



802.11n Wireless PCI-E Card

User Manual 1.0

© 2012

Table of Contents

| | | |
|-------|---|----|
| 1. | Introduction..... | 3 |
| 1.1 | Welcome..... | 3 |
| 1.2 | Contents of Package..... | 3 |
| 2. | Designing Your PCI Adapter..... | 3 |
| 3. | Installation..... | 3 |
| 3.1 | Install Your PCI Adapter..... | 3 |
| 3.2 | Install Driver and Utility..... | 4 |
| 4. | Windows Wireless Utility | 8 |
| 4.1 | Windows AutoConfig Service for Win 7 | 8 |
| 4.1.1 | Ralink Wireless Utility and Windows AutoConfig Service..... | 8 |
| 4.1.2 | Windows AutoConfig Service | 9 |
| 5. | Ralink Wireless Utility (RaUI) | 17 |
| 5.1 | Start..... | 17 |
| 5.1.1 | Start RaUI | 17 |
| 5.2 | Profile..... | 20 |
| 5.2.1 | Profile..... | 20 |
| 5.2.2 | Add/Edit Profile | 21 |
| 5.2.3 | Pre-logon Connect | 24 |
| 5.3 | Network..... | 24 |
| 5.3.1 | Network..... | 24 |
| 5.4 | Advanced | 27 |
| 5.4.1 | Advanced | 27 |
| 5.4.2 | Certificate Management..... | 28 |
| 5.5 | Link Information..... | 28 |
| 5.5.1 | Link Status | 28 |
| 5.5.2 | Throughput..... | 29 |
| 5.5.3 | Statistics | 29 |
| 5.6 | About..... | 30 |
| 5.6.1 | About..... | 30 |
| 5.7 | WPS | 31 |
| 5.7.1 | WPS | 31 |
| 6. | Security | 33 |
| 6.1 | Auth.\ Encry. Setting – WEP/TKIP/AES..... | 33 |
| 6.2 | 802.1x Setting | 34 |
| 7. | Trouble Shooting..... | 38 |

1. Introduction

1.1 Welcome

PCI Adapter connects you with IEEE802.11n networks at receiving rate up to an incredible 300Mbps!

By using the reflection signal, 802.11n technology increases the range and reduces "dead spots" in the wireless coverage area.

Unlike ordinary wireless networking of 802.11b/g standards that are confused by wireless reflections,

802.11n can actually use these reflections to increase four times transmission range of 802.11g products.

Besides, when both ends of the wireless link are 802.11n products, The PCI can utilize twice radio band to increase three times transmission speed of ordinary 802.11g standard products, and can comply with backwards 802.11b/802.11g standards.

Soft AP supported by PCI Adapter can help you establish wireless LAN networking with lowest cost.

Besides, WPS (PBC and PIN) encryption method can free you from remembering the long passwords.

Complete WMM function makes your voice and video more smooth.

1.2 Contents of Package

- One PCI Card
- One Installation CD
- Detachable 2 dBi antenna

Contact your local authorized reseller or the store purchased from for any items damaged and/or missing.

2. Designing Your PCI Adapter

The status LED indicators of PCI Card are described in the following.

- Lnk/Act ON (Green): Indicates a valid connection.
- Lnk/Act Flashing: Indicates the Adapter is transmitting or receiving data.

3. Installation

3.1 Install Your PCI Adapter

✓ Open your PC case and locate an available PCI on the motherboard.

Slide PCI Adapter into the PCI slot. Make sure that all of its pins are touching the slot's contacts. You may have to apply a bit of pressure to slide PCI Adapter all the way in. after it is firmly in place, secure its fastening tab to your PC's chassis with a mounting screw. Then close your PC.

Attach the external antennas to PCI Adapter's antenna port.

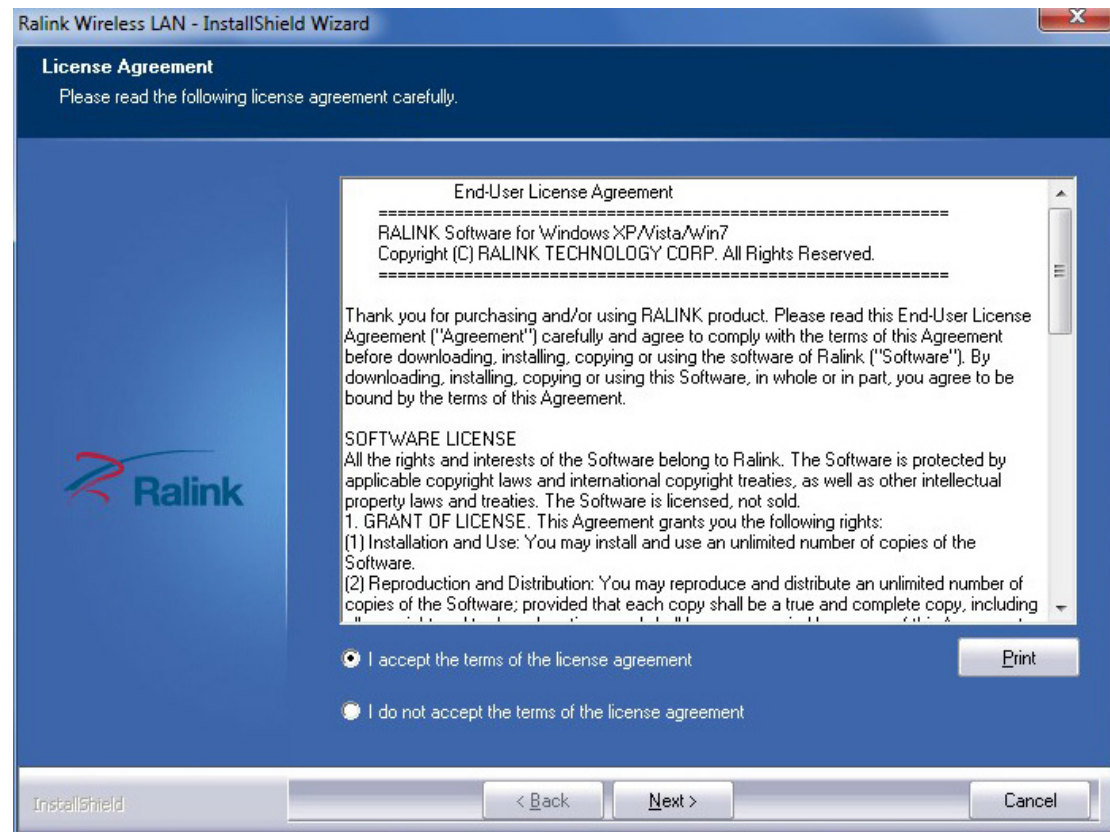
Power on the PC.

Note: Select **Cancel** when "Found New Hardware" window appears.

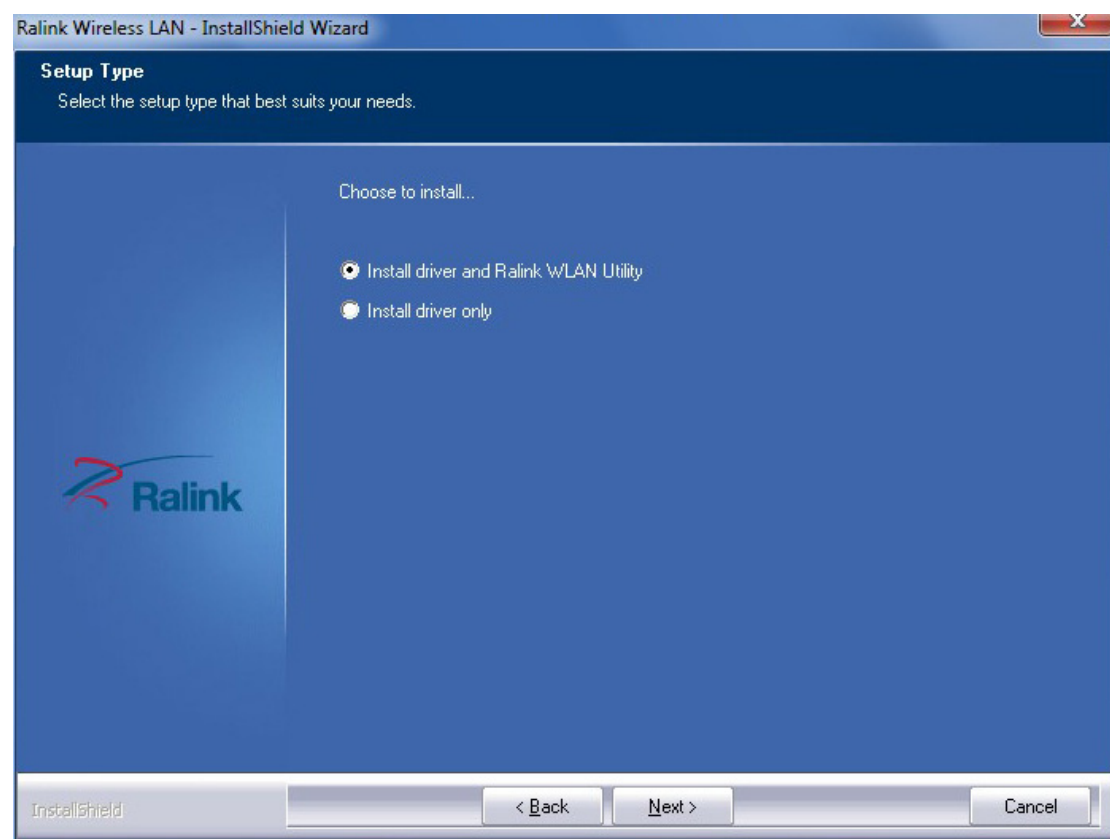
3.2 Install Driver and Utility

NOTE: Snap-shot screens of the following installation procedure are based on Windows 7 Installation procedures will be similar for other windows operating systems.

