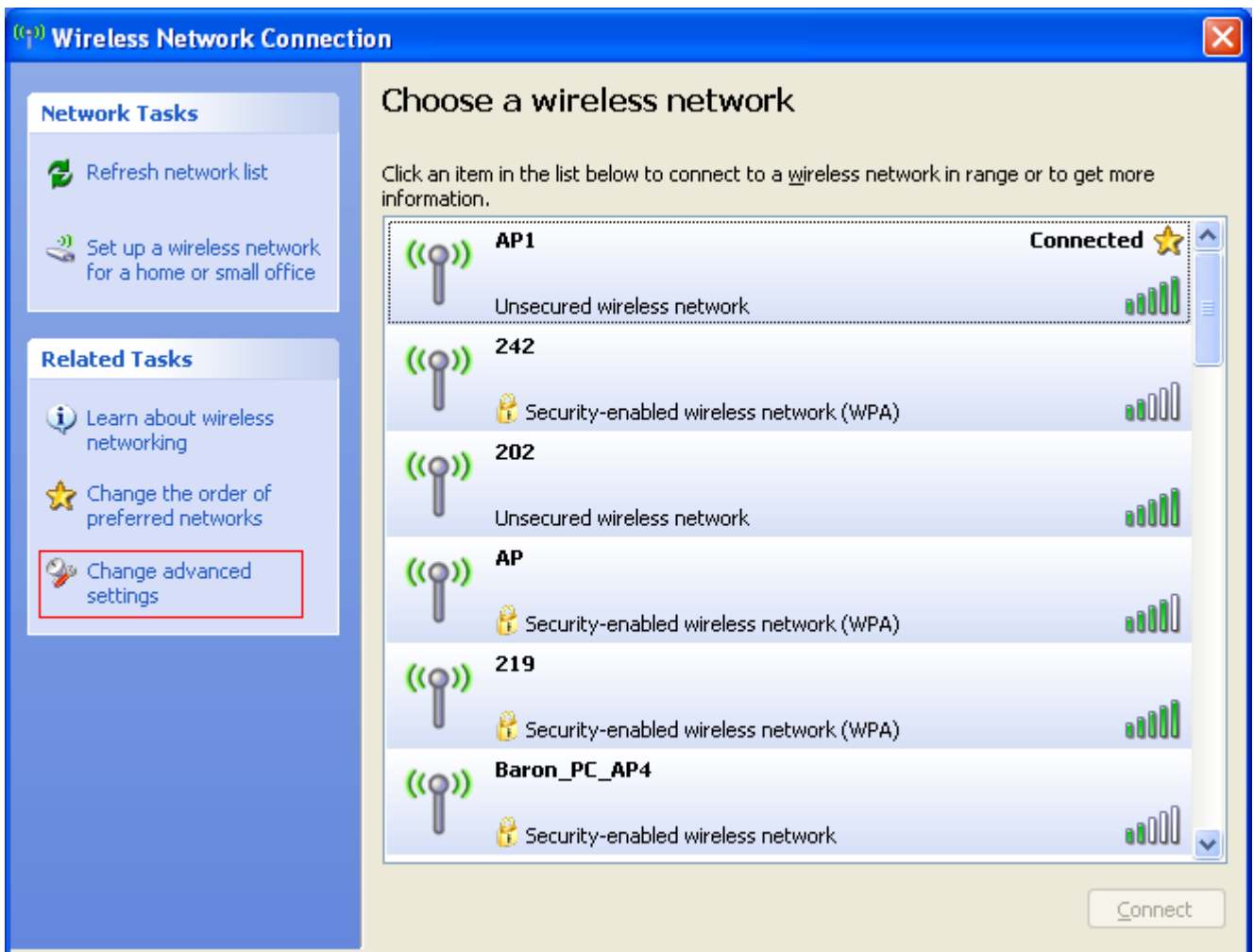


Figure 1-9 Click "Change advanced settings"

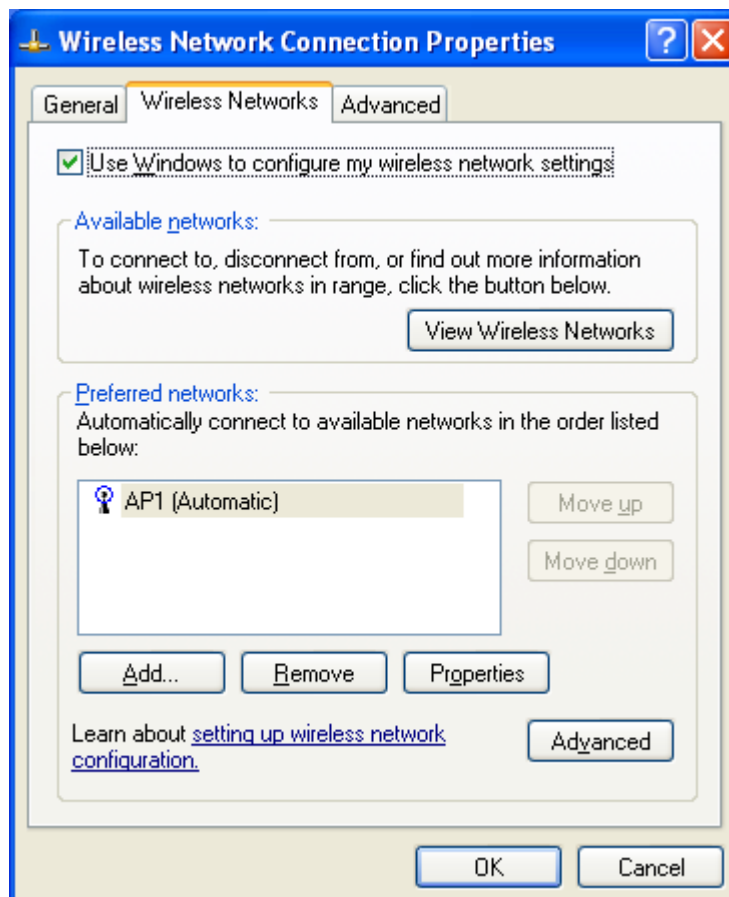


Figure 1-10 Choose "Wireless Networks" label



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

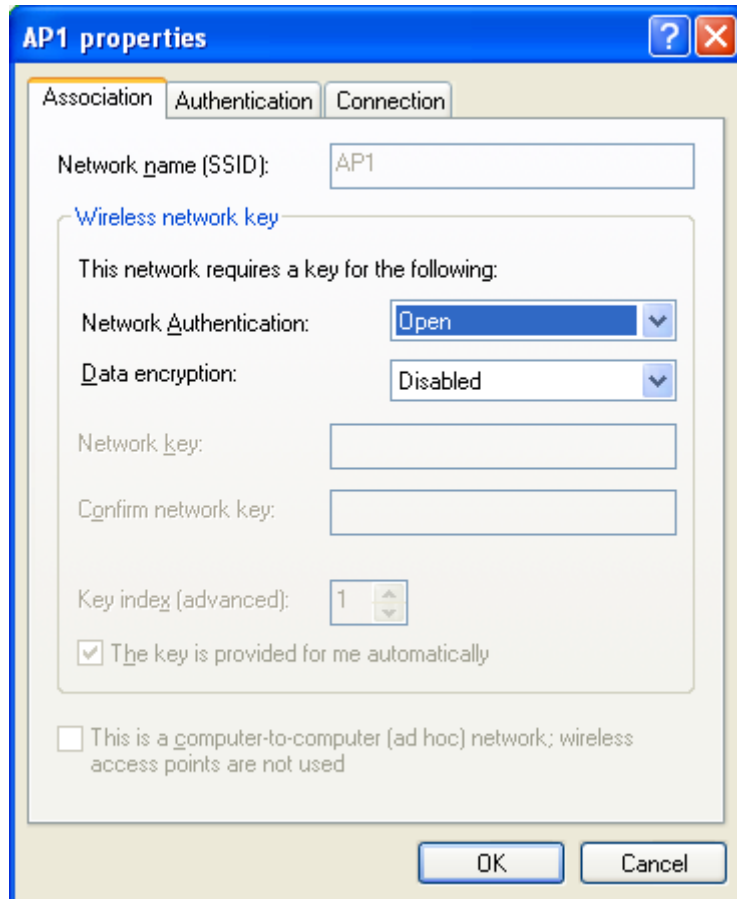


Figure 1-11 AP's properties

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

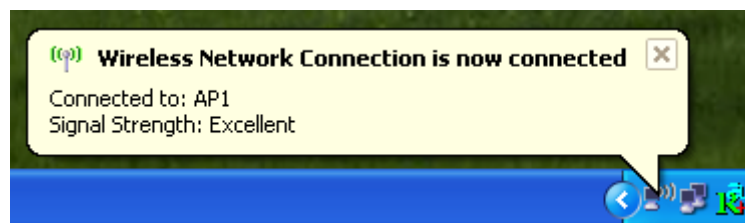


Figure 1-12 Network connection status

- 8 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.

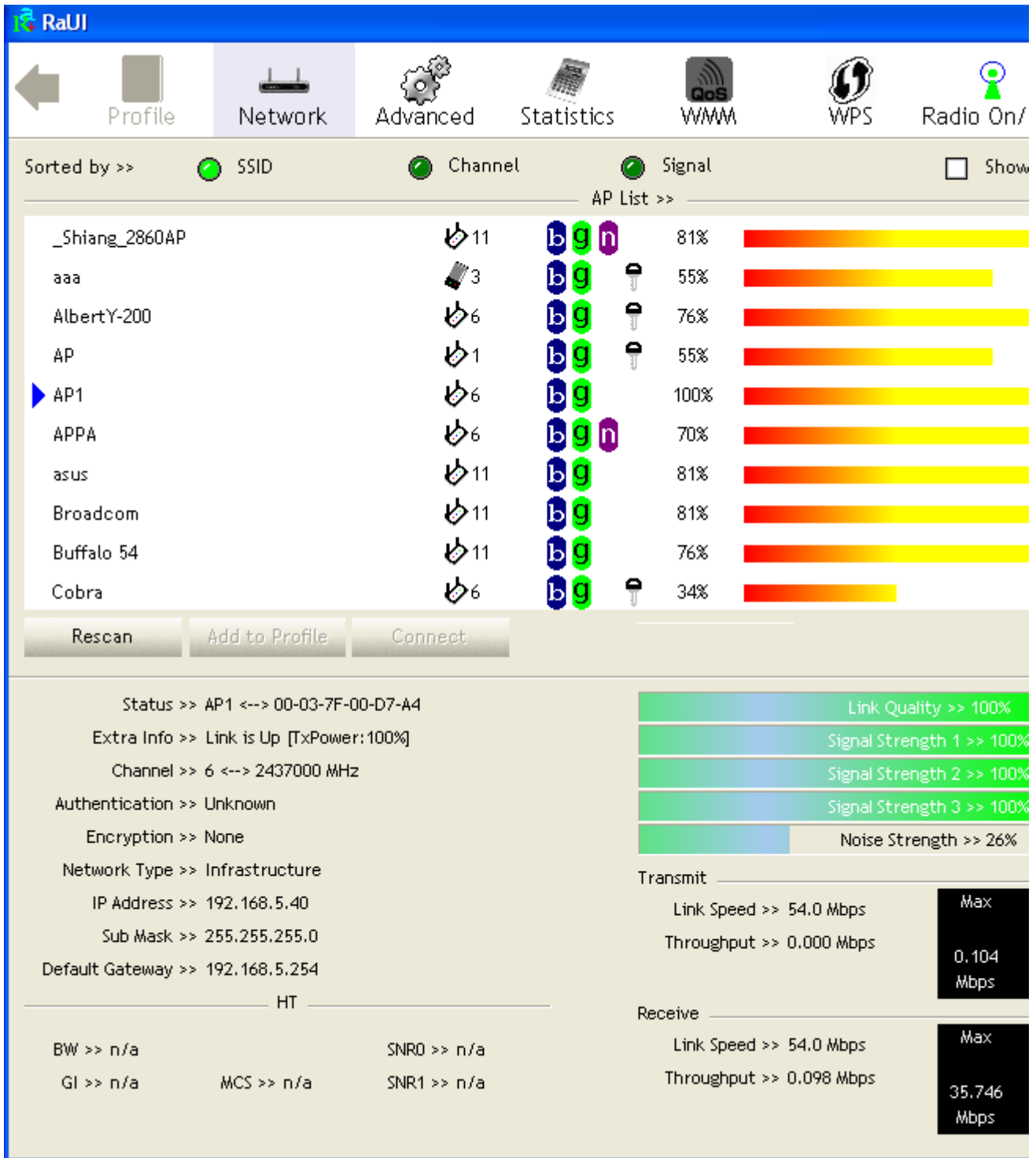


Figure 1-13 Show connection status by using WZC to do connection

## 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.

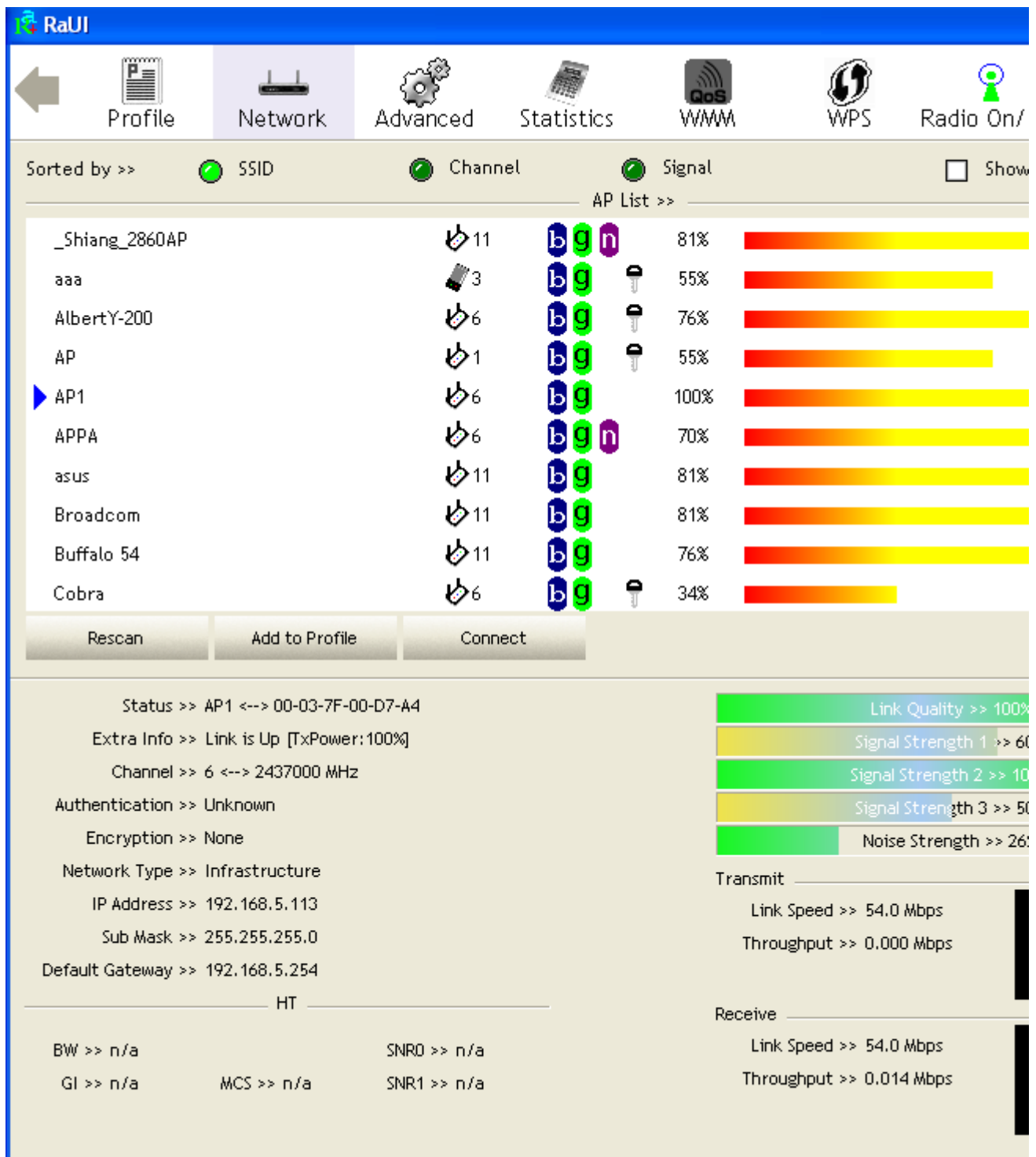


Figure 2-1-1 RaUI section introduction

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

1 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

2 Function Section : Corresponding button.

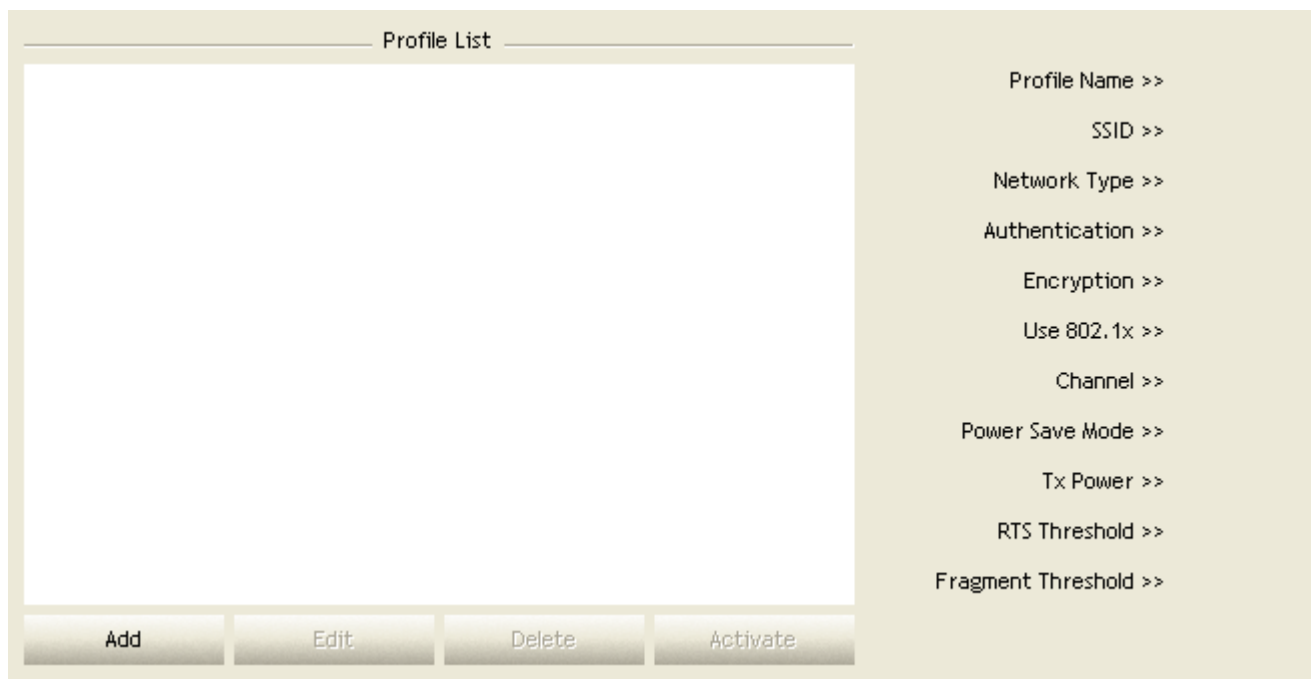


Figure 2-1-5 Profile page



Figure 2-1-6 Network page

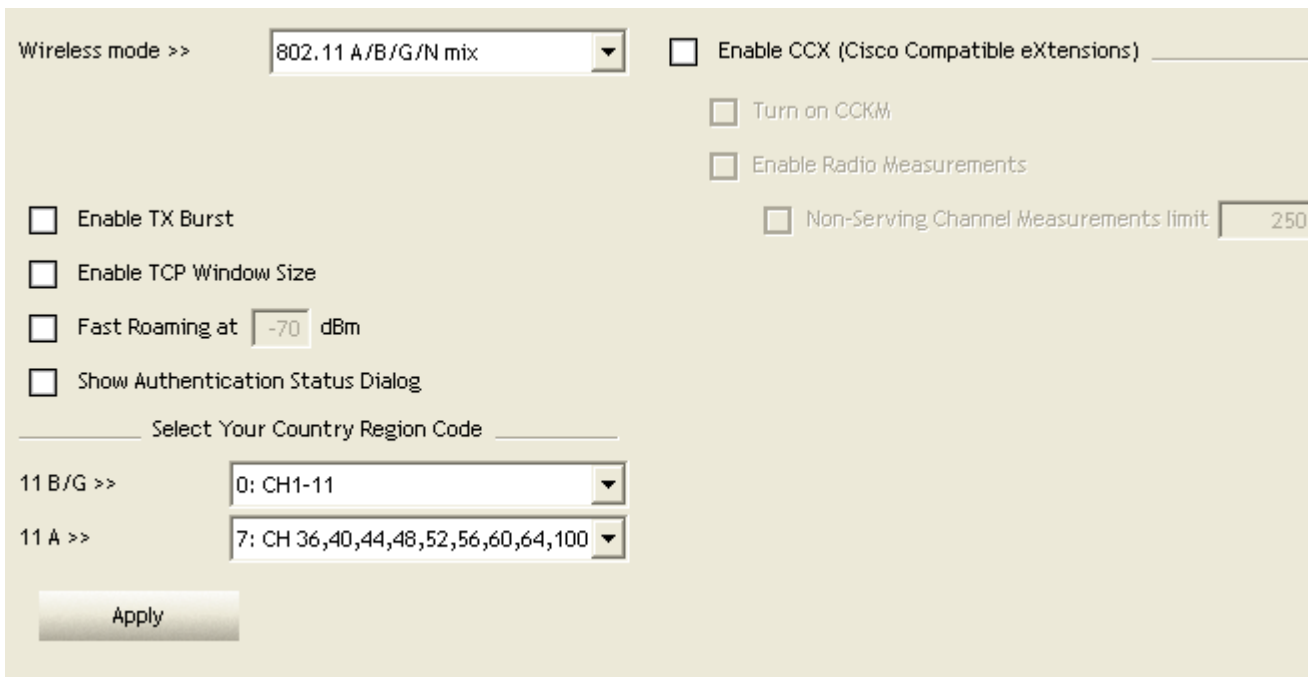


Figure 2-1-7 Advance page



Figure 2-1-8 Statistics page

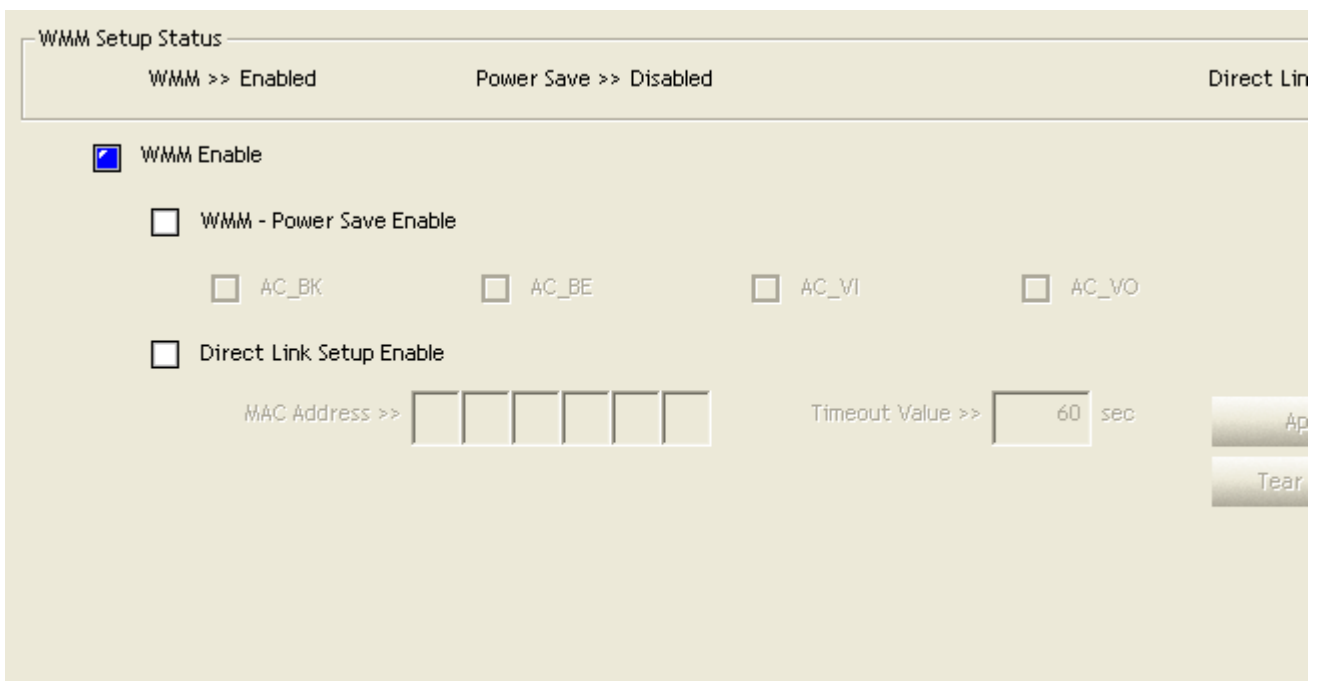


Figure 2-1-9 WMM page

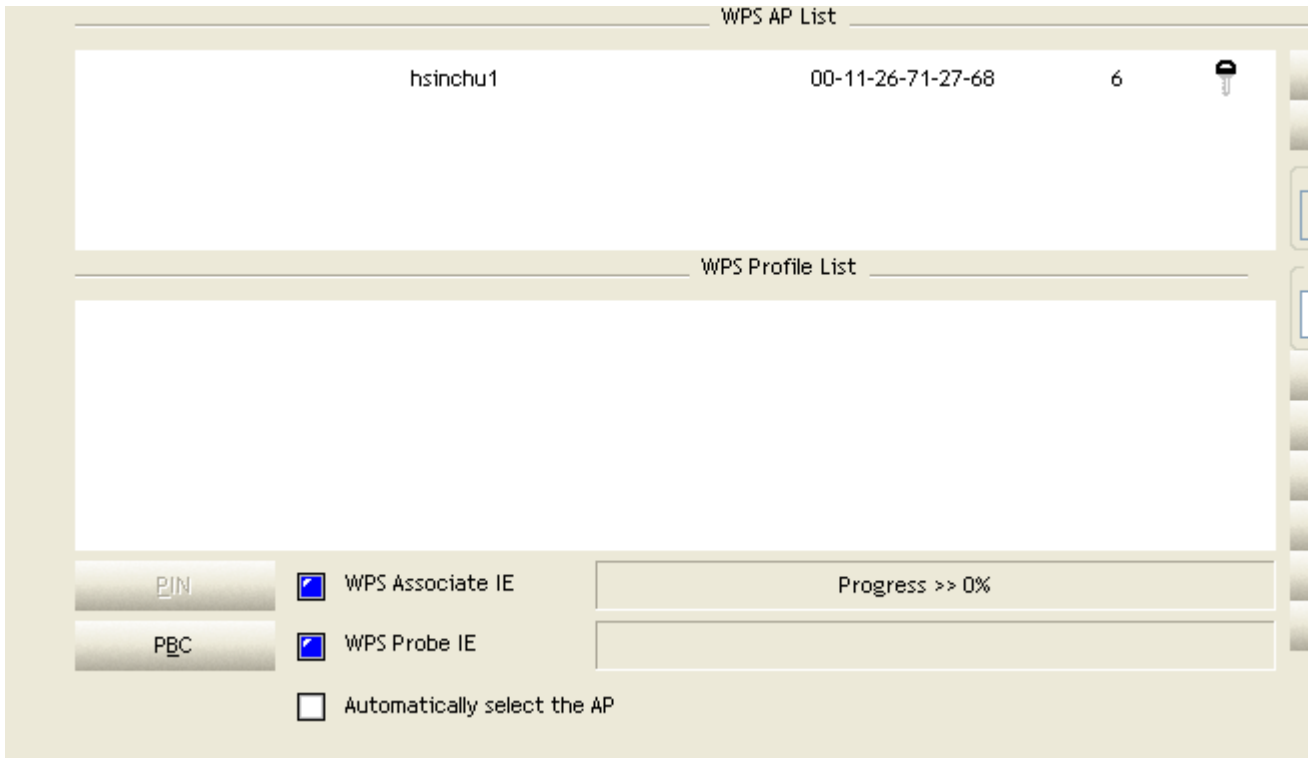


Figure 2-1-10 WPS page



Figure 2-1-11 About page

- ④ Status Section : Include Link Status, Authentication Status, AP's information, Configuration and retrying the connection when authentication is failed.

