Wireless LAN PCI Card

User Manual V1.1

Content

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 802.1b/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 became 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.

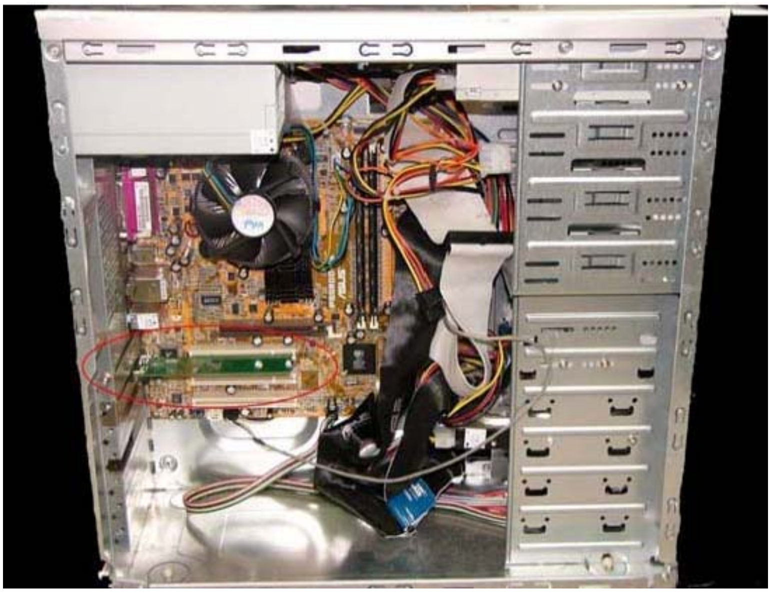
Specifications

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

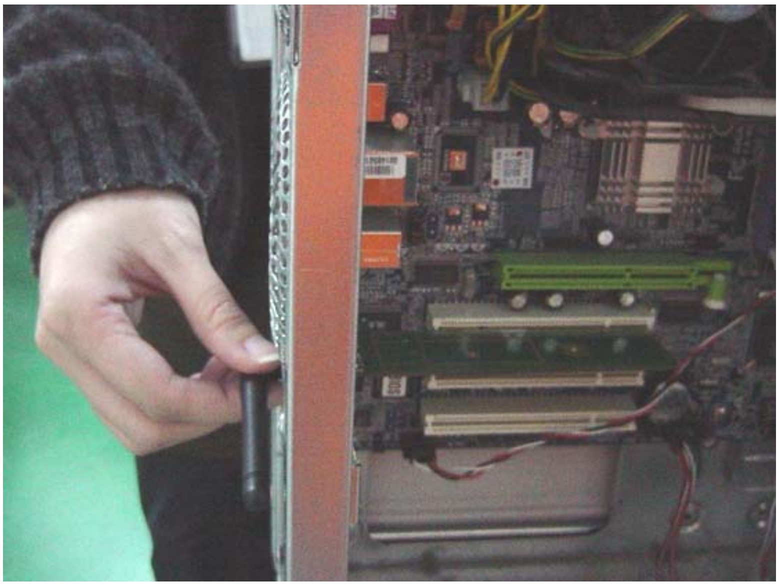
Installation

Hardware Installation

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

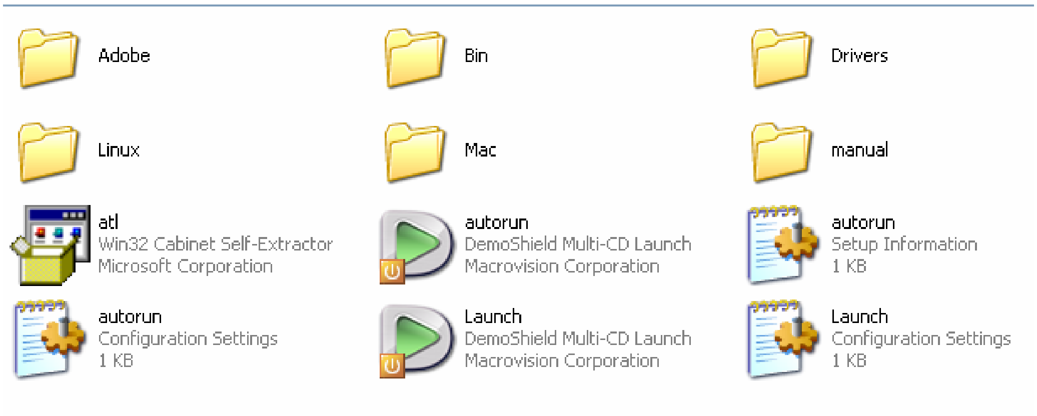


Install antenna to your Wireless LAN PCI Card as picture below.

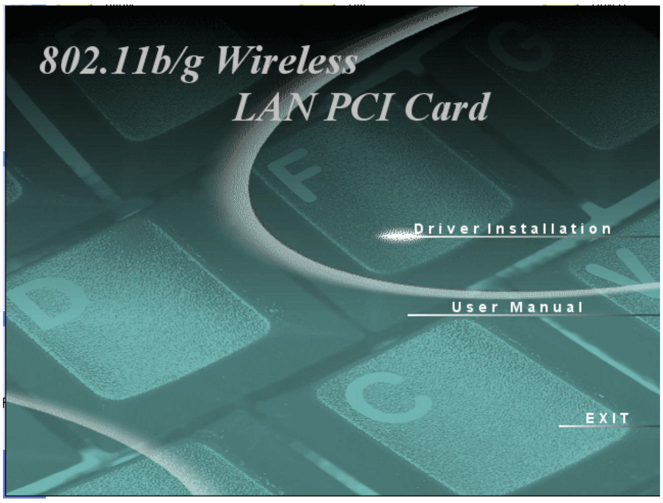


Software Installation

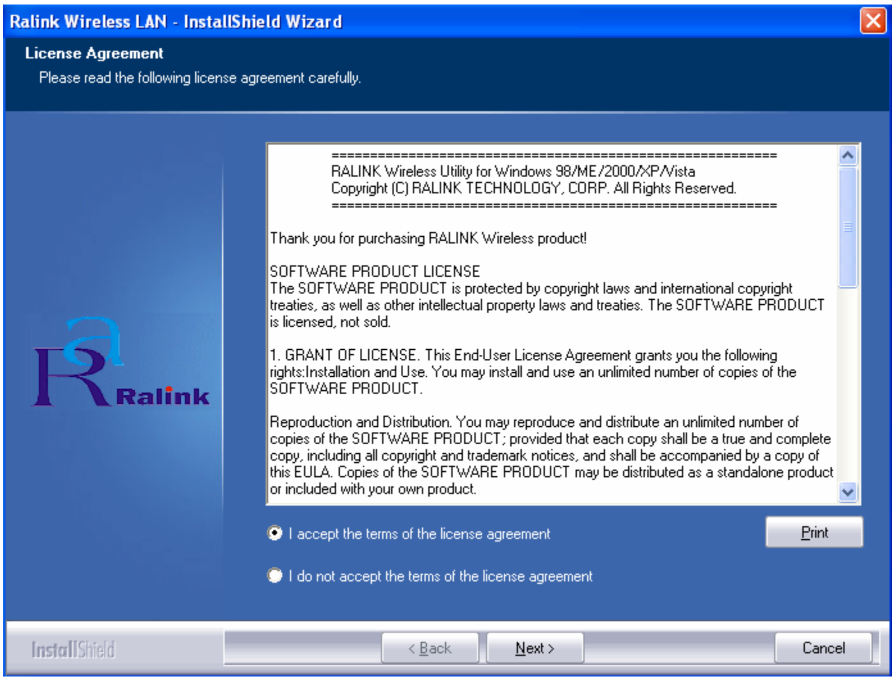
Click My Computer icon, then click DVD, then click autorun



Click Driver Installation



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


Ralink Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Ralink

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

Thank you for purchasing RALINK Wireless product!

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

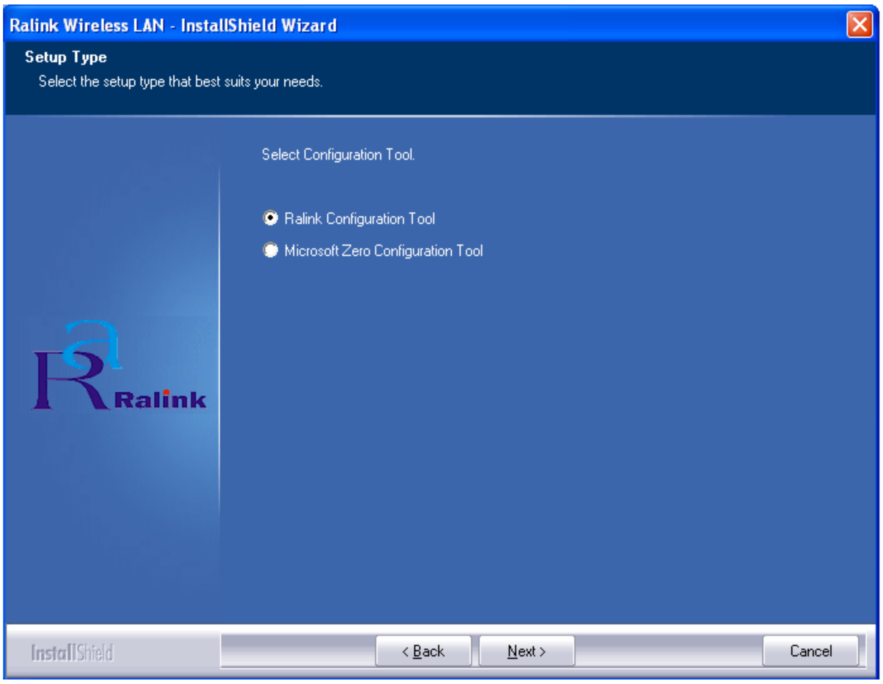
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

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

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Click Ralink Configuration Tool, then click Next icon.



Ralink Wireless LAN - InstallShield Wizard

Setup Type

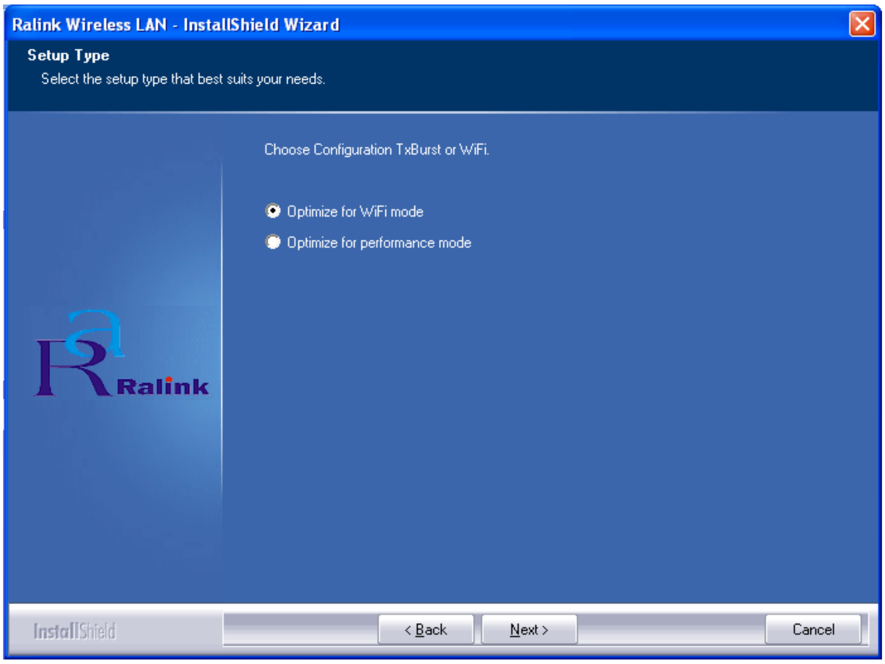
Select the setup type that best suits your needs.

Select Configuration Tool.

● Ralink Configuration Tool

○ Microsoft Zero Configuration Tool

Click Optimize for WiFi modes, then click Next icon.



Ralink Wireless LAN - InstallShield Wizard

Setup Type

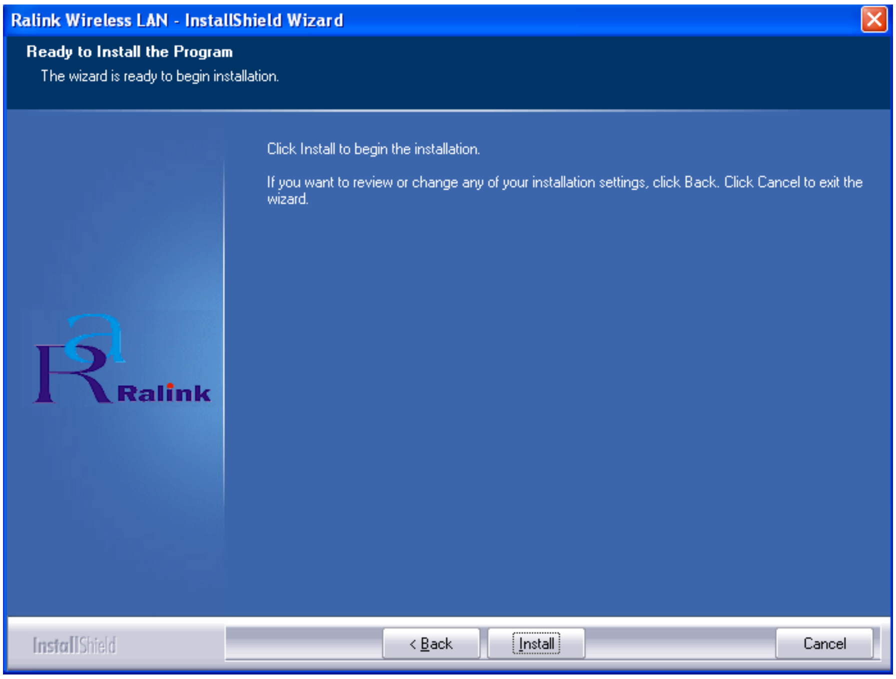
Select the setup type that best suits your needs.

Choose Configuration TxBurst or WiFi.

● Optimize for WiFi mode

○ Optimize for performance mode

Click Install icon.



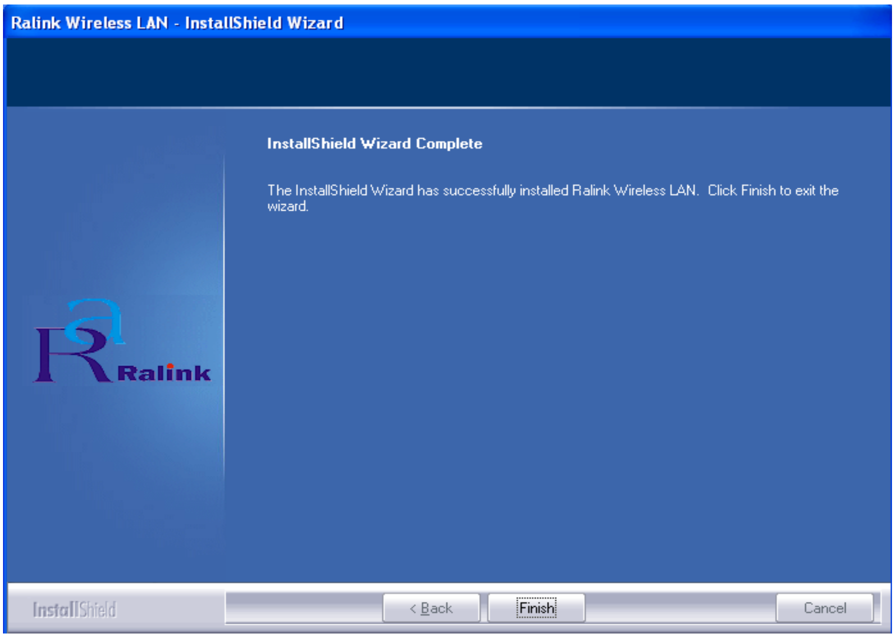
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Click Finish icon.

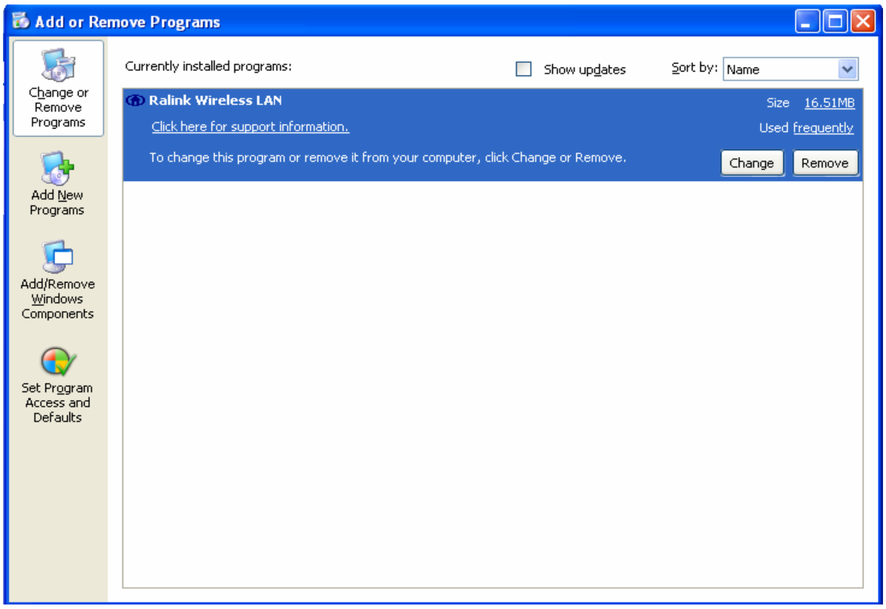


InstallShield Wizard Complete

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

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.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Change
Remove

Currently installed programs:

□ Show updates

Sort by: Name

Ralink Wireless LAN

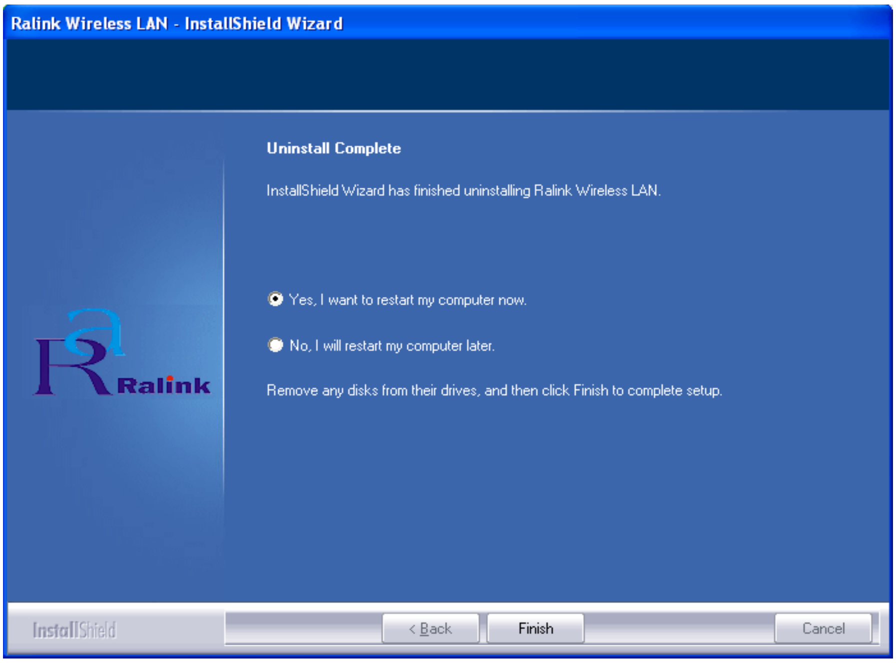
Size 16.51MB

Click here for support information.

Used frequently

To change this program or remove it from your computer, click Change or Remove.

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



Uninstall Complete

InstallShield Wizard has finished uninstalling Ralink Wireless LAN.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

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.

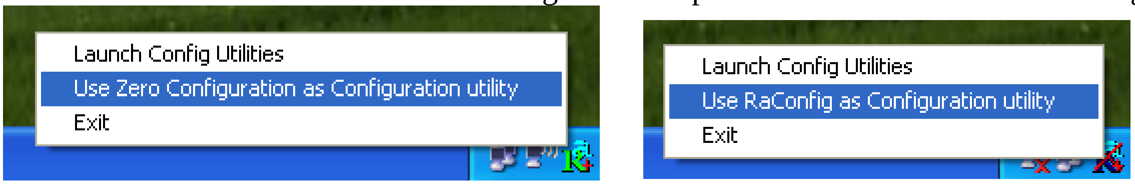
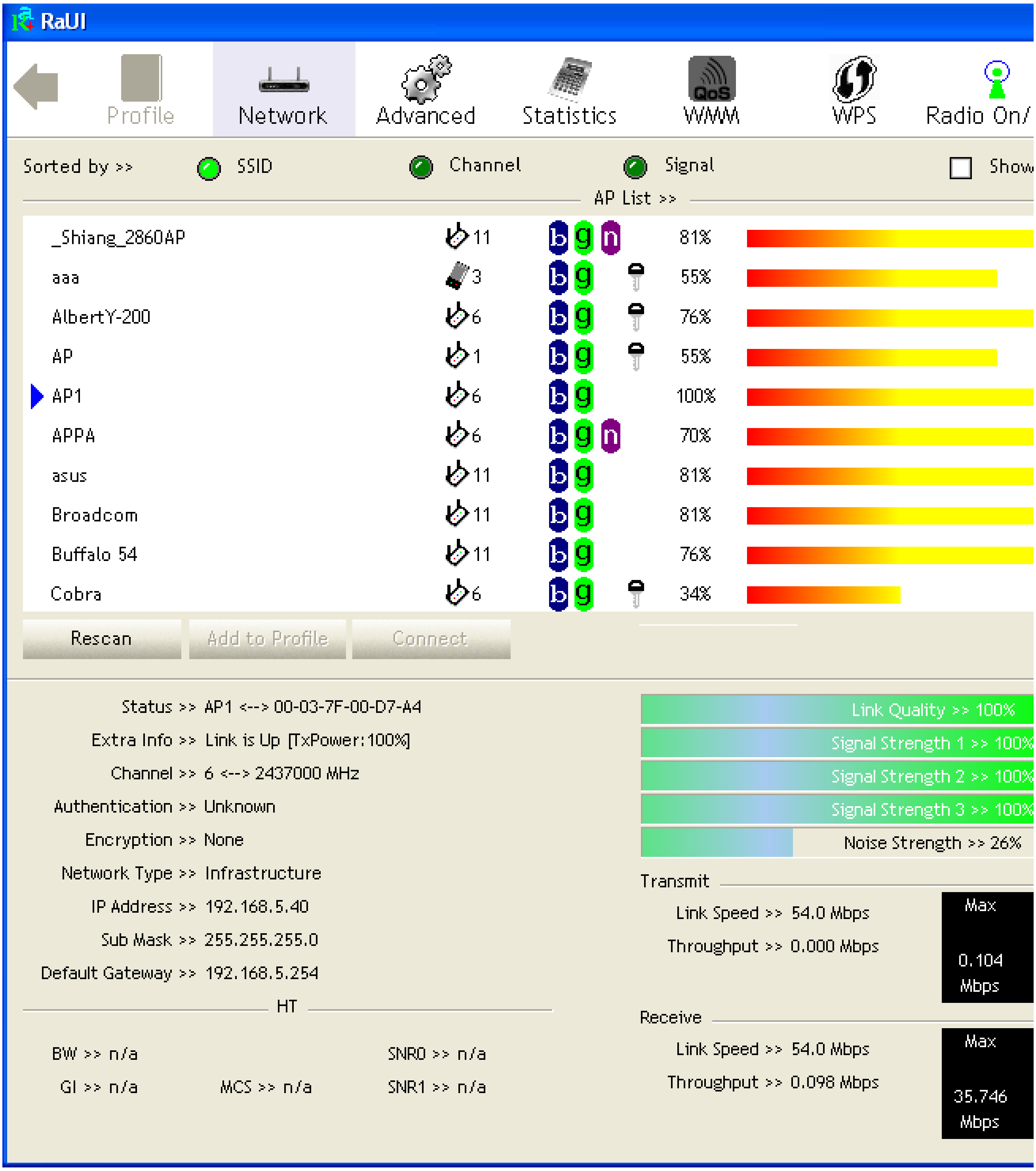

Launch Config Utilities
Use Zero Configuration as Configuration utility
Exit
Launch Config Utilities
Use RaConfig as Configuration utility
Exit

Figure 1-2 Select WZC or RaUI

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

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



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

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

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

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

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

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

Figure 1-3 RaUI status with WZC active

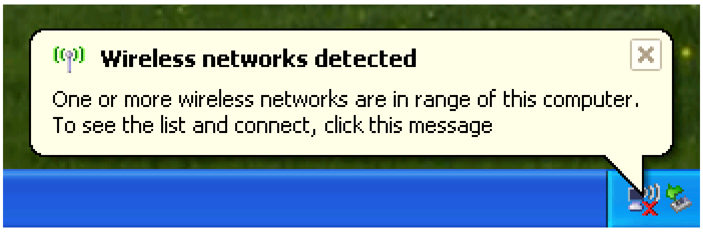
When activating WZC, there are couple difference on RaUI status compared to that with out WZC running.

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

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

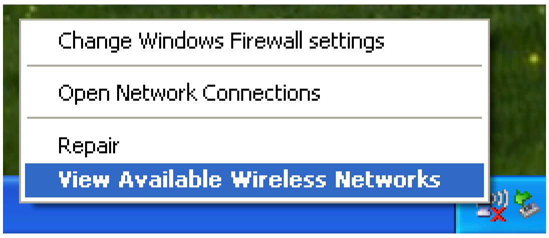


Wireless networks detected

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

Figure 1-4 status prompt of no connection

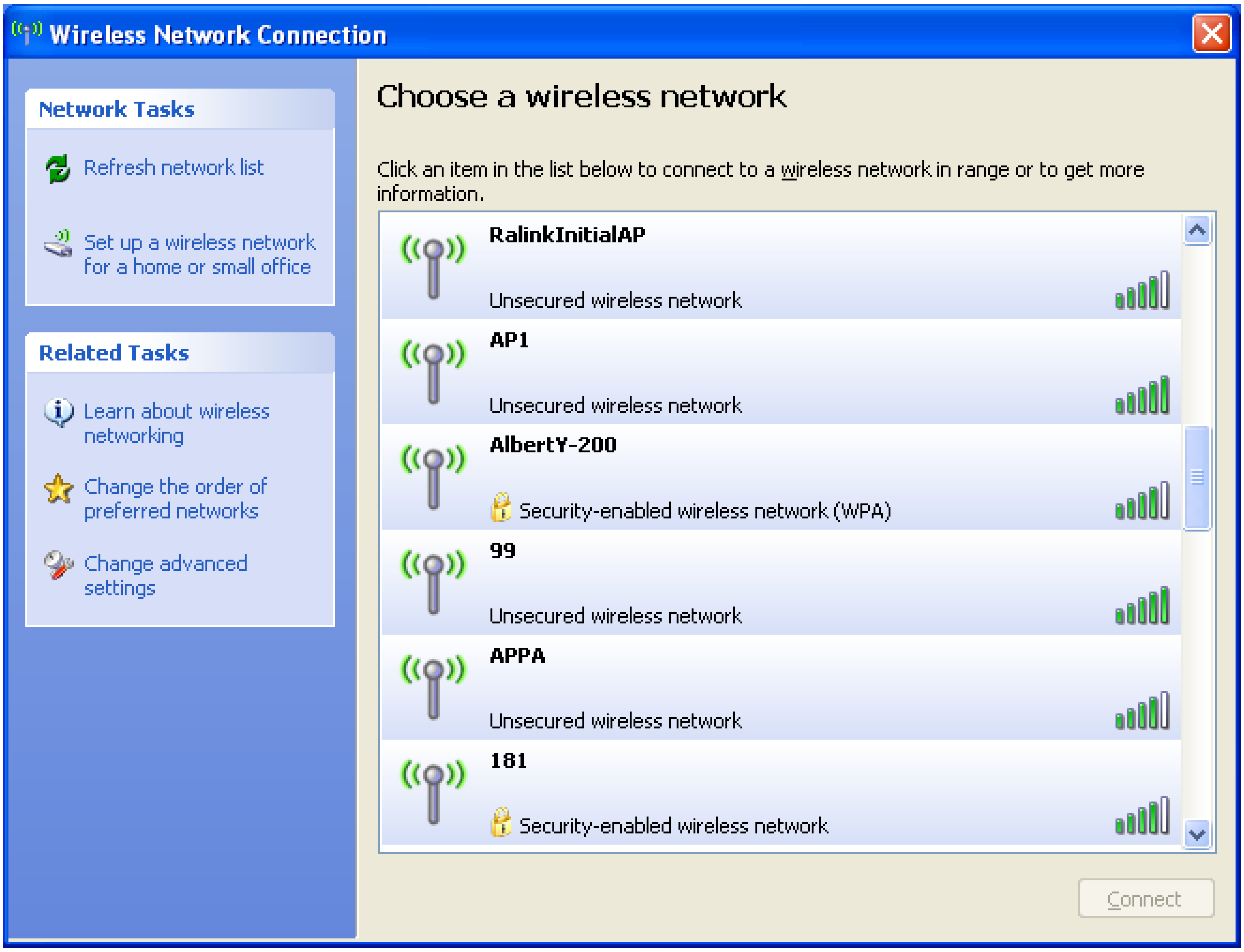
❷ Right-click the network connection icon in task bar.



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

Figure 1-5 Select WZC main status

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


Wireless Network Connection

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

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

RalinkInitialAP
Unsecured wireless network

AP1
Unsecured wireless network

AlbertY-200
Security-enabled wireless network (WPA)

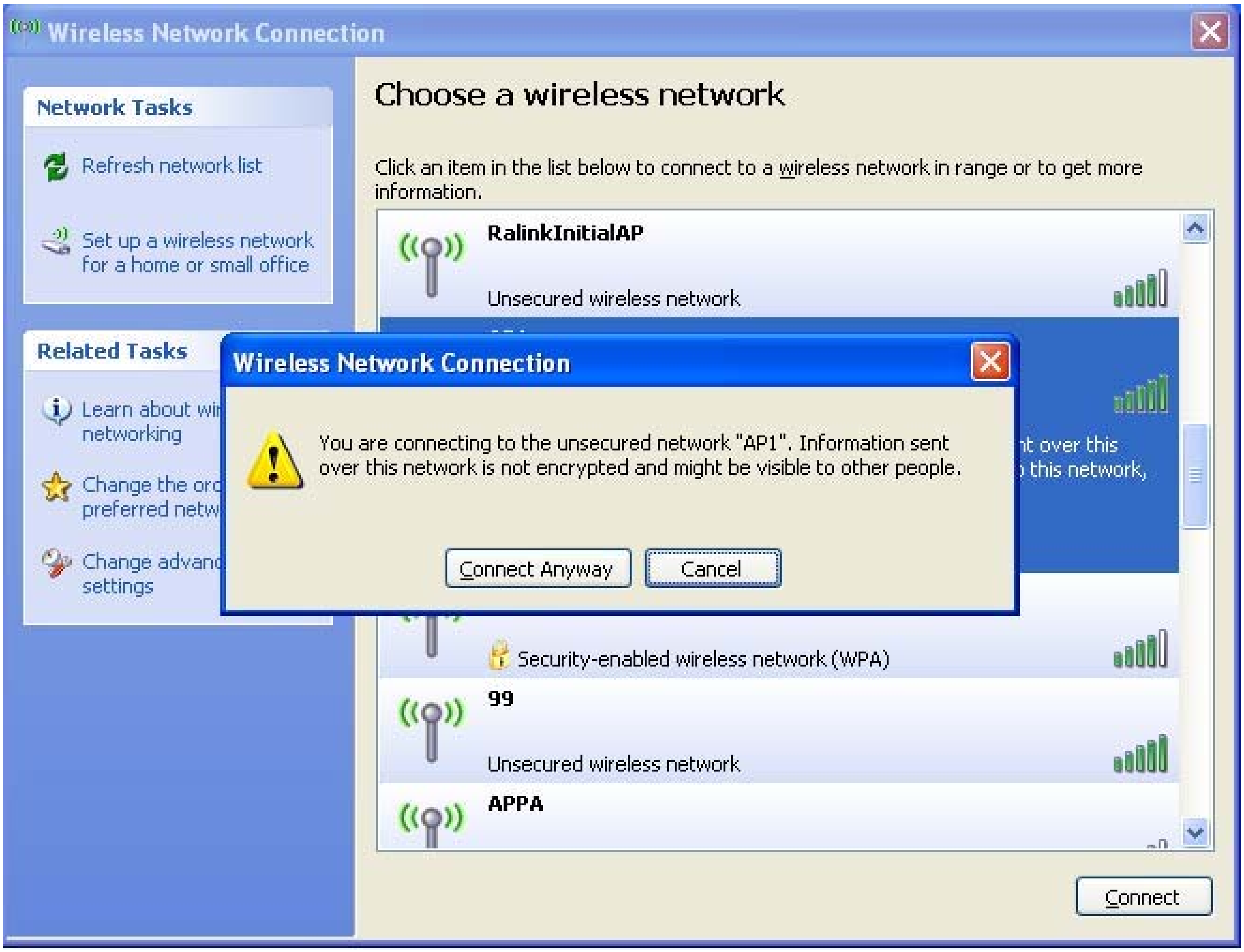
99
Unsecured wireless network

APPA
Unsecured wireless network

181
Security-enabled wireless network

Figure 1-6 Wireless Network Connection

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



Wireless Network Connection

Choose a wireless network

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

RalinkInitialAP

Unsecured wireless network

Security-enabled wireless network (WPA)

99

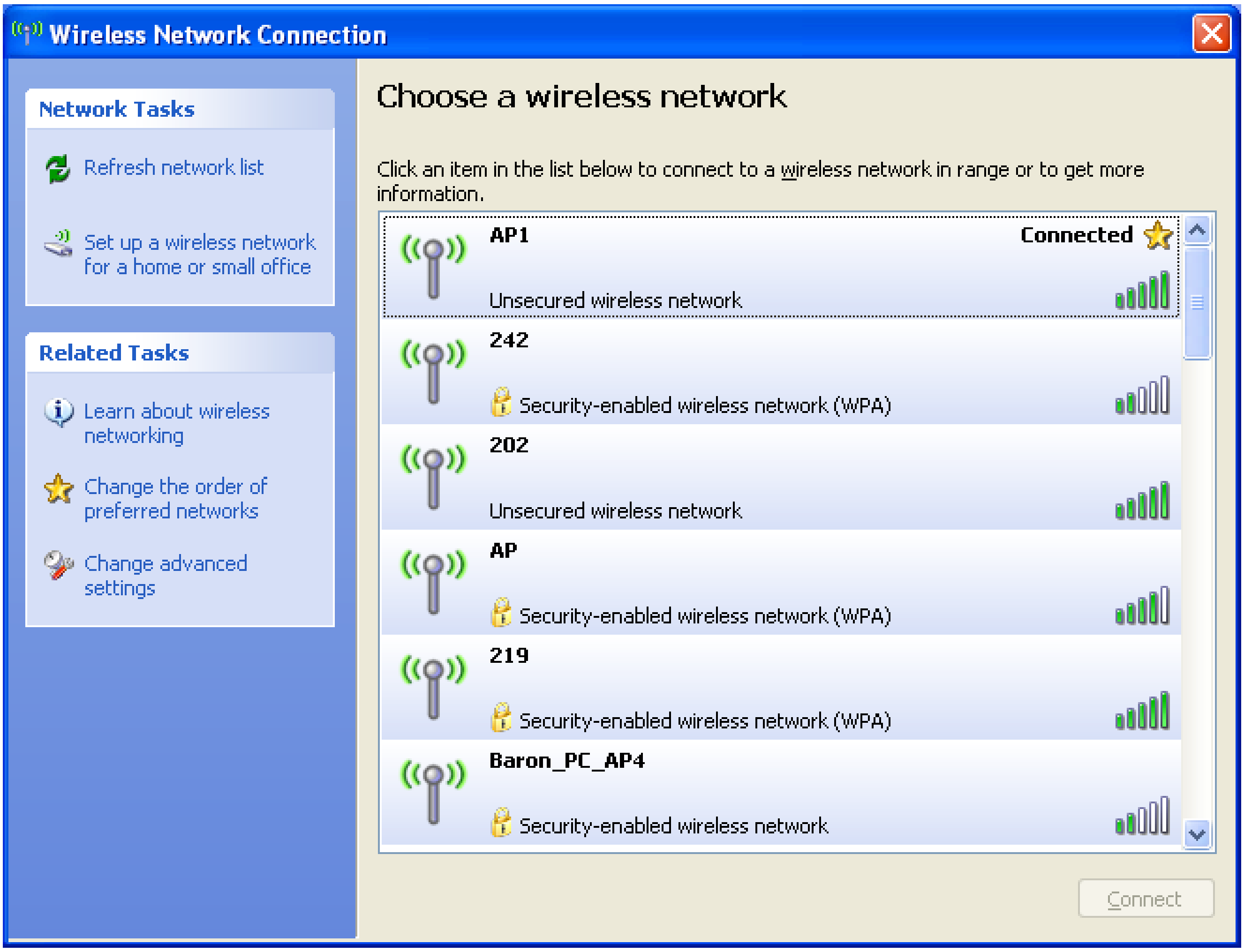
Unsecured wireless network

APPA

Wireless Network Connection

You are connecting to the unsecured network "AP1". Information sent over this network is not encrypted and might be visible to other people.

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



Wireless Network Connection

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

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

AP1 — Connected — Unsecured wireless network

242 — Security-enabled wireless network (WPA)

202 — Unsecured wireless network

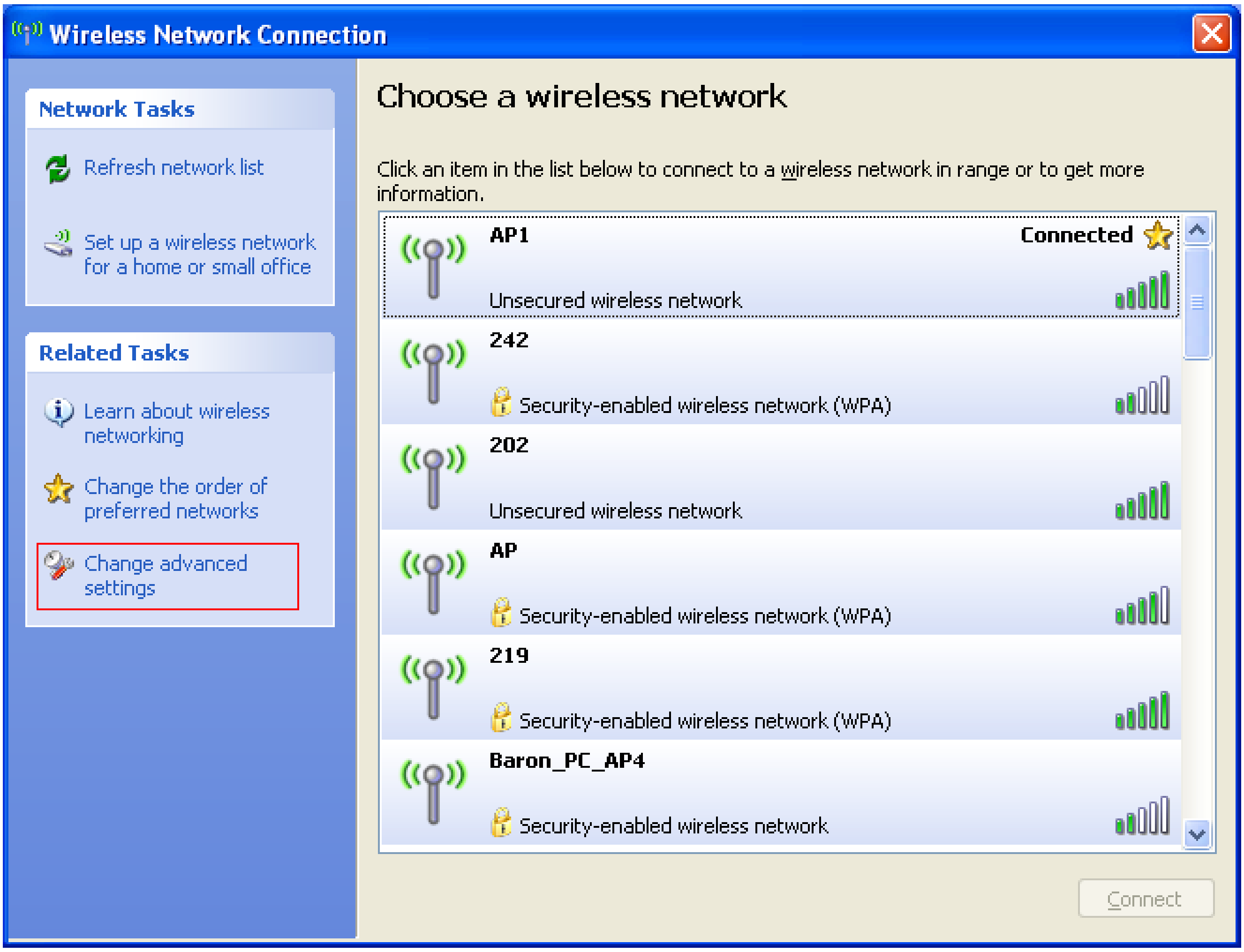
AP — Security-enabled wireless network (WPA)

219 — Security-enabled wireless network (WPA)

Baron_PC_AP4 — Security-enabled wireless network

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.



Wireless Network Connection

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

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

AP1 — Connected ☆ — Unsecured wireless network

242 — Security-enabled wireless network (WPA)

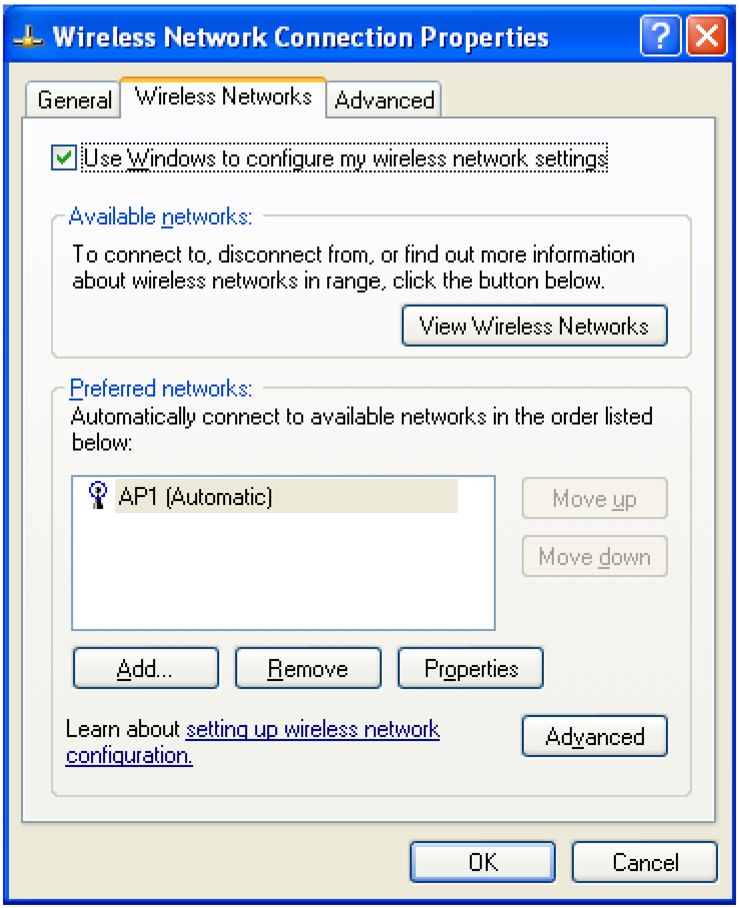
202 — Unsecured wireless network

AP — Security-enabled wireless network (WPA)

219 — Security-enabled wireless network (WPA)

Baron_PC_AP4 — Security-enabled wireless network

Figure 1-9 Click "Change advanced settings"



Wireless Network Connection Properties

☑ Use Windows to configure my wireless network settings

Available networks:

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

Preferred networks:

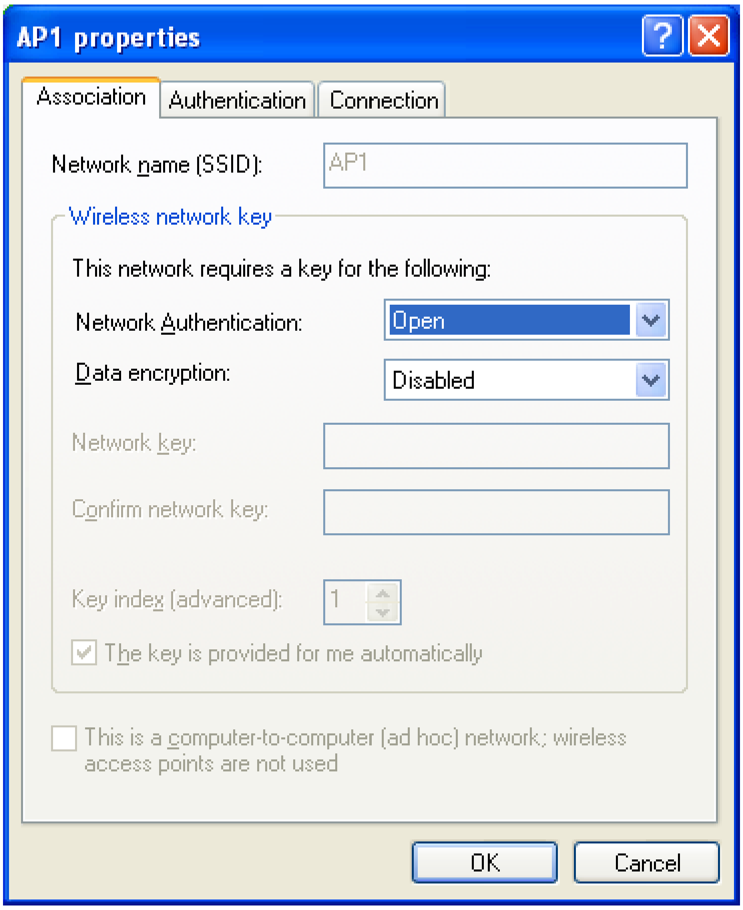
Automatically connect to available networks in the order listed below:

AP1 (Automatic)

Learn about setting up wireless network configuration.

Figure 1-10 Choose "Wireless Networks" label

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



AP1 properties

Association | Authentication | Connection

Network name (SSID): AP1

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key:

Confirm network key:

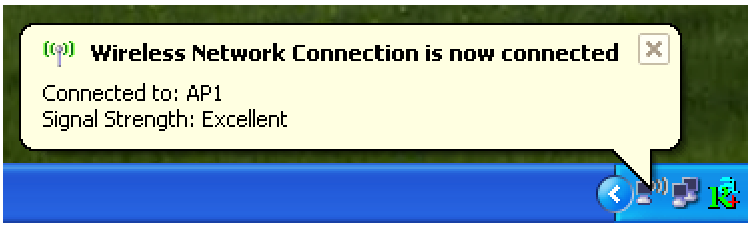
Key index (advanced): 1

☑ The key is provided for me automatically

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

Figure 1-11 AP's properties

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



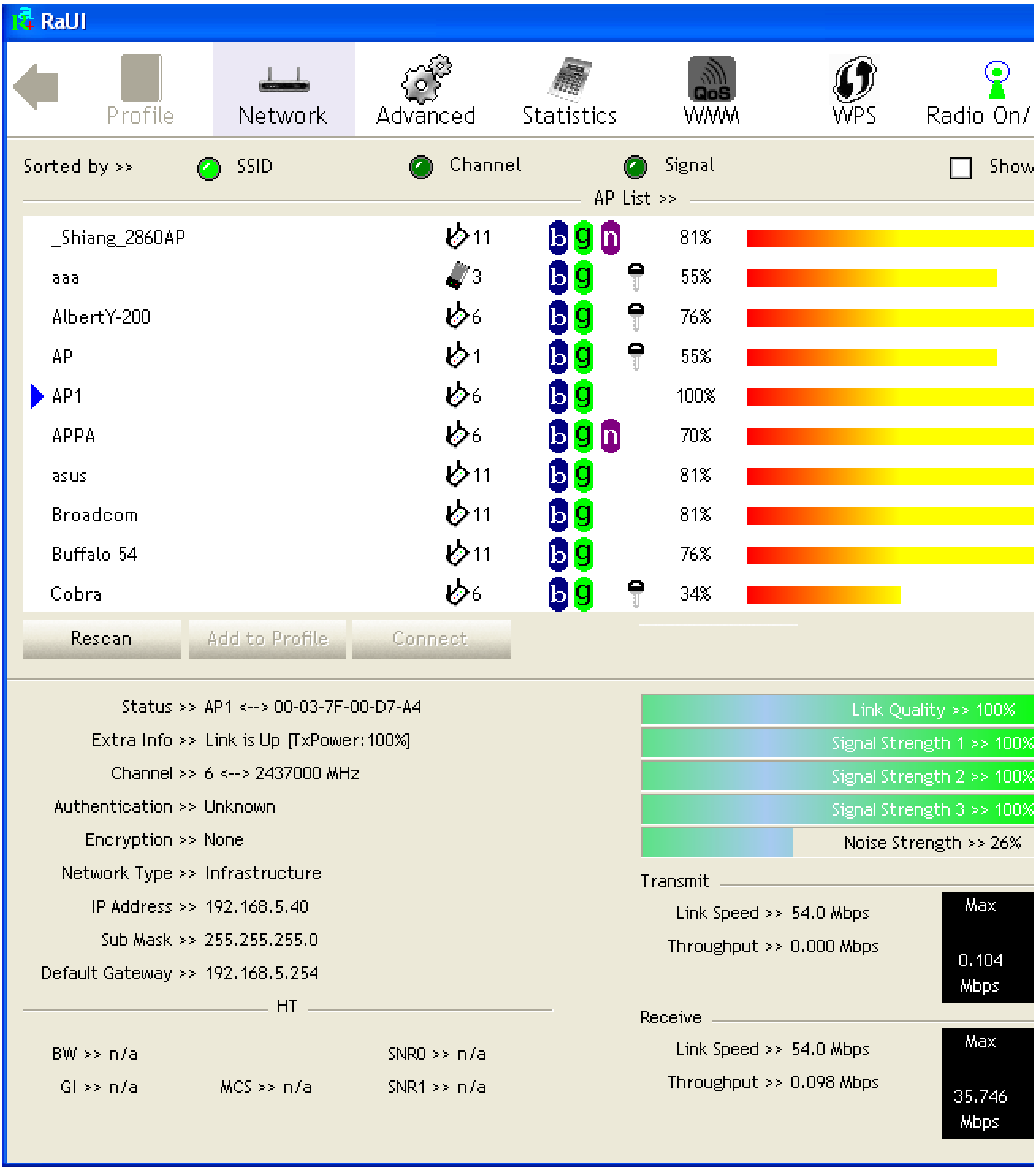
Wireless Network Connection is now connected

Connected to: AP1

Signal Strength: Excellent

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.