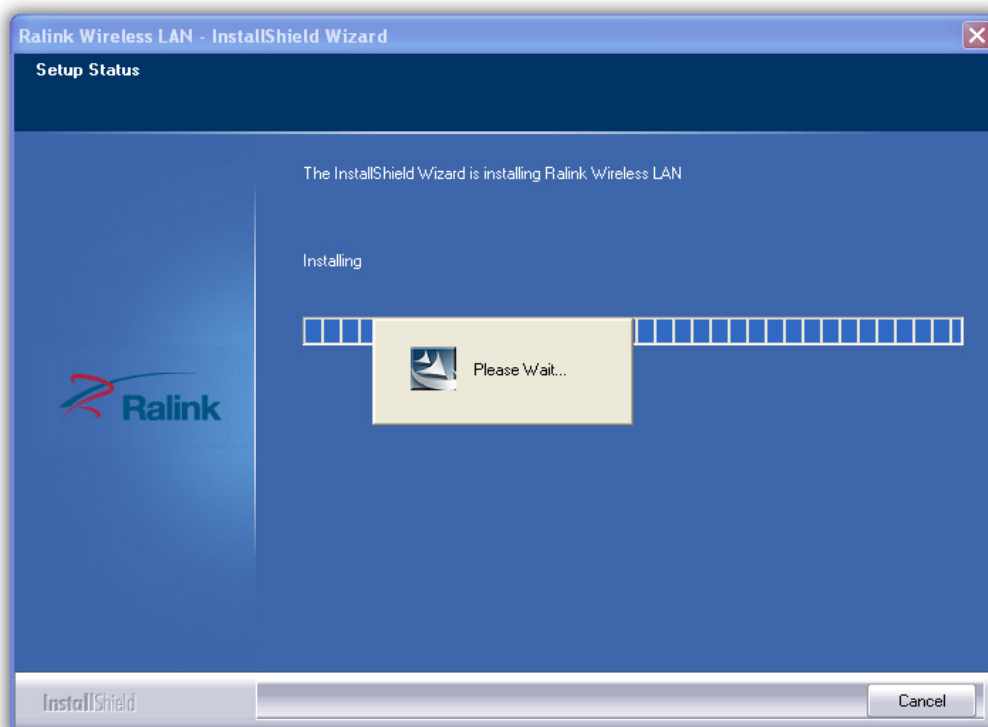
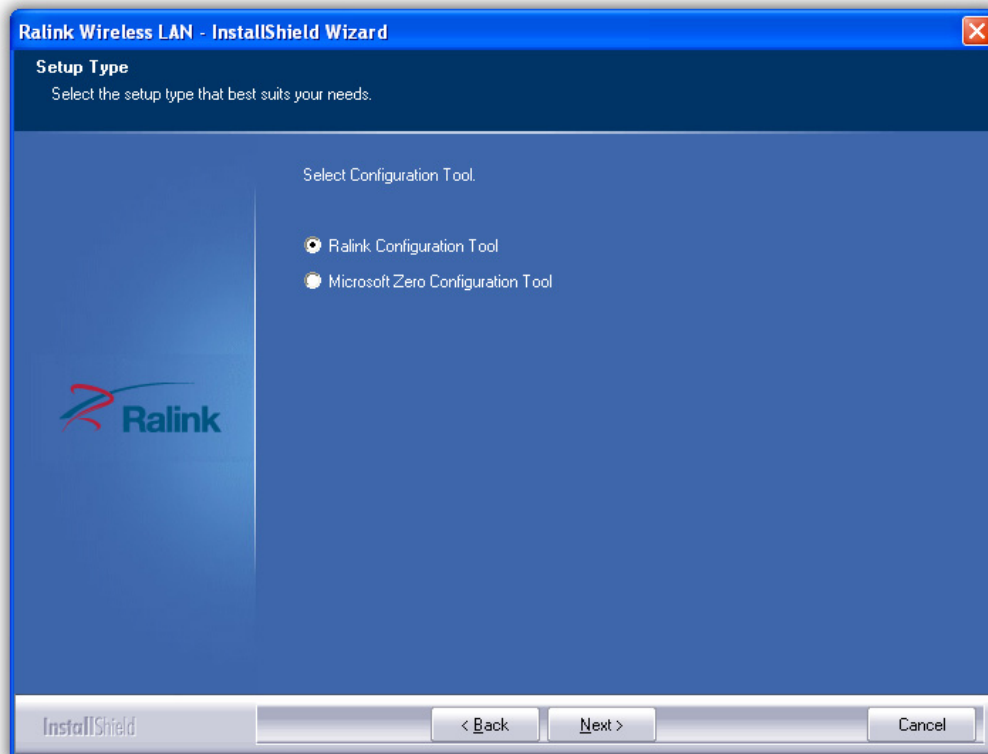
1. Insert Installation CD to your CD-ROM drive. And click **Driver Installation**. The wizard will run and install all necessary files to your computer automatically.
2. Click **Next** to accept the Agreement. Or click **Cancel** to cancel the installation



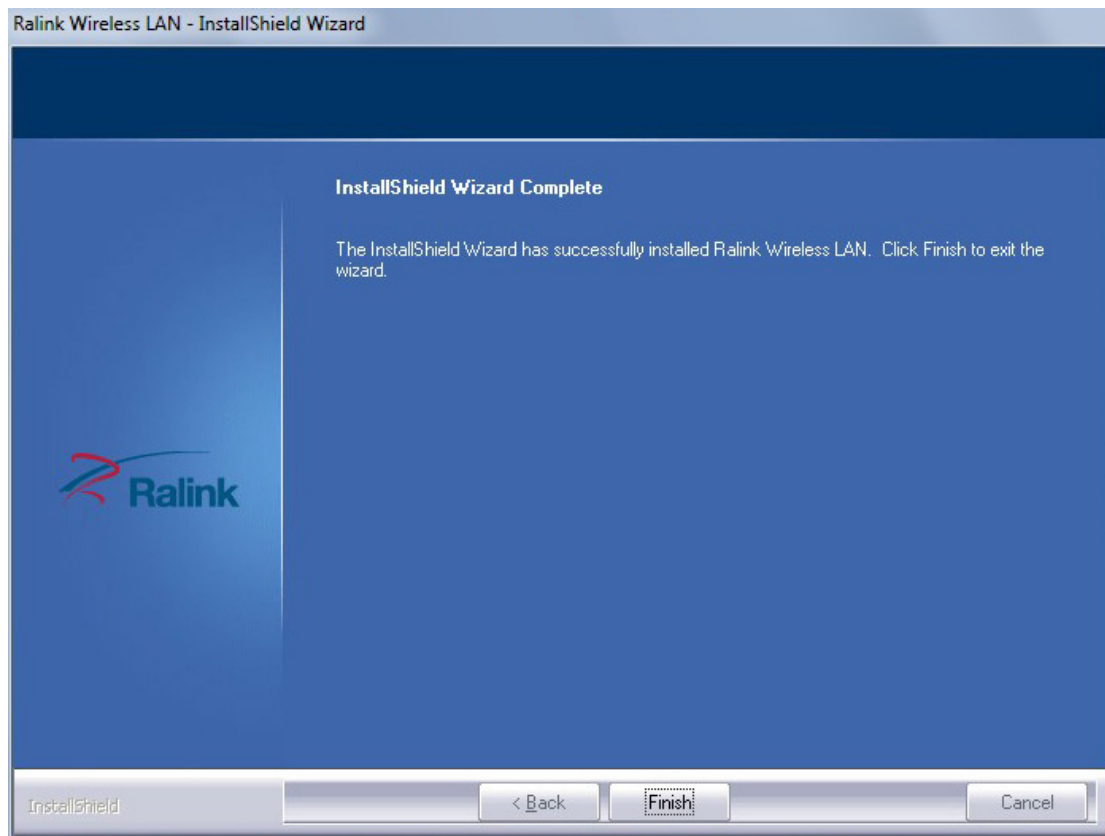
3. Click Next



4. Select Ralink Configuration Tool or Microsoft Zero Configuration Tool then click Next.
 - a. It's recommended to select Ralink Configuration Tool, which provides fully access to all function of PCI Adapter.
 - b. If you prefer to use the wireless configuration tool provided by Windows 7, please select Microsoft Zero Configuration Tool



5. Click **Finish** to complete the software installation.



4. Windows Wireless Utility

4.1 Windows AutoConfig Service for Win 7

4.1.1 Ralink Wireless Utility and Windows AutoConfig Service

Notes: The following installation was operated under Windows 7. (Procedures are similar for Windows XP /vista)

In Windows 7, the AutoConfig service provides basic wireless configuration functions for the Ralink Wireless Network Interface Controller. In order to perform these functions, the AutoConfig service should first be enabled (Refer to Section 1-2-2).

Once the Ralink wireless utility is minimized, click the Ralink icon as shown in Figure 1-1. This will bring up the option menu shown as Figure 1-2 for the user to restore the utility window or terminate the utility.



Figure 1-1

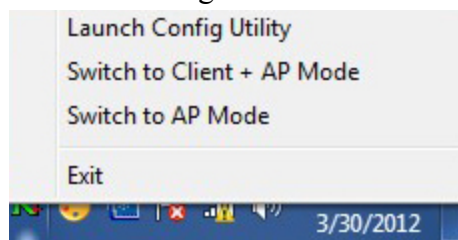


Figure 1-2

The Ralink wireless utility as shown in Figure 1-3, provides profile management, the available networks listing, a statistical counter display, Wi-Fi multimedia (WMM), protected Wi-Fi setup, Cisco compatible extensions (CCX), call admission control (CAC), radio controls, Ralink driver/utility information, and help functions.

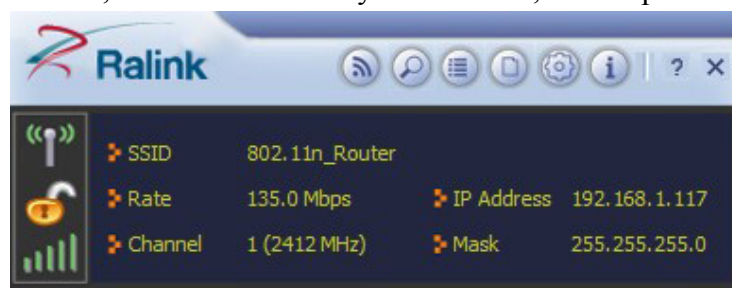


Figure 1-3 Ralink Utility

The Ralink wireless utility starts in compact mode as shown in Figure 1-3. Clicking the expanding icon at the bottom-right corner can change to the full mode as shown in Figure 1-4.