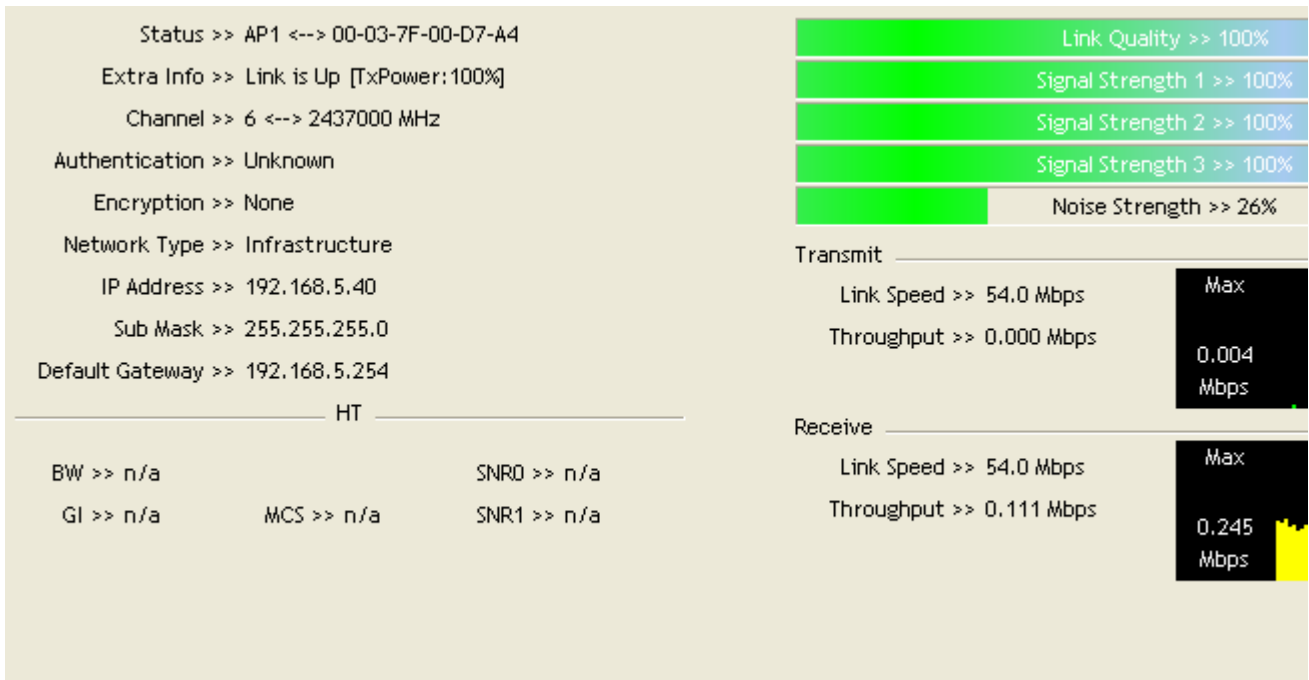


Figure 2-1-12 Link Status



Figure 2-1-13 Authentication Status

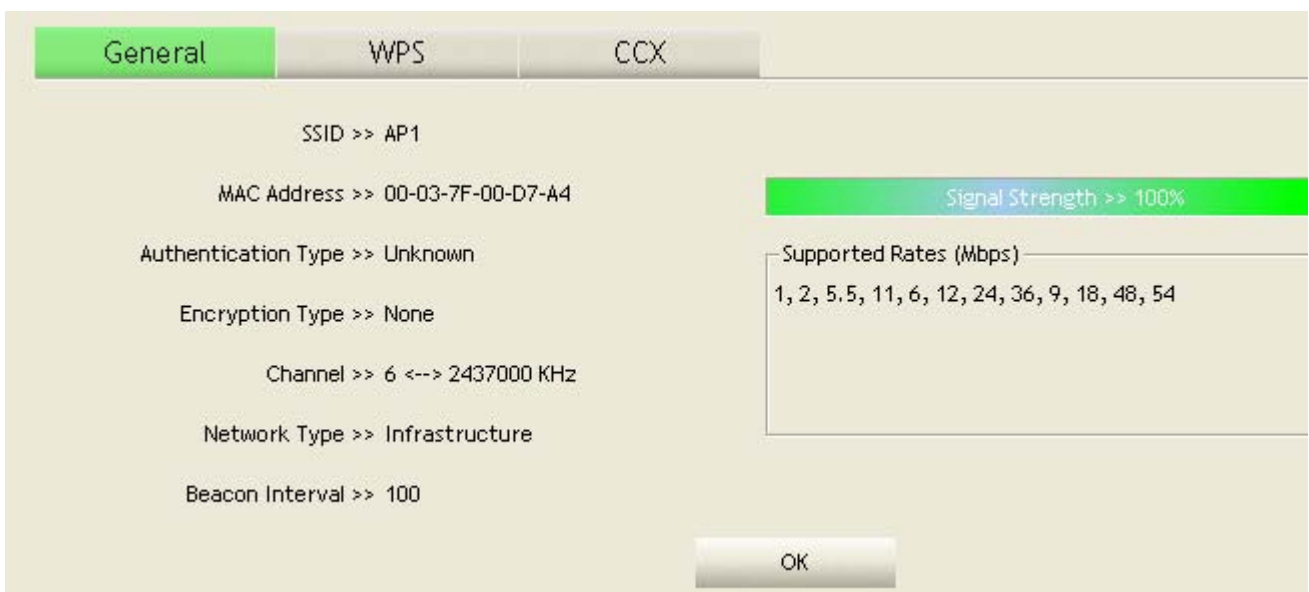


Figure 2-1-14 AP's Information





Figure 2-1-15 Retry the connection

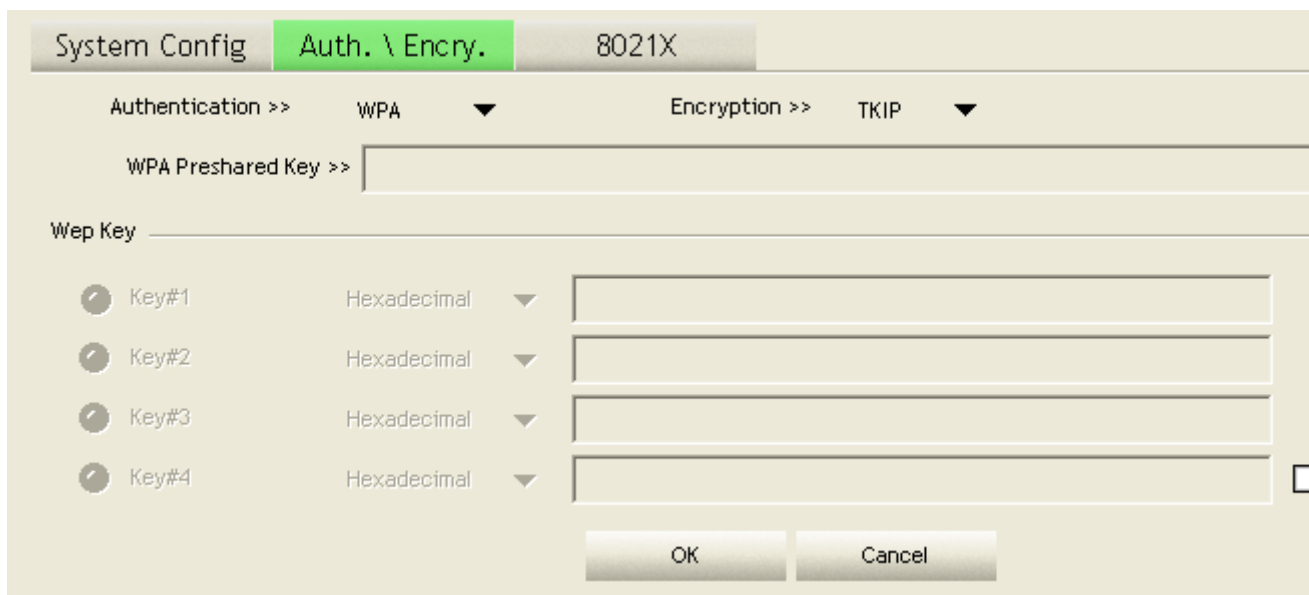







Figure 2-1-16 Configuration

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 eariler. 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.

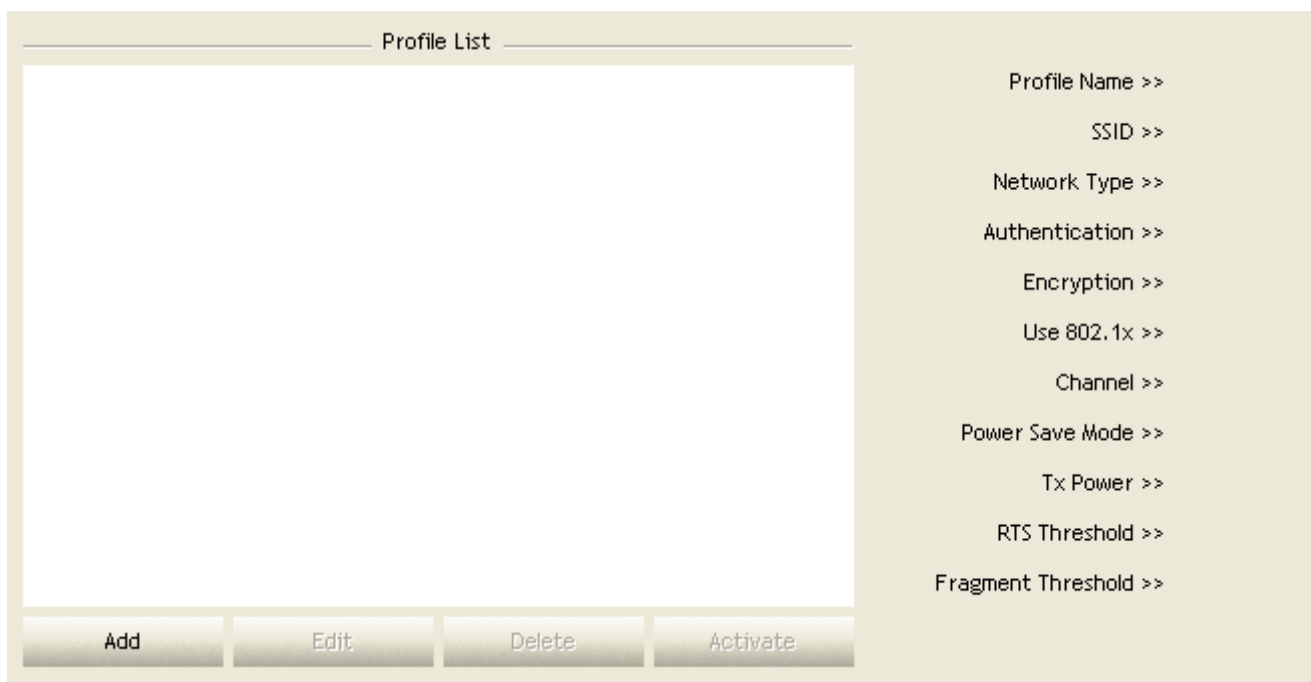


Figure 2-2-1 Profile function

Definition of each field :

- 1 Profile Name : Name of profile, preset to PROF\* (\* indicate 1, 2, 3...).
- 2 SSID : AP or Ad-hoc name.
- 3 Network Type : Network's type, including infrastructure and Ad-Hoc.
- 4 Authentication : Authentication mode.
- 5 Encryption : Encryption Type.
- 6 Use 802.1x : Whether or not use 802.1x feature.
- 7 Cannel : Channel in use for Ad-Hoc mode.
- 8 Power Save Mode : Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
- 9 Tx Power : Transmit power, the amount of power used by a radio transceiver to send the signal out.
- 10 RTS Threshold : User can adjust the RTS threshold number by sliding the bar or key in the value directly.
- 11 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.

- 1 You can open it from "Add to Profile" button in Site Survey function.
- 2 You can open it from "Add" button in Profile function.
- 3 You can open it from "Edit" button in Profile function.

The screenshot shows the 'System Config' tab of the Profile Editor. The 'Auth. \ Encry.' sub-tab is selected, and the profile type is '802.1X'. The 'Profile Name' field contains 'PROF1'. The 'SSID' field is a dropdown menu showing 'AP1'. Under 'Power Save Mode', both 'CAM' and 'PSM' radio buttons are selected. Below these are two checkboxes: 'RTS Threshold' and 'Fragment Threshold'. The 'RTS Threshold' is set to 0, and the 'Fragment Threshold' is set to 256. To the right, there are sliders for 'Tx Power' (set to 2347) and 'Preamble' (set to 2346). At the bottom are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Auth. \ Encry.' sub-tab of the Profile Editor. The 'Authentication' dropdown is set to 'Open' and the 'Encryption' dropdown is set to 'None'. There is an unchecked checkbox for '802.1X'. Below these is a text field for 'WPA Preshared Key'. A section titled 'Wep Key' contains four rows, each with a selected radio button, the label 'Key#1' through 'Key#4', a 'Hexadecimal' dropdown menu, and an empty text input field. At the bottom are 'OK' and 'Cancel' buttons.

Figure 2-2-2 Configuration

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

- ④ Network Type : There are two types, infrastructure and 802.11 Ad-hoc mode. Under Ad- hoc mode, user can also choose the preamble type, the available preamble type includes auto and long. In addition to that, the channel field will be available for setup in Ad-hoc mode.
- ⑤ RTS Threshold : User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
- ⑥ Fragment Threshold : User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.
- ⑦ Channel : Only available for setting under Ad-hoc mode. User can choose the channel frequency to start their Ad-hoc network.
- ⑧ Authentication Type : There are 7 type of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.
- ⑨ Encryption Type : For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
- ⑩ 802.1x Setting : This is introduced in the topic of "[Section 3-2 : 802.1x Setting](#)".
- ⑪ WPA Pre-shared Key : This is the 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.
- ⑫ 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

- 1 Click Add in Profile function.

The screenshot displays the RaUI web interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The 'Profile' tab is selected. Below the navigation bar, the 'Profile List' section is empty. To the right of the profile list, there are configuration options for a profile, including Profile Name, SSID, Network Type, Authentication, Encryption, Use 802.1x, Channel, Power Save Mode, Tx Power, RTS Threshold, and Fragment Threshold. At the bottom of the profile list, there are four buttons: Add, Edit, Delete, and Activate. The 'Add' button is highlighted with a red box. Below the profile list, there is a detailed view of a profile's status and configuration. The status shows 'AP1 <--> 00-03-7F-00-D7-A4' and 'Link is Up [TxPower:100%]'. The channel is '6 <--> 2437000 MHz'. The authentication is 'Unknown', encryption is 'None', and network type is 'Infrastructure'. The IP address is '192.168.5.60', sub mask is '255.255.255.0', and default gateway is '192.168.5.254'. The HT section shows BW, GI, SNRD, and SNR1 as 'n/a'. On the right side, there are performance metrics: Link Quality (100%), Signal Strength 1, 2, and 3, and Noise Strength. Below these are Transmit and Receive sections, each showing Link Speed (54.0 Mbps) and Throughput (0.000 Mbps and 0.025 Mbps respectively).

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

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

Link Quality >> 100%  
Signal Strength 1 >> 6  
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

2 Add Profile page will pop up.

The screenshot displays the RaUI interface for configuring a profile. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The main content area is titled 'Profile List' and contains a table with four columns: Add, Edit, Delete, and Activate. Below the table, there are three tabs: 'System Config' (highlighted in green), 'Auth. \ Encry.', and '8021X'. The 'System Config' tab is active, showing various configuration options. The 'Profile Name' field is set to 'PROF1'. The 'SSID' field is empty. The 'Network Type' is set to 'Infras'. The 'Tx Power' is set to 'A'. The 'Preamble' is set to 'A'. The 'Power Save Mode' section has two radio buttons: 'CAM' and 'PSM', both of which are checked. The 'RTS Threshold' is set to 0, and the 'Fragment Threshold' is set to 256. There are sliders and input boxes for these threshold values. At the bottom, there are 'OK' and 'Cancel' buttons.

3 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 shows the RaUI interface for configuring a profile. The top navigation bar includes Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The main area is titled 'Profile List' and contains a large empty box for the profile list. To the right of this box are configuration options: Profile Name >>, SSID >>, Network Type >>, Authentication >>, Encryption >>, Use 802.1x >>, Channel >>, Power Save Mode >>, Tx Power >>, RTS Threshold >>, and Fragment Threshold >>. Below the profile list are buttons for Add, Edit, Delete, and Activate.

Below the Profile List section, there are tabs for System Config, Auth. \ Encry., and 8021X. The 'Auth. \ Encry.' tab is active, showing configuration options for Profile Name >> (PROF1), Network Type >> (Infras), Tx Power >> (A), and Preamble >> (A). The SSID >> dropdown menu is open, displaying a list of APs with their corresponding MAC addresses. The 'AP-1' entry is selected.

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

On the left side of the configuration area, there are checkboxes for RTS Threshold and Fragment Threshold, both of which are currently unchecked.



- 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 web interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The 'Profile' tab is selected, showing a 'Profile List' table with one entry: PROF1 (AP1). Below the table are buttons for Add, Edit, Delete, and Activate. To the right of the table, the configuration details for the selected profile are shown:

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

Below the configuration details, there is a section for 'Status' and 'Extra Info':

- 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

On the right side, there are several performance metrics shown with green bars:

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

At the bottom, there are sections for 'Transmit' and 'Receive' statistics:

- Transmit:** Link Speed >> 54.0 Mbps, Throughput >> 0.000 Mbps
- Receive:** Link Speed >> 54.0 Mbps, Throughput >> 0.033 Mbps

At the very bottom, there are additional statistics:

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

## 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.

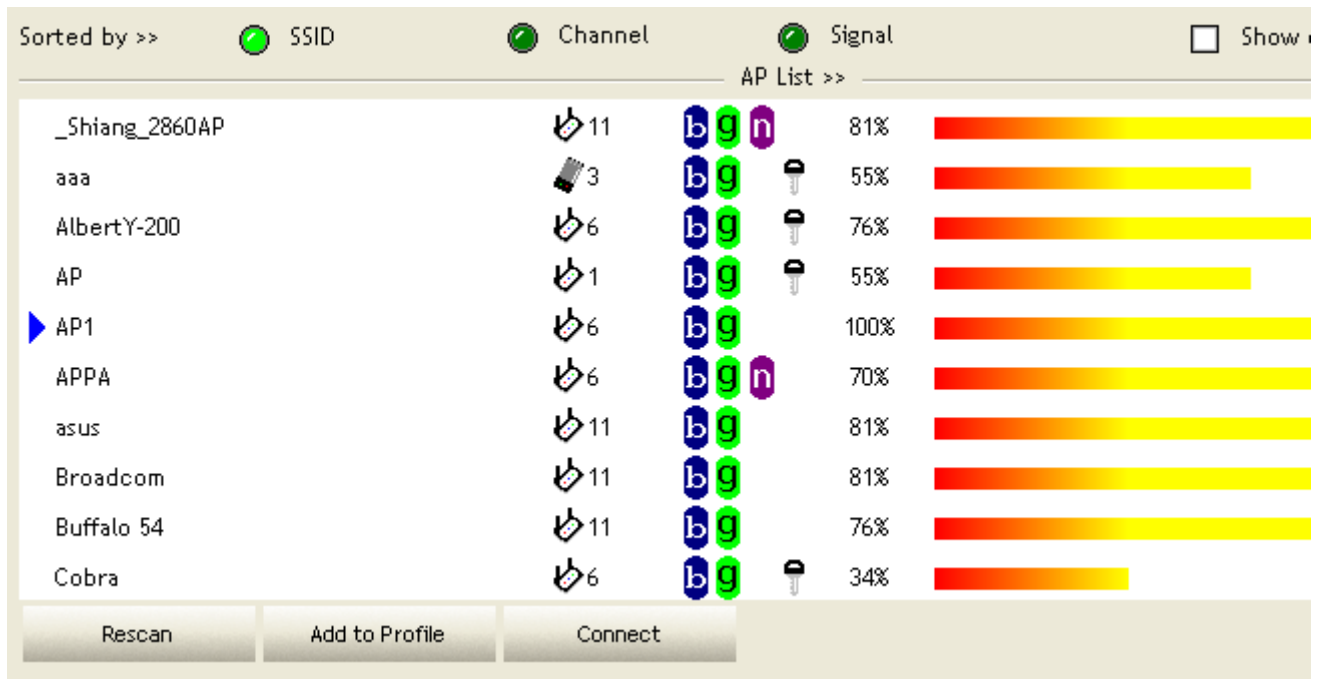


Figure 2-3-1-1 Network function

Definition of each field :

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



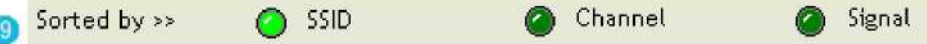
Indicate 802.11b wireless.



Indicate 802.11g wireless mode.



Indicate 802.11n wireless mode



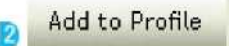
Indicate that AP list are sorted by SSID, Channel or Signal.



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 :

- ① When RaUI first ran, it will select the best AP to connect automatically.
- ② If user wants to connect to other AP. He can click "Connect" button for the intended AP to make connection.
- ③ 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 :

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.

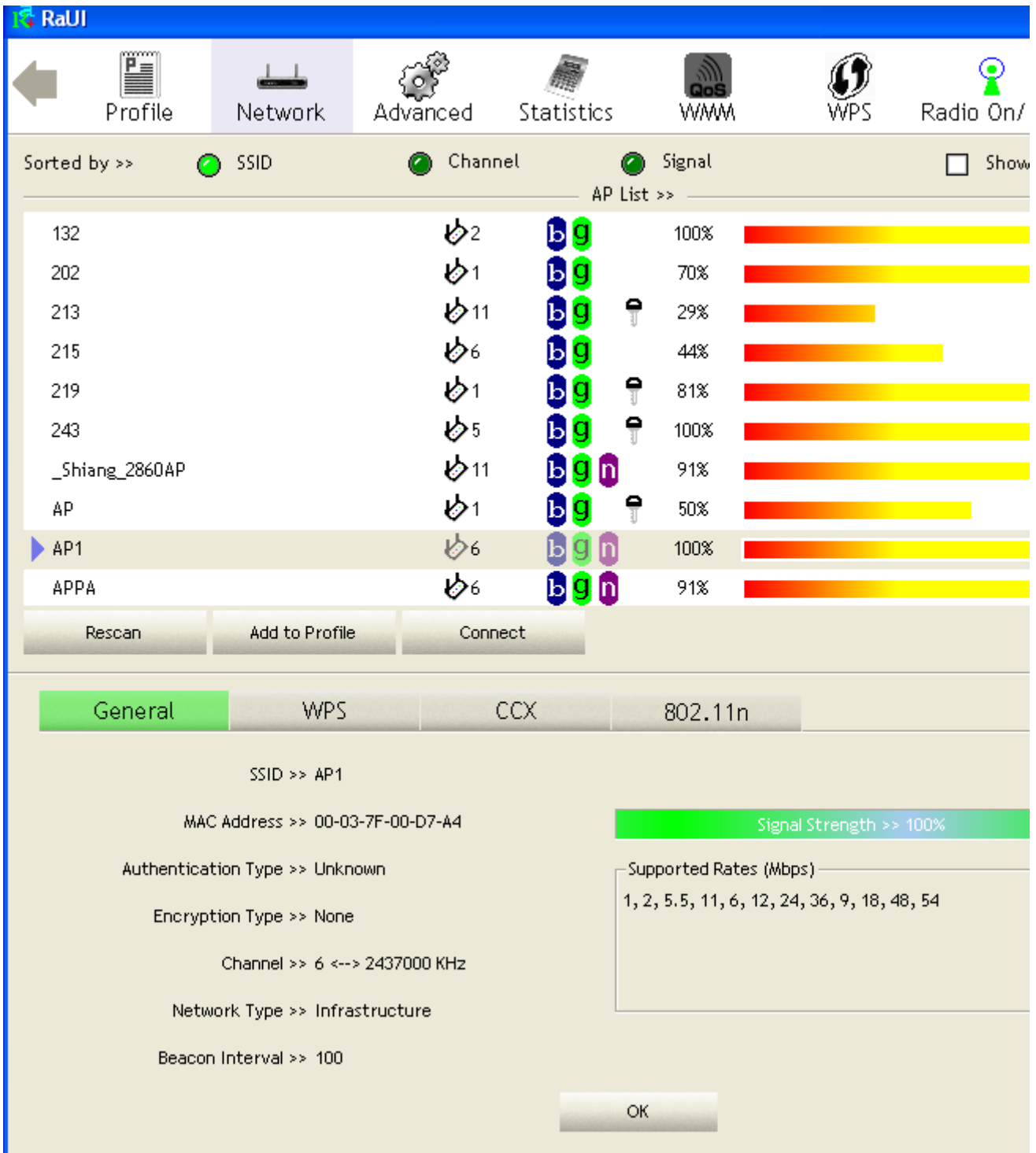


Figure 2-3-1-2 General informaion about AP's detal information

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 :

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

② Encryption Type : For open and shared authentication mode, the 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.

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

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

④ Device Password ID : 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

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

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

⑦ Version : WPS specified version.

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

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

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".

