

### → About Page

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

RaConfig Version >> 2.0.3.0                      Date >> 08-02-2007  
Driver Version >> 1.0.4.0                      Date >> 07-28-2007  
EEPROM Version >> 134.0  
Firmware Version >> 0.4  
Phy\_Address >> 00-06-4F-55-88-77

WWW.RALINKTECH.COM

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

### → Link Status

Status >> Default\_11G <-> 00-06-4F-44-CB-F0  
Extra Info >> Link is Up [TxPower:100%]  
Channel >> 6 <-> 2437 MHz  
Authentication >> Unknown  
Encryption >> None  
Network Type >> Infrastructure  
IP Address >> 192.168.10.21  
Sub Mask >> 255.255.255.0  
Default Gateway >> 192.168.10.1

HT

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

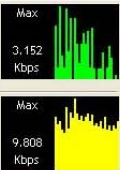
Link Quality >> 92%  
Signal Strength 1 >> 41%  
Signal Strength 2 >> 50%  
Noise Strength >> 26%

Transmit

Link Speed >> 48.0 Mbps  
Throughput >> 2.320 Kbps

Receive

Link Speed >> 11.0 Mbps  
Throughput >> 7.420 Kbps



### → Authentication 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.

Cancel

### → AP's Information

General WPS CCX

SSID >> AP1

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

Authentication Type >> Unknown

Encryption Type >> None

Channel >> 6 <-> 2437000 KHz

Network Type >> Infrastructure

Beacon Interval >> 100

Signal Strength >> 100%

Supported Rates (Mbps)

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

OK

### → Retry the Connection

Card Name >> Ralink 802.11n Wireless LAN Card

Profile Name >> PROF1

Message >> Invalid identity or password

Identity >>

Password >>

OK Cancel

### → Configuration

System Config Auth. \ Encry. 8021X

Authentication >> WPA Encryption >> TKIP

WPA Preshared Key >>

Wep Key

Key#1 Hexadecimal

Key#2 Hexadecimal

Key#3 Hexadecimal

Key#4 Hexadecimal






Show Password

OK Cancel

- At the mean time of starting RaUI, there is also a small Ralink icon appears within windows taskbar as below. You may double click it to bring up the main menu if you selected to close RaUI menu earlier. You may also use mouse's right button to close RaUI utility.



→→ 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
  -  -- indicate Wireless NIC is not connected yet
  -  -- indicate Wireless NIC is not detected
  -  -- indicate Connected and Signal Strength is Weak

### 3.1.2 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.



#### [Definition of each field]

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

**SSID:** AP or Ad-Hoc name

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

**Authentication:** Authentication mode

**Encryption:** Encryption Type

**Use 802.1x:** Whether or not use 802.1x feature

**Channel:** channel in use for Ad-Hoc mode






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

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

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

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

### [Icons and buttons]

-  → indicate connection is successful on currently activated profile
-  → indicate connection is failed on currently activate profile
-  → indicate network type is infrastructure mode
-  → indicate network type is Ad-Hoc
-  → indicate security-enabled wireless network

 → Add a new profile

 → Edit an existing profile

 → Delete an existing profile

 → Activate selected profile

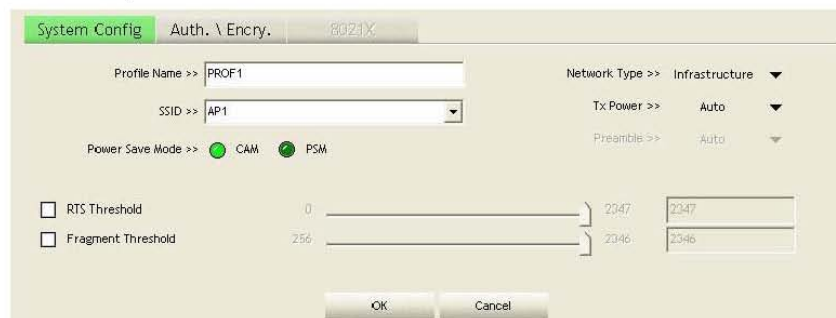
 → Show the information of Status Section

 → Hide the information of Status Section

#### 3.1.2.1 Add/Edit Profile

There are 3 methods to open Profile Editor form:

- You can open it from “Add to Profile” button in Site Survey function
- You can open it form “Add” button in Profile function
- You can open it from “Edit” button in Profile function



System Config    Auth. \ Encry.    8021X

Profile Name >> PROF1      Network Type >> Infrastructure

SSID >> AP1      Tx Power >> Auto

Power Save Mode >>  CAM     PSM      Presimble >> Auto

RTS Threshold      0      2047    2347

Fragment Threshold      256      2046    2346

OK    Cancel



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

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

**Power Save Mode:** Choose from CAM [Constantly Awake Mode] or Power Saving Mode.

**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.

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

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

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

**Authentication Type:** There are 7 type of authentication modes supported by RaUI. They are Open, Shared, LEAP, WPA, WPA-PSK, WPA2, WPA2-PSK.

**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.

**802.1x Setting:** It is an authentication for WPA and WPA2 certificate to server.

**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 lengths.

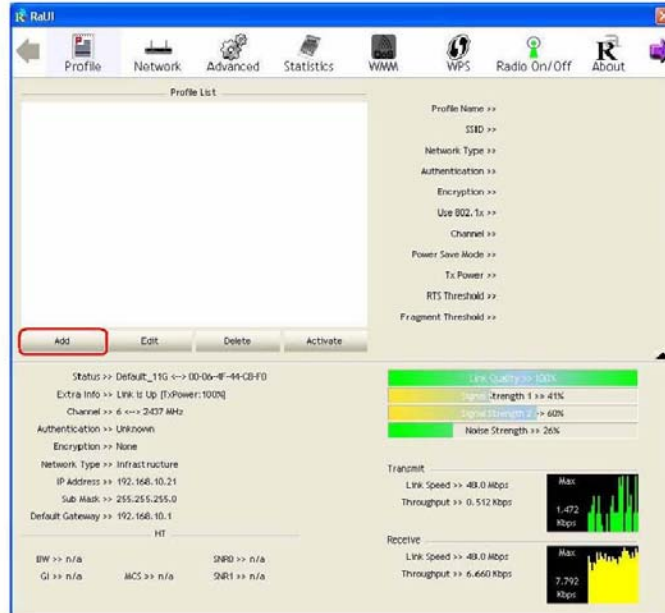
**WEP Key:** Only valid when using WEP encryption algorithm. The key must matched AP's key.

There are several formats to enter the keys:

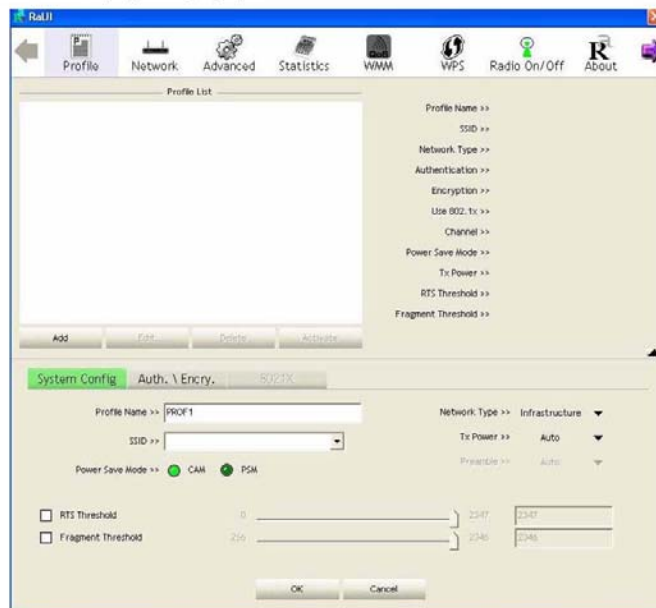
- Hexadecimal – 40bits: 10 Hex characters
- Hexadecimal – 128bits: 26 Hex characters.
- ASCII – 40bits: 5 ASCII characters
- ASCII – 128bits: 13 ASCII characters