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

AP List >>

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

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.40

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Max

0.104 Mbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.098 Mbps

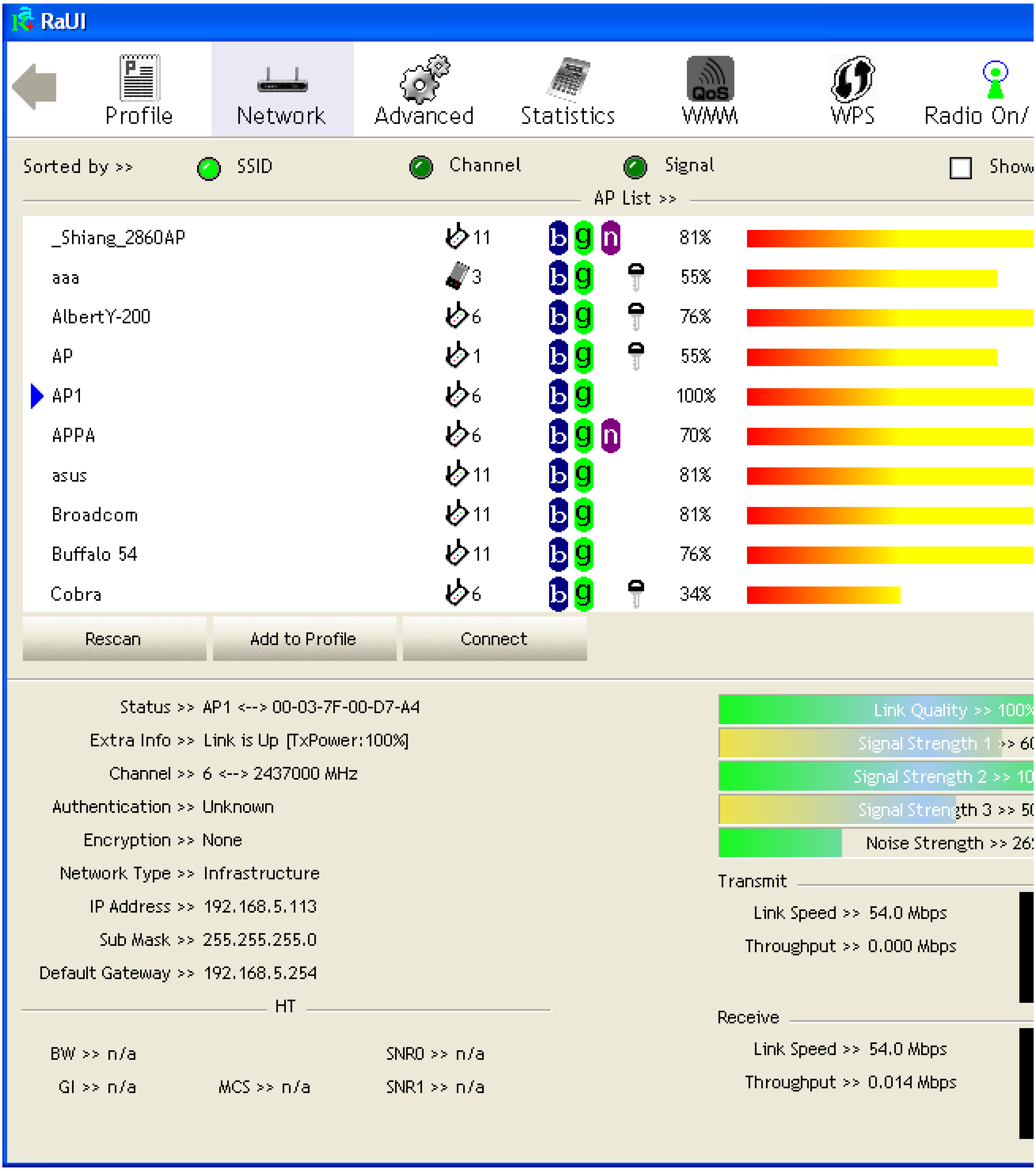
Max

35.746 Mbps

Figure 1-13 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.



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

AP List >>

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

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.113
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

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

Link Quality >> 100%
Signal Strength 1 >> 6(
Signal Strength 2 >> 10
Signal Strength 3 >> 5(
Noise Strength >> 26:

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

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

Figure 2-1-1 RaUI section introduction

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

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

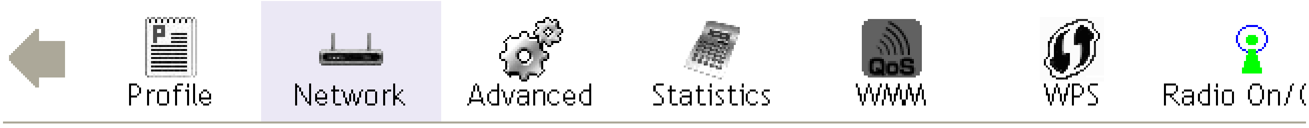


Figure 2-1-2 Button section

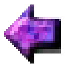


Figure 2-1-3 Move to the left

Figure 2-1-4 Move to the right

❷ Function Section : Corresponding button.

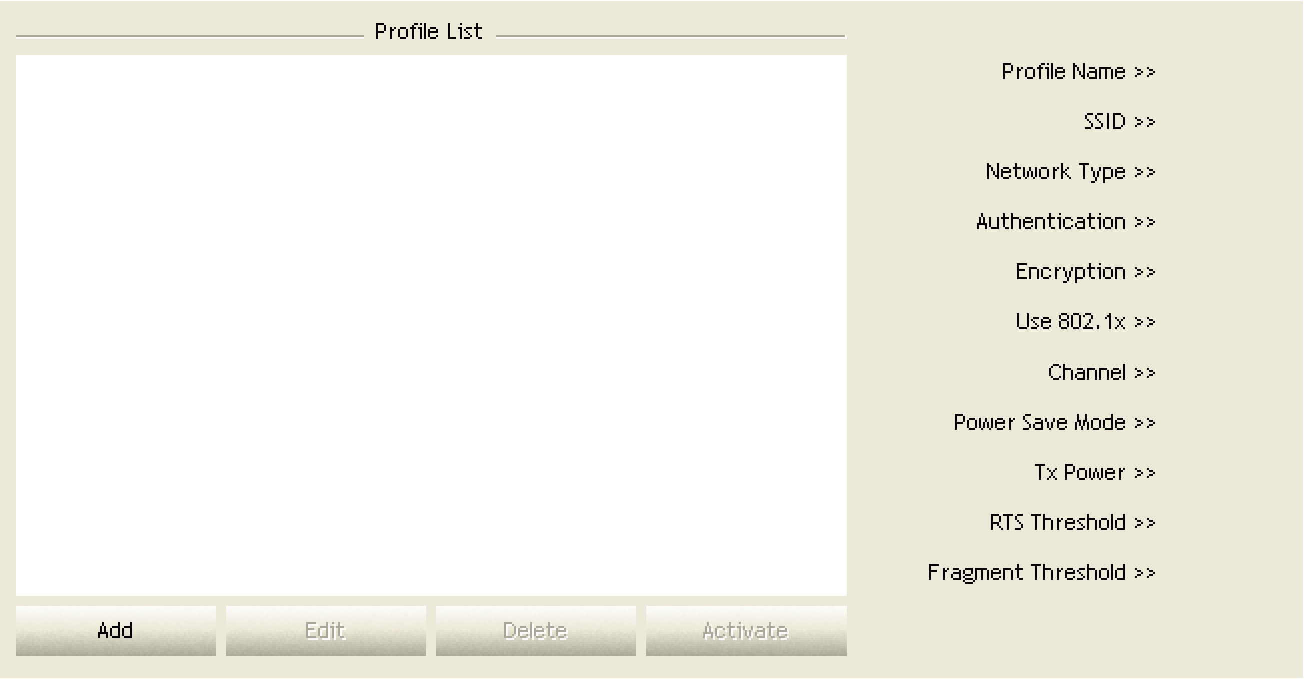
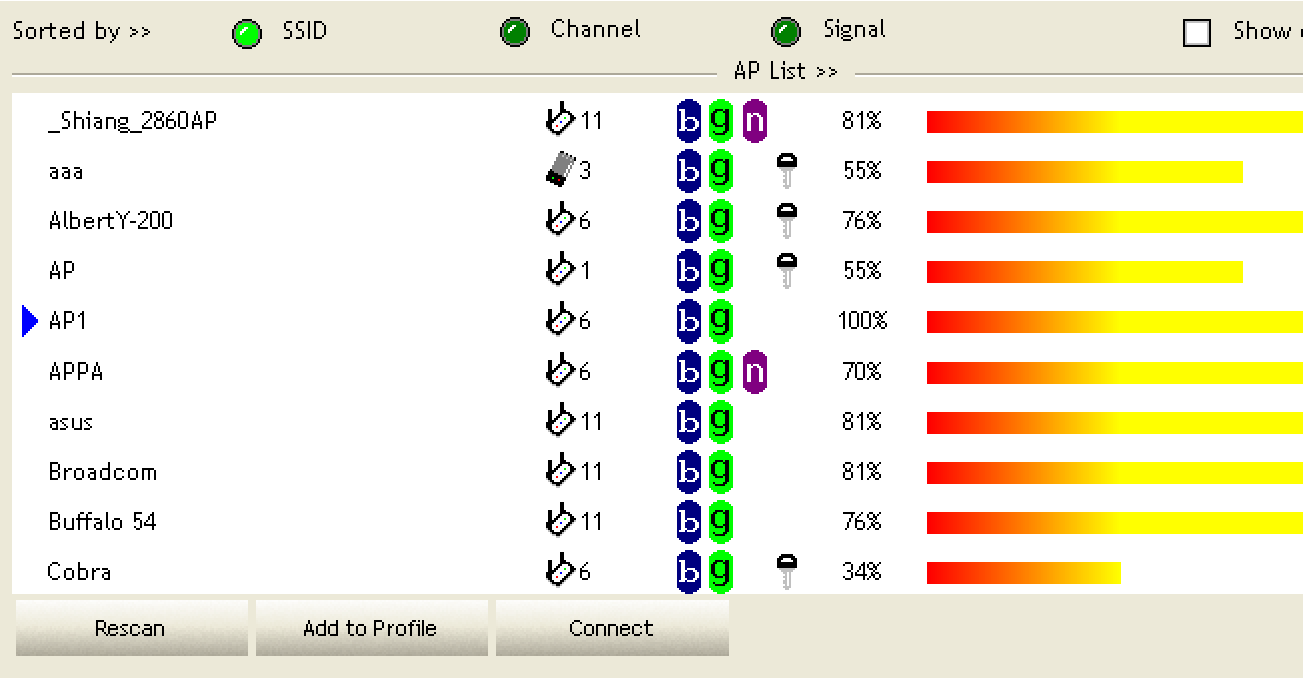


Figure 2-1-5 Profile page

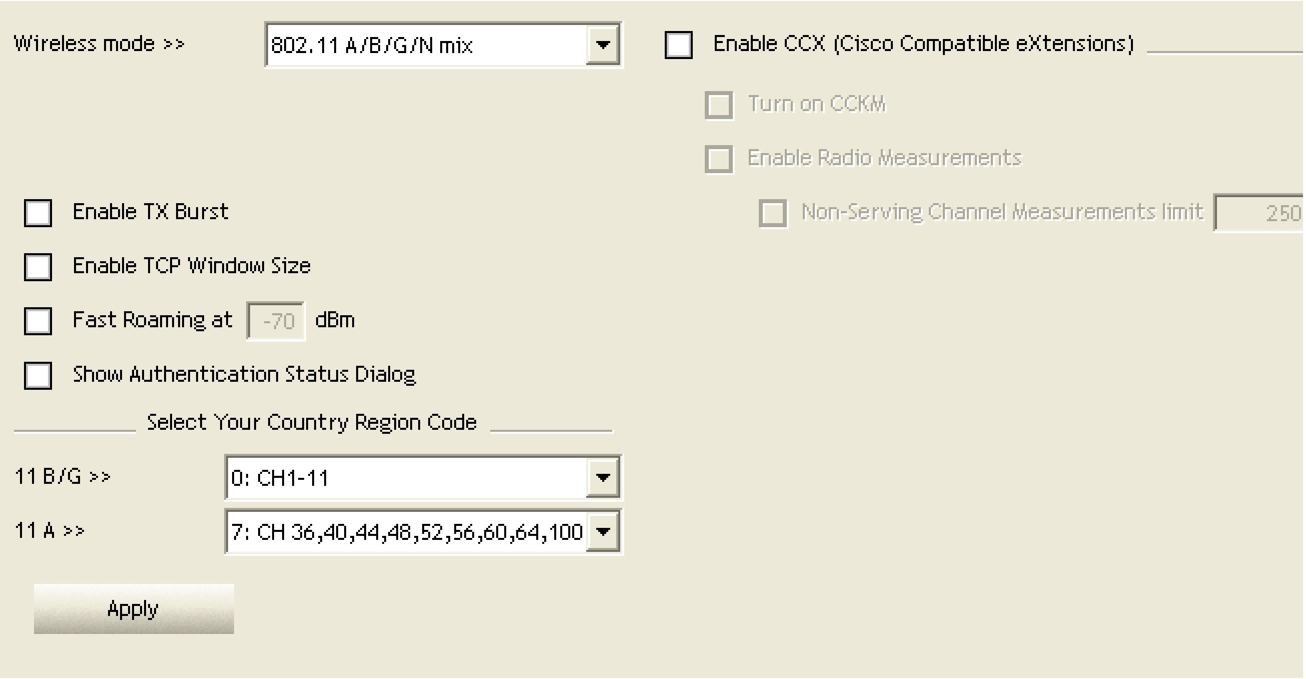


Sorted by >> ● SSID ● Channel ● Signal □ Show

AP List >>

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

Figure 2-1-6 Network page



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

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements limit 250

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

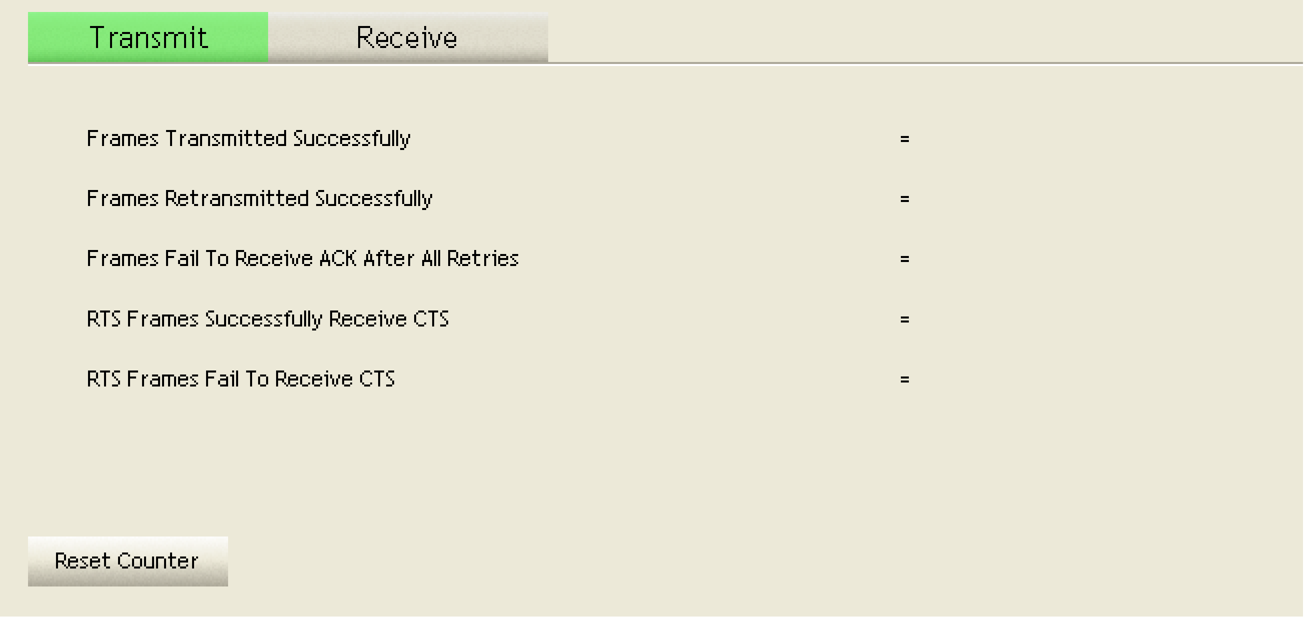
□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

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

Figure 2-1-7 Advance page



Frames Transmitted Successfully =

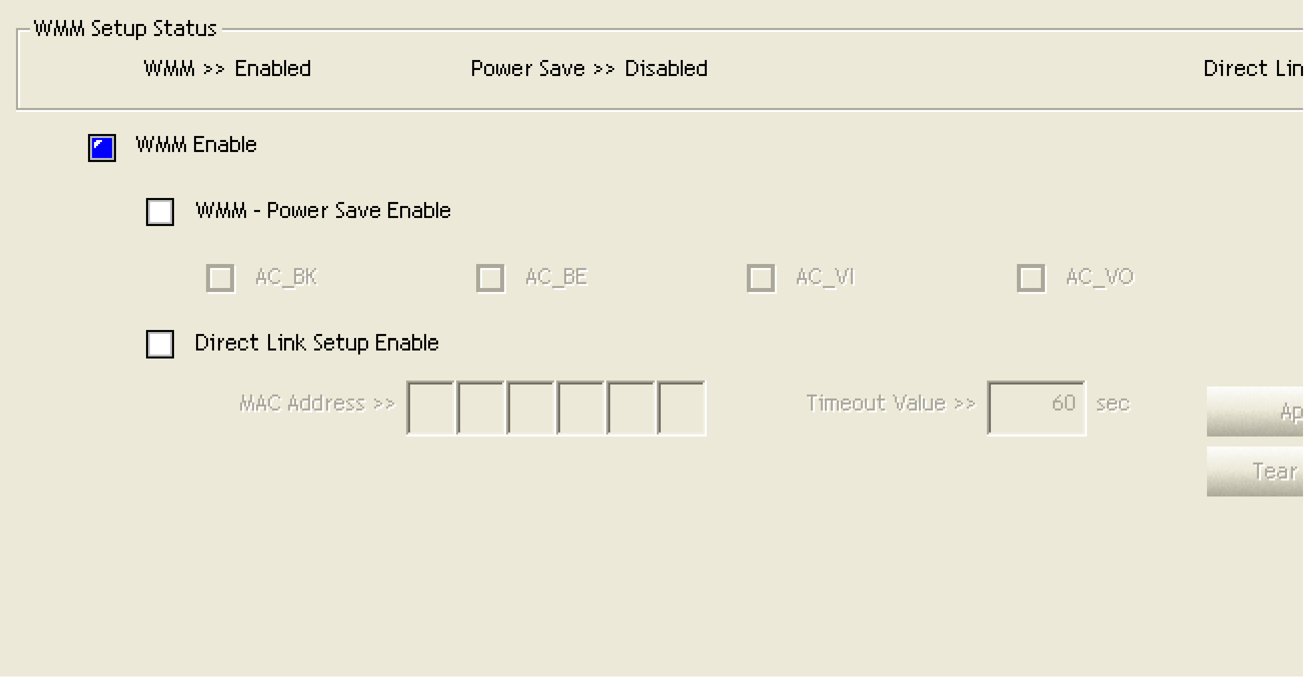
Frames Retransmitted Successfully =

Frames Fail To Receive ACK After All Retries =

RTS Frames Successfully Receive CTS =

RTS Frames Fail To Receive CTS =

Figure 2-1-8 Statistics page



WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lin

☑ WMM Enable

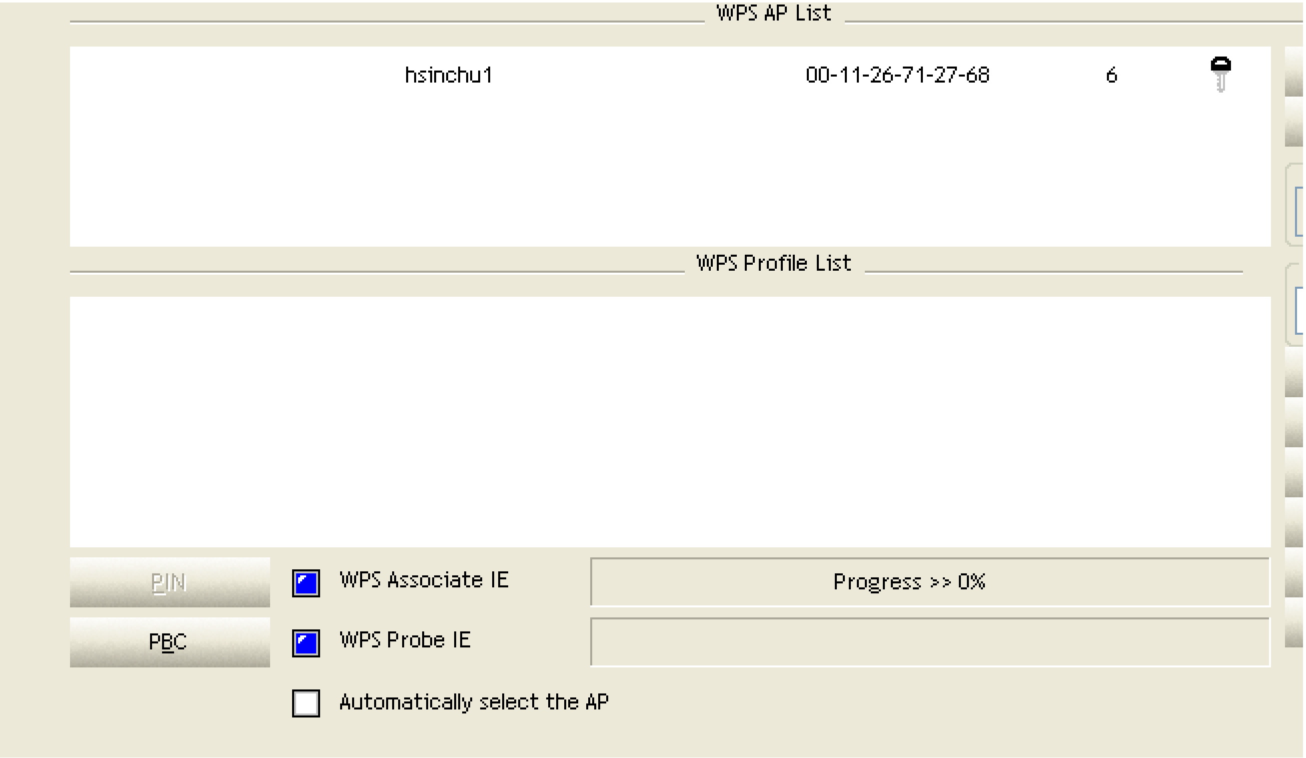
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

Figure 2-1-9 WMM page



WPS AP List

hsinchu1	00-11-26-71-27-68	6	🔑

WPS Profile List

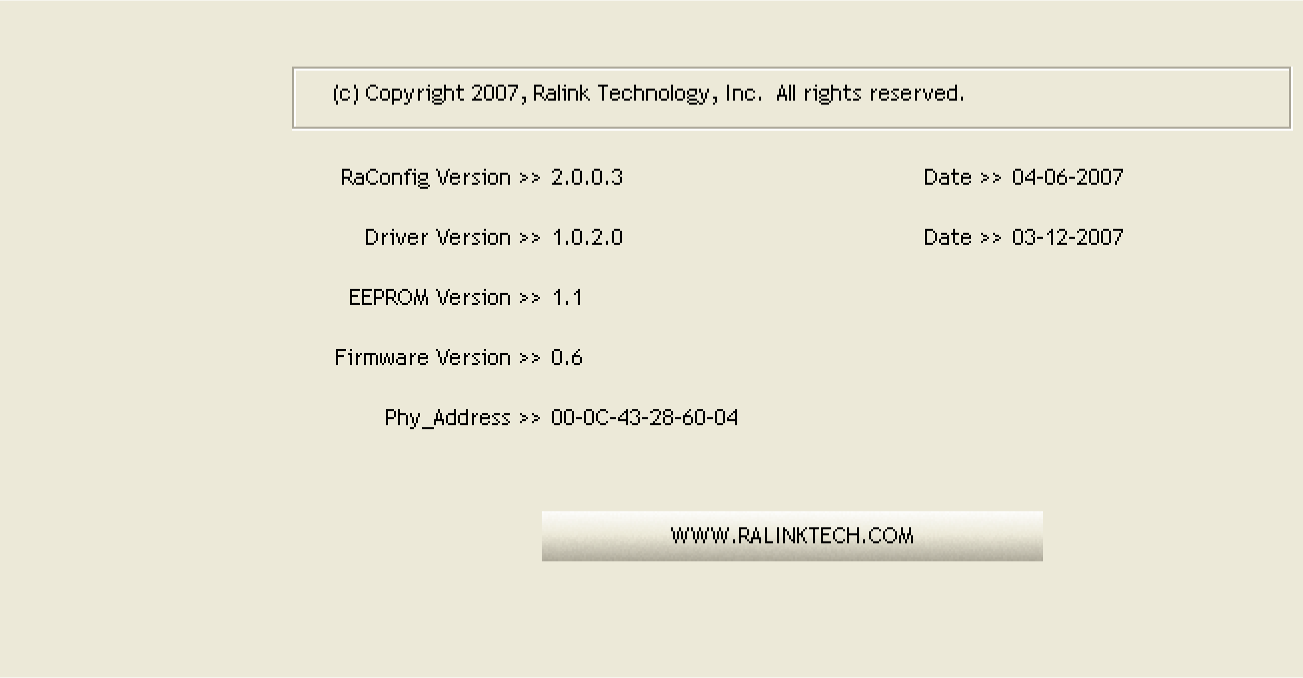
☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

Figure 2-1-10 WPS page

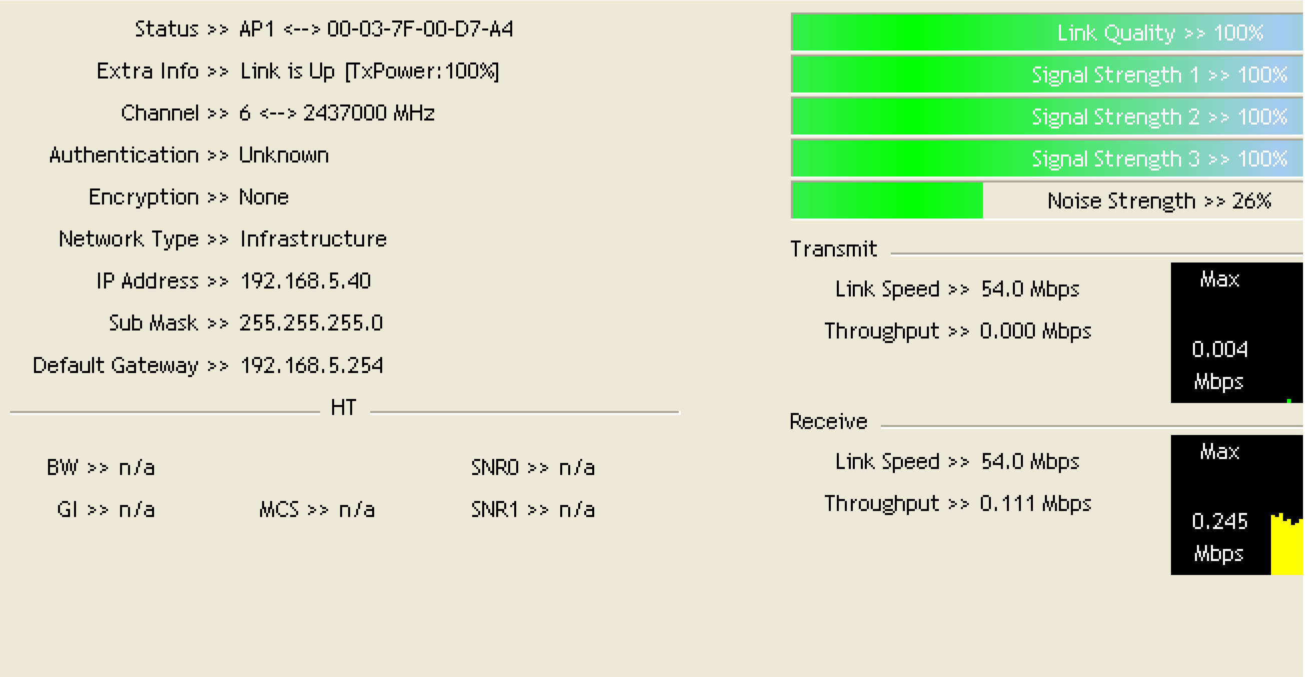


(c) Copyright 2007, Ralink Technology, Inc. All rights reserved.

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

Figure 2-1-11 About page

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



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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.40

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Max

0.004 Mbps

Receive

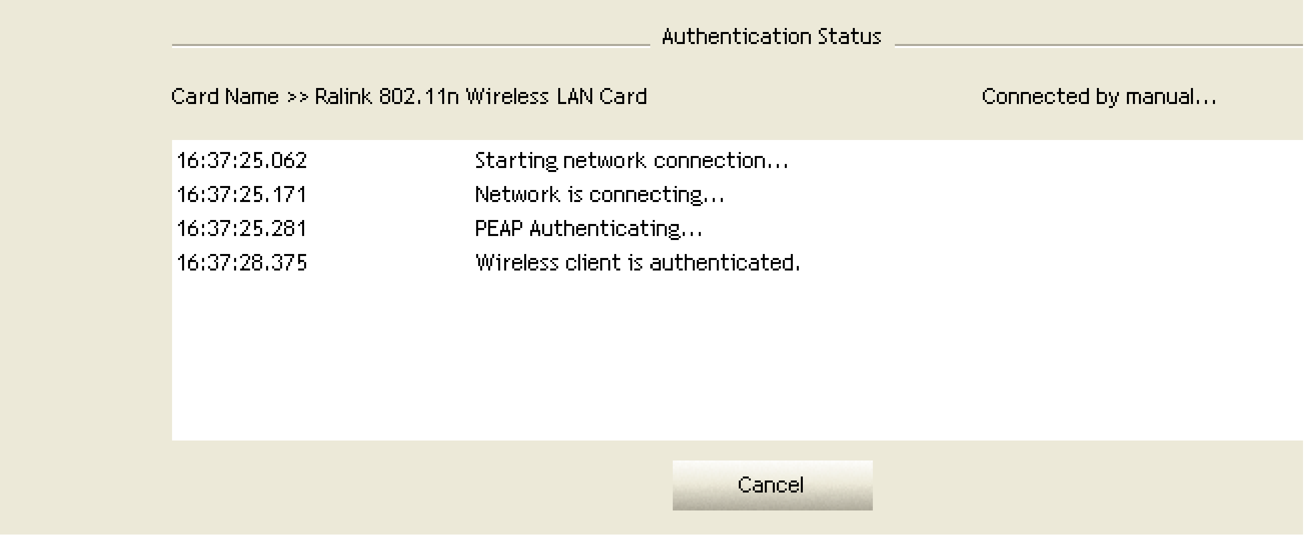
Link Speed >> 54.0 Mbps

Throughput >> 0.111 Mbps

Max

0.245 Mbps

Figure 2-1-12 Link Status



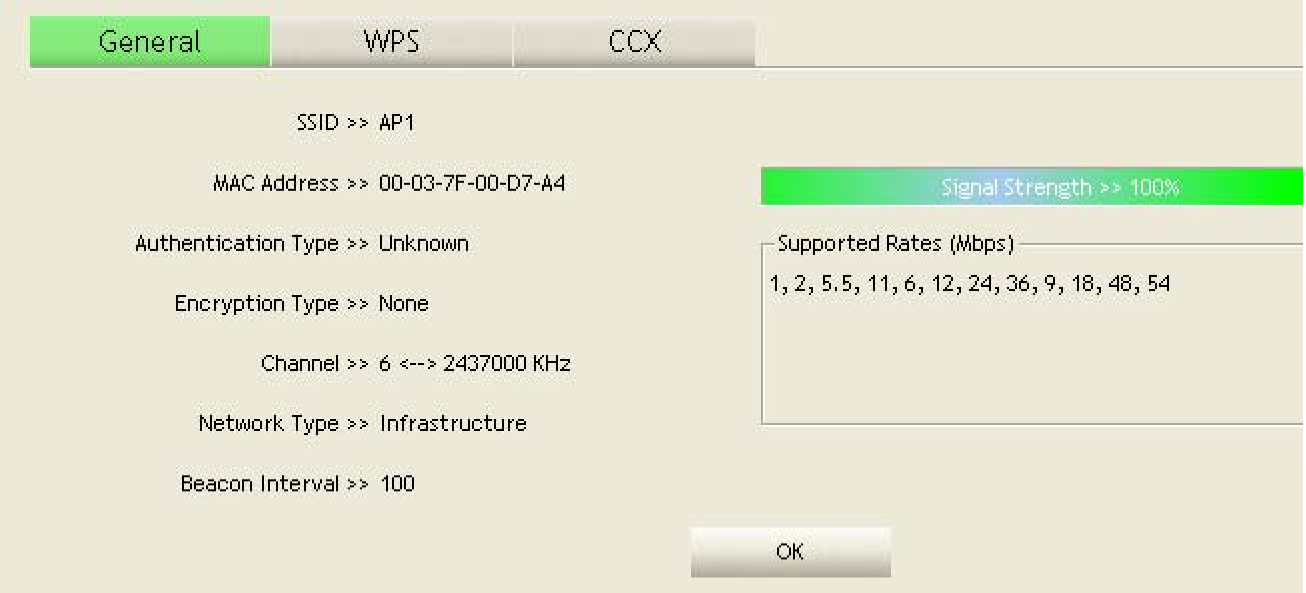
Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card

Connected by manual...

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

Figure 2-1-13 Authentication Status



SSID >> AP1

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

Authentication Type >> Unknown

Encryption Type >> None

Channel >> 6 <--> 2437000 KHz

Network Type >> Infrastructure

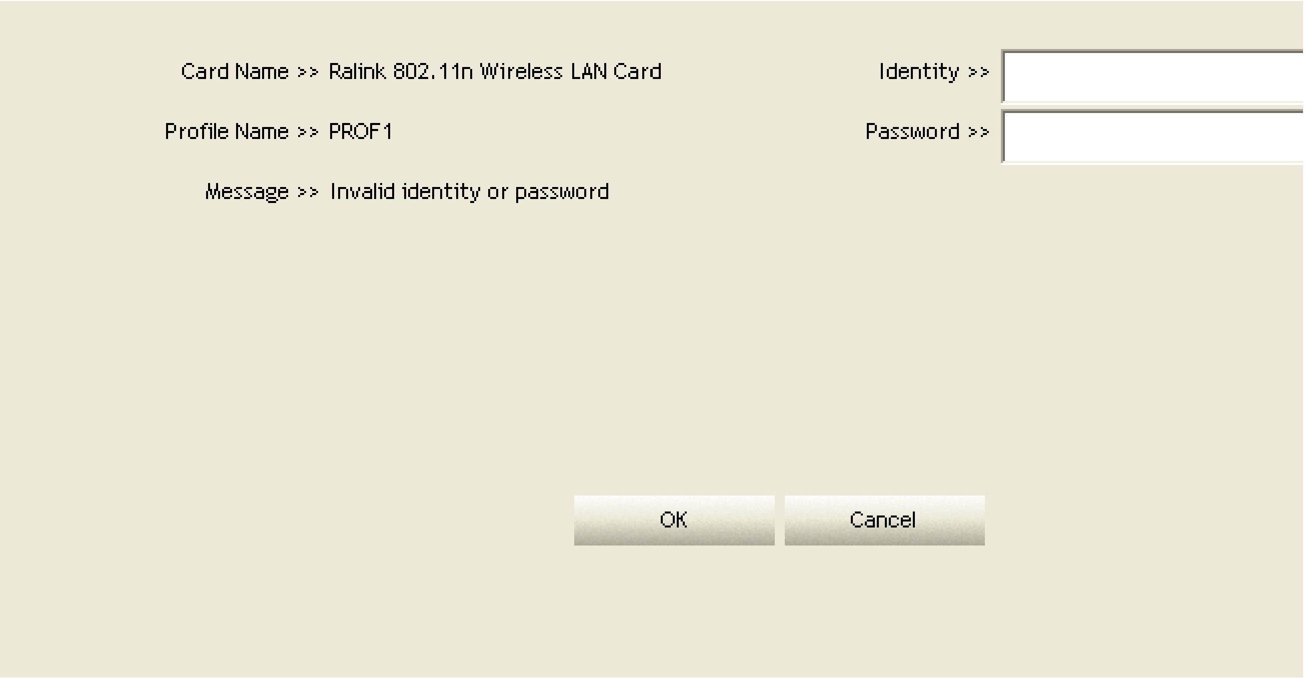
Beacon Interval >> 100

Signal Strength >> 100%

Supported Rates (Mbps)

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

Figure 2-1-14 AP's Information



Card Name >> Ralink 802.11n Wireless LAN Card

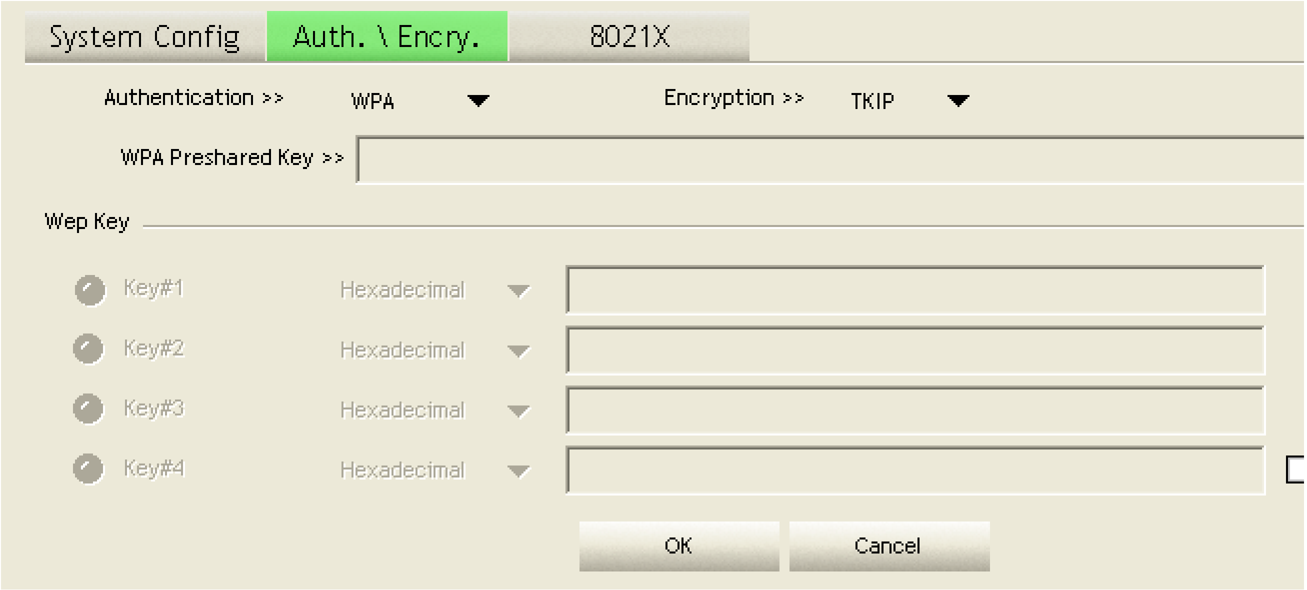
Profile Name >> PROF1

Message >> Invalid identity or password

Identity >>

Password >>

Figure 2-1-15 Retry the connection



Authentication >> WPA

Encryption >> TKIP

WPA Preshared Key >>

Wep Key

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.

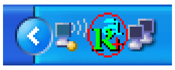


Figure 2-1-17 Ralink icon in system tray

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.

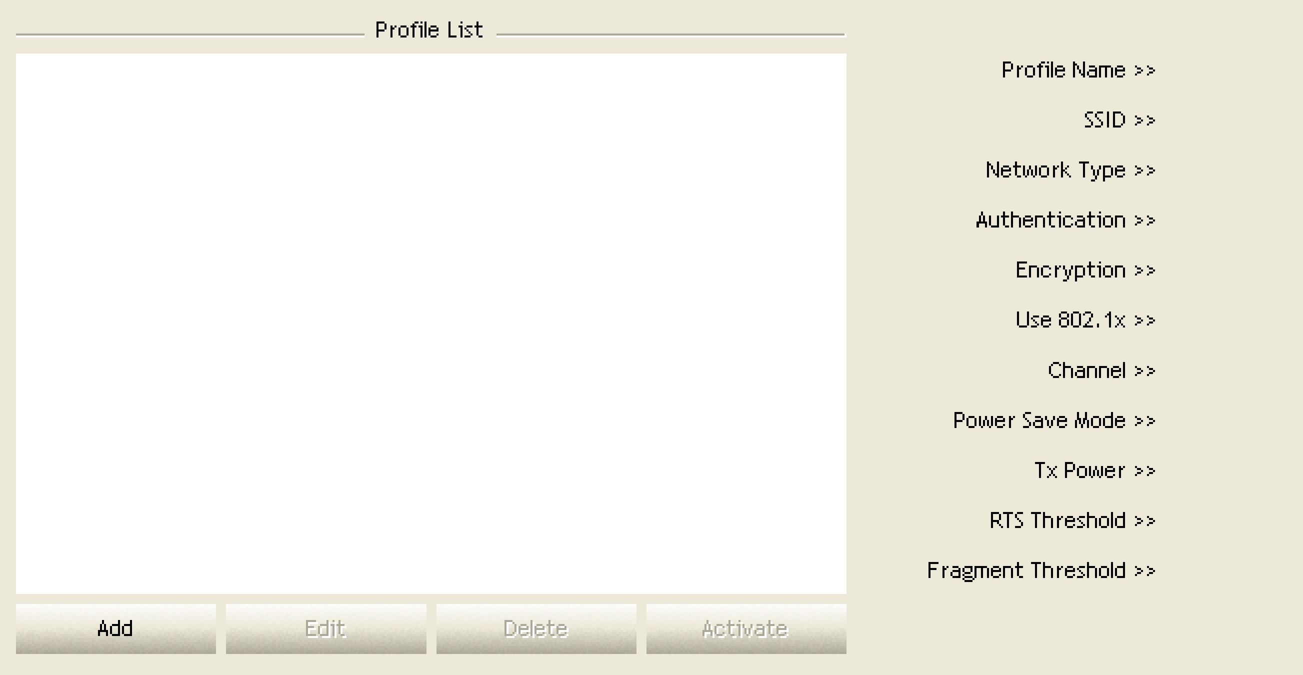
: Indicated not connected yet.

: 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.



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

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 :

① ▶

Indicate connection is successful on currently activated profile.

② ▶

Indicate connection is failed on currently activated profile.

③

Indicate network type is infrastructure mode.

④

Indicate network type is Ad-hoc mode.

⑤ 🔑

Indicate security-enabled wireless network.

⑥ Add

Add a new profile.

⑦ Edit

Edit an existing profile.

⑧ Delete

Delete an existing profile.

⑨ Activate

Activate selected profile.

⑩ ▼

Show the information of Status Section.

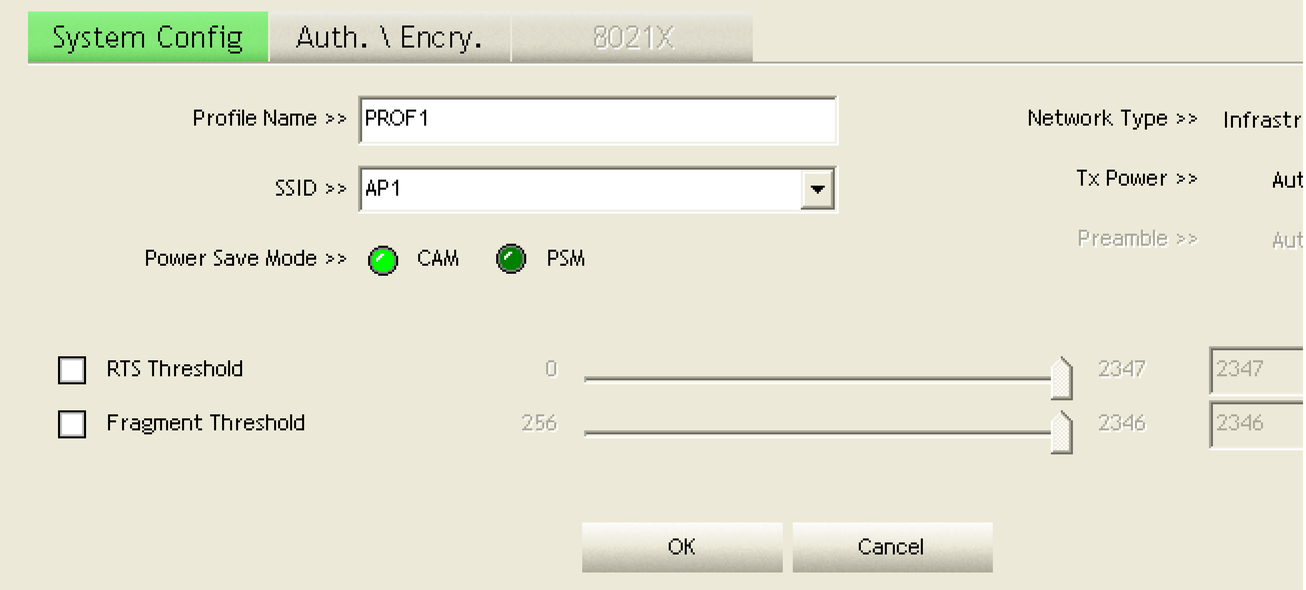
⑪ ▲

Hide the information of Status Section.

Add/Edit Profile

There are three methods to open Profile Editor form.

❶ You can open it from "Add to Profile" button in Site Survey function.
❷ You can open it from "Add" button in Profile function.
❸ You can open it from "Edit" button in Profile function.



Profile Name >> PROF1

SSID >> AP1

Power Save Mode >> ● CAM ○ PSM

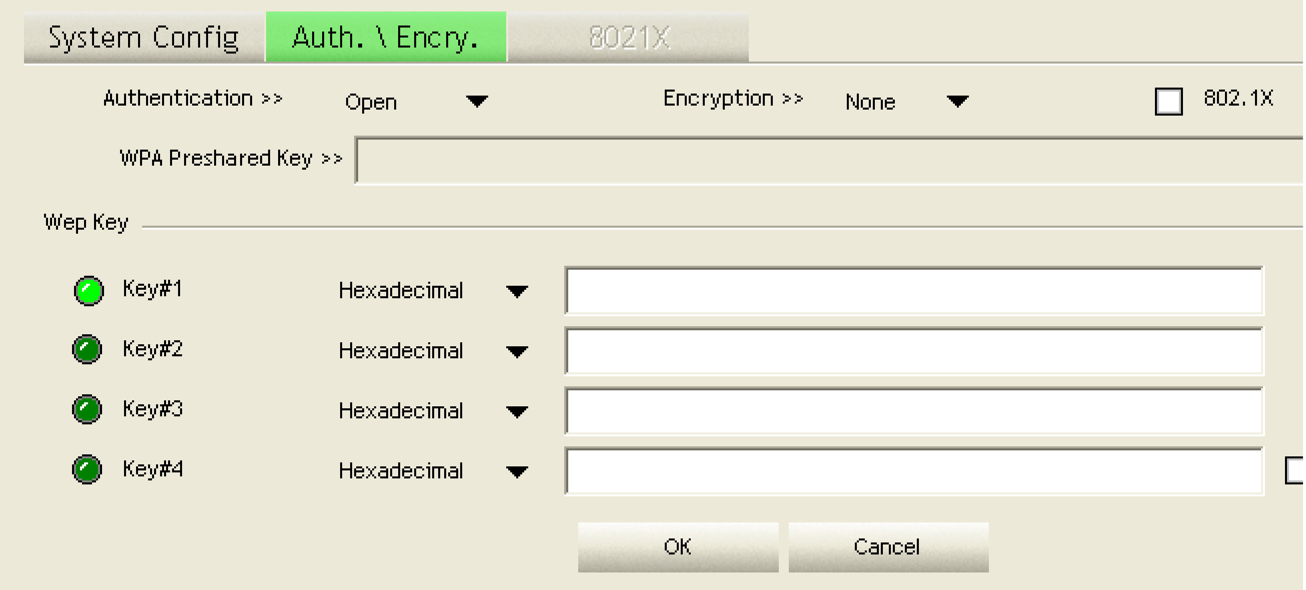
Network Type >> Infrastr

Tx Power >> Aut

Preamble >> Aut

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346



Authentication >> Open

Encryption >> None

□ 802.1X

WPA Preshared Key >>

Wep Key

● Key#1 Hexadecimal

○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

Figure 2-2-2 Configuration

❶ Profile Name : User can chose name for this profile, or use default name defined by system.

❷ SSID : User can key in the intended SSID name or use pull down menu to select from available APs.

❸ Power Save Mode : Choose from CAM Constantly Awake Mode for Power Saving Mode.

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

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

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

❽ 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.

❾ 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.

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

⓫ 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.

⓬ 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.

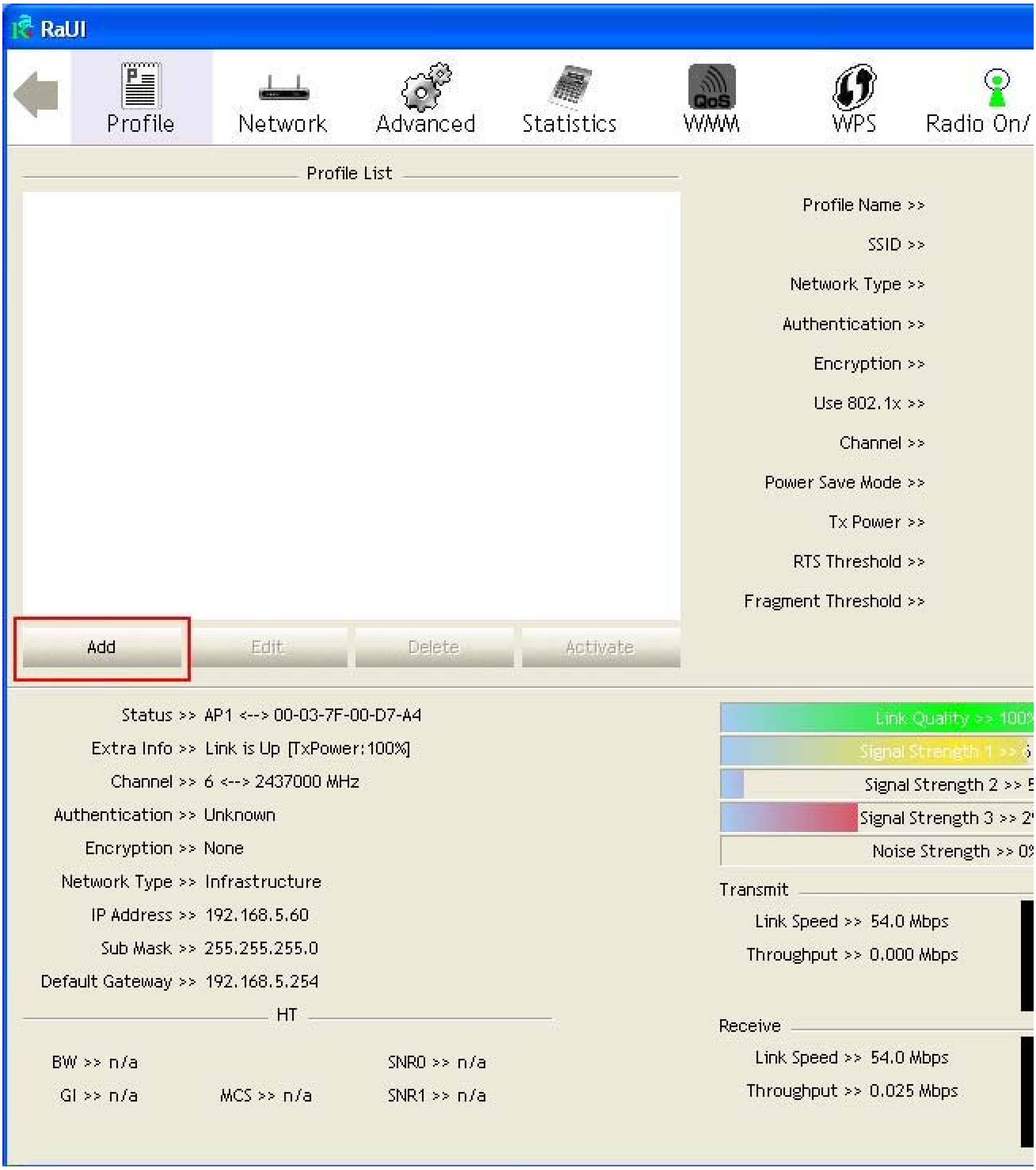
2. Hexadecimal - 128bits : 26Hex characters.