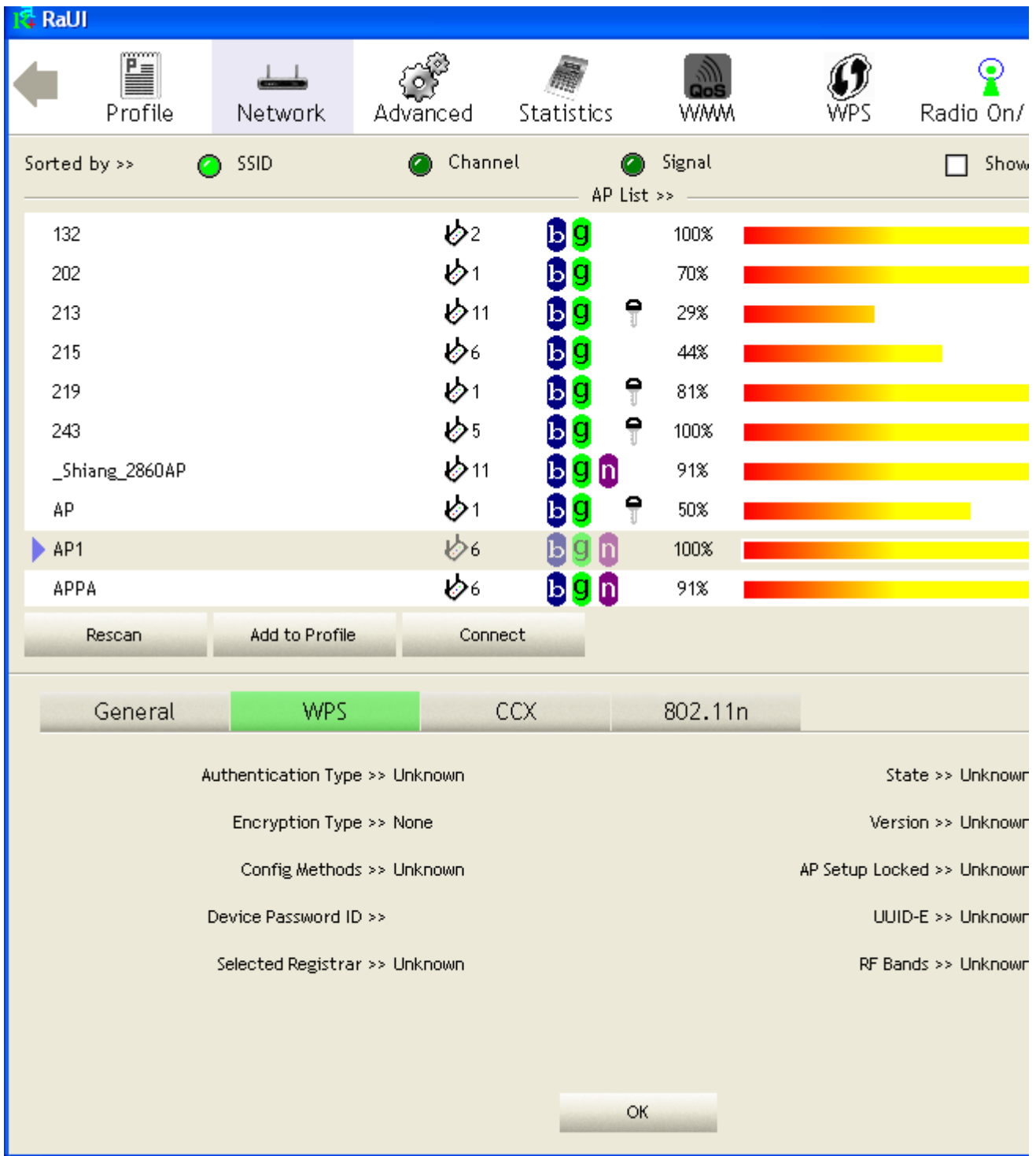


Figure 2-3-1-3 WPS information about AP's detail information

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

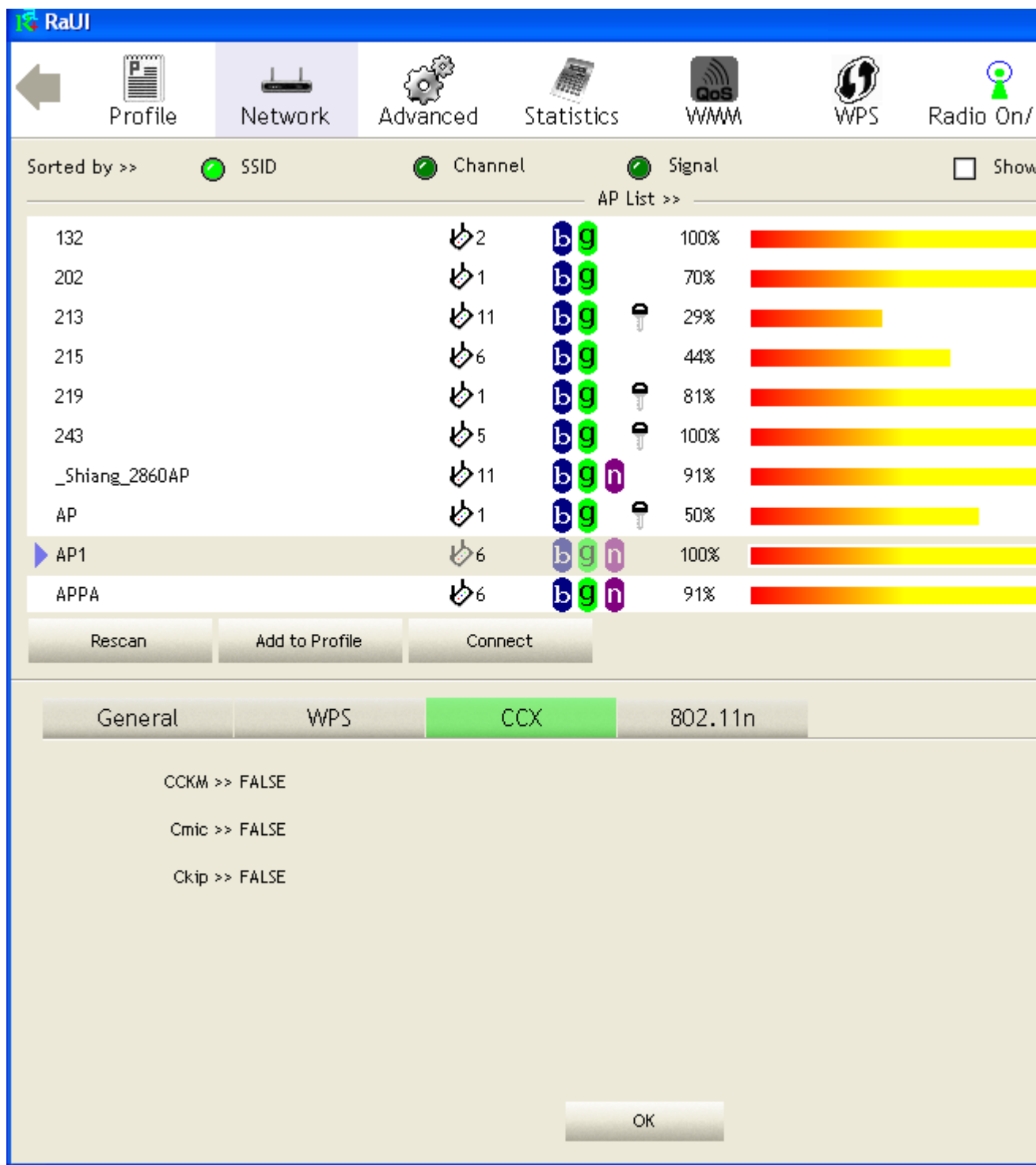


Figure 2-3-1-4 CCX information about AP's detail information



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

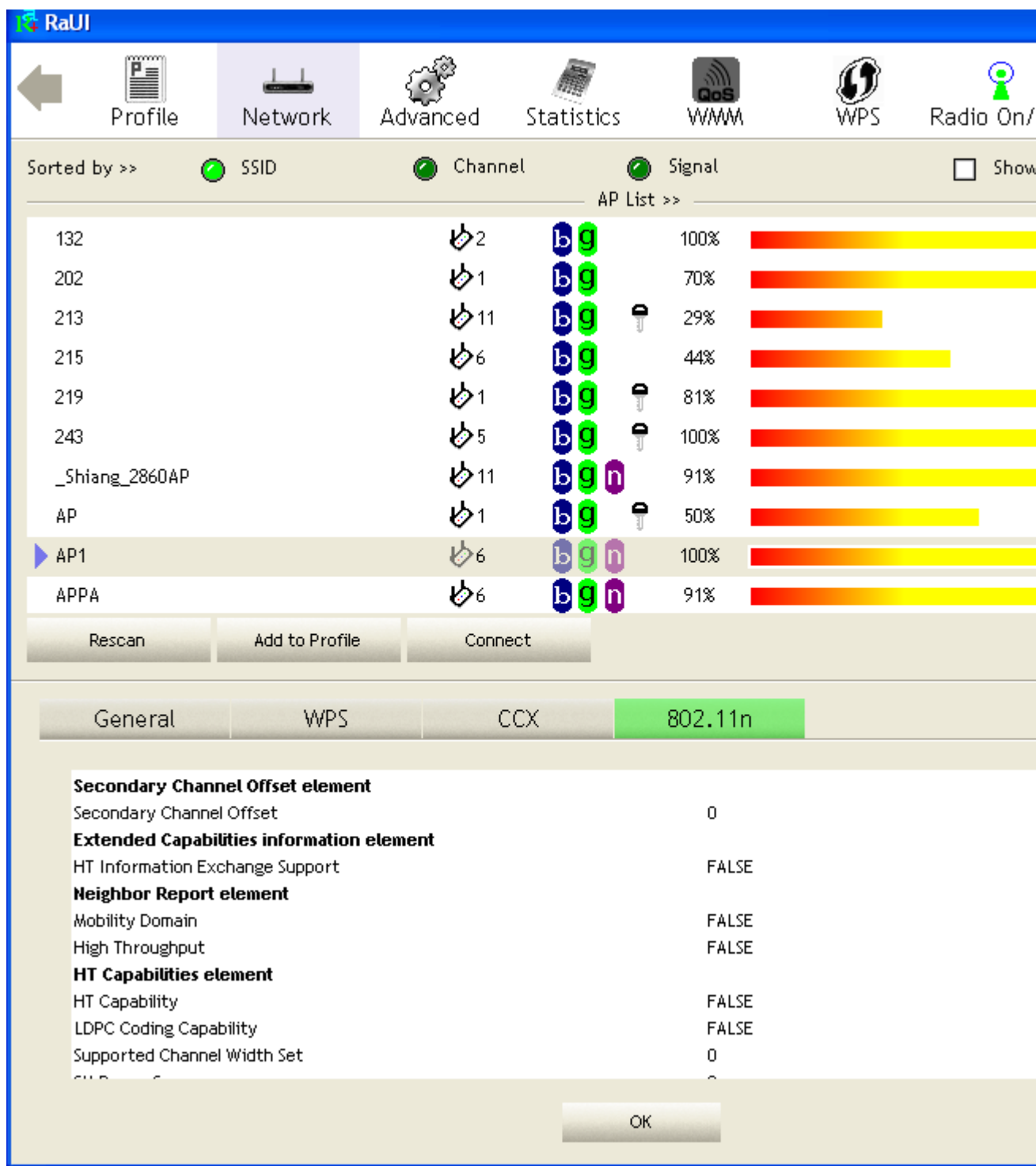


Figure 2-3-1-5 802.11n information

## Example on Adding Profile in Network

- 1 Select the intended network from AP list in Network function.

The screenshot shows the RaUI Network function interface. The 'Network' tab is active, and the 'AP List' is displayed. The 'AP1' entry is highlighted with a red box, indicating it is the selected network. Below the AP list, the status and configuration details for the selected AP are shown.

AP Name	Channel	Signal	Link Quality
AlbertY-200	6	60%	100%
AP	1	70%	100%
<b>AP1</b>	<b>6</b>	<b>100%</b>	<b>100%</b>
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%

**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

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Receive

Link Speed >> 48.0 Mbps

Throughput >> 0.104 Mbps

2 Click "Add to Profile".

The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by Signal strength. The 'AP1' entry is highlighted, and the 'Add to Profile' button is circled in red. Below the list, the status and configuration details for AP1 are displayed.

AP Name	Channel	Signal	Percentage
AlbertY-200	6	bg	60%
AP	1	bg	70%
<b>AP1</b>	<b>6</b>	<b>bg</b>	<b>100%</b>
Broadcom	11	bg	70%
BroadcomWPS	1	bg	100%
DennisAP	6	bg n	76%
Fiona-Ap	11	bg n	44%
ISSI-3F-asus11b	3	b	20%
knilar	8	bg	60%
NB27-PC_Network	6	bg n	81%

**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

**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

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

The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by SSID, Channel, and Signal. The System Config dialog is open, showing configuration for profile 'PROF1' with SSID 'AP1'. The dialog includes options for Power Save Mode (CAM and PSM), RTS Threshold, and Fragment Threshold.

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

**System Config Dialog:**

- Profile Name: PROF1
- SSID: AP1
- Network Type: Infrast...
- Tx Power: A
- Preamble: A
- Power Save Mode:  CAM,  PSM
- RTS Threshold: 0 (range 0-2347)
- Fragment Threshold: 256 (range 256-2346)

4 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 web interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The 'Profile' tab is selected. Below the navigation bar, the 'Profile List' section shows a table with one entry: 'PROF1' with 'AP1' as the SSID and an 'Activate' button. To the right of the table, the configuration details for 'PROF1' are listed, including Profile Name, SSID, Network Type, Authentication, Encryption, Use 802.1x, Channel, Power Save Mode, Tx Power, RTS Threshold, and Fragment Threshold. Below the profile list, there are buttons for 'Add', 'Edit', 'Delete', and 'Activate'. The bottom section of the interface shows the status and extra information for the selected profile, including the MAC address, link status, channel, authentication, encryption, network type, IP address, sub mask, and default gateway. On the right side, there are performance metrics for Link Quality, Signal Strength, and Noise Strength, along with Transmit and Receive statistics for Link Speed and Throughput.

Profile Name	SSID	Activate
PROF1	AP1	[Activate]

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

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

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 >> 0.092 Mbps

## Advanced

Figure 2-4 shows Advance function of RaUI.

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

Enable CCX (Cisco Compatible eXtensions)

Turn on CCKM

Enable Radio Measurements

Enable TX Burst

Non-Serving Channel Measurements limit 250

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 2-4 Advance function

- ① 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)
- ② Wireless Protection : User can choose from Auto, On, and Off. (only 802.11n adapter don't support.)
  - ① Auto : STA will dynamically change as AP announcement.
  - ② On : Always send frame with protection.
  - ③ Off : Always send frame without protection.
- ③ TX Rate : Manually force the Transmit using selected rate. Default is auto. (802.11n wireless card don't support TX Rate now)
- ④ Enable TX Burst : Ralink's proprietary frame burst mode.
- ⑤ Enable TCP Window Size : Enhance throughput.
- ⑥ Fast Roaming at : fast to roaming, setup by transmit power.
- ⑦ Select Your Country Region Code : eight countries to choose. Country channel list : Country channel list. (11A ListBox only shows for A/B/G adapter.)
- ⑧ 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.
- ⑨ Enable CCX (Cisco Compatible eXtensions) : support Cisco Compatible Extensions function.
  - ① LEAP turn on CCKM.
  - ② Enable Radio Measurement : can channel measurement every 0~2000 milliseconds.
- ⑩ 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 :



① Frames Transmitted Successfully : Frames successfully sent.

② Frames Fail To Receive ACK After All Retries : Frames failed transmit after hitting retry limit.

- ③ RTS Frames Successfully Receive CTS : Successfully receive CTS after sending RTS frame.
- ④ RTS Frames Fail To Receive CTS : Failed to receive CTS after sending RTS.
- ⑤ Frames Retransmitted Successfully : Successfully retransmitted frames numbers.
- ⑥ Reset counters to zero.

Receive Statistics :



- ① Frames Received Successfully : Frames received successfully.
- ② Frames Received With CRC Error : Frames received with CRC error.
- ③ Frames Dropped Due To Out-of-Resource : Frames dropped due to resource issue.
- ④ Duplicate Frames Received : Duplicate received frames. ⑤

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 :

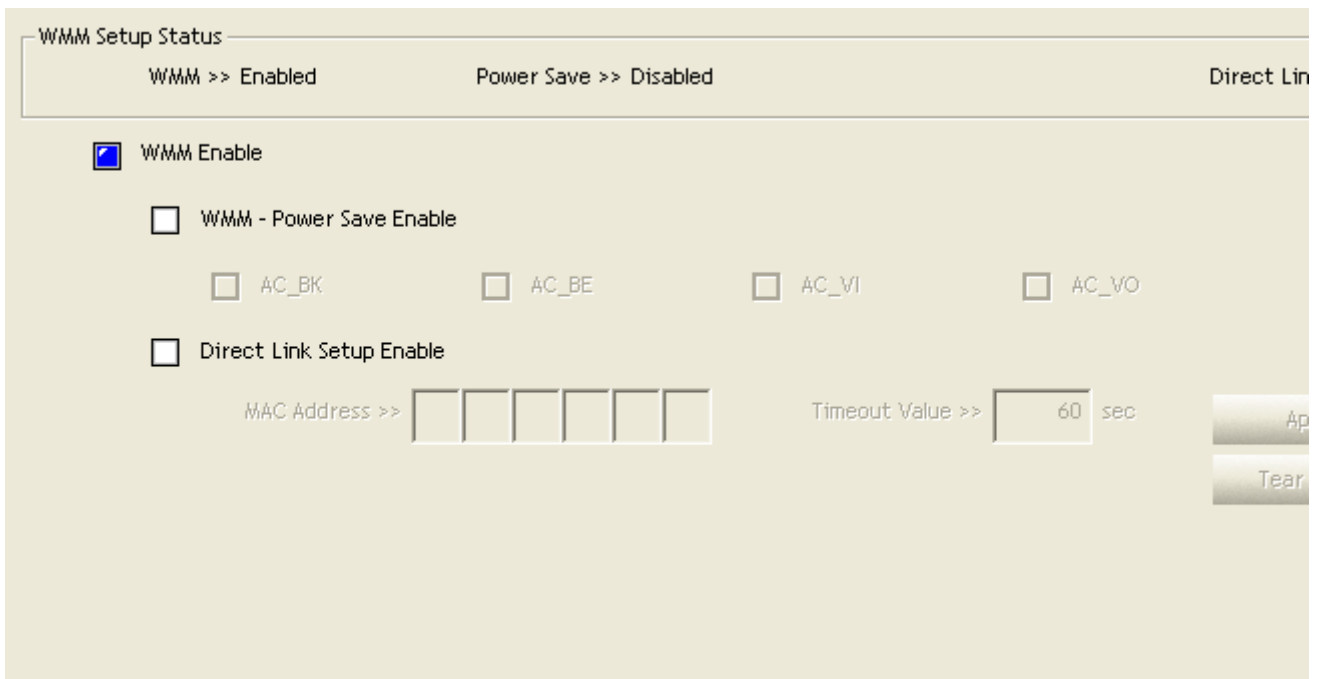


Figure 2-6-1 WMM function

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

Icons and buttons:



Show the information of Status Section.



Hide the information of Status Section.

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

- 1 Click "Direct Link Setup Enable"

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

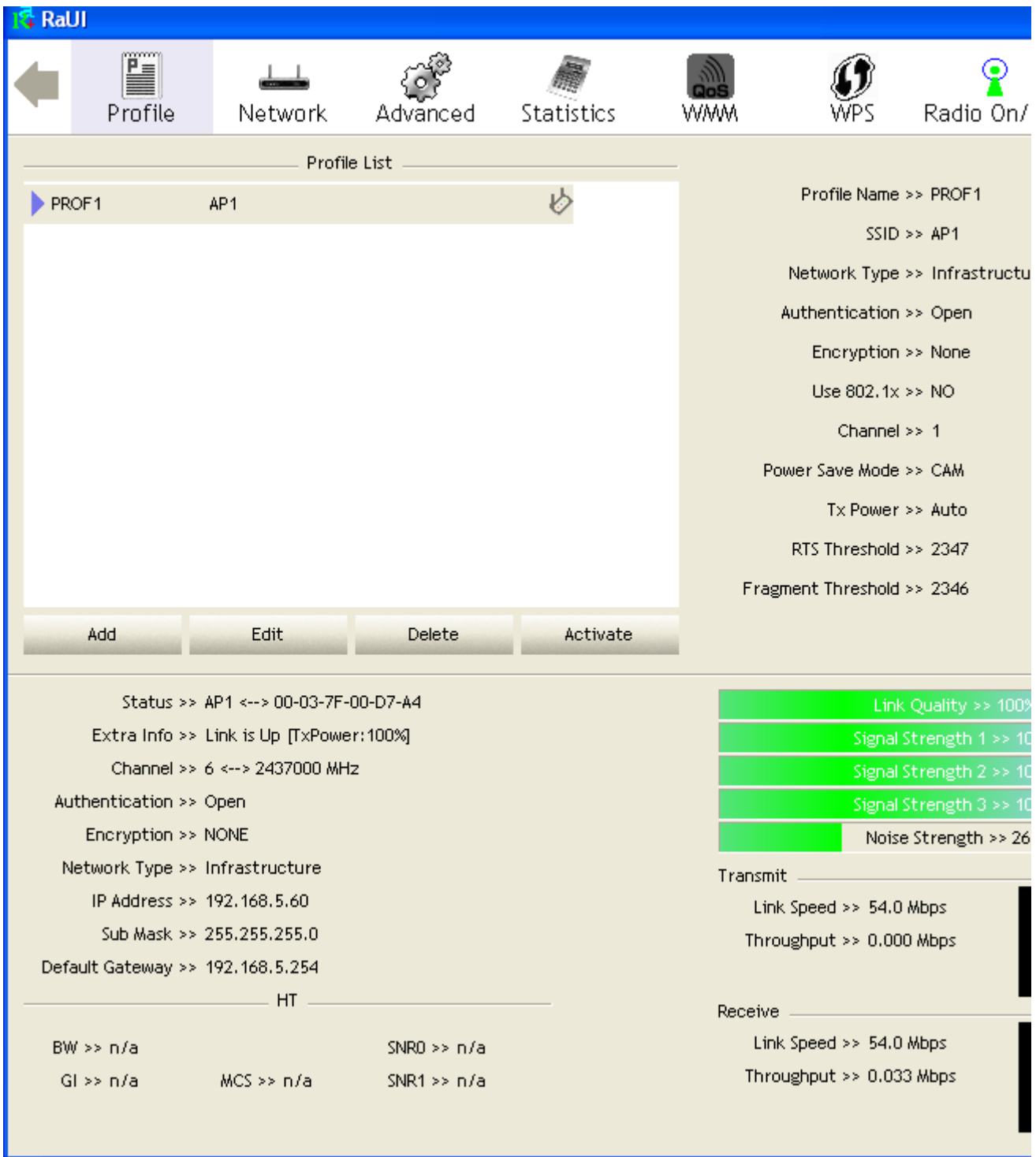
AC\_BK       AC\_BE       AC\_VI       AC\_VO

Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec


Apply      Tear Down

2 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 :

1 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 >>            Timeout Value >>  sec


Ap  
Tear

② 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

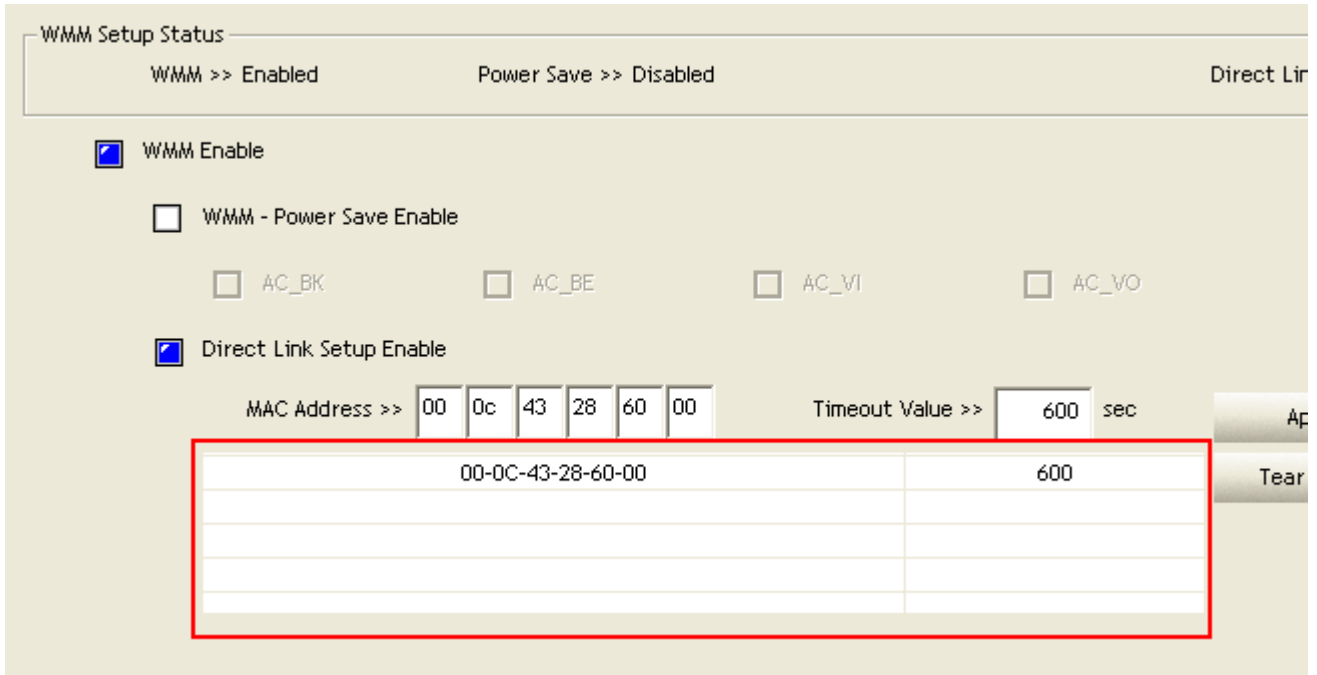
AC\_BK       AC\_BE       AC\_VI       AC\_VO

Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec


Ap  
Tear

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

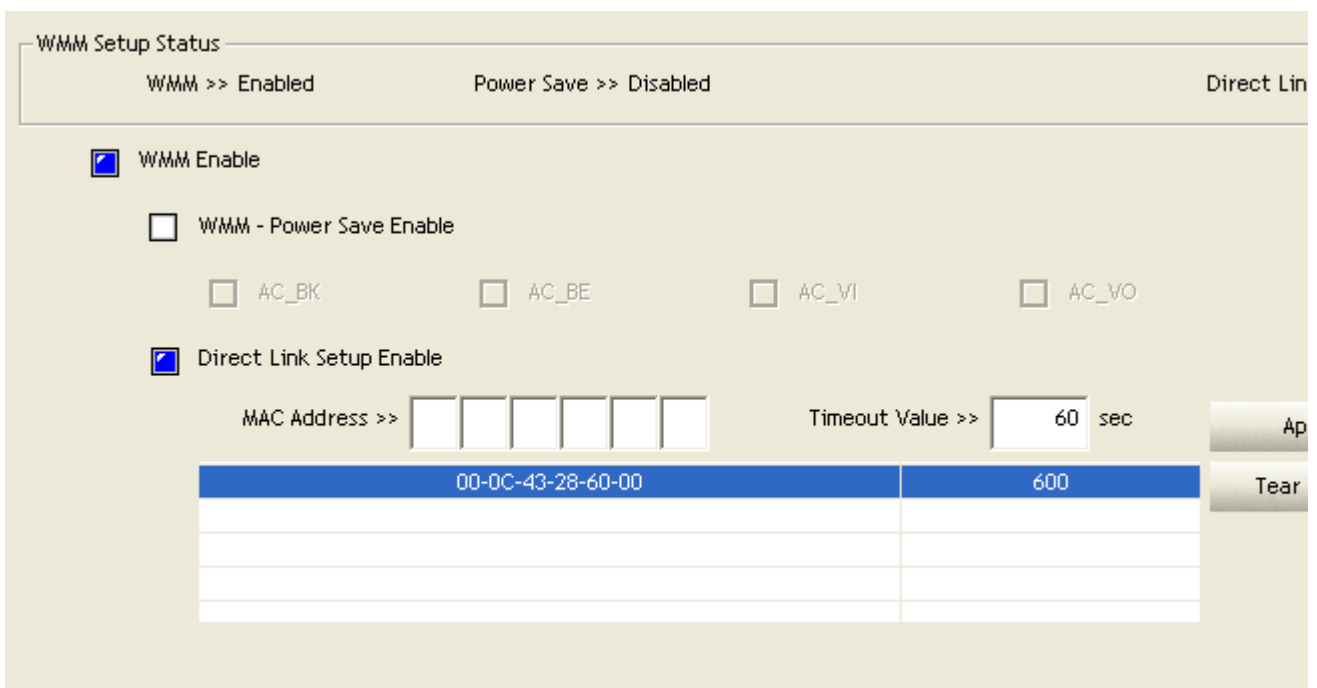


Describe "DLS Status" as follow :

1 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.

