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]

Frames Transmitted Successfully: Frames successfully sent.

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

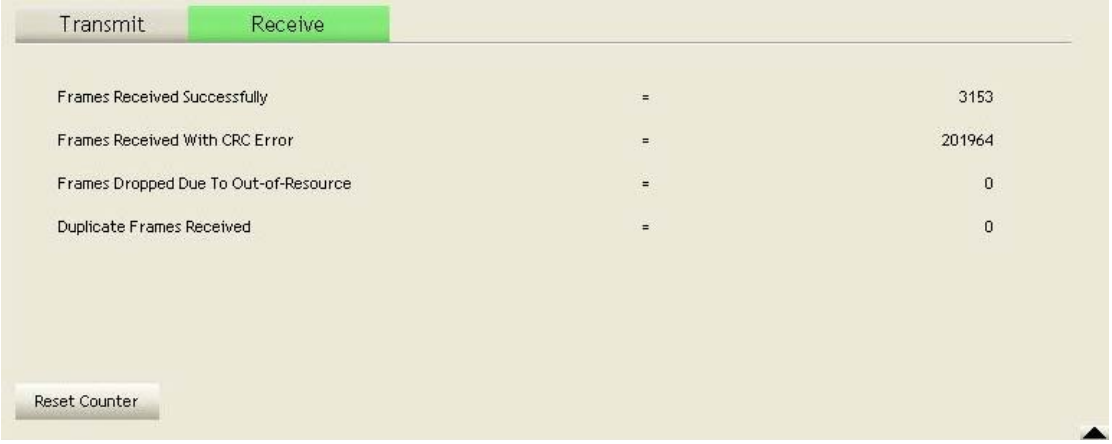
RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.

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]



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.

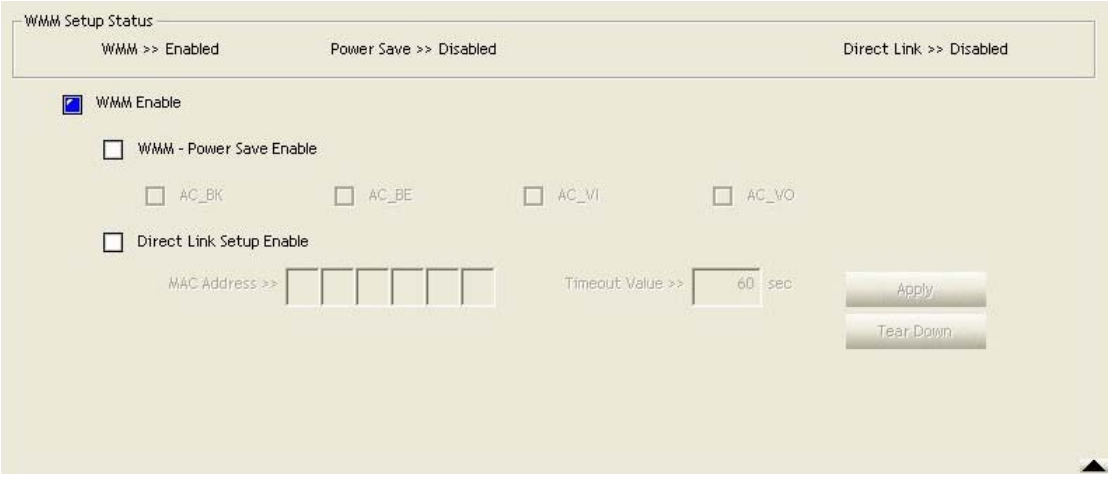
Reset Counter: Reset counters to zero

➔ 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: Enabe Wi-Fi Multi-Media.

WMM-Power Save Enable: Enable WMM Power Save.

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

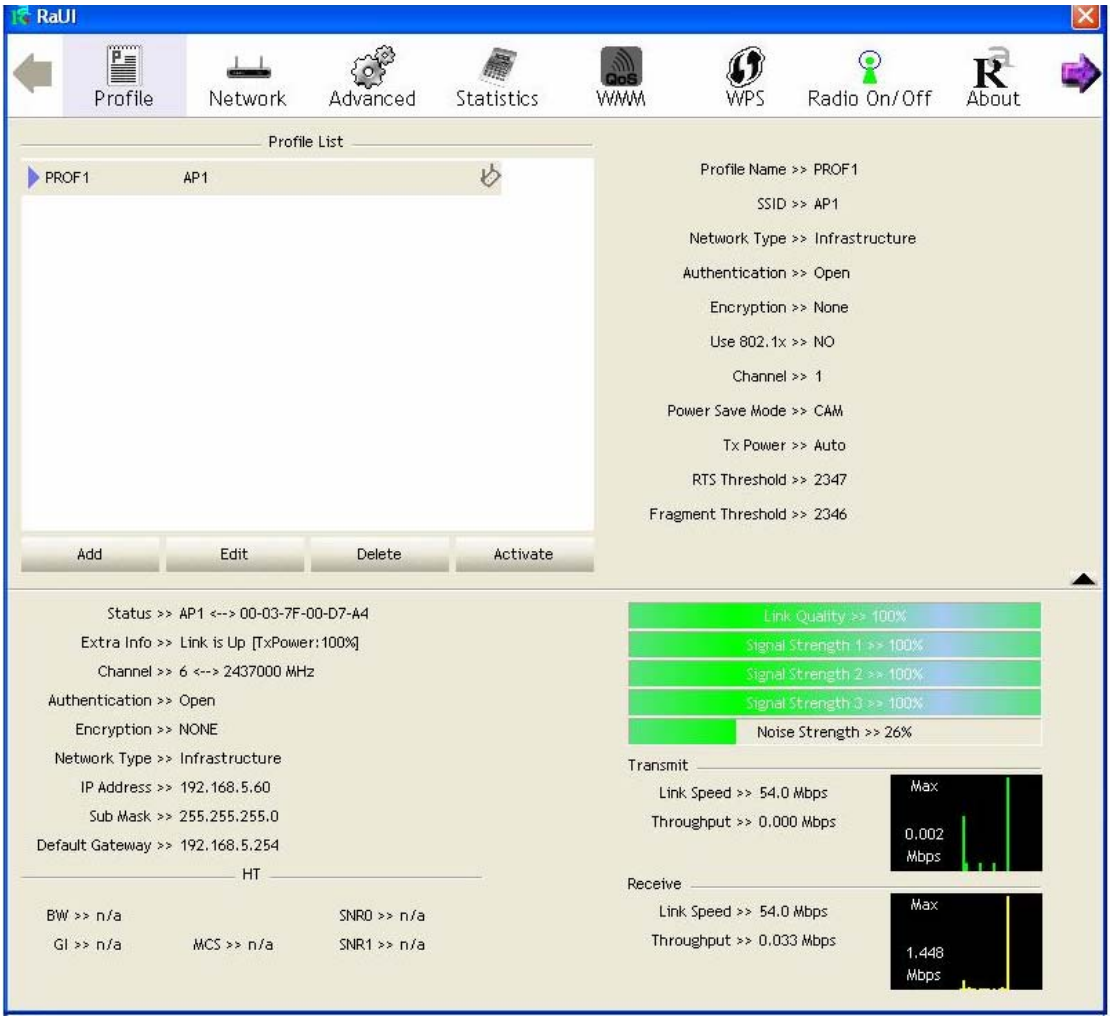
[WMM Enable – Enable Wi-Fi Multi-Media]

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:

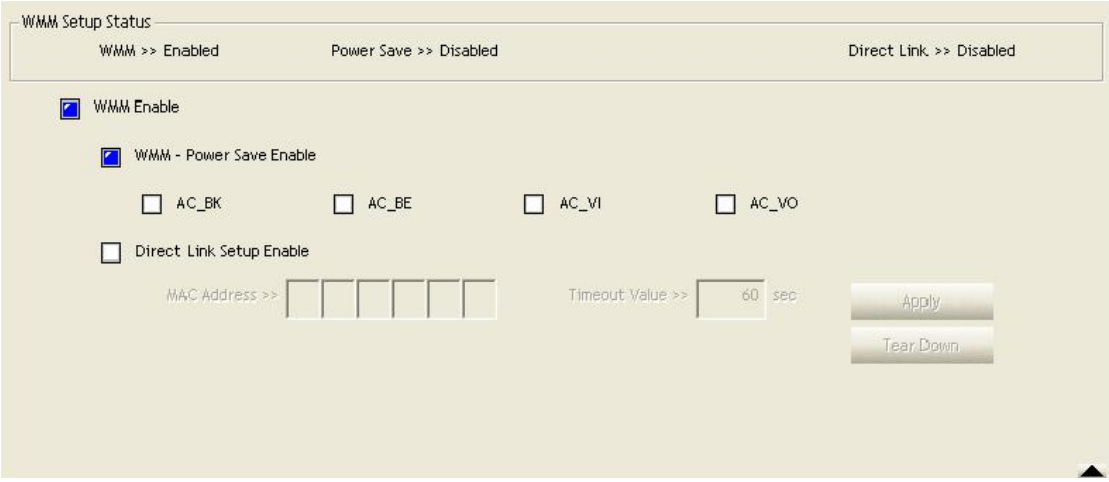
Step 1: Click "**WMM Enable**"

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.

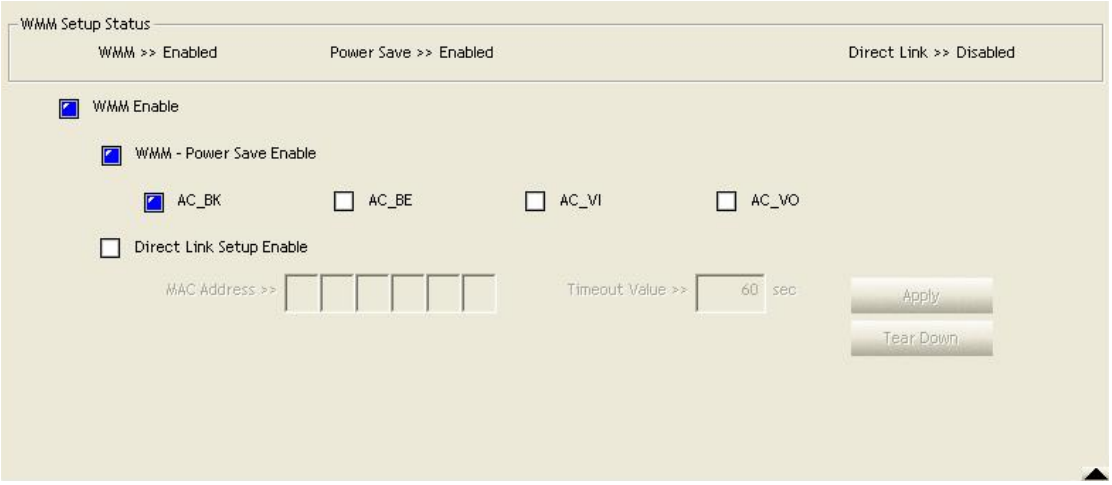


[WMM-Power Save Enable – Enable WMM Power Save]

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

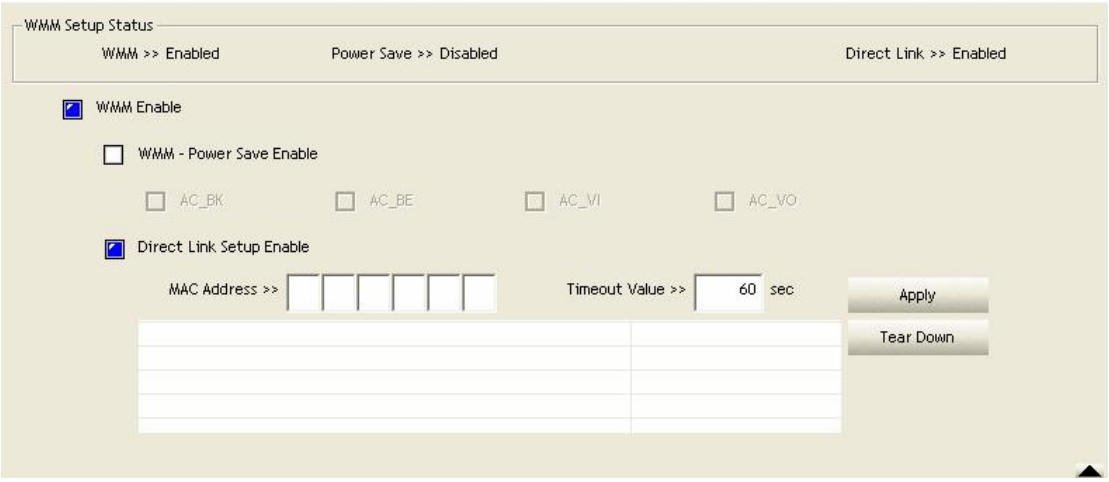


Step 2: Please select which ACs you want to enable. The setting of enabling WMM-Power Save is successfully.