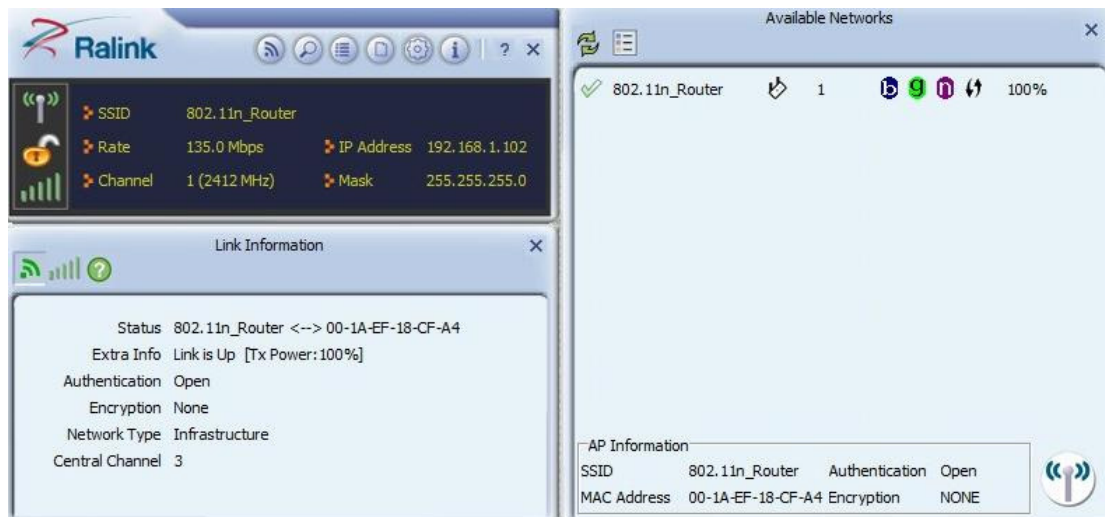
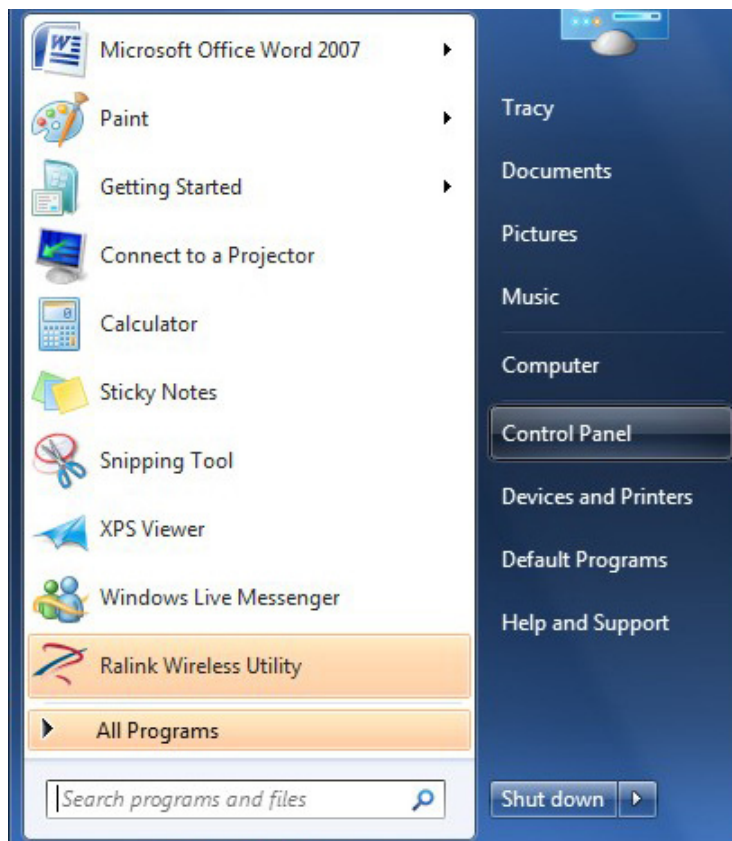


Figure 1-4 Ralink Utility in full mode

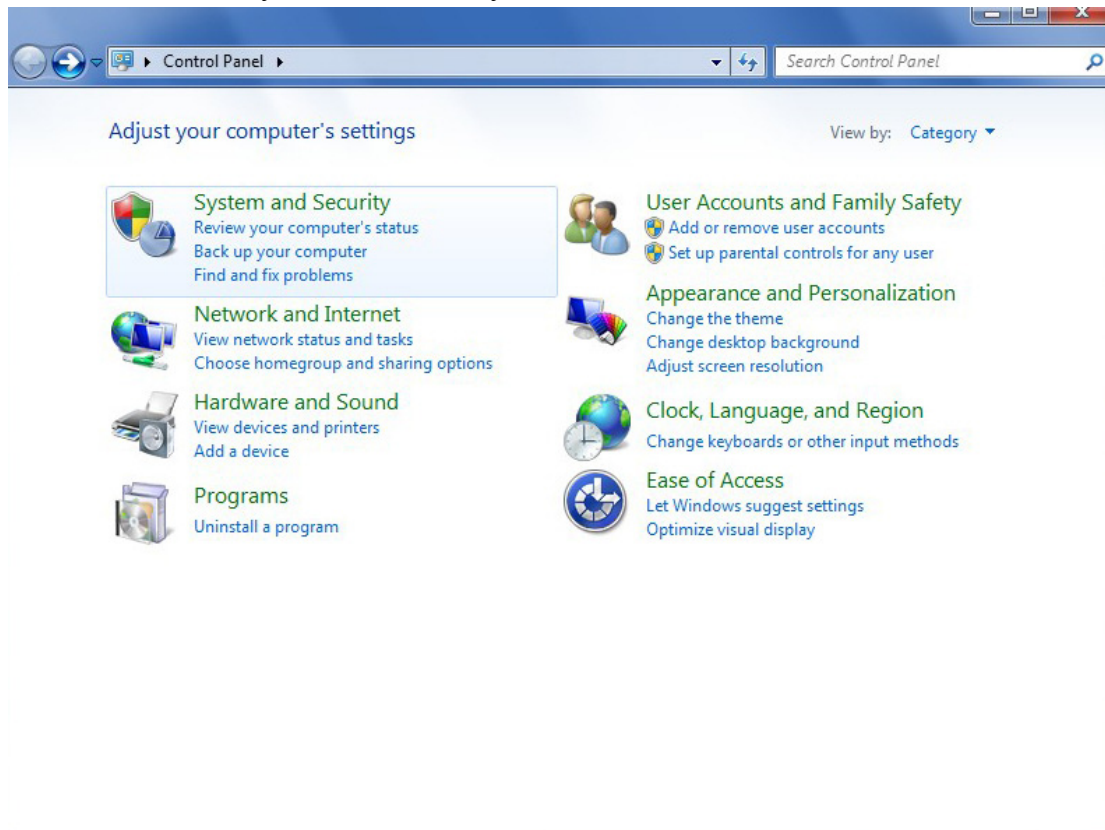
4.1.2 Windows AutoConfig Service

The following steps outline the procedure for starting/stopping the Windows AutoConfig service.

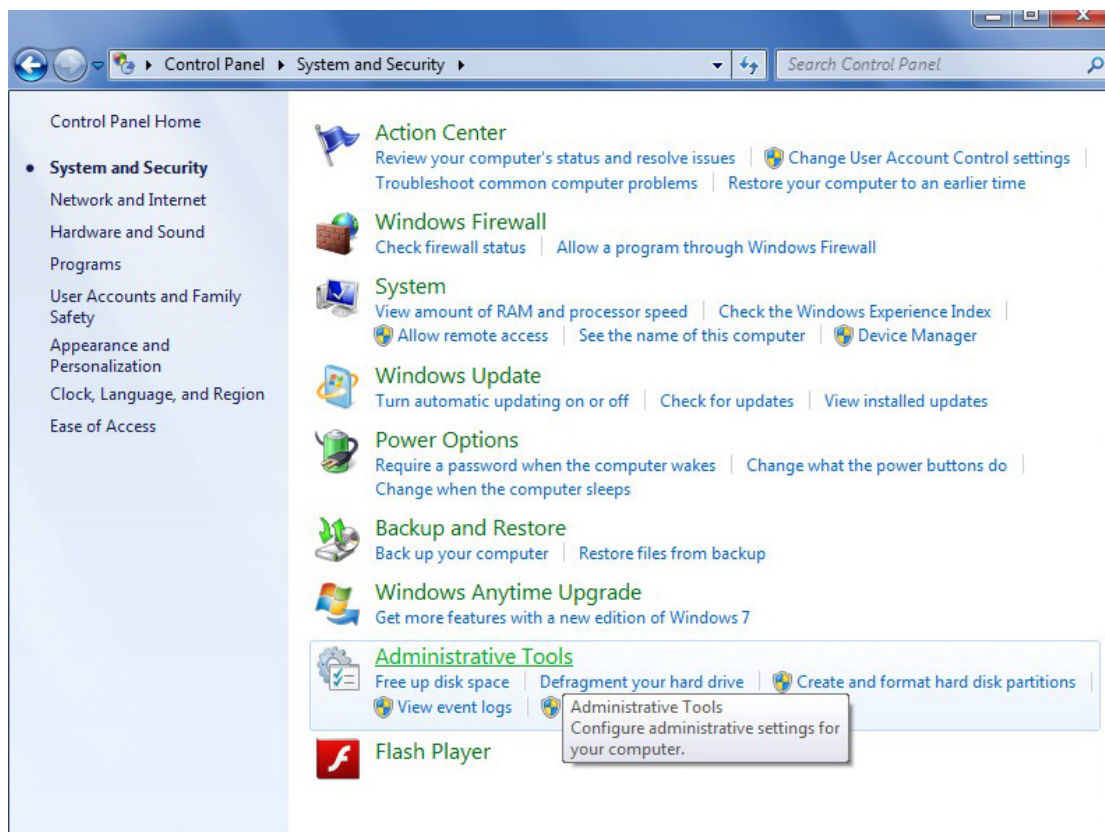
Select "Control Panel" in the start menu