3. ASCII - 40bits : 5 ASCII characters.

4. ASCII - 128bits : 13 ASCII characters.

Example to Add Profile in Profile

1. Click Add in Profile function.



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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.60

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 6

Signal Strength 2 >> 5

Signal Strength 3 >> 2

Noise Strength >> 0%

Transmit

Link Speed >> 54.0 Mbps

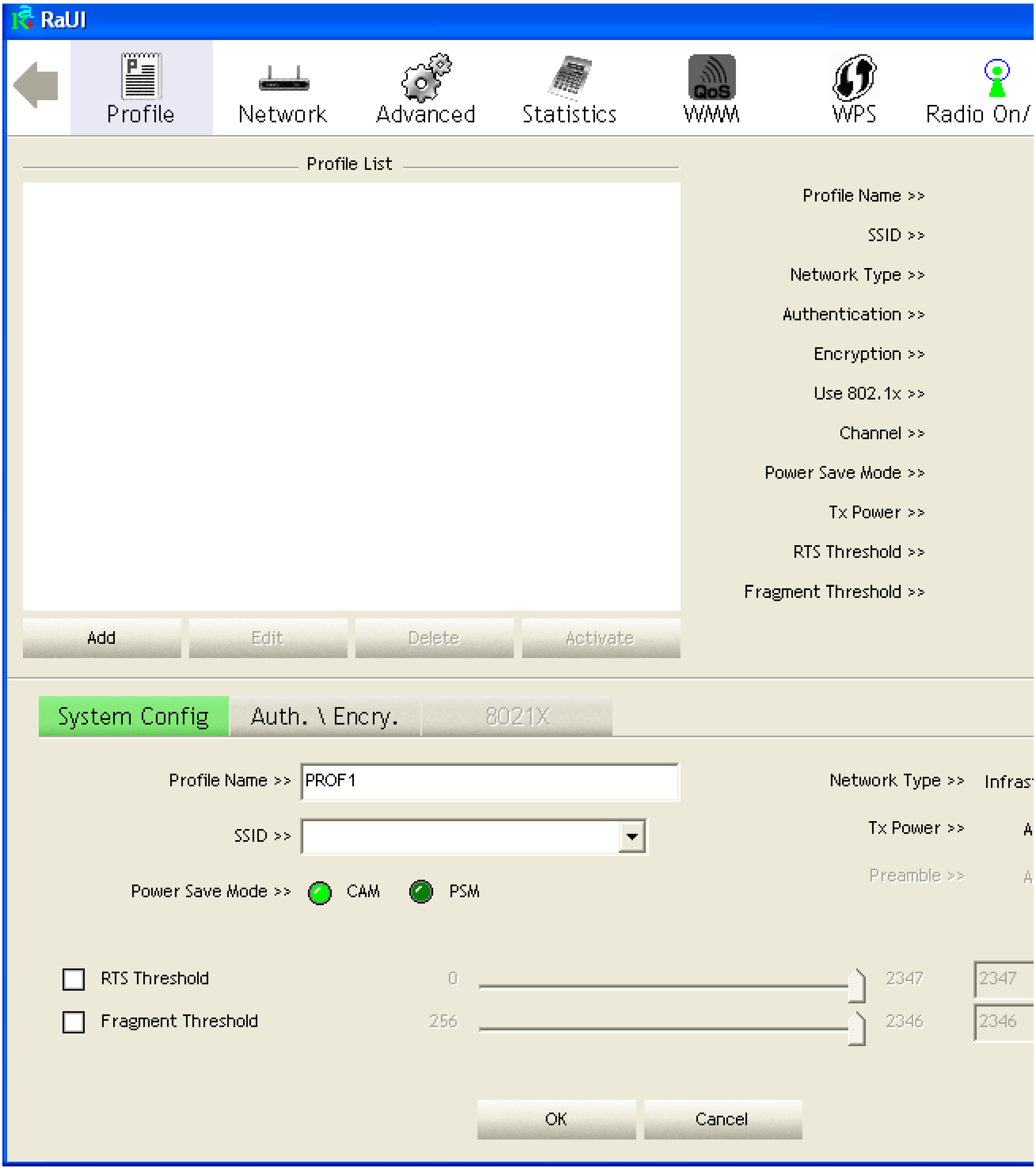
Throughput >> 0.000 Mbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.025 Mbps

❷ Add Profile page will pop up.



Profile Name >> PROF1

SSID >>

Power Save Mode >> ● CAM ● PSM

Network Type >> Infras

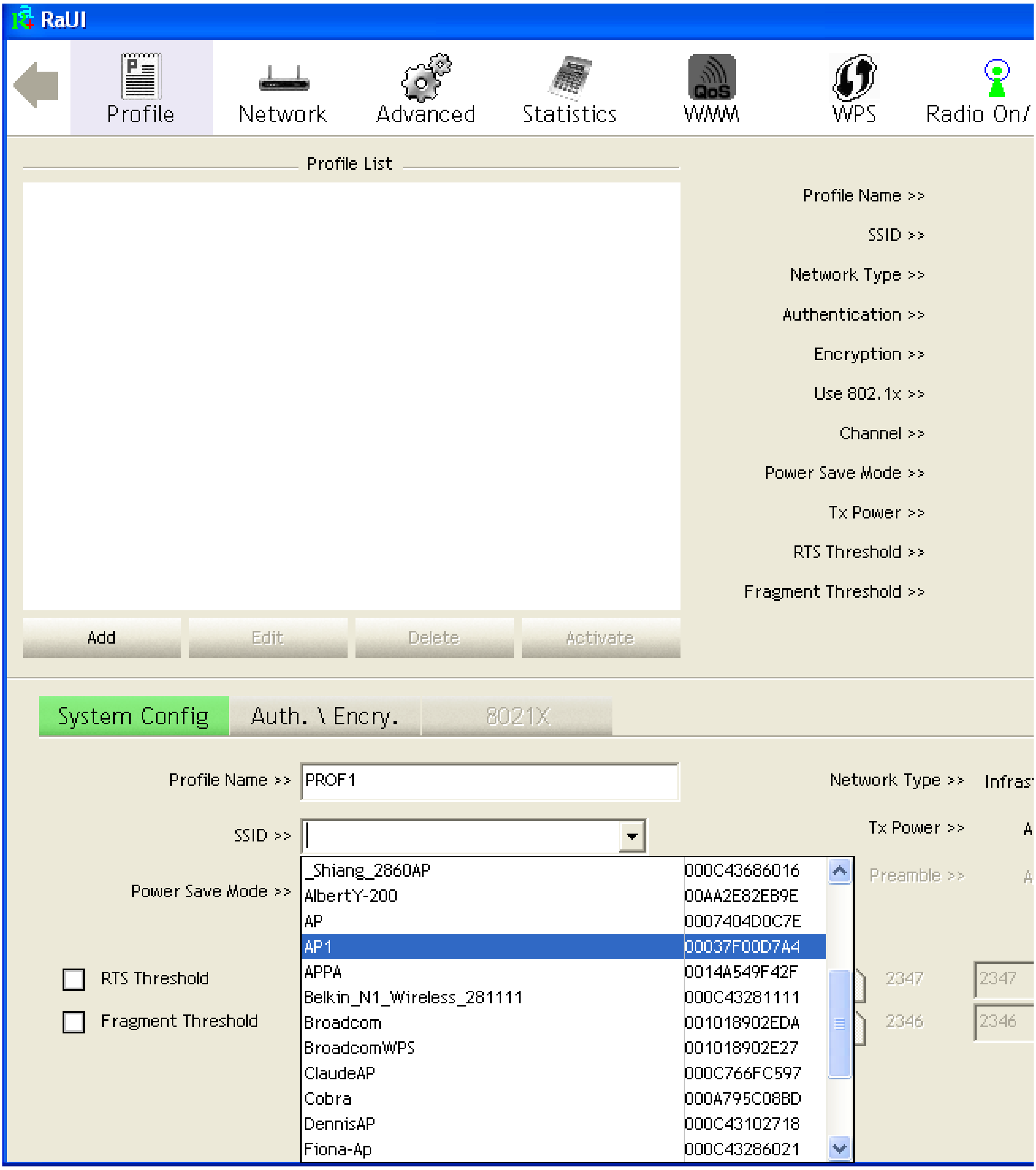
Tx Power >> A

Preamble >> A

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

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.



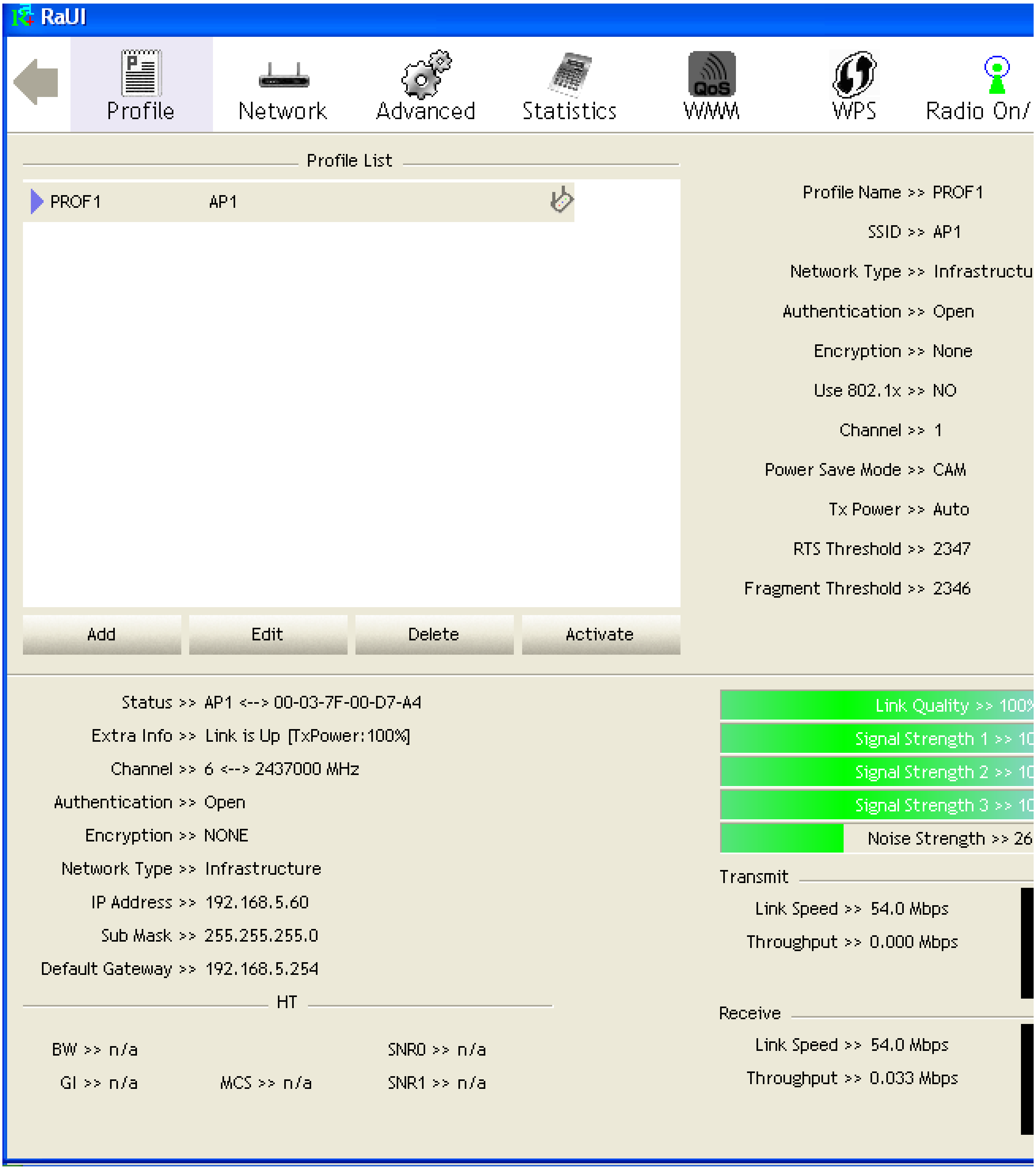
Profile Name >> PROF1

SSID >>

Network Type >> Infras

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

④ Then, you can see the profile which you set appear in the profile list. Click "Activate". Activate the profile setting.



PROF1 AP1

Profile Name >> PROF1

SSID >> AP1

Network Type >> Infrastructu

Authentication >> Open

Encryption >> None

Use 802.1x >> NO

Channel >> 1

Power Save Mode >> CAM

Tx Power >> Auto

RTS Threshold >> 2347

Fragment Threshold >> 2346

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 192.168.5.60

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

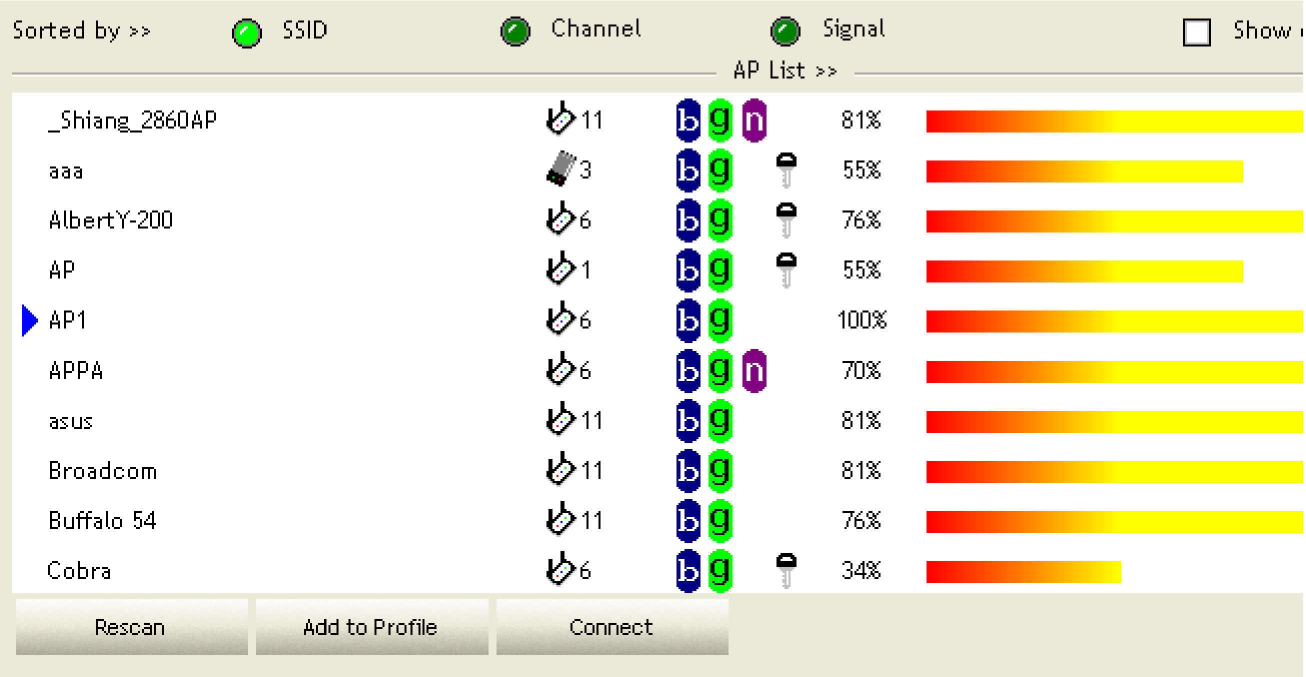
Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.033 Mbps

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.



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

Figure 2-3-1-1 Network fuction

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 :

① ▶

Indicate connection is successful.

②

Indicate network type is infrastructure mode.

③

Indicate network type is Ad-hoc mode.

④ 🔑

Indicate security-enabled wireless network.

⑤ a

Indicate 802.11a wireless mode. mode.

⑥ b

Indicate 802.11b wireless.

⑦ g

Indicate 802.11g wireless mode.

⑧ n

Indicate 802.11n wireless mode

⑨ Sorted by >> ● SSID ● Channel ● Signal

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

⑩ Connect

Command to connect to the selected network.

⑪ Rescan

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

⑫ Add to Profile

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

⑬ ▼

Show the information of Status Section.

⑭ ▲

Hide the information of Status Section.

Connected network :

① When RaUI first ran, it will select the best AP to connect automatically.

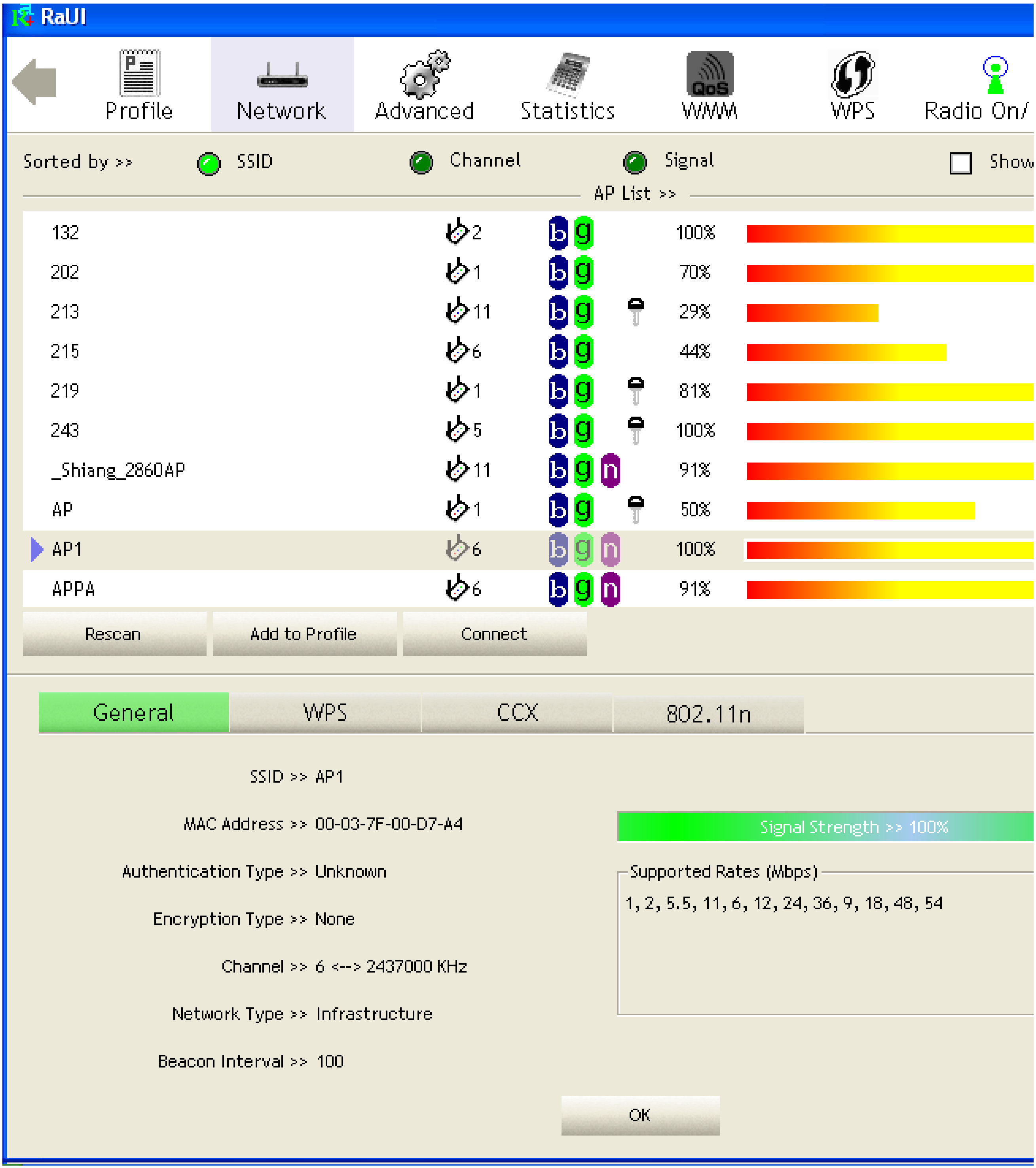
② If user wants to connect to other AP. He can click "Connect" button for the intended AP to make connection.

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 :

❶ 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.



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

SSID >> AP1

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

Authentication Type >> Unknown

Encryption Type >> None

Channel >> 6 <--> 2437000 KHz

Network Type >> Infrastructure

Beacon Interval >> 100

Signal Strength >> 100%

Supported Rates (Mbps)

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

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

❷ 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 :

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

❷ 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.

❸ 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

❹ 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

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

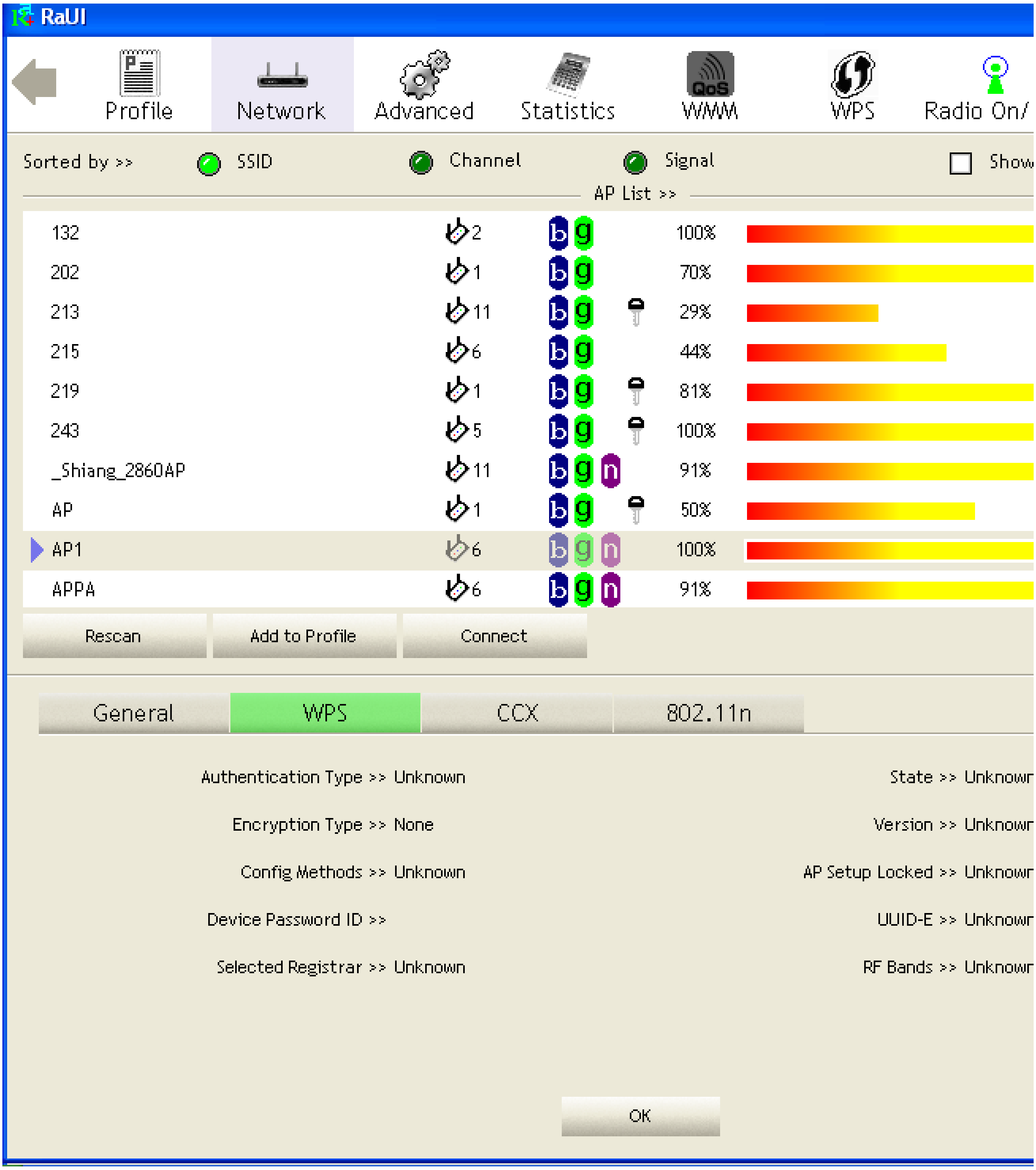
❻ State : The current configuration state on AP. The values are "Unconfigured" and "Configured".

❼ Version : WPS specified version.

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

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

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



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

Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Unknown

Version >> Unknown

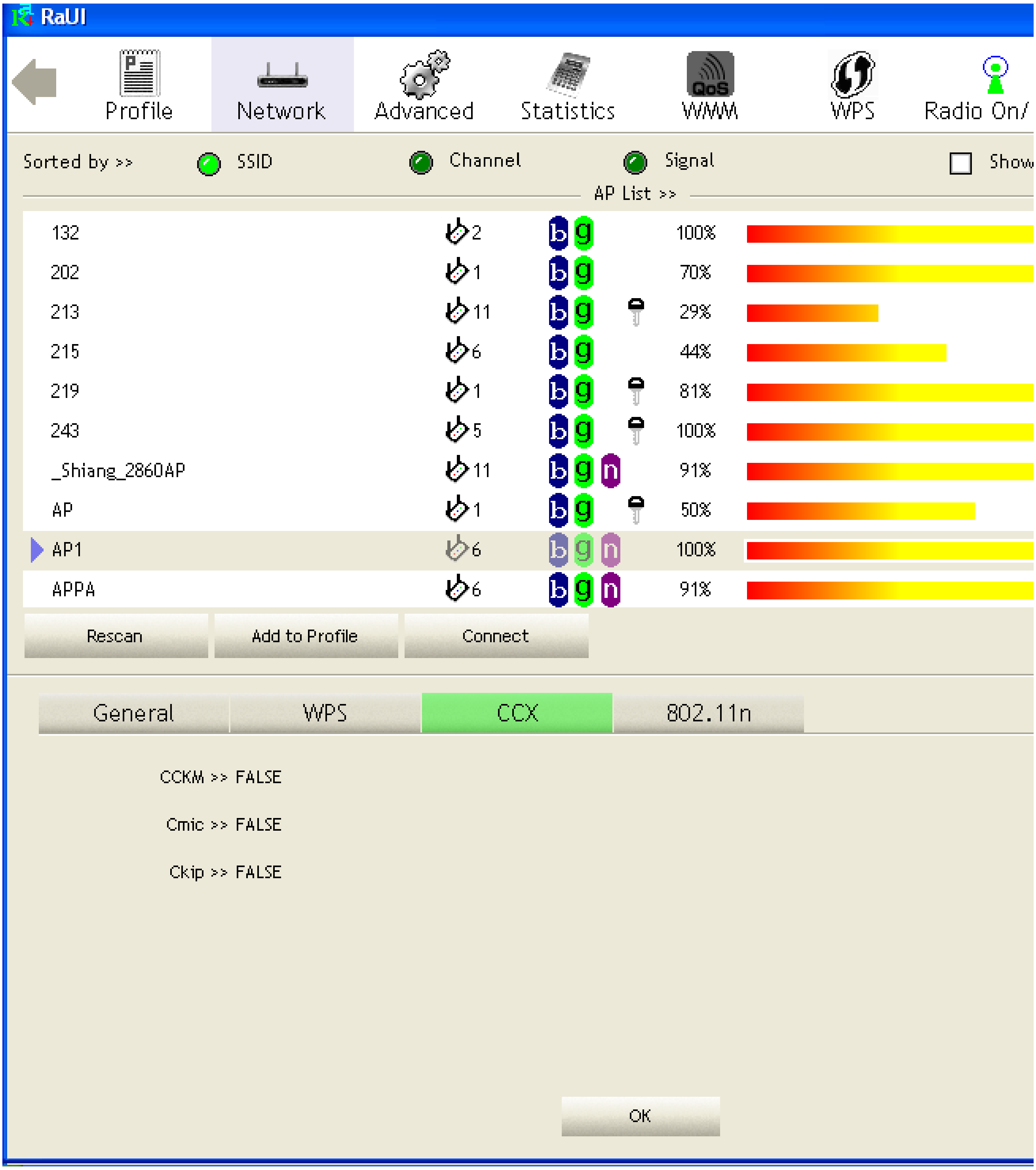
AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

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

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



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

AP List >>

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

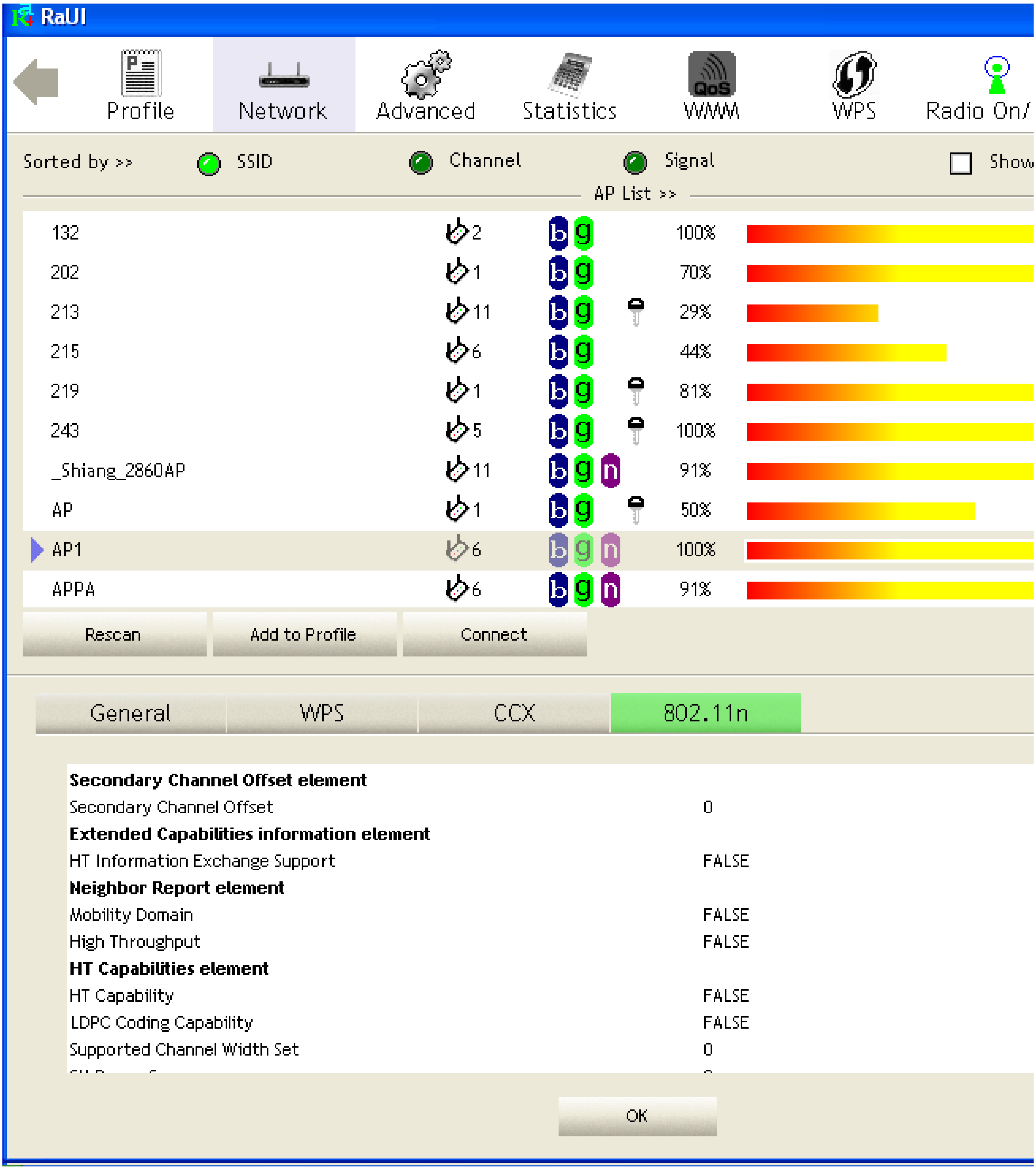
CCKM >> FALSE

Cmic >> FALSE

Ckip >> FALSE

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

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



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

AP List >>

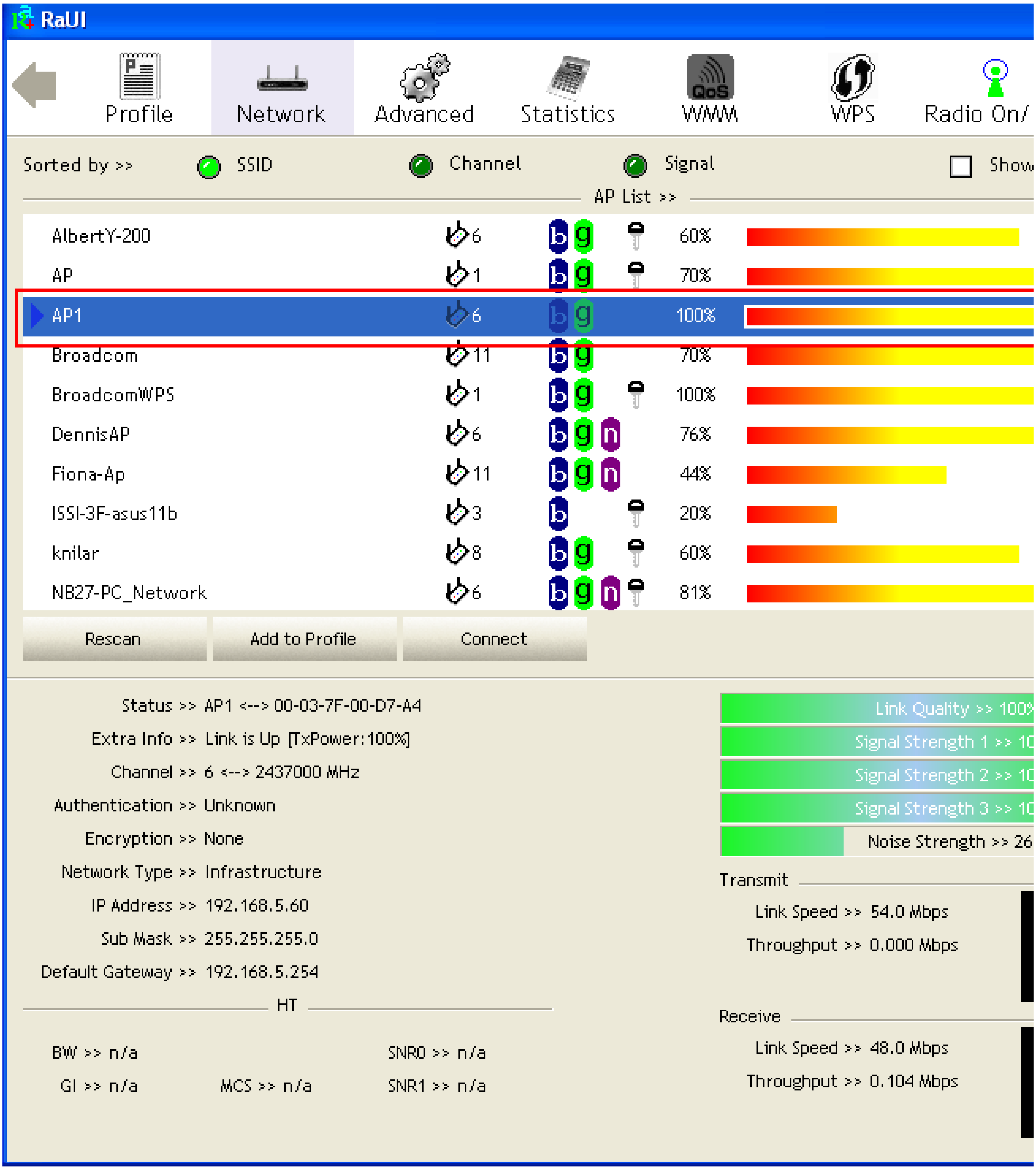
SSID	Channel	Mode		Signal
132	2	b g		100%
202	1	b g		70%
213	11	b g	🔑	29%
215	6	b g		44%
219	1	b g	🔑	81%
243	5	b g	🔑	100%
_Shiang_2860AP	11	b g n		91%
AP	1	b g	🔑	50%
AP1	6	b g n		100%
APPA	6	b g n		91%

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

Figure 2-3-1-5 802.11n information

Example on Adding Profile in Network

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



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

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.60

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

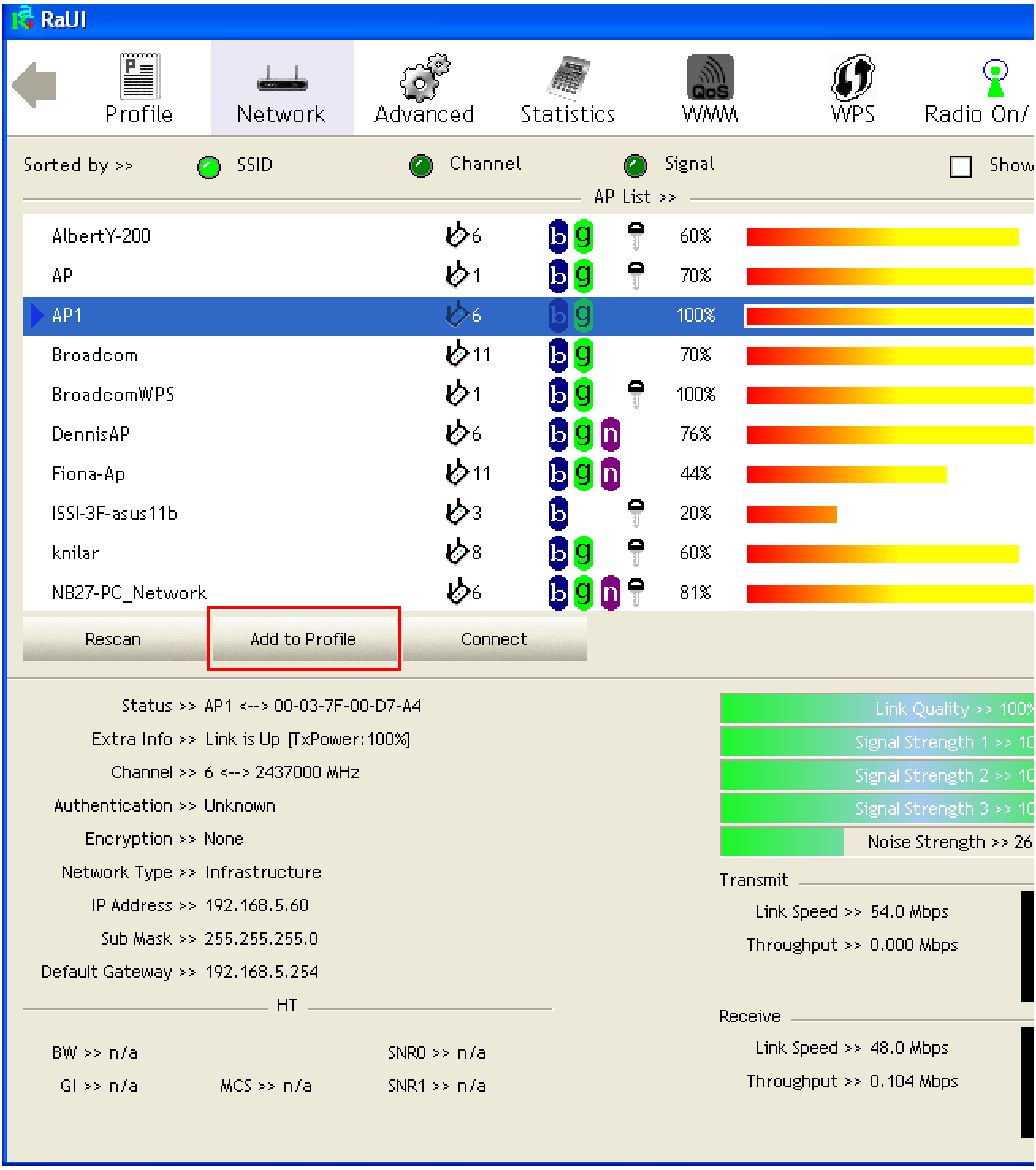
Throughput >> 0.000 Mbps

Receive

Link Speed >> 48.0 Mbps

Throughput >> 0.104 Mbps

2 Click "Add to Profile".



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

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

HT

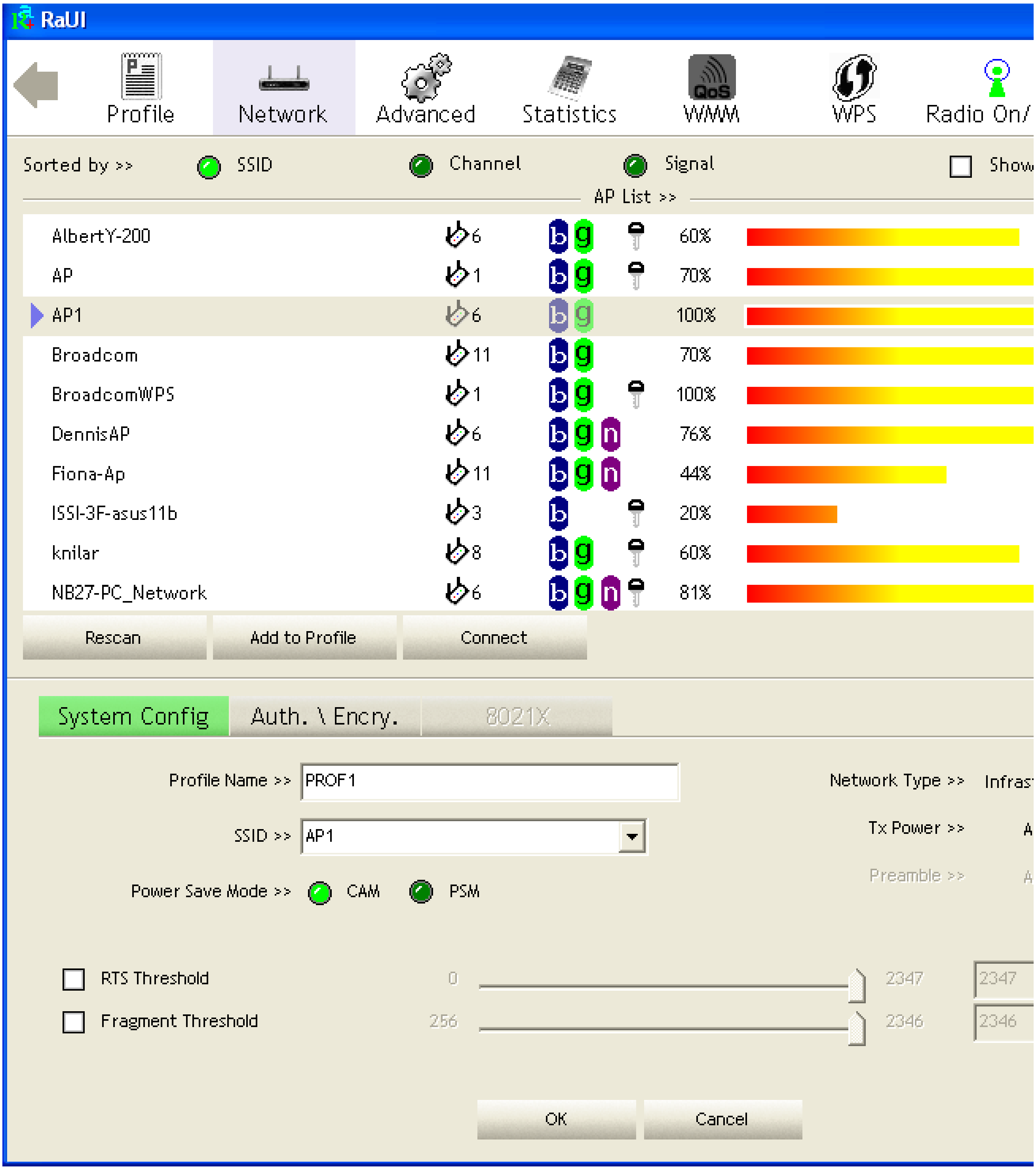
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

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



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

AP List >>

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

Profile Name >> PROF1

SSID >> AP1

Power Save Mode >> ● CAM ○ PSM

Network Type >> Infras

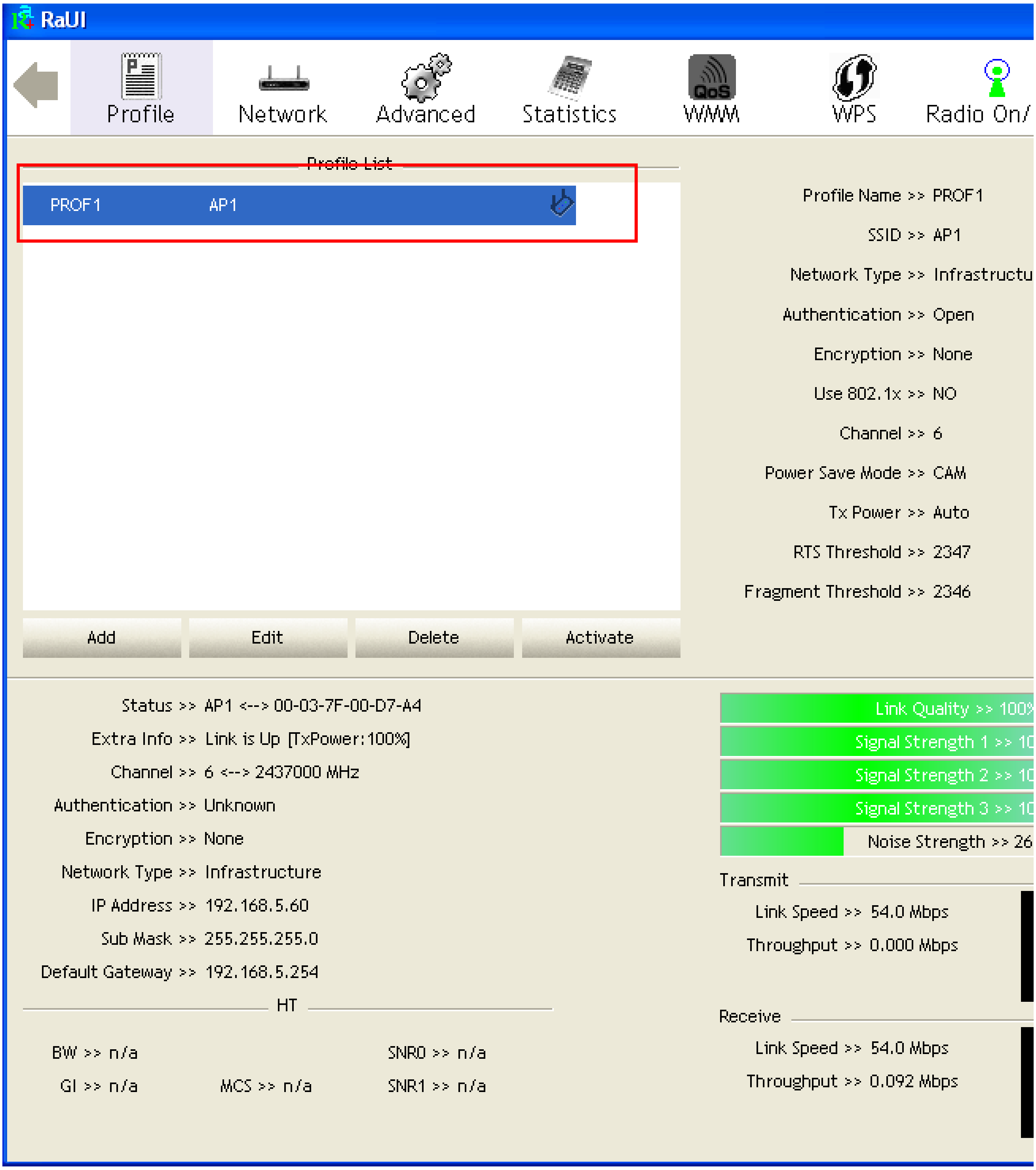
Tx Power >> A

Preamble >> A

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

④ Then, you can see the profile which you set appear in the profile list. Click "Activate". Activate the profile setting.



PROF1 AP1

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

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

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

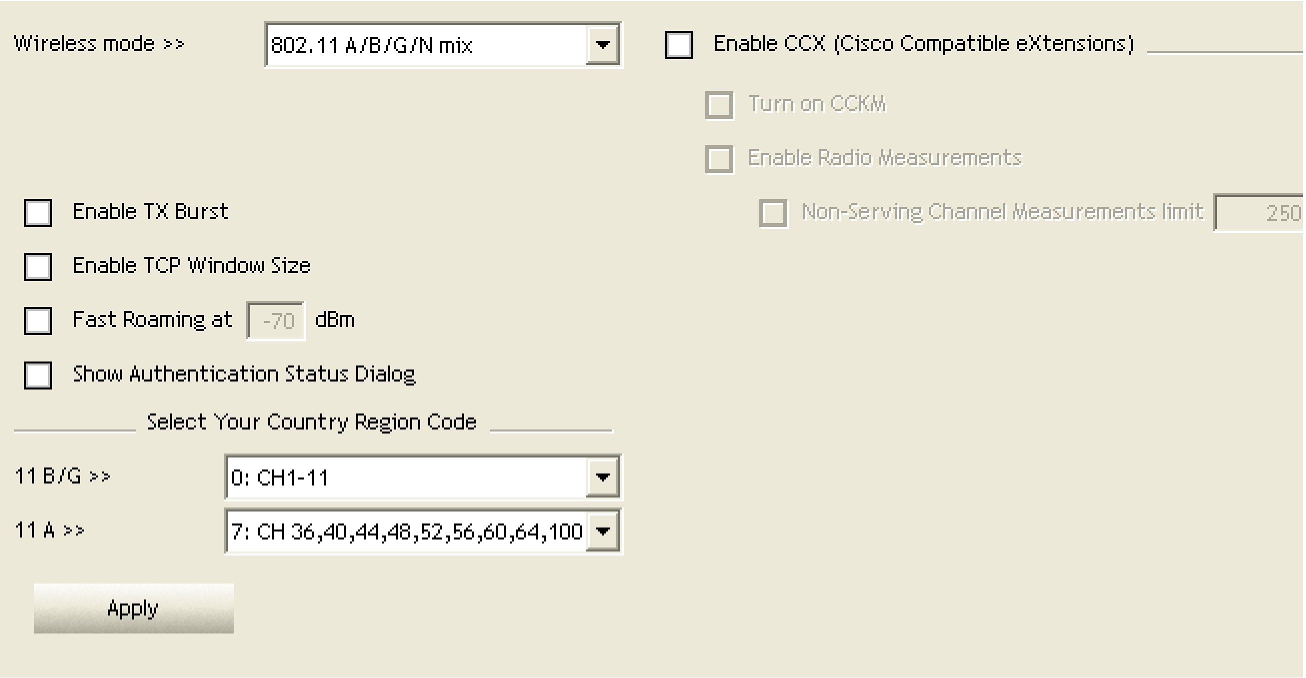
Link Quality >> 100%
Signal Strength 1 >> 10
Signal Strength 2 >> 10
Signal Strength 3 >> 10
Noise Strength >> 26

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

□ Non-Serving Channel Measurements limit 250

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

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

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.)

❶ Auto : STA will dynamically change as AP announcement.

❷ On : Always send frame with protection.

❸ 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.

❶ LEAP turn on CCKM.

❷ Enable Radio Measurement : can channel measurement every 0~2000 milliseconds.

⑩ Apply the above changes.

Icons and buttons:

① ▼

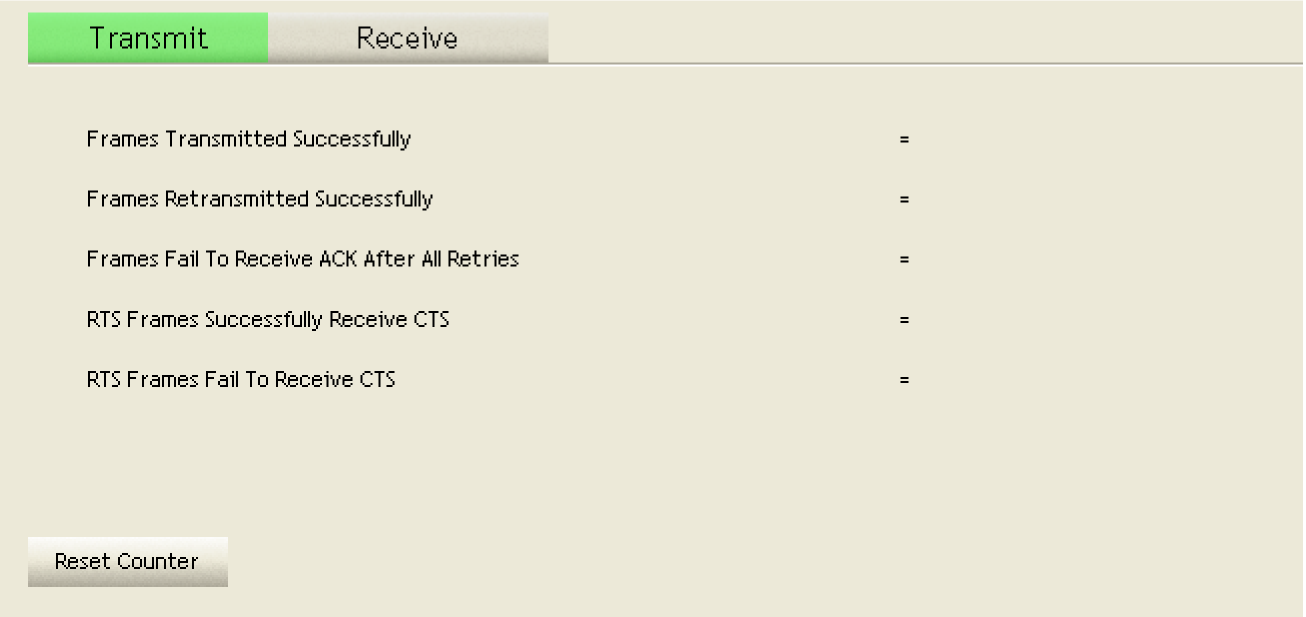
Show the information of Status Section.

② ▲

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.