### 3.1.2.2 Example to Add Profile in Profile

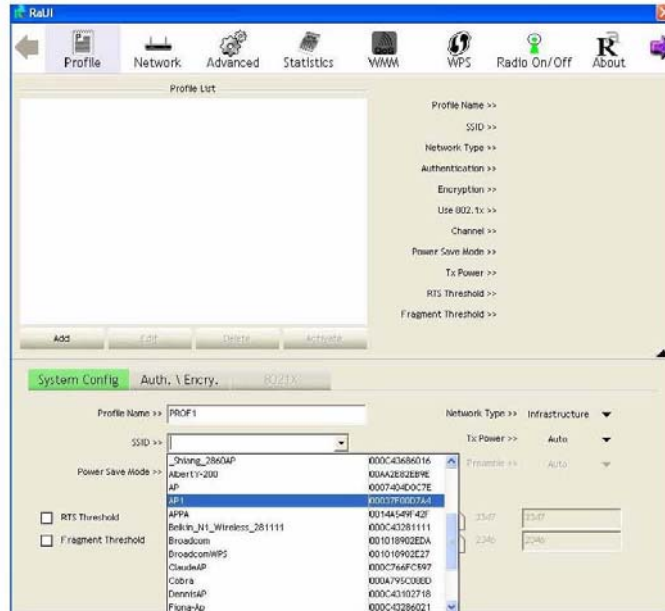
Step 1: Click Add in Profile function



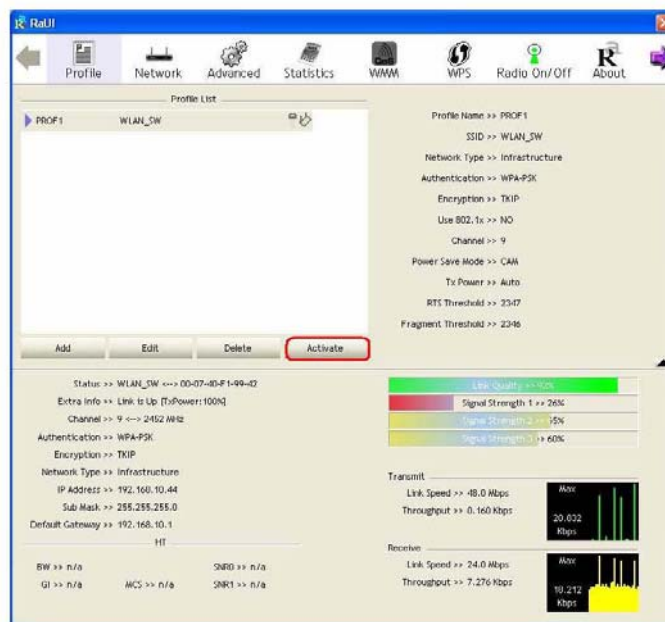
Step 2: Add Profile page will pop up.



**Step 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.



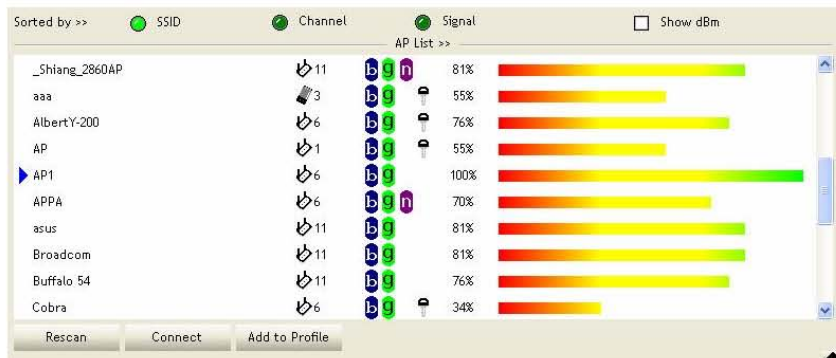
**Step 4:** Then, you can see the profile which you set appear in the profile list. Click "Activate" to activate the profile setting.





### 3.1.3 Network

Under the Network function, system will display the information of surrounding APs from last scan result. List information includes SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as below:



#### [Definition of each field]

**SSID:** Name of BSS or IBSS network

**Network Type:** Network type in use, infrastructure for BBS, Ad-Hoc for IBSS network

**Channel:** Channel in use.

**Wireless Mode:** AP support wireless mode. IT may support, 802.11b, 802.11g or 802.11n wireless mode.

**Security-Enable:** Whether AP provides security-enabled wireless network

**Signal:** Receive signal strength of specified network

#### [Icons & Buttons]

→ Indicate connection is successful.