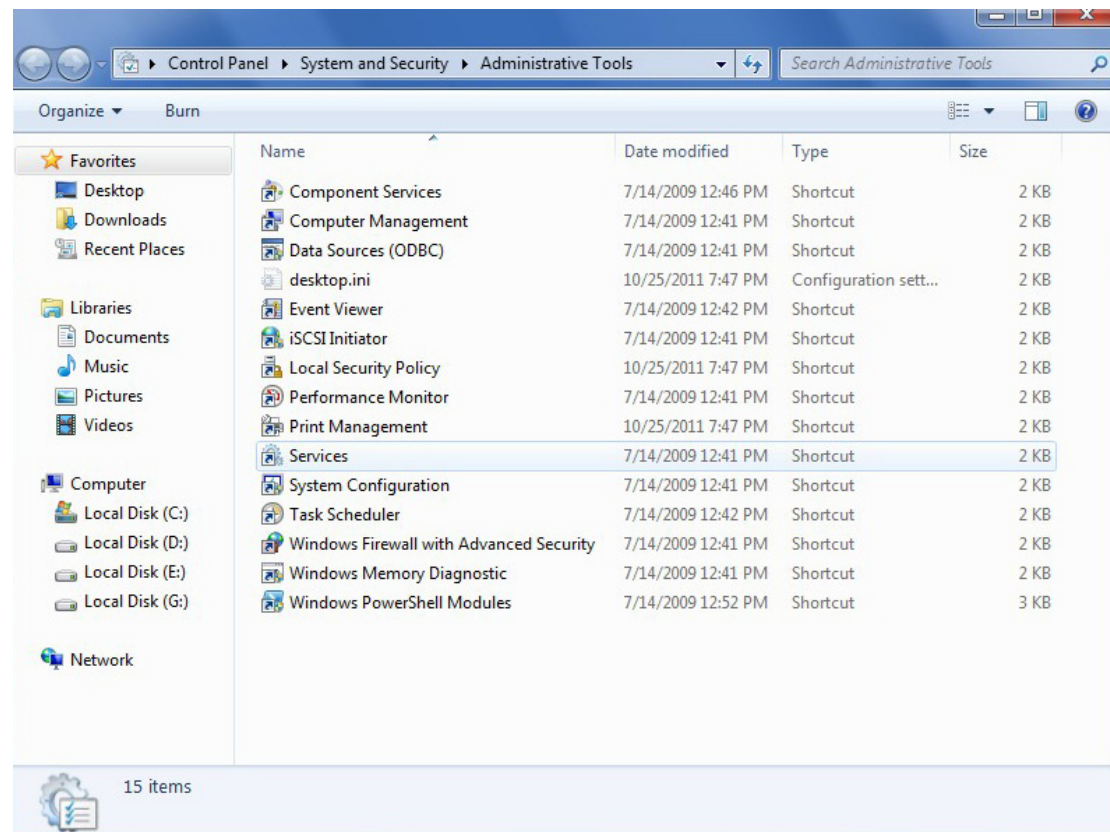
Double-click the "System and Security" icon



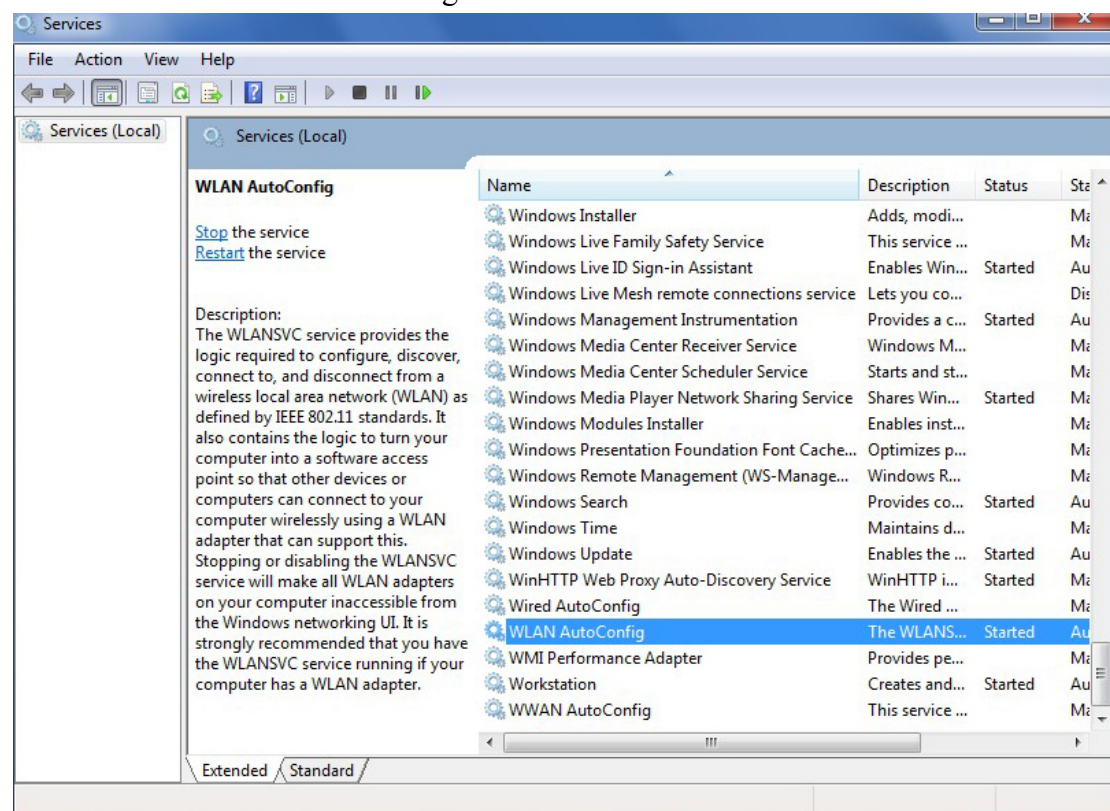
Double-click the "Administrative Tools" icon



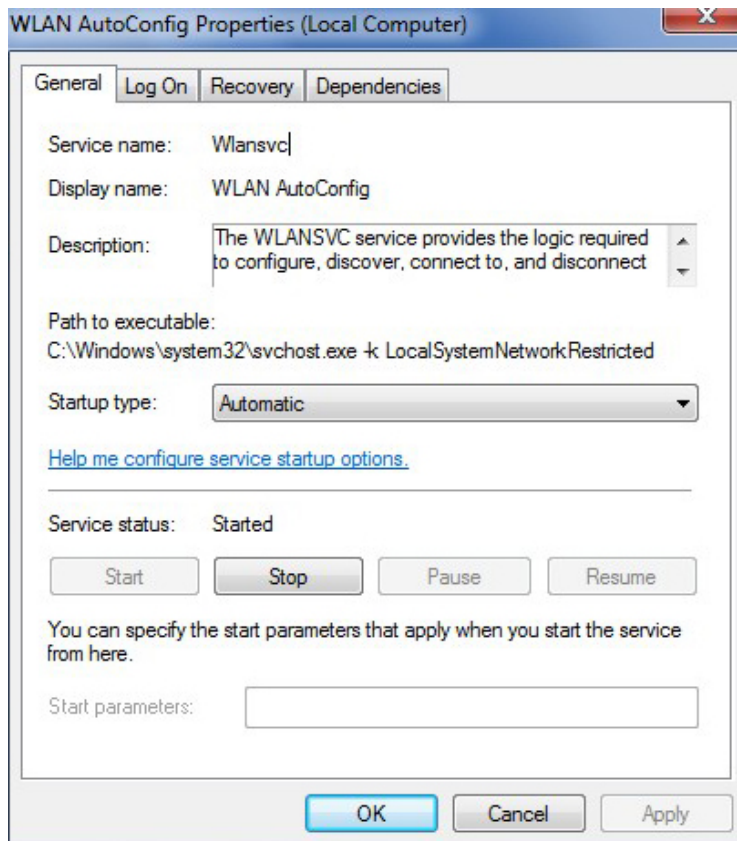
Double-click "Services"



Double-click "WLAN AutoConfig"



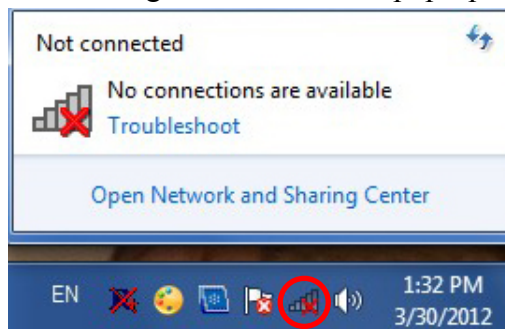
Manage the AutoConfig properties in the dialog box