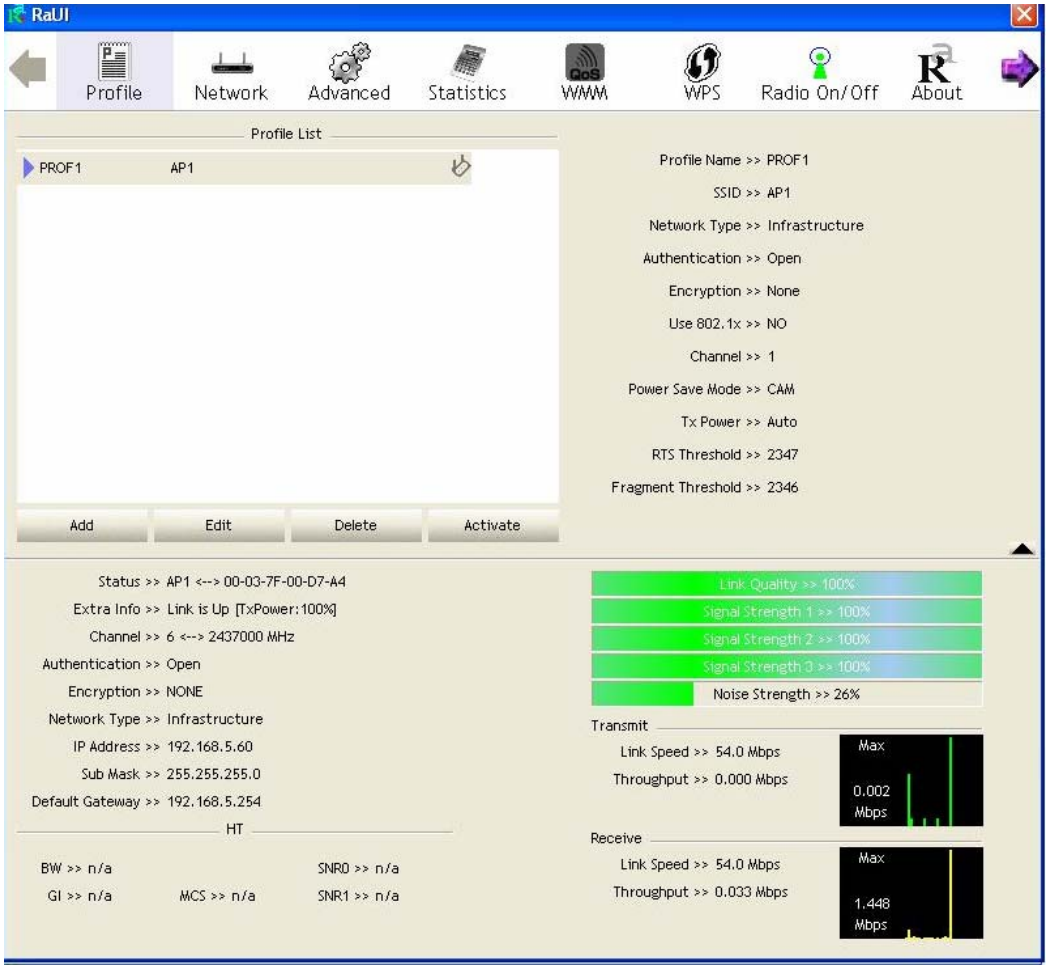


[Direct Link Setup Enable – Enable DLS (Direct Link Setup)]

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.

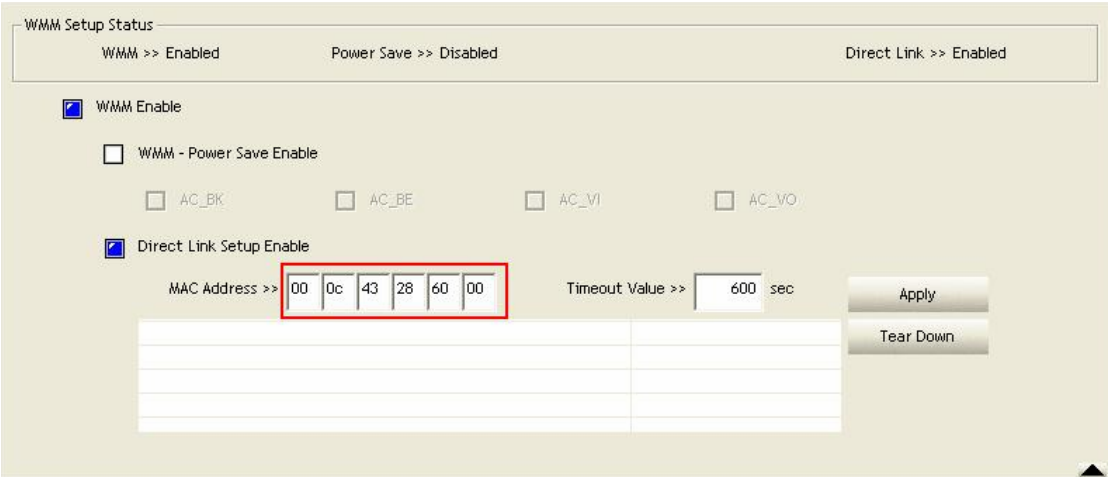


The Setting of DLS indicates as follow:

(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.

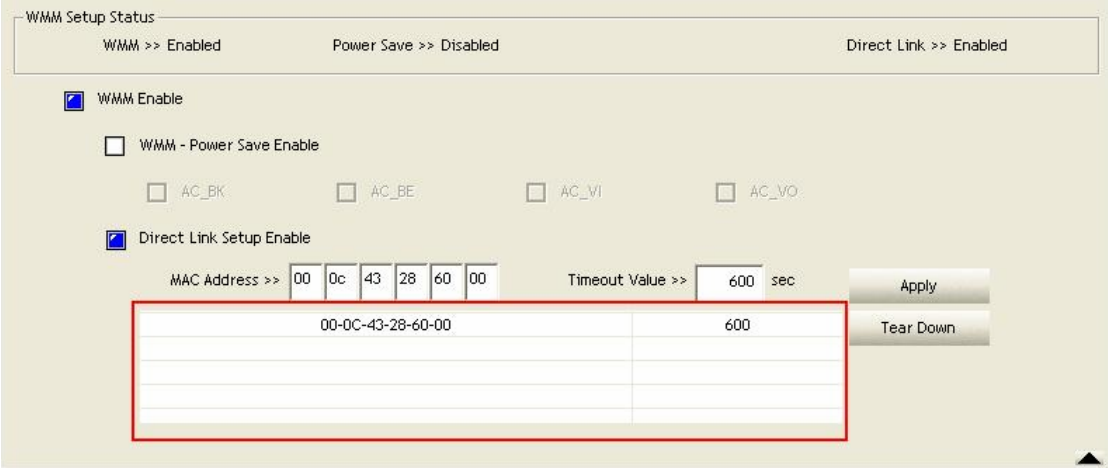
➔ Have to enable DLS



(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.

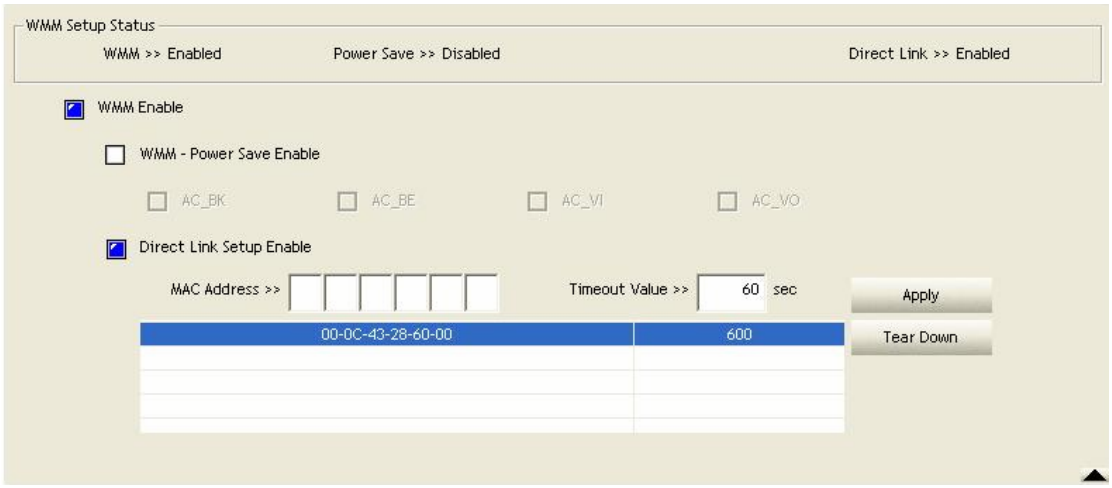


Describe "DLS Status" as follow:

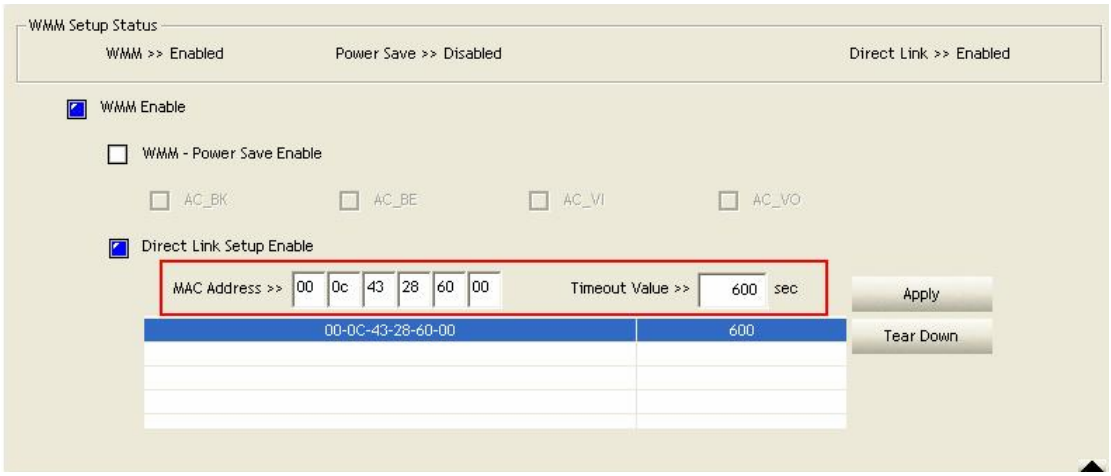
(1) As the up figure, after configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in "**DLS Status**". In "**DLS Status**" of the opposite side, it shows MAC address of itself and Timeout Value of setting.

(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**".