→ Indicate network type is infrastructure mode.

→ Indicate network type is Ad-Hoc mode.

→ Indicate security-enabled wireless network.

→ Indicate 802.11b wireless mode.

→ Indicate 802.11g wireless mode.

→ Indicate 802.11n wireless mode.

Sorted by >> SSID Channel Signal → Indicate the AP lists are sorted by SSID, Channel, or Signal.

→ Command to connect to the selected network.



**Rescan** → Issue a rescan command to wireless NIC to update information on surrounding wireless network.

**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.

### [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 appropriate information to make the connection.
- (4) When you double-click on the intended AP, you can see AP's detail information.

### 3.1.4 Advanced

Wireless mode >> 802.11 B/G/N mix  Enable CCX (Cisco Compatible extensions)  Turn on CCKM  Enable Radio Measurements  Non-Serving Channel Measurements limit: 250 ms (0-2000)

Enable TX Burst  Enable TCP Window Size  Fast Roaming at: -70 dBm  Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

Apply

**Wireless Mode:** Select wireless mode. 802.11B only, 802.11B/G mix, and 802.11B/G/N mix modes are supported. (802.11 A/B/G mix selection item only exists for A/B/G adapter; 802.11B/G/N mix selection item only exists for B/G/N adapter; 802.11B/G/N mix selection item only exists for A/B/G/N adapter.)

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

- **Auto:** STA will dynamically change as AP announcement
- **ON:** Always send frame with protection.
- **Off:** Always send frame without protection.

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

**Enable Tx Burst:** Ralink's proprietary frame burst mode.

**Enable TCP Windows Size:** Enhance throughout.

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

**Select your Country Region Code:** 8 countries to choose.

**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 802.11x Authentication.

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

→ LEAP turn on CCKM

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

**Apply:** Save the save changes

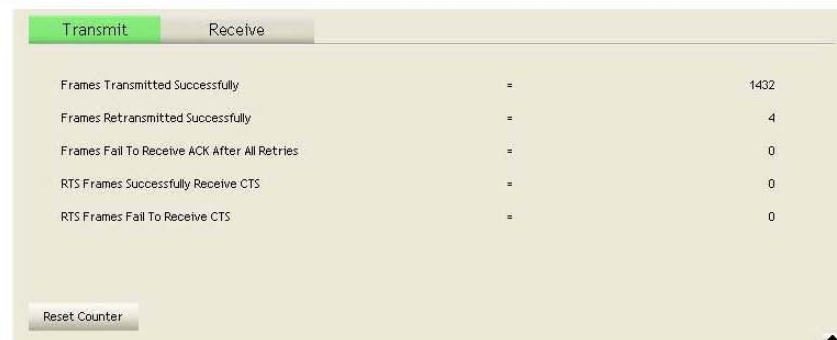
▼ → Show the information of Status Section

▲ → Hide the information of Status Section

### 3.1.5 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand.

#### [Transmit Statistics]



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

Reset Counter

**Frames Transmitted Successfully:** Frames successfully sent.

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

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

**RTS Frames Fail to Receive CTS:** Fail to receive CTS after sending RTS frame.

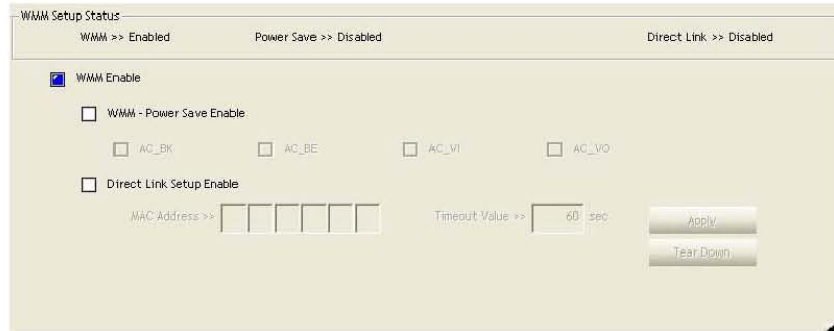
**Frames Retransmitted Successfully:** Successfully retransmitted frames numbers