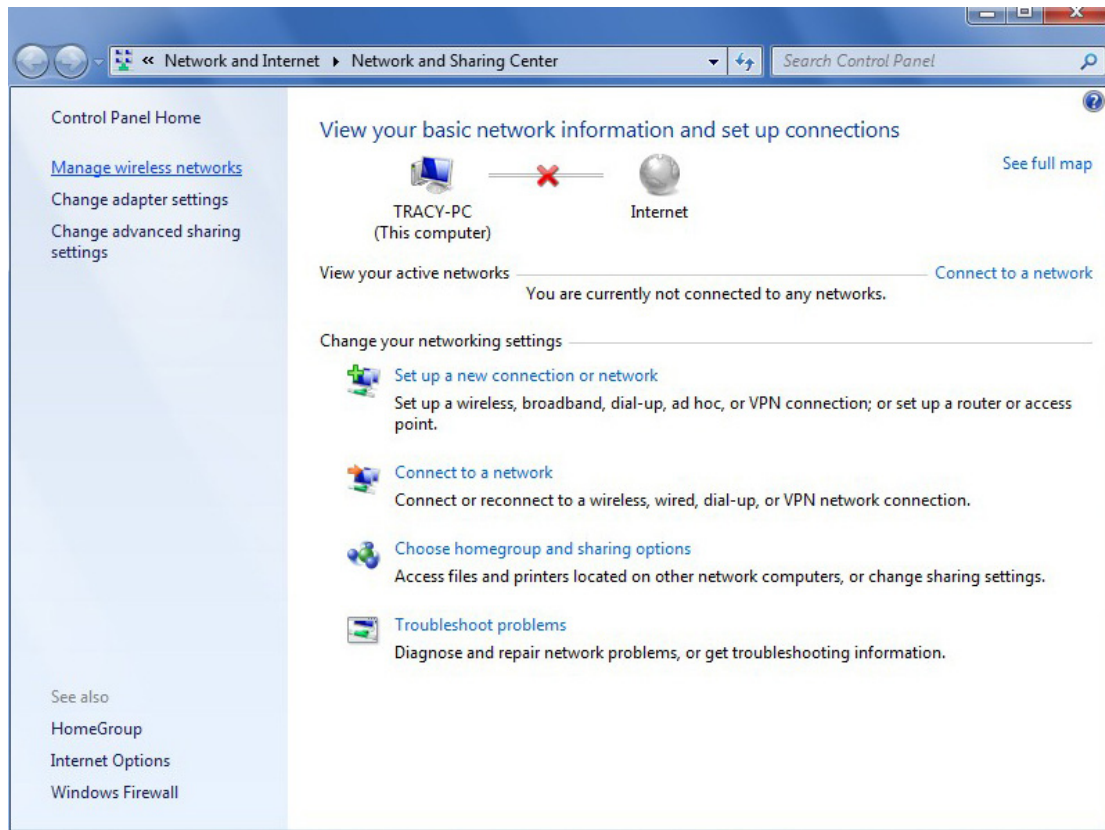
Windows profile manager can be accessed via control panel or network connection icon in the task bar.

1. Access via network connection icon

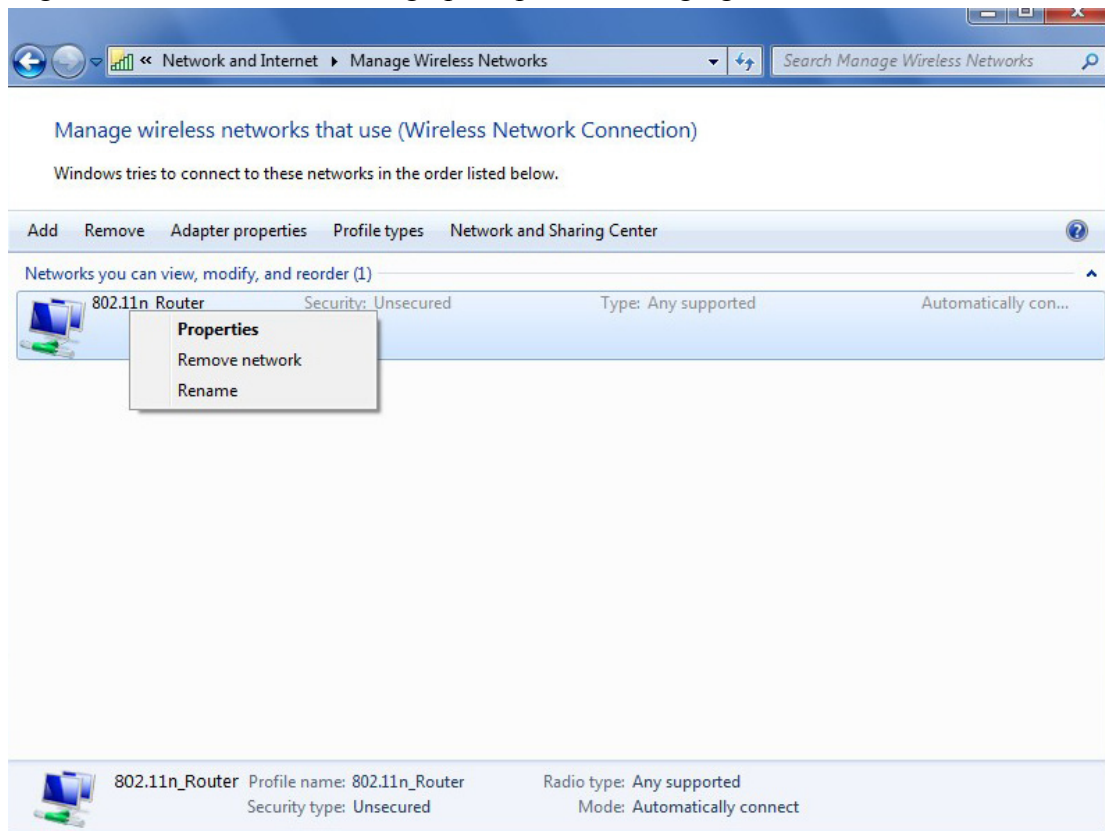
Right-click the network connection icon in the taskbar, then select "Open Network and Sharing Center" from the pop-up menu