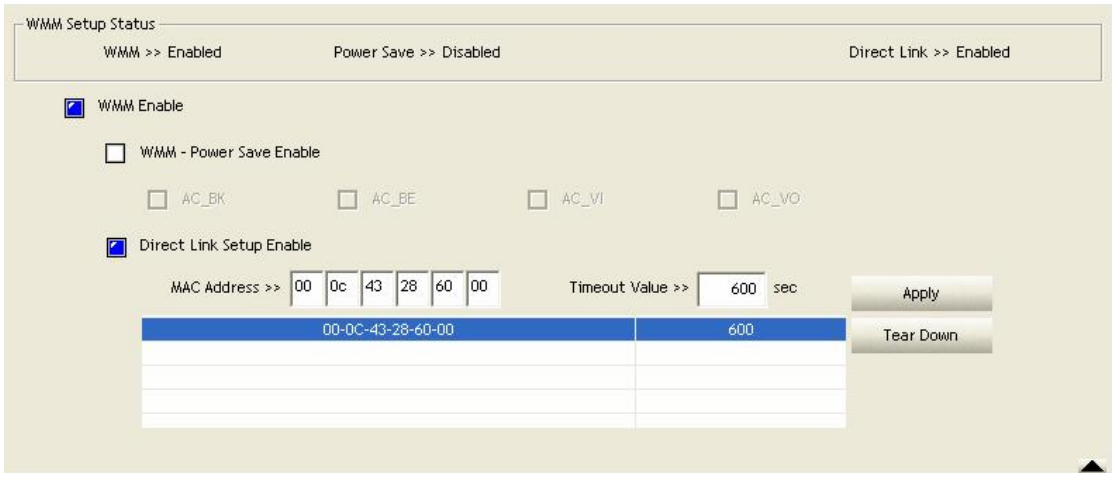


Step 2: Double-Click and the result will look like the below figure.



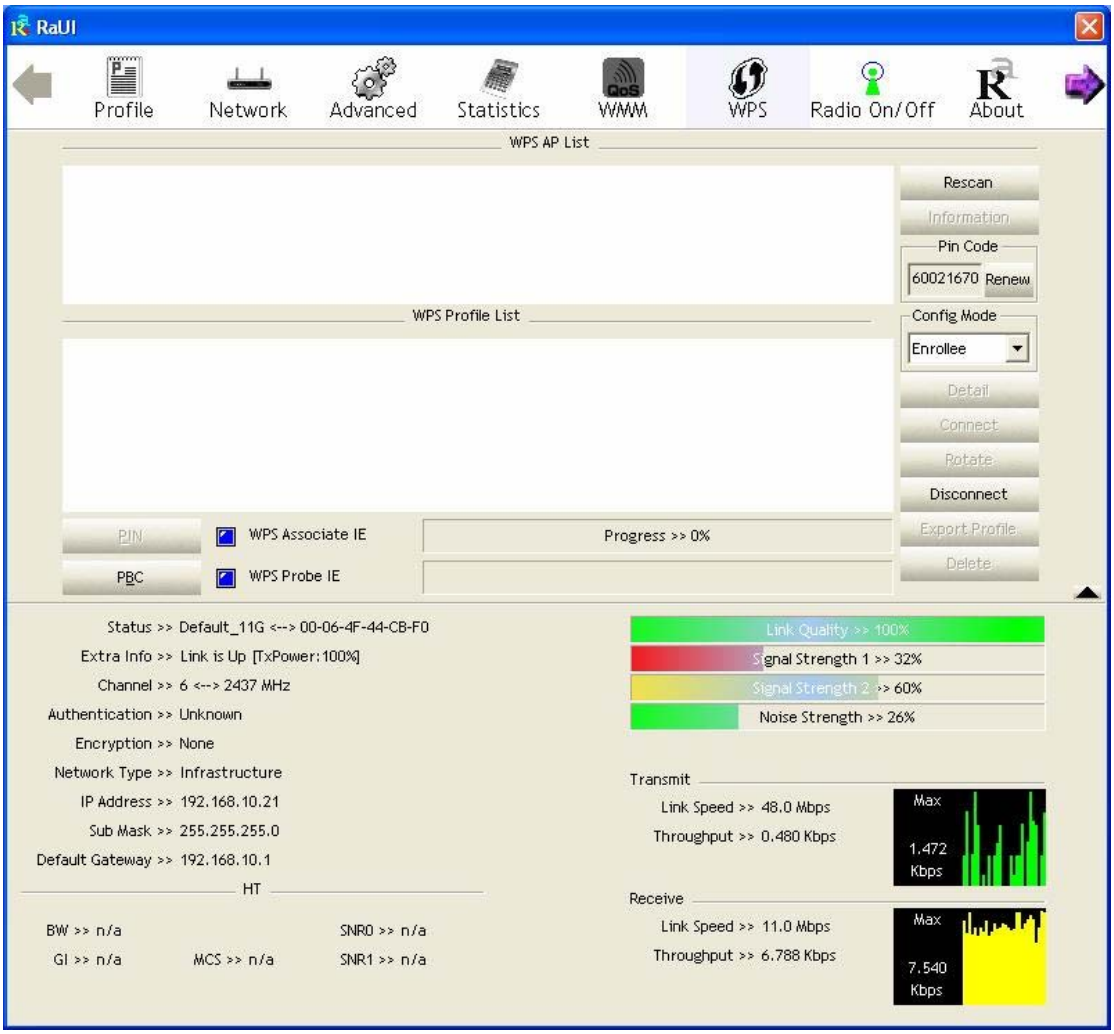
(3) Disconnect Direct Link Setup as follow:

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 simply 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.

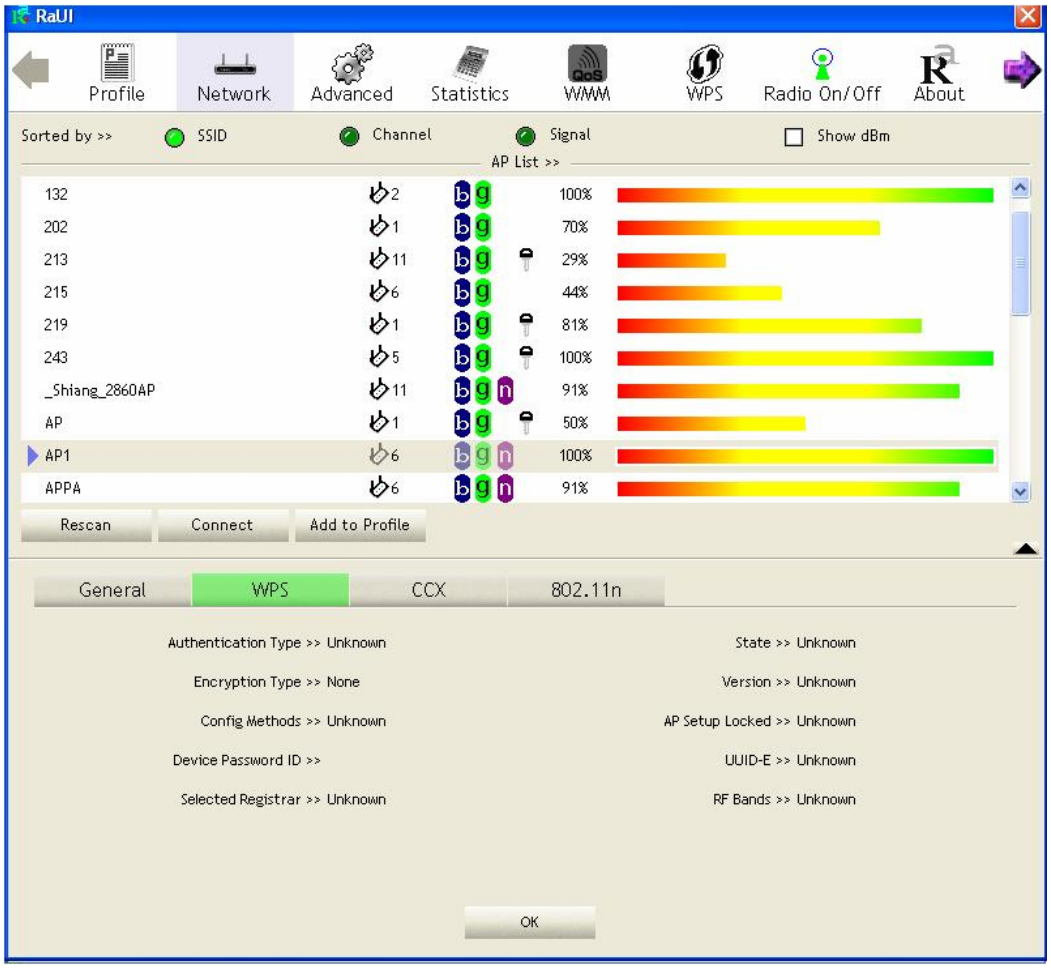
Status Bar: Display currently WPS Status.

[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.

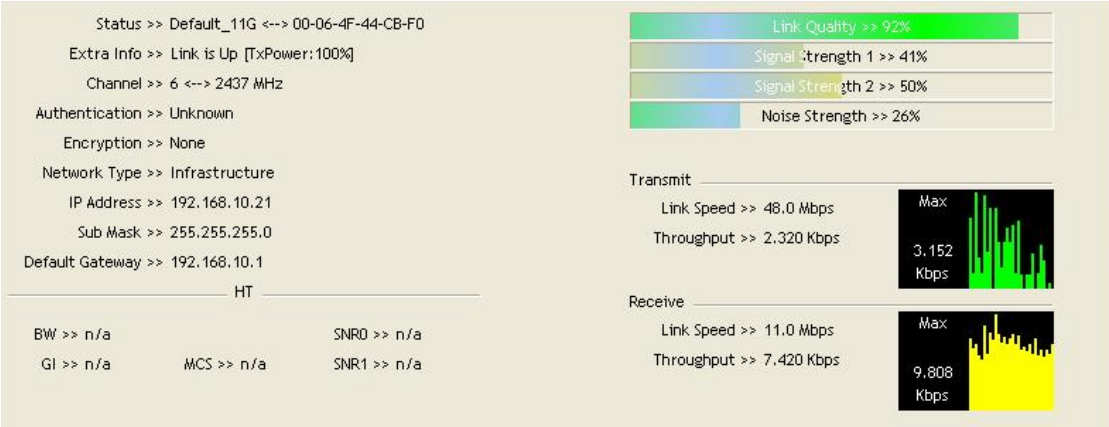
(1) Connect to Ralink's Website: WWW.RALINKTECH.COM

(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.

Throughout: 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.

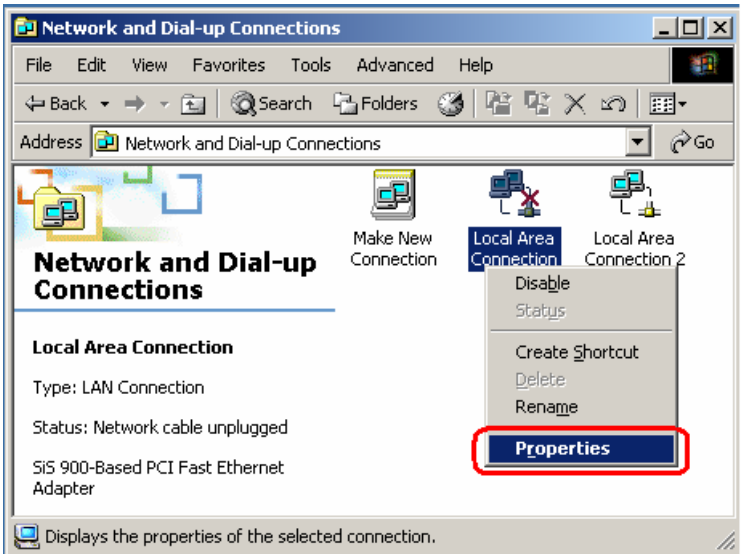
Noise Strength: Display noise signal strength.

