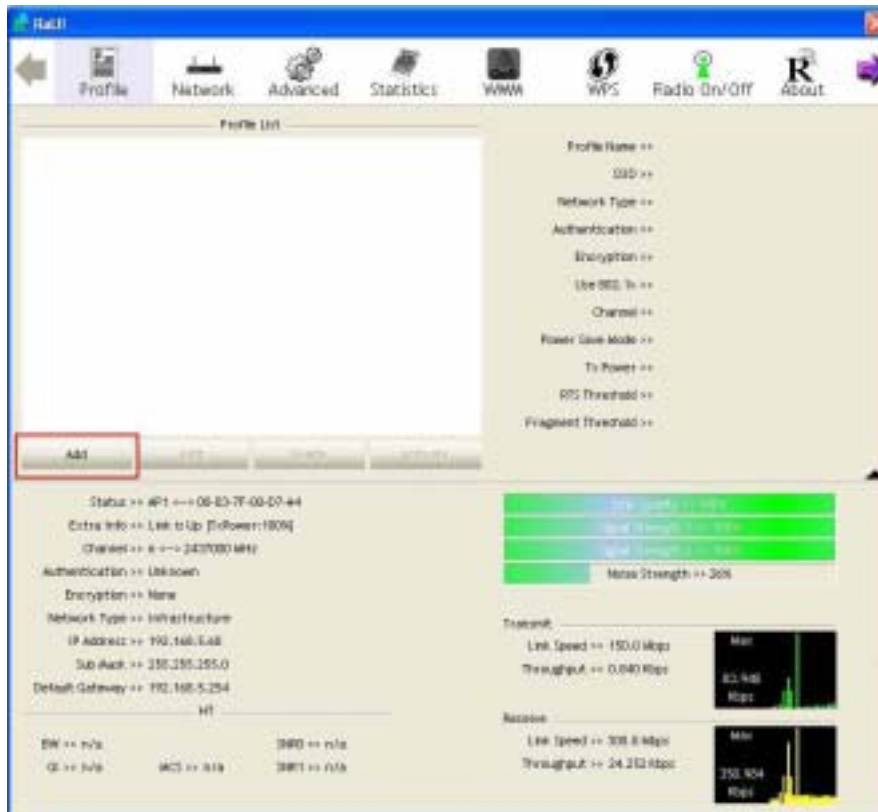


### 3.1.2.2 Example to Add Profile in Profile

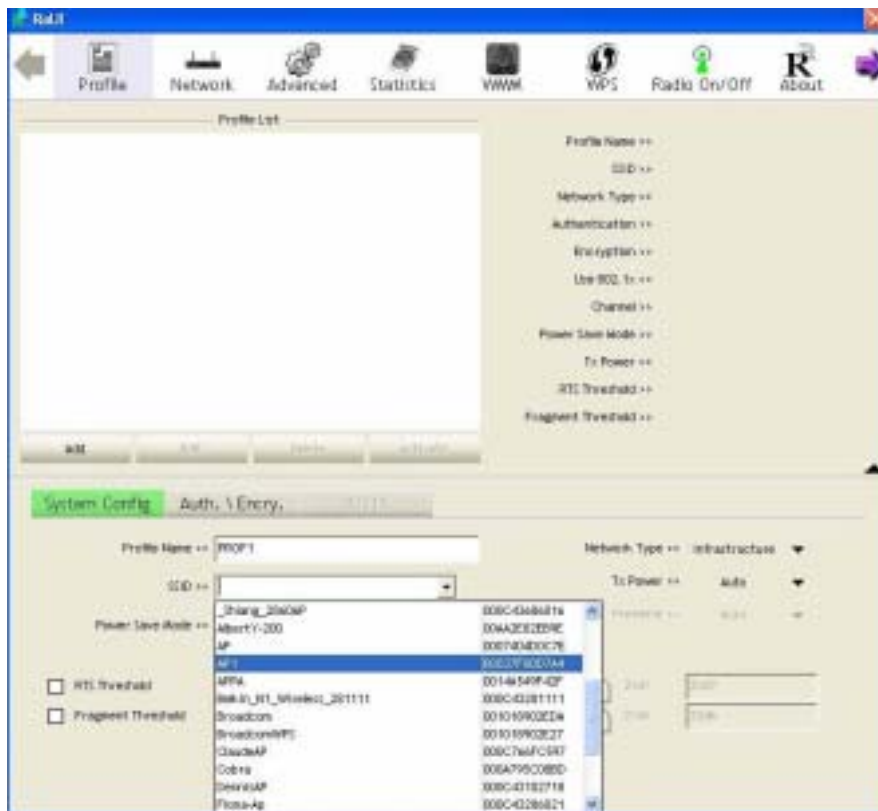
Step 1: Click **Add** in Profile function



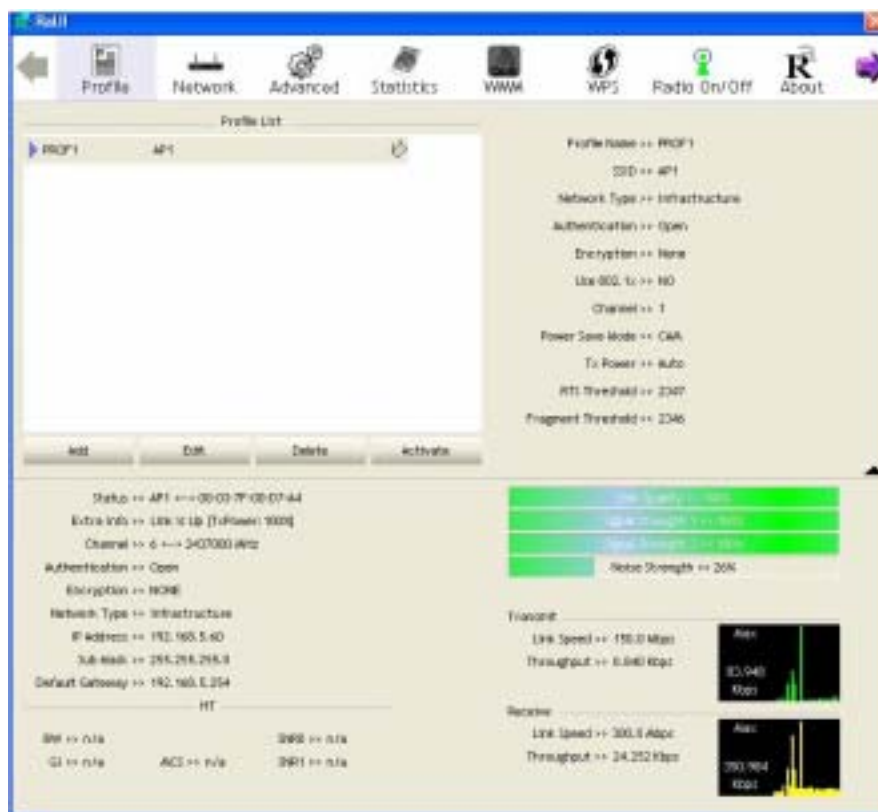
Step 2: Add Profile page will pop up.