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

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



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

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

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

Ap  
Tear

3. Disconnect Direct Link Setup as follow :

1. Select a direct link STA.

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

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

Ap  
Tear

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

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

AC\_BK       AC\_BE       AC\_VI       AC\_VO

Direct Link Setup Enable

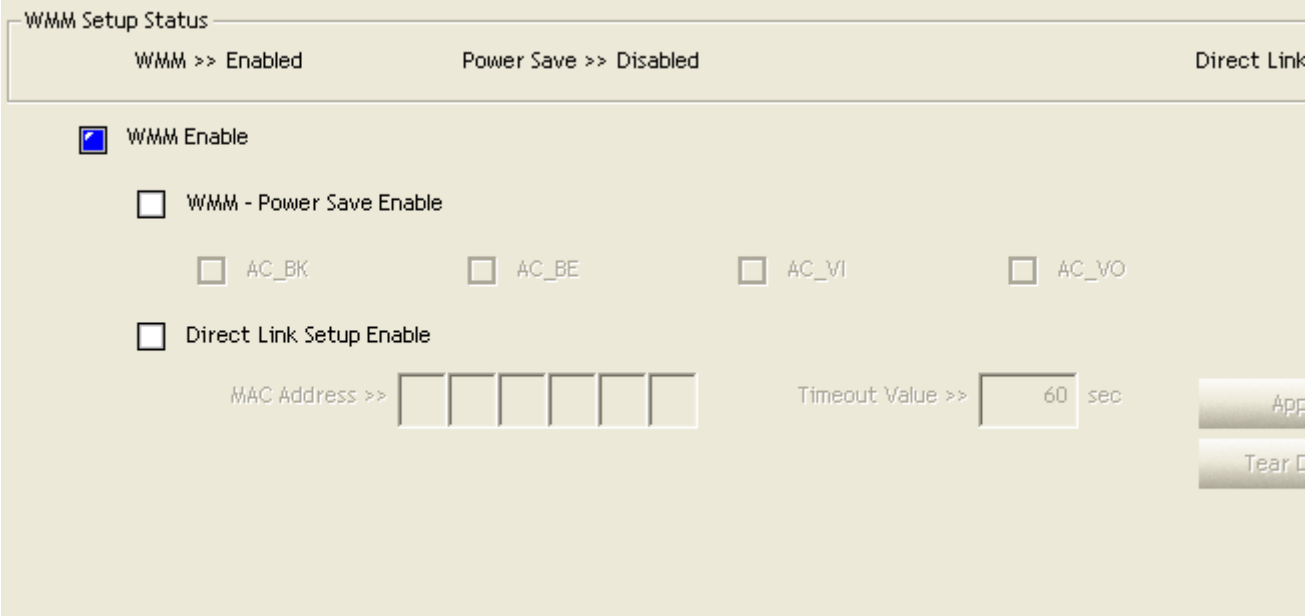
MAC Address >>            Timeout Value >>  sec


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:

- 1 Click "WMM Enable".



The screenshot shows a configuration window titled "WMM Setup Status". At the top, it displays the current status: "WMM >> Enabled", "Power Save >> Disabled", and "Direct Link". Below this, there are several checkboxes and input fields:

- WMM Enable
- WMM - Power Save Enable
  - AC\_BK
  - AC\_BE
  - AC\_VI
  - AC\_VO
- Direct Link Setup Enable
  - MAC Address >> [ ][ ][ ][ ][ ][ ][ ]
  - Timeout Value >> [ 60 ] sec

On the right side of the window, there are two buttons: "Apply" and "Tear D".



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

The screenshot shows the RaUI interface for configuring a profile. The top navigation bar includes 'Profile', 'Network', 'Advanced', 'Statistics', 'WMM', 'WPS', and 'Radio On/Off'. The 'Profile List' table shows a single entry 'PROF1' with 'AP1' as the AP. Below the table are buttons for 'Add', 'Edit', 'Delete', and 'Activate'. The configuration details for 'PROF1' are as follows:

- 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 and Link Information:

- 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) Section:

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

Transmit Section:

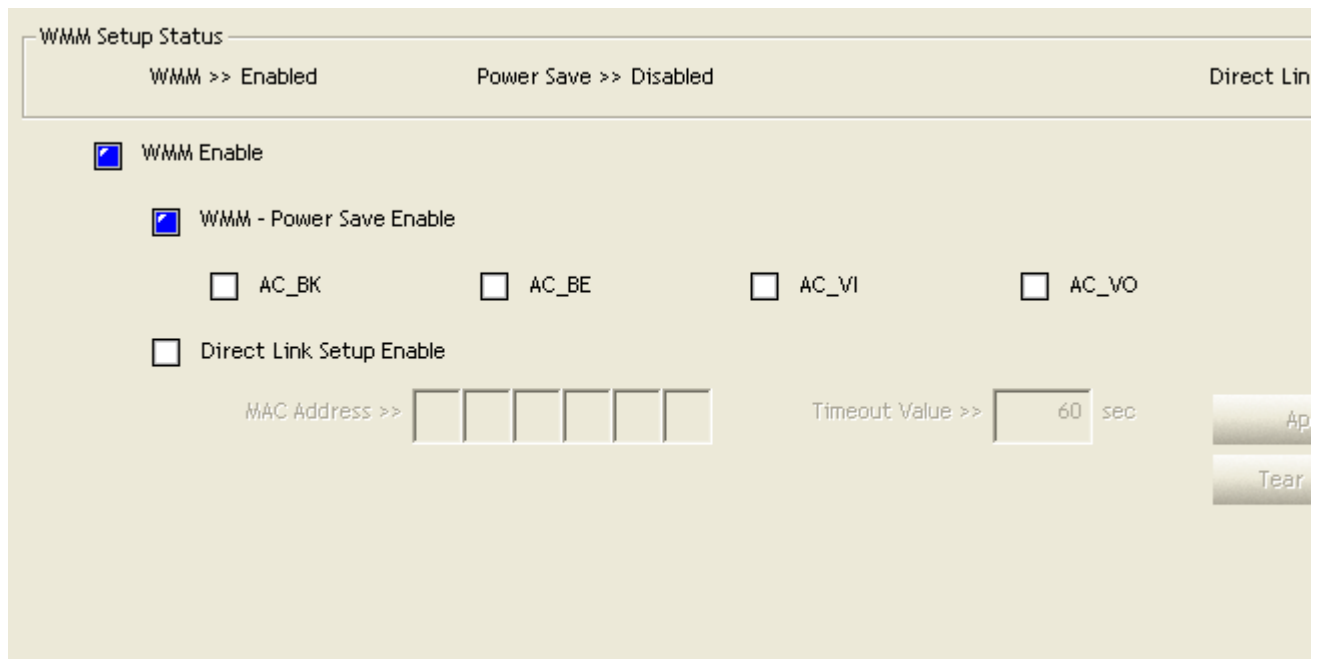
- Link Quality >> 100%
- Signal Strength 1 >> 10
- Signal Strength 2 >> 10
- Signal Strength 3 >> 10
- Noise Strength >> 26
- Link Speed >> 54.0 Mbps
- Throughput >> 0.000 Mbps

Receive Section:

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

## Example to Configure to Enable WMM Power Save

- 1 Click "WMM-Power Save Enable".



WMM Setup Status

WMM >> Enabled      Power Save >> Disabled      Direct Lin

WMM Enable

WMM - Power Save Enable

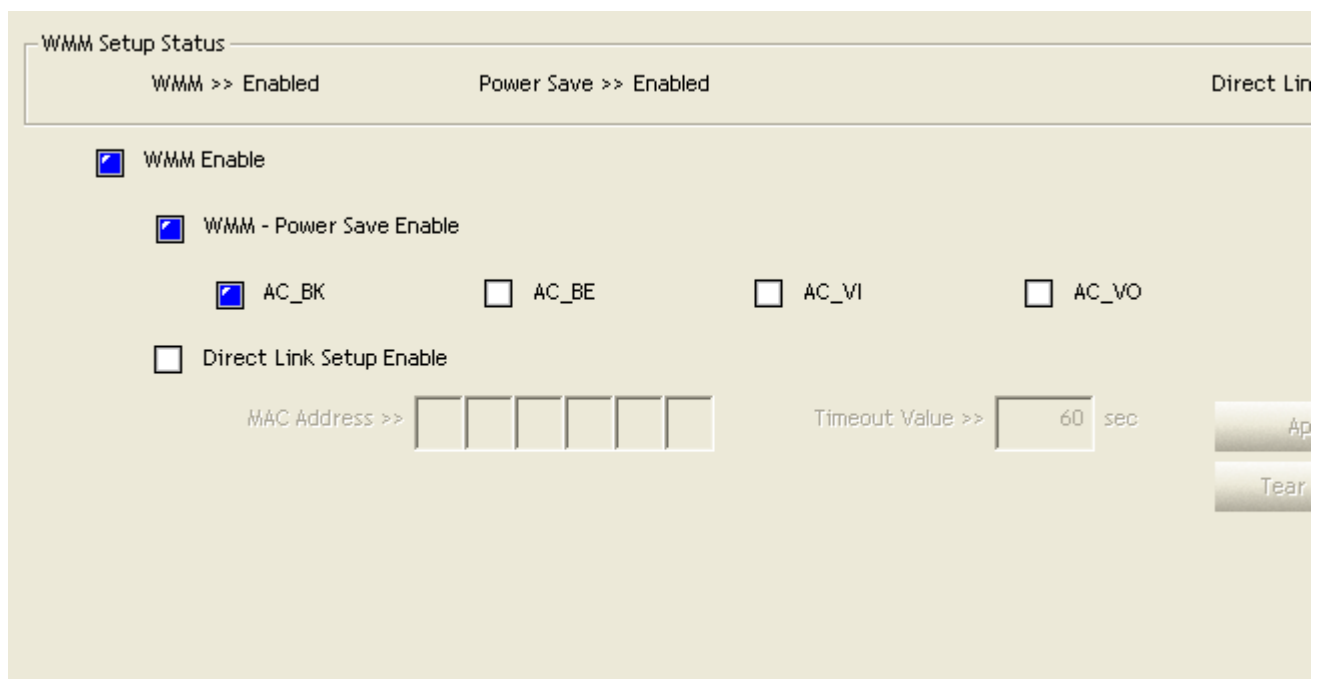
AC\_BK       AC\_BE       AC\_VI       AC\_VO

Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec

Ap  
Tear

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



WMM Setup Status

WMM >> Enabled      Power Save >> Enabled      Direct 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

# WPS

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

The screenshot displays the RaUI WPS configuration page. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), and Radio On/Off. Below the navigation bar, the main content area is divided into several sections:

- WPS AP List:** A table listing discovered APs.
 

ID	AP Name	MAC Address	Channel
Unknown	AP1-WPS	00-10-18-90-2E-27	1
Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
Unknown	arvint-2860AP	00-0C-43-28-60-60	3
Unknown	default	00-18-02-4A-0A-6B	6
- WPS Profile List:** Currently empty.
- Configuration Options:**
  - Buttons for PIN and PBC.
  - Checkboxes for  WPS Associate IE,  WPS Probe IE, and  Automatically select the AP.
  - Progress indicator: Progress >> 0%
  - Status: WPS status is disconnected.
- Connection Status:**
  - Status >> AP1 <--> 00-03-7F-00-D7-A4
  - Extra Info >> Link is Up [TxPower:100%]
  - Channel >> 6 <--> 2437000 MHz
  - Authentication >> WPA
  - Encryption >> TKIP+AES
  - Network Type >> Infrastructure
  - IP Address >> 192.168.2.8
  - Sub Mask >> 255.255.255.0
  - Default Gateway >> 192.168.2.254
- Performance Metrics:**
  - Link Quality >> 98%
  - Signal Strength 1 >> 60%
  - Signal Strength 2 >> 60%
  - Signal Strength 3 >> 70%
  - Noise Strength >> 26%
- Transmit/Receive Statistics:**
  - Transmit:** Link Speed >> 54.0 Mbps, Throughput >> 0.000 Kbps
  - Receive:** Link Speed >> 48.0 Mbps, Throughput >> 143.052 Kbps
- HT (High Throughput) Section:**
  - BW >> n/a, SNRD >> n/a
  - GI >> n/a, MCS >> n/a, SNR1 >> n/a

Figure 2-7-1 WPS function

① WPS Configuration : The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA as an Enrollee or external Registrar supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

② 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.

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

④ 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](#).

⑤ 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.

⑥ Config Mode : Our station role-playing as an Enrollee or an external Registrar.

⑦ 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.

⑧ Control items on credentials

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

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

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

4. Disconnect : 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.

5. Export Profile: Export all credentials to Profile.

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.

⑨ PIN : Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.

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

*\*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.*

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

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

⑬ Progress Bar : Display rate of progress from Start to Connected status.

⑭ Status Bar: Display currently WPS Status.

⑮ 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 :

The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by SSID, Channel, and Signal strength. The WPS details for the selected AP (AP1) are shown below.

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

General	WPS	CCX	802.11n
Authentication Type >> Unknown	State >> Unknown		
Encryption Type >> None	Version >> Unknown		
Config Methods >> Unknown	AP Setup Locked >> Unknown		
Device Password ID >>	UUID-E >> Unknown		
Selected Registrar >> Unknown	RF Bands >> Unknown		

Buttons: Rescan, Add to Profile, Connect, OK

- ① Authentication Type : There are three type of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.
- ② Encryption Type : For open and shared authentication mode, the 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.
- ③ Config Methods : Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (a bitwise OR of values)

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

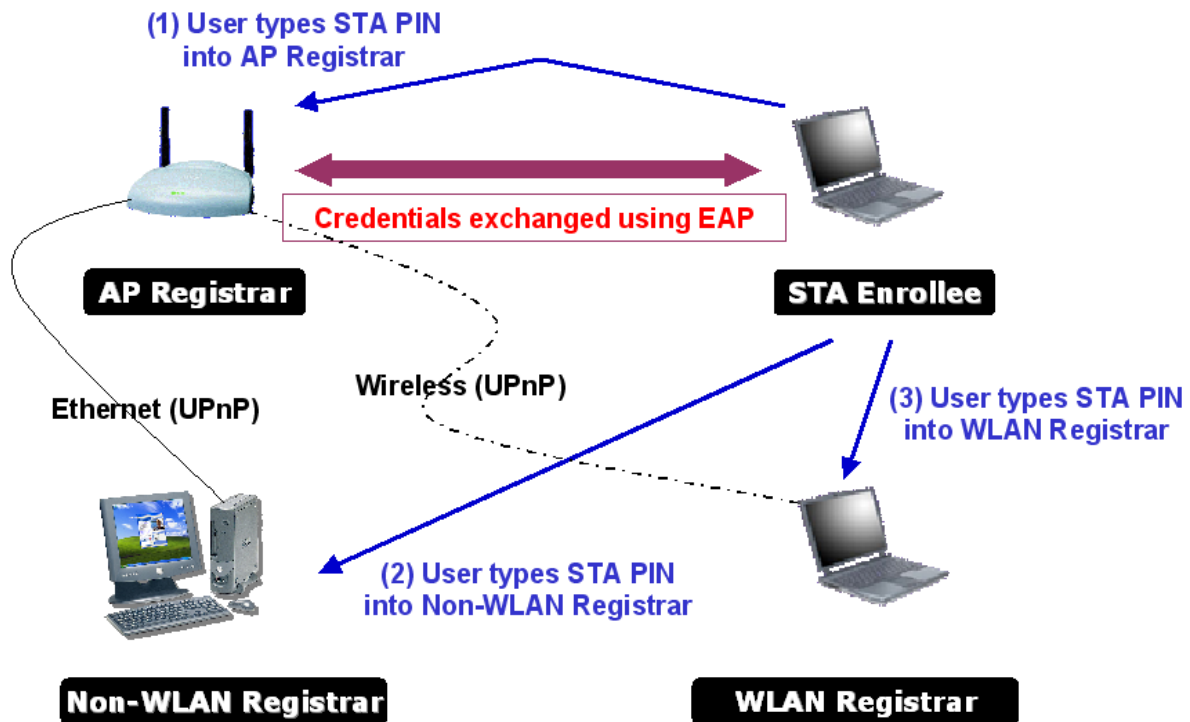
- ④ Device Password ID : Indicate the method or identifies the specific password that the selected Registrar intends to use. AP in PBC mode must indicate 0x0004 within two-minute Walk Time.

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

- ⑤ Selected Registrar : Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
- ⑥ State : The current configuration state on AP. The values are "Unconfigured" and "Configured".
- ⑦ Version : WPS specified version.
- ⑧ AP Setup Locked : Indicate if AP has entered a setup locked state.
- ⑨ UUID-E : The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.
- 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".

## 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.



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

WPS AP List				
ID : Unknown	Uicom_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	

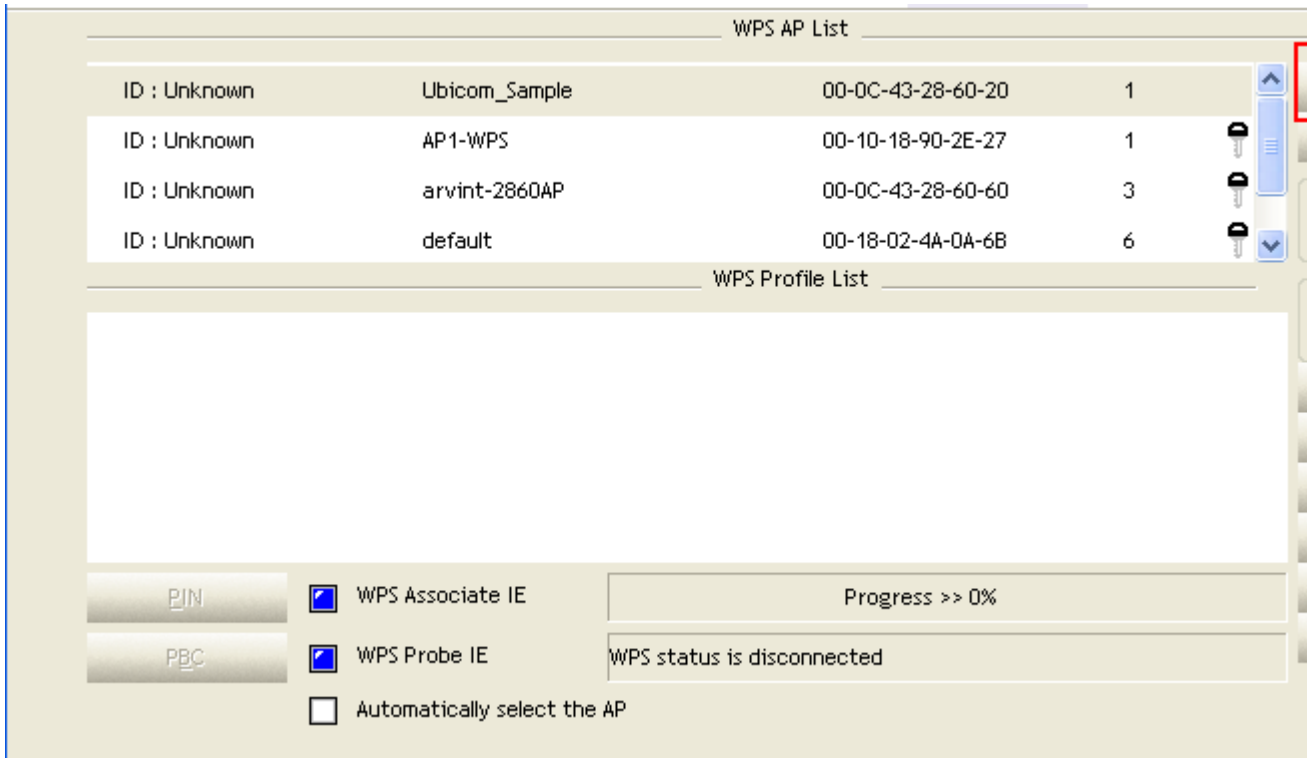
  

WPS Profile List		

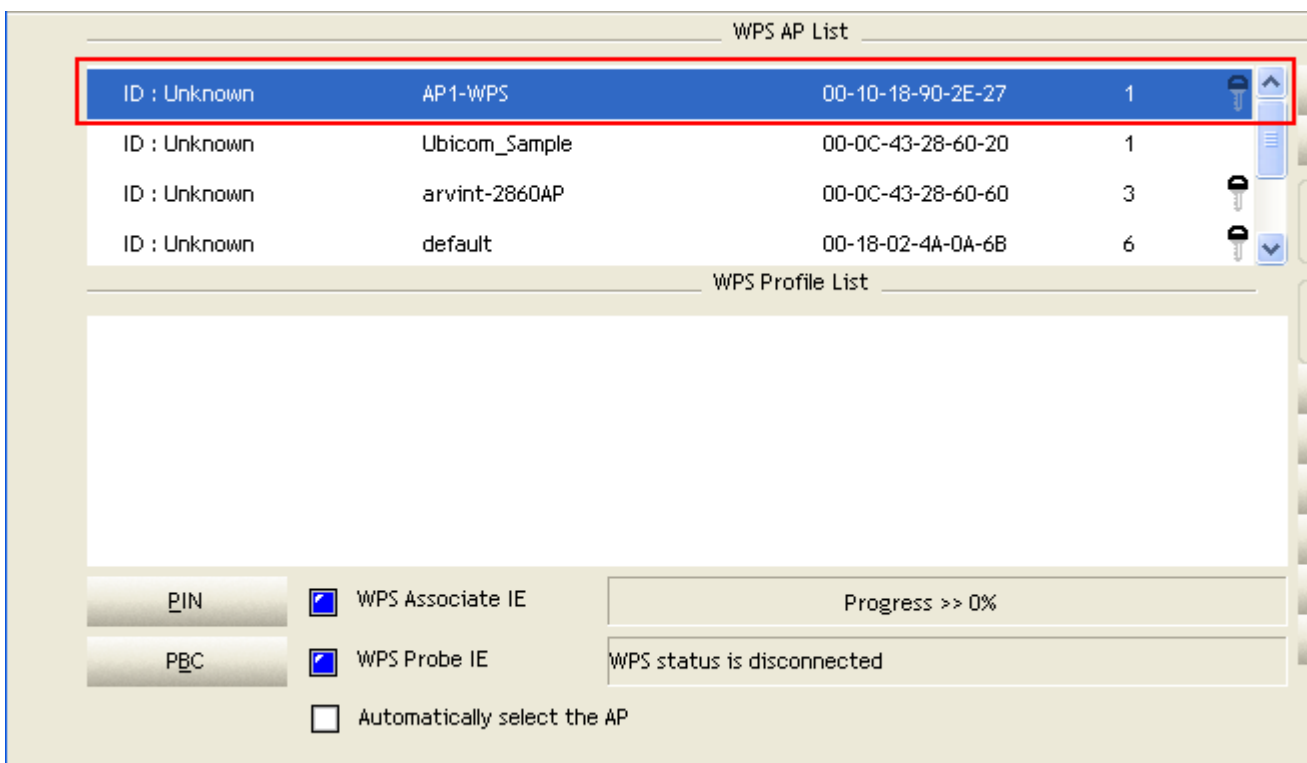
  

PIN	<input checked="" type="checkbox"/> WPS Associate IE	Progress >> 0%
PBC	<input checked="" type="checkbox"/> WPS Probe IE	WPS status is disconnected
	<input type="checkbox"/> Automatically select the AP	

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



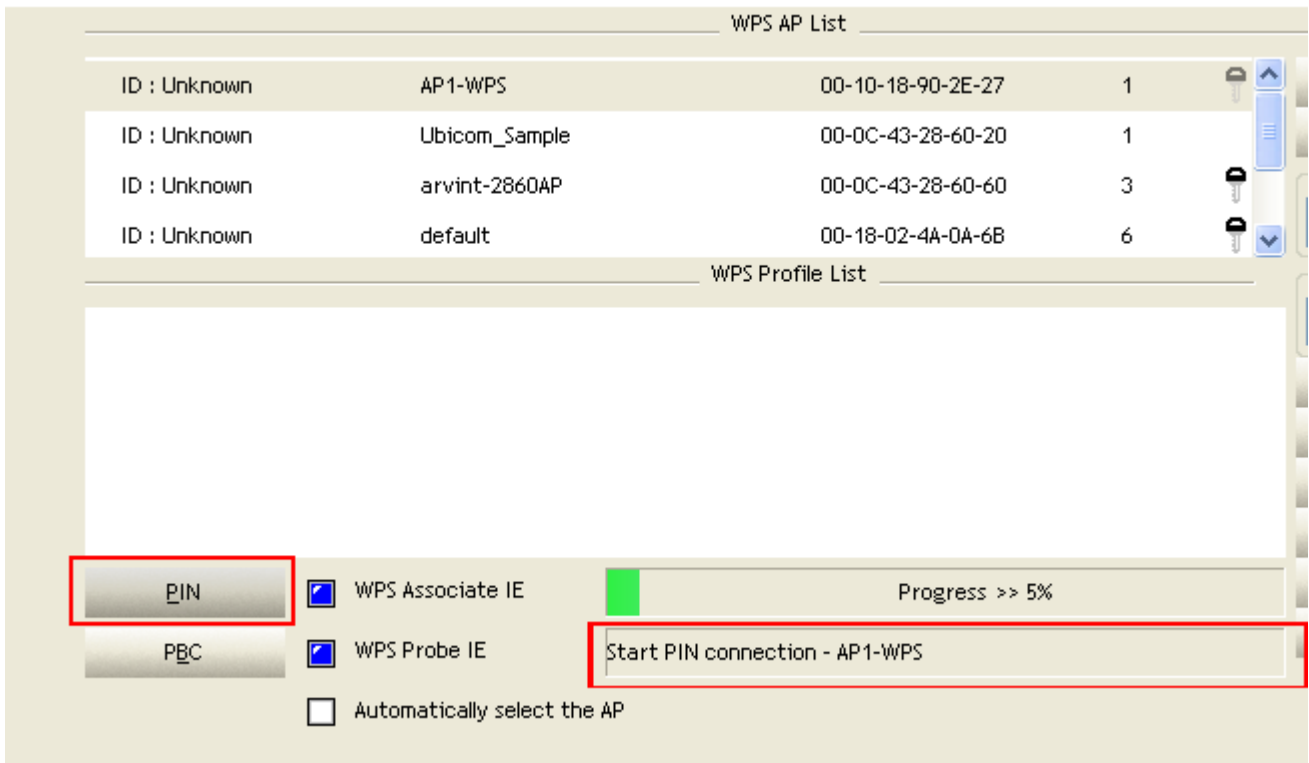
3 Select an AP (SSID/BSSID) that STA will join to.