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

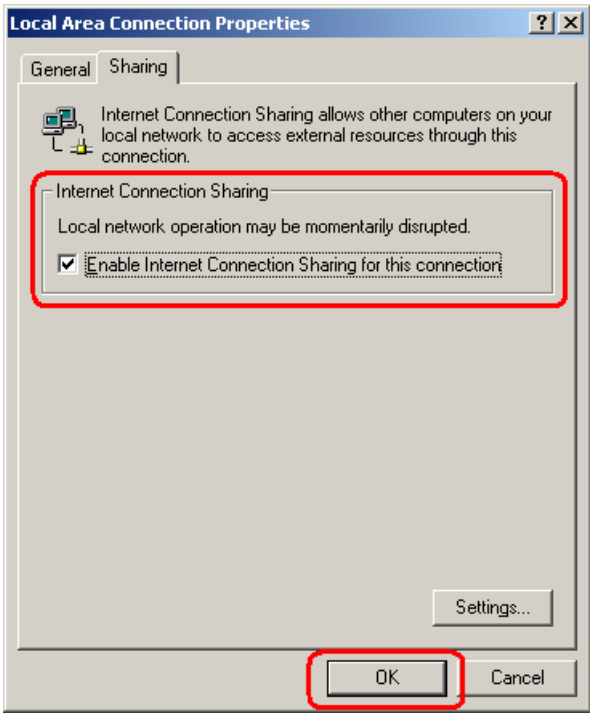
3.1.10 Enable AP Mode Feature in Windows 2000 OS

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.

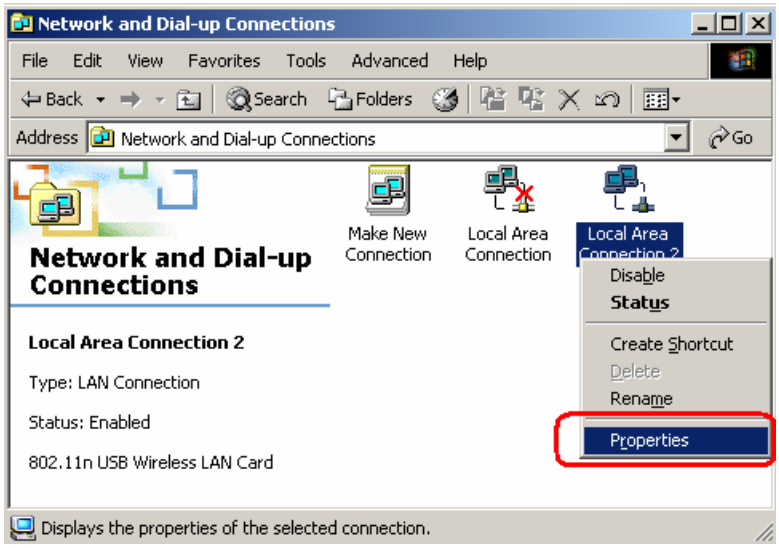
Step 1: After the Wireless PCI Adapter is installed properly in Windows 2000 Operation System, go to **Start ➔ Settings ➔ Control Panel ➔ Choose "Network and Dial-up Connections**" option. Right-Click your local area connection (such as another LAN Card in the same computer), and choose "**Properties**".



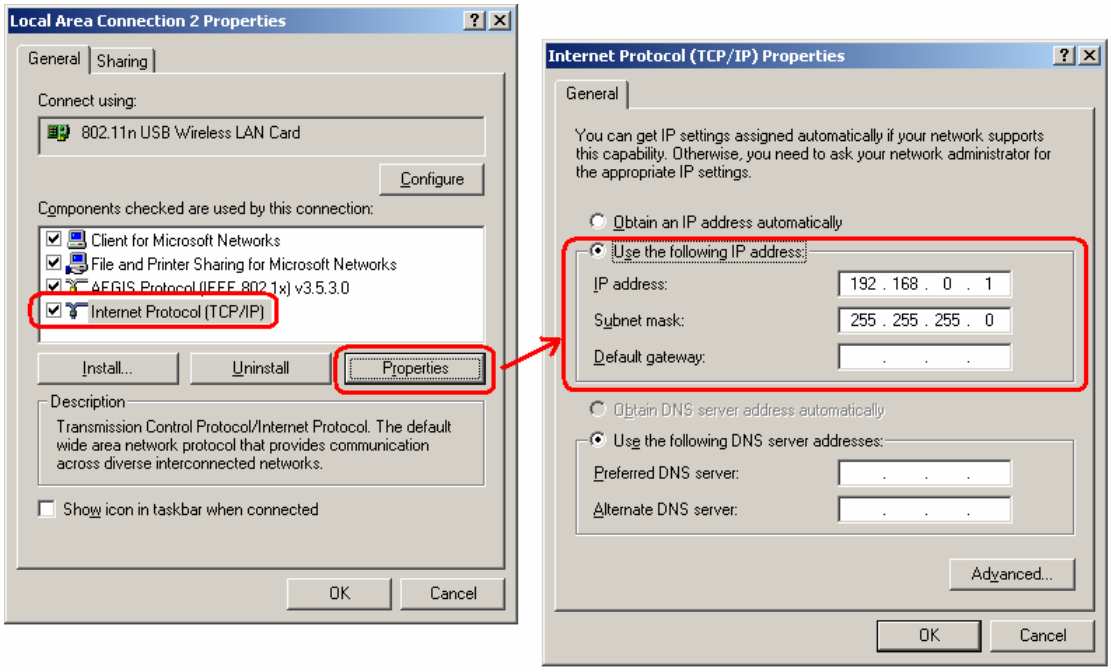
Step 2: In **Sharing** tab, enable **Internet Connection Sharing for this connection** and click "**OK**"



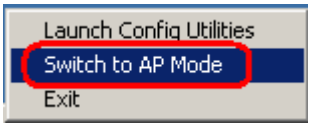
Step 3: Back to Network and Dial-up Connection screen, right-click "**Local Area Connection 2**" (for 802.11n Wireless LAN card) and choose "**Properties**".



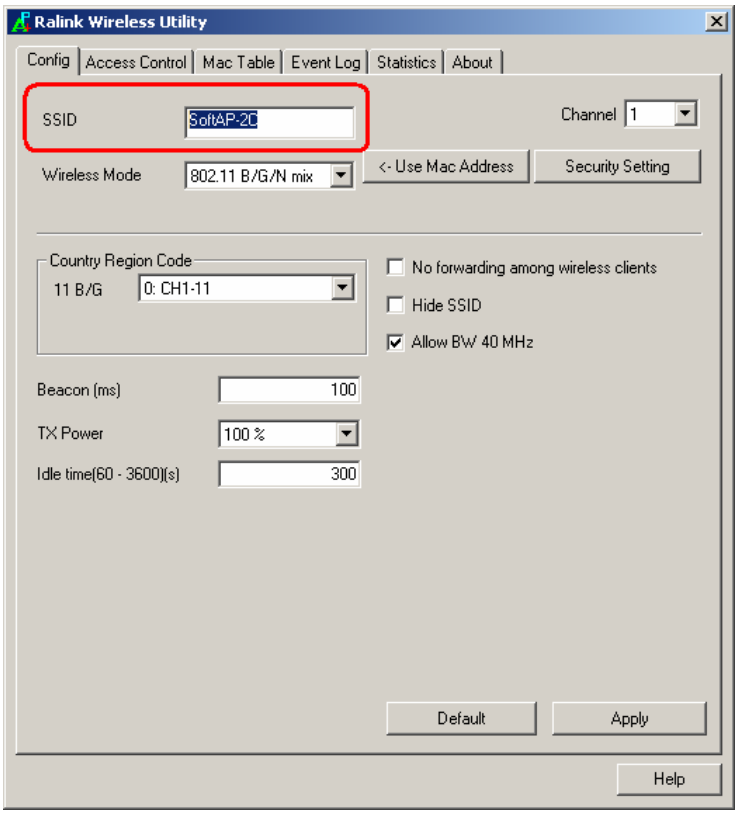
Step 4: Select "**Internet Protocol (TCP/IP)**" and click "**Properties**". You will see 802.11n Wireless PCI adapter will be automatically assigned an IP address as Access Point.



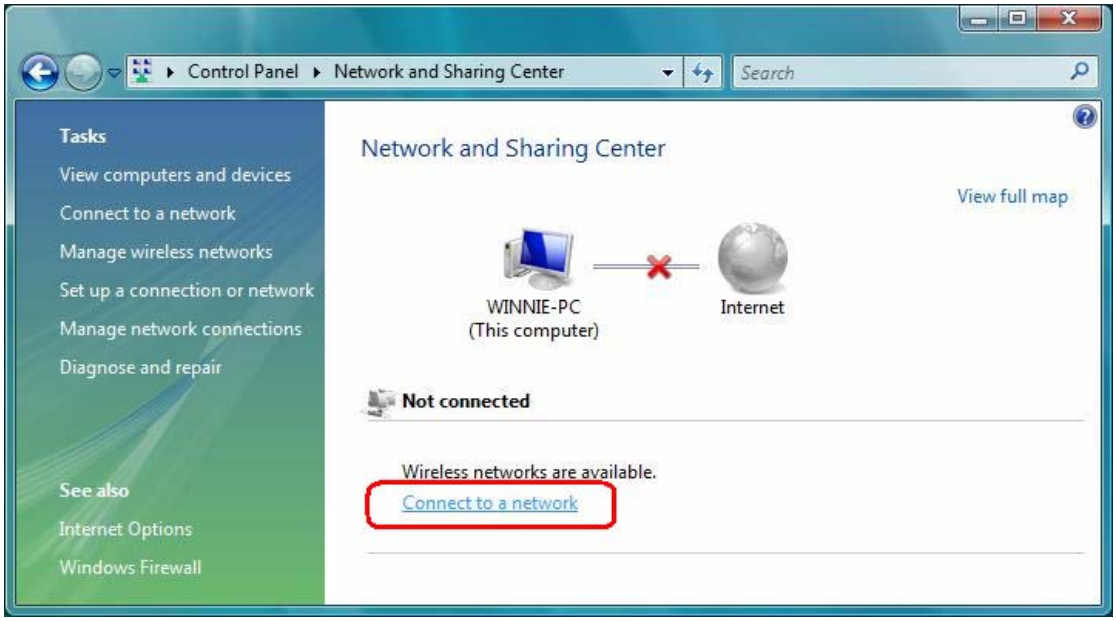
Step 5: In the System tray, now you can switch 802.11n Wireless PCI Adapter to AP Mode.



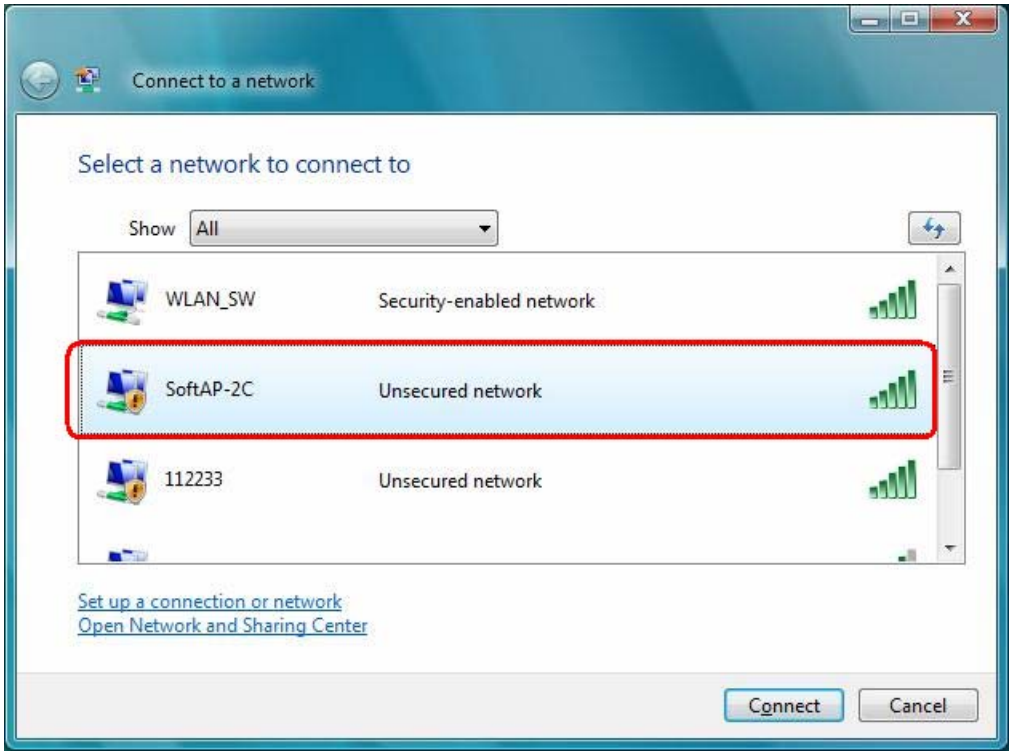
Step 6: After switch to AP mode, Ralink Wireless Utility will automatically pup-up. The Wireless Default SSID is assigned as "**SoftAP-2C**".