**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.

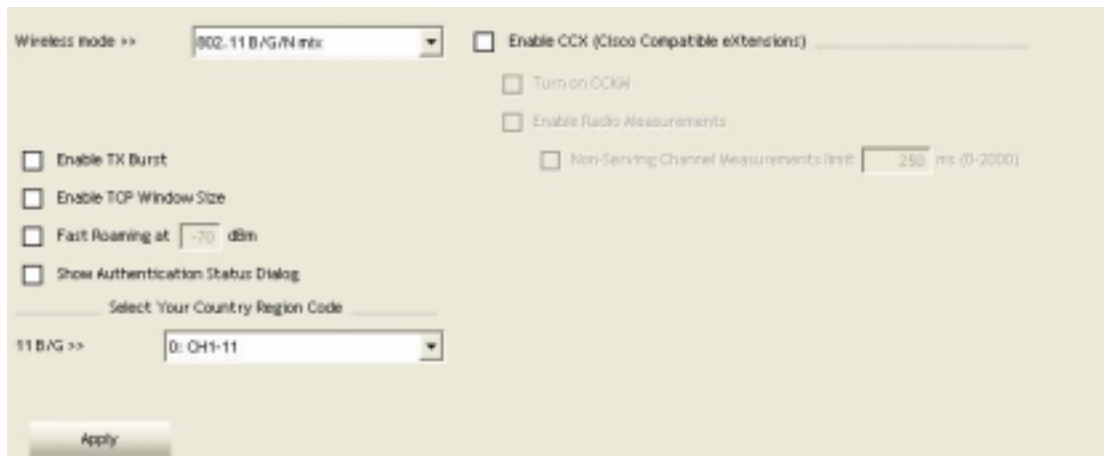
**Rescan** → Issue a rescan command to wireless NIC to update information on surrounding wireless network.

**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:** 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:** The available channel differs from different countries. For example: USA (FCC) is channel 1-11, Europe (ETSI) is channel 1-13. The operating frequency channel will be restricted to the country user located before importing. If you are in different country, you have to adjust the channel setting to comply the regulation of the country. Supporting region code for this section has CH1-11, CH1-13, CH10-11, CH10-13, CH14, CH1-14, CH3-9, and CH5-13. Please refer to below Channel Classification and range, Country Channel list to select your Country Region Code:

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

**Figure 1: Channel Classification and range**

Country Name	Classification	Range	Country Name	Classification	Range
Argentina	0	CH1-11	Lebanon	1	CH1-13
Australia	1	CH1-13	Liechtenstein	1	CH1-13
Austria	1	CH1-13	Lithuania	1	CH1-13
Bahrain	1	CH1-13	Luxembourg	1	CH1-13
Belarus	1	CH1-13	Macedonia	1	CH1-13
Belgium	1	CH1-13	Malaysia	1	CH1-13
Bolivia	1	CH1-13	Mexico	0	CH1-11
Brazil	0	CH1-11	Morocco	1	CH1-13
Bulgaria	1	CH1-13	Netherlands	1	CH1-13
Canada	0	CH1-11	New Zealand	1	CH1-13
Chile	1	CH1-13	Nigeria	1	CH1-13
China	1	CH1-13	Norway	1	CH1-13
Colombia	0	CH1-11	Panama	1	CH1-13
Costa Rica	1	CH1-13	Paraguay	1	CH1-13
Croatia	1	CH1-13	Peru	1	CH1-13
Cyprus	1	CH1-13	Philippines	1	CH1-13
Czech Republic	1	CH1-13	Poland	1	CH1-13
Denmark	1	CH1-13	Portugal	1	CH1-13
Ecuador	1	CH1-13	Puerto Rico	1	CH1-13
Egypt	1	CH1-13	Romania	1	CH1-13
Estonia	1	CH1-13	Russia	1	CH1-13
Finland	1	CH1-13	Saudi Arabia	1	CH1-13
France	3	CH10-13	Singapore	1	CH1-13
France2	1	CH1-13	Slovakia	1	CH1-13
Germany	1	CH1-13	Slovenia	1	CH1-13
Greece	1	CH1-13	South Africa	1	CH1-13
Hong Kong	1	CH1-13	South Korea	1	CH1-13
Hungary	1	CH1-13	Spain	2	CH10-11
Iceland	1	CH1-13	Sweden	1	CH1-13
India	1	CH1-13	Switzerland	1	CH1-13
Indonesia	1	CH1-13	Taiwan	0	CH1-11
Ireland	1	CH1-13	Thailand	1	CH1-13
Israel	6	CH3-9	Turkey	1	CH1-13
Italy	1	CH1-13	United Arab Emirates	1	CH1-13
Japan	5	CH1-14	United Kingdom	1	CH1-13
Japan2	4	CH14-14	United States of America	0	CH1-11
Japan3	1	CH1-13	Uruguay	1	CH1-13
Jordan	3	CH10-13	Venezuela	1	CH1-13
Kuwait	1	CH1-13	Yugoslavia	0	CH1-11
Latvia	1	CH1-13			

**Figure 2: Country Channel list**

**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]



The screenshot shows a web interface for Transmit Statistics. At the top, there are two tabs: 'Transmit' (highlighted in green) and 'Receive'. Below the tabs is a table with five rows of statistics. Each row has a label, a small icon, and a numerical value. At the bottom left of the table area is a 'Reset Counter' button.

Statistic	Value
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

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

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

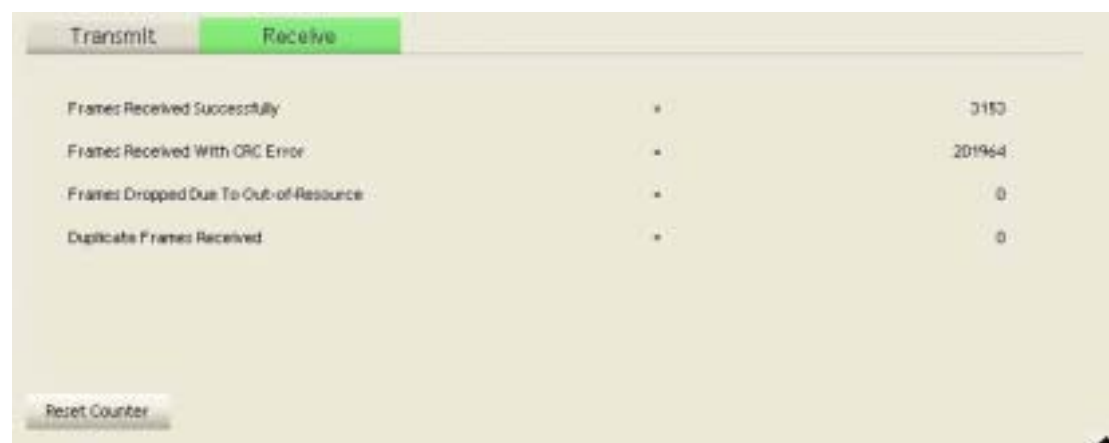
**RTS Frames Successfully Receive CTS:** Successfully receive CTS after sending RTS frame.