4 Click "PIN" button to start PIN connection.

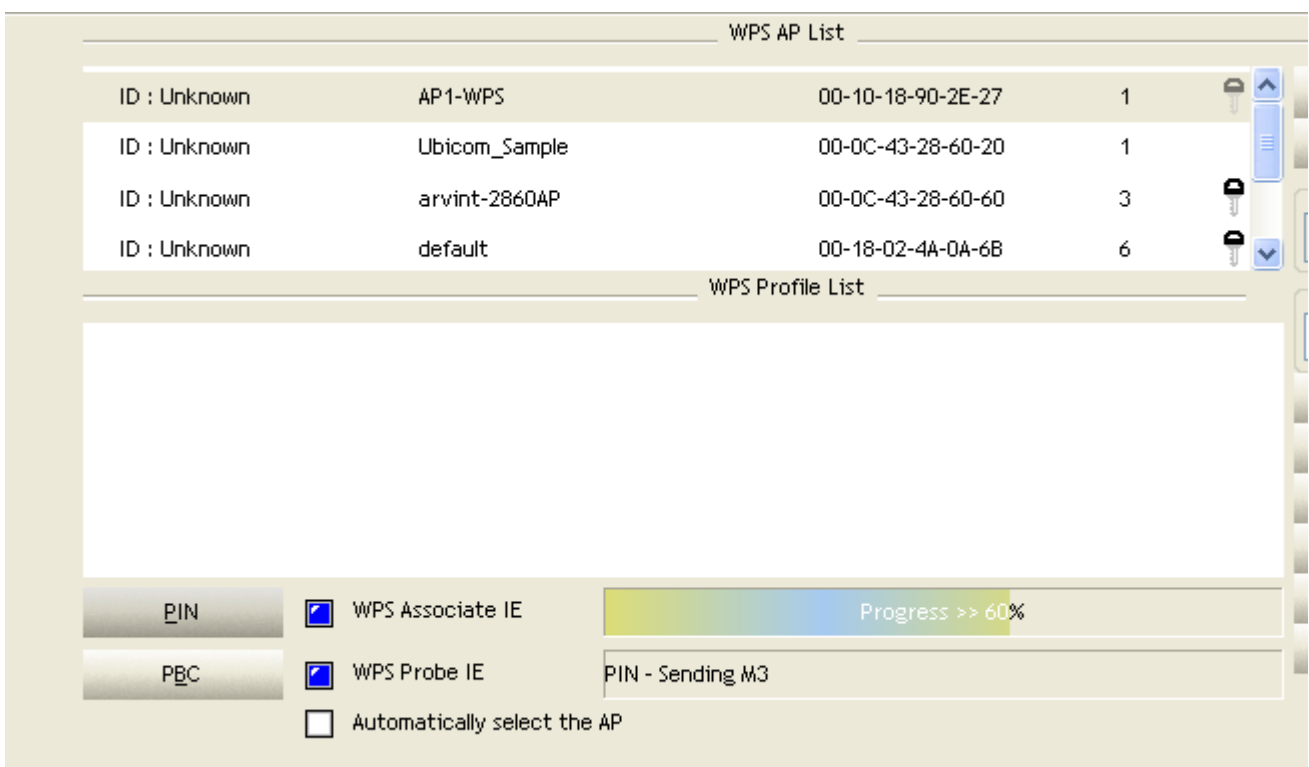
5 Enter PIN Code of STA into the Registrar when prompted by the Registrar.



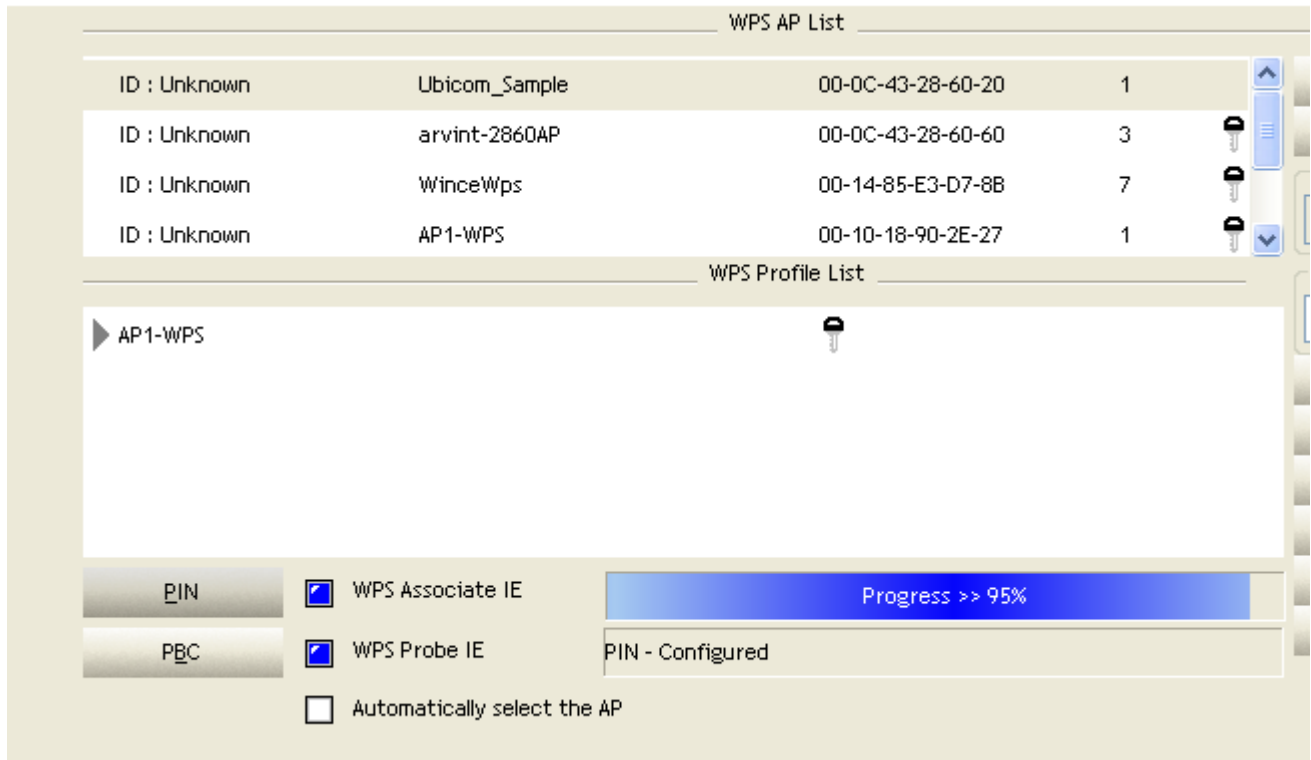
\*Allow of an exchange between Step 4 and Step 5.

\*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.

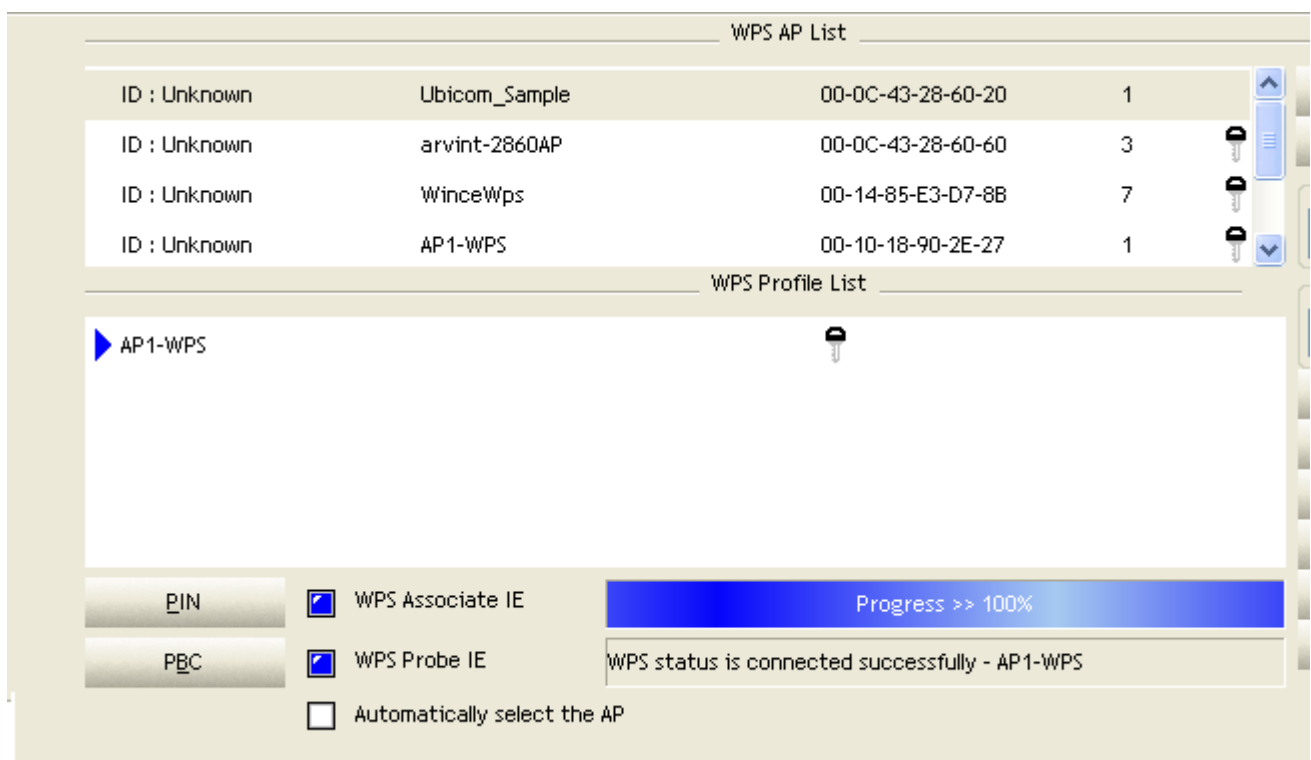
6 The result will look like the below figure.



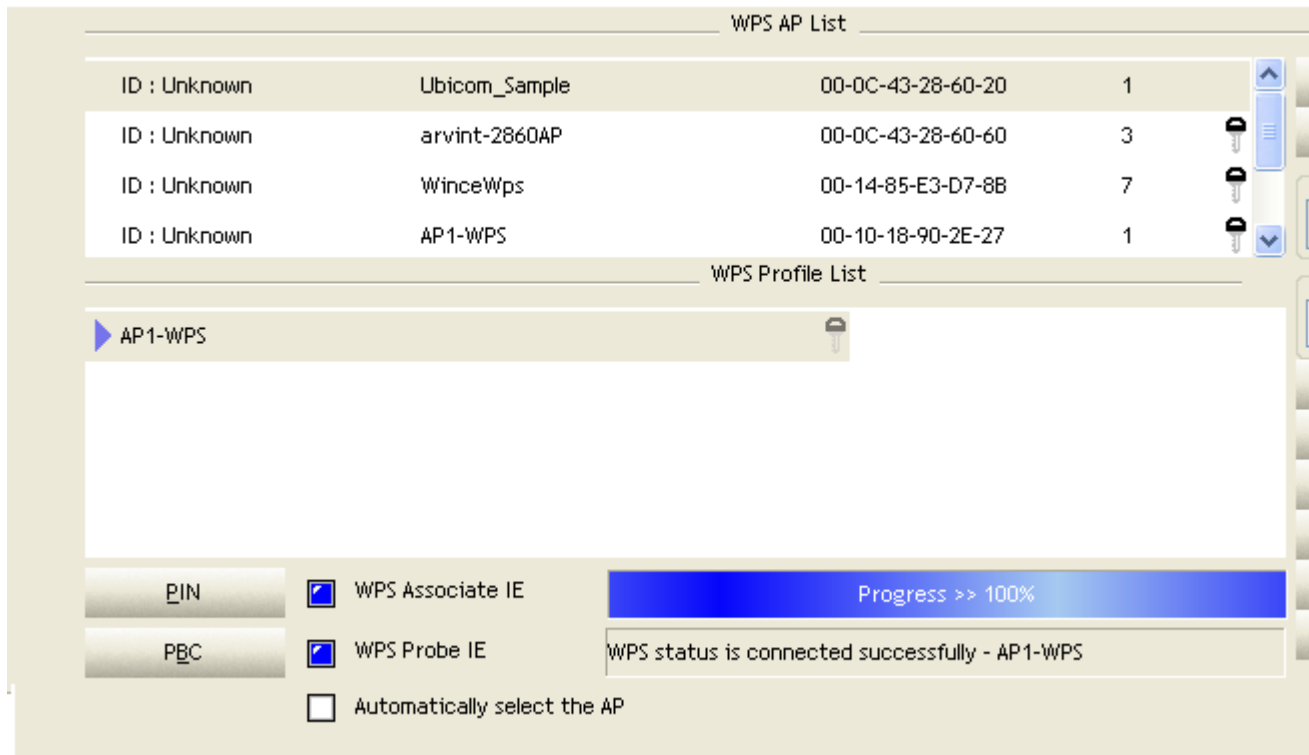
7 Configured and got one or multiple credential(s).



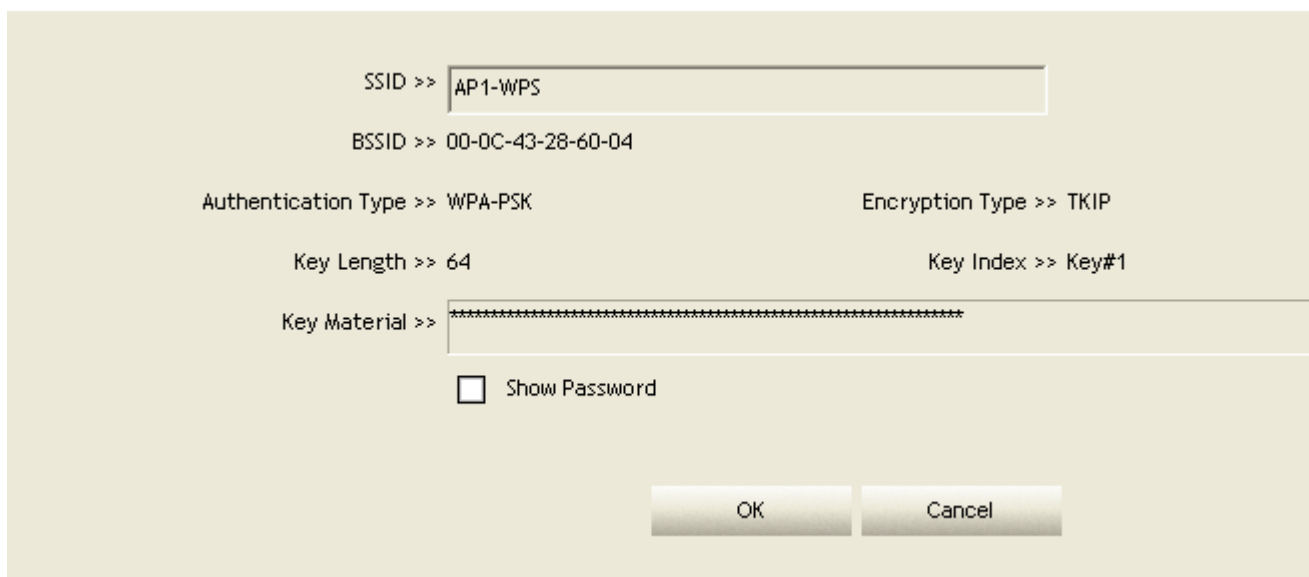
8 Then connect successfully. The result will look like the below figure.



9 Click "Detail" button.



10 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 :

① 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 EAP-Req (Start) ~>  
Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending  
M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending  
EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected  
successfully-SSID

② WPS configuration doesn't complete after **two-minute connection** : WPS Eap  
process failed.

③ 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.

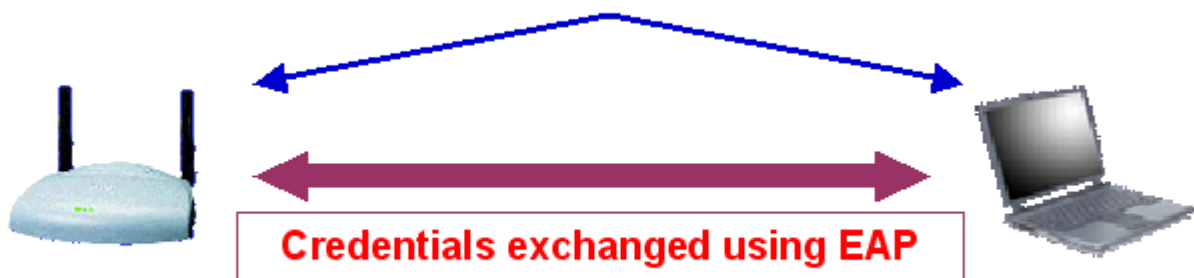
## Example to Add to Registrar Using PBC Method

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.*

### Push PBC button on both Registrar and Enrollee



**AP Registrar**

**STA Enrollee**

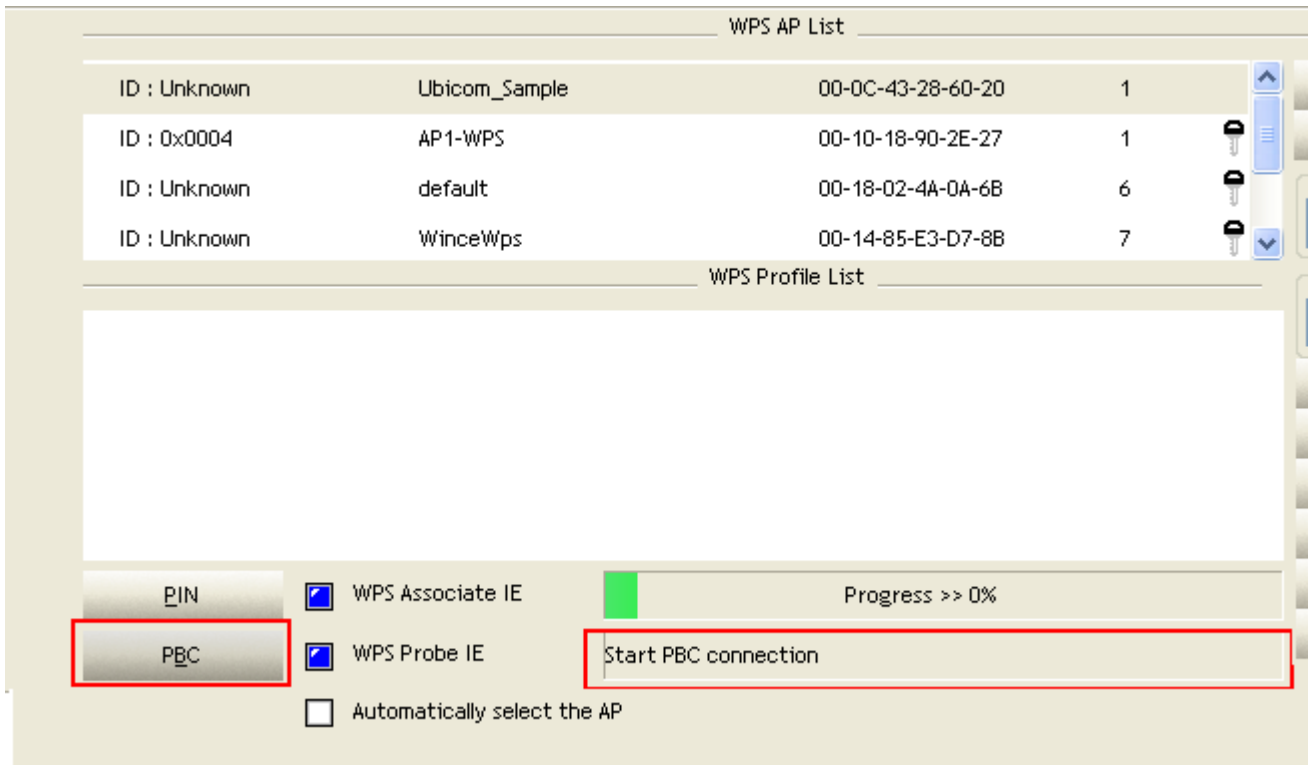
1 Go to the box of Config Mode and select Enrollee.

The screenshot shows the WPS configuration interface. At the top, there is a 'WPS AP List' table with the following data:

ID	AP Name	MAC Address	Count	Actions
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, Up arrow, Down arrow
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3	Key icon, Up arrow, Down arrow
ID : Unknown	default	00-18-02-4A-0A-6B	6	Key icon, Up arrow, Down arrow

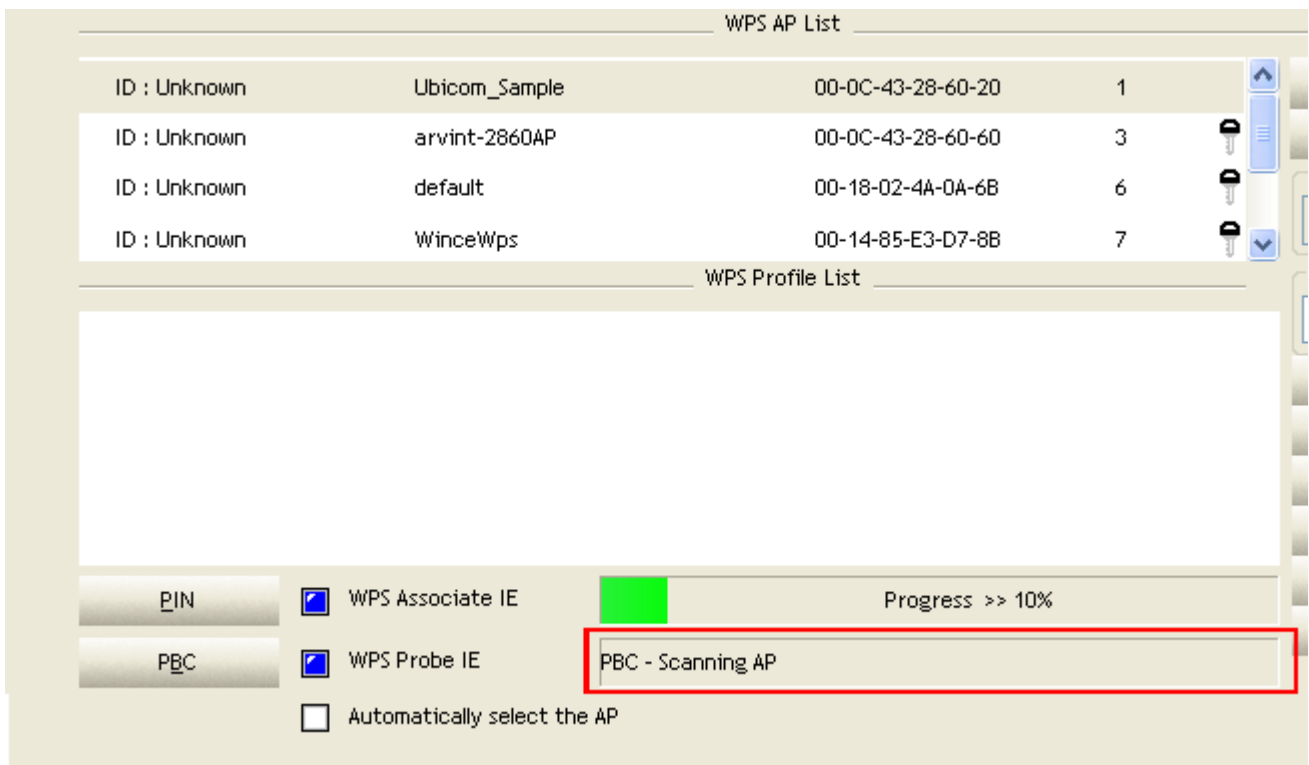
Below the table is a 'WPS Profile List' section, which is currently empty. At the bottom of the interface, there are two buttons: 'PIN' and 'PBC'. To the right of these buttons are three checkboxes: 'WPS Associate IE' (checked), 'WPS Probe IE' (checked), and 'Automatically select the AP' (unchecked). A progress bar shows 'Progress >> 0%' and a status message reads 'WPS status is disconnected'.

- 2 Click PBC to start PBC connection.
- 3 Push PBC on AP.

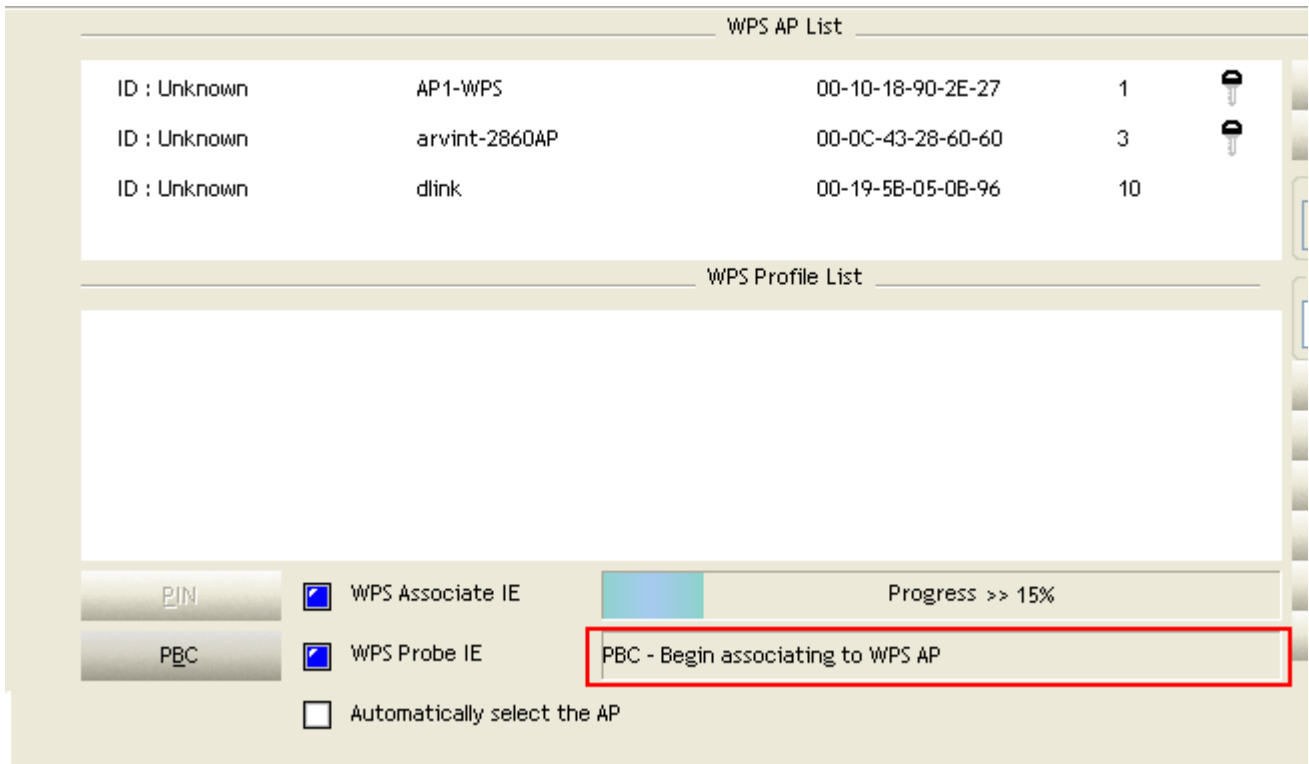


\*Allow of an exchange between Step 2 and Step 3.