**Reset Counter:** Reset counters to zero

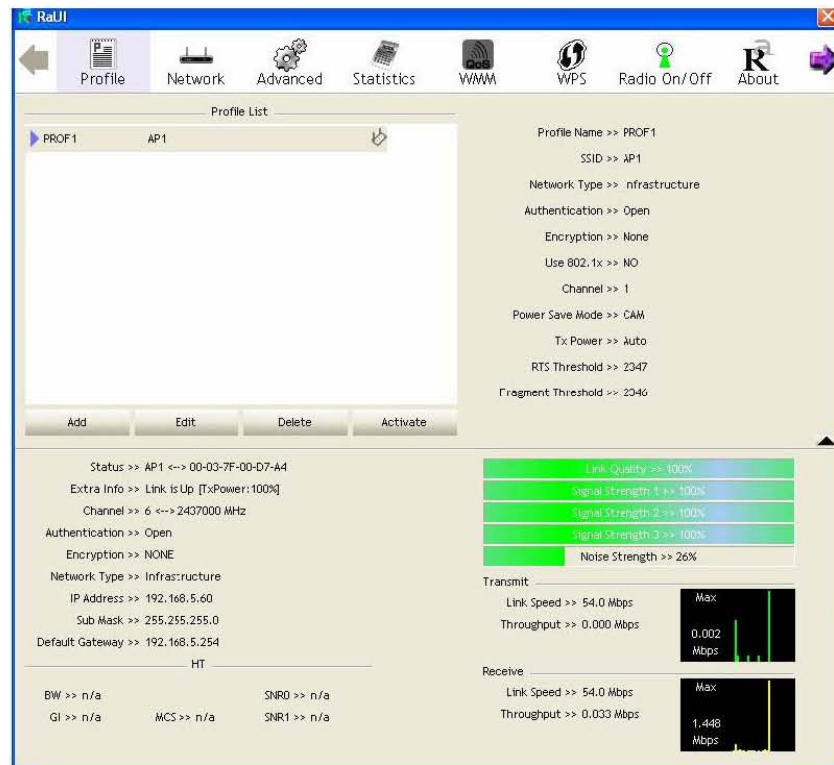


setting methods of enabling WMM indicating as follow:

**Step 1: Click "WMM Enable"**



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



**[WMM-Power Save Enable – Enable WMM Power Save]**

**Step 1: Click "WMM-Power Save Enable"**

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

MAC Address >>

Timeout Value >>  sec.

Apply

Tear Down

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

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

MAC Address >>

Timeout Value >>  sec.

Apply

Tear Down

**[Direct Link Setup Enable – Enable DLS (Direct Link Setup)]**

**Step 1:** Click “Direct Link Setup Enable”

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

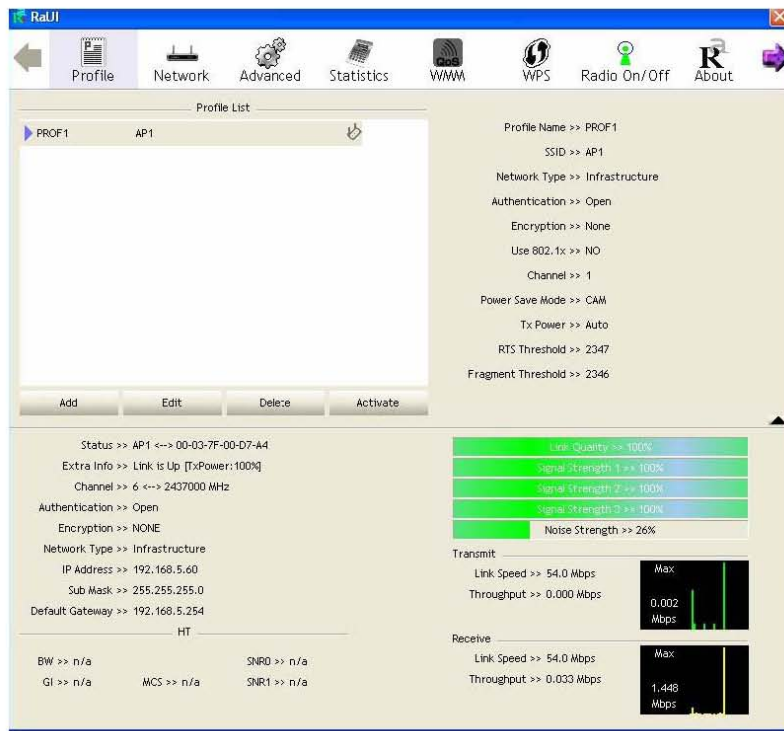
MAC Address >>

Timeout Value >>  sec.