**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

#### [Receive Statistics]



The screenshot shows a web interface for Receive Statistics. At the top, there are two tabs: 'Transmit' and 'Receive' (highlighted in green). Below the tabs is a table with four rows of statistics. Each row has a label, a small icon, and a numerical value. At the bottom left of the table area is a 'Reset Counter' button.

Statistic	Value
Frames Received Successfully	3153
Frames Received With CRC Error	201964
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0

**Frames Received Successfully:** Frames received successfully.

**Frames Received With CRC Error:** Frames receive with CRC error.

**Frames Dropped Due To Out-Of-Resource:** Frames dropped due to resource issue.

**Duplicate Frames Received:** Duplicate received frames.

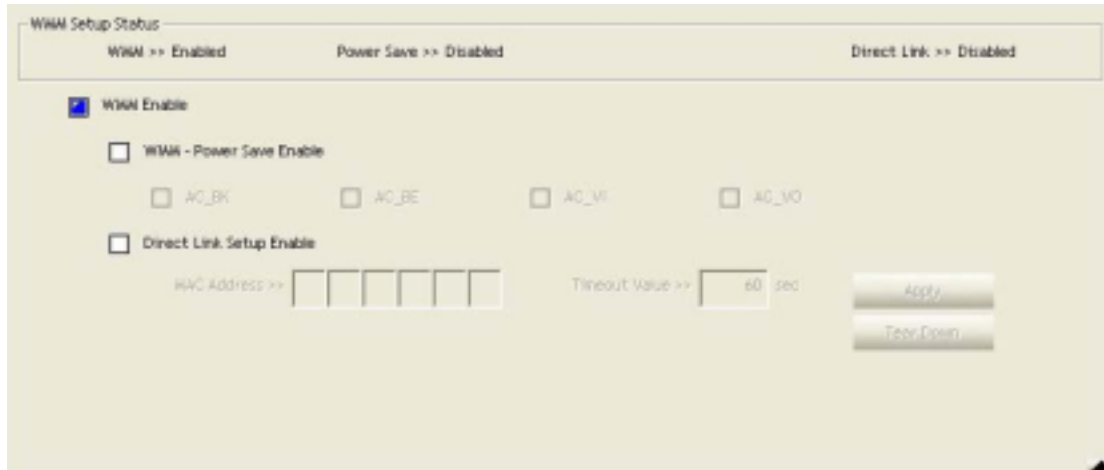
**Reset Counter:** Reset counters to zero

▼ → Show the information of Status Section

▲ → Hide the information of Status Section

### 3.1.6 WMM

WMM function involves “WMM Enable”, “WMM-Power Save Enable” and “DSL Setup”.



**WMM Enable:** Enable Wi-Fi Multi-Media.

**WMM-Power Save Enable:** Enable WMM Power Save.

**Direct Link Setup Enable:** Enable DLS (direct Link Setup).

#### [WMM Enable – Enable Wi-Fi Multi-Media]

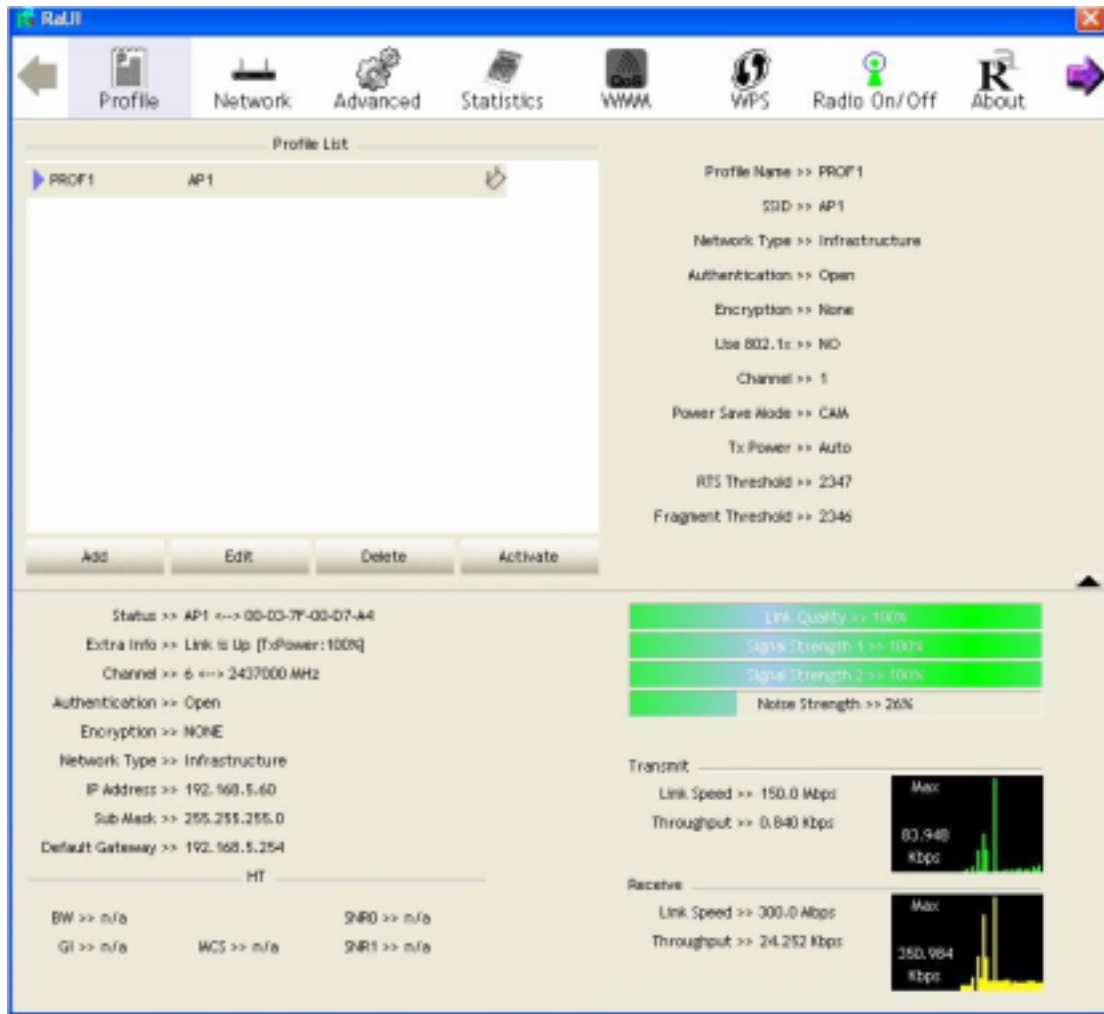
If you want to use “WMM-Power Save” or “Direct Link Setup” you must enable WMM. The setting methods of enabling WMM indicating as follow:

**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.



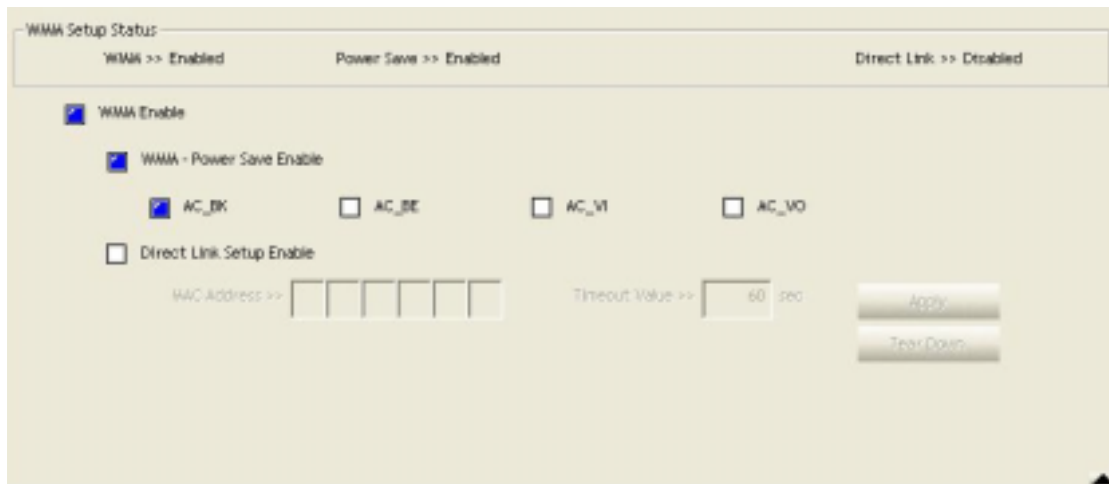


**[WMM-Power Save Enable – Enable WMM Power Save]**

**Step 1: Click “WMM-Power Save Enable”**

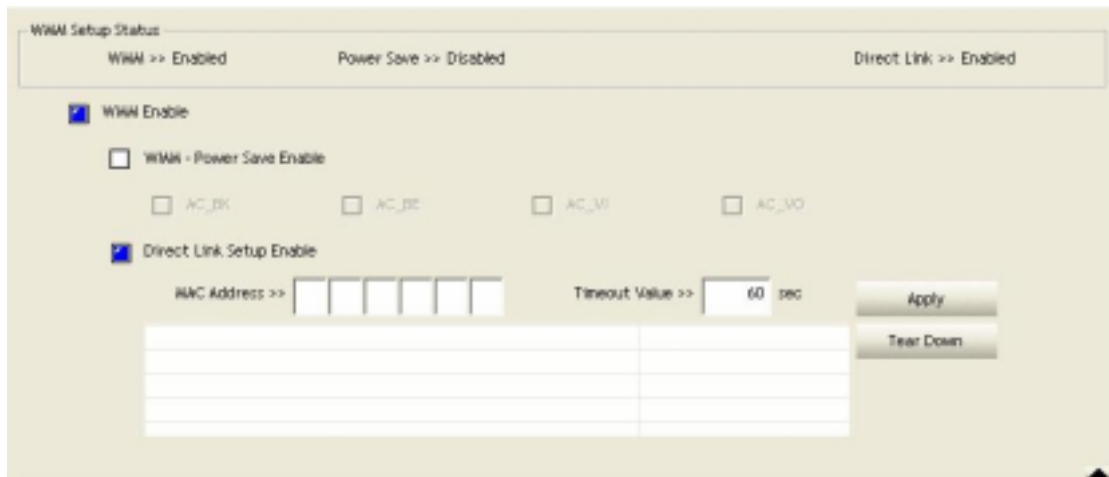


**Step 2:** Please select which ACs you want to enable. The setting of enabling WMM-Power Save is successfully.

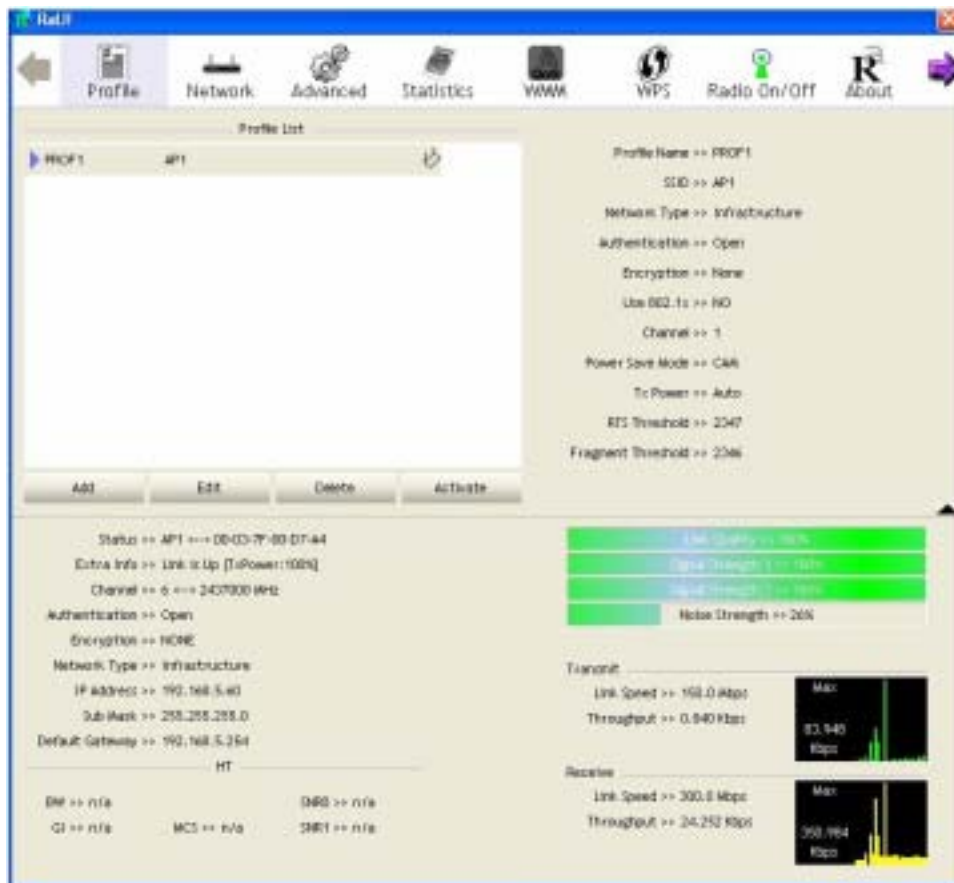


**[Direct Link Setup Enable – Enable DLS (Direct Link Setup)]**

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