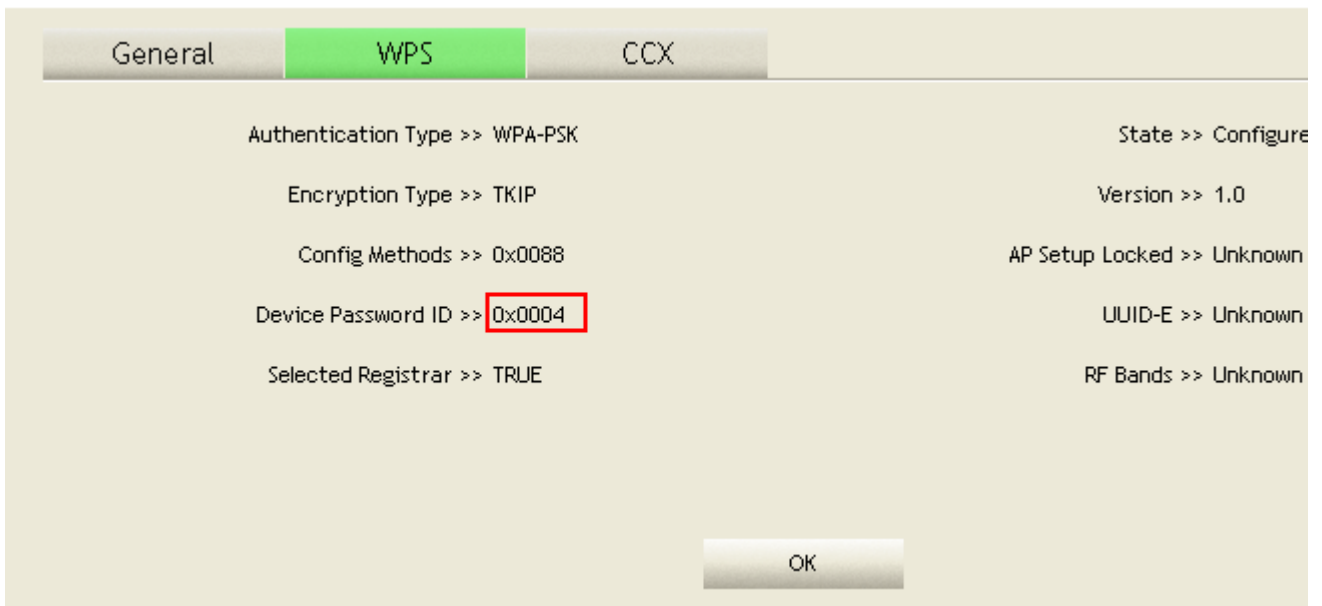
- 4 Then it can be shown "Rcanning AP" as the below figure.



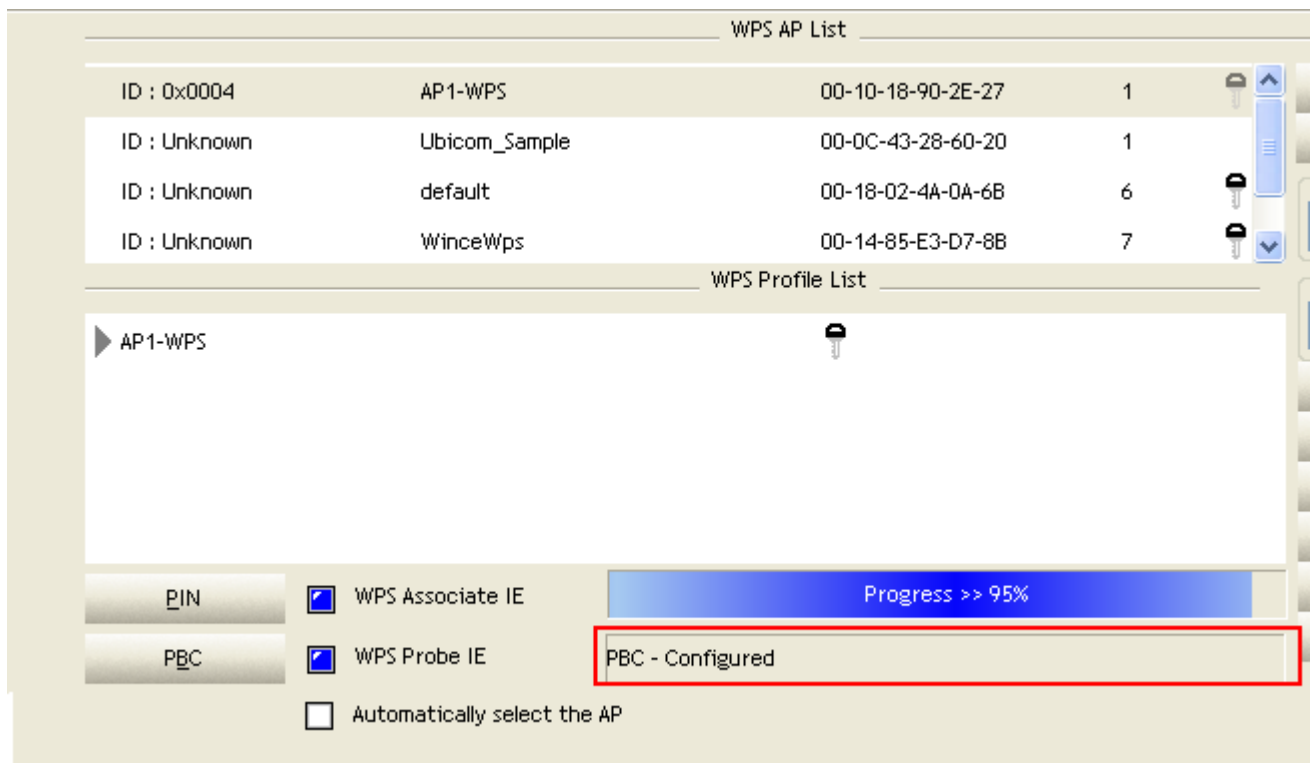
5 When finding only one AP, join it.



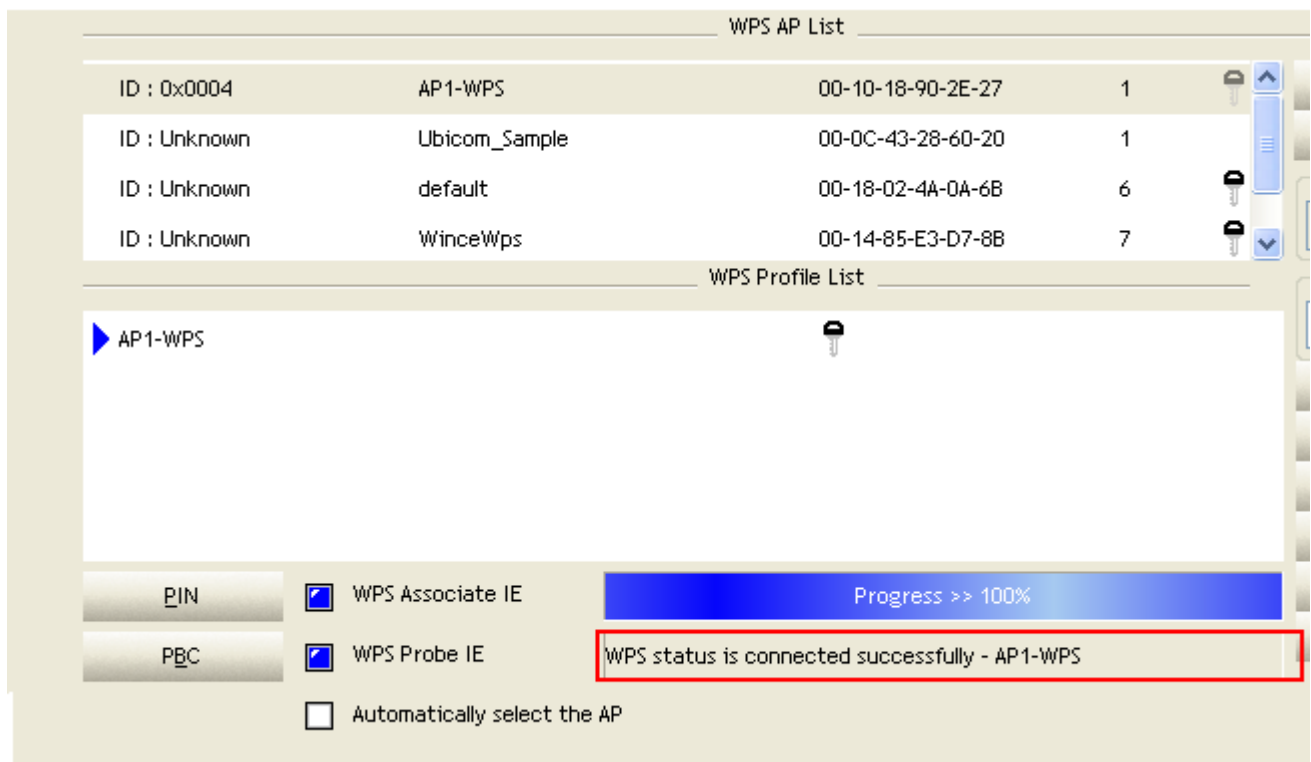
6 Check WPS Information on available WPS APs



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



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



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



① A successful PBC Configuration :

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

② No PBC AP available :

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

③ Too Many PBC AP available :

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

④ WPS configuration doesn't complete after **two-minute connection** : WPS Eap process failed.

⑤ When Errors occur within **two-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 :

① Dual bands :

AP1 is a G-Band AP using PBC mode. (ID = 0x0004) AP2 is a A-Band AP using PBC mode. (ID = 0x0004) They have the same UUID-E.

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

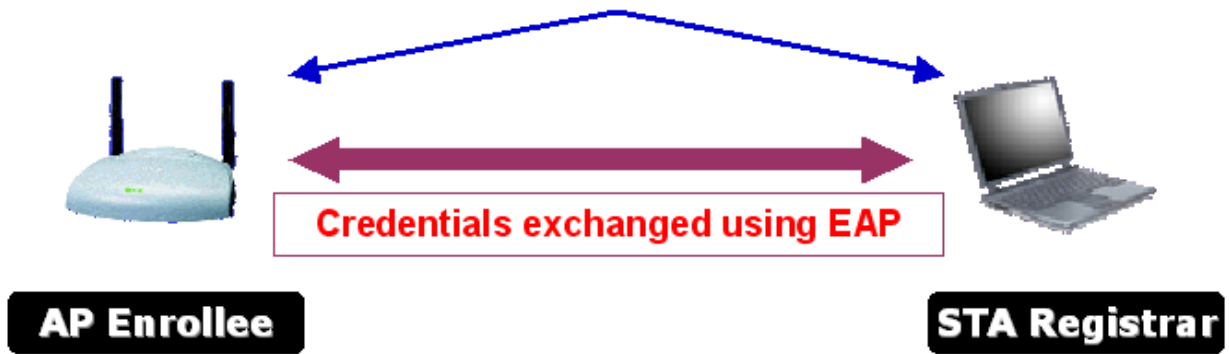
② Different UUID-E :

AP1 is a G-Band AP using PBC mode. (ID = 0x0004) AP2 is a G-Band AP using PBC mode. (ID = 0x0004) They have the different UUID-E.

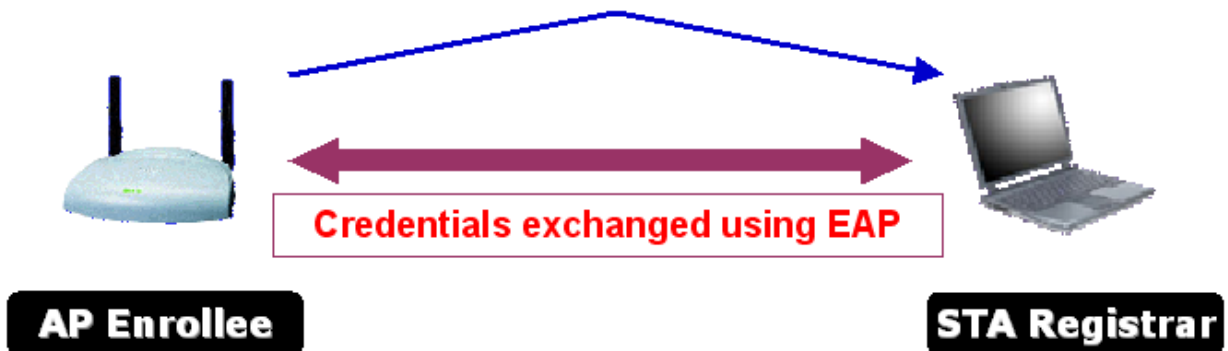
STA would regard these two APs as two different APs and wait until only one PBC AP is available.

## 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

PBC

WPS Associate IE

WPS Probe IE

Automatically select the AP

Progress >> 0%

WPS status is disconnected

- 2 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

- 3 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	

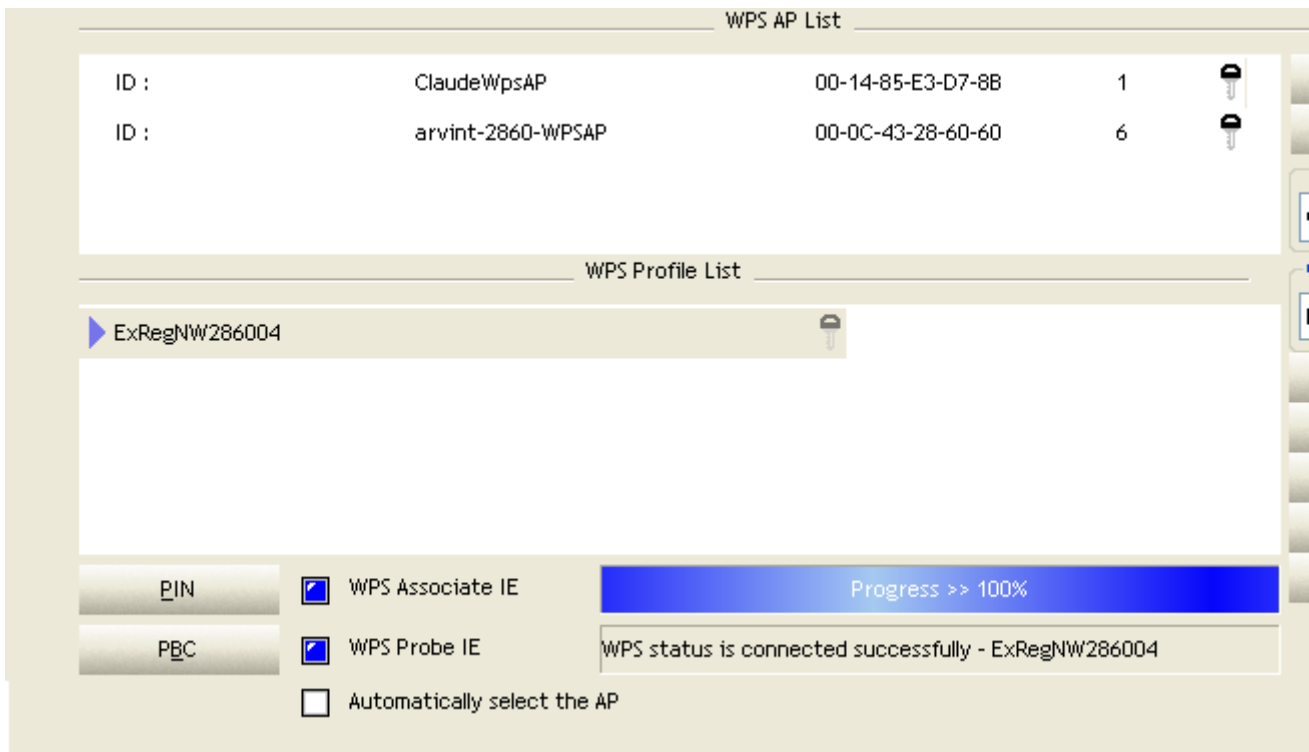
WPS Profile List

ExRegNW286004	
---------------	--

PIN PBC  
 WPS Associate IE  
 WPS Probe IE  
 Automatically select the AP  
Progress >> 0%  
WPS status is disconnected

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

- 5 If your AP Enrollee has been configured before 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.

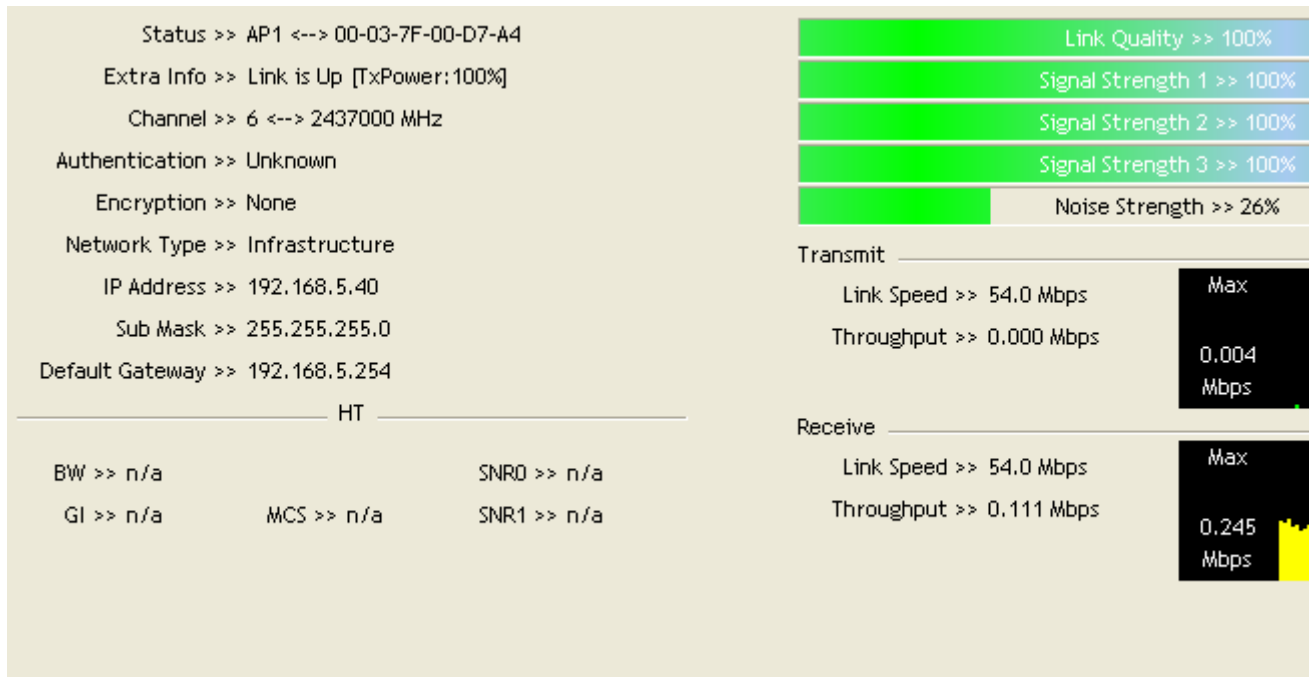


Figure 2-9 Link Status function

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

## Auth. \ Encry. Setting - WEP/TKIP/AES

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

The screenshot shows a configuration window for wireless security settings. The title bar indicates the current SSID is '8021X'. Under the 'Auth. \ Encry.' tab, the 'Authentication' is set to 'WPA-PSK' and 'Encryption' is set to 'AES'. A 'WPA Preshared Key' field is present but empty. Below, the 'Wep Key' section allows for up to four keys, each with a radio button, a 'Hexadecimal' dropdown, and a text input field. 'OK' and 'Cancel' buttons are at the bottom.

Figure 3-1 Auth. \ Encry. Setting

- ① 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.
- 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.
- ③ 8021X : This is introduced in the topic of [Section 3-2](#).
- ④ 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.
- ⑤ 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 : 32Hex characters.
  - ③ ASCII - 40bits : 5 ASCII characters.
  - ④ ASCII - 128bits : 13 ASCII characters.

**\*\*Powered by Meetinghouse.**

## 802.1x Setting

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

The screenshot shows a configuration window for 802.1x authentication. The 'EAP Method' is set to PEAP, and 'Tunnel Authentication' is set to EAP-MSCHAP v2. The 'ID \ PASSWORD' tab is active, displaying fields for 'Authentication ID / Password' (Identity, Password, Domain Name) and 'Tunnel ID / Password' (Identity, Password). The 'Sess' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom.

### Authentication type :

- 1 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.
- 2 TLS/Smart Card : Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
- 3 TTLS : Tunneled Transport Layer Security. This security method provides for certificate- based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- 4 EAP-FAST : Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be 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.](#)
- 5 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.
- 6 MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

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

## Authentication :

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

### - ID \ PASSWORD -

- 1 Authentication ID / Password : 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.
- 2 Tunnel ID / Password : Identity and Password for server.

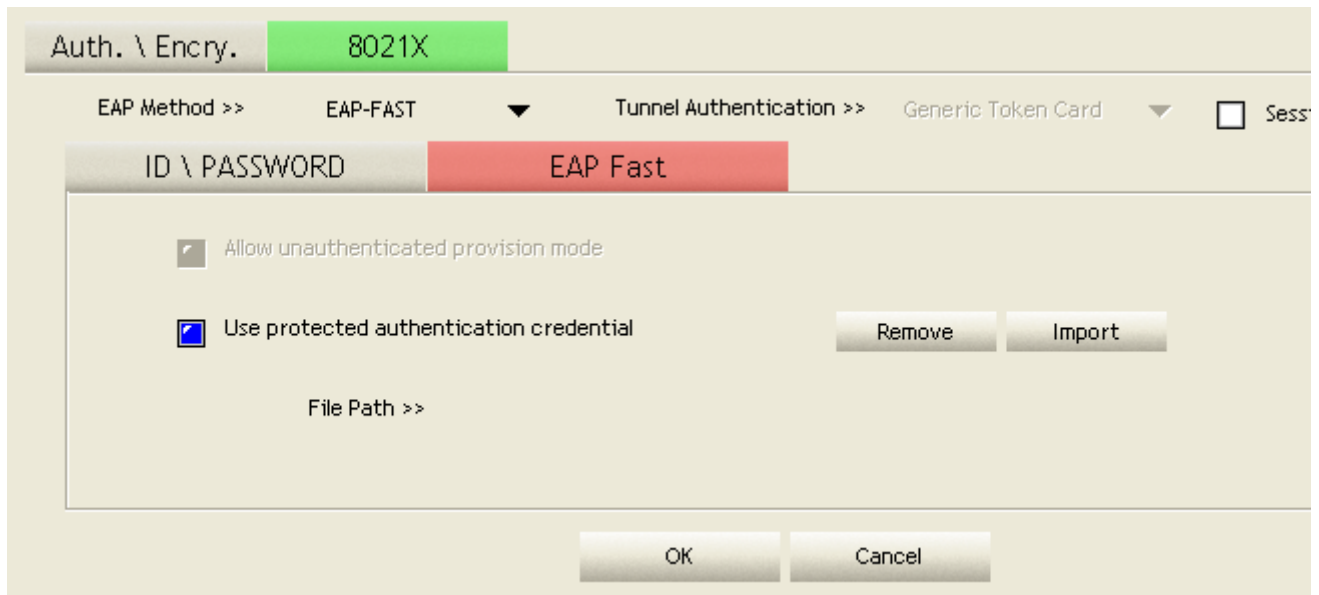
### - Client Certification -

The screenshot shows a configuration window for Client Certification. At the top, there are tabs for 'Auth. \ Encry.' (selected), '8021X', 'ID \ PASSWORD', 'Client Certification' (selected), and 'Server Certification'. Below the tabs, there are dropdown menus for 'EAP Method >>' (set to PEAP) and 'Tunnel Authentication >>' (set to EAP-MSCHAP v2). A checkbox for 'Sess' is also visible. The 'Client Certification' section contains a checkbox for 'Use Client certificate' which is unchecked. To its right, there are three input fields containing the text 'wpatest2', '2003serv', and '4/9/2008'. Below these fields, there are labels for 'Issued To >> wpatest2', 'Issued By >> 2003serv', 'Expired On >> 4/9/2008', and 'Friendly Name >>'. At the bottom of the window are 'OK' and 'Cancel' buttons.

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

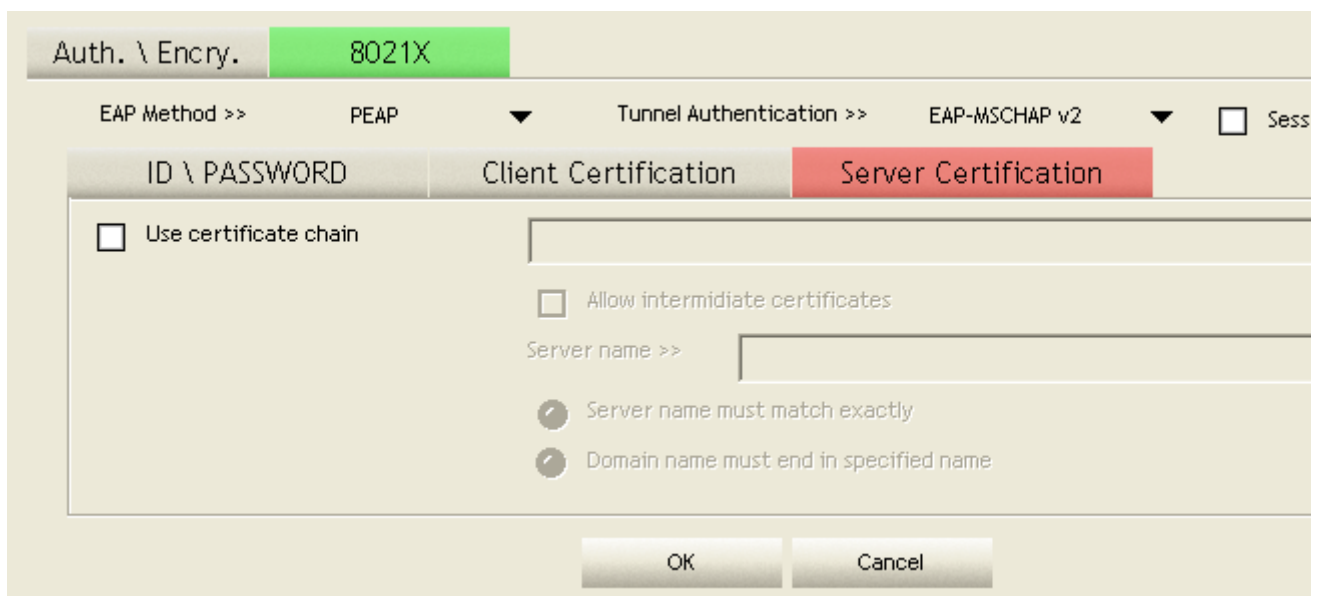


## - EAP Fast -



- 1 Allow unauthenticated provision mode : During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.
- 2 Use protected authentication credential : During the PAC can be provisioned to the client manually via disk or a secured network distribution method.