Frames Transmitted Successfully =

Frames Retransmitted Successfully =

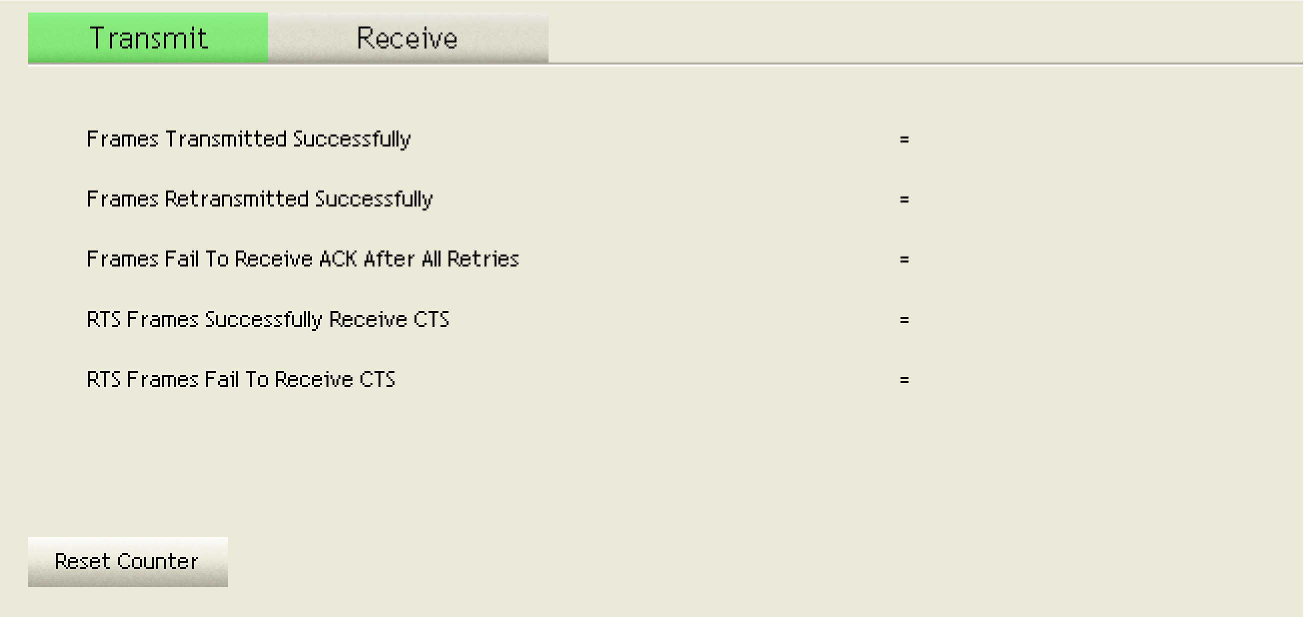
Frames Fail To Receive ACK After All Retries =

RTS Frames Successfully Receive CTS =

RTS Frames Fail To Receive CTS =

Figure 2-5-1 Statistics function

Transmit Statistics :



Frames Transmitted Successfully =

Frames Retransmitted Successfully =

Frames Fail To Receive ACK After All Retries =

RTS Frames Successfully Receive CTS =

RTS Frames Fail To Receive CTS =

① Frames Transmitted Successfully : Frames successfully sent.

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

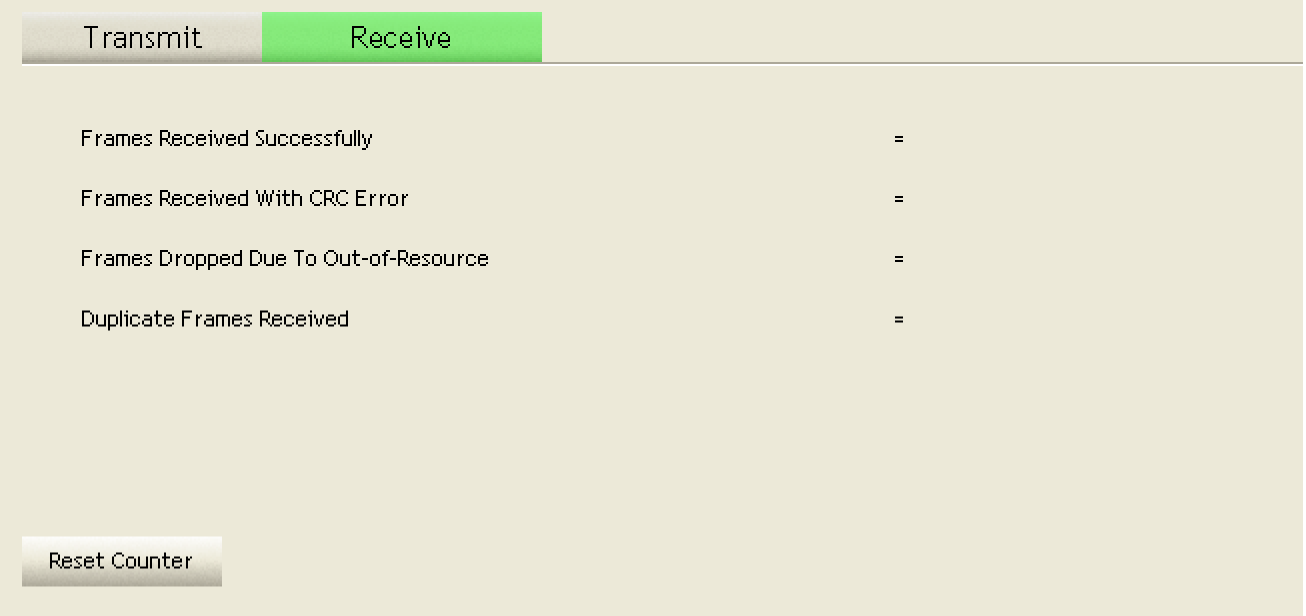
❸ RTS Frames Successfully Receive CTS : Successfully receive CTS after sending RTS frame.

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

❺ Frames Retransmitted Successfully : Successfully retransmitted frames numbers.

❻ Reset counters to zero.

Receive Statistics :



Frames Received Successfully =

Frames Received With CRC Error =

Frames Dropped Due To Out-of-Resource =

Duplicate Frames Received =

❶ Frames Received Successfully : Frames received successfully.

❷ Frames Received With CRC Error : Frames received with CRC error.

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

❹ Duplicate Frames Received : Duplicate received frames. ❺

Reset counters to zero.

Icons and buttons:

❶ ▼

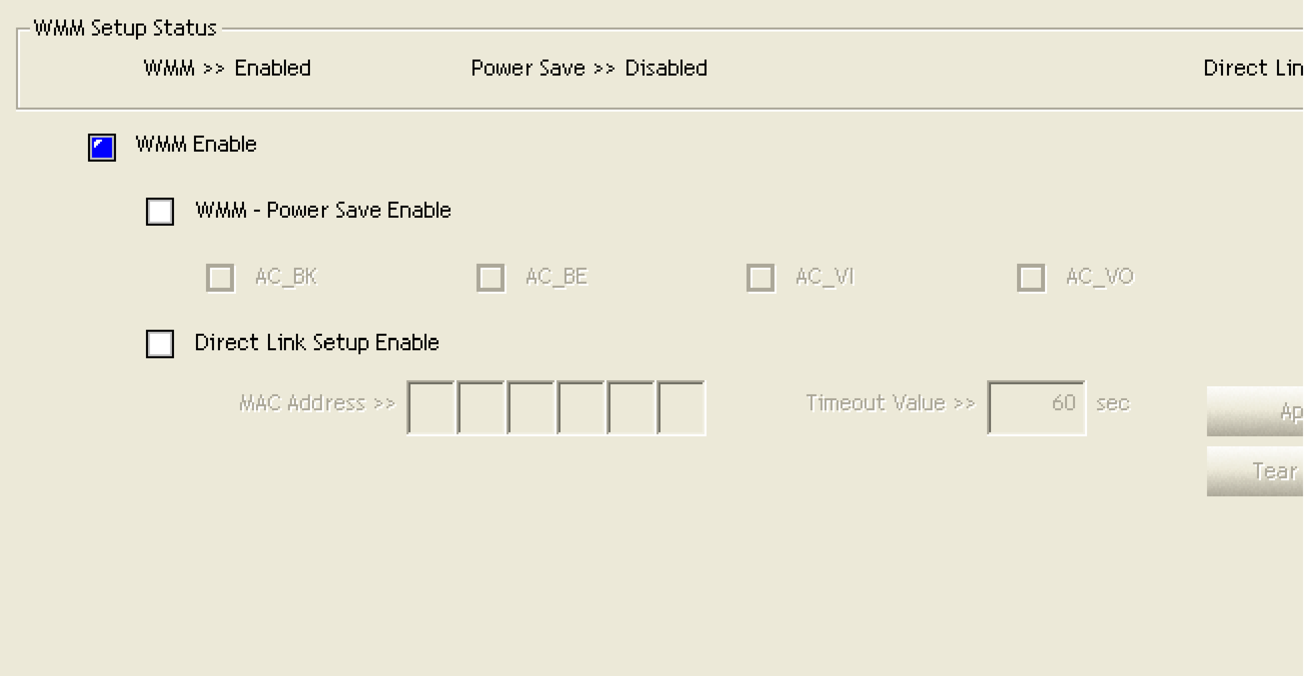
Show the information of Status Section.

❷ ▲

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 :



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lin

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >> □ □ □ □ □ □   Timeout Value >> 60 sec

Figure 2-6-1 WMM function

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

Icons and buttons:

❶ ▼

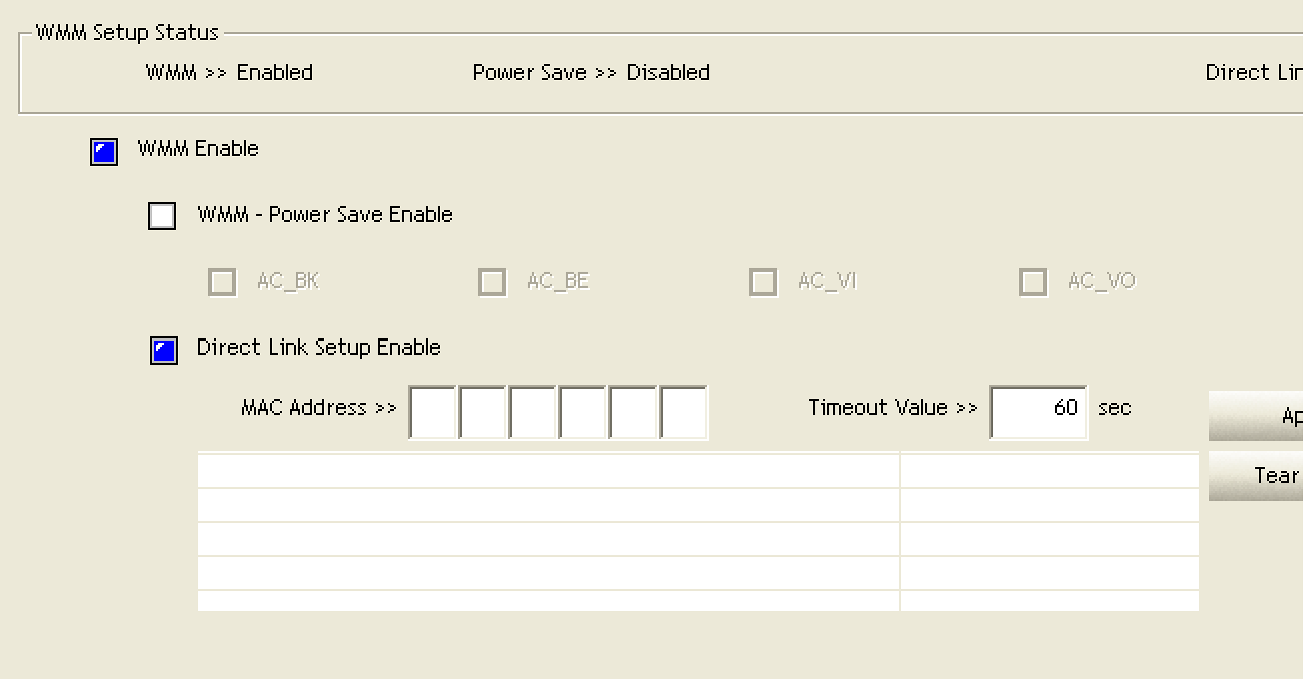
Show the information of Status Section.

❷ ▲

Hide the information of Status Section.

Example to Configure to Enable DLS (Direct Link Setup)

❶ Click "Direct Link Setup Enable"



WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Lir

☑ WMM Enable

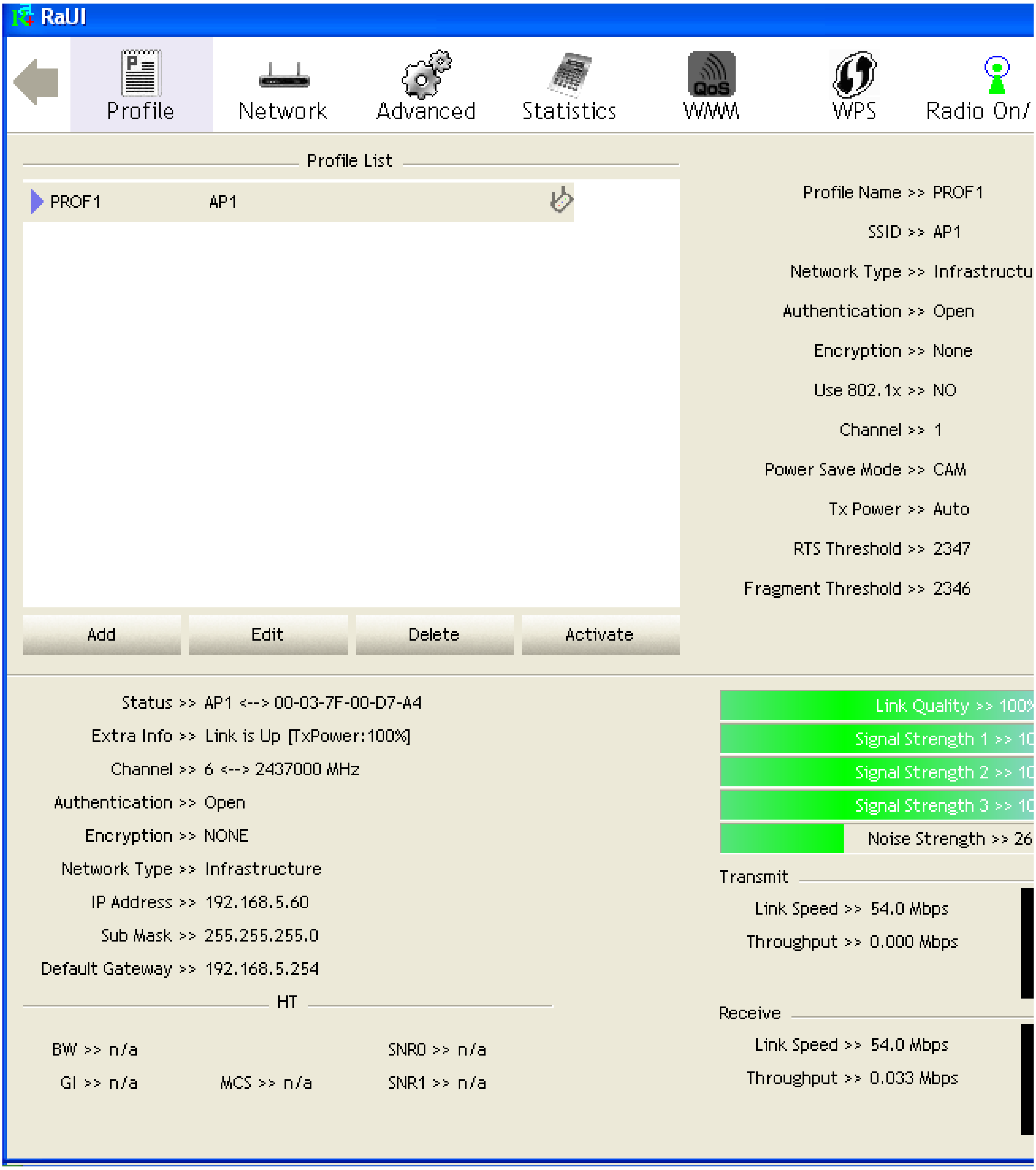
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

❷ 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.



PROF1 AP1

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

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

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

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

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

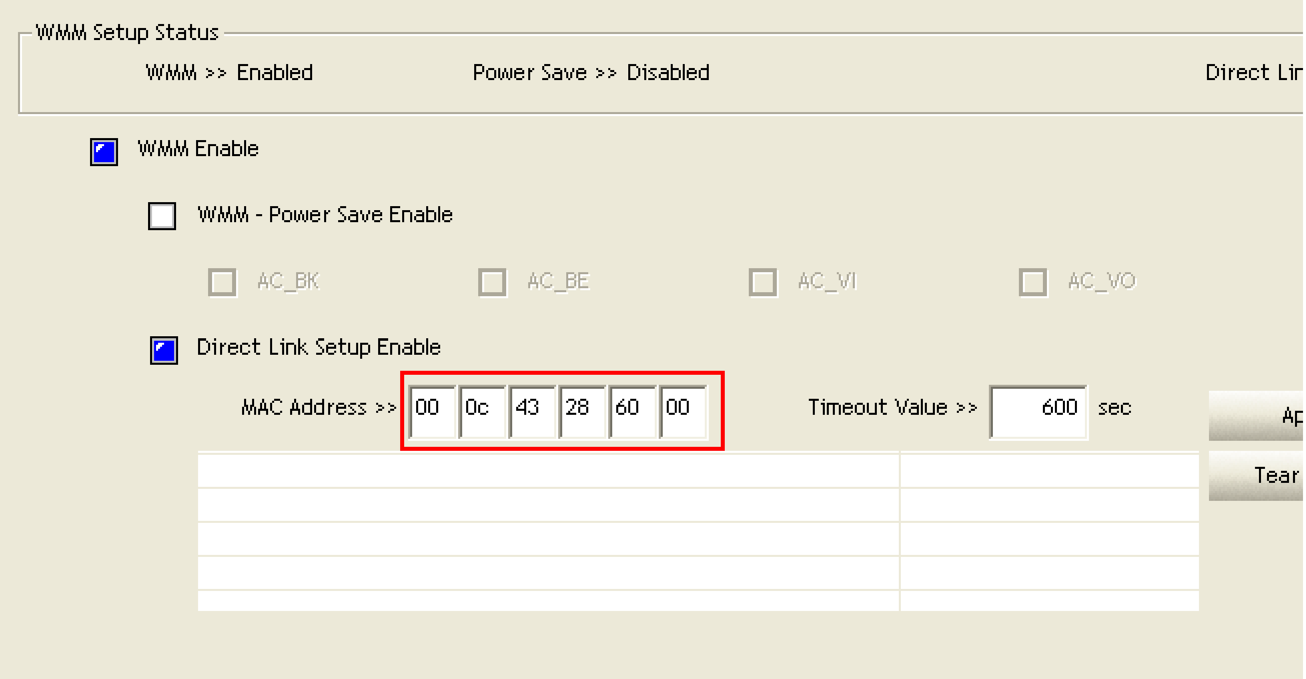
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps

The setting of DLS indicates as follow :

❶ 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 Lir

☑ WMM Enable

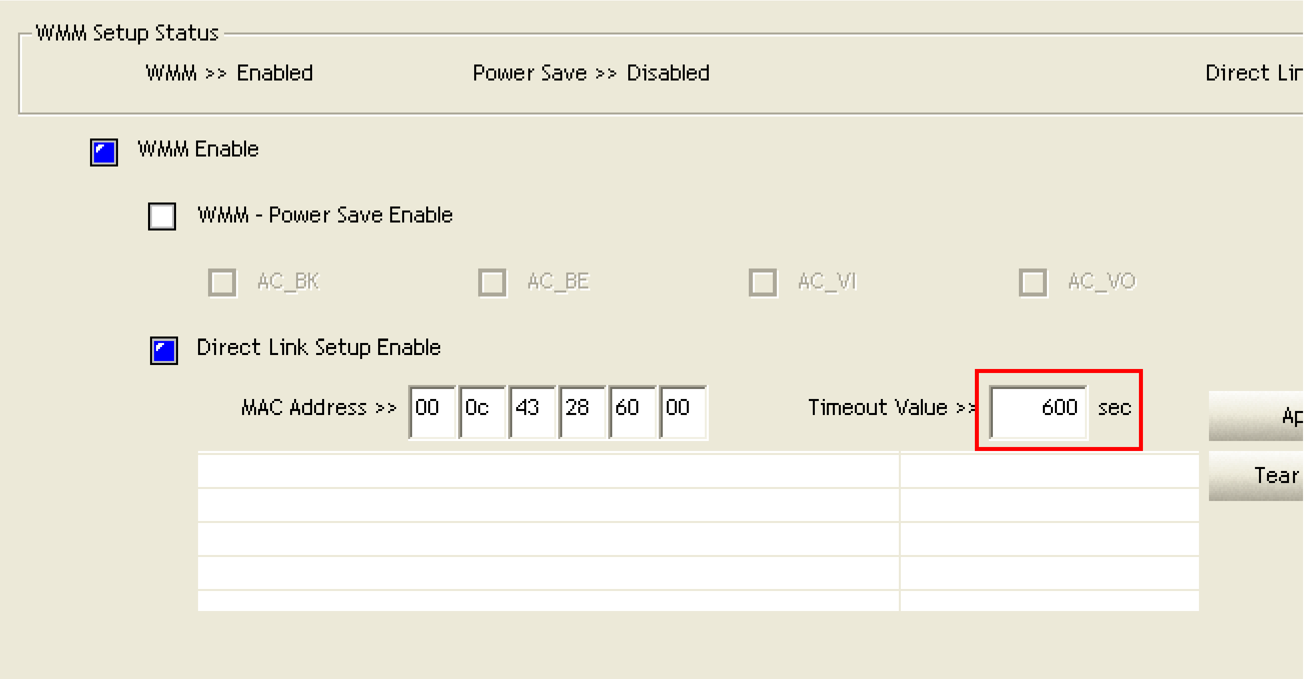
□ WMM - Power Save Enable

□ AC_BK　□ AC_BE　□ AC_VI　□ AC_VO

☑ Direct Link Setup Enable

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

② 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 Lir

☑ WMM Enable

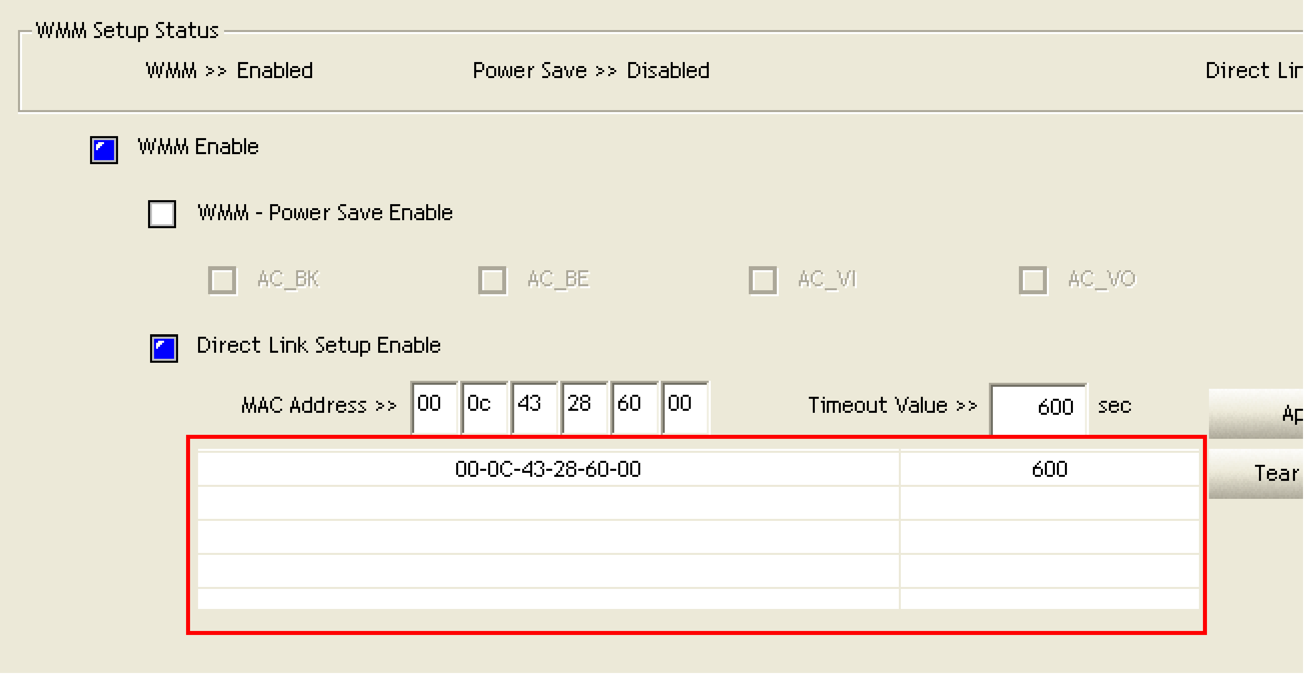
□ WMM - Power Save Enable

□ AC_BK　□ AC_BE　□ AC_VI　□ AC_VO

☑ Direct Link Setup Enable

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

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



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lir

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

☑ Direct Link Setup Enable

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

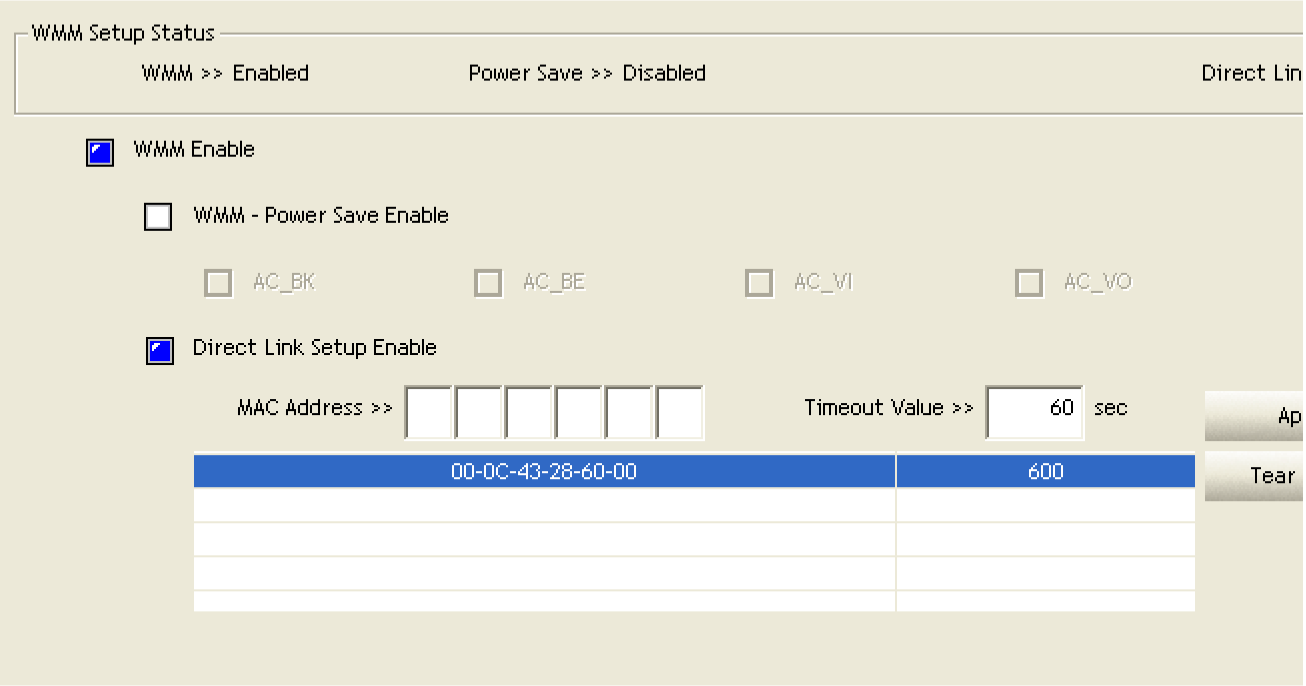
00-0C-43-28-60-00	600

Describe "DLS Status" as follow :

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".



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lin

☑ WMM Enable

□ WMM - Power Save Enable

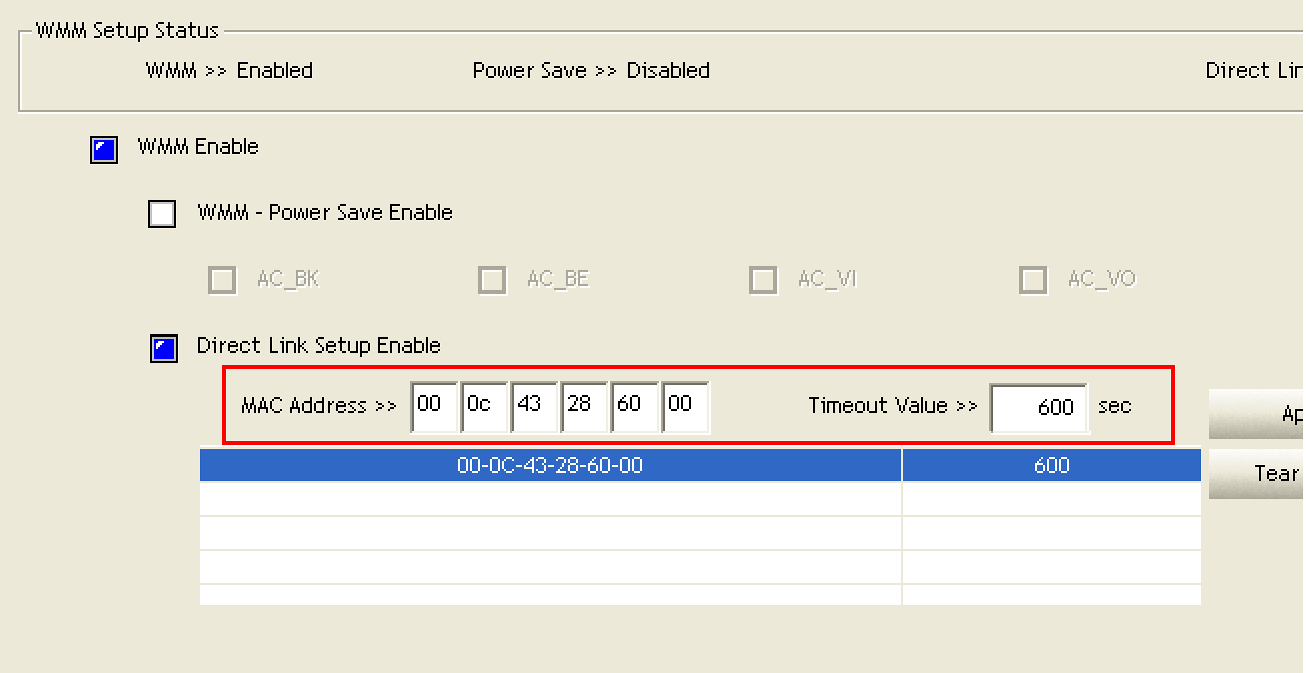
□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

☑ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

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

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



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lir

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

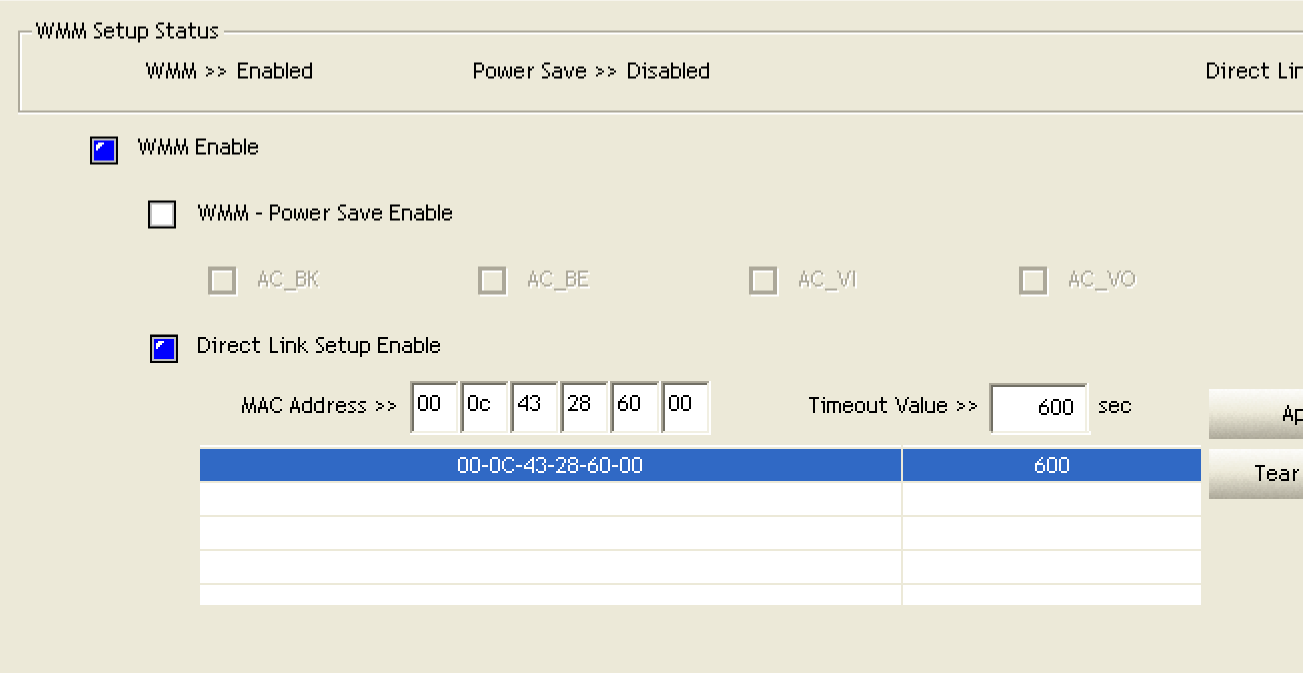
☑ Direct Link Setup Enable

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

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

③ Disconnect Direct Link Setup as follow :

1. Select a direct link STA.



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lir

☑ WMM Enable

□ WMM - Power Save Enable

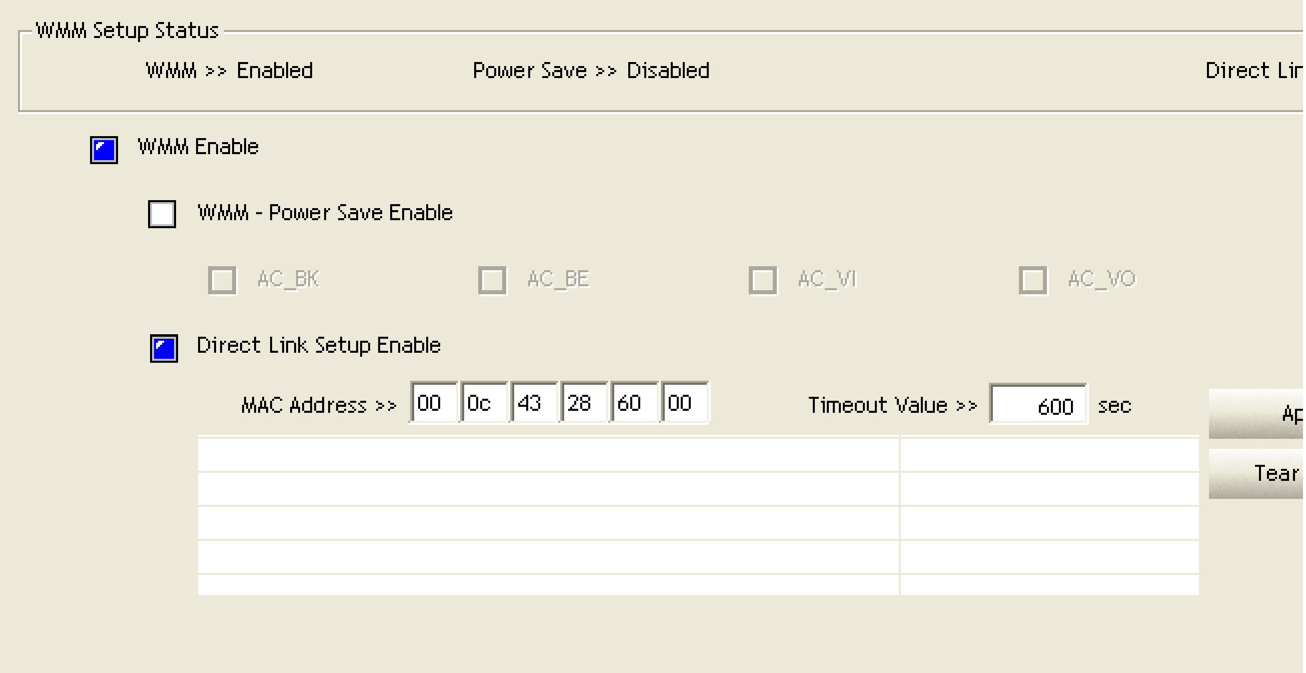
□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

☑ Direct Link Setup Enable

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

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

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



WMM Setup Status

WMM >> Enabled

Power Save >> Disabled

Direct Lir

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

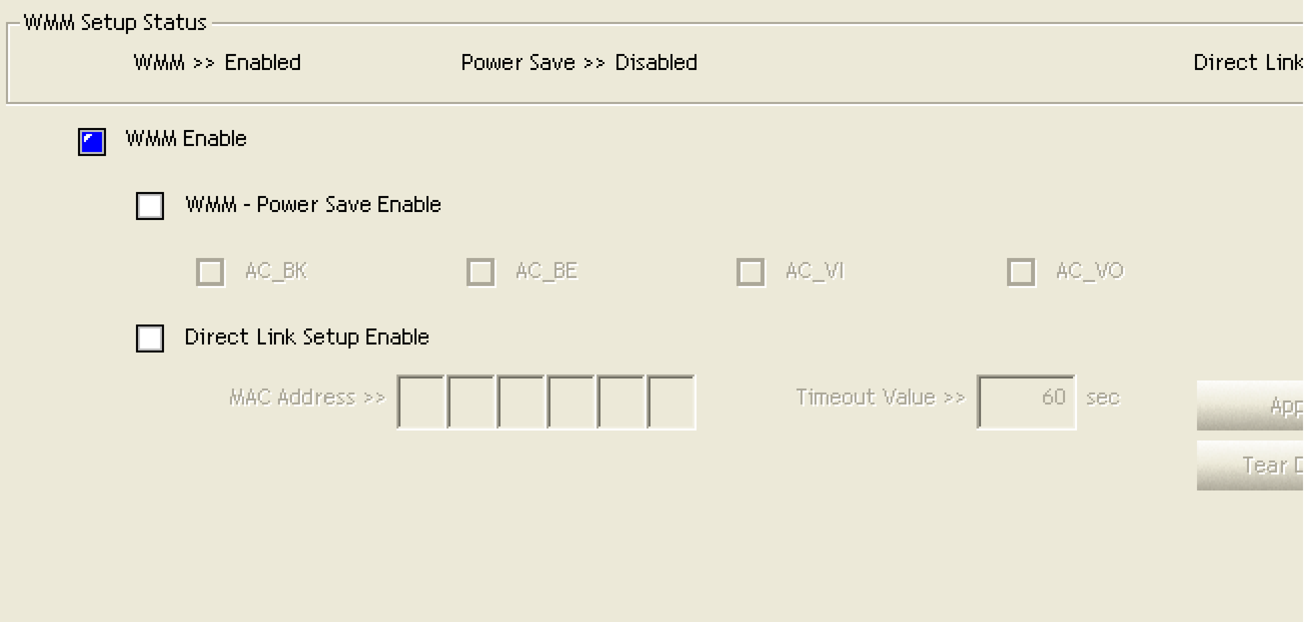
MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

Example to Configure to Enable Wi-Fi Multi-Media

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

1 Click "WMM Enable".



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link

☑ WMM Enable

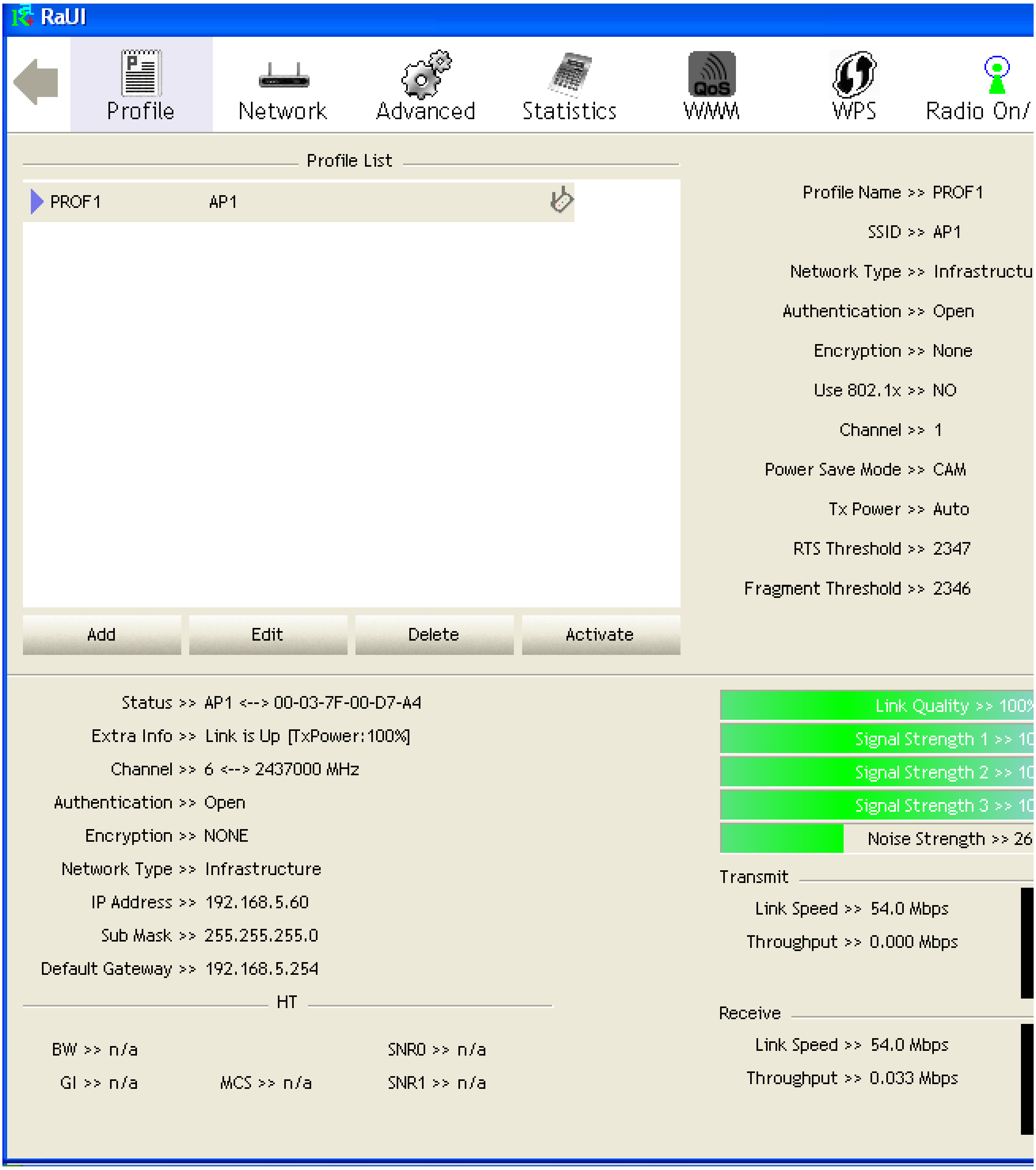
□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

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



PROF1 AP1

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

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

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

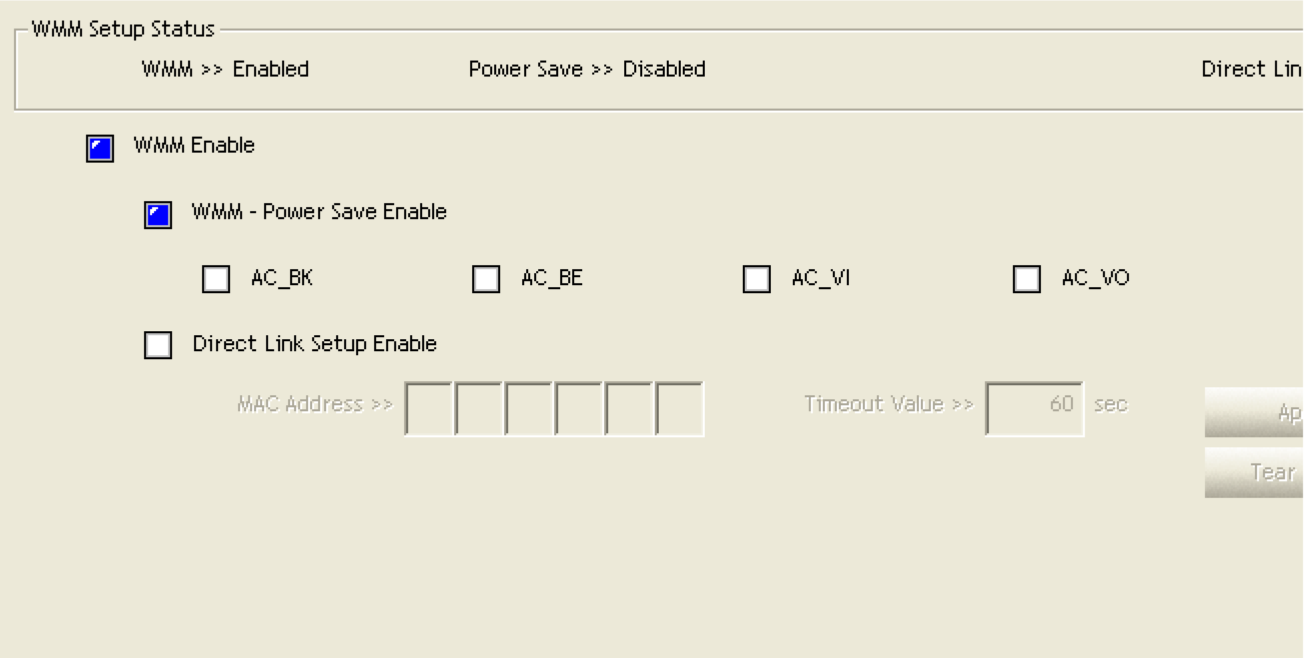
Link Quality >> 100%
Signal Strength 1 >> 10
Signal Strength 2 >> 10
Signal Strength 3 >> 10
Noise Strength >> 26

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

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

Example to Configure to Enable WMM Power Save

1 Click "WMM-Power Save Enable".



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Lin

☑ WMM Enable

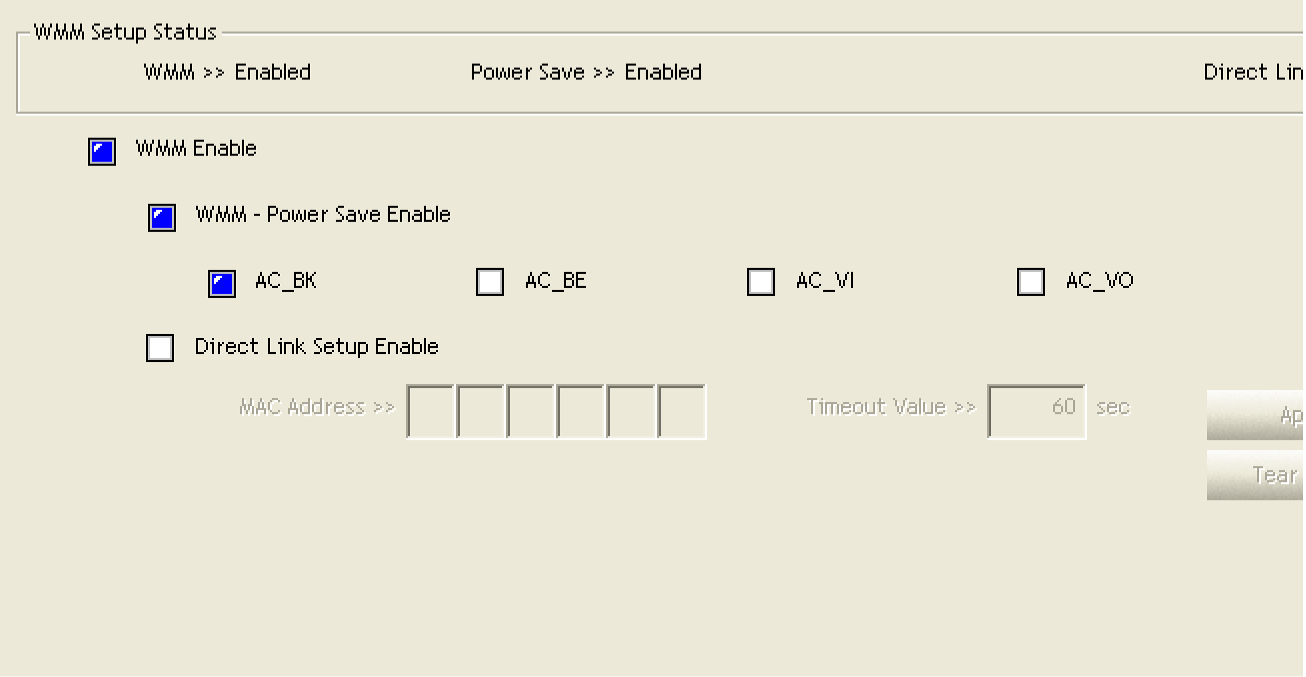
☑ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

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



WMM Setup Status

WMM >> Enabled   Power Save >> Enabled   Direct Lin

☑ WMM Enable

☑ WMM - Power Save Enable

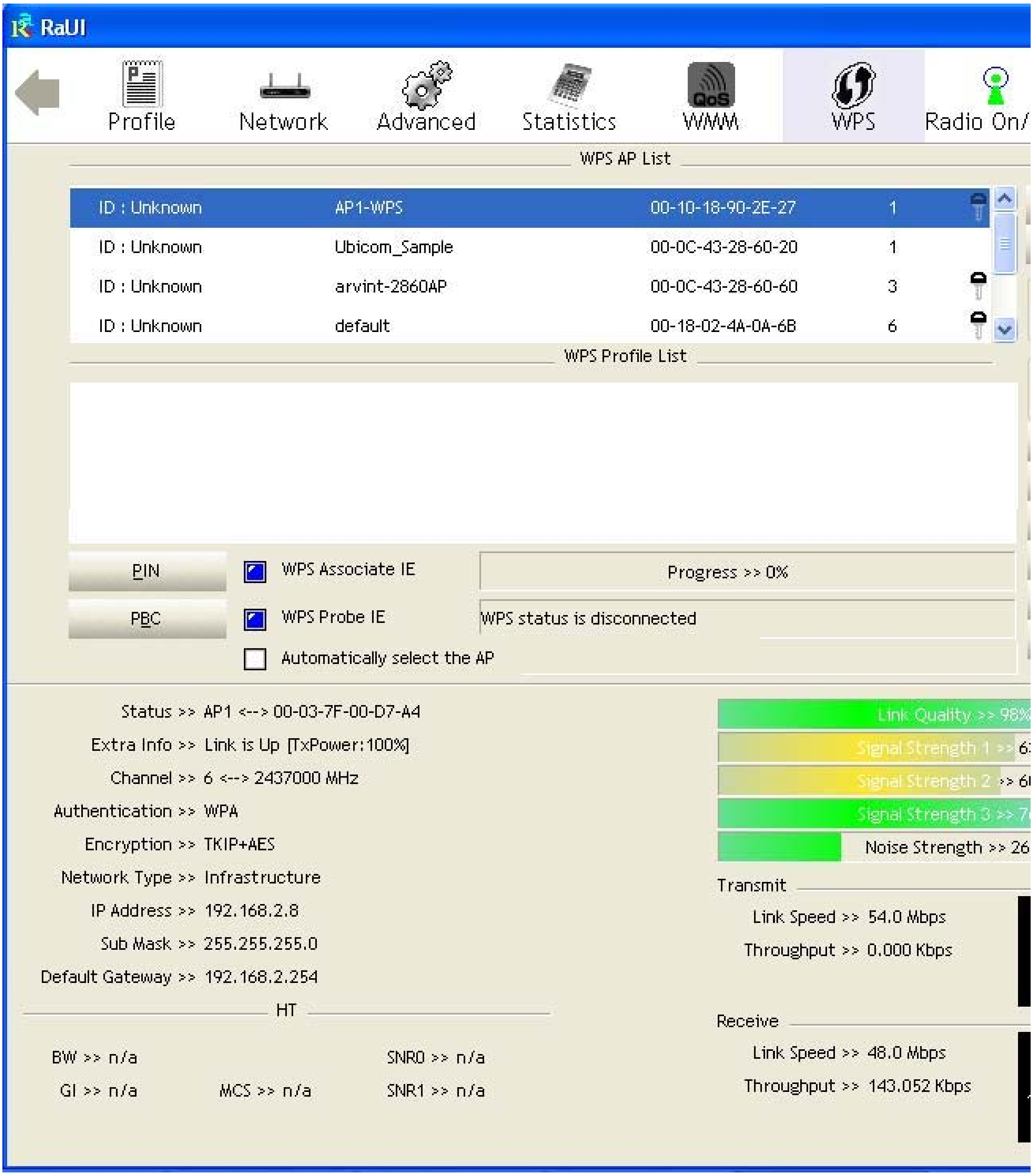
☑ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

WPS

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



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

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.2.8

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.2.254

BW >> n/a

SNR0 >> n/a

GI >> n/a

MCS >> n/a

SNR1 >> n/a

Link Quality >> 98%

Signal Strength 1 >> 6

Signal Strength 2 >> 6

Signal Strength 3 >> 7

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

Receive

Link Speed >> 48.0 Mbps

Throughput >> 143.052 Kbps

Figure 2-7-1 WPS function

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

① ▼

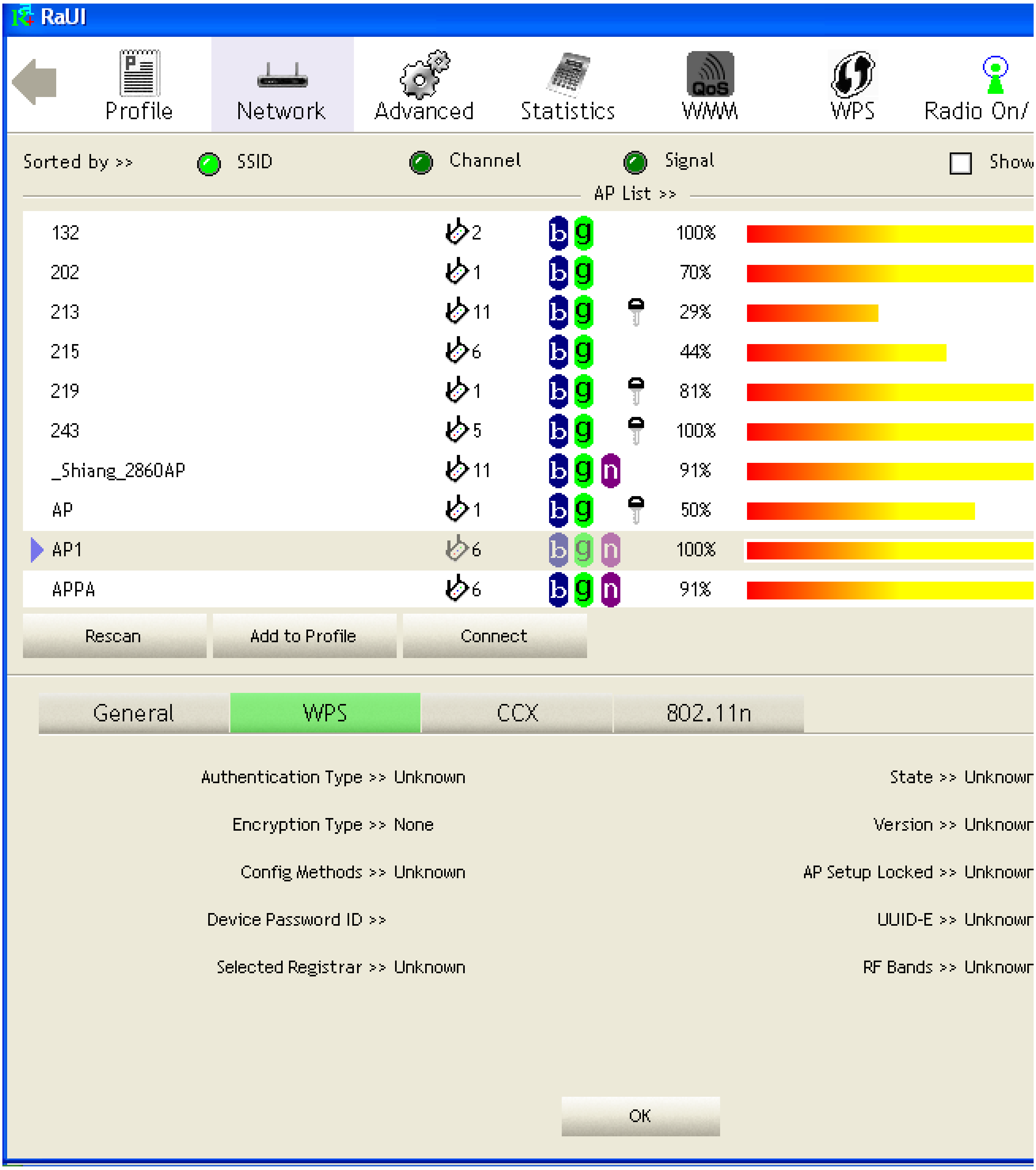
Show the information of Status Section. Hide

② ▲

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 :



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

AP List >>

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

Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Unknowr

Version >> Unknowr

AP Setup Locked >> Unknowr

UUID-E >> Unknowr

RF Bands >> Unknowr

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

❷ 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.