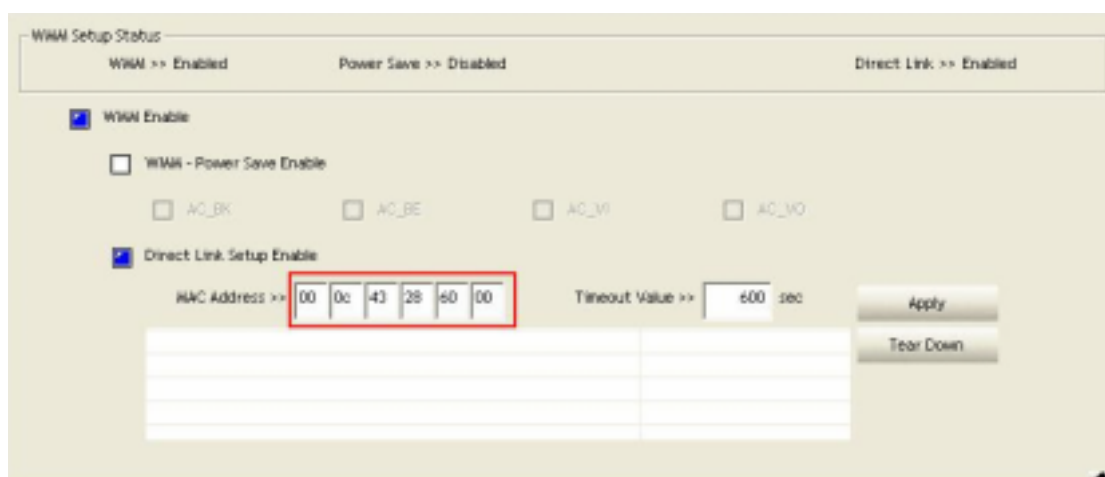


**Step 2:** Change to “Network” function. And add an AP that supports DLS features to a Profile. The result will look like the below figure in Profile page.



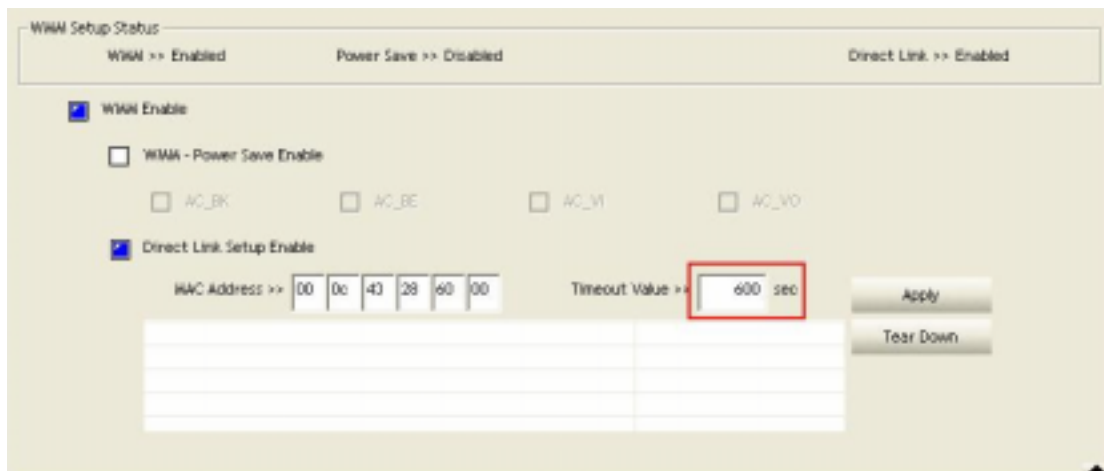
**The Setting of DLS indicates as follow:**

- (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

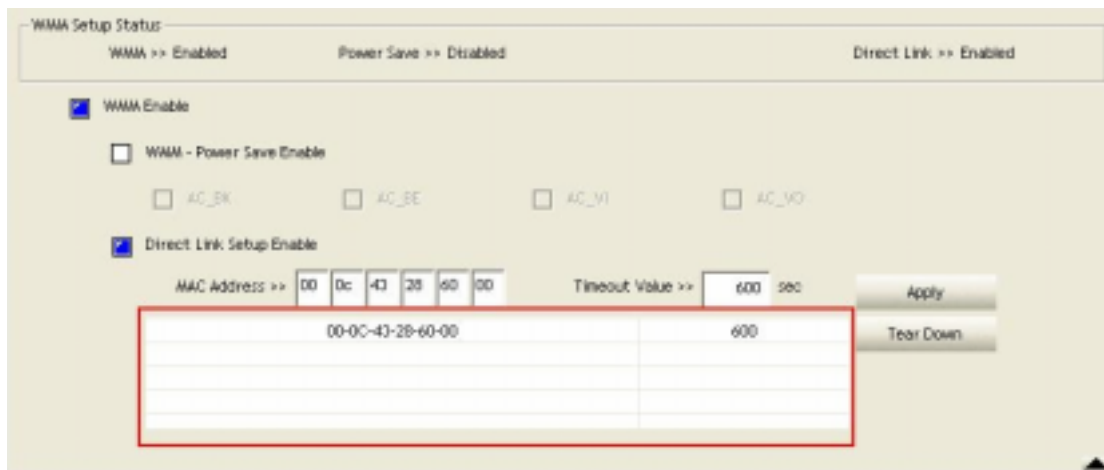


- (2) Timeout Value represent that it disconnect automatically after some seconds. The value is

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.