## - Server Certification -



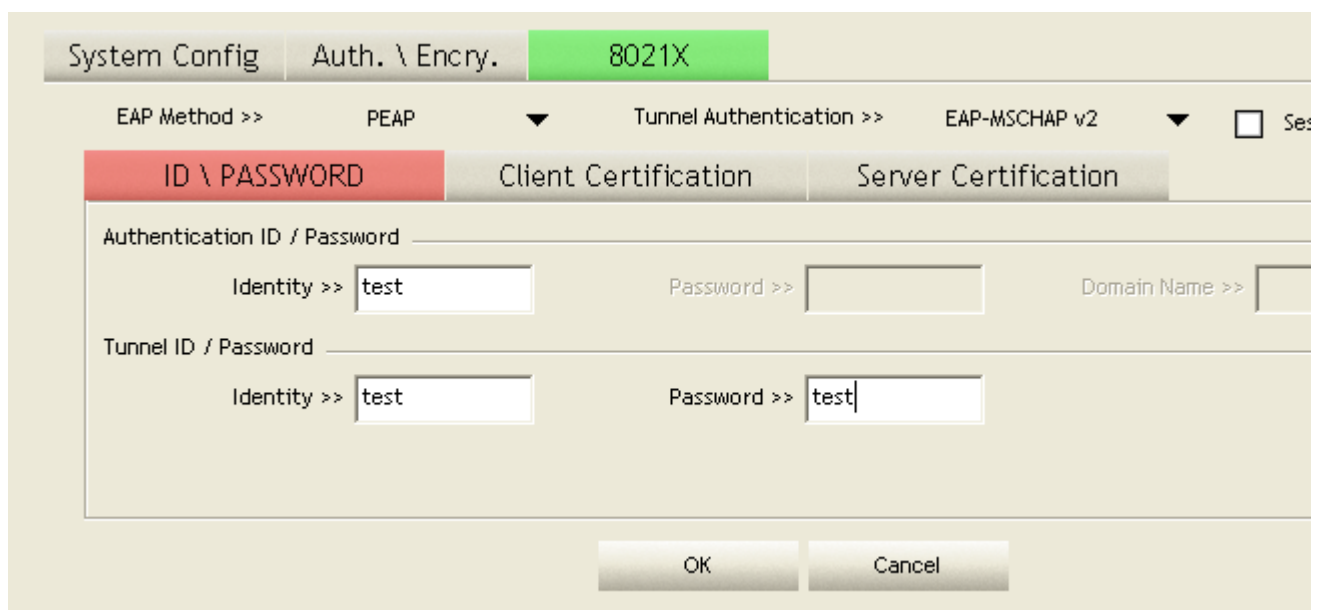
- 1 Certificate issuer : Choose use server that issuer of certificates.
- 2 Allow intimidate certificates : It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.
- 3 Server name : Enter an authentication sever root.

## Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is Failed in Profile

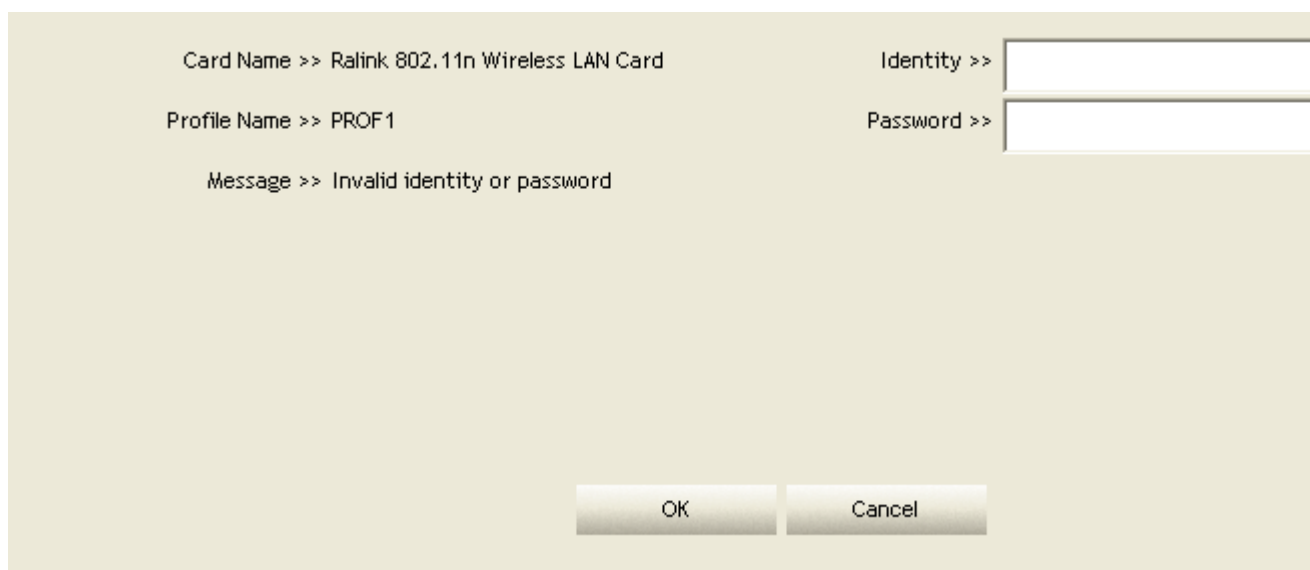
There are two situations to be able to reconnect 802.1x authenticated connection and authenticate successfully after 802.1x authenticated connection is failed in profile page. Two examples about this case are as follows:

When keying in error identity, password or domain name :

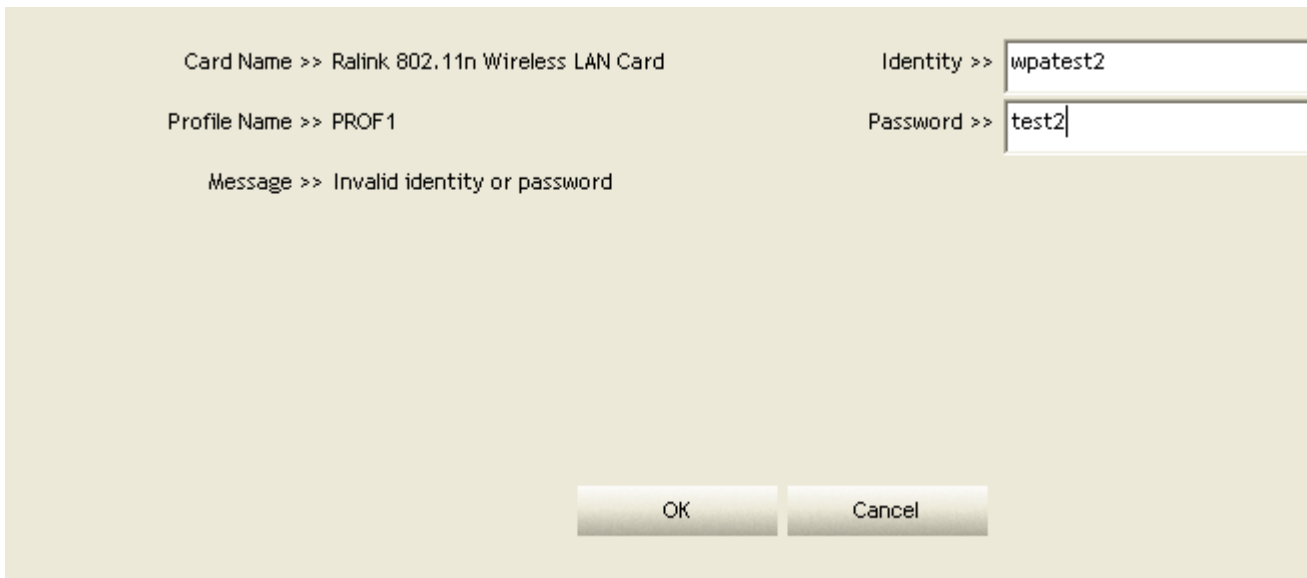
① Authentication type chooses "PEAP", key identity into test. Tunnel Protocol is "EAP- MSCHAP- v2, and tunnel identity is test and tunnel password is test. Those setting are same as our intended AP's setting.



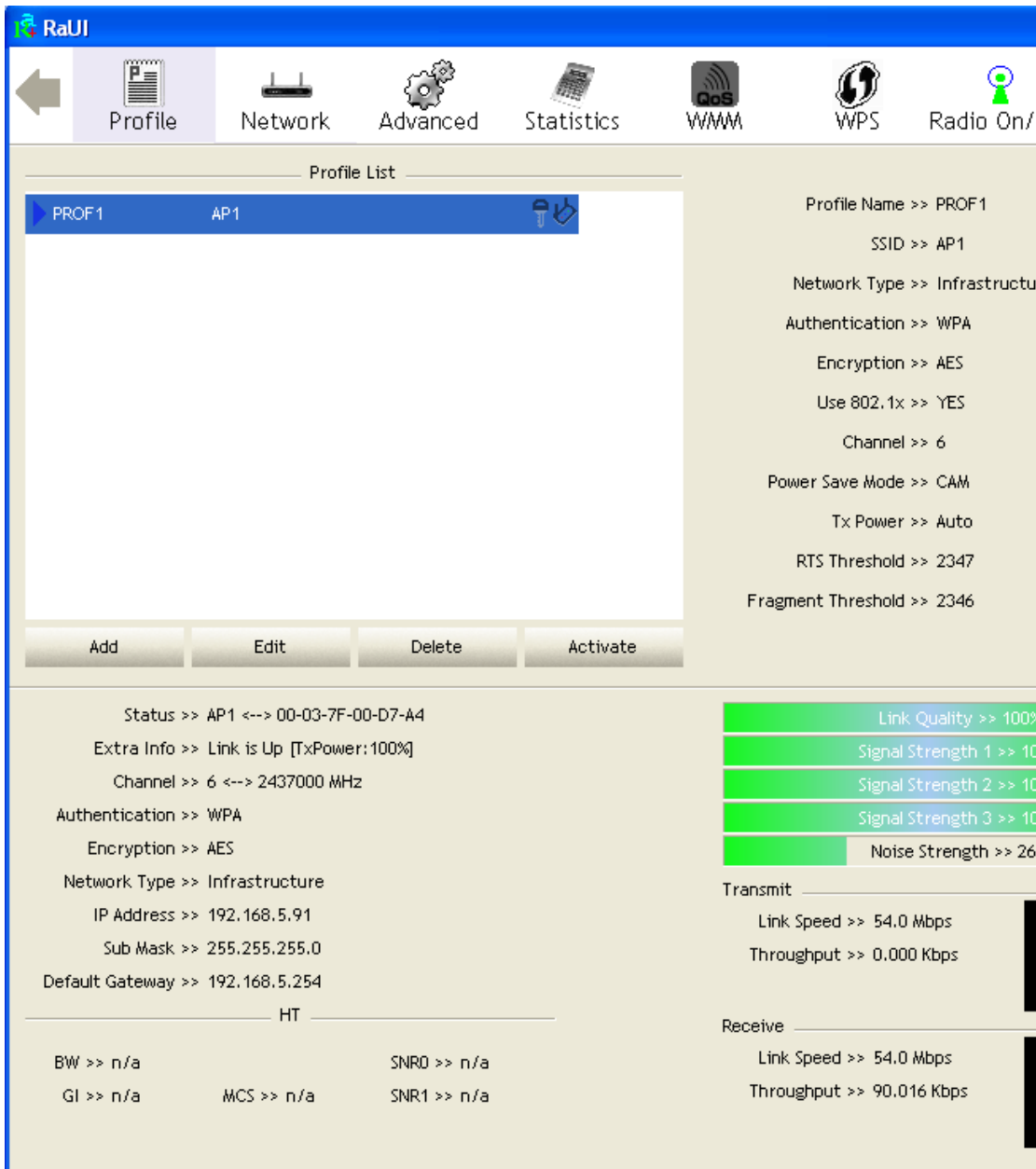
② Because keying error identity and error password, the result will look like the below figure.



③ If you want to disconnect, click cancel button in Authentication Failure dialog. If you want to reconnect, key identity into wpatetest2. And tunnel identity is wpatetest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

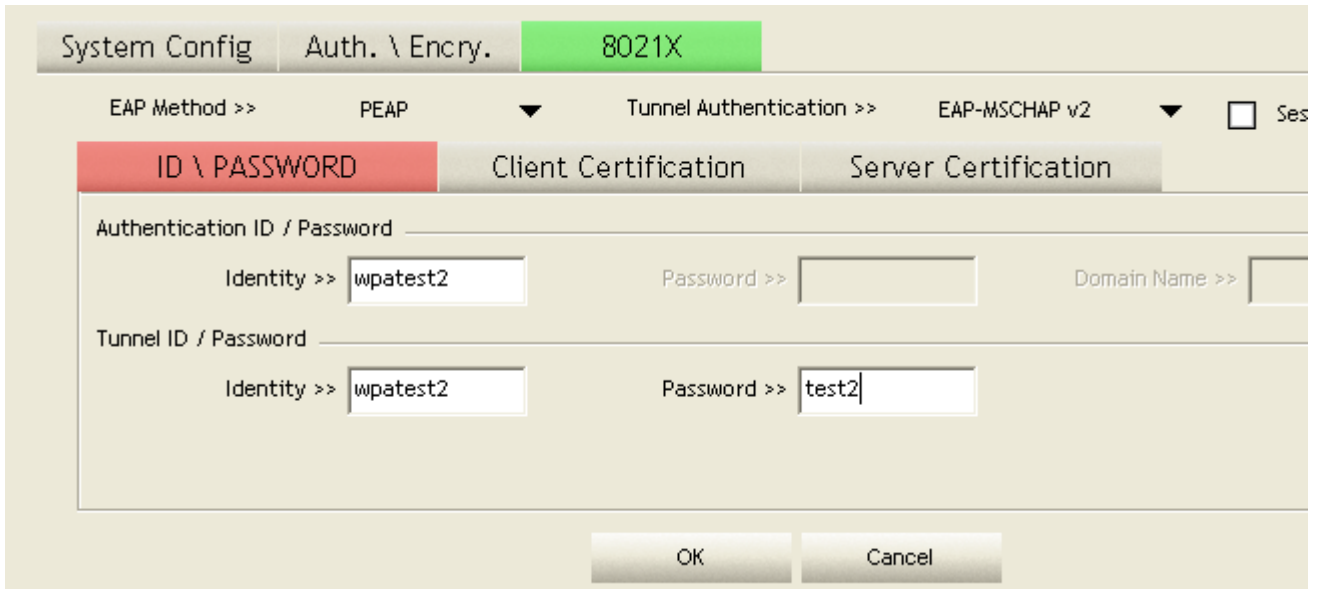


4 Click "OK" button. If it connected successfully, the result will look like the below figure.



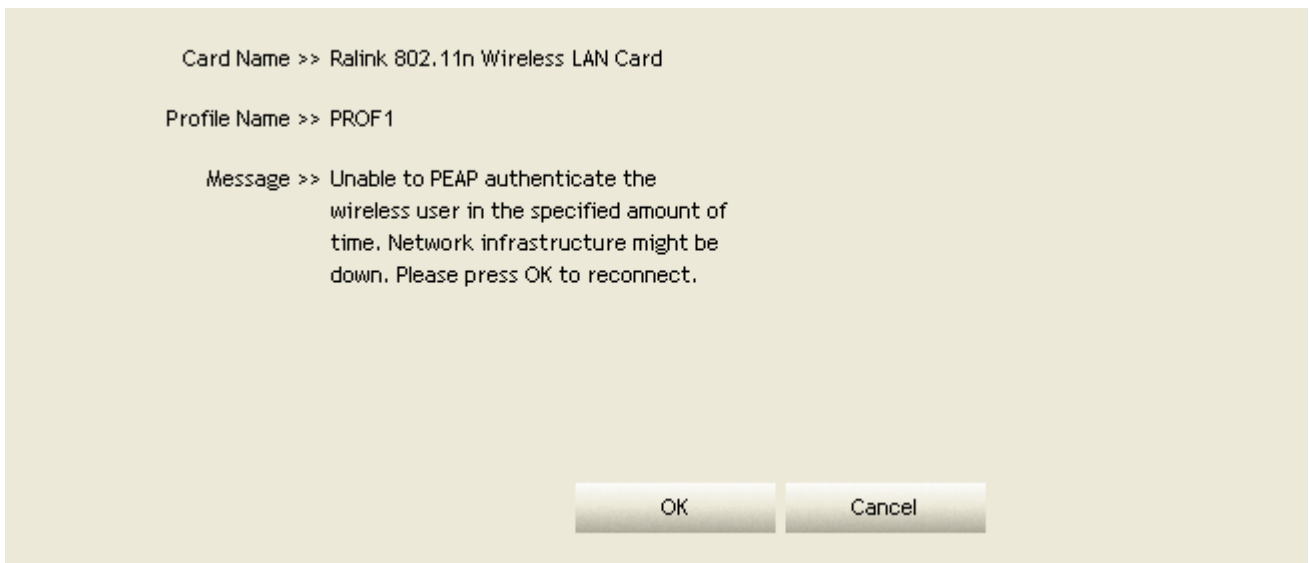
When occurring "Timeout" :

- 1 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 a configuration window for 8021X. The tabs at the top are "System Config", "Auth. \ Encry.", and "8021X". Below the tabs, the "EAP Method" is set to "PEAP" and "Tunnel Authentication" is set to "EAP-MSCHAP v2". There are three sub-tabs: "ID \ PASSWORD" (selected), "Client Certification", and "Server Certification". Under "ID \ PASSWORD", there are two sections: "Authentication ID / Password" and "Tunnel ID / Password". In the "Authentication ID / Password" section, "Identity" is "wpatest2", "Password" is empty, and "Domain Name" is empty. In the "Tunnel ID / Password" section, "Identity" is "wpatest2" and "Password" is "test2". At the bottom, there are "OK" and "Cancel" buttons.

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



The screenshot shows a message dialog box with the following text: "Card Name >> Ralink 802.11n Wireless LAN Card", "Profile Name >> PROF1", and "Message >> Unable to PEAP authenticate the wireless user in the specified amount of time. Network infrastructure might be down. Please press OK to reconnect." At the bottom, there are "OK" and "Cancel" buttons.

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

The screenshot displays the RaUI web interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. The 'Profile' tab is selected, showing a 'Profile List' with one entry: 'PROF1' with SSID 'AP1'. Below the list are buttons for 'Add', 'Edit', 'Delete', and 'Activate'. To the right of the list, configuration details for 'PROF1' are shown:

- 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

Below the configuration, the status and extra information for the profile are displayed:

- 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

On the right side, there are signal strength and noise strength indicators:

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

At the bottom, there are sections for 'Transmit' and 'Receive' statistics:

- Transmit:** Link Speed >> 54.0 Mbps, Throughput >> 0.000 Kbps
- Receive:** Link Speed >> 54.0 Mbps, Throughput >> 90.016 Kbps

At the very bottom, there are additional parameters:

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

## Example to Configure Connection with WEP on

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

The screenshot shows the RaUI Network configuration page. The 'Network' tab is active, displaying a list of available APs. The 'AP1' entry is selected, showing 100% signal strength and WEP encryption. Below the list, the connection status for 'arscadre' is detailed, including link quality, signal strength, and network parameters.

AP ID	Channel	Encryption	Signal (%)
202	1	bg	60%
219	1	bg	65%
230	2	bg	50%
243	5	bg	81%
99	6	bg n	81%
<b>AP1</b>	<b>6</b>	<b>bg</b>	<b>100%</b>
arscadre	1	bg n	100%
Broadcom	11	bg	60%
BroadcomWPS	1	bg	60%
BUFFALO_A	44	a n	29%

Parameter	Value
Status	arscadre <--> 00-0C-43-28-70-11
Extra Info	Link is Up [TxPower:100%]
Channel	1 <--> 2412000 MHz; central channel : 3
Authentication	Unknown
Encryption	None
Network Type	Infrastructure
IP Address	169.254.73.184
Sub Mask	255.255.0.0
Default Gateway	
HT	
BW	40
GI	long
MCS	15
SNR0	n/a
SNR1	n/a
Link Quality	100%
Signal Strength 1	1
Signal Strength 2	10
Signal Strength 3	C
Noise Strength	26
Transmit Link Speed	270.0 Mbps
Transmit Throughput	0.000 Mbps
Receive Link Speed	1.0 Mbps
Receive Throughput	0.026 Mbps

2 Auth. \ Encry. function pop up.

The screenshot shows the RaUI interface with the Network tab selected. The AP List table is as follows:

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

The 'Auth. \ Encry.' dialog box is open, showing the following configuration:

- Authentication: Open
- Encryption: WEP
- 802.1X:
- WPA Preshared Key:
- Wep Key section:
  - Key#1: Hexadecimal
  - Key#2: Hexadecimal
  - Key#3: Hexadecimal
  - Key#4: Hexadecimal



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

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' table displays various access points with their signal strengths and security settings. Below the table, the 'Auth. \ Encry.' dialog is open, showing '802.1X' authentication and 'WEP' encryption. The 'Wep Key' section has 'Key#1' selected with a 'Hexadecimal' dropdown and the value '1234567890' entered in the text field.

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

Auth. \ Encry. 802.1X

Authentication >> Open Encryption >> WEP 802.1X

WPA Preshared Key >>

Wep Key

- Key#1 Hexadecimal 1234567890
- Key#2 Hexadecimal
- Key#3 Hexadecimal
- Key#4 Hexadecimal

OK Cancel



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

The screenshot shows the RaUI interface with the Network tab selected. The AP List table is as follows:

AP Name	Channel	Signal	Quality
219	1	76%	76%
223	1	50%	50%
243	5	94%	94%
99	6	65%	65%
_Shiang_2860AP	11	60%	60%
<b>AP1</b>	6	100%	98%
arscadre	1	89%	89%
BroadcomWPS	1	70%	70%
BUFFALO_A	44	44%	44%
ClaudeAP	1	60%	60%

Below the AP list, the connection details for AP1 are shown:

- Status >> AP1 <-> 00-03-7F-00-D7-A4
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 6 <-> 2437000 MHz
- Authentication >> Unknown
- Encryption >> WEP
- Network Type >> Infrastructure
- IP Address >> 192.168.5.113
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.5.254

Performance metrics:

- Link Quality >> 98%
- Signal Strength 1 >> 5
- Signal Strength 2 >> 10
- Signal Strength 3 >> 3
- Noise Strength >> 26

Transmit:

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

Receive:

- Link Speed >> 54.0 Mbps
- Throughput >> 0.022 Mbps

## Example to Configure Connection with WPA-PSK

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

The screenshot shows the RaUI Network configuration page. The 'Network' tab is selected. The AP list is sorted by SSID, Channel, and Signal. The 'arscadre' AP is selected, showing 100% link quality and 99% signal strength.

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

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 \_\_\_\_\_

Transmit

- Link Speed >> 270.0 Mbps
- Throughput >> 0.000 Mbps

Receive

- Link Speed >> 54.0 Mbps
- Throughput >> 0.012 Mbps

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 99%

Signal Strength 3 >> 99%

Noise Strength >> 26

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

The screenshot shows the RaUI interface with the 'Network' tab selected. The 'AP List' is sorted by Signal strength. Below the list, the 'Auth. \ Encry.' dialog is open, showing 'WPA-PSK' authentication and 'AES' encryption. The dialog also includes a 'Wep Key' section with four keys, each set to 'Hexadecimal'.

AP Name	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%
arscadre	1	b g n	99%

Auth. \ Encry. 8021X

Authentication >> WPA-PSK Encryption >> AES

WPA Preshared Key >> [Empty Field]

Wep Key

- Key#1 Hexadecimal [Empty Field]
- Key#2 Hexadecimal [Empty Field]
- Key#3 Hexadecimal [Empty Field]
- Key#4 Hexadecimal [Empty Field]

OK Cancel

3 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 page. At the top, there are navigation tabs: Profile, Network (selected), Advanced, Statistics, WMM, WPS, and Radio On/Off. Below the tabs, there are sorting options: Sorted by >> SSID, Channel, Signal, and a Show checkbox. The main area displays an AP List with columns for SSID, Channel, Encryption, Signal, and a signal strength bar. The AP list includes entries like 0148-1, 11n, 132, 202, 219, 243, 99, \_Shiang\_2860AP, AP1, and arscadre. The 'arscadre' AP is selected, showing 100% signal strength and WPA-PSK encryption. Below the AP list, there are buttons for Rescan, Add to Profile, and Connect. The bottom section shows the configuration for the selected AP, with 'Auth. \ Encry.' set to '8021X'. The Authentication type is set to WPA-PSK and the Encryption type is set to AES. The WPA Preshared Key is entered as 12345678. There are also sections for Wep Key configuration with four keys, each set to Hexadecimal, and OK/Cancel buttons at the bottom.

SSID	Channel	Encryption	Signal	Signal Strength
0148-1	60	a	20%	Low
11n	1	b g n	50%	Medium
132	2	b g	60%	Medium-High
202	1	b g	60%	Medium-High
219	1	b g	76%	High
243	5	b g	91%	Very High
99	6	b g n	81%	High
_Shiang_2860AP	11	b g n	65%	Medium-High
AP1	6	b g	100%	Maximum
arscadre	1	b g n	99%	Very High

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

4 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.

The screenshot shows the RaUI Network configuration window. The 'Network' tab is active, displaying a list of available APs. The selected AP is 'AP1', which is connected at 100% signal strength. Below the list, the connection status and details are shown, including link quality, signal strength, and network parameters.

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

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-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

Transmit

- Link Quality >> 88%
- Signal Strength 1 >> 4
- Signal Strength 2 >> 10
- Signal Strength 3 >> C
- Noise Strength >> 26
- Link Speed >> 54.0 Mbps
- Throughput >> 0.001 Mbps

Receive

- Link Speed >> 54.0 Mbps
- Throughput >> 0.021 Mbps

Additional Metrics:

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

## Example to Configure Connection with WPA

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

The screenshot shows the RaUI Network configuration page. The 'Network' tab is active. The interface includes a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, and Radio On/Off. Below the navigation bar, there are sorting options for SSID, Channel, and Signal, and a 'Show' checkbox. The main area displays an 'AP List' table with columns for AP ID, Channel, Authentication Mode, Signal Strength, and a visual signal strength bar. The 'AP1' entry is highlighted in blue. Below the table are buttons for 'Rescan', 'Add to Profile', and 'Connect'. The bottom section shows connection status and various configuration options for the selected AP.