Apply

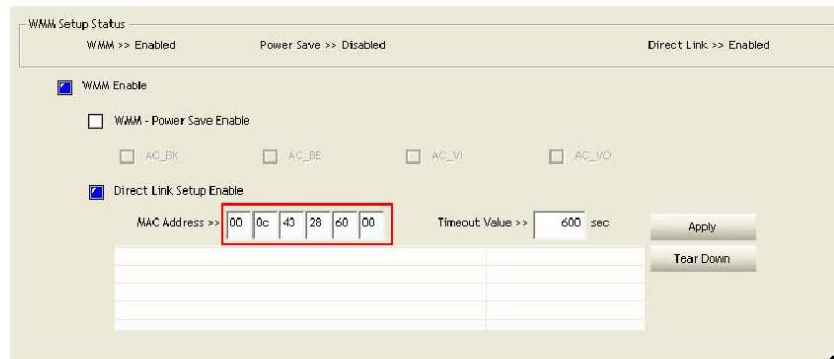
Tear Down


**Step 2:** Change to “Network” function. And add an AP that supports DLS features to a Profile. The result will look like the below figure in Profile page.



**The Setting of DLS indicates as follow:**

- (1) Fill in the blanks of Direct Link with MAC address of STA. The STA must conform to 2 conditions as follow:
  - Connect with the same AP that support DLS features.
  - Have to enable DLS



- (2) Timeout Value represent 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 Link >> Enabled

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

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

Apply      Tear Down

(3) Click “Apply” button. The result will look like the below figure.

WMM Setup Status

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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

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

00-0C-43-28-60-00      600

Apply      Tear Down

**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 itself and Timeout Value of setting.
- (2) Display the values of “DLS Status” to “Direct Link Setup” as follow:

**Step 1:** In “DLS Status”, select a direct link STA what you want to show its values in “Direct Link Setup”.



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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec

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

Apply      Tear Down

**Step 2:** Double-Click and the result will look like the below figure.

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

WMM Enable

WMM - Power Save Enable

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

Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec

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

Apply      Tear Down

(3) Disconnect Direct Link Setup as follow:

**Step 1:** Select a direct link STA.

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

WMM Enable

WMM - Power Save Enable

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

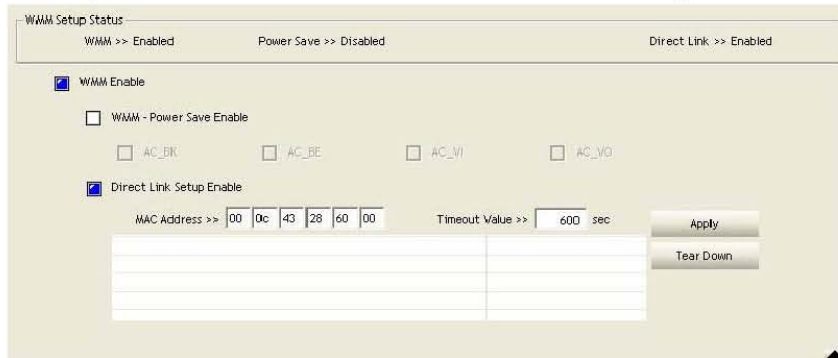
Direct Link Setup Enable

MAC Address >>            Timeout Value >>  sec

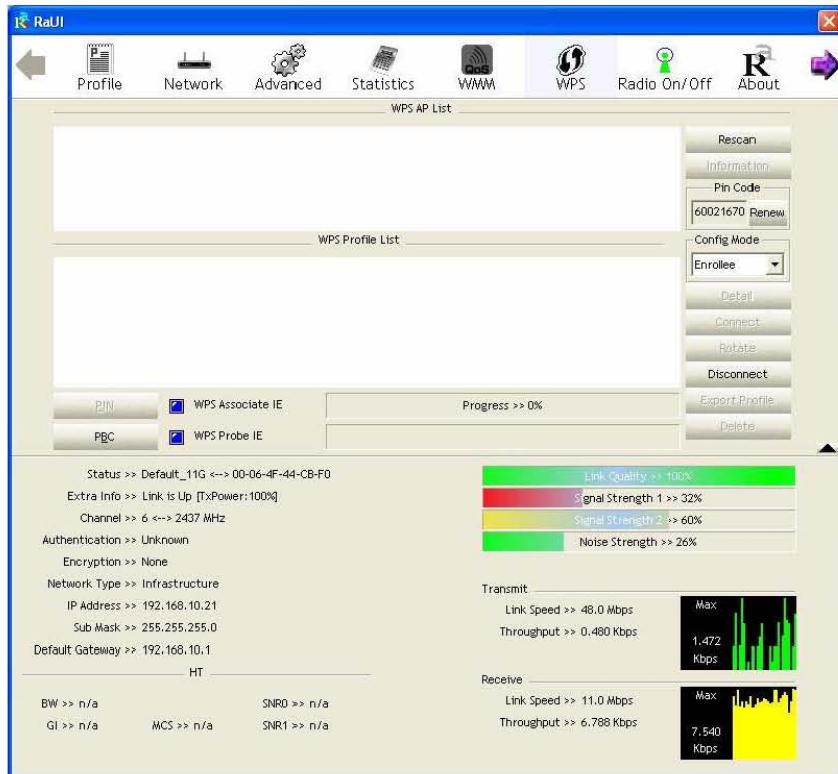
00-0C-43-28-60-00	600

Apply      Tear Down

**Step 2:** Click “Tear Down” button. The result will look like the below figure.



### 3.1.7 WPS



**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 setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

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

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

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

**PIN Code:** 8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each NIC Wireless has only one PIN Code of Enrollee.

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

**WPS Profile List:** Display all of credentials got from the Registrar. List information includes 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.

**Control items on WPS Profile List:**

- **Detail:** Information about Security and Key in the credential
- **Connect:** Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
- **Rotate:** Command to rotate to connect to the next inside credentials
- **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.
- **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.

**PIN:** Start to add to Registrar using PIN configuration method. IF STA Registrar, remember that enter PIN Code read from you Enrollee before starting PIN.

**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 connection.

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

**WPS probe IE:** Send the probe request with WPS IE during WPS setup. IT is optional for STA.

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

**Status Bar:** Display currently WPS Status.

**[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.

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

**Encryption Type:** For Open and shared authentication mode, the selection of encryption are **None** and **WEP**. For WPA, WPA2, WPA-PSK, and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.



**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

**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

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

**State:** The current configuration state on AP. The value are "Unconfigured" and "Configured".

**Version:** WPS specified version.

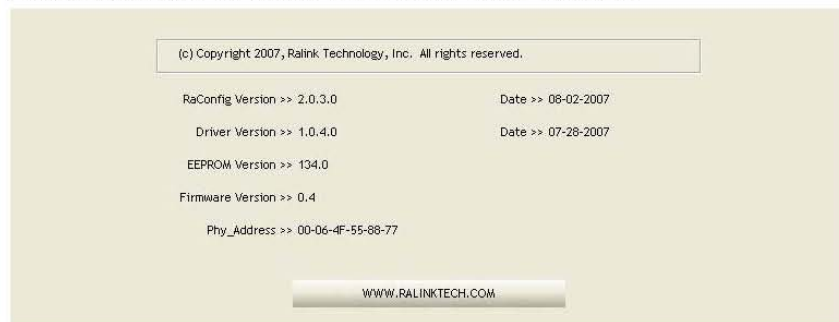
**AP Setup Locked:** Indicate if AP has entered a setup locked state.

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

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

### 3.1.8 About

About function display the wireless card and driver version information.



- (1) Connect to Ralink's Website: [WWW.RALINKTECH.COM](http://WWW.RALINKTECH.COM)
- (2) Display Configuration Utility, Driver, and EEPROM version information
- (3) Display Wireless NIC MAC Address.