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

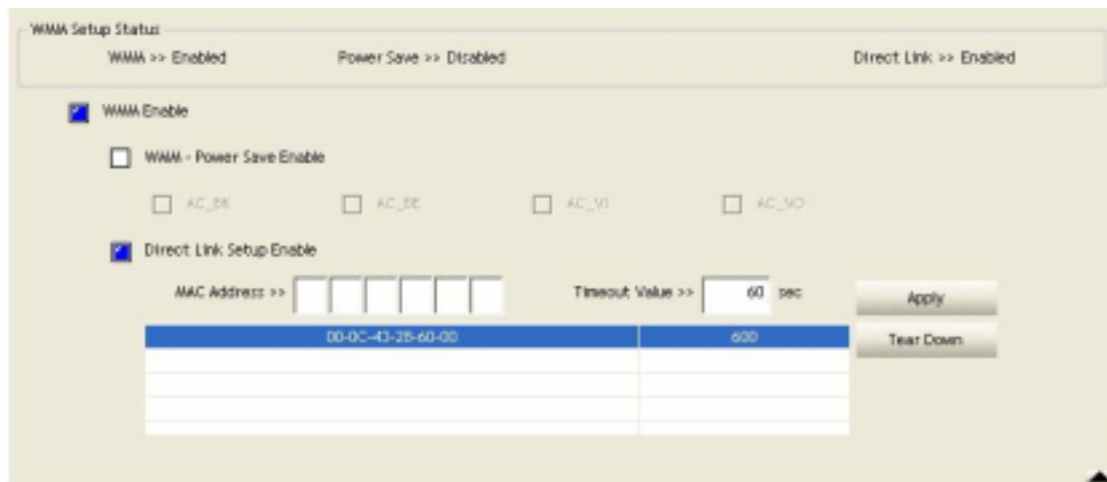


**Describe “DLS Status” as follow:**

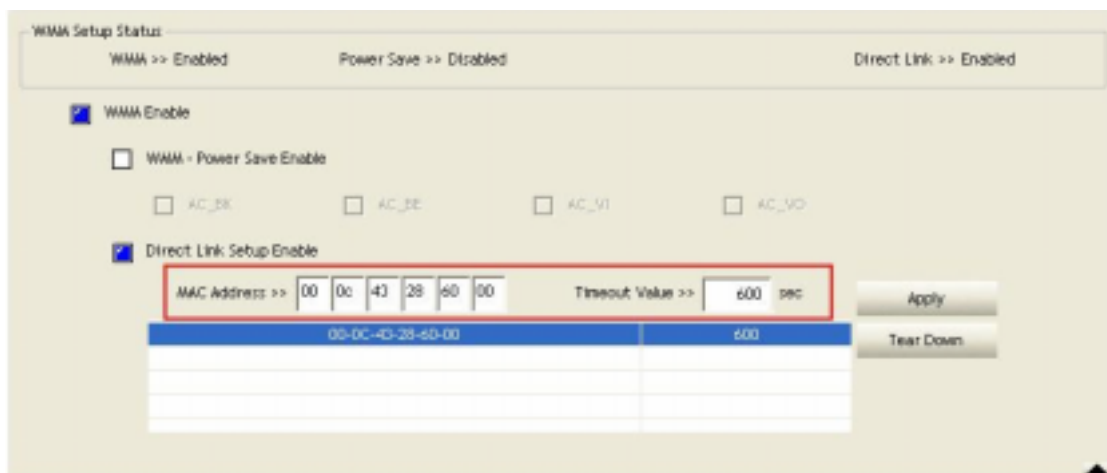
- (1) As the up figure, after configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in **“DLS Status”**. In **“DLS Status”** of the opposite side, it shows MAC address of itself and Timeout Value of setting.
- (2) Display the values of **“DLS Status”** to **“Direct 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”.

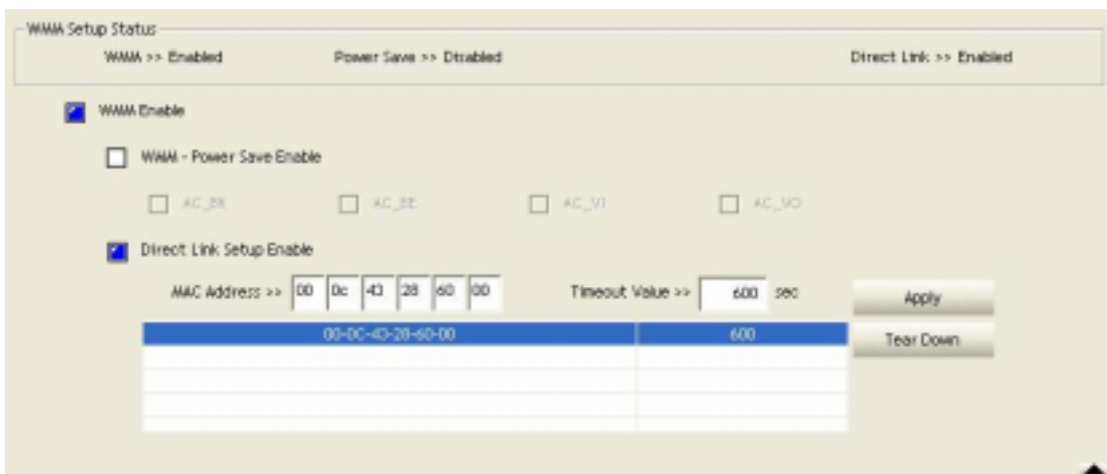


**Step 2:** Double-Click and the result will look like the below figure.

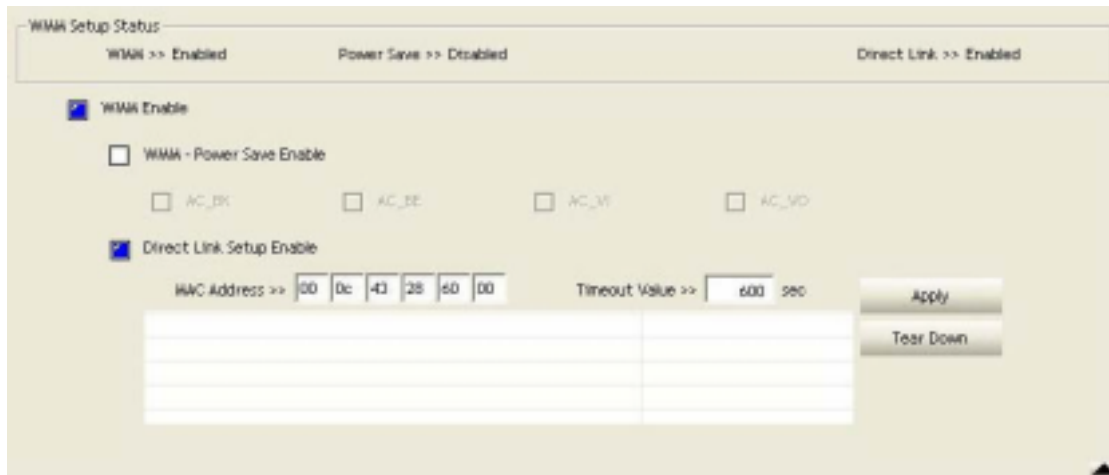


(3) Disconnect Direct Link Setup as follow:

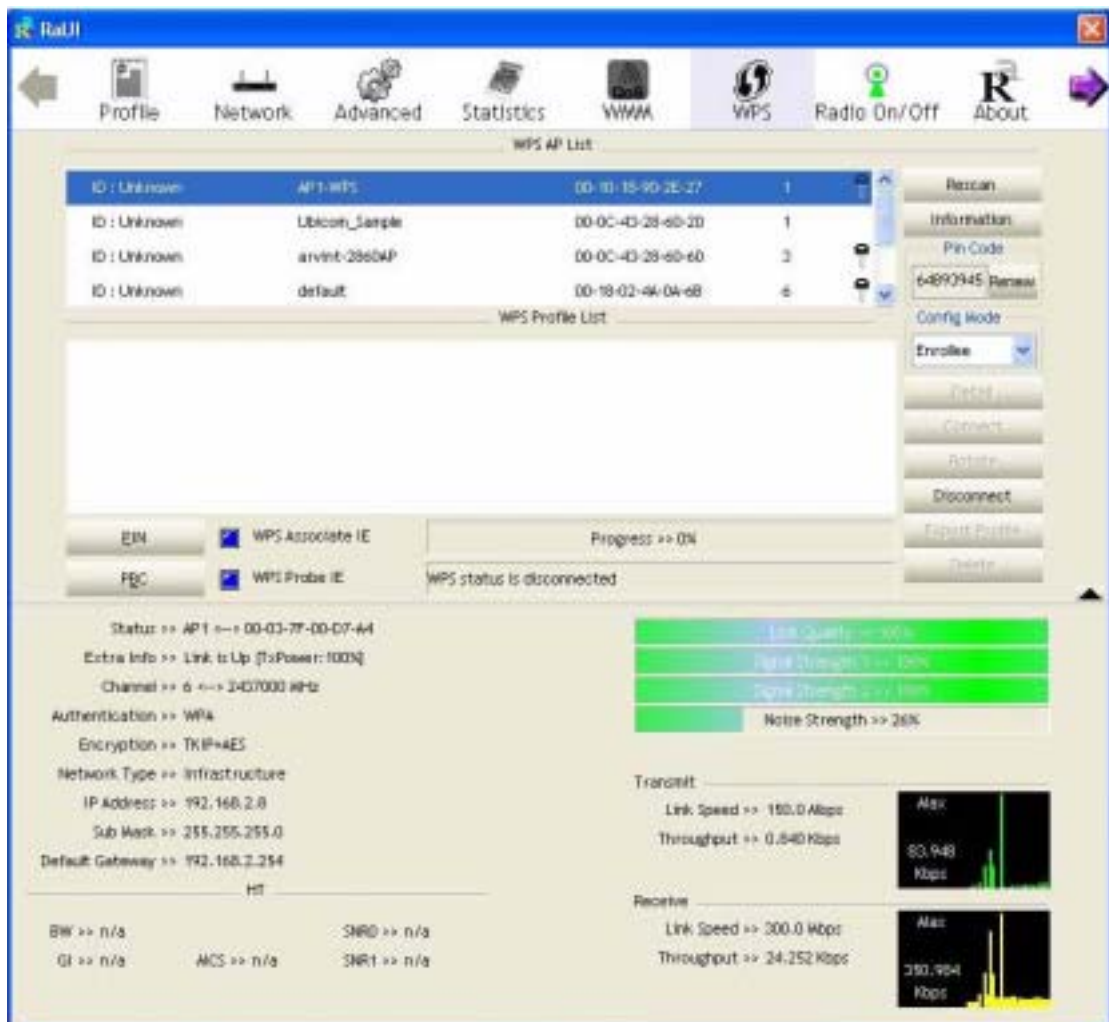
**Step 1:** Select a direct link STA.



**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

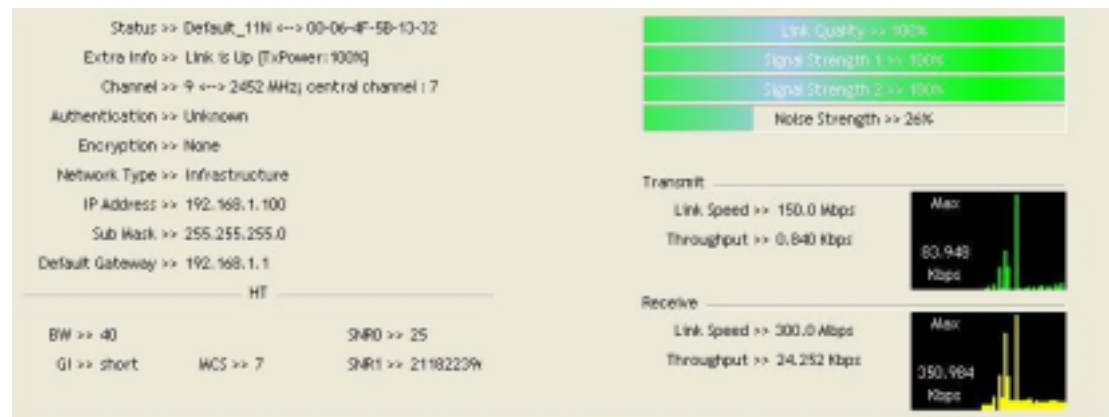
About function display the wireless card and driver version information.



- (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.

### 3.1.9 Link Status

Link Status displays the detail information current connection



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

**Extra Info:** Display link status in use.

**Channel:** Display current channel in use.

**Authentication:** Authentication mode in use.

**Encryption:** Encryption type in use.

**Network Type:** Network type in use.

**IP Address:** IP address about current connection.

**Sub Mask:** Sub Mast about current connection.

**Default Gateway:** Default gateway about current connection.

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

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

**Link Quality:** Display Connection quality based on signal strength and Tx/Rx packet error rate.

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

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

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

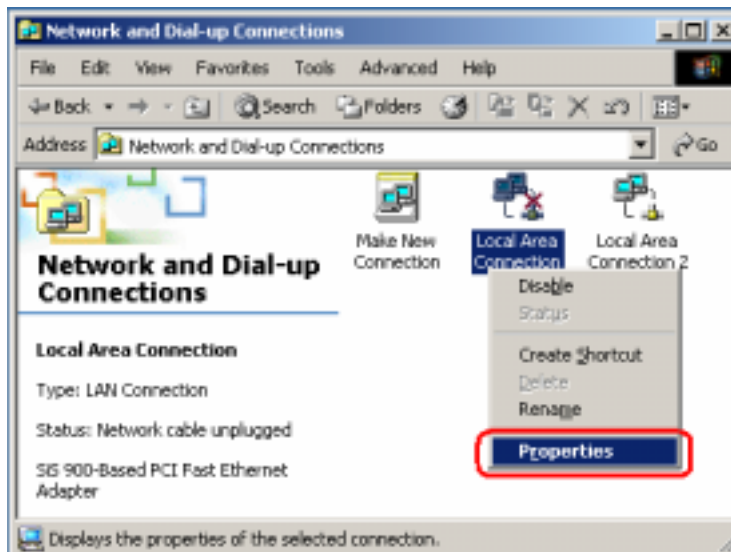
**Noise Strength:** Display noise signal strength.