AP ID	Channel	Auth Mode	Signal	Visual Bar
223	11	b g	65%	[Bar]
240	11	b g n	91%	[Bar]
243	4	b g	29%	[Bar]
99	6	b g n	91%	[Bar]
_Shiang_2860AP	11	b g n	91%	[Bar]
Ap-03	11	b g	70%	[Bar]
<b>AP1</b>	<b>6</b>	<b>b g</b>	<b>100%</b>	[Bar]
AP47-g	1	b g	29%	[Bar]
arscadre	1	b g n	100%	[Bar]
arvint-2860AP	7	b g n	86%	[Bar]

Buttons: Rescan, Add to Profile, Connect

Status: Disconnected

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

HT

BW, GI, SNR0, MCS, SNR1

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

The screenshot shows the RaUI Network interface. At the top, there are navigation tabs: Profile, Network (selected), Advanced, Statistics, WMM, WPS, and Radio On/. Below the tabs, there are sorting options: Sorted by >> SSID, Channel, Signal, and a Show checkbox. The main area displays an 'AP List >>' table with columns for SSID, Channel, Security, Signal, and a signal strength bar.

SSID	Channel	Security	Signal	Strength
240	11	b g n	91%	High
243	4	b g	15%	Low
99	6	b g n	91%	High
_Shiang_2860AP	11	b g n	96%	High
Ap-03	11	b g	70%	Medium
AP1	6	b g	100%	Max
AP47-g	1	b g	24%	Low
arscadre	1	b g n	91%	High
arvint-2860AP	7	b g n	91%	High
Broadcom	11	b g	76%	Medium

Below the table are buttons for Rescan, Add to Profile, and Connect. A dialog box titled 'Auth. \ Encry.' is open, showing '8021X' as the selected mode. The Authentication is set to WPA and Encryption to AES. There is a field for WPA Preshared Key and a section for Wep Key with four keys, each set to Hexadecimal. The dialog has OK and Cancel buttons.

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

The screenshot shows the RaUI interface with the Network tab selected. The AP List table is as follows:

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

Below the AP list, the 802.1X authentication dialog is open. The 'Auth. \ Encry.' tab is selected, and the '8021X' sub-tab is active. The EAP Method is set to PEAP, and Tunnel Authentication is set to EAP-MSCHAP v2. The 'ID \ PASSWORD' sub-tab is selected, showing fields for Identity and Password for both Authentication and Tunnel ID.



#### 4 Authentication type and setting method :

PEAP :

1. 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.

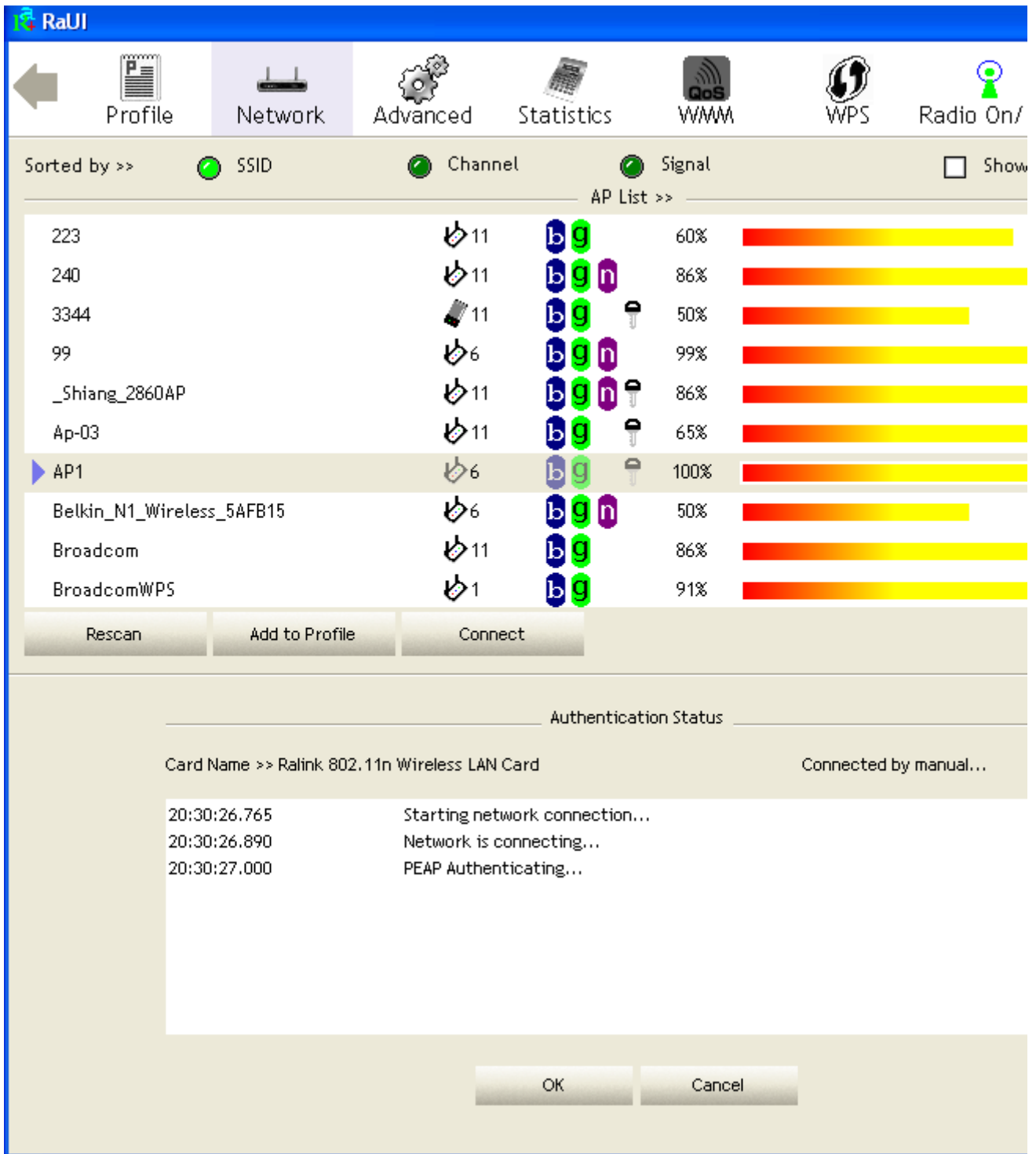
The screenshot shows the RaUI interface with the Network tab selected. The AP List table is as follows:

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

Below the AP list, the authentication settings are configured as follows:

- Auth. \ Encry.: 8021X
- EAP Method: PEAP
- Tunnel Authentication: EAP-MSCHAP v2
- Authentication ID / Password:
  - Identity: wpatest2
  - Password: [empty]
  - Domain Name: [empty]
- Tunnel ID / Password:
  - Identity: wpatest2
  - Password: test2

2. 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.

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

The screenshot displays the RaUI Network interface. At the top, there are navigation tabs: Profile, Network (selected), Advanced, Statistics, WMM, WPS, and Radio On/Off. Below the tabs, there are sorting options for SSID, Channel, and Signal, and a 'Show' checkbox. The main area is titled 'AP List >>' and contains a table of detected APs. The selected AP, 'AP1', is highlighted in blue. Below the table, there are three buttons: 'Rescan', 'Add to Profile', and 'Connect'. The bottom section shows detailed connection information for 'AP1' (MAC: 00-03-7F-00-D7-A4), including link status, channel, authentication, encryption, network type, IP address, and throughput statistics for both transmit and receive directions.

AP ID	Channel	Mode	Signal	Strength
202	1	bg	81%	[Bar]
213	11	bg	60%	[Bar]
219	1	bg	76%	[Bar]
223	11	bg	44%	[Bar]
240	11	bg n	86%	[Bar]
99	6	bg n	99%	[Bar]
_Shiang_2860AP	11	bg n	81%	[Bar]
Ap-03	11	bg	65%	[Bar]
<b>AP1</b>	<b>6</b>	<b>bg</b>	<b>100%</b>	<b>[Bar]</b>
arscadre	1	bg n	100%	[Bar]

**AP1 Connection Details:**

- 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

**Transmit Statistics:**

- 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 Statistics:**

- Link Speed >> 54.0 Mbps
- Throughput >> 57.148 Kbps

**Other Metrics:**

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

## TLS / Smart Card :

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

The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by Signal strength. Below the AP list, the authentication settings are configured for TLS/SmartCard.

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

Auth. \ Encry. 8021X

EAP Method >> TLS/SmartCard

Client Certification

Authentication ID / Password

Identity >> wpatest2

Password >> [ ]

Domain Name >> [ ]

Tunnel ID / Password

Identity >> [ ]

Password >> [ ]

OK Cancel

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

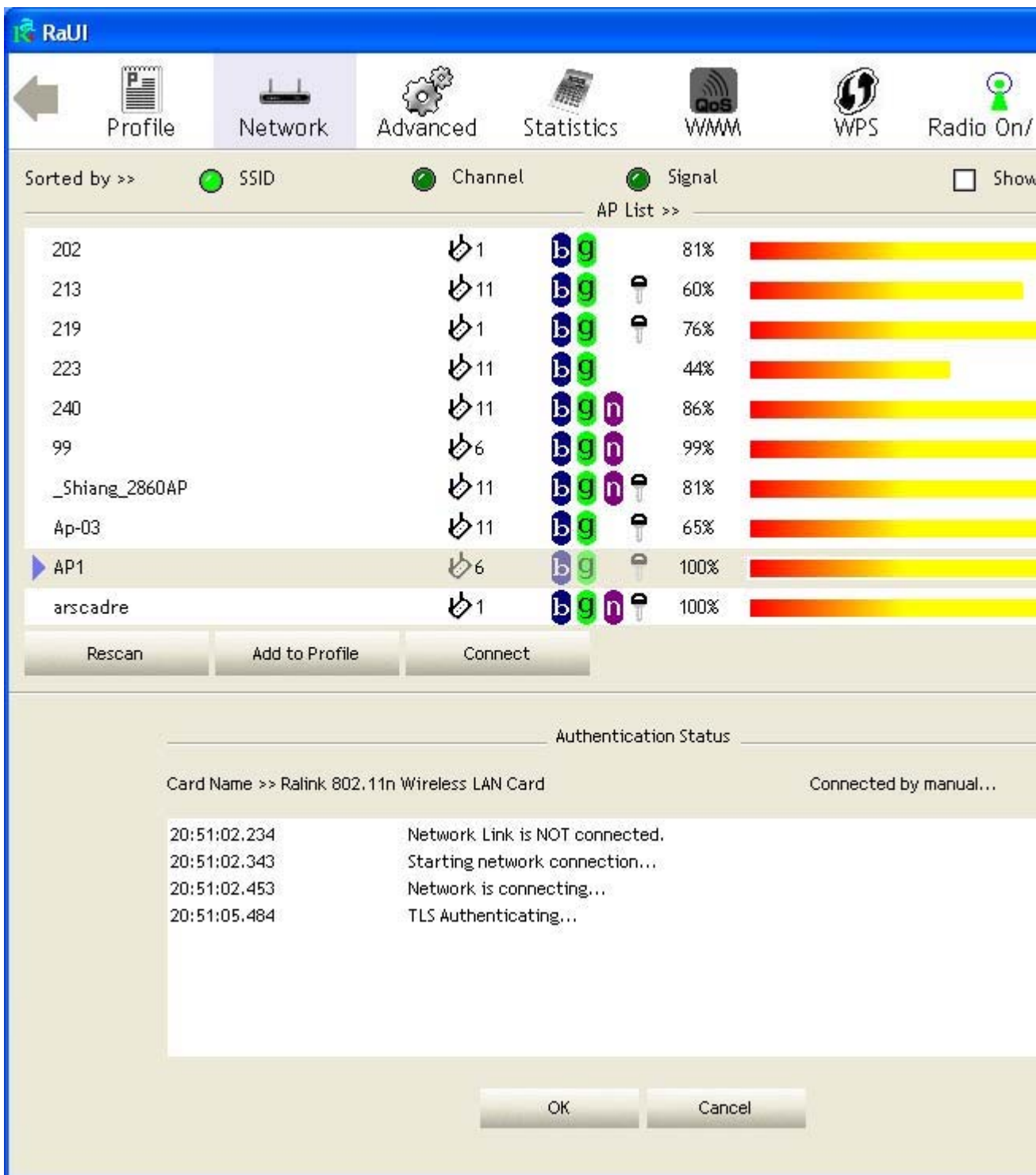
The screenshot shows the RaUI interface with the Network tab selected. The AP List is sorted by SSID, Channel, and Signal. Below the list, the Client Certification dialog is open, showing the 'Client Certification' tab selected. The dialog includes a table of certificates and fields for 'Issued To', 'Issued By', 'Expired On', and 'Friendly Name'.

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

ID \ PASSWORD	Client Certification	Server Certification
<input checked="" type="checkbox"/> Use Client certificate	wpatest2   2003serv   4/9/2008	
	Issued To >> wpatest2	
	Issued By >> 2003serv	
	Expired On >> 4/9/2008	
	Friendly Name >>	

3. 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.

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

The screenshot displays the RaUI interface with the 'Network' tab selected. The 'AP List' table shows various access points, with 'AP1' selected. Below the table, the status and configuration for 'AP1' are detailed, including link quality, signal strength, and network parameters.

AP ID	Channel	Mode	Signal	Strength
202	1	bg	81%	81%
213	11	bg	60%	60%
219	1	bg	76%	76%
223	11	bg	44%	44%
240	11	bg n	86%	86%
99	6	bg n	99%	99%
_Shiang_2860AP	11	bg n	81%	81%
Ap-03	11	bg	65%	65%
<b>AP1</b>	<b>6</b>	<b>bg</b>	<b>100%</b>	<b>100%</b>
arscadre	1	bg n	100%	100%

Parameter	Value
Status	AP1 <--> 00-03-7F-00-D7-A4
Extra Info	Link is Up [TxPower:100%]
Channel	6 <--> 2437000 MHz
Authentication	WPA
Encryption	TKIP+AES
Network Type	Infrastructure
IP Address	192.168.5.79
Sub Mask	255.255.255.0
Default Gateway	192.168.5.254
HT	
BW	n/a
SNR0	n/a
GI	n/a
MCS	n/a
SNR1	n/a
Link Quality	89%
Signal Strength 1	10
Signal Strength 2	10
Signal Strength 3	10
Noise Strength	26
Transmit Link Speed	54.0 Mbps
Transmit Throughput	0.000 Kbps
Receive Link Speed	54.0 Mbps
Receive Throughput	57.148 Kbps



TTLS :

1. 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 SSID, Channel, and Signal. Below the list, the authentication settings are configured for TTLS and CHAP.

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

Auth. \ Encry. 8021X

EAP Method >> TTLS Tunnel Authentication >> CHAP

ID \ PASSWORD Client Certification Server Certification

Authentication ID / Password

Identity >> wpatest2 Password >> Domain Name >>

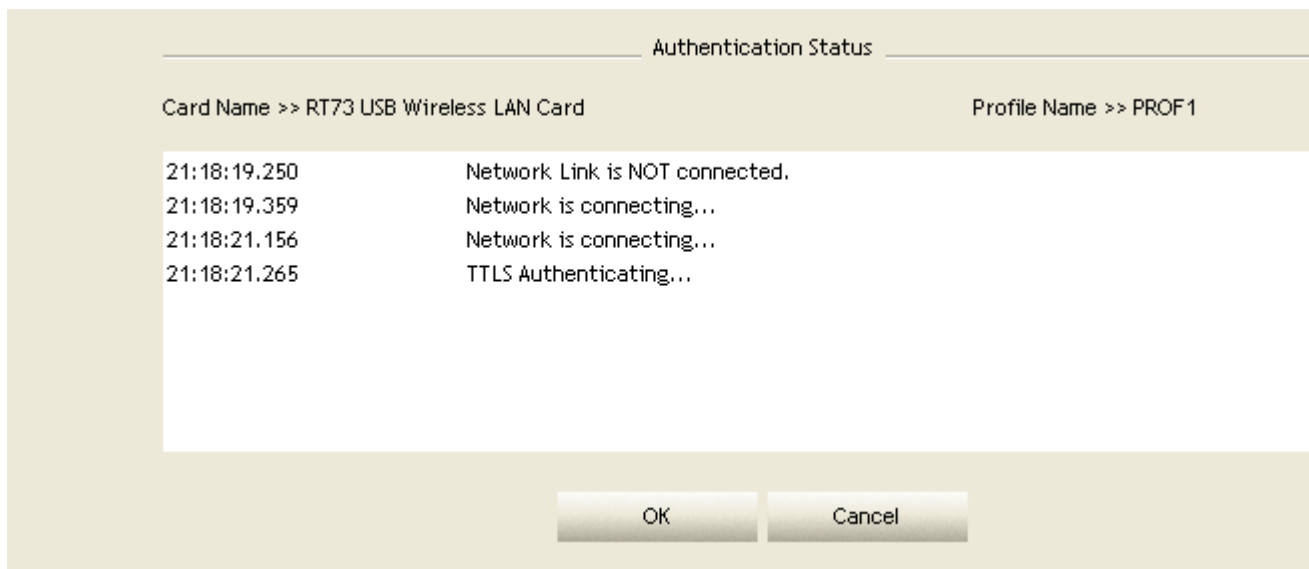
Tunnel ID / Password

Identity >> wpatest2 Password >> test2

OK Cancel



2. 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.

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

The screenshot displays the RaUI interface with the 'Network' tab selected. The 'AP List' table shows various access points, with 'AP1' selected and highlighted. Below the table, the connection status for 'AP1' is detailed, including link quality, signal strength, and network parameters.

AP ID	Channel	Mode	Signal	Strength
202	1	bg	81%	High
213	11	bg	60%	Medium
219	1	bg	76%	High
223	11	bg	44%	Low
240	11	bg n	86%	High
99	6	bg n	99%	Very High
_Shiang_2860AP	11	bg n	81%	High
Ap-03	11	bg	65%	Medium
<b>AP1</b>	<b>6</b>	<b>bg</b>	<b>100%</b>	<b>Very High</b>
arscadre	1	bg n	100%	Very High

**AP1 Connection Details:**

- 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

**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

## EAP-FAST :

1. 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 top navigation bar includes Profile, Network (selected), Advanced, Statistics, WMM, WPS, and Radio On/Off. Below the navigation bar, there are sorting options for SSID, Channel, and Signal, and a 'Show' checkbox. The main area displays an 'AP List' table with columns for AP Name, Channel, SSID, Security, Signal Strength, and a signal strength bar. Below the table are 'Rescan', 'Add to Profile', and 'Connect' buttons. The bottom section is for 'Auth. \ Encry.' settings, currently set to '8021X'. Underneath, 'EAP Method' is set to 'EAP-FAST' and 'Tunnel Authentication' is set to 'Generic Token Card'. A sub-window titled 'ID \ PASSWORD' is open, showing 'EAP Fast' settings. It has two tabs: 'ID \ PASSWORD' (selected) and 'EAP Fast'. The 'Authentication ID / Password' section has 'Identity' set to 'wpatest2', 'Password' empty, and 'Domain Name' empty. The 'Tunnel ID / Password' section has 'Identity' set to 'wpatest2' and 'Password' set to 'test2'. At the bottom, 'Password Mode' has 'Soft Token' and 'Static Password' both selected. 'OK' and 'Cancel' buttons are at the bottom.

AP Name	Channel	SSID	Security	Signal	Signal Bar
	6	bg	Key	50%	50%
	11	bg	Key	50%	50%
132	2	bg	Key	81%	81%
185	6	b	Key	60%	60%
202	1	bg	Key	76%	76%
219	1	bg	Key	76%	76%
240	11	bg n	Key	86%	86%
Ap-03	11	bg	Key	65%	65%
AP1	6	bg	Key	100%	100%
Broadcom	11	bg	Key	76%	76%

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

The screenshot displays the RaUI Network configuration window. The 'Network' tab is active, showing a list of available APs sorted by SSID. The 'AP List' table includes columns for AP Name, Channel, Standards, Security, Signal Strength, and a visual signal bar. Below the list are buttons for 'Rescan', 'Add to Profile', and 'Connect'. The 'Authentication Status' section shows the card name 'Ralink 802.11n Wireless LAN Card' and a log of connection events.

AP Name	Channel	Standards	Security	Signal
Ap-03	11	b g	WPA	55%
AP1	6	b g	WPA	100%
arvint-2860AP	7	b g n	WPA	86%
Broadcom	11	b g	WPA	86%
BroadcomWPS	1	b g	WPA	94%
Cobra	6	b g	WPA	34%
dlink	11	b g n	WPA	86%
jan	6	b g n	WPA	100%
SoftAP-03	1	b g n	WPA	55%
SoftAP-kce	1	b g	WPA	70%

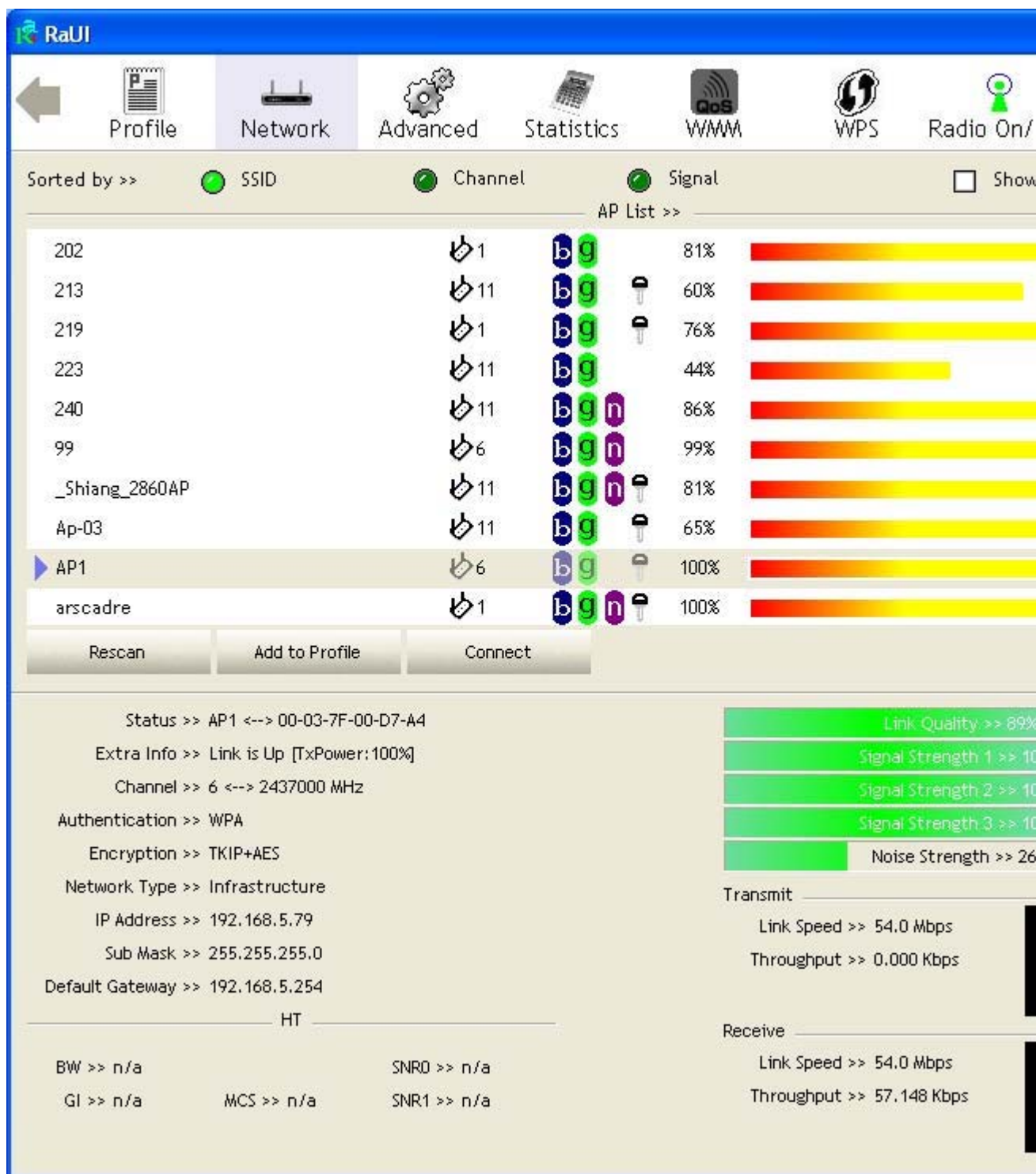
Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card Connected by manual...

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

OK Cancel

3. 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.

## Country Channel List

Country channel list, channel classification and range.

Classification	Range
0:GFCC	CH1 ~ CH11
1:GIC (Canada)	CH1 ~ CH11
2:GETSI	CH1 ~ CH13
3:GSPAIN	CH10 ~ CH11
4:GFRANCE	CH10 ~ CH13
5:GMKK	CH14 ~ CH14
6:GMKKI (TELEC)	CH1 ~ CH14
7:GISRAEL	CH3 ~ CH9

Country Name	Classification	Range
Argentina	0	CH1~11
Australia	1	CH1~13
Austria	1	CH1~13
Bahrain	1	CH1~13
Belarus	1	CH1~13
Belgium	1	CH1~13
Bolivia	1	CH1~13
Brazil	0	CH1~11
Bulgaria	1	CH1~13
Canada	0	CH1~11
Chile	1	CH1~13
China	1	CH1~13
Colombia	0	CH1~11
Costa Rica	1	CH1~13
Croatia	1	CH1~13
Cyprus	1	CH1~13
Czech Republic	1	CH1~13
Denmark	1	CH1~13
Ecuador	1	CH1~13
Egypt	1	CH1~13
Estonia	1	CH1~13
Finland	1	CH1~13
France	3	CH10~13
France2	1	CH1~13
Germany	1	CH1~13
Greece	1	CH1~13

Hong Kong	1	CH1~13
Hungary	1	CH1~13
Iceland	1	CH1~13
India	1	CH1~13
Indonesia	1	CH1~13
Ireland	1	CH1~13
Israel	6	CH3~9
Italy	1	CH1~13
Japan	5	CH1~14
Japan2	4	CH14~14
Japan3	1	CH1~13
Jordan	3	CH10~13
Kuwait	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1~13
Luxembourg	1	CH1~13
Macedonia	1	CH1~13
Malaysia	1	CH1~13
Mexico	0	CH1~11
Morocco	1	CH1~13
Netherlands	1	CH1~13
New Zealand	1	CH1~13
Nigeria	1	CH1~13
Norway	1	CH1~13
Panama	1	CH1~13
Paraguay	1	CH1~13
Peru	1	CH1~13
Philippines	1	CH1~13
Poland	1	CH1~13
Portugal	1	CH1~13
Puerto Rico	1	CH1~13
Romania	1	CH1~13
Russia	1	CH1~13
Saudi Arabia	1	CH1~13
Singapore	1	CH1~13
Slovakia	1	CH1~13
Slovenia	1	CH1~13
South Africa	1	CH1~13

South Korea	1	CH1~13
Spain	2	CH10~11
Sweden	1	CH1~13
Switzerland	1	CH1~13
Taiwan	0	CH1~11
Thailand	1	CH1~13
Turkey	1	CH1~13
United Arab Emirates	1	CH1~13
United Kingdom	1	CH1~13
United States of America	0	CH1~11
Uruguay	1	CH1~13
Venezuela	1	CH1~13
Yugoslavia	0	CH1~11

## 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 (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).



## FCC INFORMATION

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on , the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval Form loopcomm technology. Modification could void authority to use this equipment.