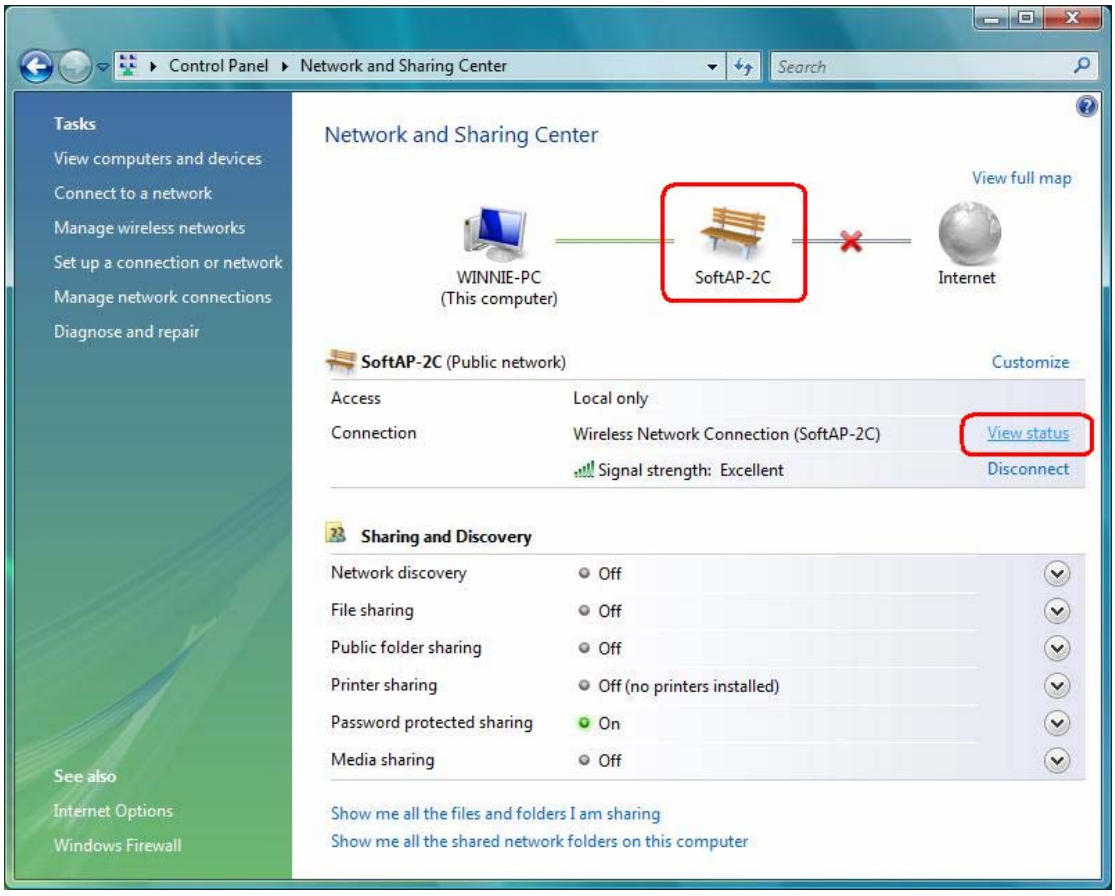
Step 7: To make sure your Soft AP is working properly, you need to use another computer which with Wireless LAN feature to access SoftAP-2C AP. In the below example, use another PC with Wireless feature in Vista Operation System. Go to **Start ➔ Control Panel ➔** Choose "**Network and Sharing Center**" option ➔ Click "**Connect to a network**" to search the available networks.



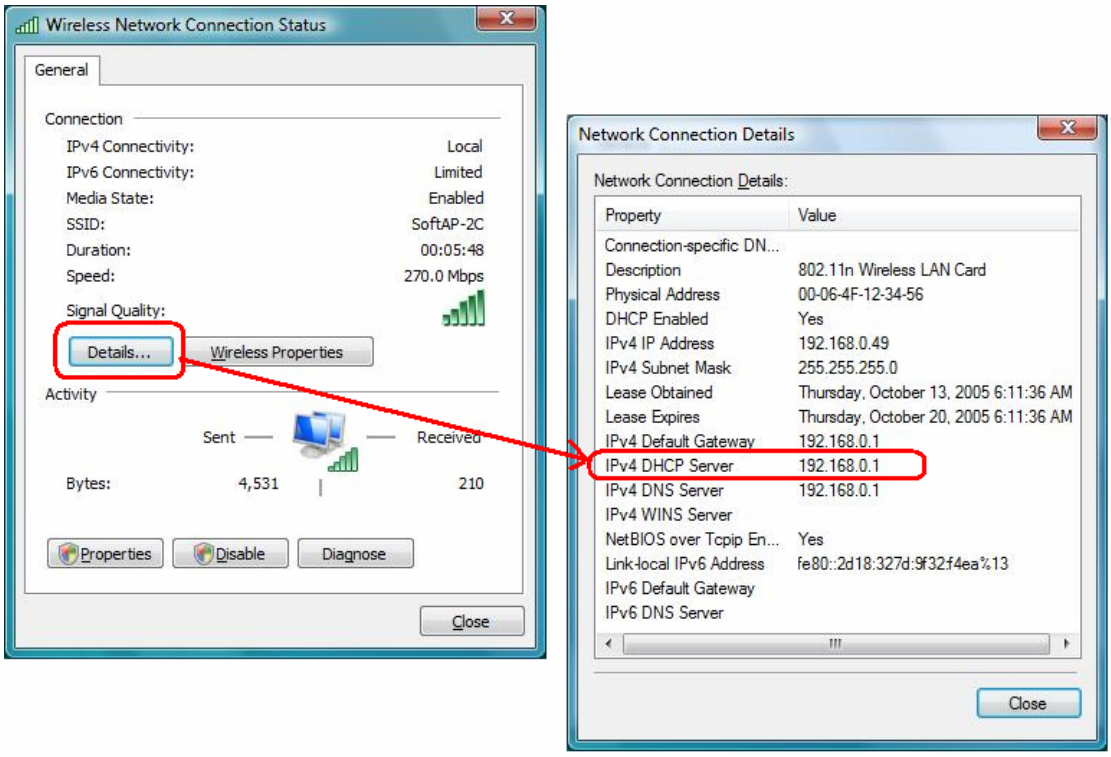
Step 8: Select the network "**SoftAP-2C**" and click "**Connect**" to establish the connection.



Step 9: After the computer is successful connected to SoftAP-2C, Network and Sharing Center screen will be shown as below. Click "**View Status**" to see the detail.

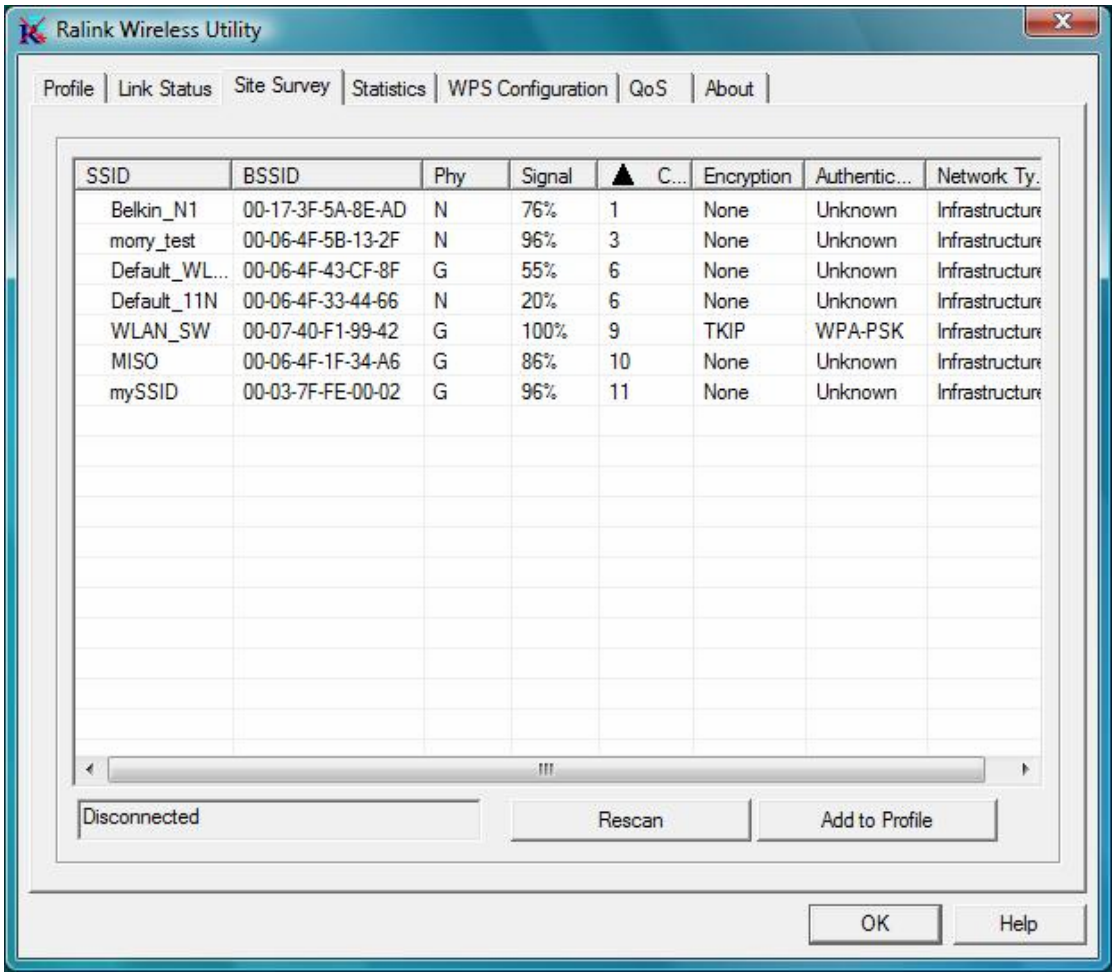


Step 10: In General tab, click "**Detail…**", and then you can see the current Network connection details. If this computer is successful connect to SoftAP-2C Access Point, the DHCP server will be assigned to same IP address.