❸ 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

❹ 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

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

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

❼ Version : WPS specified version.

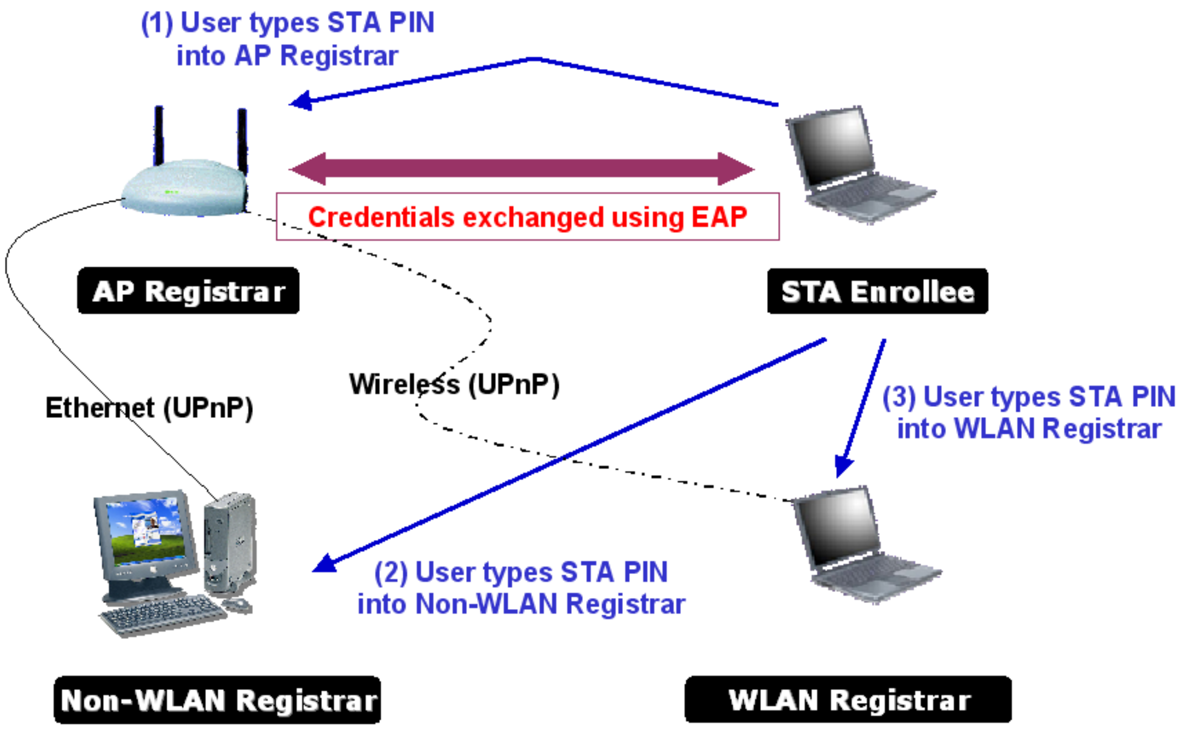
❽ AP Setup Locked : Indicate if AP has entered a setup locked state.

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

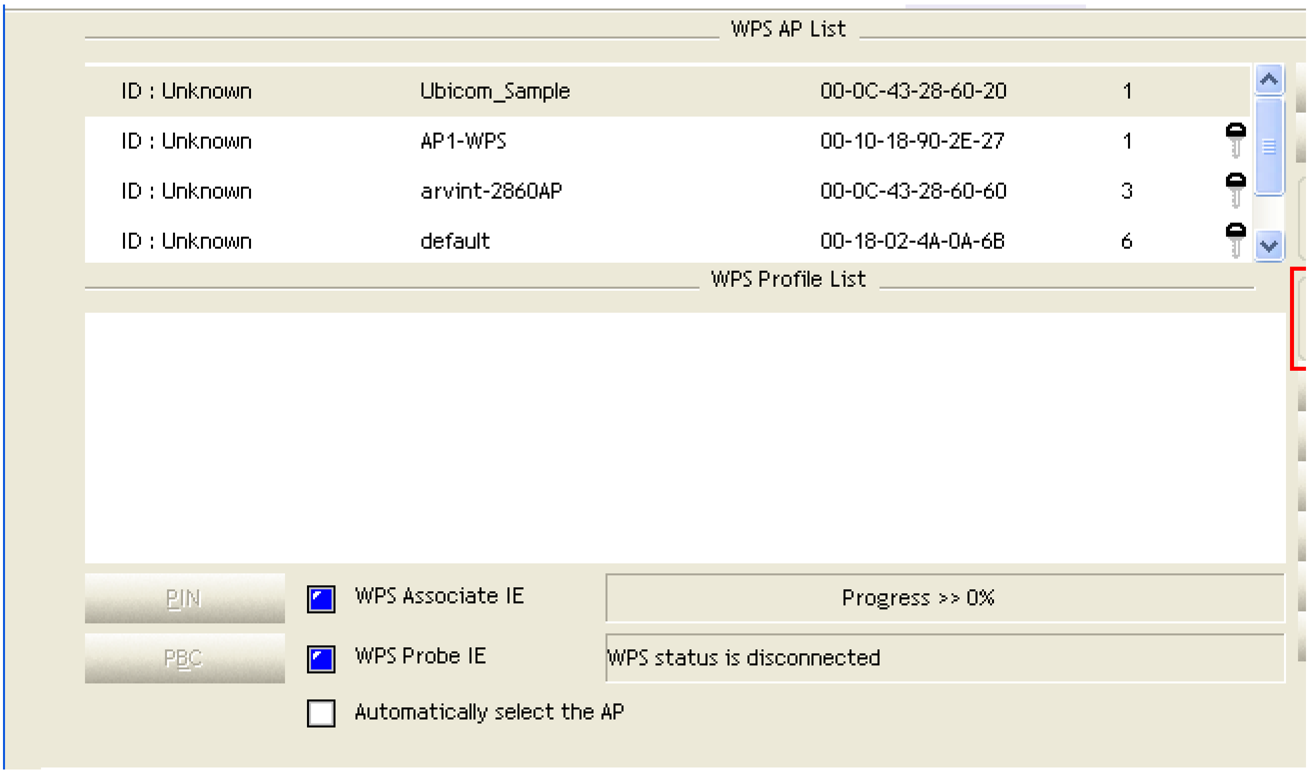
❿ RF Bands : Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

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.



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

☑ WPS Associate IE

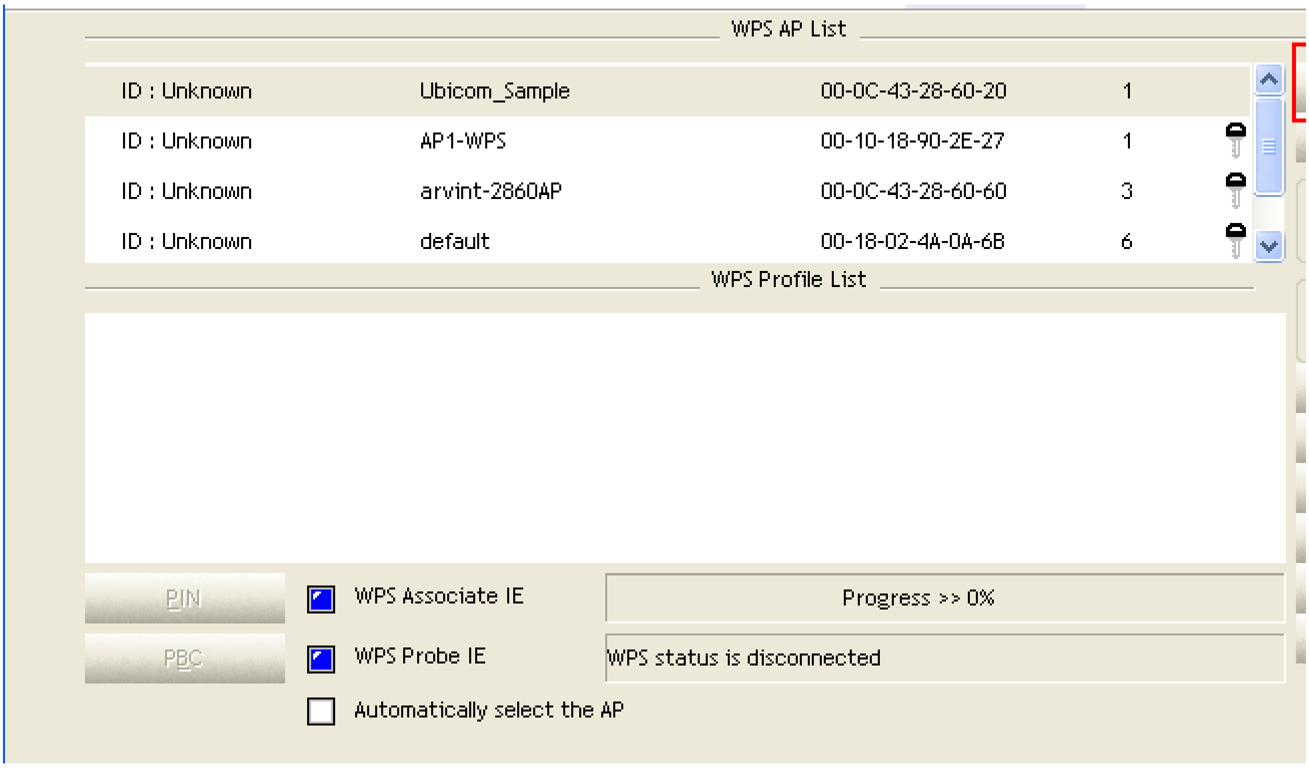
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



WPS AP List

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

WPS Profile List

PIN

PBC

☑ WPS Associate IE

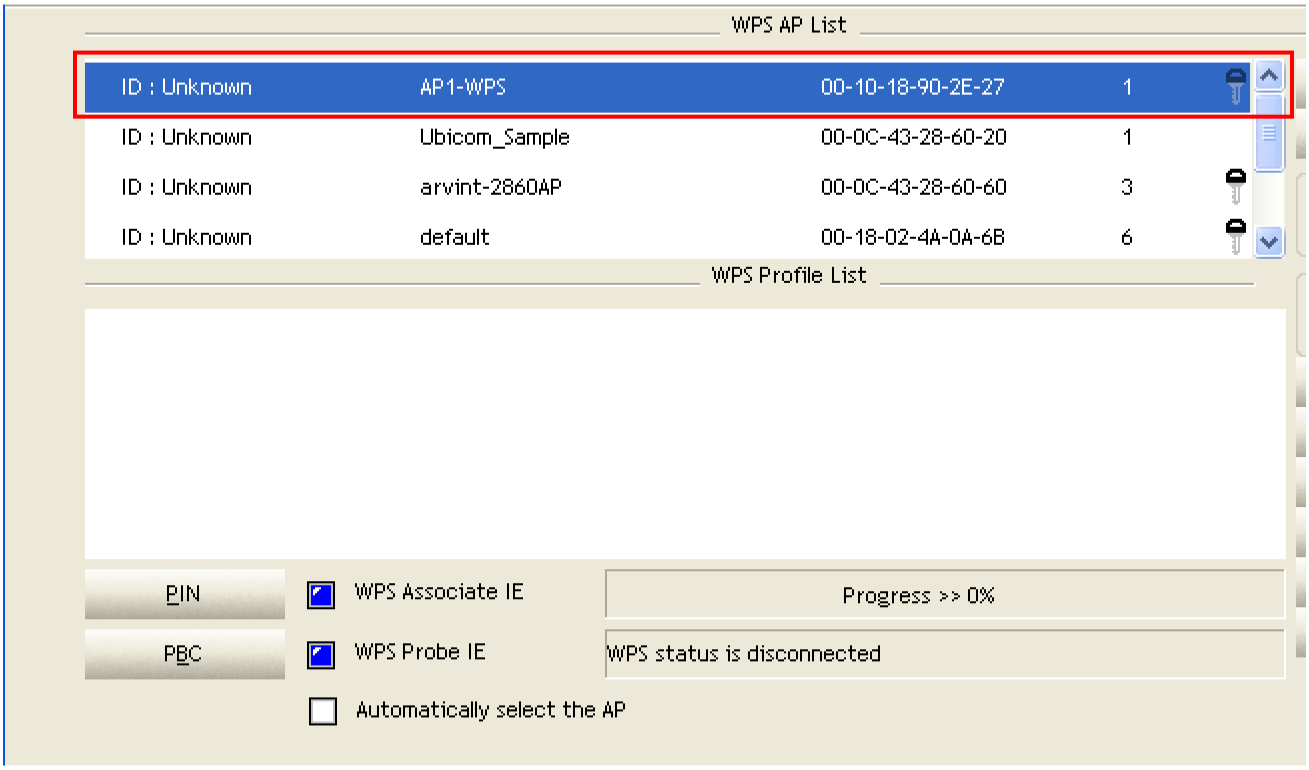
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



WPS AP List

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

WPS Profile List

PIN

PBC

☑ WPS Associate IE

☑ WPS Probe IE

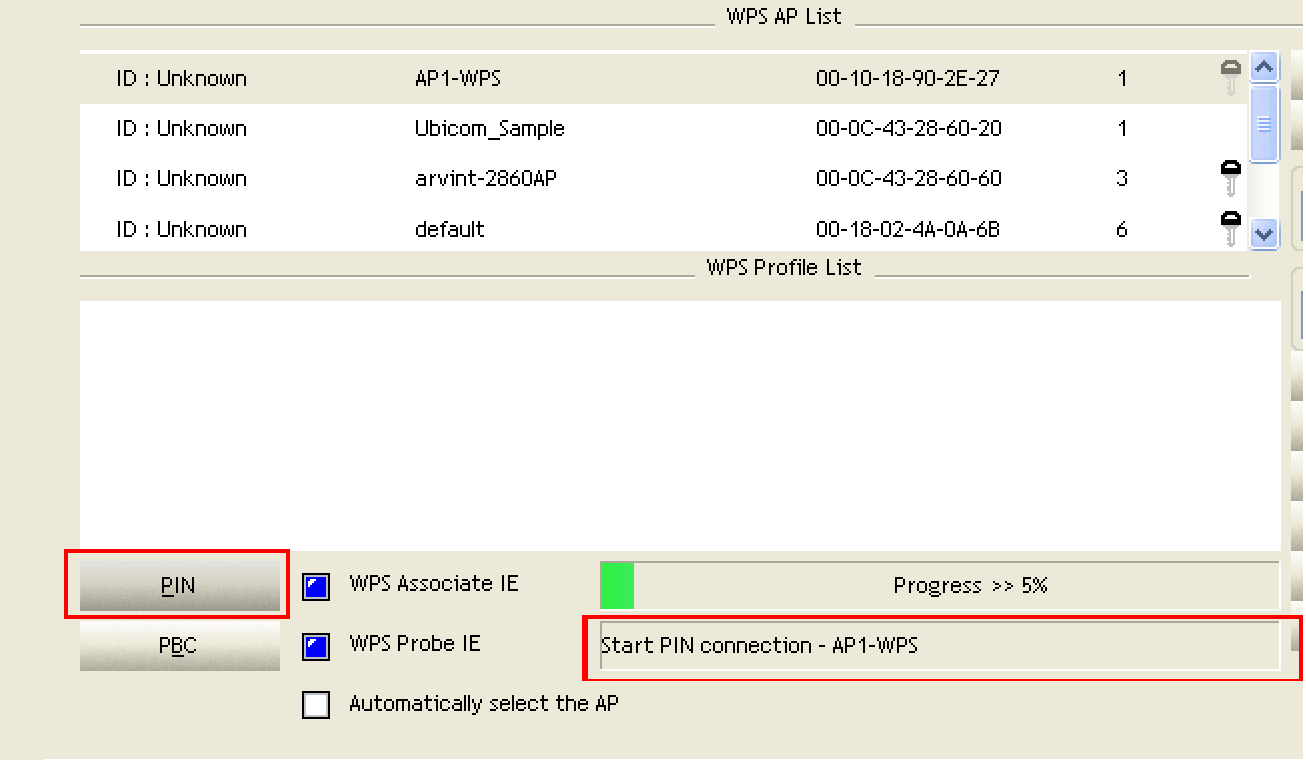
□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

4 Click "PIN" button to start PIN connection.

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



WPS AP List

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

WPS Profile List

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

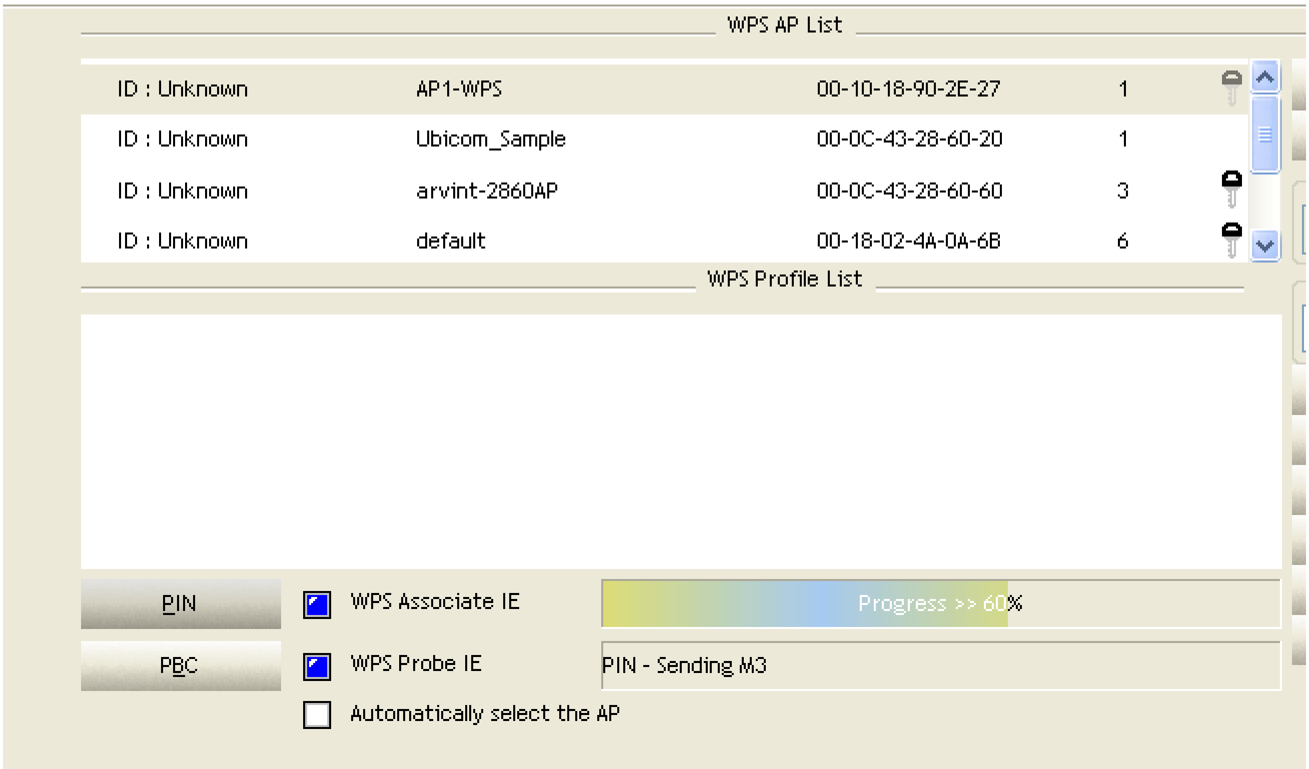
Progress >> 5%

Start PIN connection - AP1-WPS

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

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

6 The result will look like the below figure.



WPS AP List

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

WPS Profile List

☑ WPS Associate IE

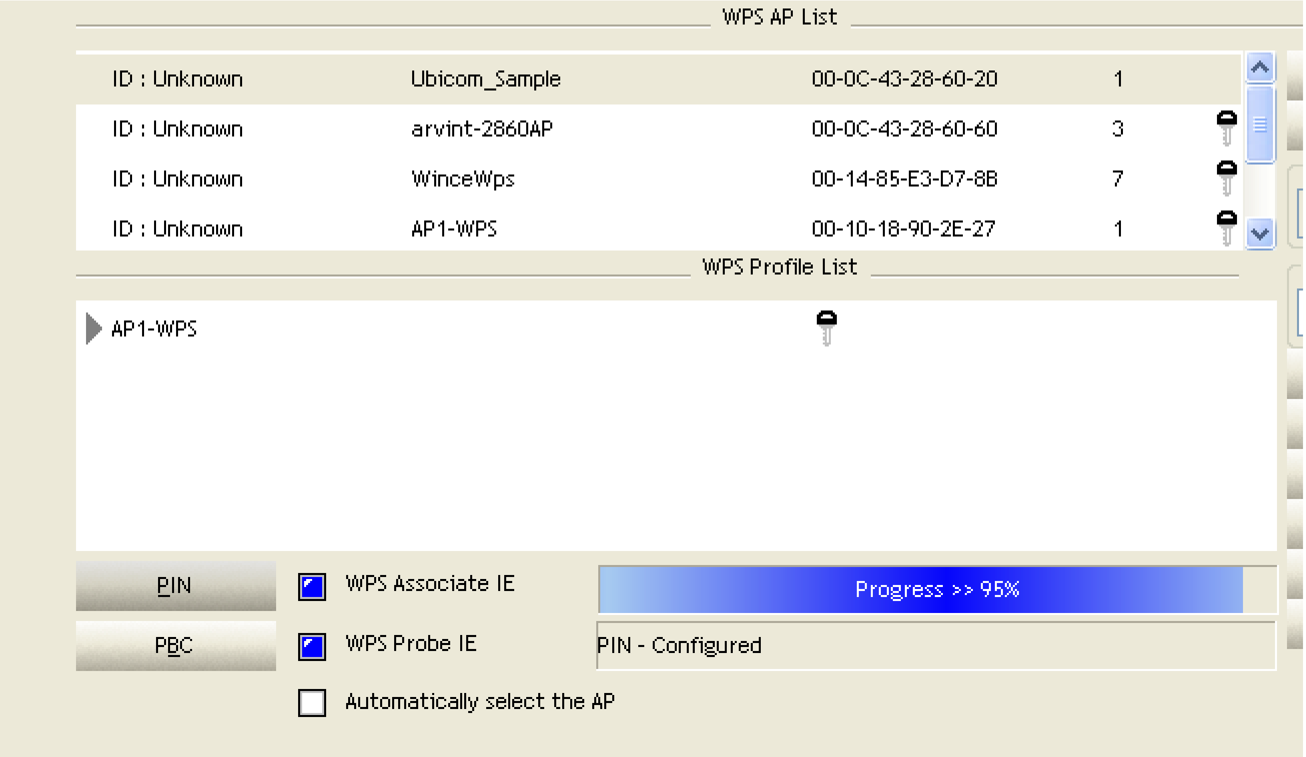
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 60%

PIN - Sending M3

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



WPS AP List

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

WPS Profile List

AP1-WPS

☑ WPS Associate IE

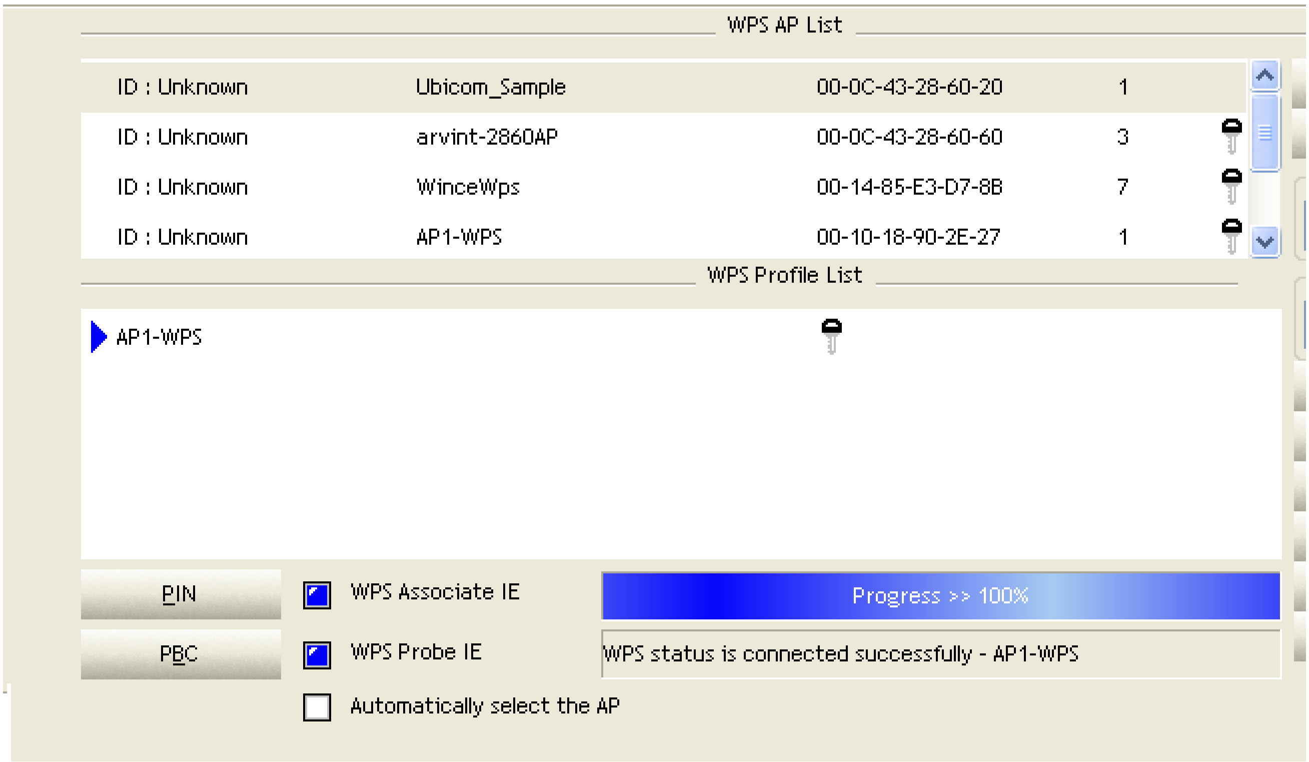
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 95%

PIN - Configured

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



WPS AP List

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

WPS Profile List

AP1-WPS

☑ WPS Associate IE

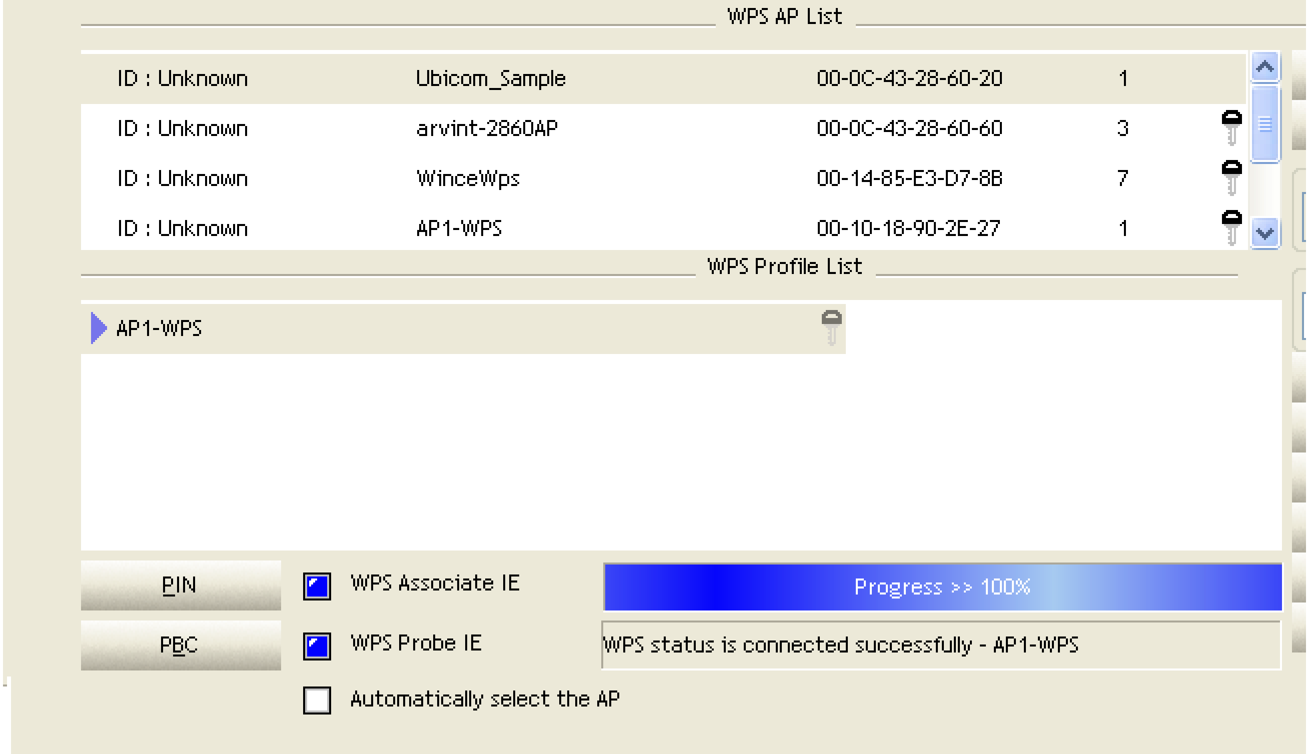
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - AP1-WPS

9 Click "Detail" button.



WPS AP List

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

WPS Profile List

AP1-WPS

☑ WPS Associate IE

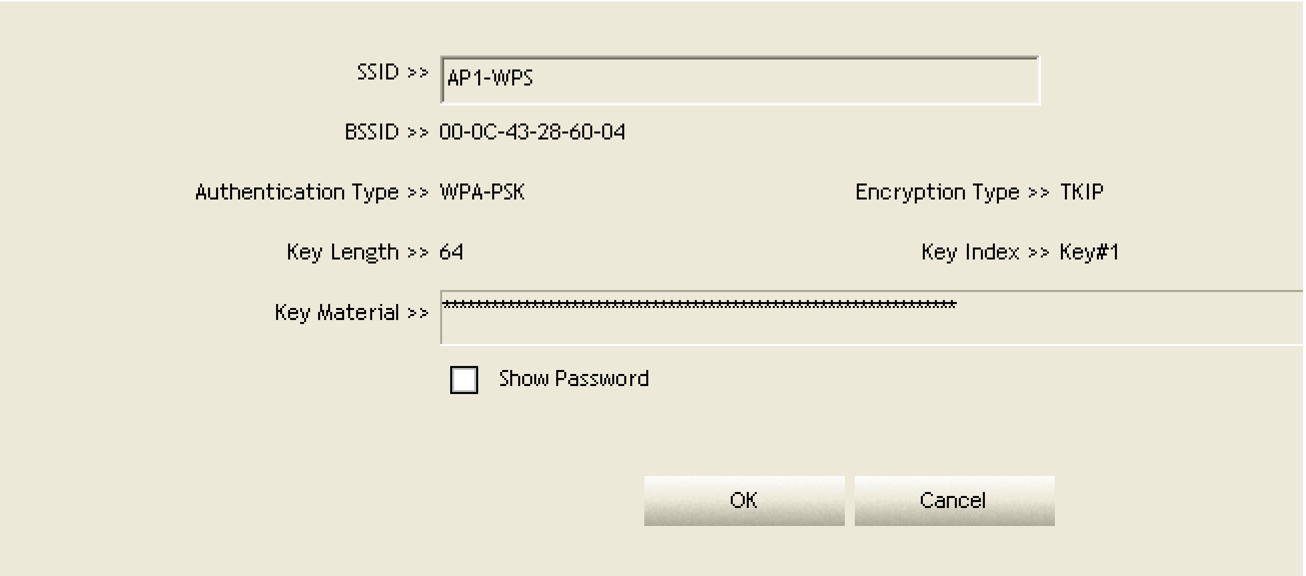
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - AP1-WPS

10 You will look like the below figure.



SSID >> AP1-WPS

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

Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Key Length >> 64

Key Index >> Key#1

Key Material >> **

□ Show Password

*If Credential#1 is reliable and present, 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 :

❶ Asuccessful PIN Configuration :

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

❷ WPS configuration doesn't complete after **two-minute connection** : WPS Eap

process failed.

❸ 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.

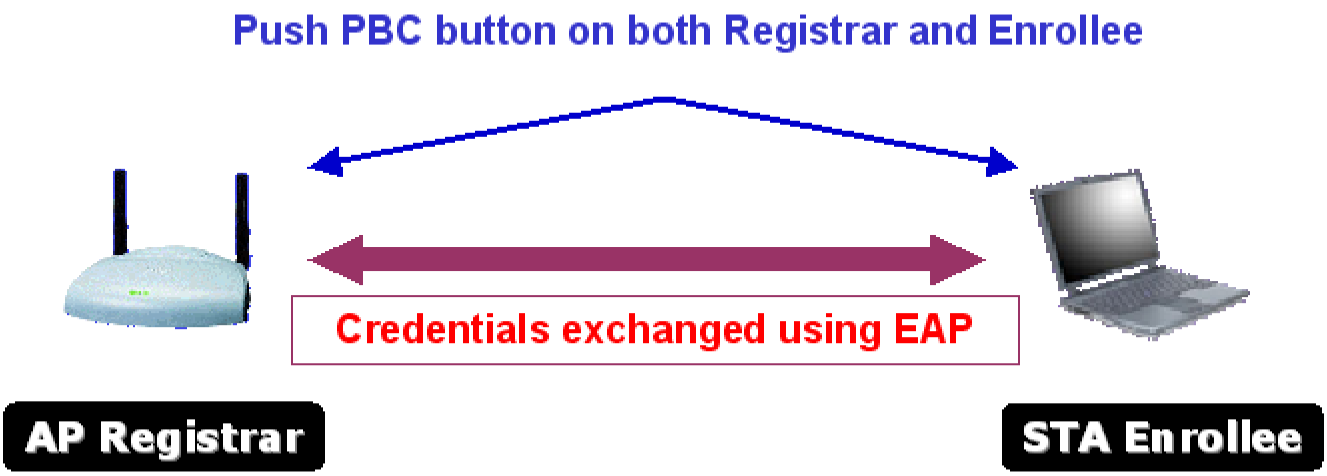
4. An inappropriate EAP-FAIL received.

Example to Add to Registrar Using PBC Method

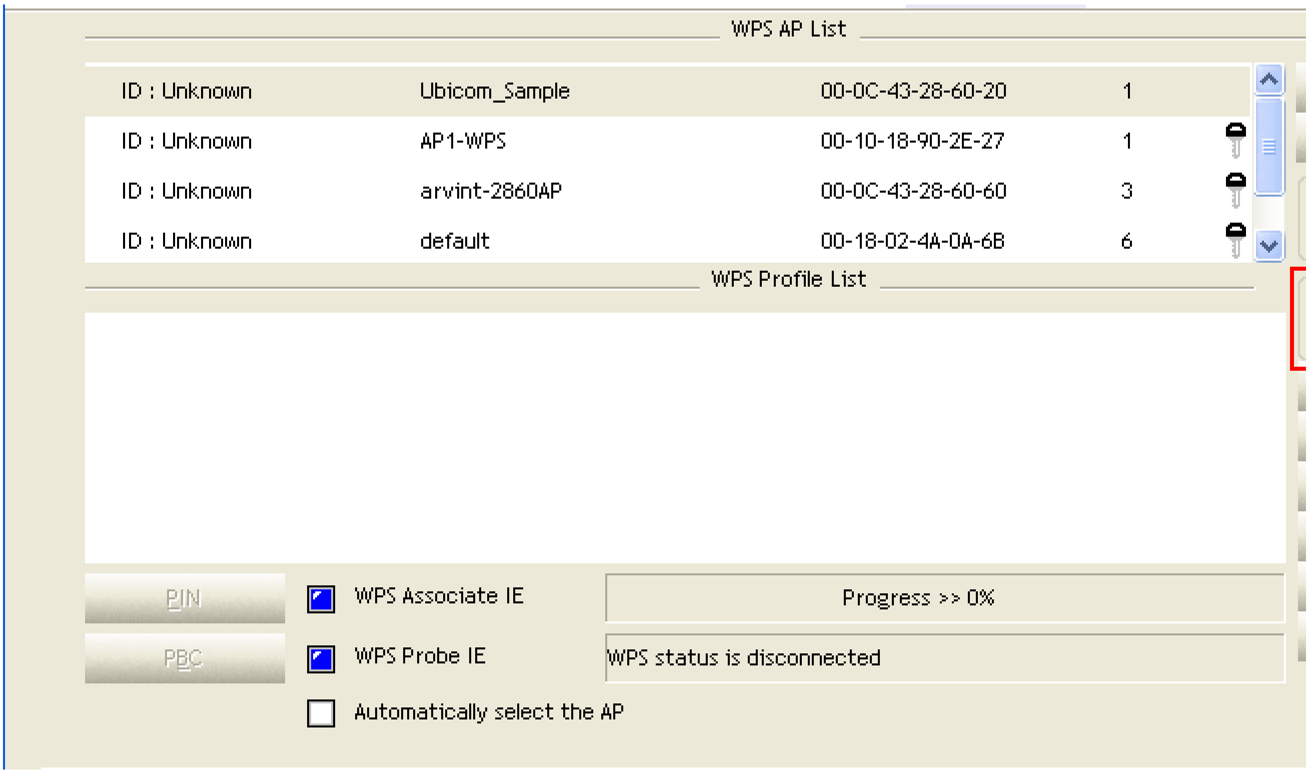
The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If only one Registrar in PBC mode, which PBC mode is obtained from ID 0x0004, is found after a complete scan, the Enrollee can immediately begin running the 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
Credentials exchanged using EAP
AP Registrar
STA Enrollee

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


WPS AP List

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

WPS Profile List

☑ WPS Associate IE

☑ WPS Probe IE

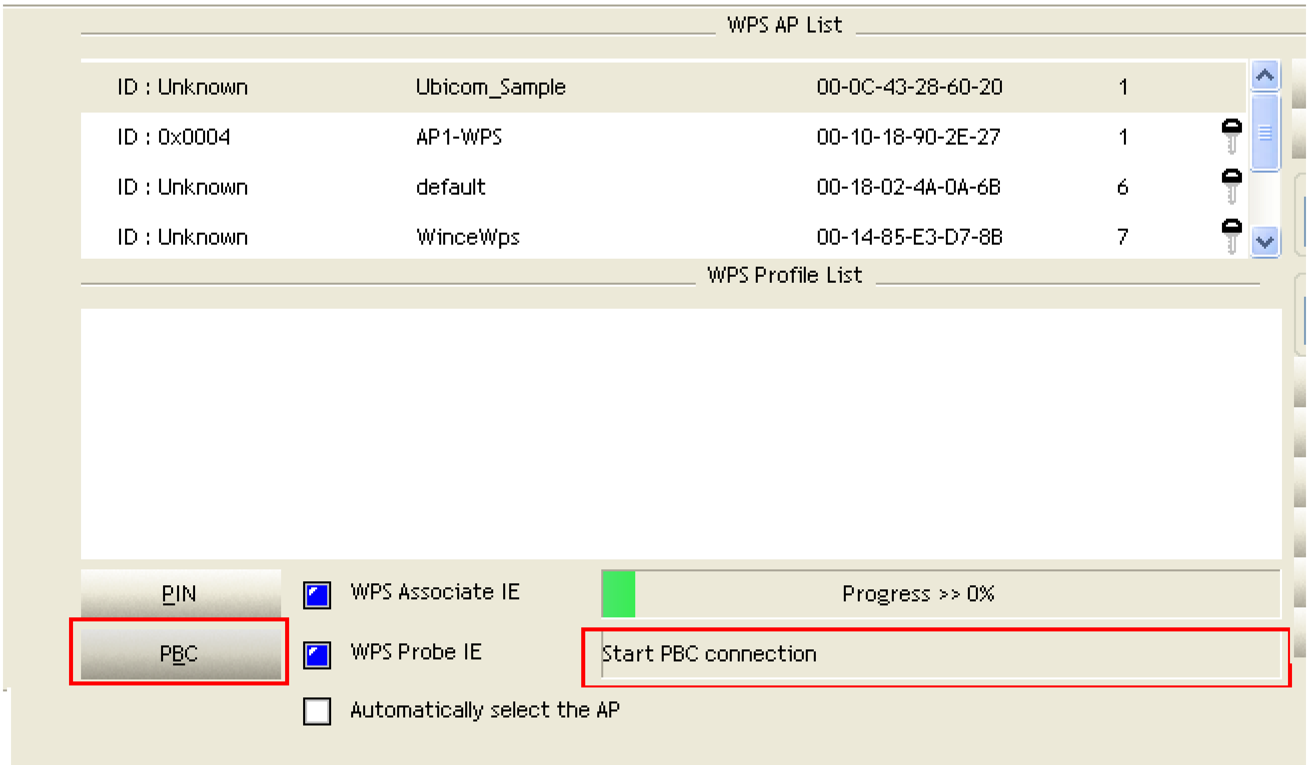
□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

2 Click PBC to start PBC connection.

3 Push PBC on AP.



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

☑ WPS Associate IE

☑ WPS Probe IE

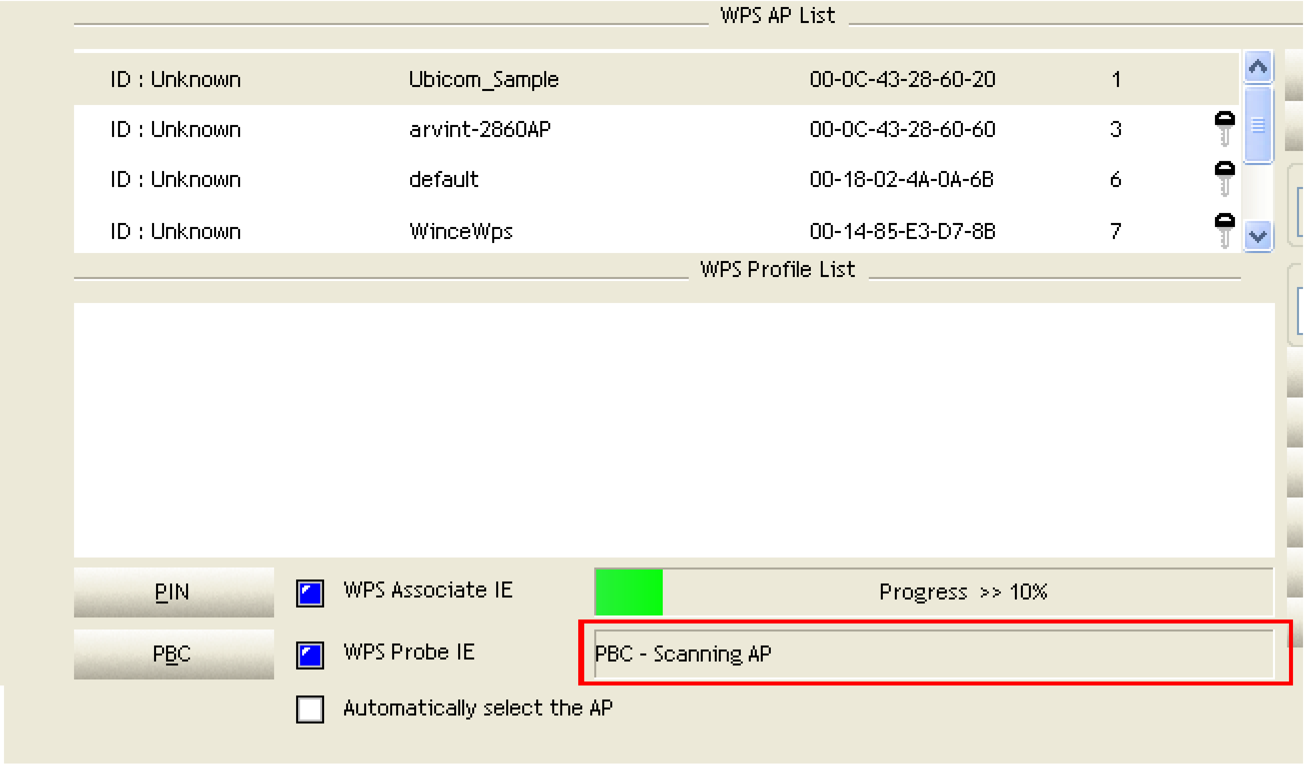
□ Automatically select the AP

Progress >> 0%

Start PBC connection

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

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



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

☑ WPS Associate IE

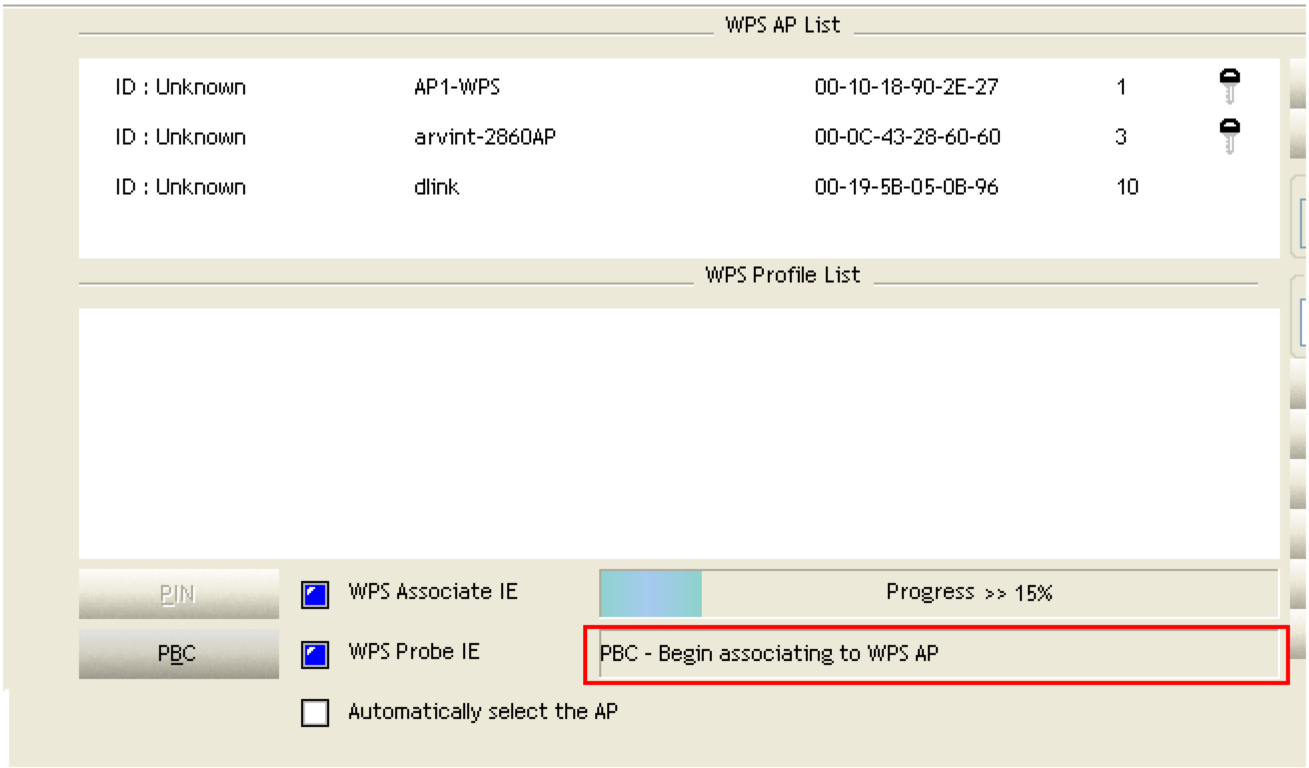
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 10%

PBC - Scanning AP

❺ When finding only one AP, join it.