Select "Manage wireless networks" from the tasks list

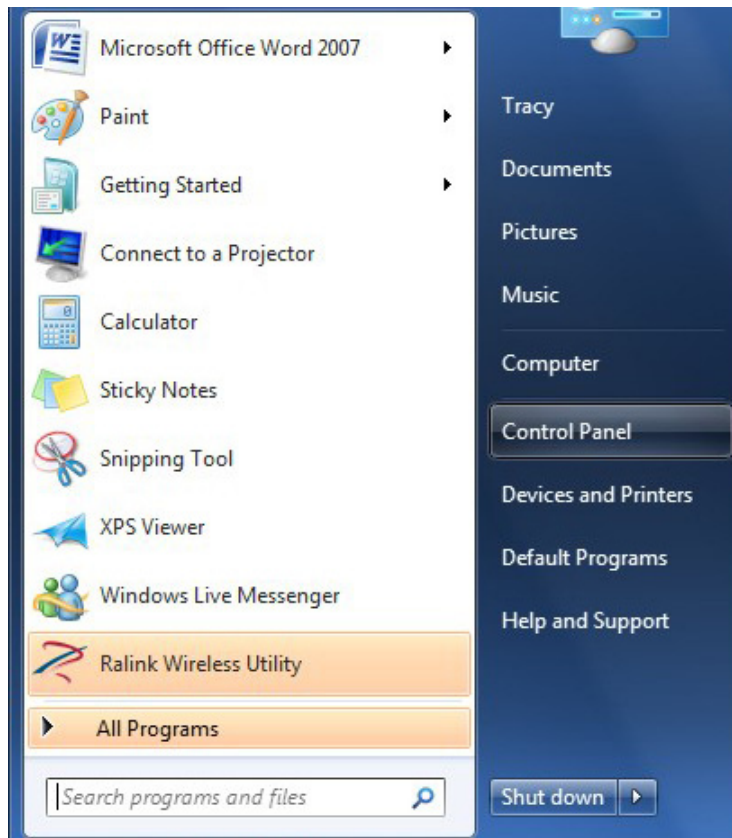


Right-click the network to bring up the profile managing menu

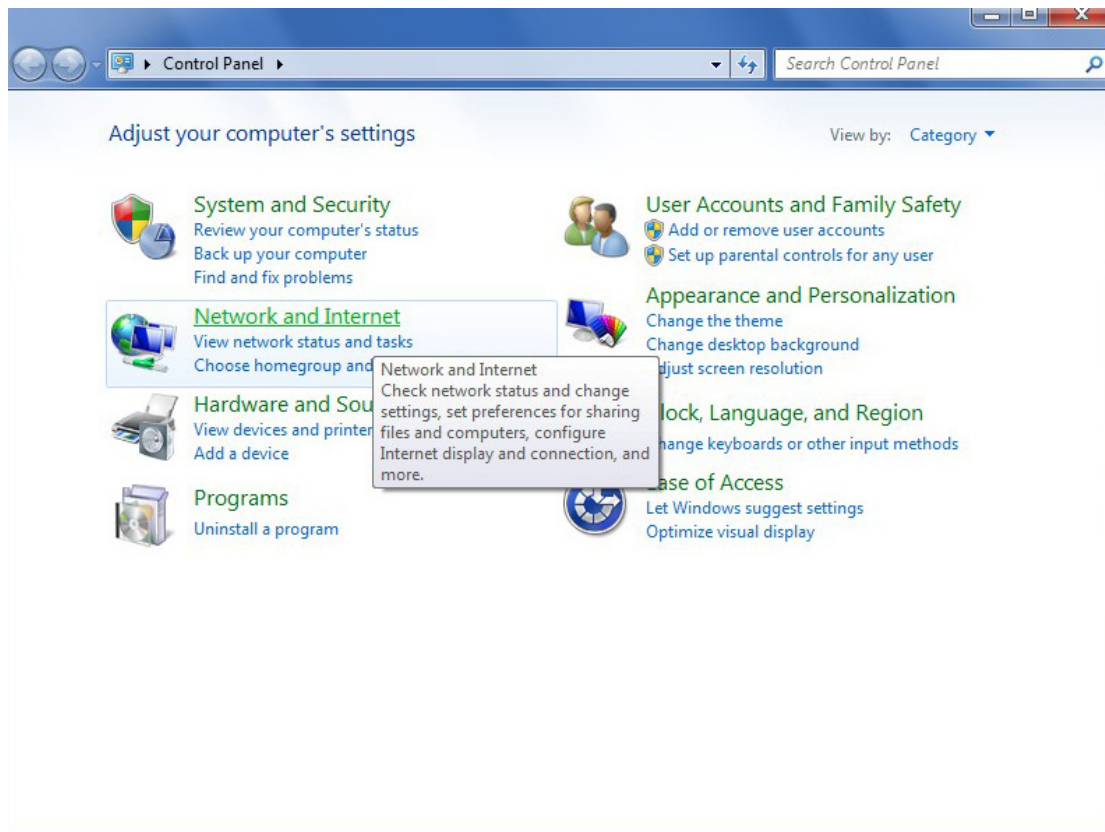


2. Access via control panel

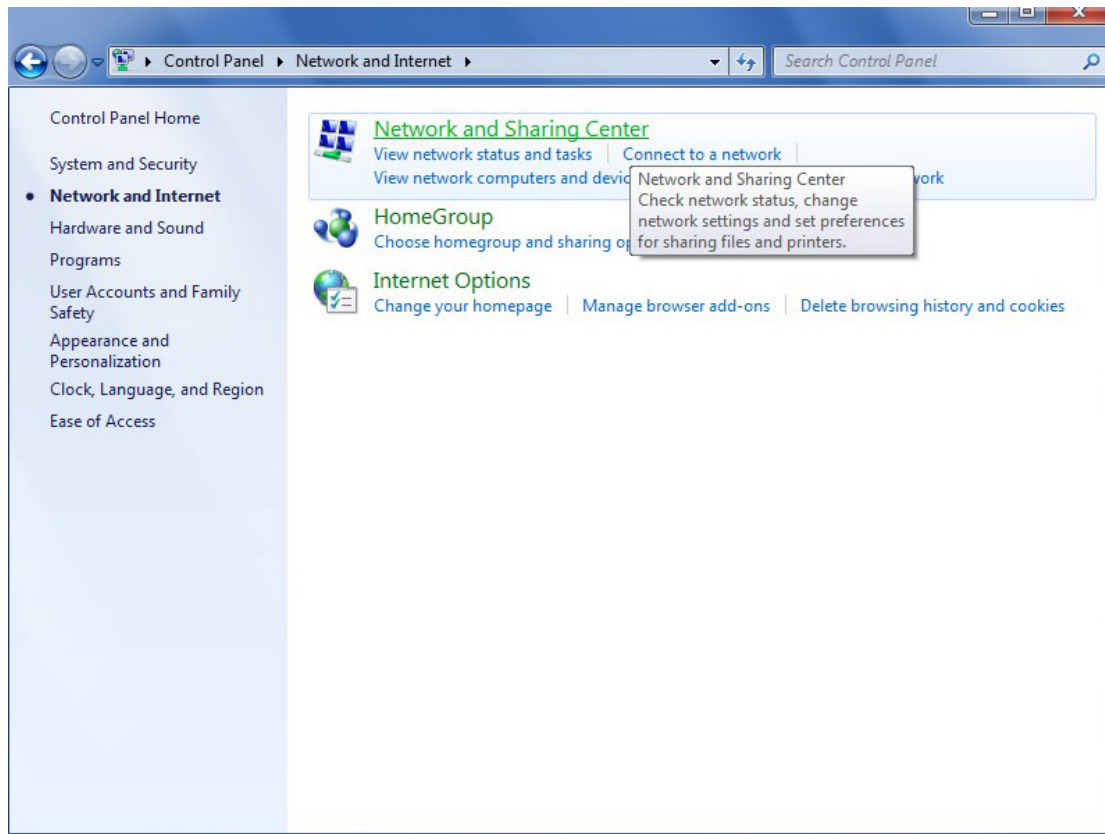
Select "Control Panel" from the start menu



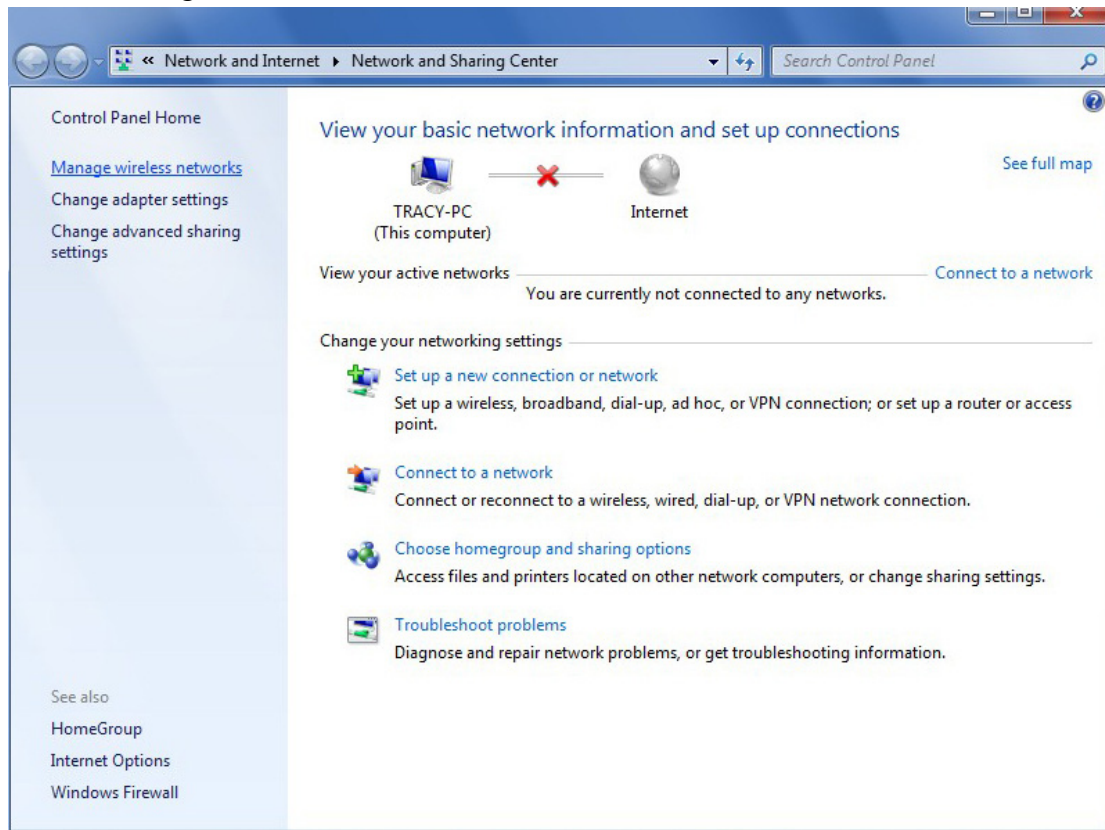
Double-click the "Network and Internet" icon



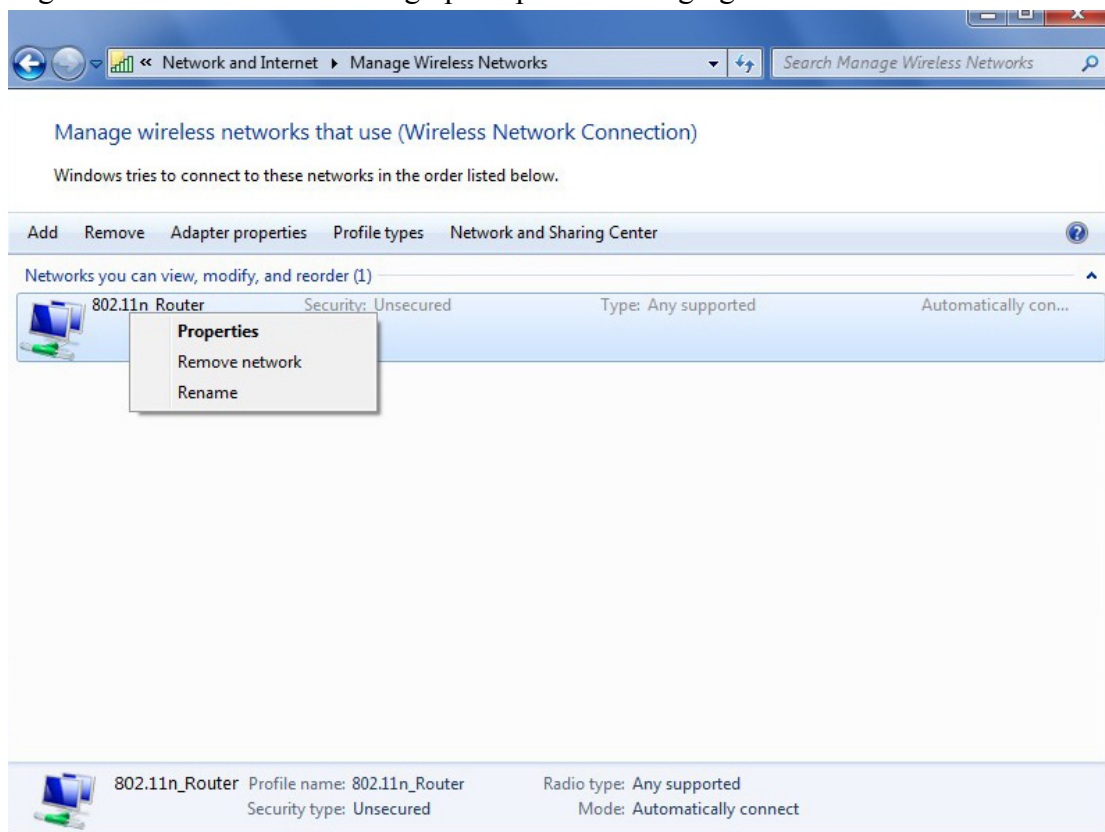
Double-click the "Network and Sharing Center" icon



Select "Manage wireless networks" from the tasks list



Right-click the network to bring up the profile managing menu



5. Ralink Wireless Utility (RaUI)

5.1 Start

5.1.1 Start RaUI

When starting RaUI, the system will connect to the AP with best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 2-1.