3.2 For Windows Vista

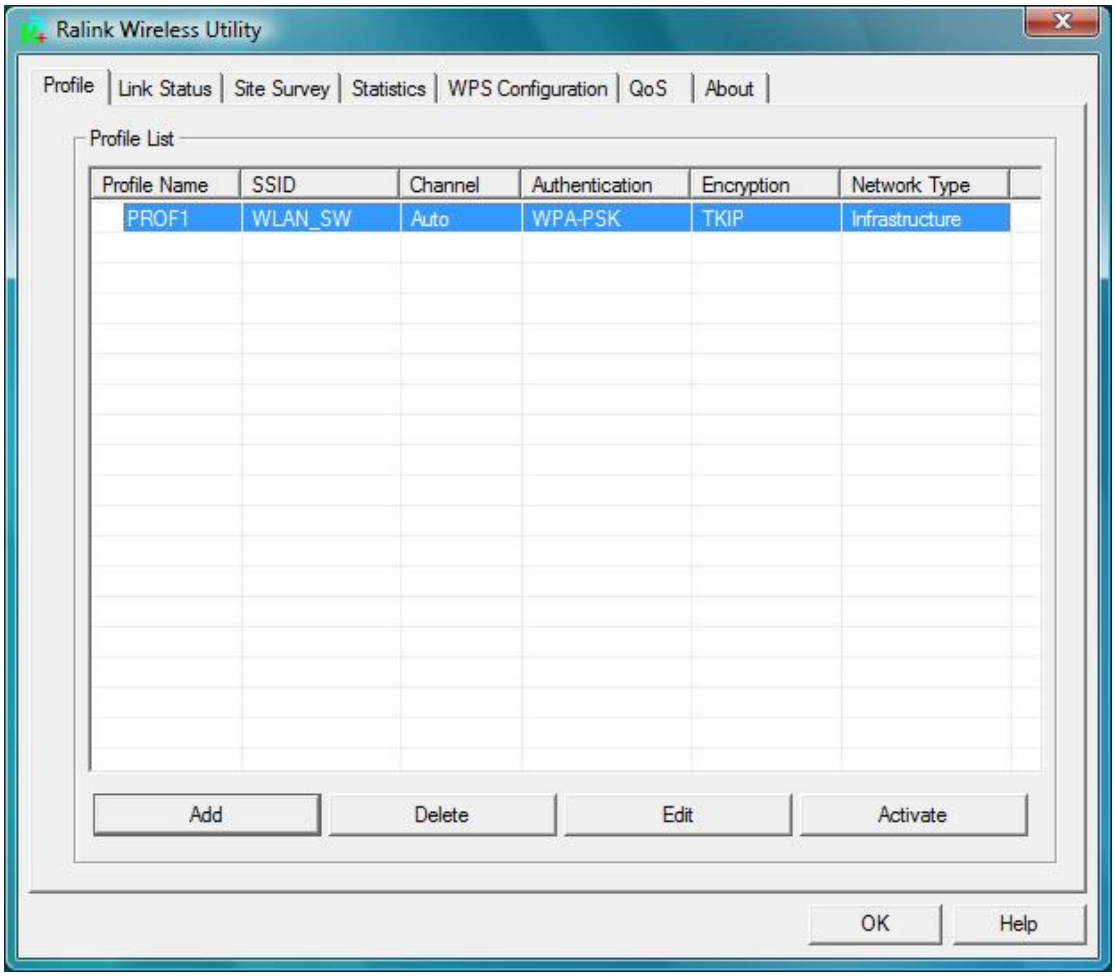
Ralink wireless utility is shown as below. There are 6 settings pages in Ralink wireless utility:



- **Profile** Page: Manage the profile.
- **Link Status** Page: Display current connection information.
- **Site Survey** Page: Display the available networks.
- **Statistics** Page: Display the packet counters
- **WPS Configuration** Page: Connect to WPS (Wi-Fi Protected Setup) capable APs.
- **QoS** Page: It involves “WMM Enable”, “WMM – Power Save Enable” and DLS setup
- **About** Page: Display Ralink driver and utility information.

3.2.1 Profile

In the **“Profile”**, you can view and manage the current using Available Point(s). You can **Add**, **Delete**, **Edit**, or **Activate** the current Available Point(s). Also you can duplicate the AP or set current AP as Default.



Profiles Name: The Profiles List displays all the profiles and the relative settings of the profiles including Profile Name, SSID, and Channel…etc; preset to **PROF*** (* indicate 1,2,3,…)

SSID: AP to Ad-hoc name.

Channel: Channel in use for Ad-Hoc mode.

Authentication: Authentication mode.

Encryption: Security algorithm in use.

Network Type: Network's type, including Infrastructure and Ad-hoc.

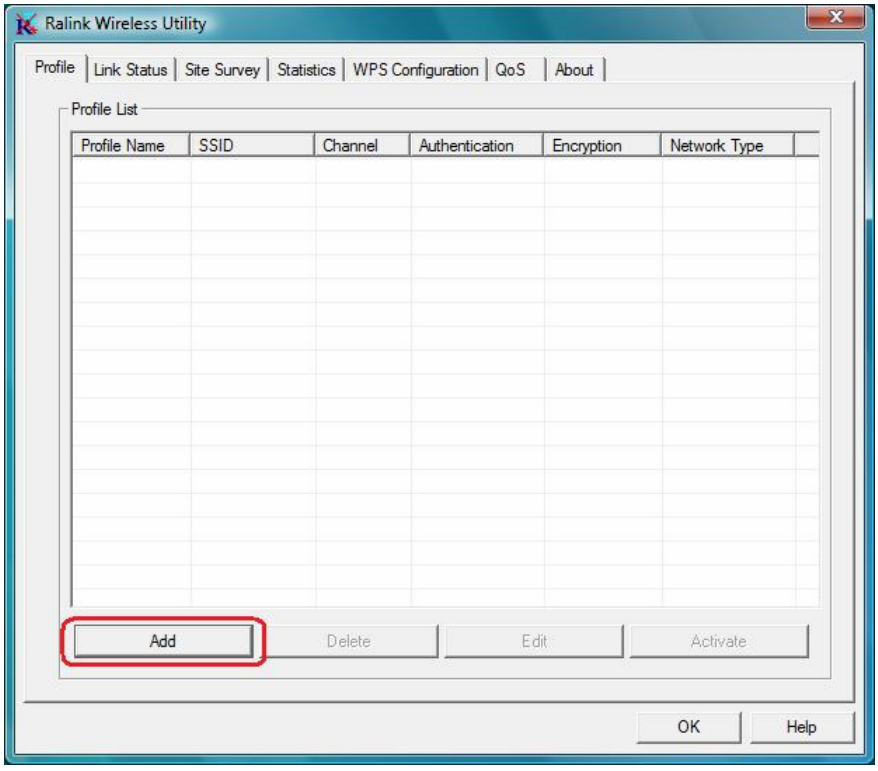
Indicate connection is successful on currently activated profile.

Indicate connection is failed on currently activate profile.

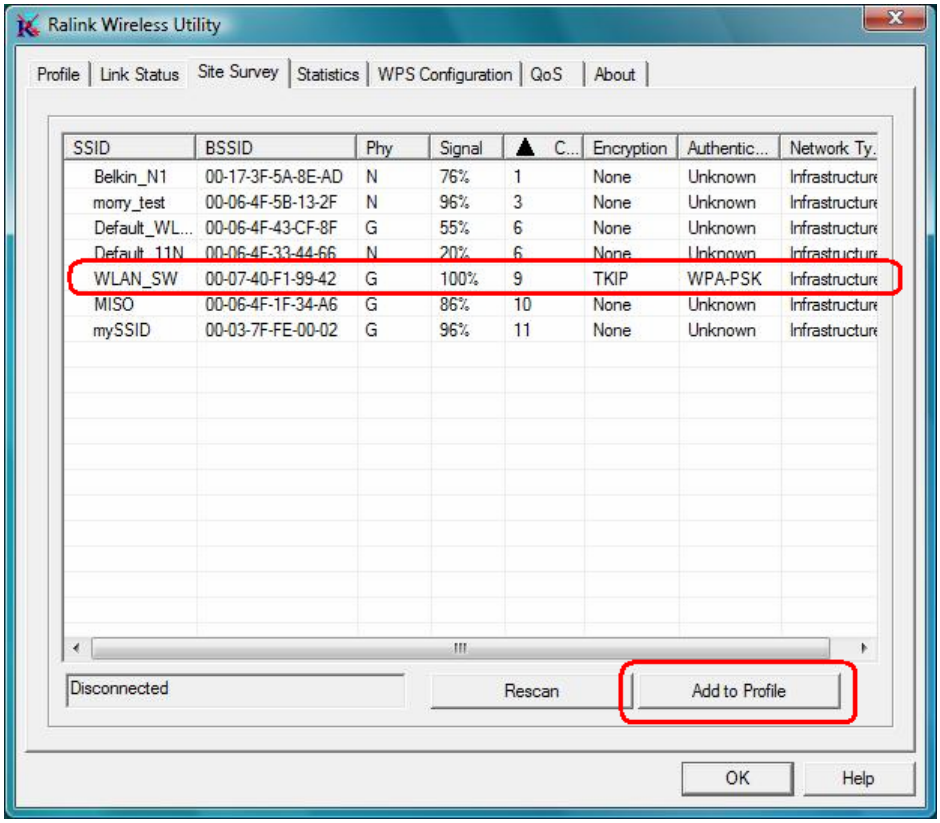
Add/Delete/Edit Button: Click these buttons to add/delete/edit the selected profiles.

Activate Button: Click **"Activate"** to connect the selected profile. When a profile is activated, the adapter will be initially connected to the profile.

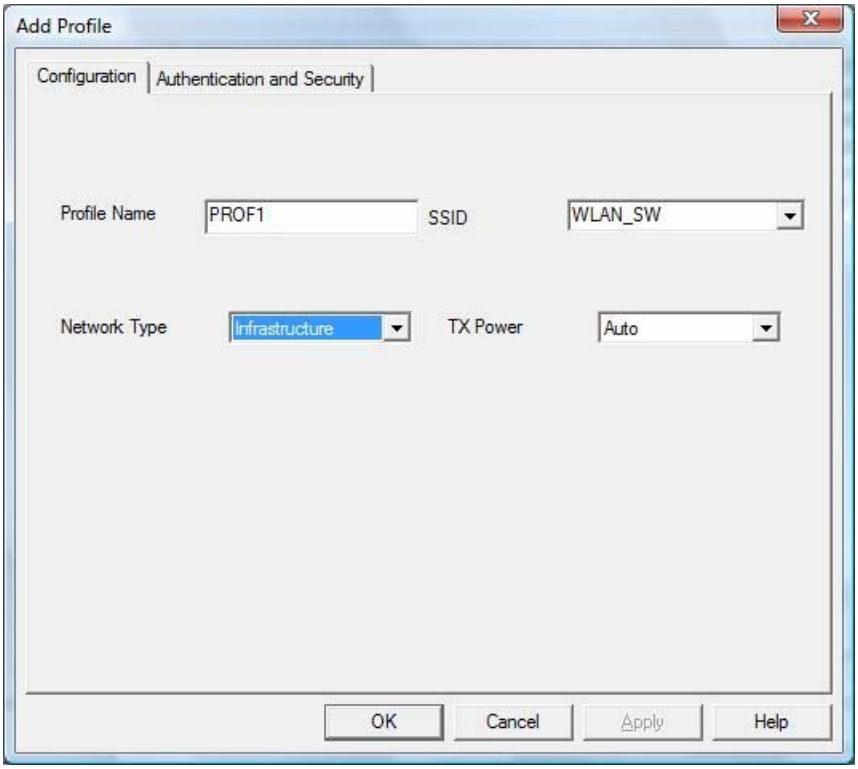
3.2.1.1 Add a profile



By either pushing the "**Add**" button on Profile Page or the "**Add to Profile**" button on Site Survey Page, it brings up the profile setting sheet which contains two setting pages -- "**Configuration**" page and "**Authentication and Security**" page.