**HT:** Display current HT Status in use, containing BW, GI, MCS, SNR0, and SNR1 value. (Show the information only for 802.11n wireless card)

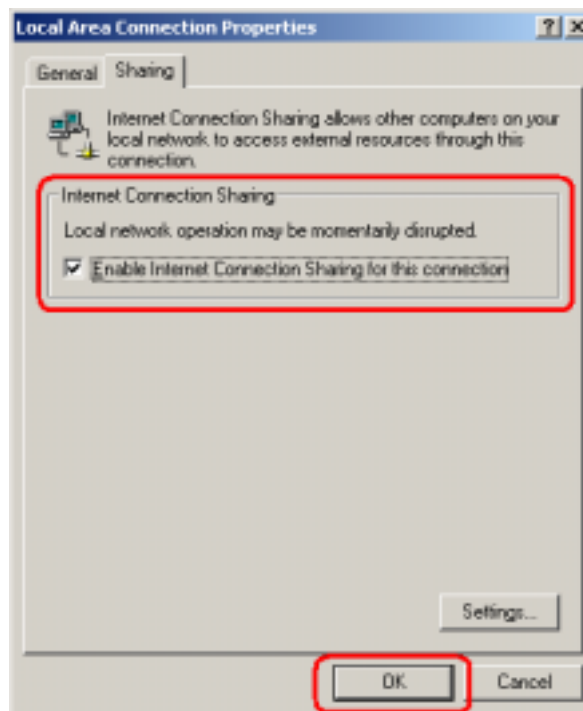
### 3.1.10 Enable AP Mode Feature in Windows 2000 OS

In Windows 2000 Operation System, the local network won't be automatically established while using Wireless PCI adapter's AP mode. Please follow the below steps to enable Internet Connection Sharing feature first before you switch Wireless PCI adapter's AP mode.

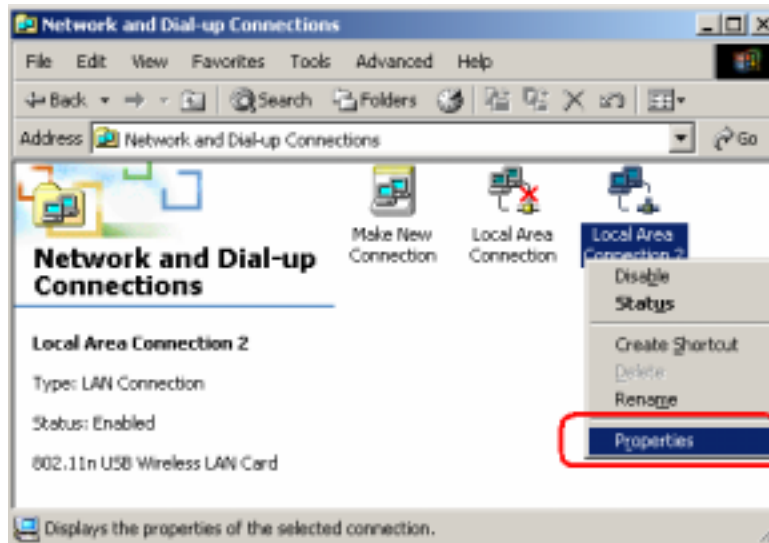
**Step 1:** After the Wireless PCI Adapter is installed properly in Windows 2000 Operation System, go to **Start → Settings → Control Panel → Choose “Network and Dial-up Connections”** option. Right-Click your local area connection (such as another LAN Card in the same computer), and choose **“Properties”**.



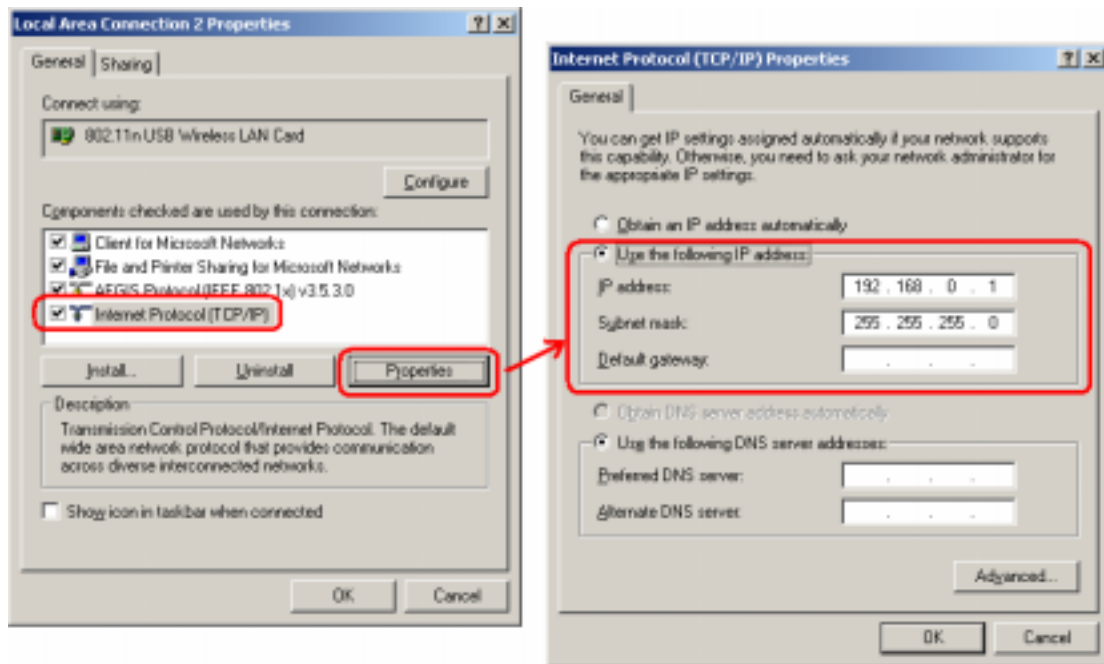
**Step 2:** In **Sharing** tab, enable **Internet Connection Sharing** for this connection and click **“OK”**



**Step 3:** Back to Network and Dial-up Connection screen, right-click “Local Area Connection 2” (for 802.11n Wireless LAN card) and choose “Properties”.



**Step 4:** Select “Internet Protocol (TCP/IP)” and click “Properties”. You will see 802.11n Wireless PCI adapter will be automatically assigned an IP address as Access Point.



**Step 5:** In the System tray, now you can switch 802.11n Wireless PCI Adapter to AP Mode.