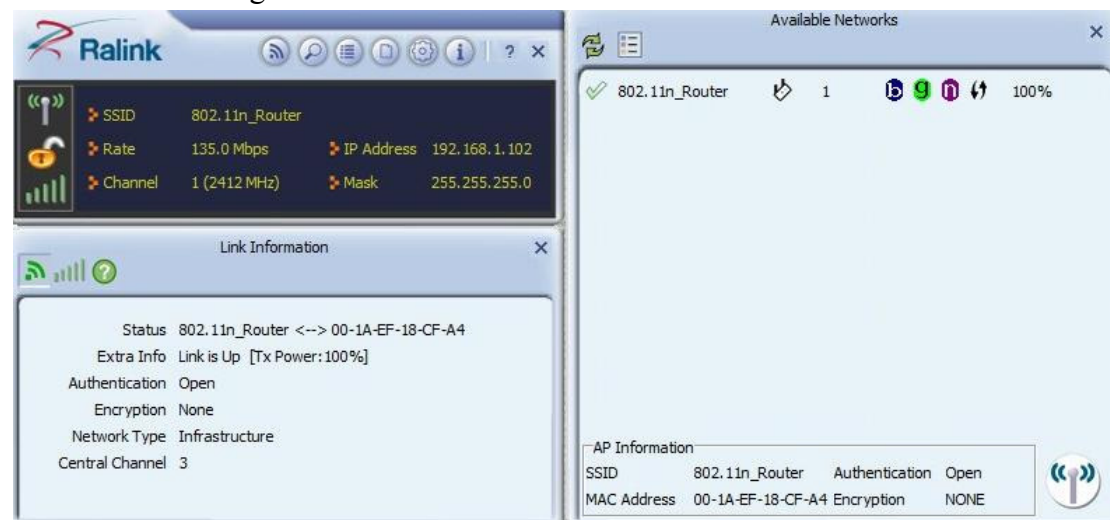


Figure 2-1-1 RaUI section introduction

There are three sections to the RaUI dialog box. These sections are briefly described as follow.

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

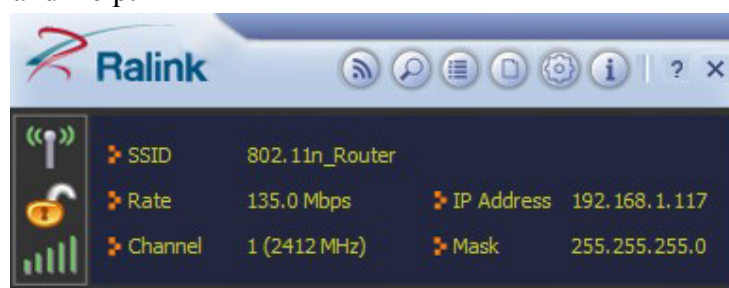


Figure 2-1-2 Button section

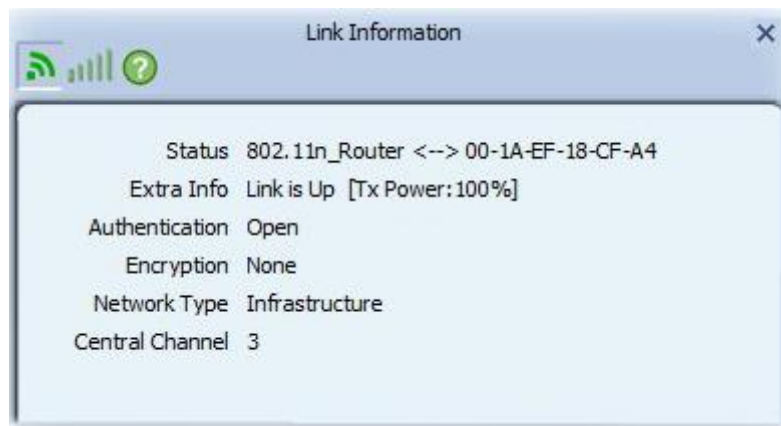


Figure 2-1-3 Link Information page



Figure 2-1-4 Profile page

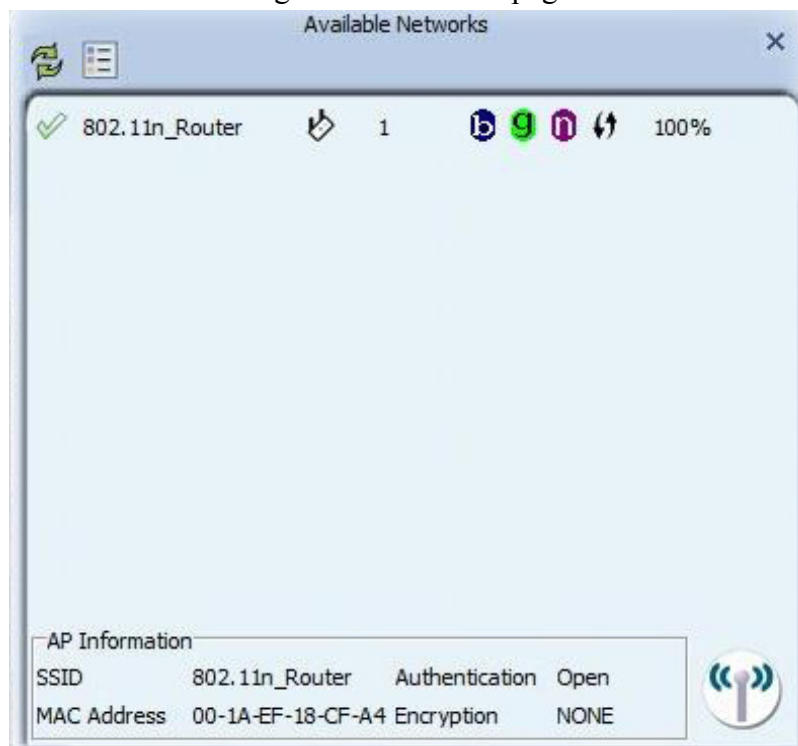


Figure 2-1-5 Network page

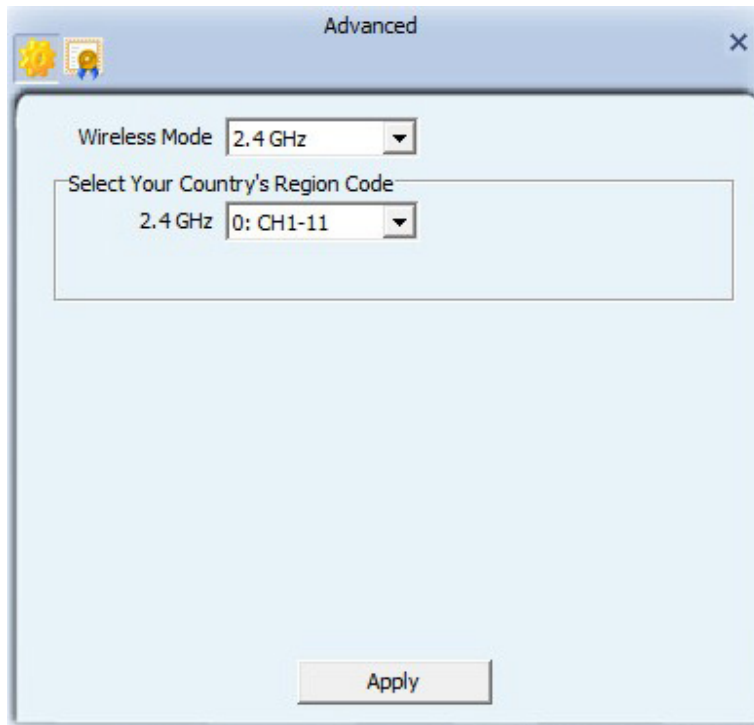


Figure 2-1-6 Advance page



Figure 2-1-7 About page

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close RaUI utility.



Figure 2-1-8 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:

R+ : Indicates the connected and signal strength is good.

R+ : Indicates the connected and signal strength is normal.

R+ : Indicates that it is not yet connected.

R+ : Indicates that a wireless NIC can not be detected.

R+ : Indicates that the connection and signal strength is weak.

5.2 Profile

5.2.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 shows the basic profile section.

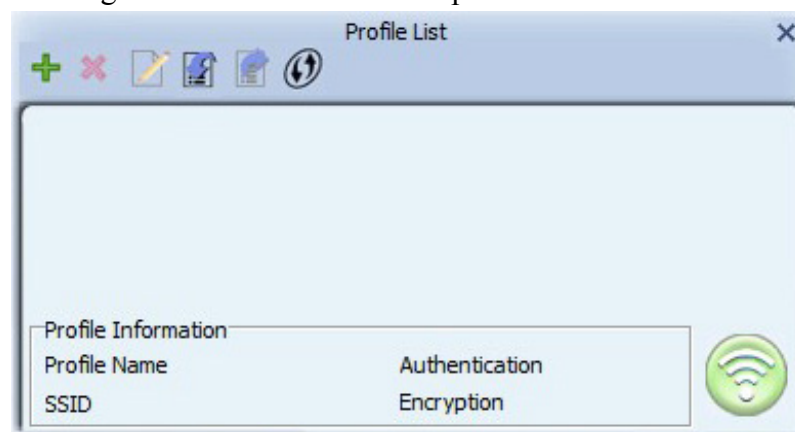













Figure 2-2-1 Profile function

Definition of each field:

- Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).
- SSID: The access point or Ad-hoc name.
- Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.
- Authentication: Indicates the authentication mode used.
- Encryption: Indicates the encryption Type used.
- Use 802.1x: Shows if the 802.1x feature is used or not.
- Cannel: Channel in use for Ad-Hoc mode.
- Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
- Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.
- RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.
- Fragment Threshold: The user can adjust the Fragment threshold number by sliding

the bar or key in the value directly.

Icons and buttons:

-  : Indicates if a connection made from the currently activated profile.
-  : Indicates if the connection has failed on a currently activated profile.
-  : Indicates the network type is infrastructure mode.
-  : Indicates the network type is in Ad-hoc mode.
-  : Indicates if the network is security-enabled.
-  : Click to add a new profile.
-  : Click to edit an existing profile.
-  : Deletes an existing profile.
-  : Import an existing profile.
-  : Export an existing profile.
-  : Activates the selected profile.