[Configuration page]

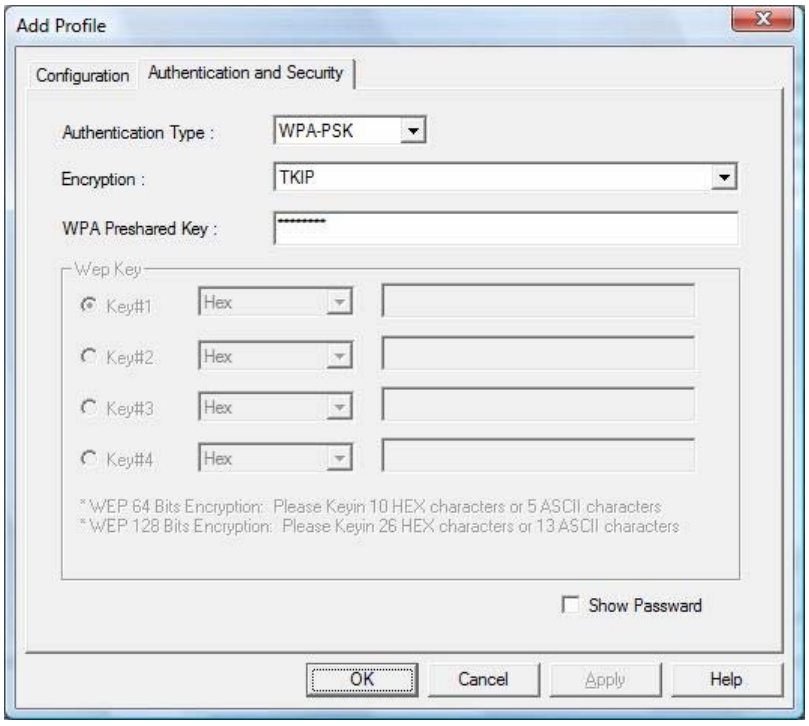


- Profile Name: Name of the profile
- SSID: Name of the desire network
- Network Type: Netowork of the desired network, either infrastructure or Ad-Hoc.

  Infrastructure – This operation mode requires the presence of a wireless Access Point. All communication is done via the Access Point or Router.

  Ad-Hoc – Select this mode if you want to connect to another wireless station in the Wireless LAN network without through an Access Point or Router.
- Tx-Power: The desired TX power level; the available options are 100%, 75%, 50% and Auto. If you want to lower the transmit power of the adapter for saving the power of the system, you can select the lower percentages from the list. The lower power will cause the lower signal strength and the coverage range.

[Authentication and Security page]



- **Authentication Type:** The authentication of the desired network. For infrastructure network, the available modes are Open, Shared, WPA, WPA-PSK, WPA2, and WPA2-PSK.

  Open: No authentication is needed among the wireless devices.

  Shared: Only Wireless device using a shared key (WEP Key identified) is allowed to connecting each other. Setup the same key as the wireless device that the adapter intends to connect.

  WPA: WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprise, small business and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

  WPA-PSK – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

WPA2 – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The different between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

WPA2-PSK – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).

- **Encryption:** The encryption of the desired network.

  -- For Open and Shared authentications, the available encryption modes are **None** and **WEP.**

  -- For WPA, WPA-PSK, WPA2 and WPA2-PSK authentications, the available modes are **TKIP** and **AES**.

  None – Disable the Encryption mode.

  WEP – Enabled the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Key Length & the key Index.

  TKIP – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10000 packets (a packet is a kind of message transmitted over a network). This insures much greater security than the standard WEP security.

  AES – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

  Note: All devices in the network should use the same encryption method to ensure the communication.

- **WPA Pre-Shared Key:** The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.

- **WEP Key (Key1~Key4):** The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit & 128-bit. Select the default encryption key form key1 to key4 by selected the radio button.

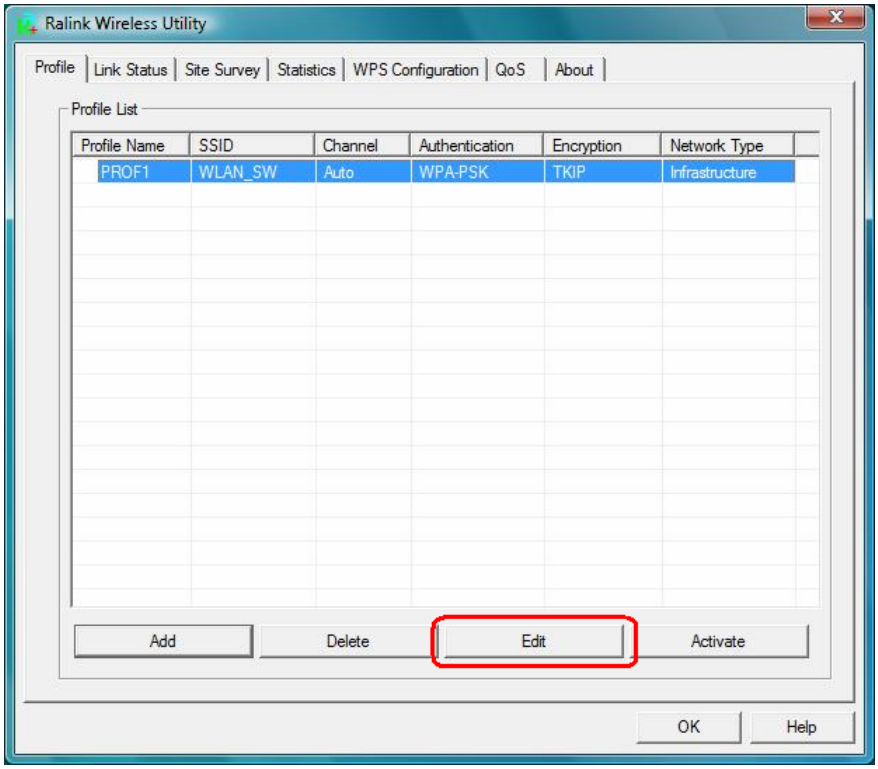
  Fill the text box by following the rule below:

  64-bit – Input 10-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 5-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**0123456aef**" or "**test1**"

  128-bit – Input 26-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 13-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**01234567890123456789abcdef**" or "**administrator**".

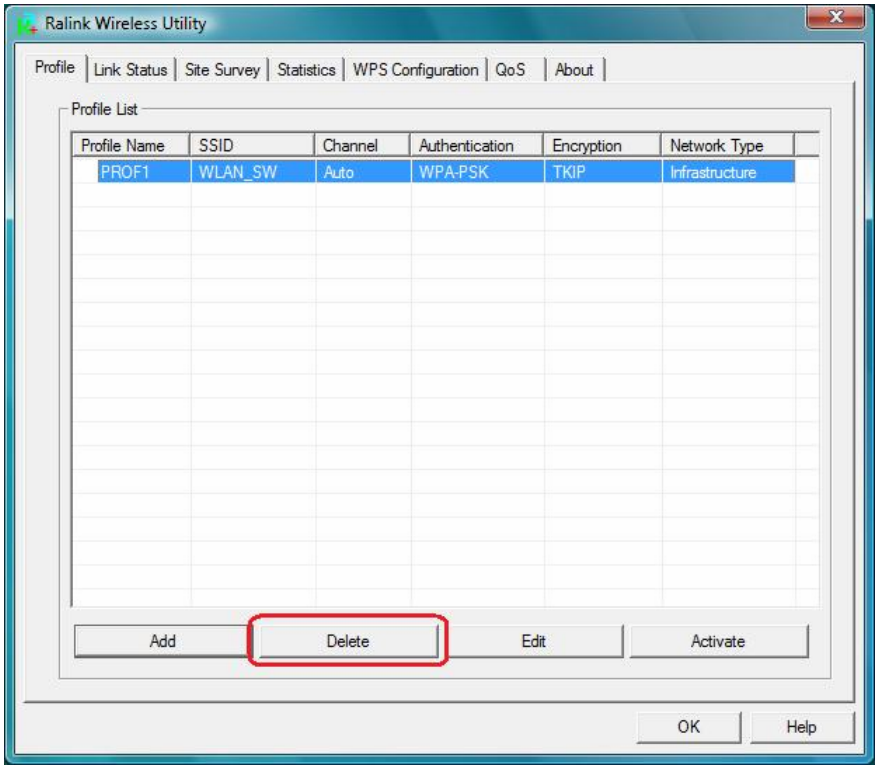
3.2.1.2 Edit a profile

Selecting an exiting profile then clicking the "**Edit**" button on Profile Page brings up the profile setting sheet filled with the profile information for user modification.



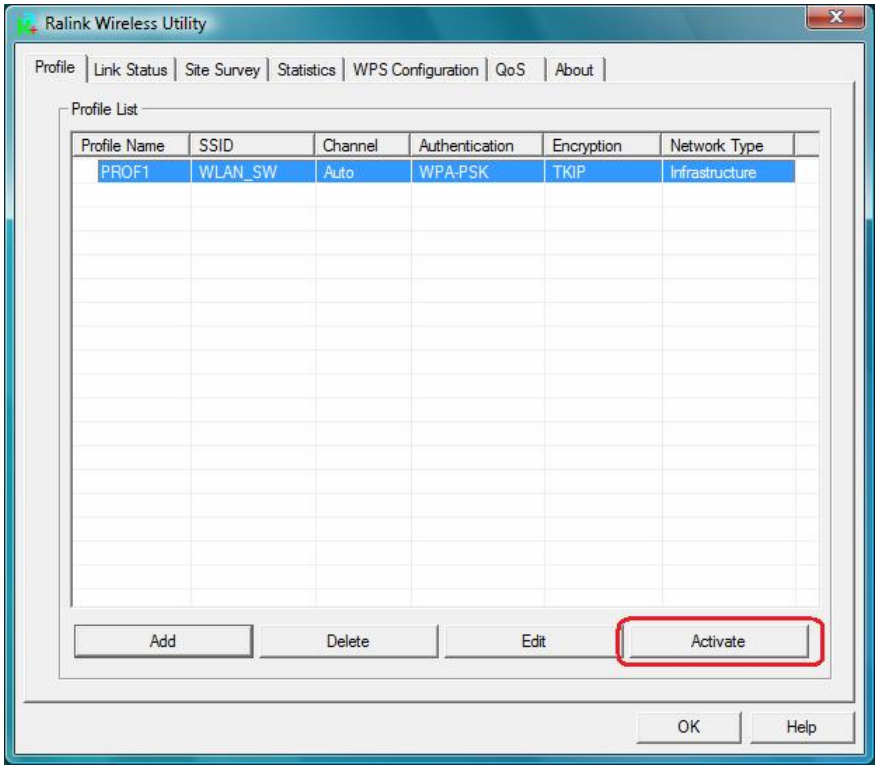
3.2.1.3 Delete a profile

Selecting an exiting profile then clicking the "Delete" button on Profile Page to deletes the profile.