WPS AP List

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

WPS Profile List

☑ WPS Associate IE

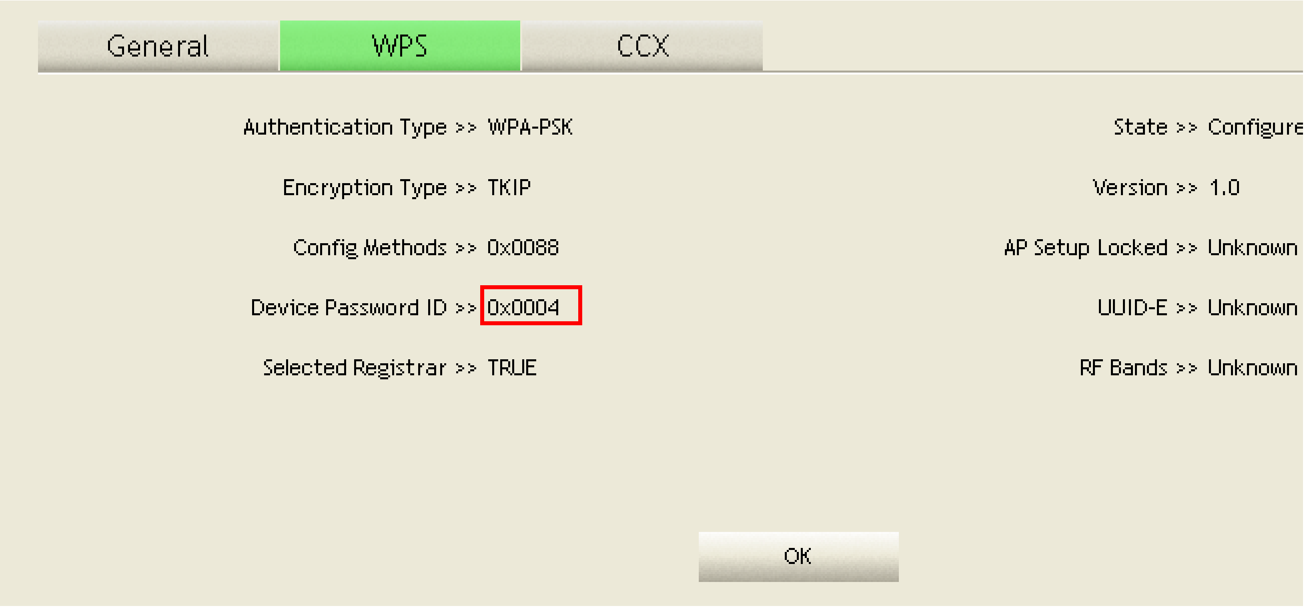
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 15%

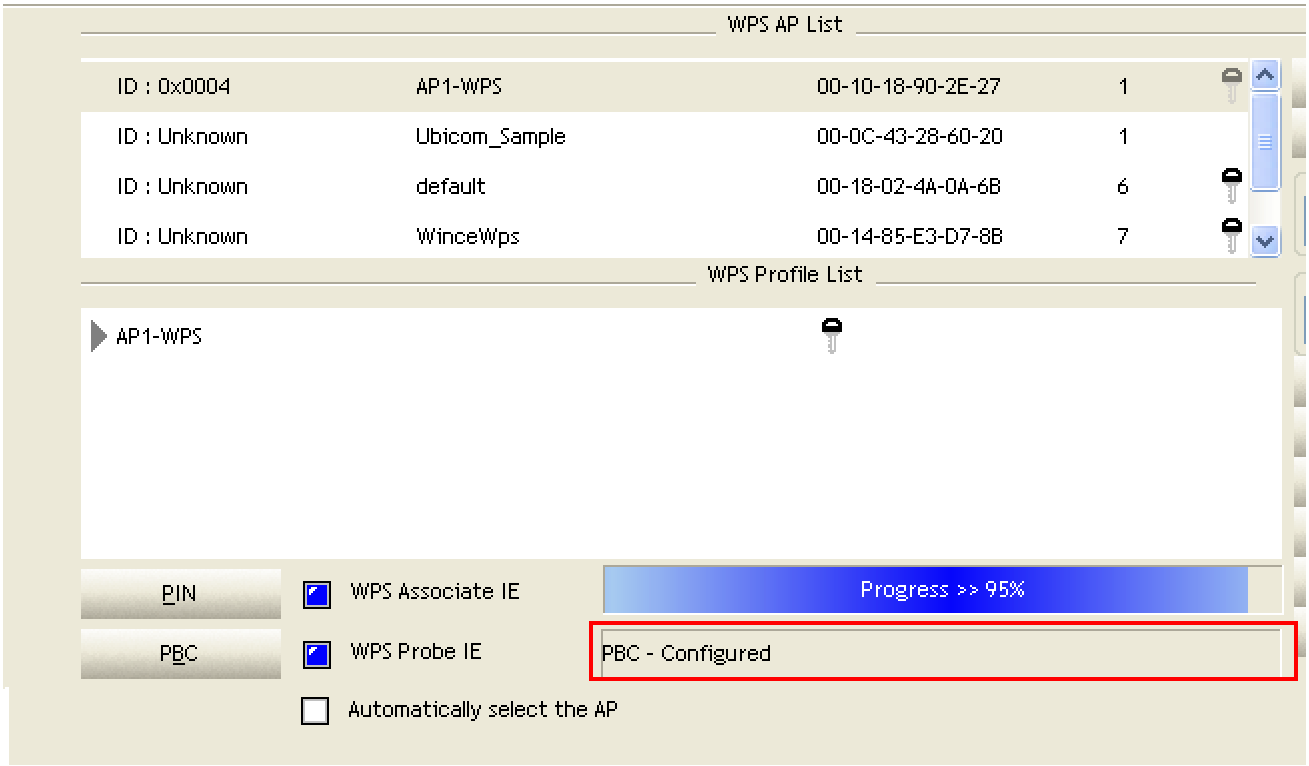
PBC - Begin associating to WPS AP

❻ Check WPS Information on available WPS APs



Authentication Type >> WPA-PSK	State >> Configure
Encryption Type >> TKIP	Version >> 1.0
Config Methods >> 0x0088	AP Setup Locked >> Unknown
Device Password ID >> 0x0004	UUID-E >> Unknown
Selected Registrar >> TRUE	RF Bands >> Unknown

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



WPS AP List

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

WPS Profile List

AP1-WPS

☑ WPS Associate IE

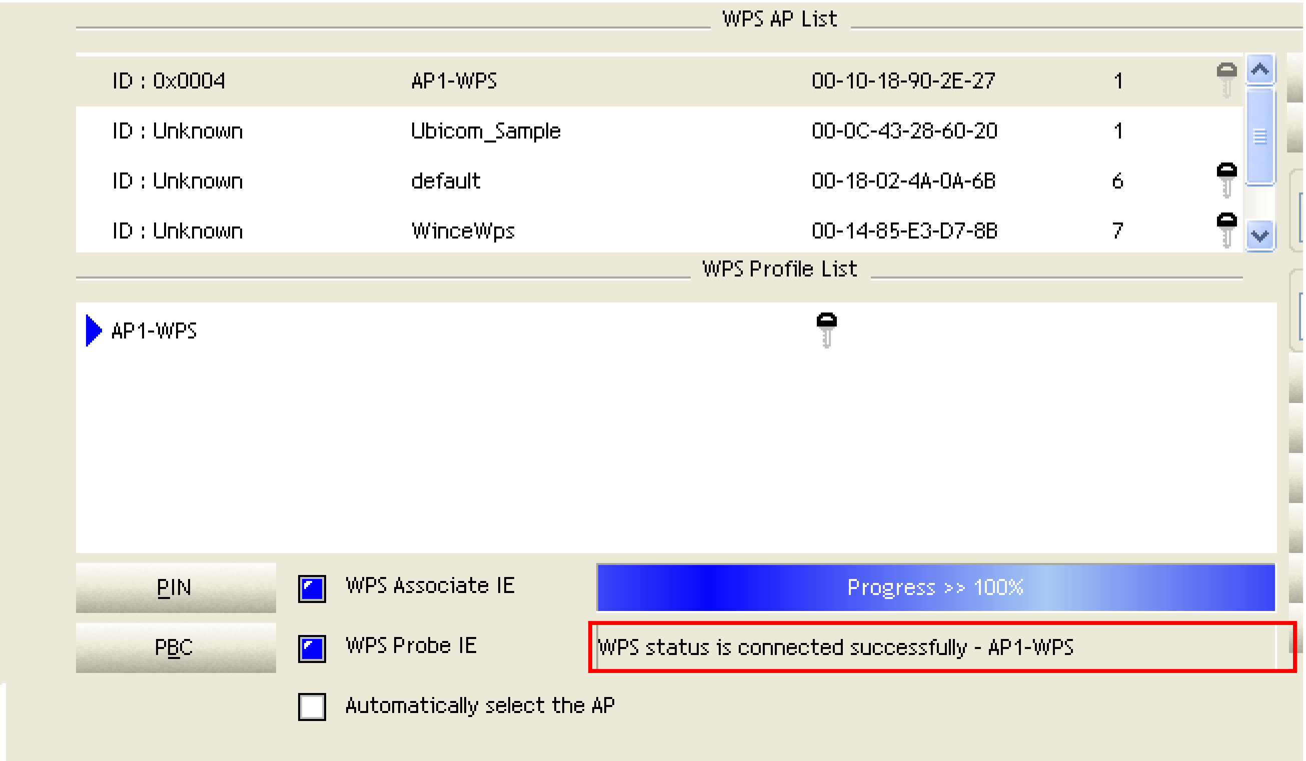
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 95%

PBC - Configured

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



WPS AP List

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

WPS Profile List

AP1-WPS

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - AP1-WPS

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

❶ 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

❷ No PBC AP available :

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

❸ Too Many PBC AP available :

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

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

❺ 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 :

❶ 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.

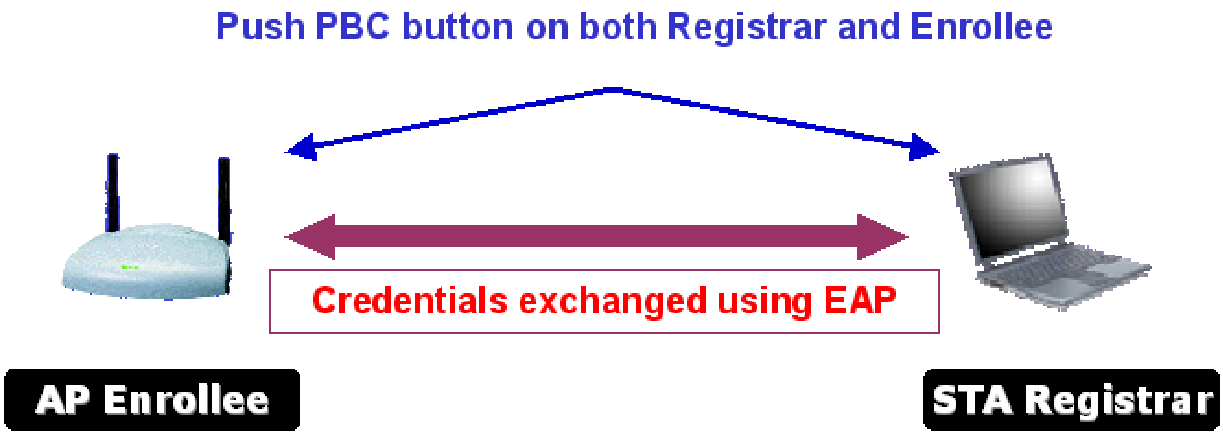
STA would regard these two APs as a dual-radio AP and select one band to connect.

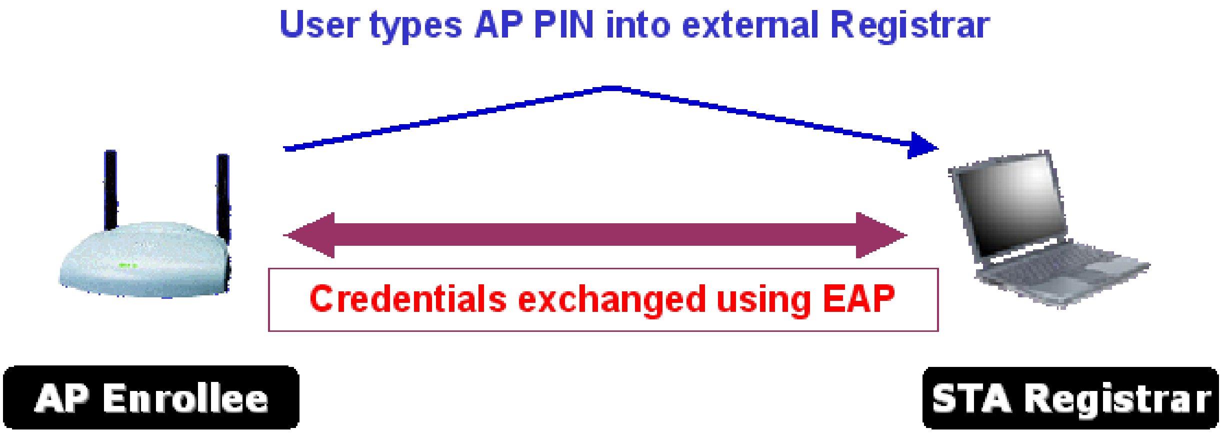
❷ Different UUID-E :

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.

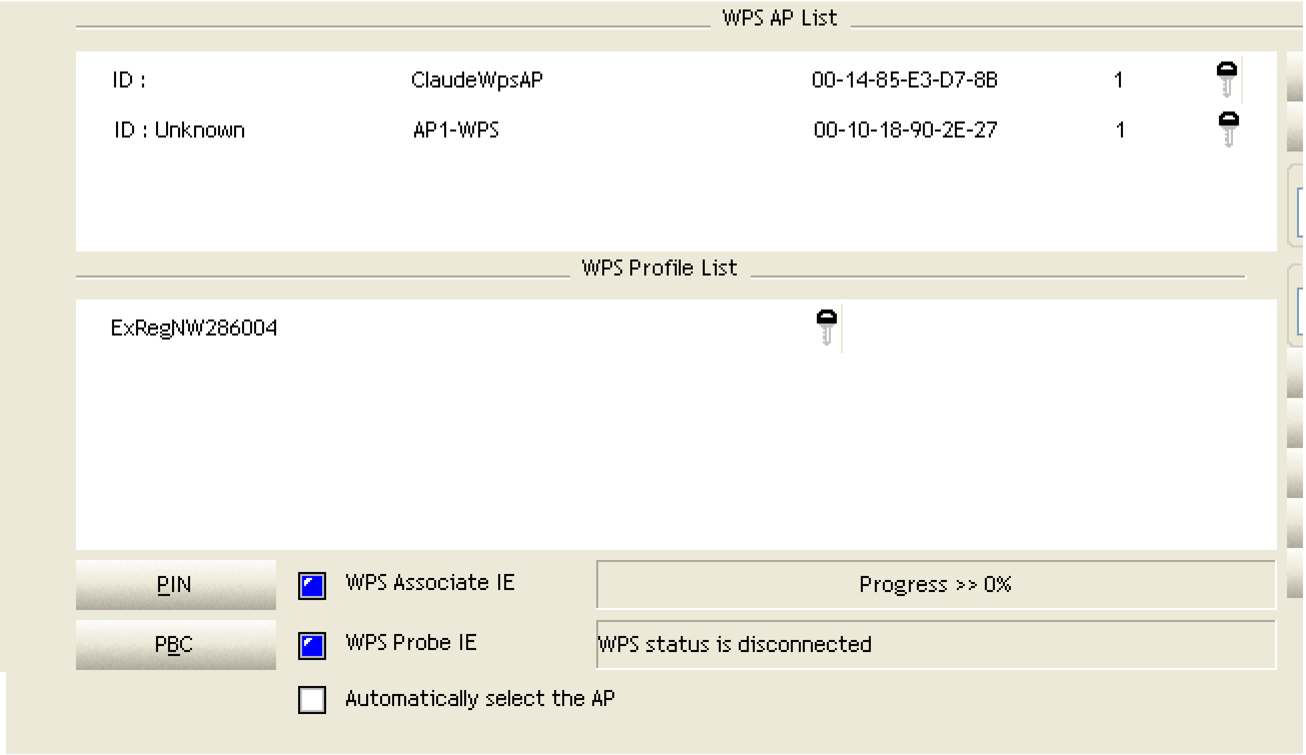
STA would regard these two APs as two different APs and wait until only one PBC AP is available.

Example to Configure a Network/AP Using PIN or PBC Method


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


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

❶ 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

☑ WPS Associate IE

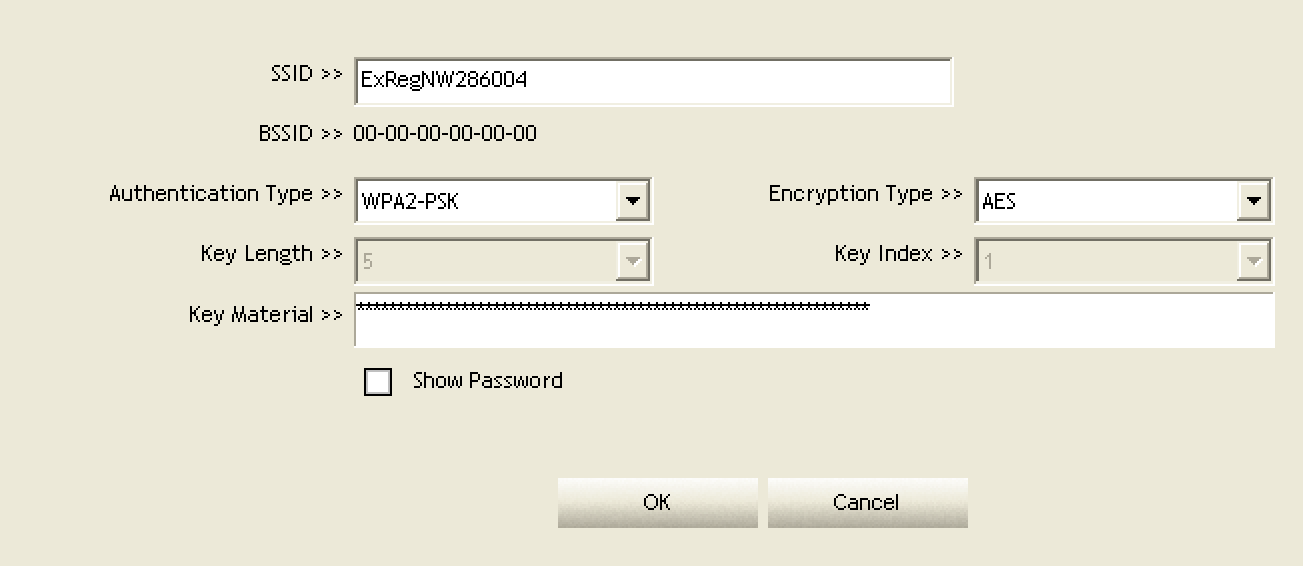
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

❷ 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

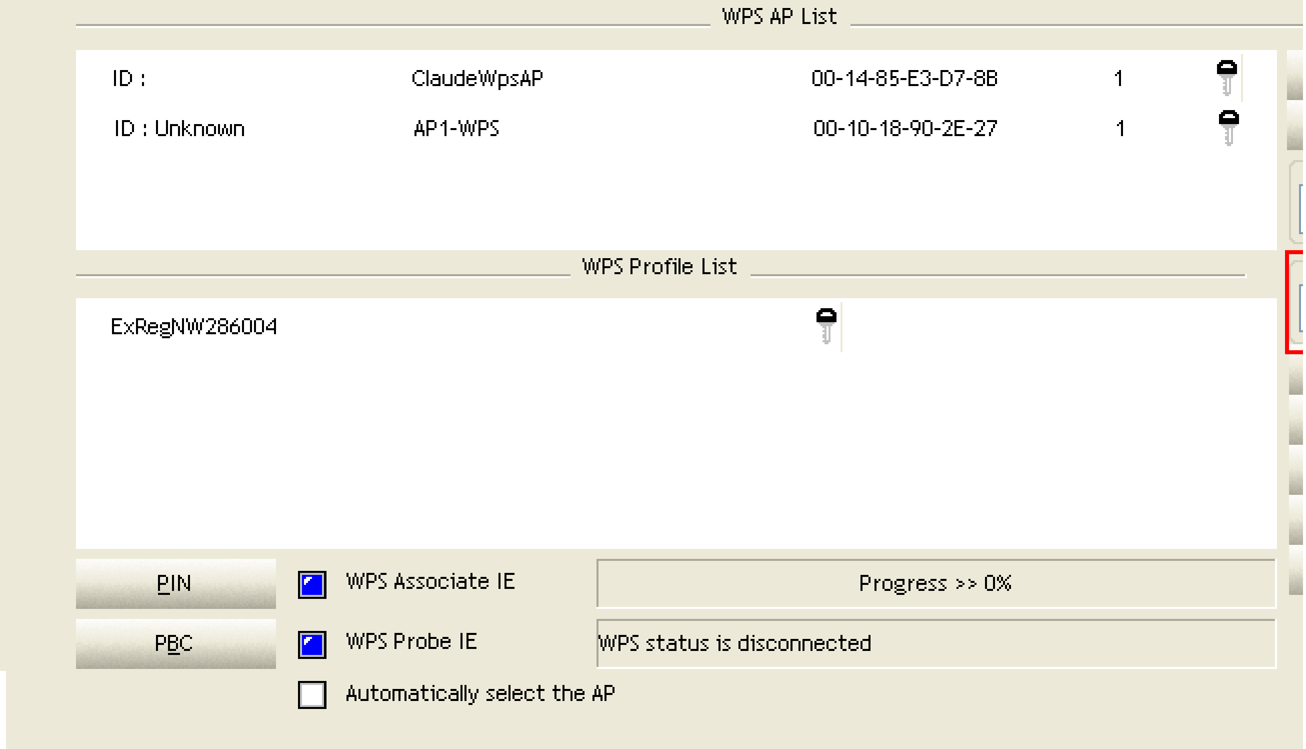
Key Index >> 1

Key Material >> **

□ Show Password

OK   Cancel

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



WPS AP List

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

WPS Profile List

ExRegNW286004

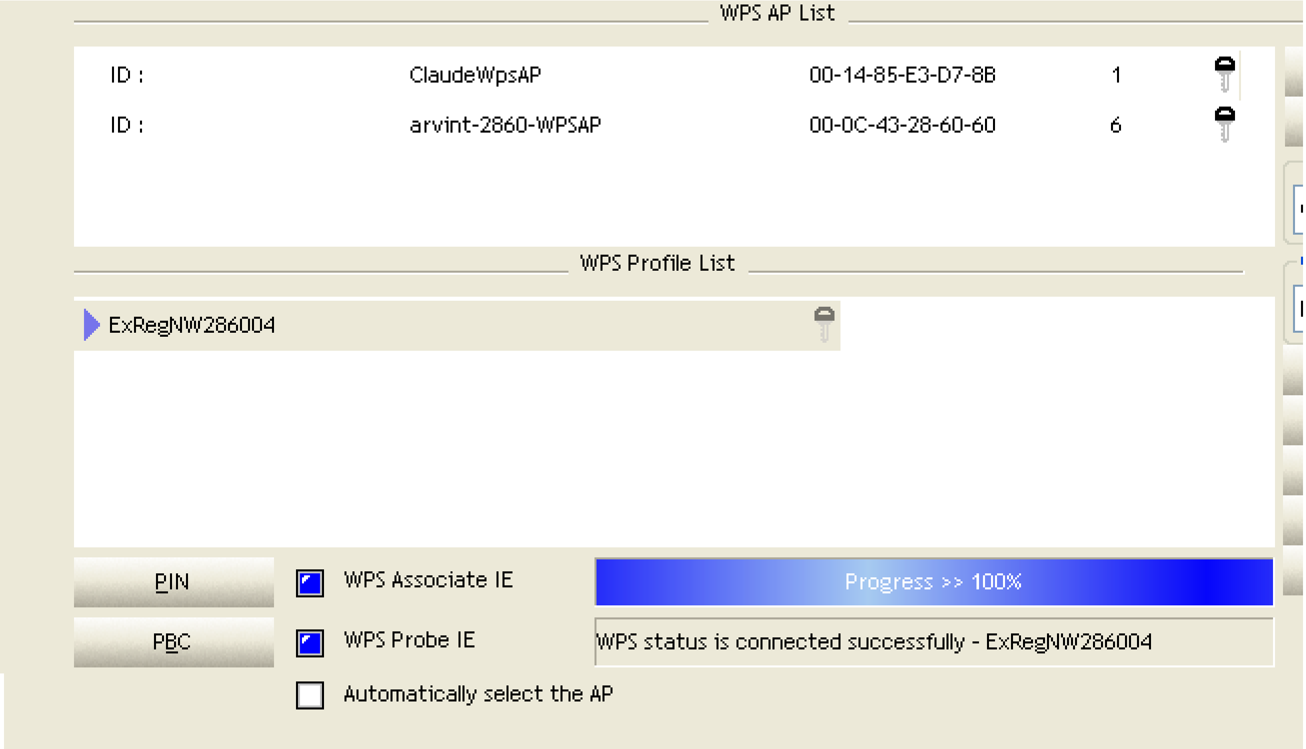
PIN   ☑ WPS Associate IE   Progress >> 0%

PBC   ☑ WPS Probe IE   WPS status is disconnected

□ Automatically select the AP

❹ 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),

❺ 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.



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

ExRegNW286004

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - ExRegNW286004

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

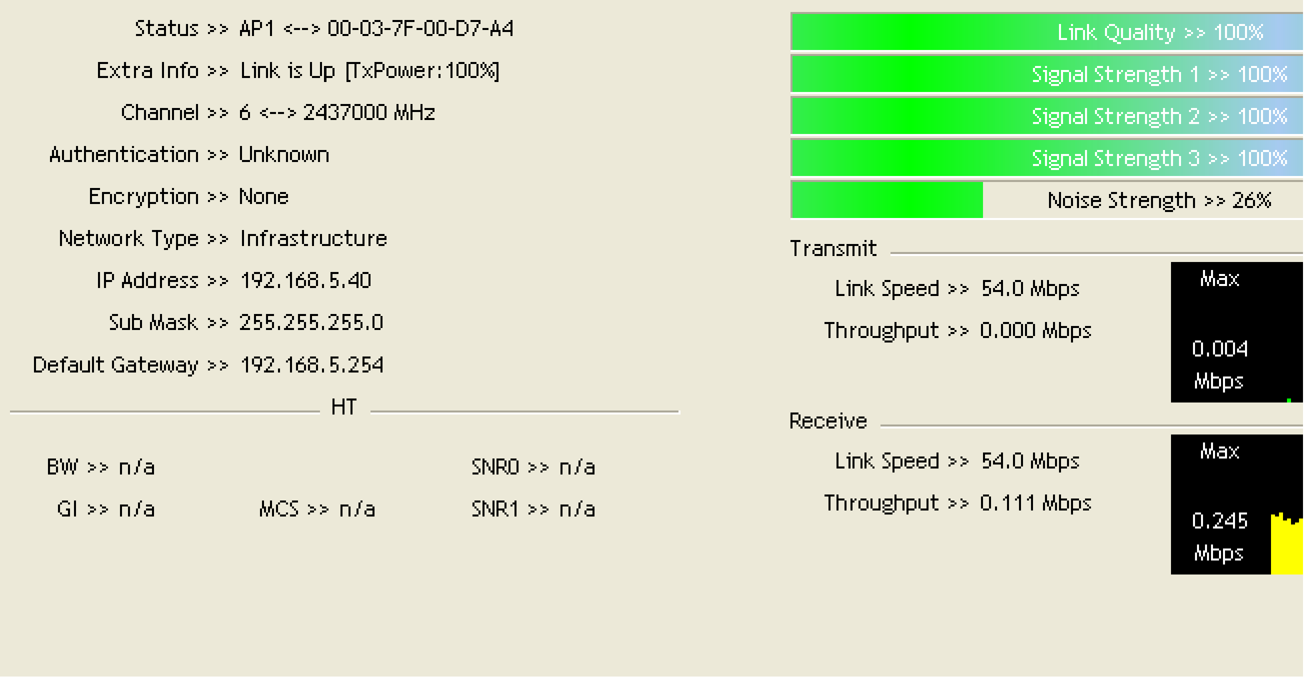
Describe "WPS Status Bar" -   "PBC - xxx" as follow :

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.



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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 192.168.5.40

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 100%

Signal Strength 2 >> 100%

Signal Strength 3 >> 100%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Max

0.004 Mbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.111 Mbps

Max

0.245 Mbps

Figure 2-9 Link Status function

① Status : Current connection status. If no connection, if 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 Throughout : Display transmits and receive throughput in unit of Mbps.

⑫ Link Quality : Display connection quality based on signal strength and TX/RX packet error rate.

⑬ Signal Strength 1 : 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.

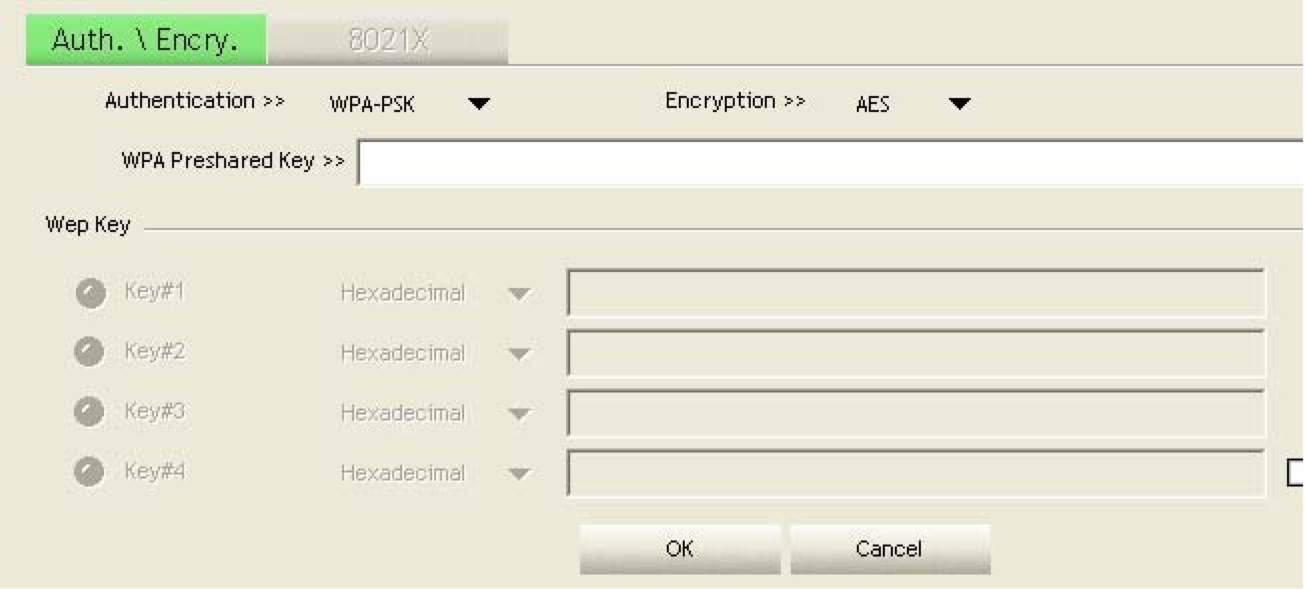
⑮ Signal Strength 3 : Receive signal strength 3, user can choose to display as percentage or dBm format.

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.


Authentication >> WPA-PSK

Encryption >> AES

WPA Preshared Key >>

Wep Key

Key#1 Hexadecimal

Key#2 Hexadecimal

Key#3 Hexadecimal

Key#4 Hexadecimal

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.

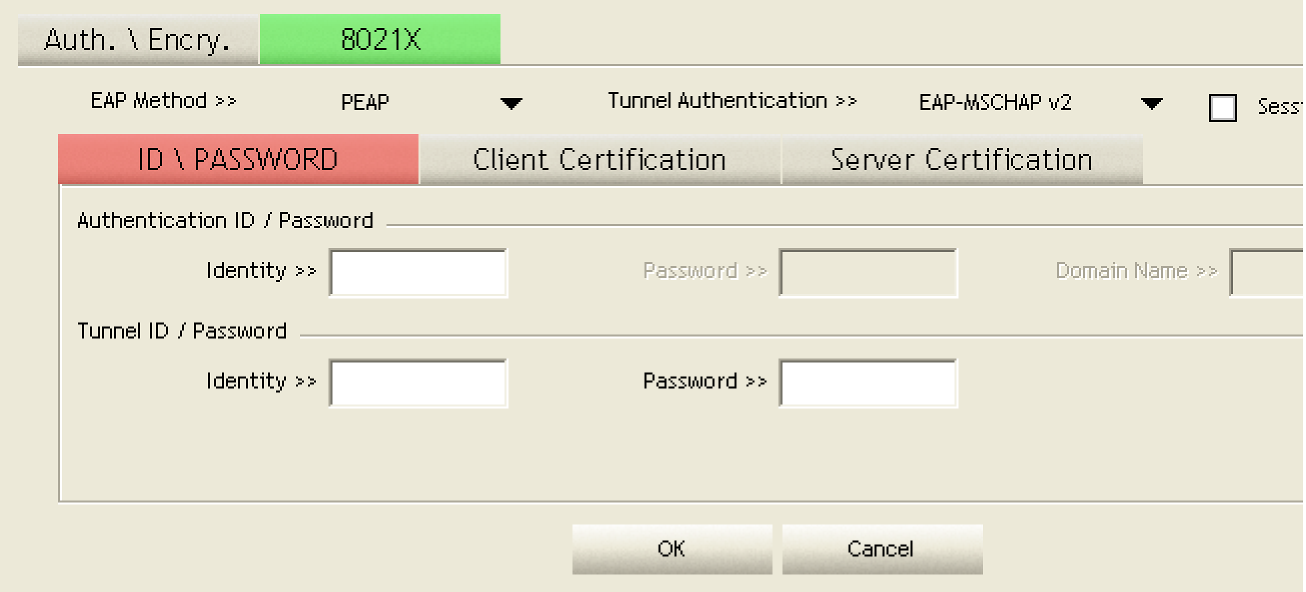
⑤ WEP Key : Only valid when using WEP encryption algorithm. The key must matched AP's key. There are several formats to enter the keys.

❶ Hexadecimal - 40bits : 10 Hex characters.
❷ Hexadecimal - 128bits : 32Hex characters.
❸ ASCII - 40bits : 5 ASCII characters.
❹ ASCII - 128bits : 13 ASCII characters.

****Powered by Meetinghouse.**

802.1x Setting

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



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Sess

Authentication ID / Password

Identity >>

Password >>

Domain Name >>

Tunnel ID / Password

Identity >>

Password >>

Authentication type :

❶ 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.

❷ TLS/Smart Card : Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

❸ TTLS : Tunneled Transport Layer Security. This security method provides for certificate- based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

❹ EAP-FAST : Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be 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.

❺ 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.

❻ MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is
no mutual authentication of wireless client and the network.

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

Authentication :

❶ 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".

❷ Tunnel Identity : Identity for tunnel.

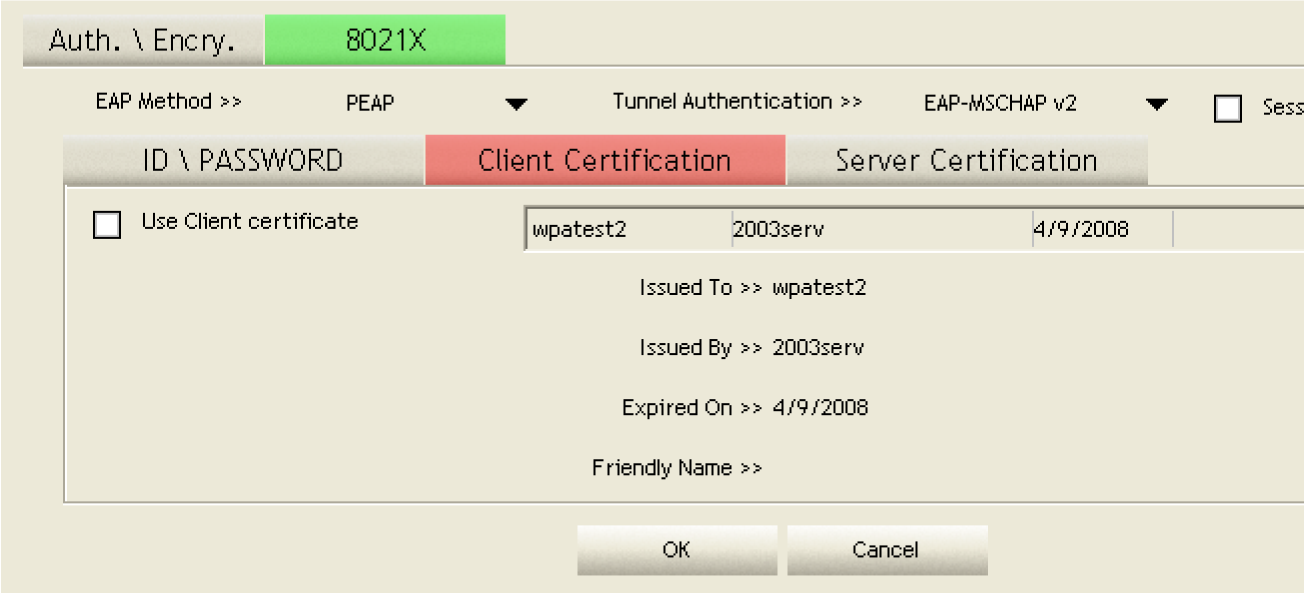
❸ Tunnel Password : Password for tunnel.

- ID \ PASSWORD -

❶ 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.

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

- Client Certification -



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Sess

□ Use Client certificate

wpatest2	2003serv	4/9/2008

Issued To >> wpatest2

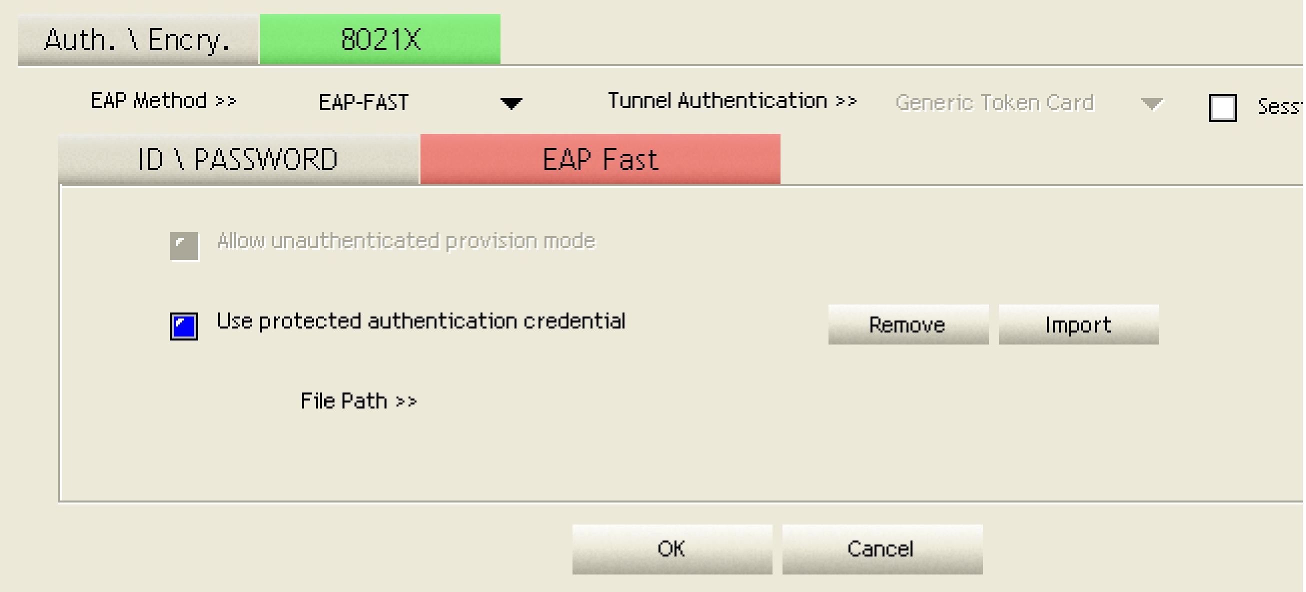
Issued By >> 2003serv

Expired On >> 4/9/2008

Friendly Name >>

❶ Use Client certificate : Client certificate for server authentication.

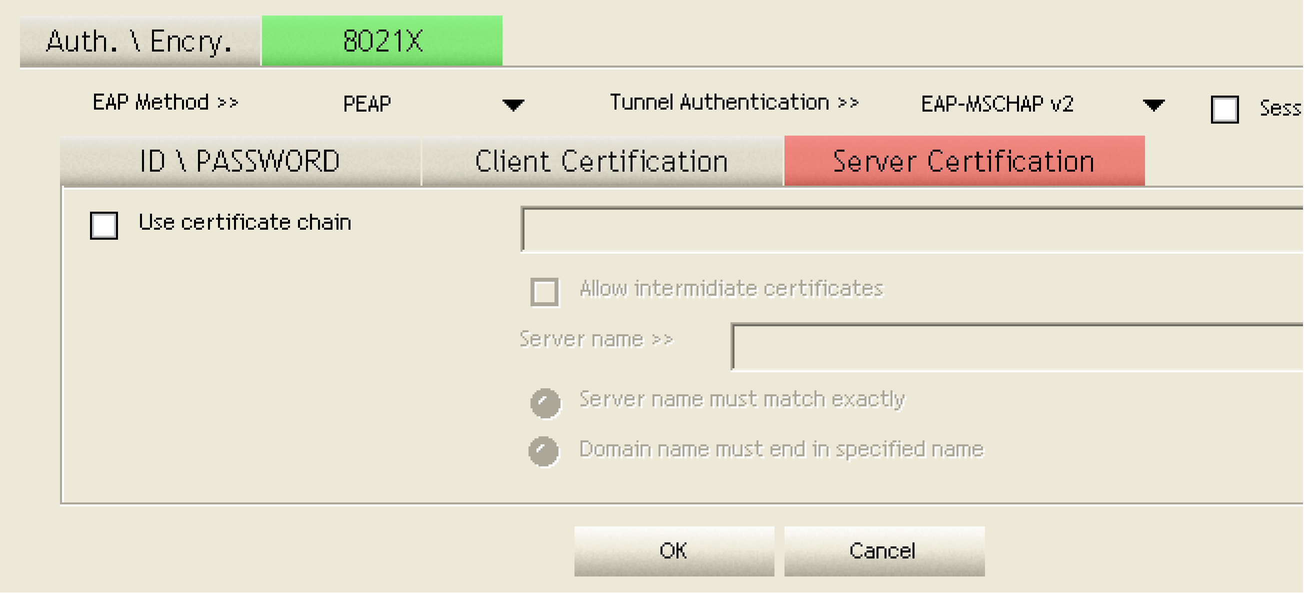
- EAP Fast -



❶ 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.

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

- Server Certification -



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

❷ 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.

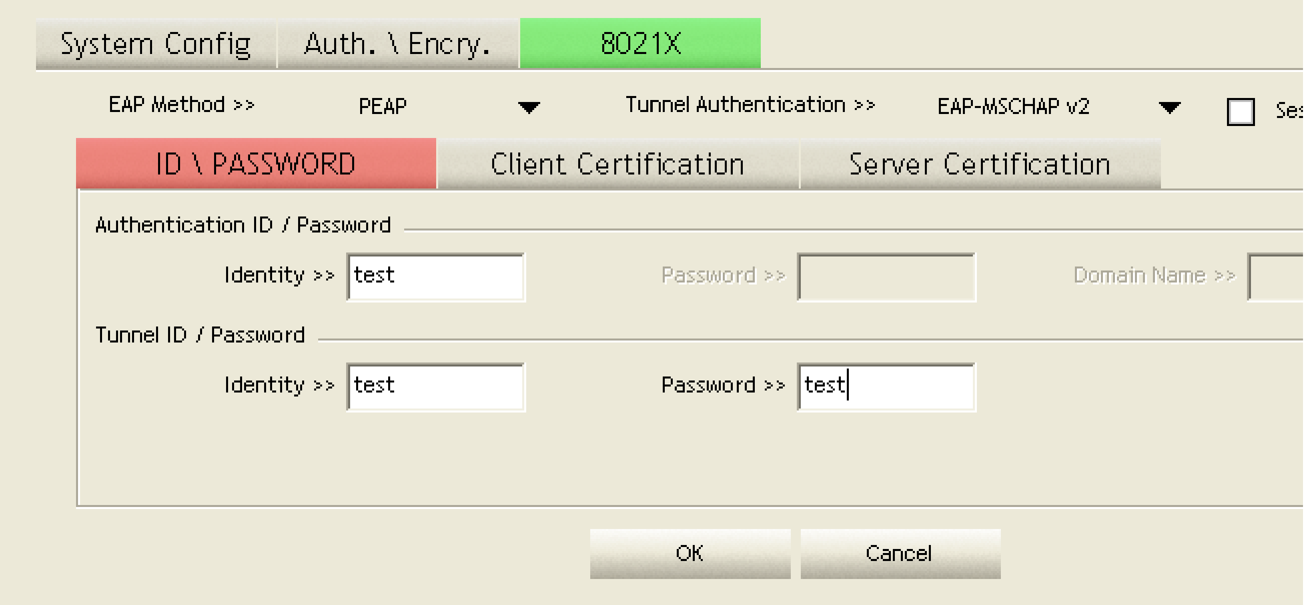
❸ Server name : Enter an authentication sever root.

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 :

❶ 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.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Ses

Authentication ID / Password

Identity >> test

Password >>

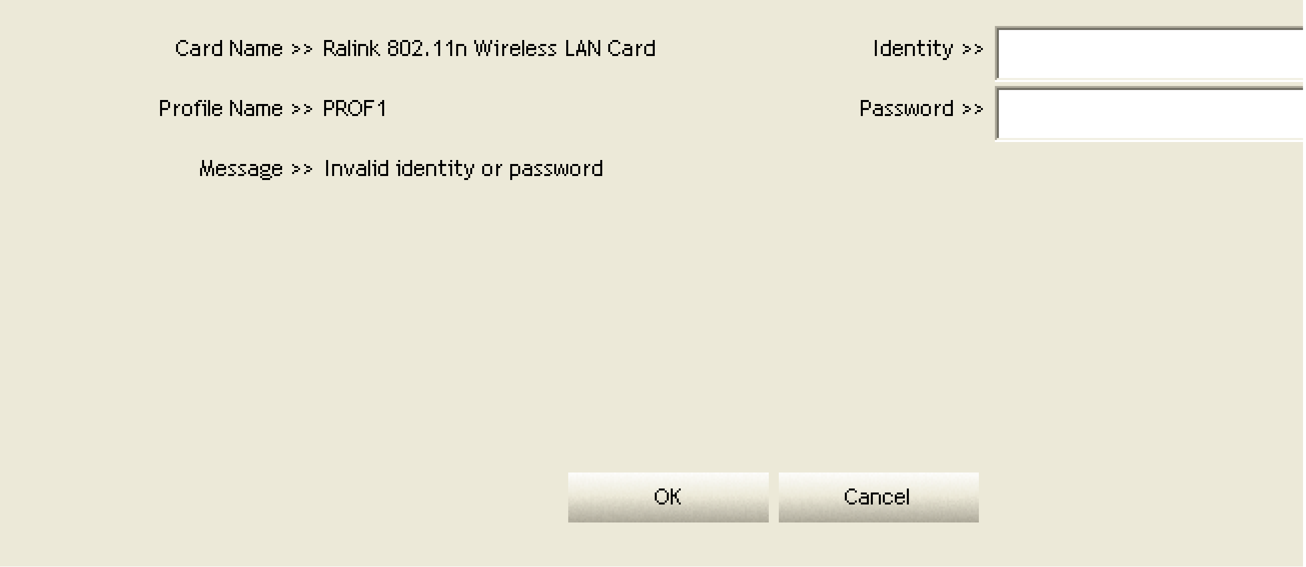
Domain Name >>

Tunnel ID / Password

Identity >> test

Password >> test

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



Card Name >> Ralink 802.11n Wireless LAN Card

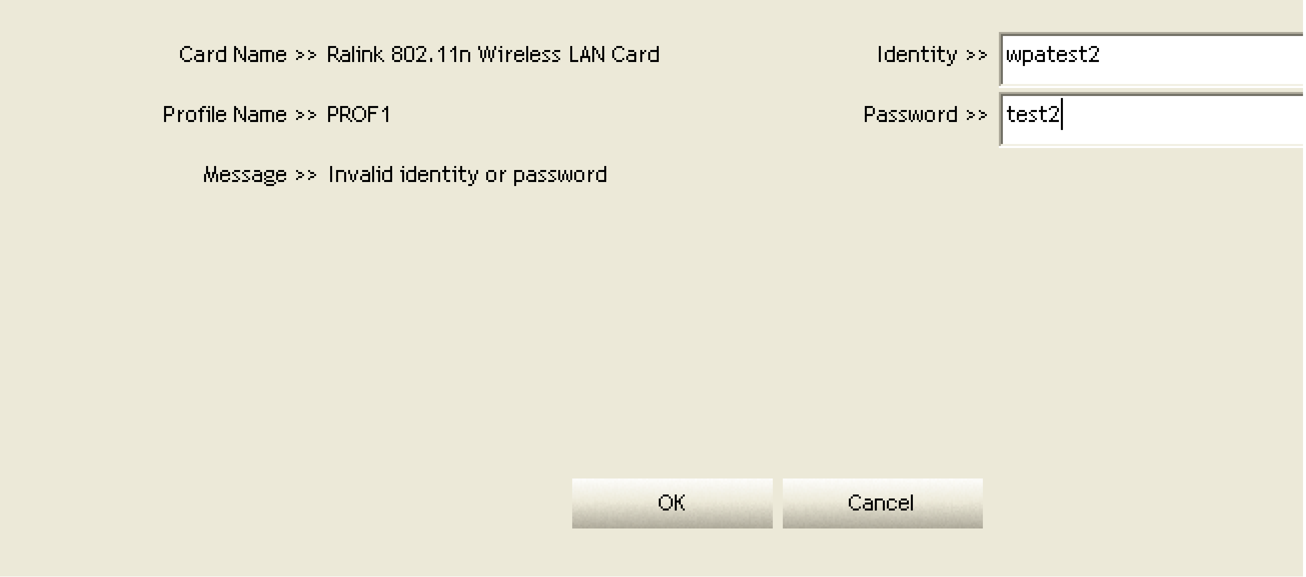
Identity >>

Profile Name >> PROF1

Password >>

Message >> Invalid identity or password

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


Card Name >> Ralink 802.11n Wireless LAN Card

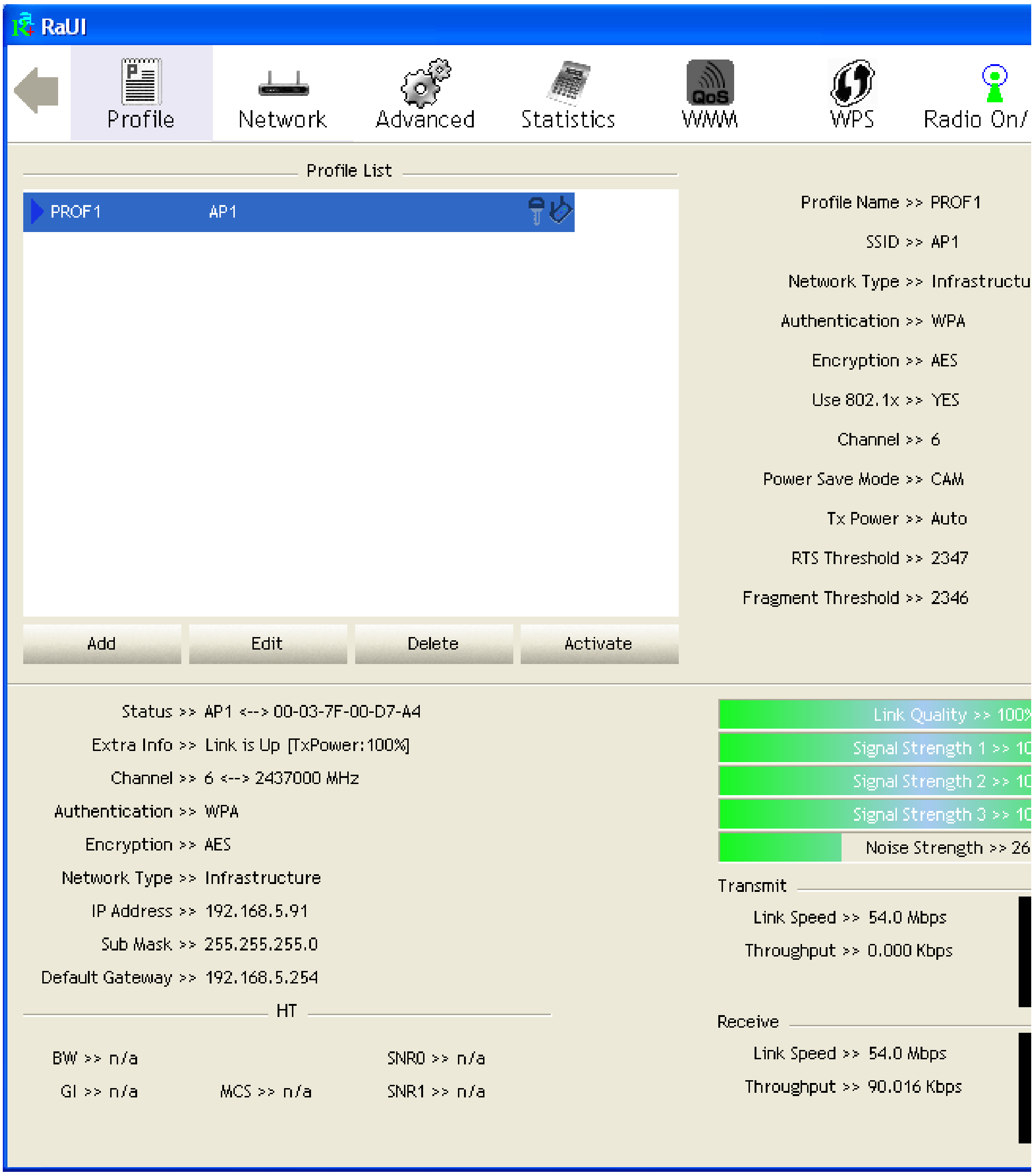
Profile Name >> PROF1

Message >> Invalid identity or password

Identity >> wpatest2

Password >> test2

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



PROF1 AP1

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

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

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

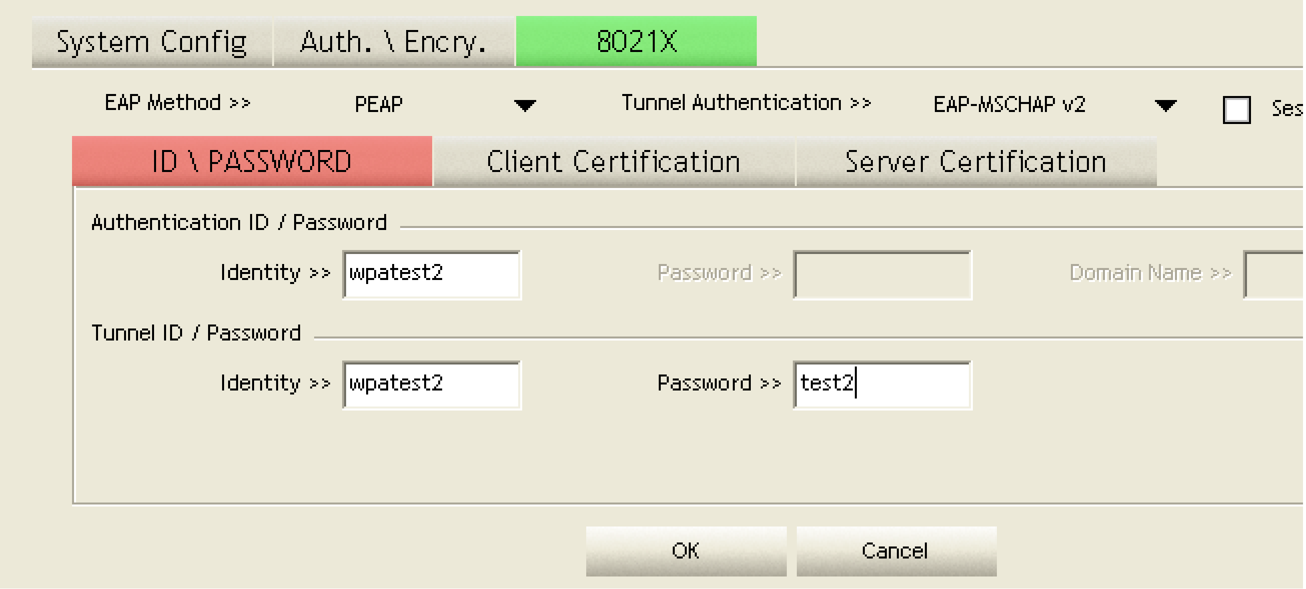
Link Quality >> 100%
Signal Strength 1 >> 10
Signal Strength 2 >> 10
Signal Strength 3 >> 10
Noise Strength >> 26

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

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

When occurring "Timeout" :

❶ 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.



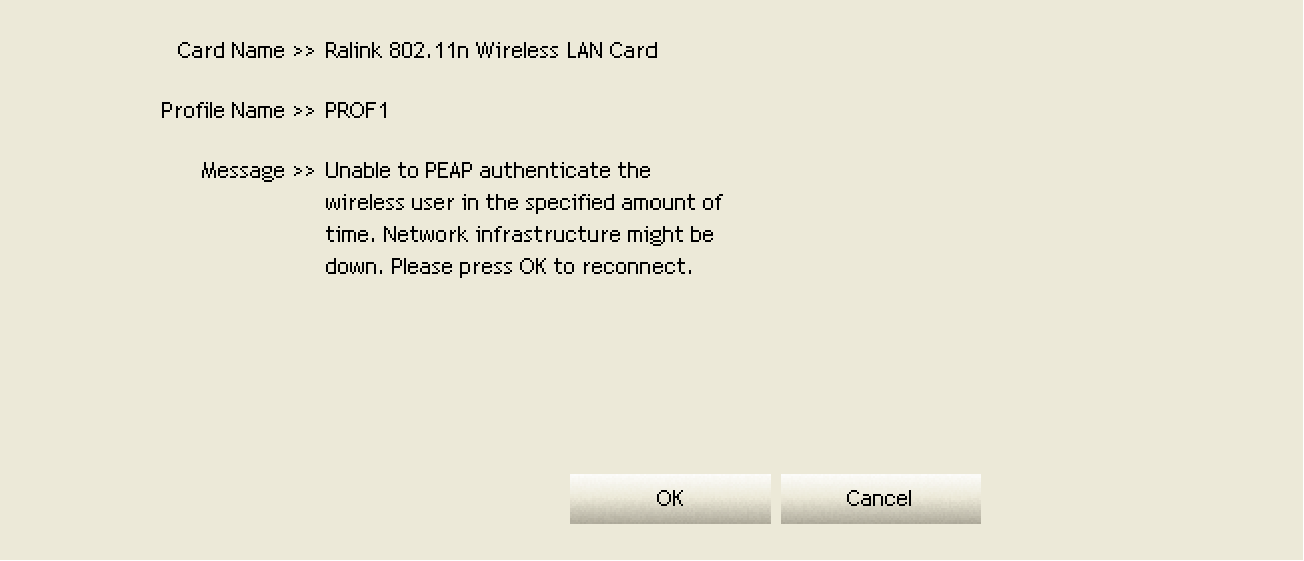
EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2 □ Ses

Authentication ID / Password: Identity >> wpatest2 Password >>

Tunnel ID / Password: Identity >> wpatest2 Password >> test2

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

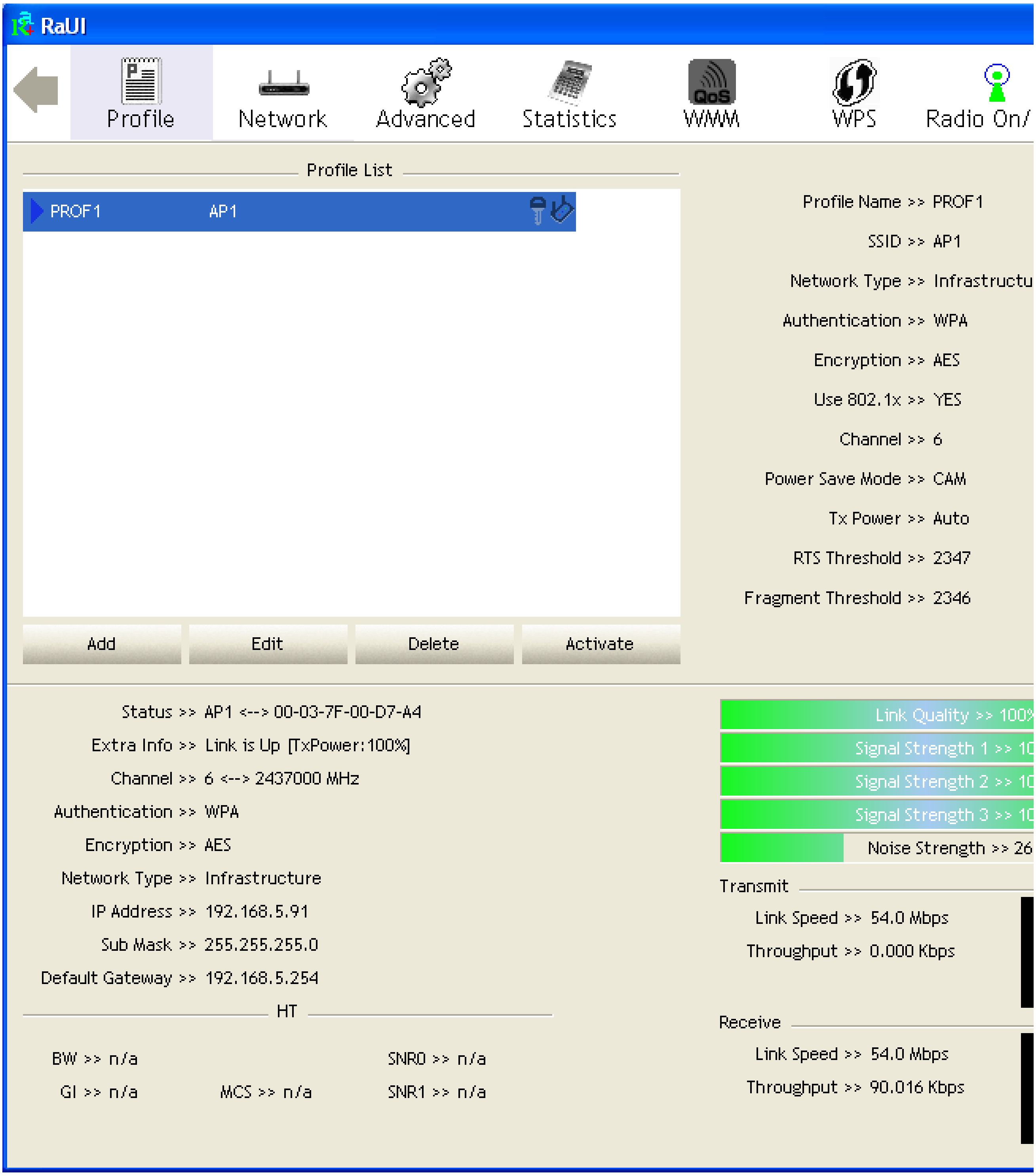


Card Name >> Ralink 802.11n Wireless LAN Card

Profile Name >> PROF1

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

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



Profile List

PROF1 AP1

Profile Name >> PROF1

SSID >> AP1

Network Type >> Infrastructu

Authentication >> WPA

Encryption >> AES

Use 802.1x >> YES

Channel >> 6

Power Save Mode >> CAM

Tx Power >> Auto

RTS Threshold >> 2347

Fragment Threshold >> 2346

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.5.91

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

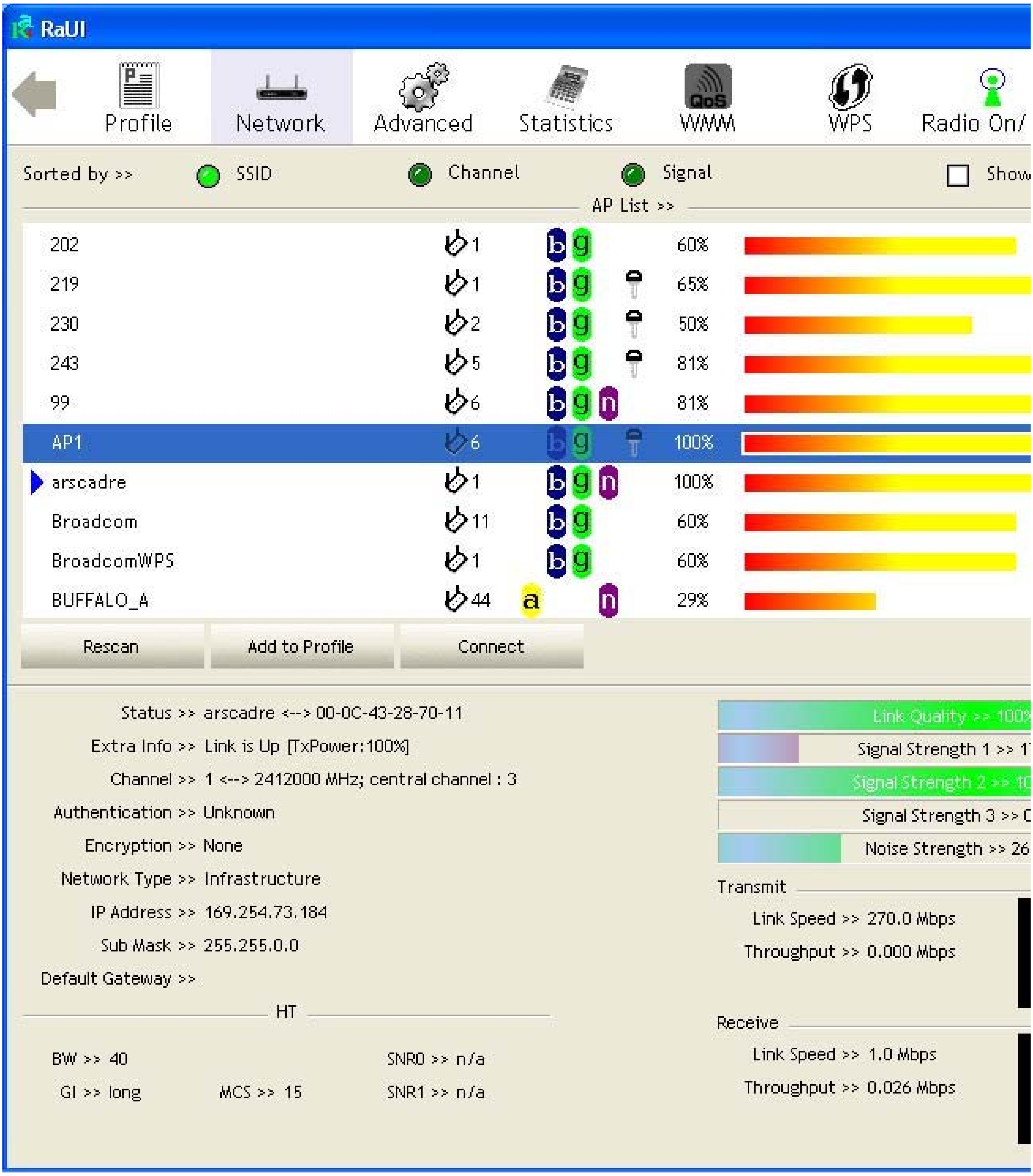
Receive

Link Speed >> 54.0 Mbps

Throughput >> 90.016 Kbps

Example to Configure Connection with WEP on

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



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

Status >> arscadre <--> 00-0C-43-28-70-11

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

Channel >> 1 <--> 2412000 MHz; central channel : 3

Authentication >> Unknown

Encryption >> None

Network Type >> Infrastructure

IP Address >> 169.254.73.184

Sub Mask >> 255.255.0.0

Default Gateway >>

HT

BW >> 40

GI >> long MCS >> 15

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 1

Signal Strength 2 >> 10

Signal Strength 3 >> 0

Noise Strength >> 26

Transmit

Link Speed >> 270.0 Mbps

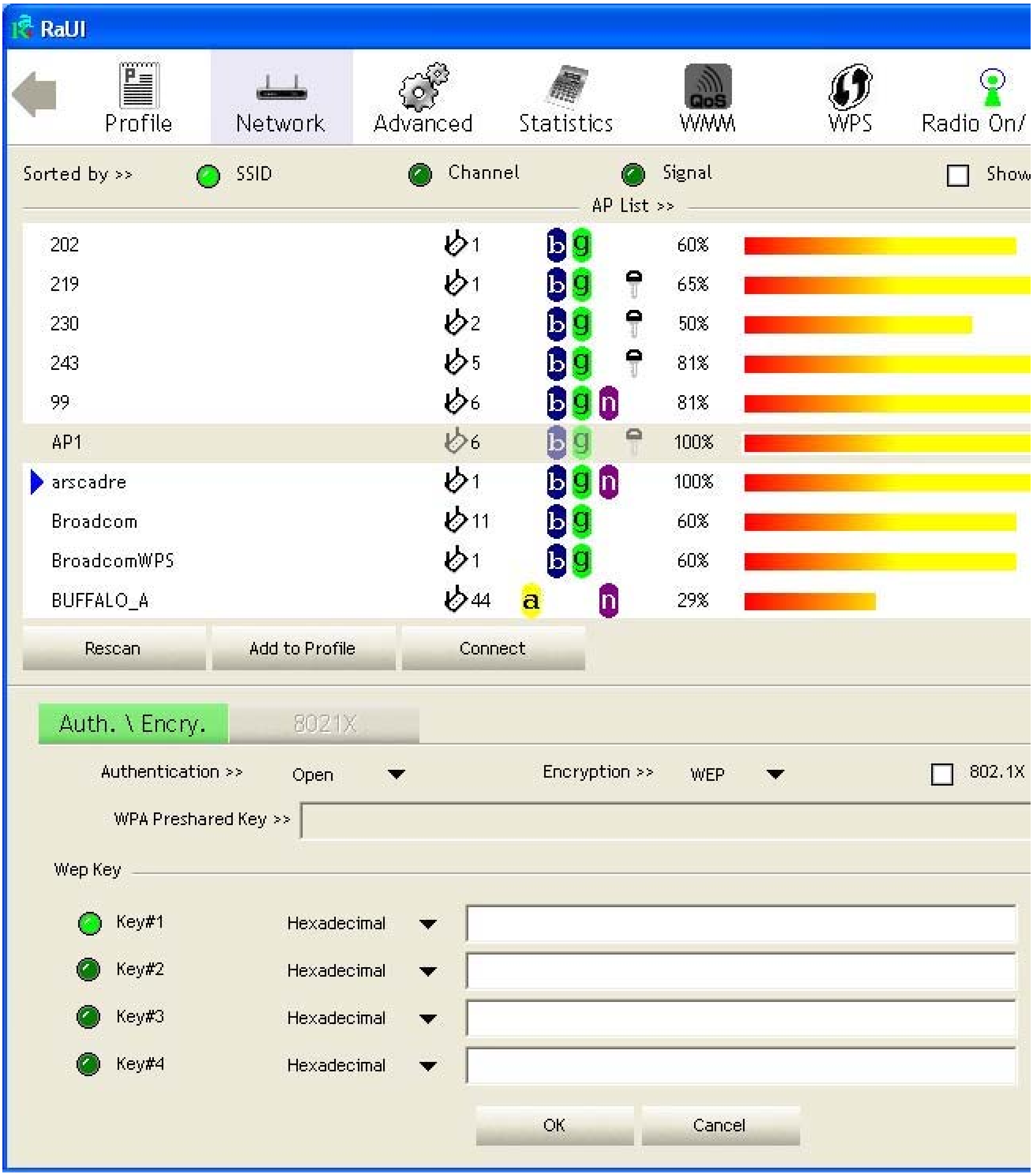
Throughput >> 0.000 Mbps

Receive

Link Speed >> 1.0 Mbps

Throughput >> 0.026 Mbps

❷ Auth. \ Encry. function pop up.



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

AP List >>

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

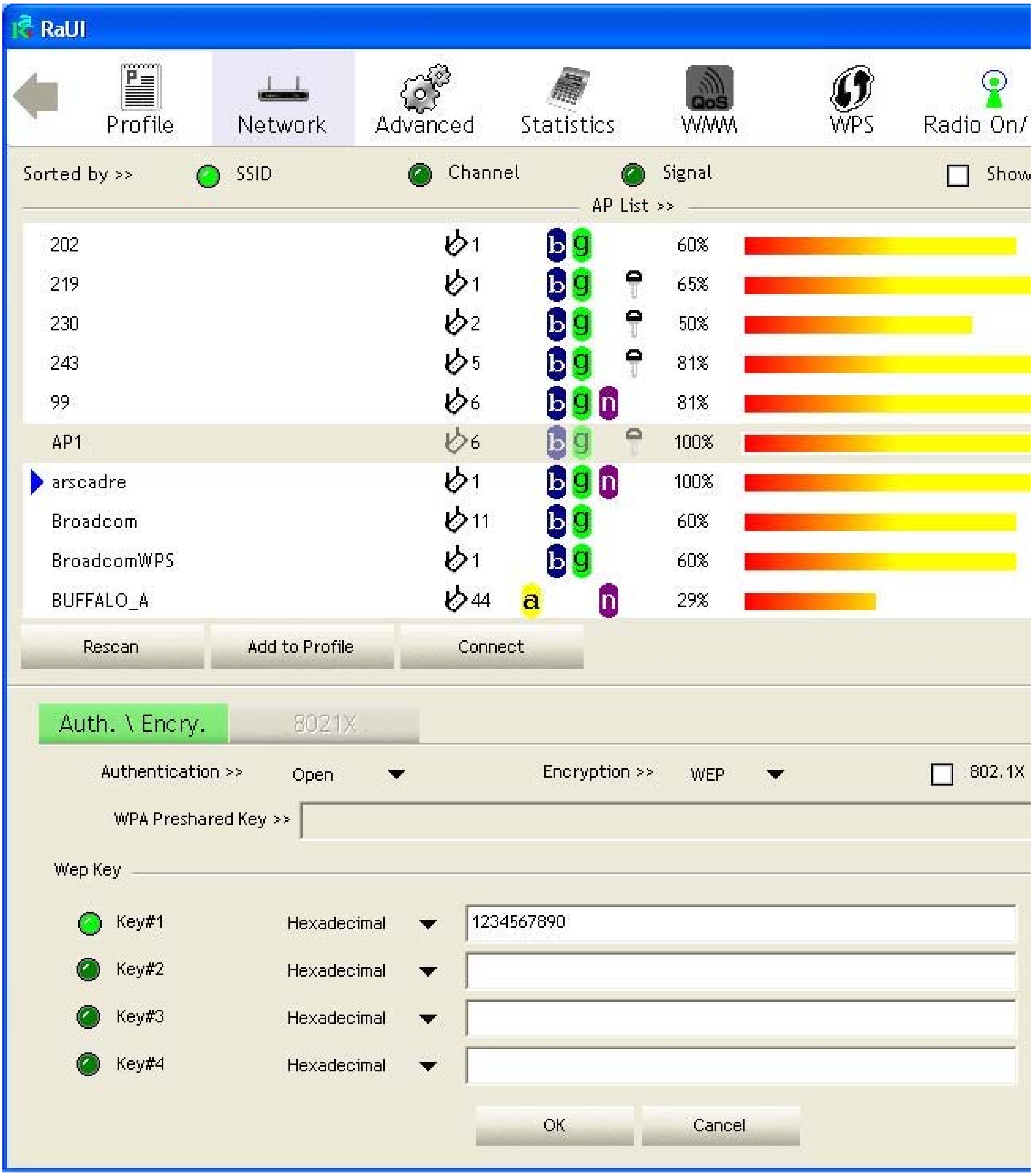
Authentication >> Open Encryption >> WEP □ 802.1X

WPA Preshared Key >>

Wep Key

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

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



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

Authentication >> Open

Encryption >> WEP

☐ 802.1X

WPA Preshared Key >>

Wep Key

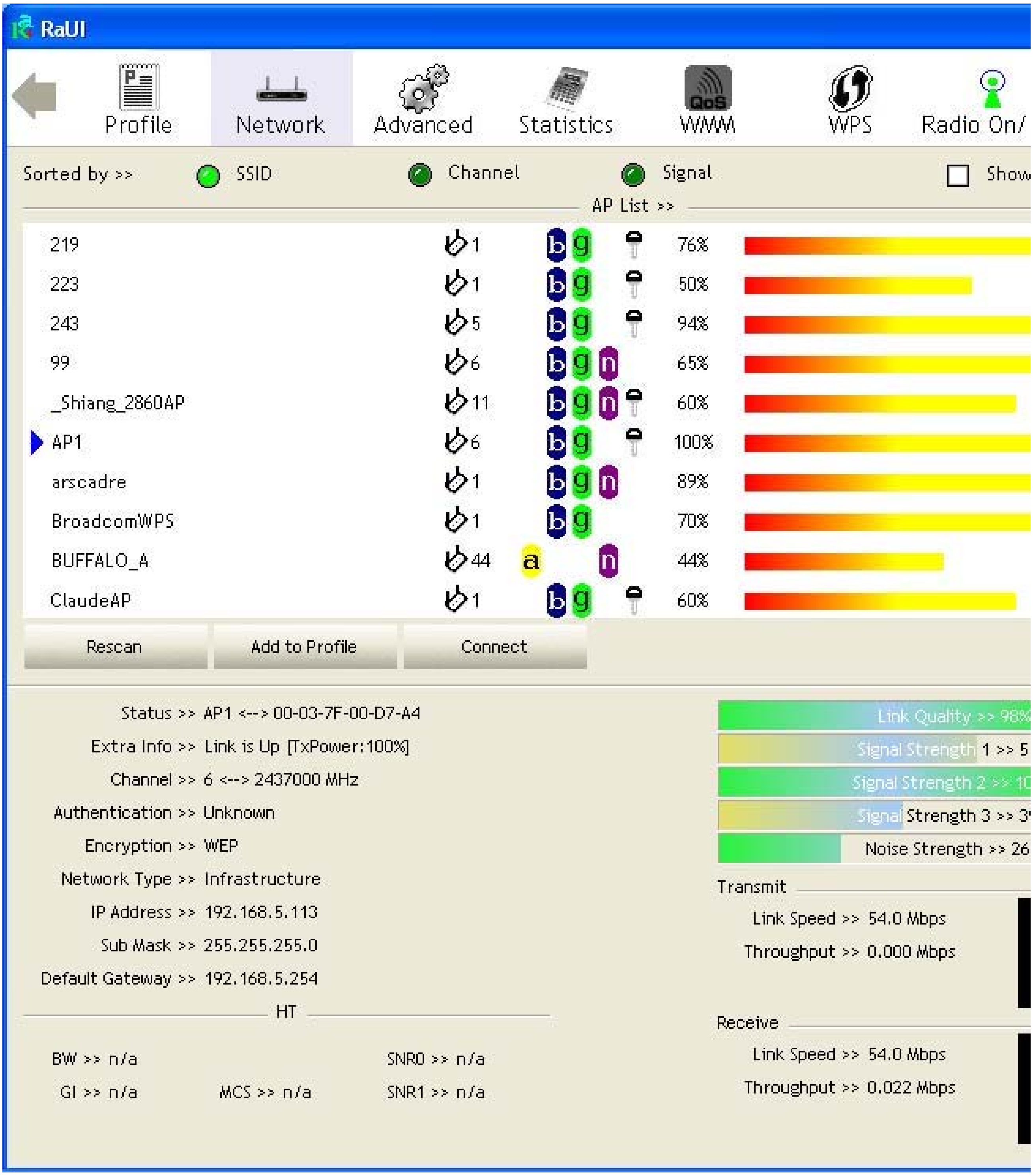
● Key#1 Hexadecimal 1234567890

○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

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



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

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

HT

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

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

Transmit

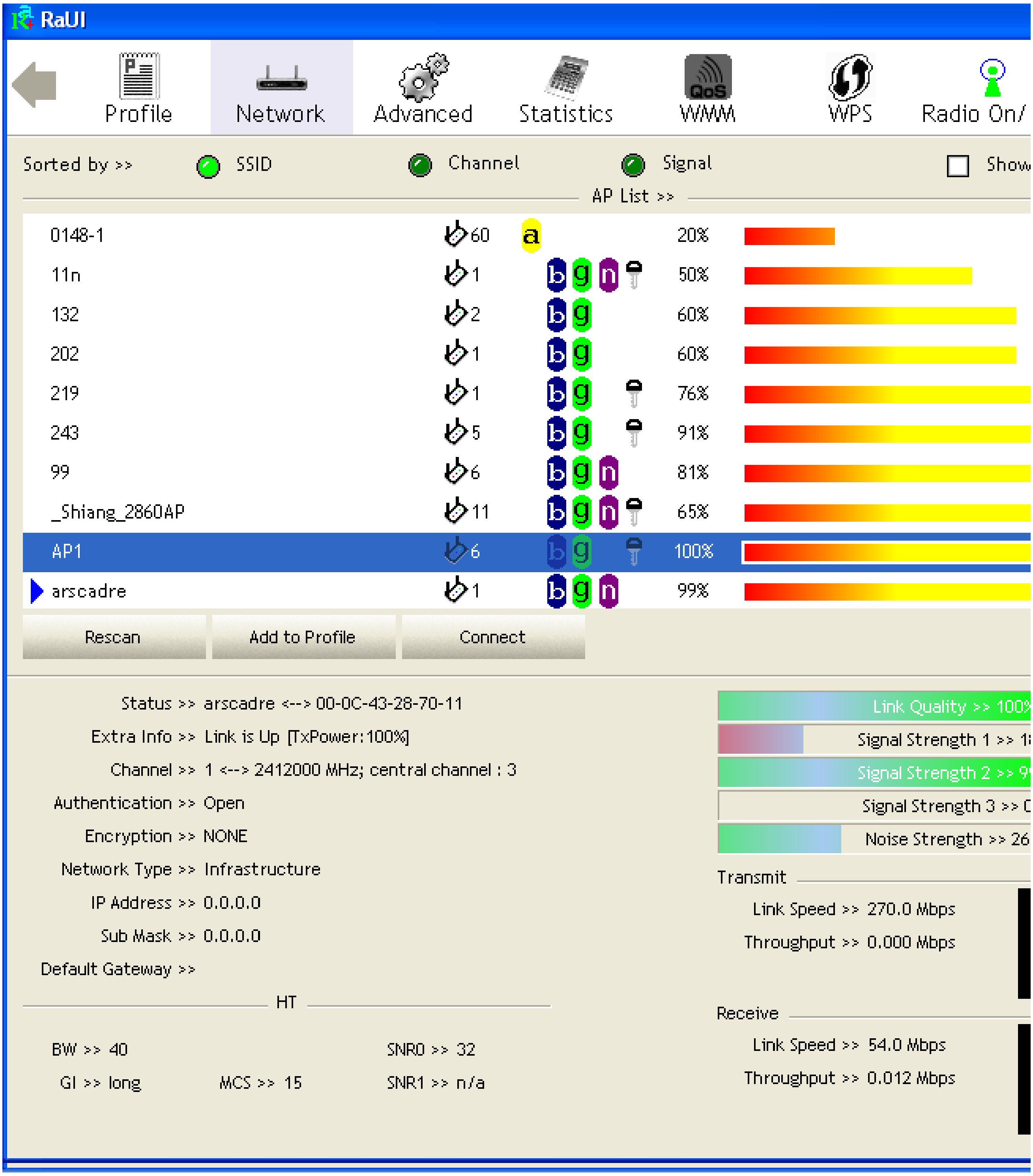
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

Receive

Link Speed >> 54.0 Mbps
Throughput >> 0.022 Mbps

Example to Configure Connection with WPA-PSK

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



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

AP List >>

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

Status >> arscadre <--> 00-0C-43-28-70-11

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

Channel >> 1 <--> 2412000 MHz; central channel : 3

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 0.0.0.0

Sub Mask >> 0.0.0.0

Default Gateway >>

HT

BW >> 40

GI >> long MCS >> 15

SNR0 >> 32

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 1

Signal Strength 2 >> 9

Signal Strength 3 >> 0

Noise Strength >> 26

Transmit

Link Speed >> 270.0 Mbps

Throughput >> 0.000 Mbps

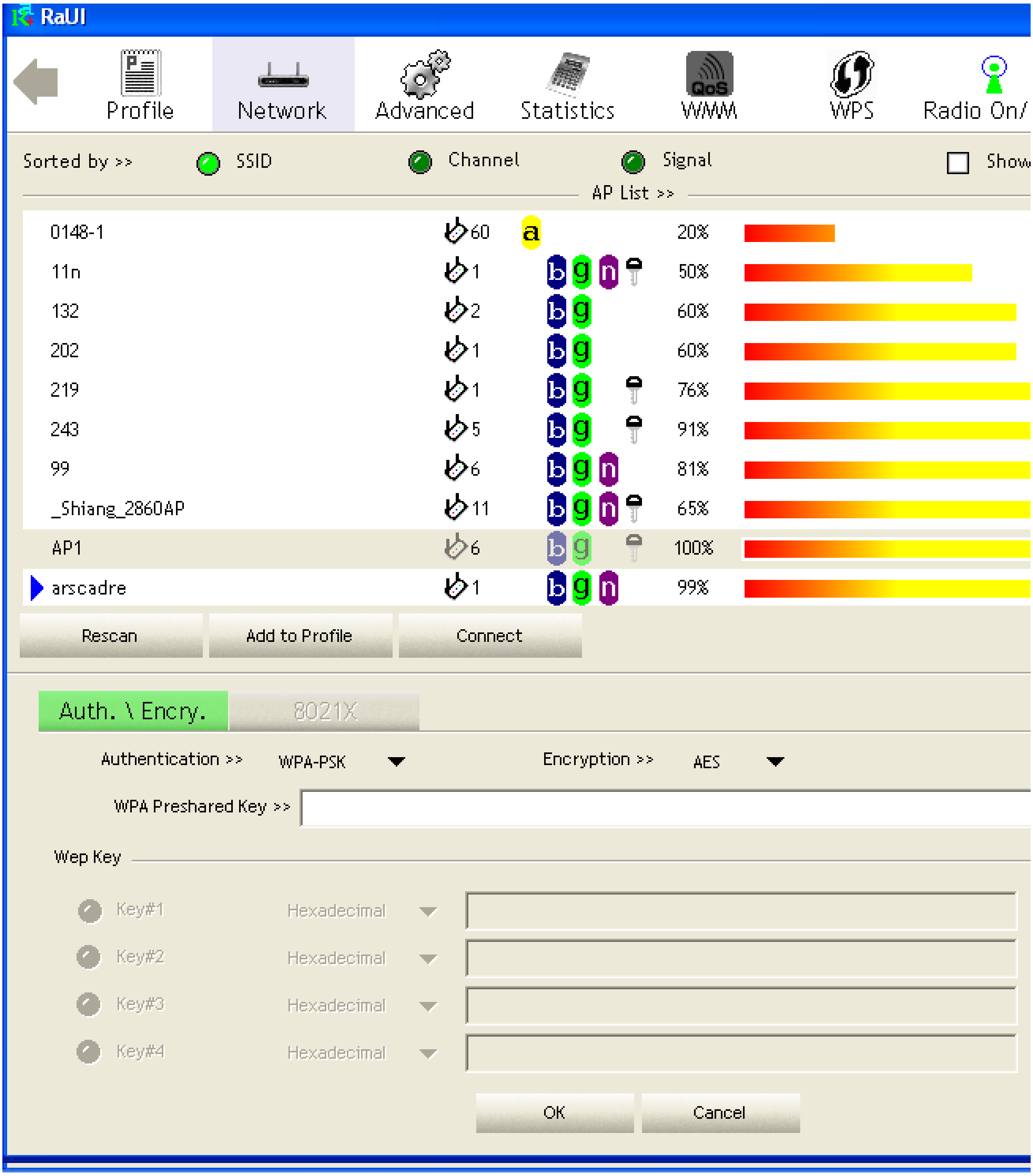
Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.012 Mbps

② Auth. \ Encry. function pop up.

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



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

AP List >>

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

Authentication >> WPA-PSK ▼ Encryption >> AES ▼

WPA Preshared Key >>

Wep Key

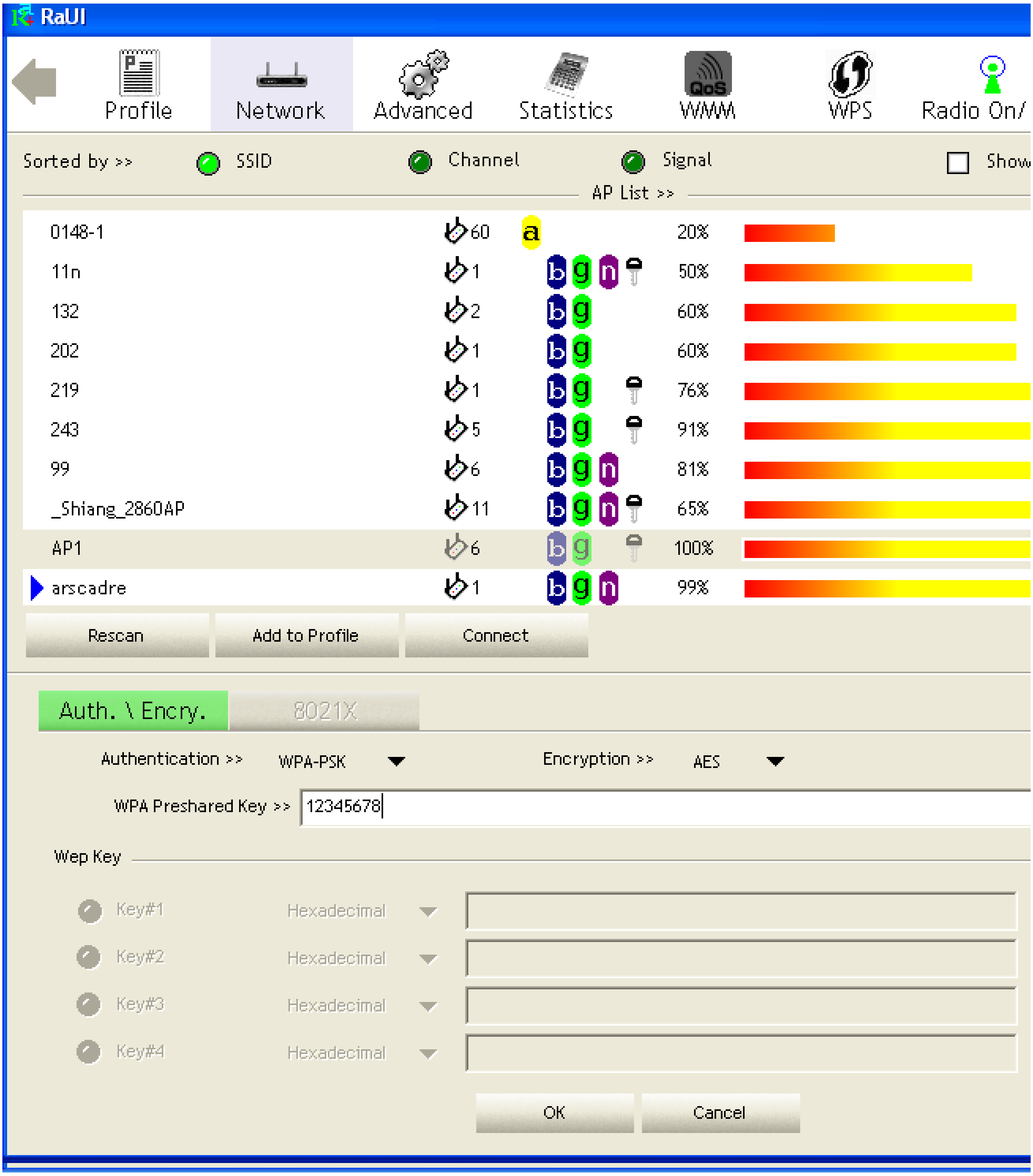
○ Key#1 Hexadecimal ▼

○ Key#2 Hexadecimal ▼

○ Key#3 Hexadecimal ▼

○ Key#4 Hexadecimal ▼

③ Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Key secret as 12345678.



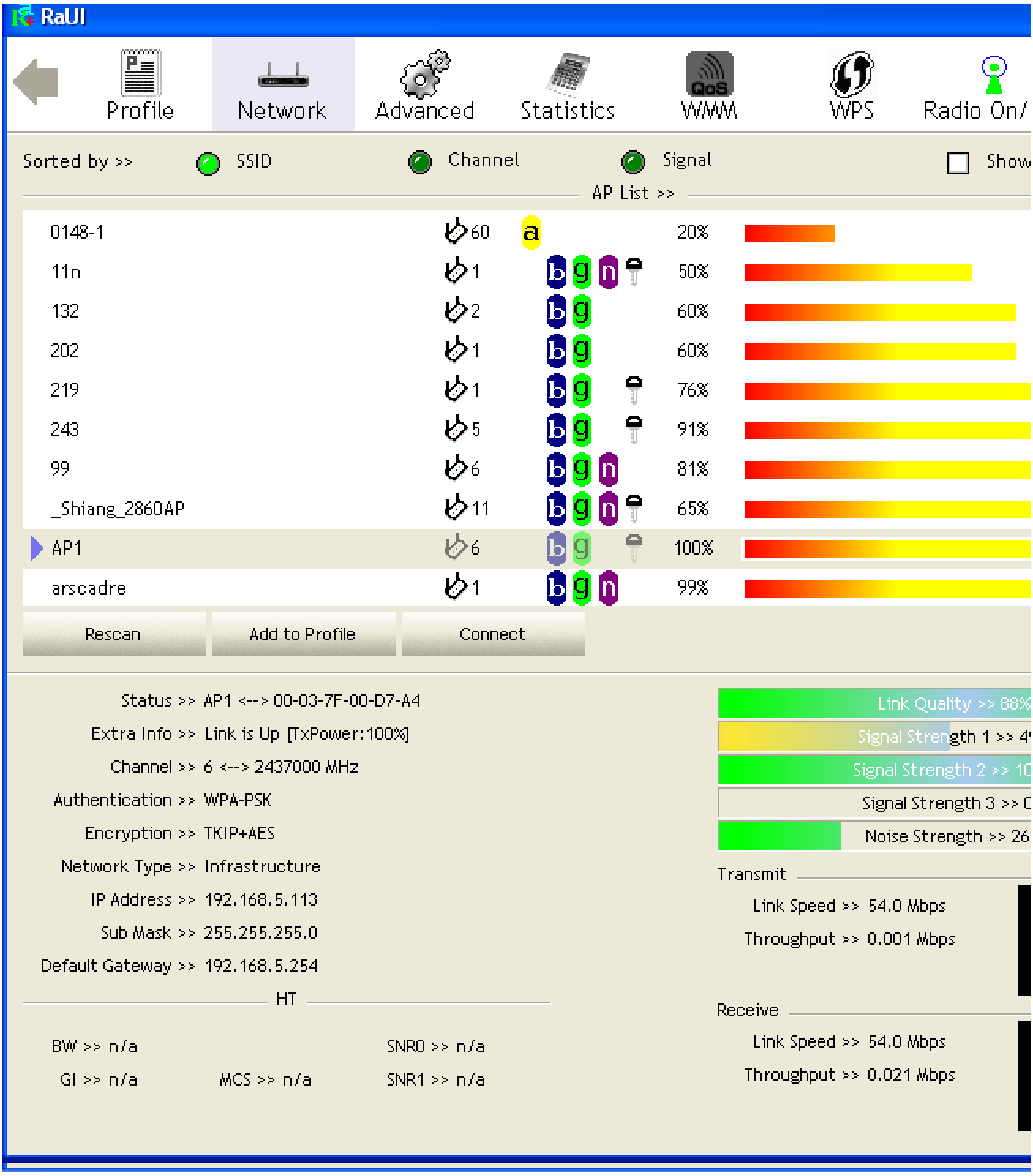
0148-1	60	a		20%
11n	1	b g n	🔒	50%
132	2	b g		60%
202	1	b g		60%
219	1	b g	🔒	76%
243	5	b g	🔒	91%
99	6	b g n		81%
_Shiang_2860AP	11	b g n	🔒	65%
AP1	6	b g	🔒	100%
▶ arscadre	1	b g n		99%

Authentication >> WPA-PSK

Encryption >> AES

WPA Preshared Key >> 12345678

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.



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

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA-PSK

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.5.113

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 88%

Signal Strength 1 >> 4

Signal Strength 2 >> 10

Signal Strength 3 >> 0

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.001 Mbps

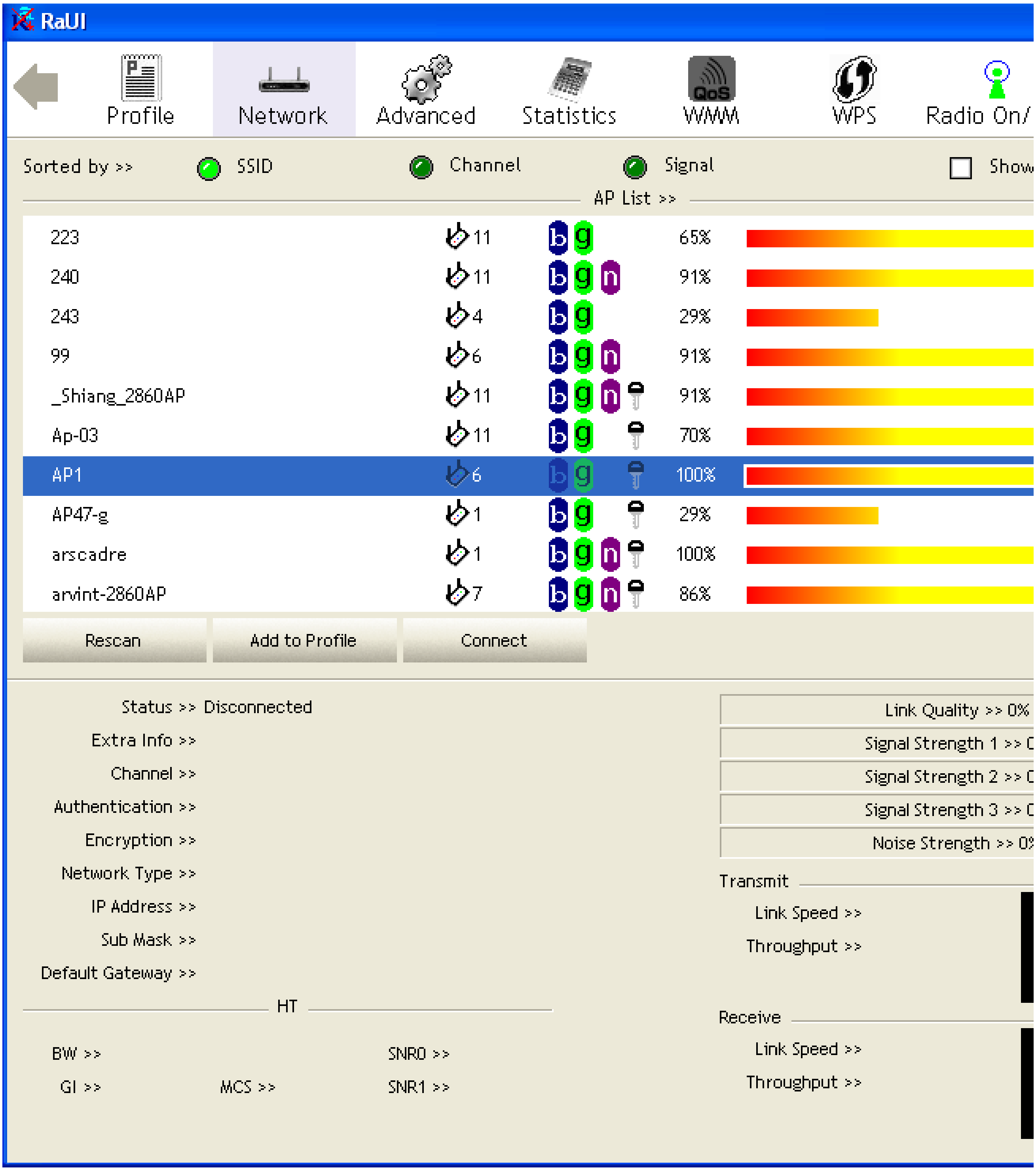
Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.021 Mbps

Example to Configure Connection with WPA

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



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

AP List >>

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

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >> SNR0 >>

GI >> MCS >> SNR1 >>

Link Quality >> 0%

Signal Strength 1 >> 0

Signal Strength 2 >> 0

Signal Strength 3 >> 0

Noise Strength >> 0%

Transmit

Link Speed >>

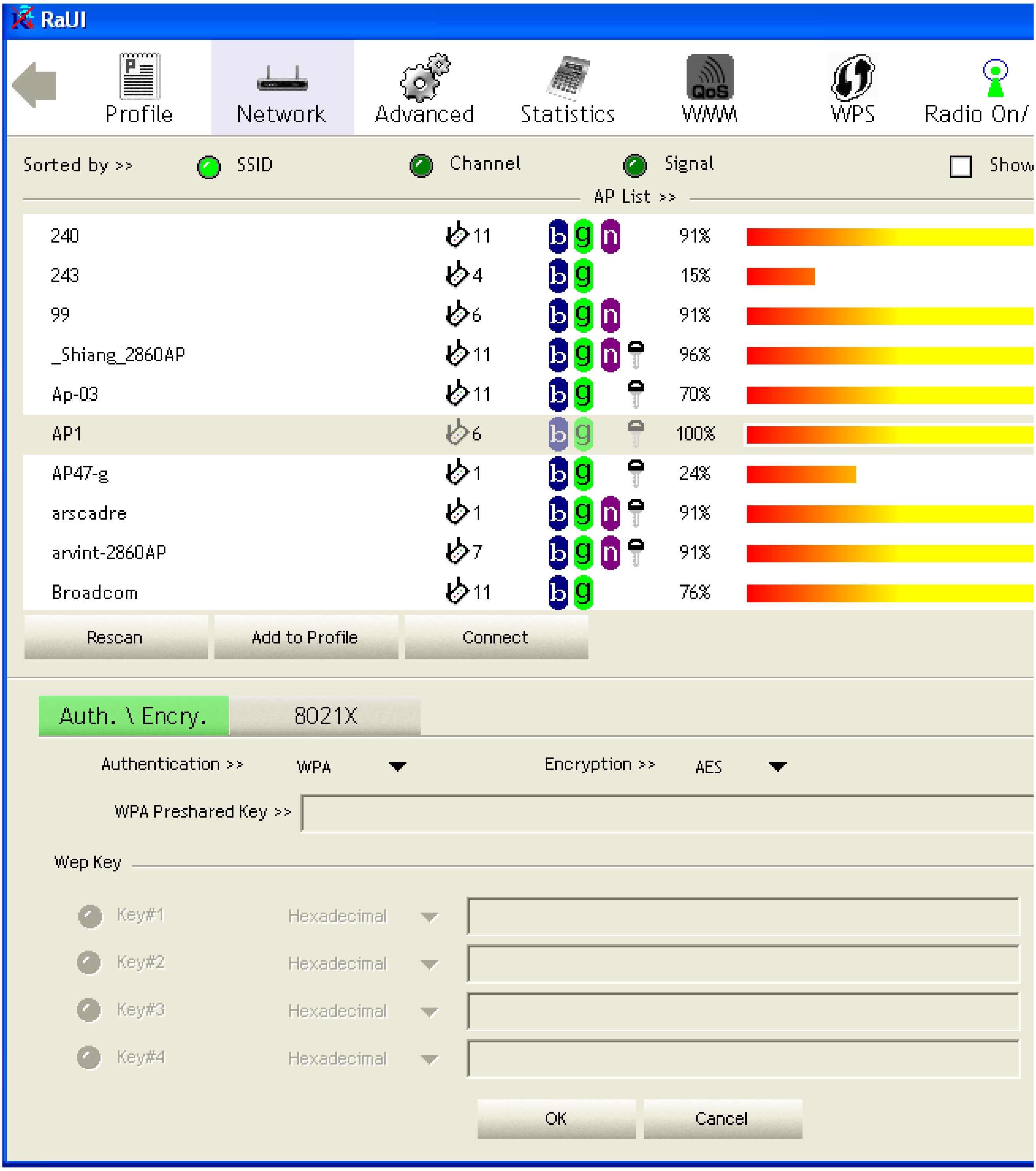
Throughput >>

Receive

Link Speed >>

Throughput >>

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



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

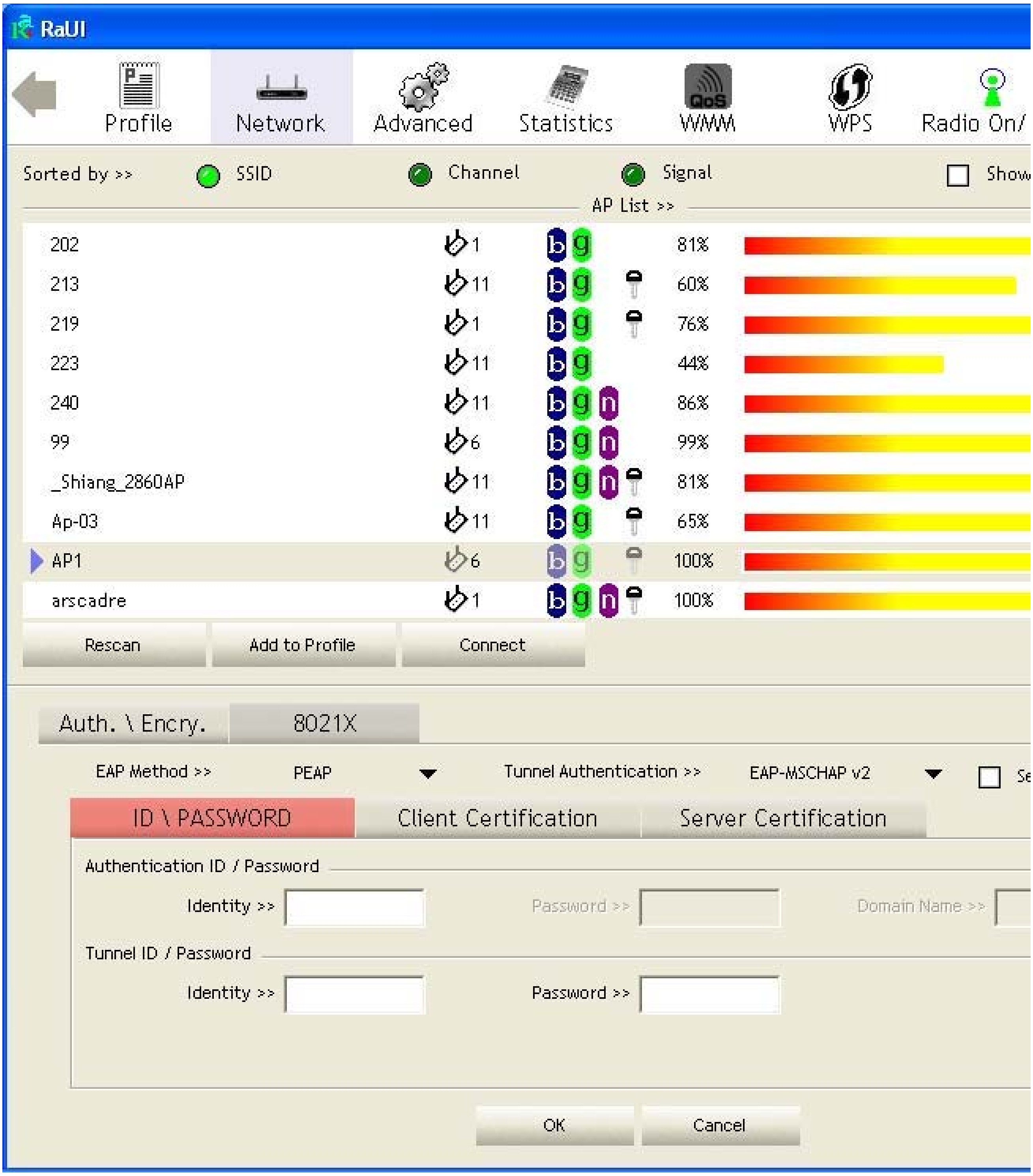
Authentication >> WPA

Encryption >> AES

WPA Preshared Key >>

Wep Key

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



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

AP List >>

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

Auth. \ Encry. | 8021X

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Se

ID \ PASSWORD | Client Certification | Server Certification

Authentication ID / Password

Identity >>

Password >>

Domain Name >>

Tunnel ID / Password

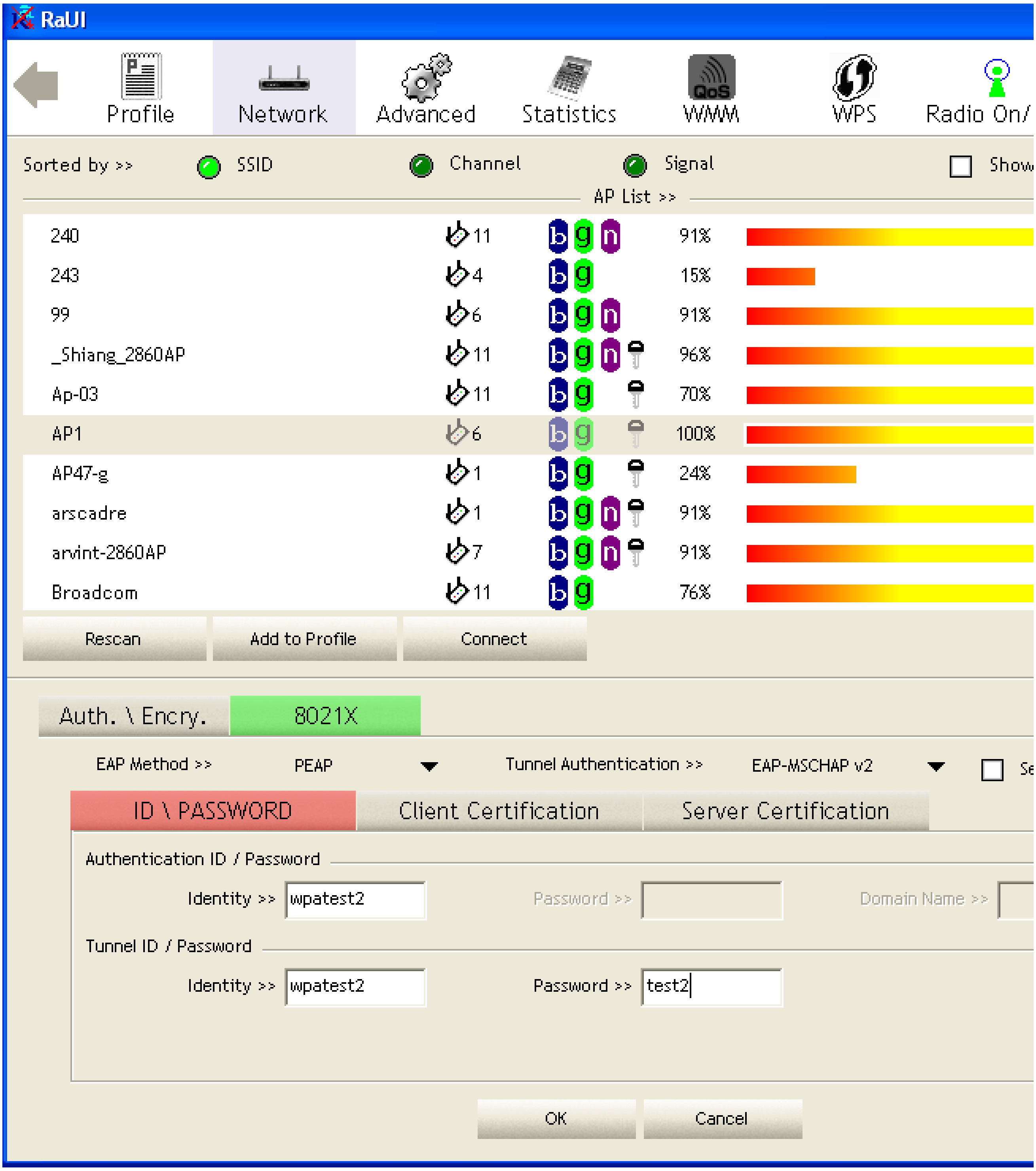
Identity >>

Password >>

④Authentication 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.