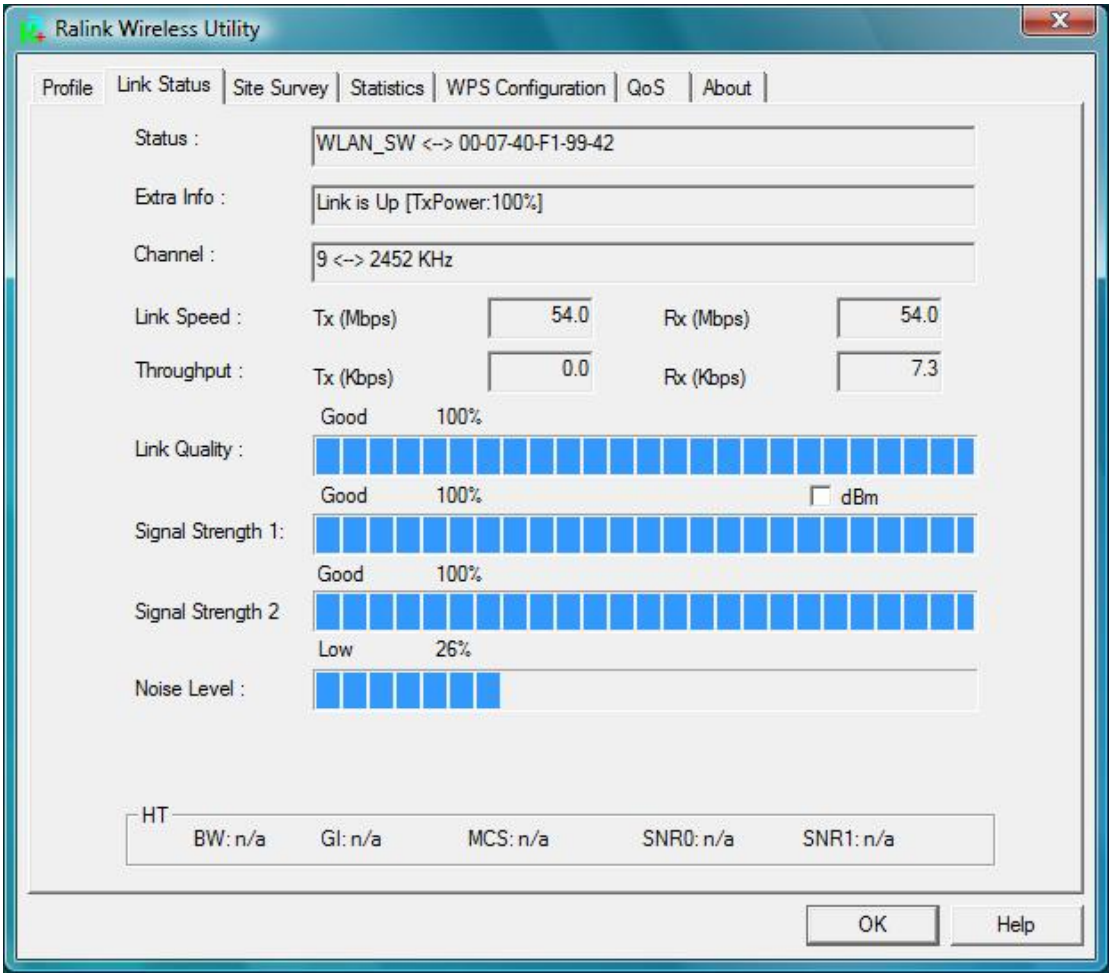
3.2.1.4 Active a profile

Selecting an exiting profile then clicking the “**Active**” button on Profile Page activates the profile.



3.2.2 Link Status

In this section, you can immediately monitor the current connected link status, such as Link Speed, Throughput, Link Quality, Signal Strength, Noise Level …etc.



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

Extra Info: Display the link status and current channel in use.

Channel: Display the number of the radio channel and the frequency used for the networking.

Link Speed (Mbps): Display the transmission and reception rate of the network. The maximum transmission rate is 54Mbps.

Throughput (Kbits/sec): Display transmits and receives throughout in unit of K bits/sec.

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

dBm: If you want to know the signal strength in the unit of dBm, select the check box.

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

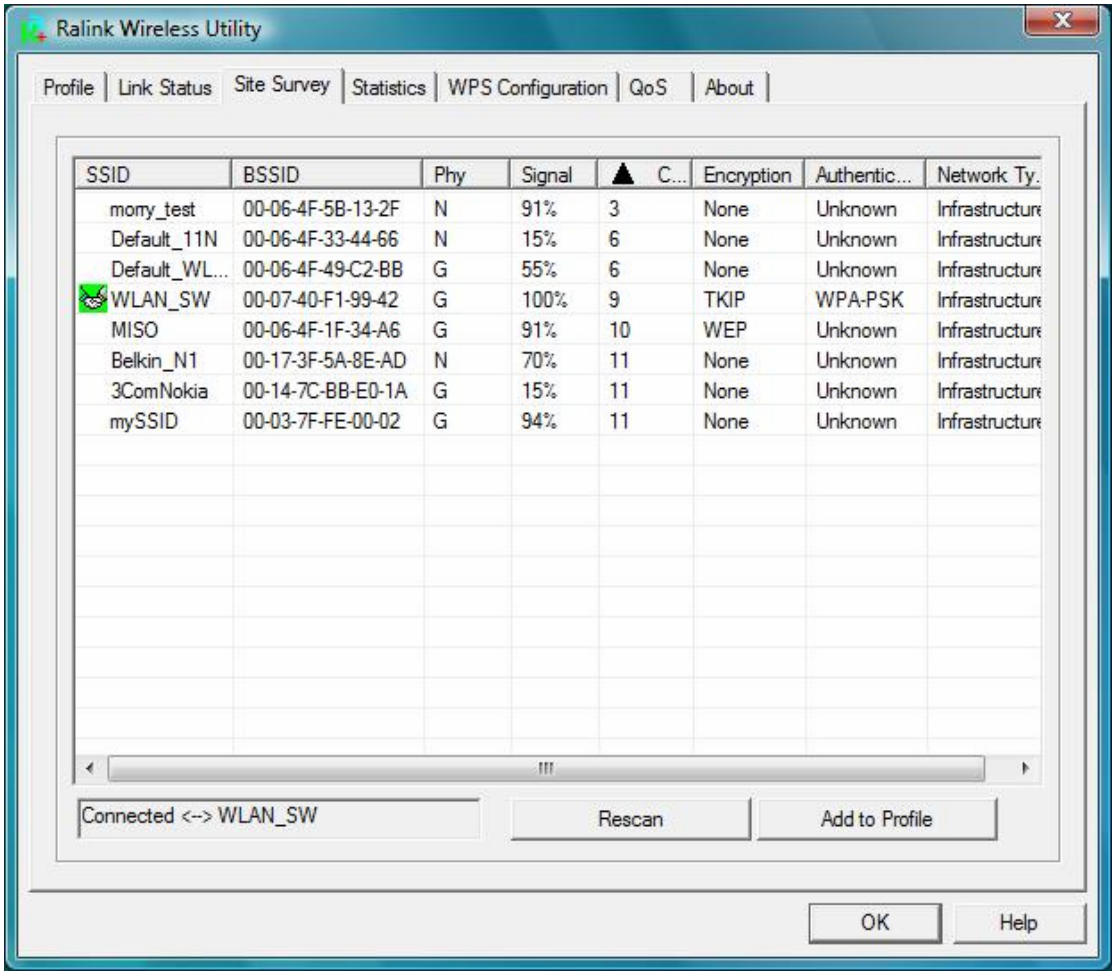
Signal Strength2: Receive signal strength 2, user can choose to display as percentage or dBm format.

Noise Level: Display the 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.)

3.2.3 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless device with the highest signal strength. From the **"Site Survey"**, all the network nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.



SSID: Name of BBS of IBSS network.

BSSID: MAC address of AP or randomly generated of IBSS.

Signal: Receive signal strength of specified network.

Channel: Channel in use.

Encryption: Encryption algorithm used within than BBS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.

Authentication: Authentication mode used within then network, including Unknown,

WPA-PSK, WPA2-PSK, WPA and WPA2.

Network Type: Network type in use, Infrastructure or Ad-Hoc.

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

Re-Scanning: Clicking the re-scan button to perform the re-scanning action.

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.

[Connect A Network]

(1) When Raconfig first ran, it will select the best AP to connect automatically.

(2) If user wants to connect to other AP, he can double-click mouse on the intended AP to make connection.

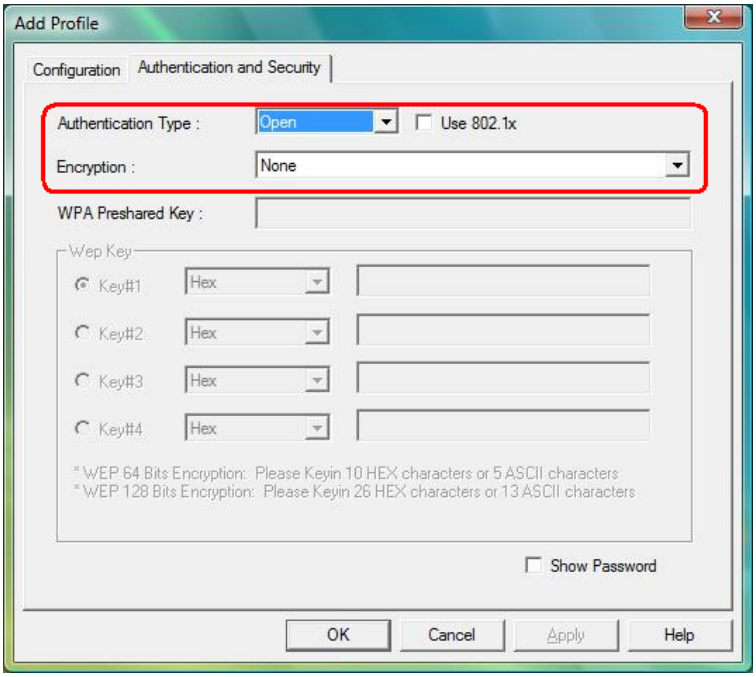
(3) If the intended network has encryption other than "Not Use", Raconfig will bring up the security page and let use input the appropriate information to make the connection.

This icon indicates the changes is successful.

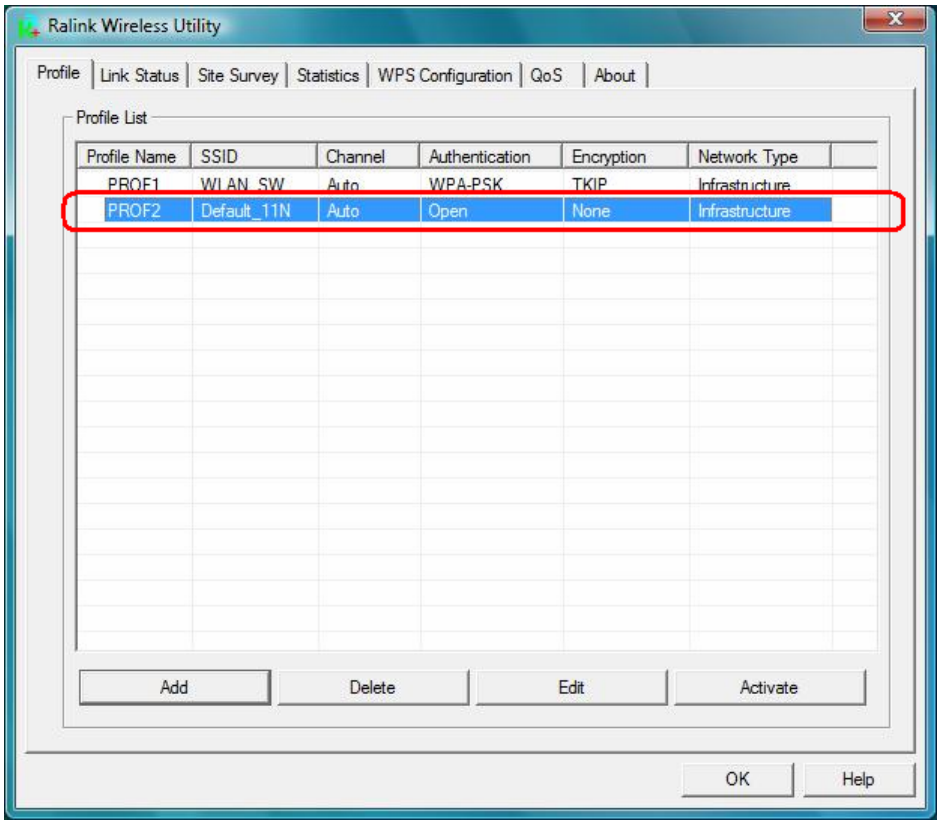
⊙Example 1: Open and Non-Encrypted

Step 1 – Choose "**Open**" authentication type

Step 2 – Choose "**None**" encryption type



Step 3 – After the profile is saved, click "**Activate**" button on Profile Page to activate the profile.



⊙ Example 2: WEP-Encrypted

Step 1 – Choose "**Open**" or "**Shared**" authentication type

Step 2 – Choose "**WEP**" encryption type

Step 3 –Enter the WEP KEY