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

AP List >>

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

Auth. \ Encry. 8021X

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Se

Authentication ID / Password

Identity >> wpatest2

Password >>

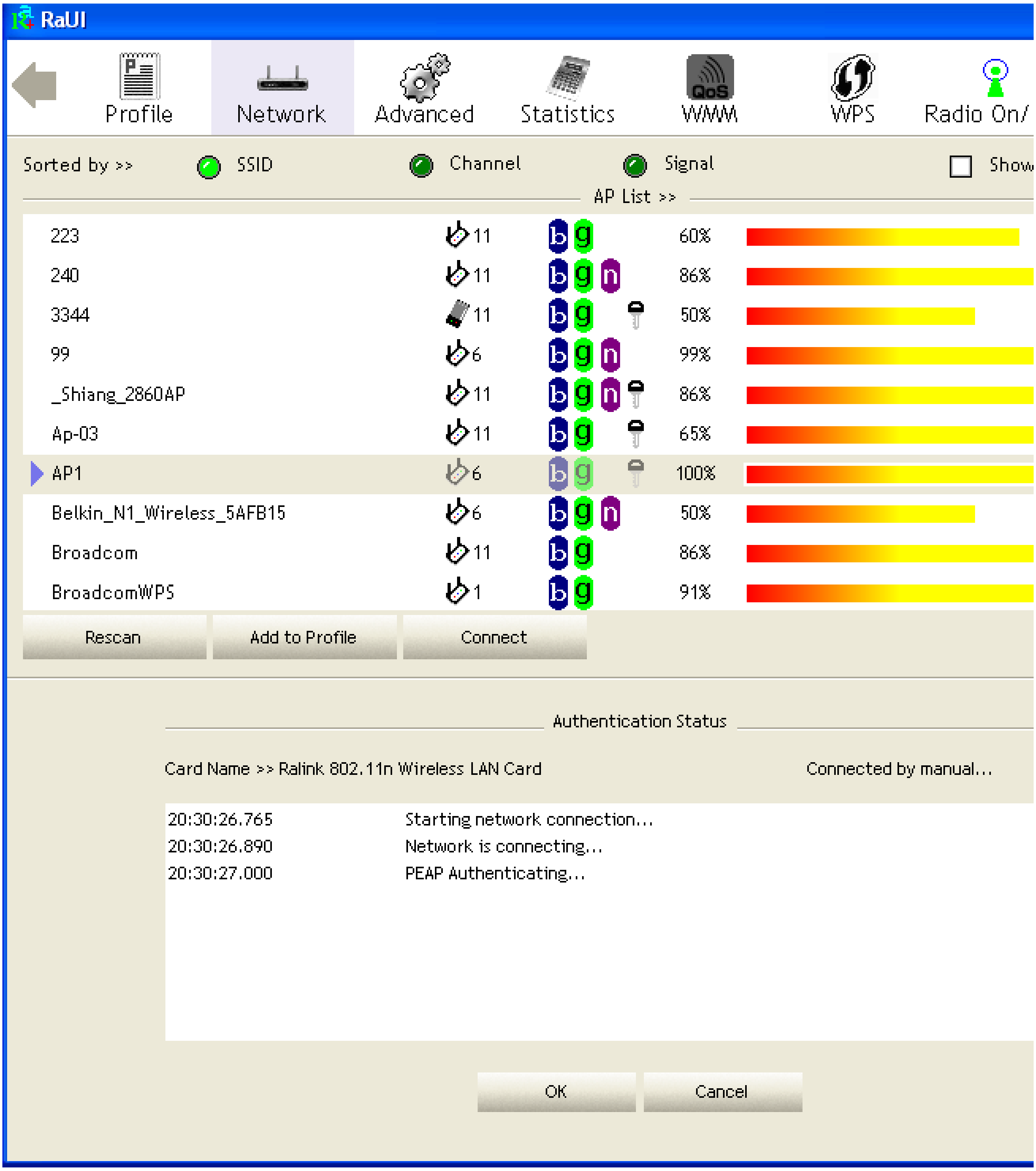
Domain Name >>

Tunnel ID / Password

Identity >> wpatest2

Password >> test2

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



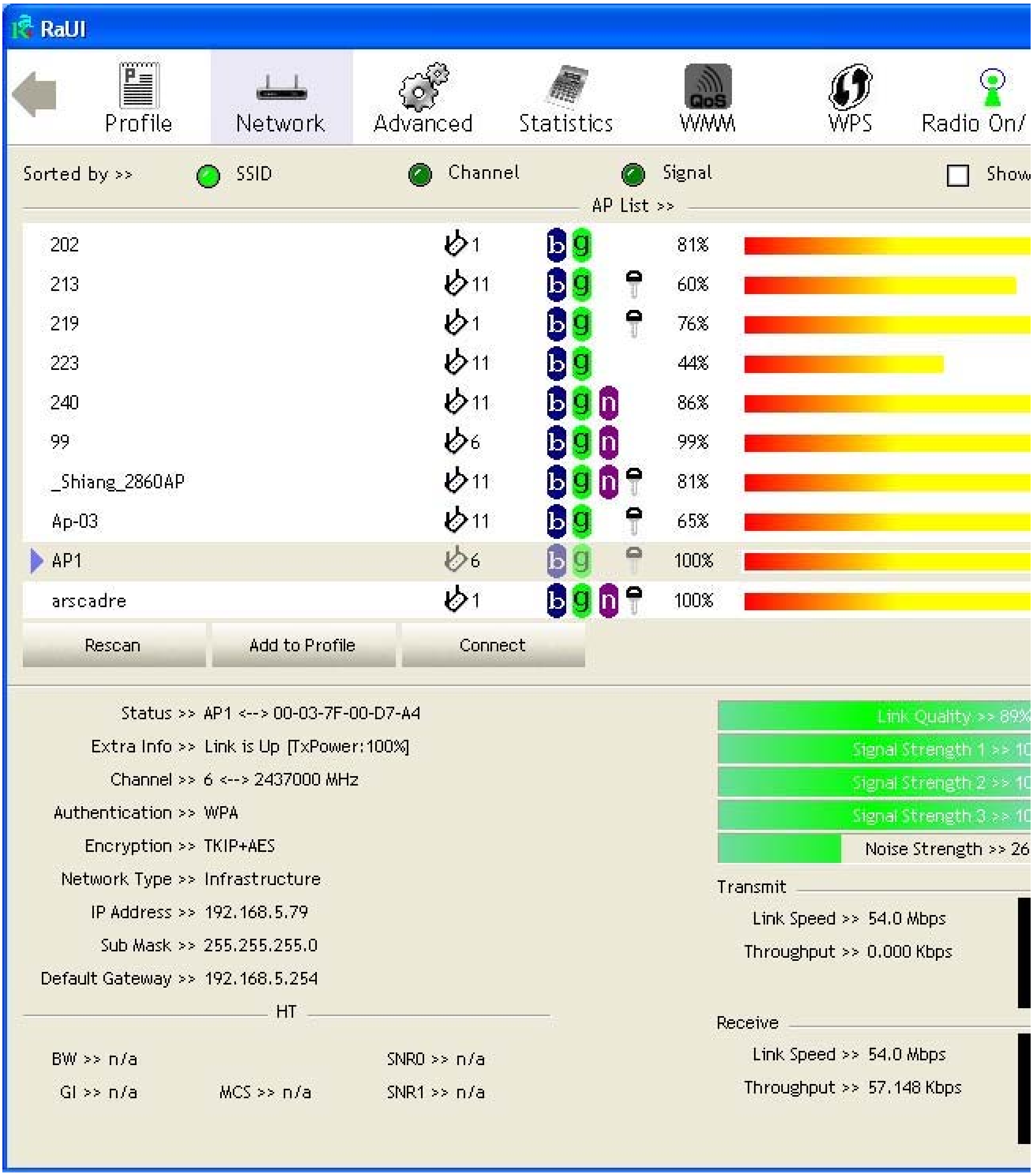
223	11	b g		60%
240	11	b g n		86%
3344	11	b g	🔑	50%
99	6	b g n		99%
_Shiang_2860AP	11	b g n	🔑	86%
Ap-03	11	b g	🔑	65%
AP1	6	b g	🔑	100%
Belkin_N1_Wireless_5AFB15	6	b g n		50%
Broadcom	11	b g		86%
BroadcomWPS	1	b g		91%

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

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

*If you want to disconnect, please click cancel button in Authentication Status function.
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

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



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

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.5.79

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 89%

Signal Strength 1 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

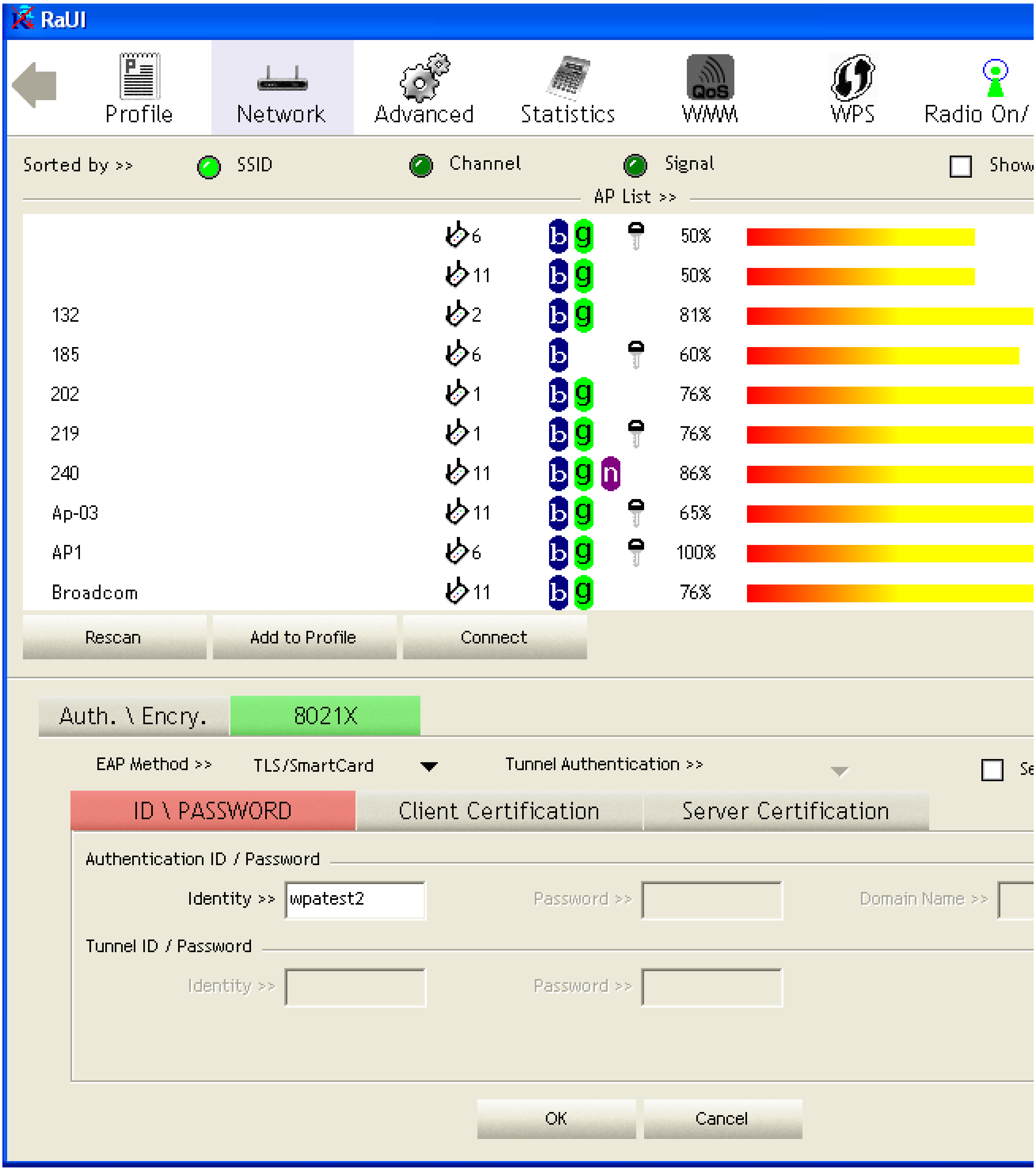
Receive

Link Speed >> 54.0 Mbps

Throughput >> 57.148 Kbps

TLS / Smart Card :

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



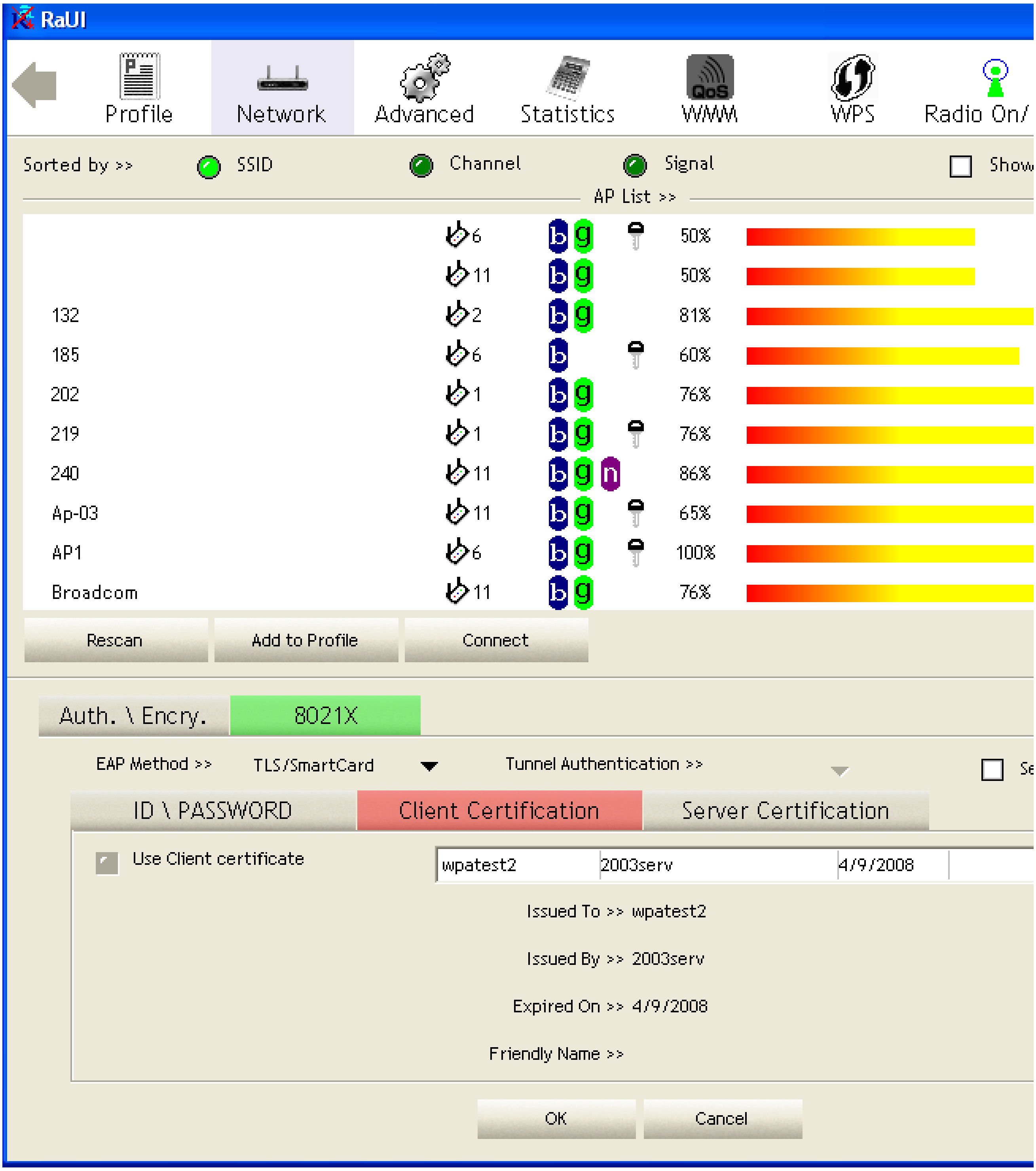
	6	b g	🔒	50%
	11	b g		50%
132	2	b g		81%
185	6	b	🔒	60%
202	1	b g		76%
219	1	b g	🔒	76%
240	11	b g n		86%
Ap-03	11	b g	🔒	65%
AP1	6	b g	🔒	100%
Broadcom	11	b g		76%

Auth. \ Encry. 8021X

EAP Method >> TLS/SmartCard

Identity >> wpatest2

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



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

Auth. \ Encry. 8021X

EAP Method >> TLS/SmartCard

Tunnel Authentication >>

☑ Use Client certificate

wpatest2	2003serv	4/9/2008

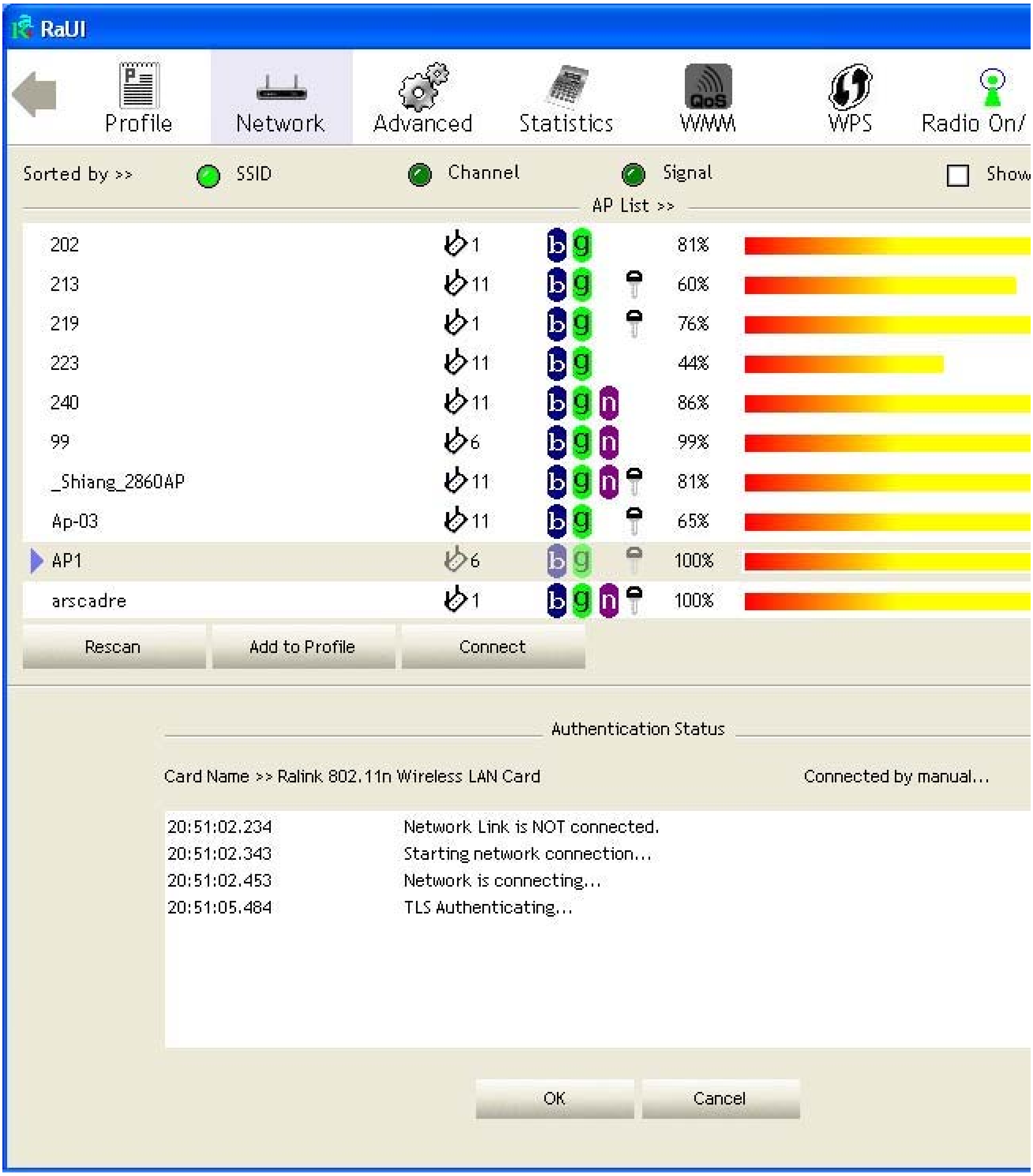
Issued To >> wpatest2

Issued By >> 2003serv

Expired On >> 4/9/2008

Friendly Name >>

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



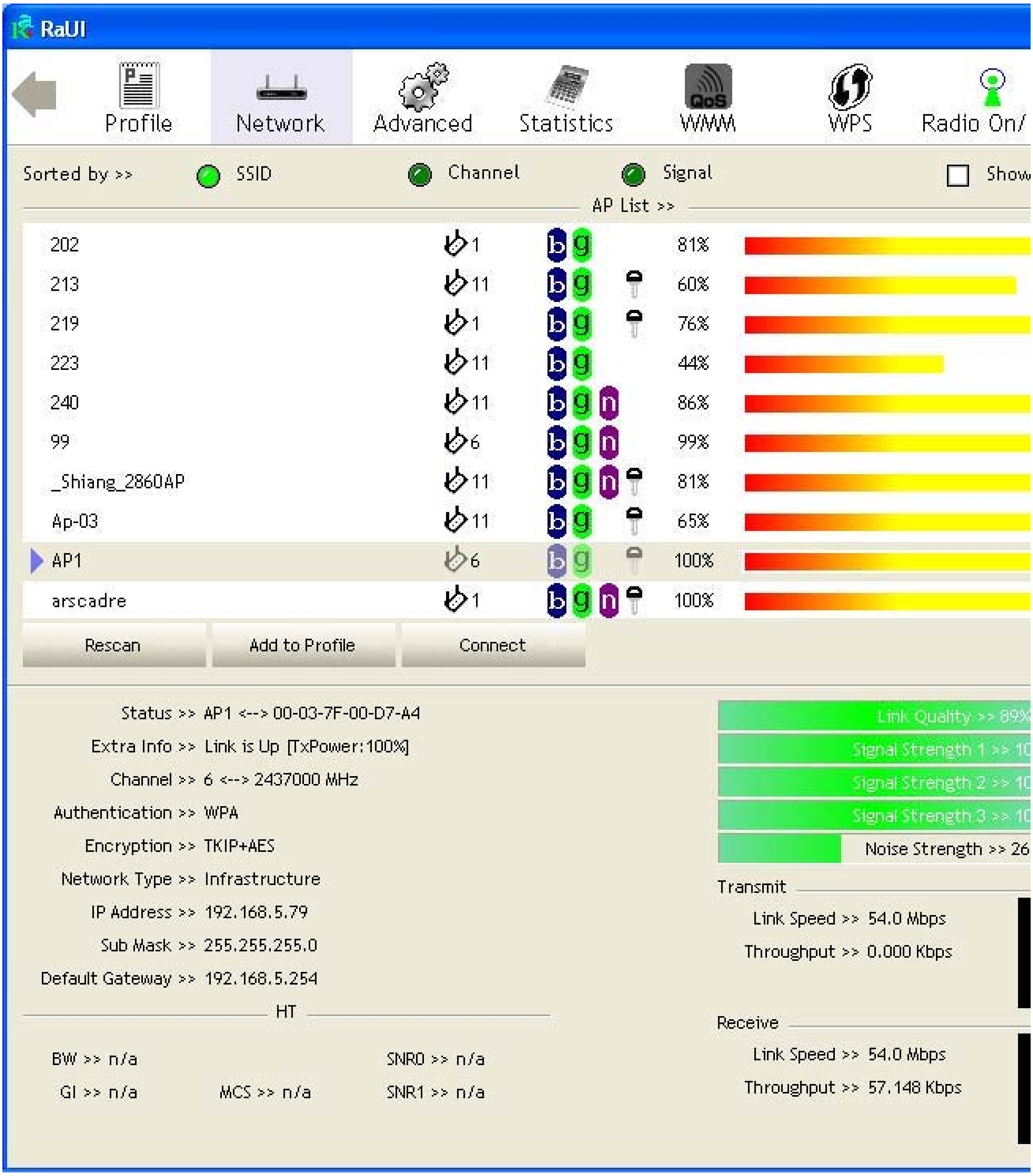
SSID	Channel		Signal
202	1	b g	81%
213	11	b g	60%
219	1	b g	76%
223	11	b g	44%
240	11	b g n	86%
99	6	b g n	99%
_Shiang_2860AP	11	b g n	81%
Ap-03	11	b g	65%
AP1	6	b g	100%
arscadre	1	b g n	100%

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

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

*If you want to disconnect, please click cancel 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.



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

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

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

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.5.79

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.5.254

HT

BW >> n/a

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

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 89%

Signal Strength 1 >> 10

Signal Strength 2 >> 10

Signal Strength 3 >> 10

Noise Strength >> 26

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

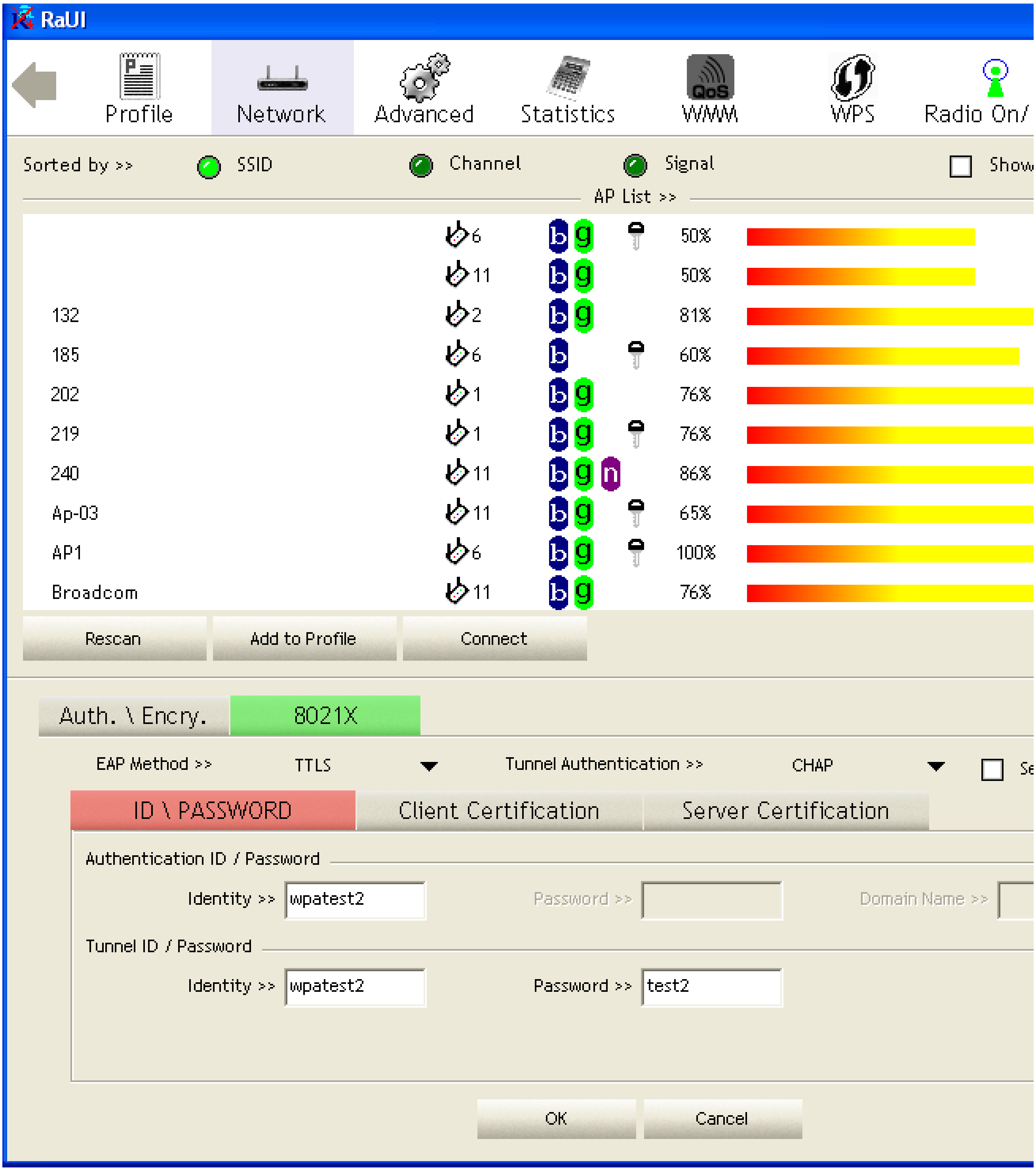
Receive

Link Speed >> 54.0 Mbps

Throughput >> 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.



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

Auth. \ Encry. 8021X

EAP Method >> TTLS   Tunnel Authentication >> CHAP   □ Se

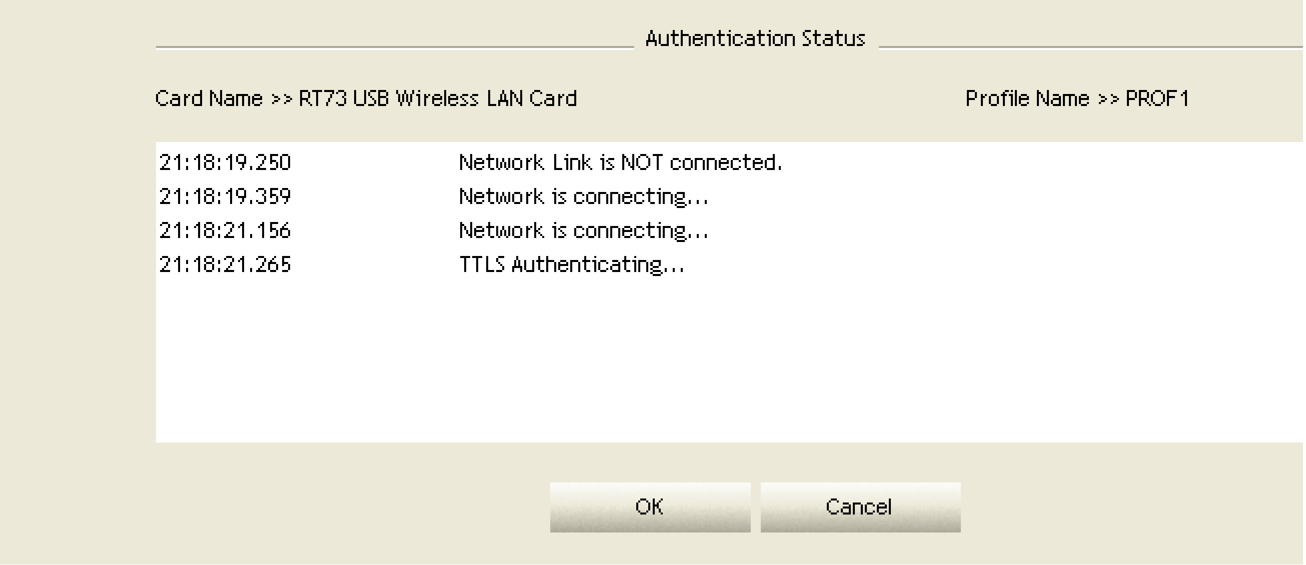
Authentication ID / Password

Identity >> wpatest2   Password >>   Domain Name >>

Tunnel ID / Password

Identity >> wpatest2   Password >> test2

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



Authentication Status

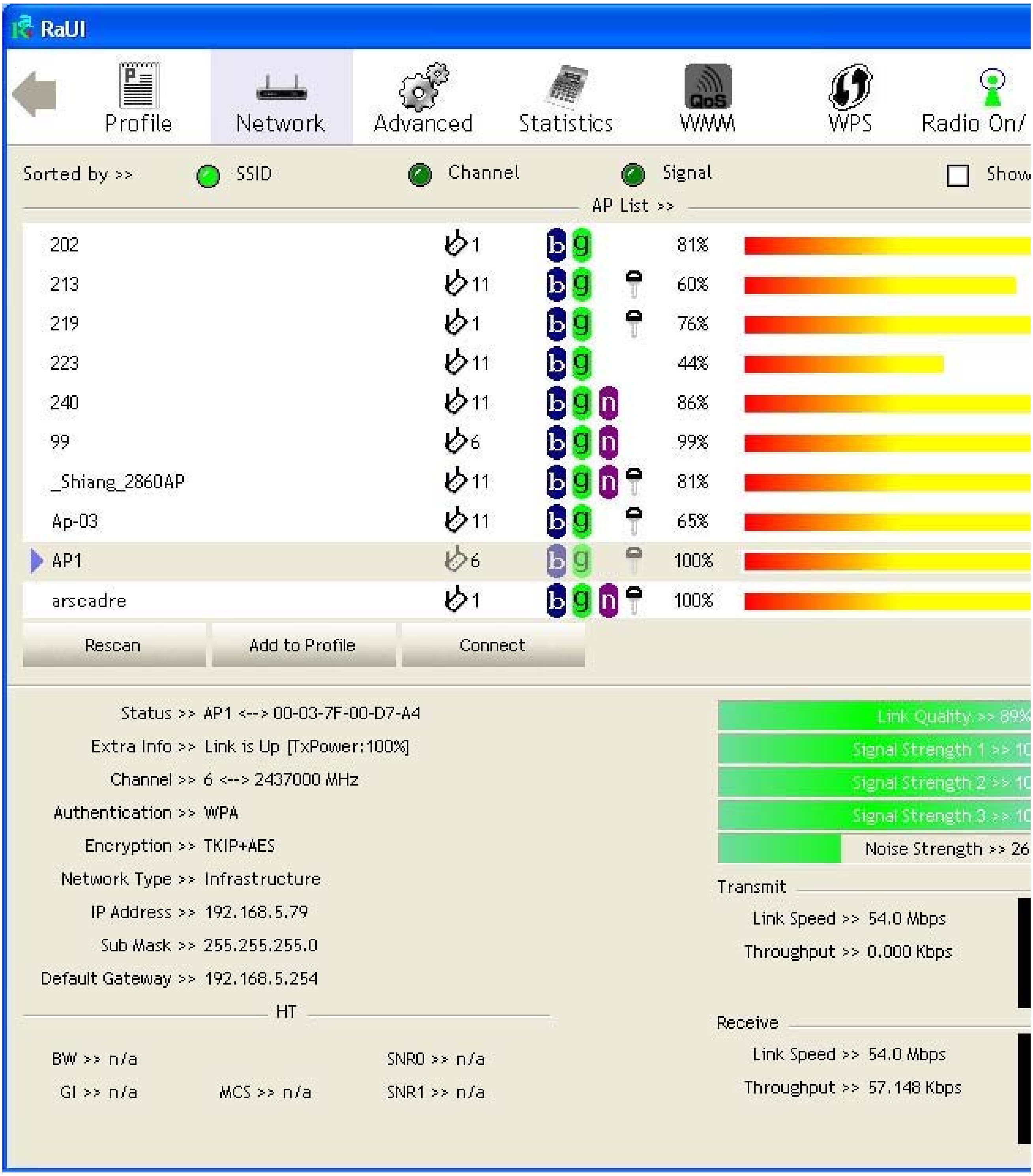
Card Name >> RT73 USB Wireless LAN Card

Profile Name >> PROF1

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

*If you want to disconnect, please click cancel 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.



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

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

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

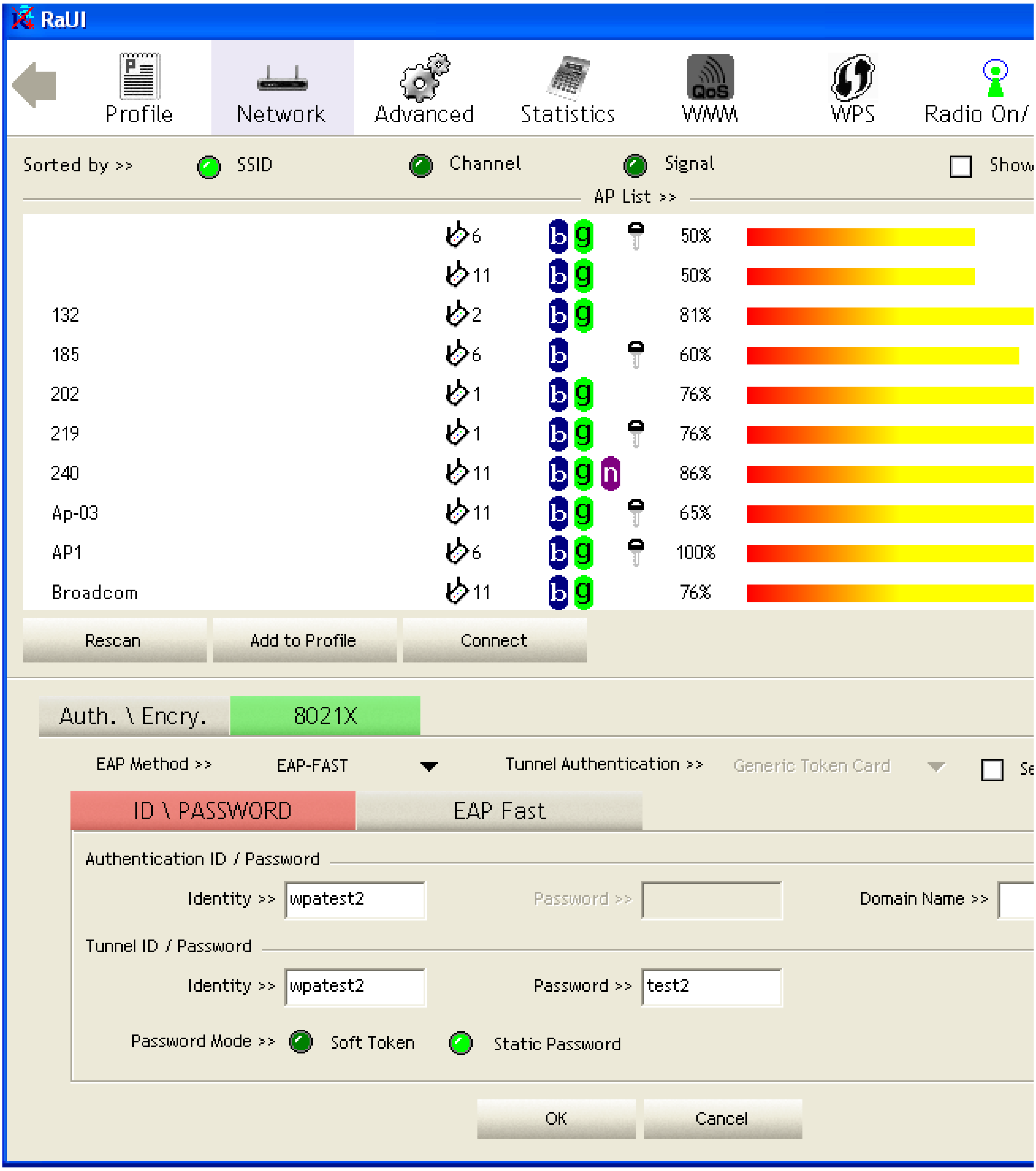
Link Quality >> 89%
Signal Strength 1 >> 10
Signal Strength 2 >> 10
Signal Strength 3 >> 10
Noise Strength >> 26

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

Receive
Link Speed >> 54.0 Mbps
Throughput >> 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.



RaUI

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

AP List >>

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

Rescan | Add to Profile | Connect

Auth. \ Encry. | 8021X

EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card □ Se

ID \ PASSWORD | EAP Fast

Authentication ID / Password

Identity >> wpatest2

Password >>

Domain Name >>

Tunnel ID / Password

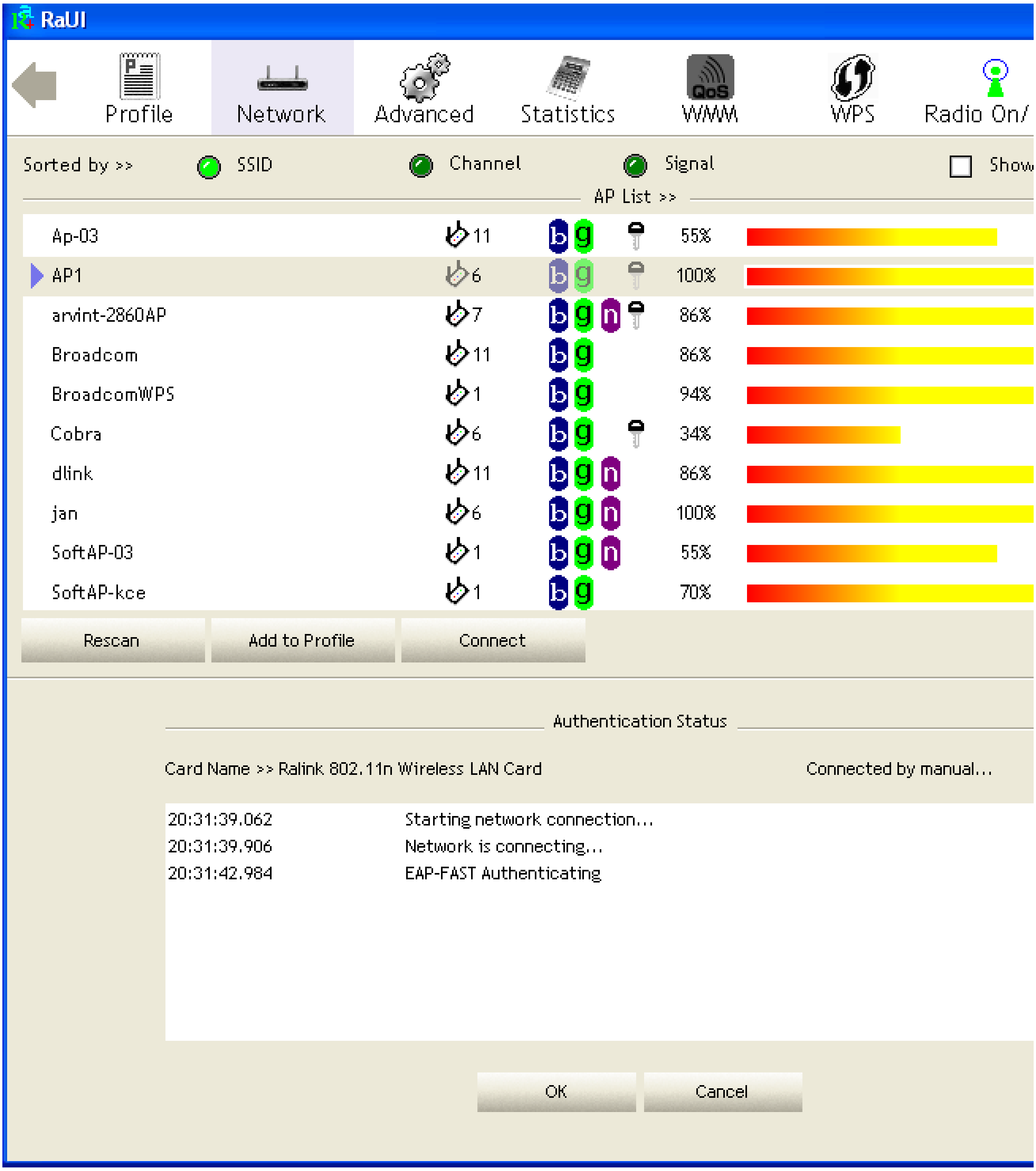
Identity >> wpatest2

Password >> test2

Password Mode >> ● Soft Token ● Static Password

OK | Cancel

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



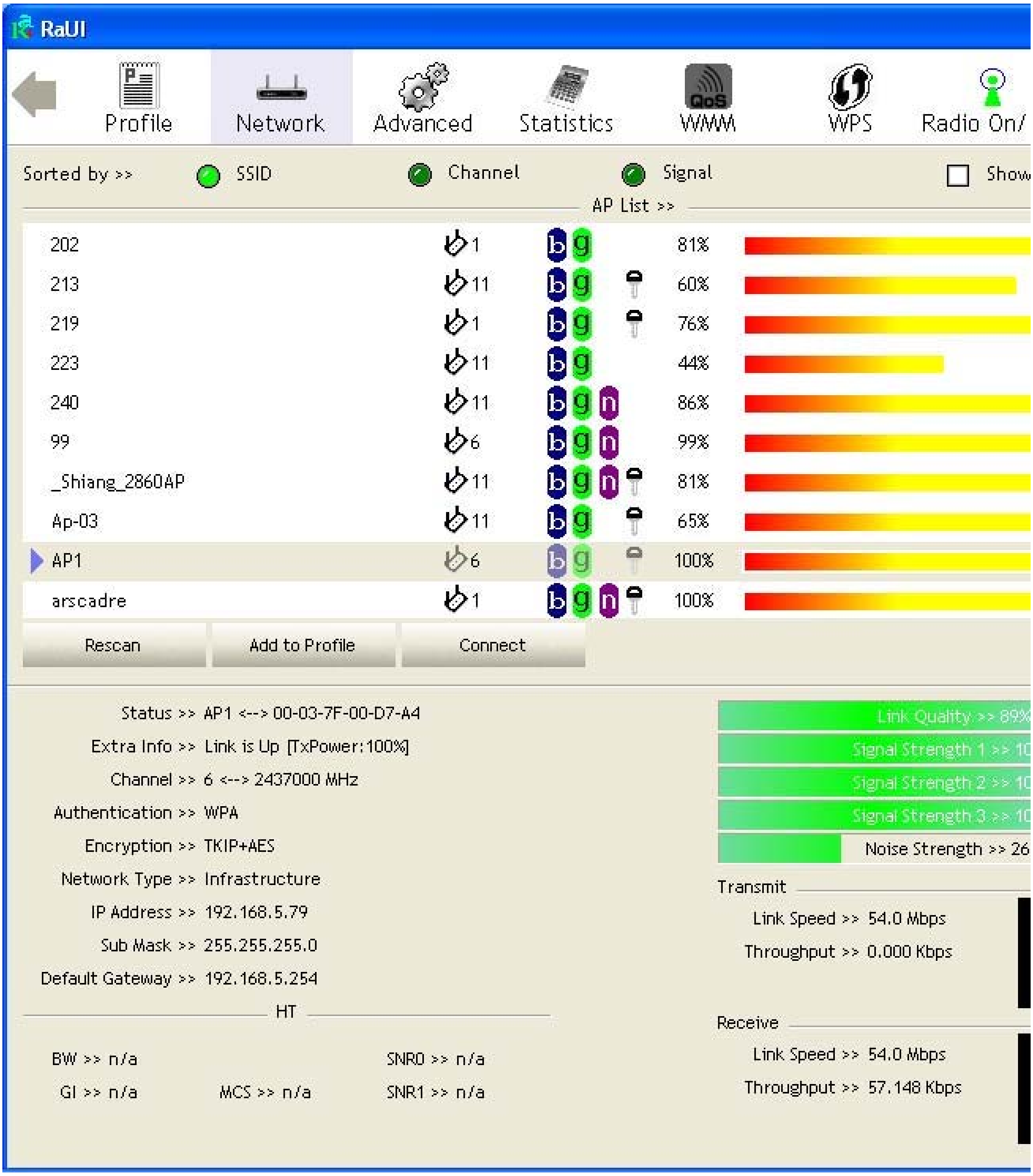
Ap-03	11	b g	🔑	55%
AP1	6	b g	🔑	100%
arvint-2860AP	7	b g n	🔑	86%
Broadcom	11	b g		86%
BroadcomWPS	1	b g		94%
Cobra	6	b g	🔑	34%
dlink	11	b g n		86%
jan	6	b g n		100%
SoftAP-03	1	b g n		55%
SoftAP-kce	1	b g		70%

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
```

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



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

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

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

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

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

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

*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.