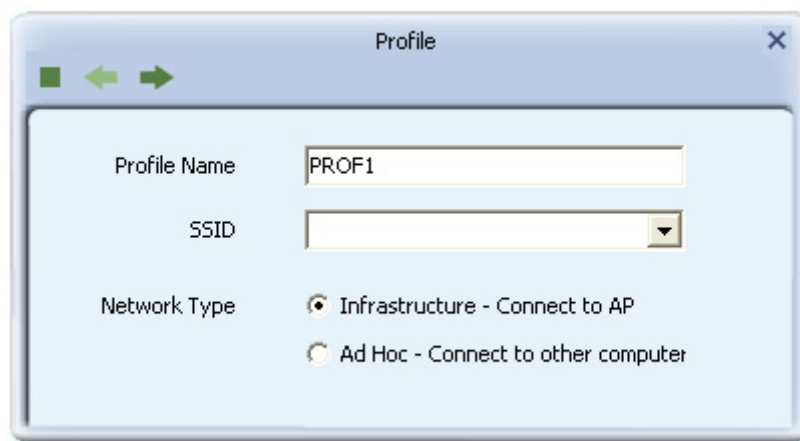
5.2.2 Add/Edit Profile

There are three methods to open the Profile Editor dialog box.

You can open it by clicking the "Add to Profile" button in the Site Survey tab.

You can open it by clicking the "Add" button in the Profile tab.

You can open it by clicking the "Edit" button on the Profile tab.






The image shows a dialog box titled "Profile" with a close button (X) in the top right corner. At the top left of the dialog, there are three navigation buttons: a green square, a green left arrow, and a green right arrow. The main area of the dialog contains the following fields and options:

- Profile Name:** A text input field containing the text "PROF1".
- SSID:** A dropdown menu with a downward arrow on the right.
- Network Type:** Two radio button options:
 - ☒ Infrastructure - Connect to AP
 - ☐ Ad Hoc - Connect to other computer

Figure 2-2-1 Add a new Profile

Icons and buttons:

-  : To the next page.
-  : Back to the previous page.
-  : Cancel button.

The image shows a 'Profile' configuration window with a title bar containing a close button (X) and navigation arrows. The window has a light blue background. Inside, there are three main sections: 'Profile Name' with a text input field containing 'PROF1'; 'SSID' with a dropdown menu; and 'Network Type' with two radio button options: 'Infrastructure - Connect to AP' (which is selected) and 'Ad Hoc - Connect to other computer'.

Figure 2-2-2 Profile Name, SSID, Network Configuration

- Profile Name: The user can chose any name for this profile, or use the default name defined by system.
- SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.
- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Network Type: There are two types, infrastructure and 802.11 Ad-hoc modes. Under Ad-hoc mode, user can also choose the preamble type. The available preamble type includes auto and long. In addition, the channel field will be available for setup in Ad-hoc mode.

The image shows the same 'Profile' configuration window, but with the 'Authentication' and 'Encryption' settings visible. 'Authentication' is set to 'Open' and 'Encryption' is set to 'None', both shown in dropdown menus. The 'Network Type' section is not visible in this view.

Figure 2-2-3 Authentication and Encryption Configuration

- Authentication Type: There are 7 types of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1X, WAPI-PSK, and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the selection of available encryption type are none and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.

Profile

Default Tx Key: Key 1

Key Format: Hex(10 or 26 hex digits)

WEP Key:

Figure 2-2-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys.
 1. Hexadecimal - 40bits: 10 Hex characters.
 2. Hexadecimal - 128bits: 26 Hex characters.
 3. ASCII - 40bits: 5 ASCII characters.
 4. ASCII - 128bits: 13 ASCII characters.

Profile

WPA Preshared Key:

Figure 2-2-5 Pre-shared Key Configuration

- Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

Profile

EAP Method: PEAP ☒ Session Resumption

Tunnel Authentication: EAP-MSCHAP v2

Tunnel ID: Authentication ID

Tunnel Password:

Domain Name:

Figure 2-2-6 802.1x Configuration

- 802.1x Setting: This is introduced in the topic of “Section 3-2 : 802.1x Setting”

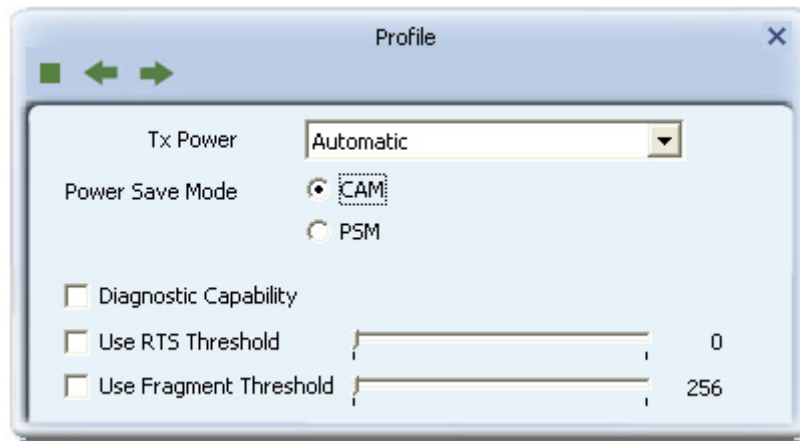


Figure 2-2-7 Advanced Configuration

- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-Hoc network.

5.2.3 Pre-logon Connect

The Pre-logon Connect configuration page as shown in Figure 2-2-4.

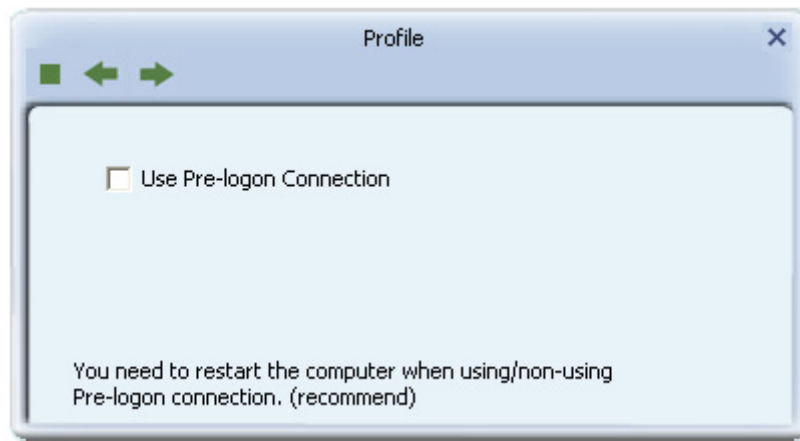


Figure 2-2-4 Pre-logon Connect Page

Field definitions:

- Pre-logon Connect: Use ID and Password in Profile.
- ** Recommend: You need to restart the computer when using/non-using Pre-logon connection.**

5.3 Network

5.3.1 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as shown in Figure 2-3-1-1.

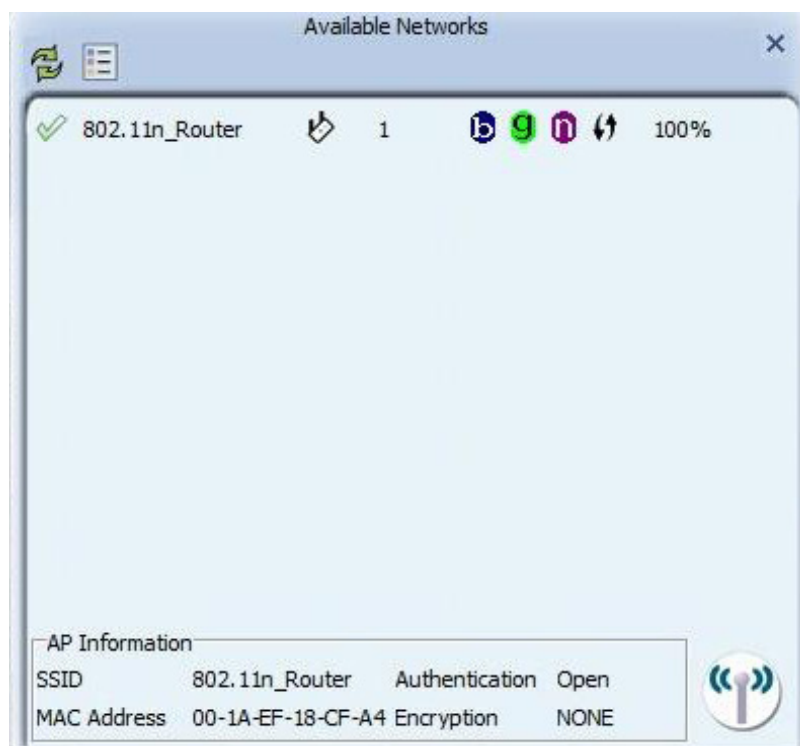


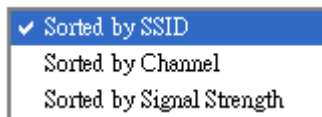
Figure 2-3-1-1 Network function

Definition of each field:

- SSID: Name of BSS or IBSS network.
- Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network
- Channel: Channel in use.
- Wireless Mode: AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode.
- Security-Enable: Indicates if the AP provides a security-enabled wireless network.
- Signal: Receive signal strength of the specified network.

Icons and buttons:

- : Indicates that the connection is successful.
- : Indicates the network type is in infrastructure mode.
- : Indicates the network type is in Ad-hoc mode.
- : Indicates that the wireless network is security-enabled.
- : Indicates 802.11a wireless mode.
- : Indicates 802.11b wireless mode.
- : Indicates 802.11g wireless mode.
- : Indicates 802.11n wireless mode.



: Indicate that the AP list is sorted by SSID, Channel or Signal.



: Button to connect to the selected network.



: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.



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

Connected network:

- When RaUI first runs, it will select the best AP to connect to automatically.
- If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.
- If the intended network uses encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to the example on how to fill in the security information.

When you double click an AP, you can see detailed information about that AP.

The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode.)

The introduction is as follows:

- General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.

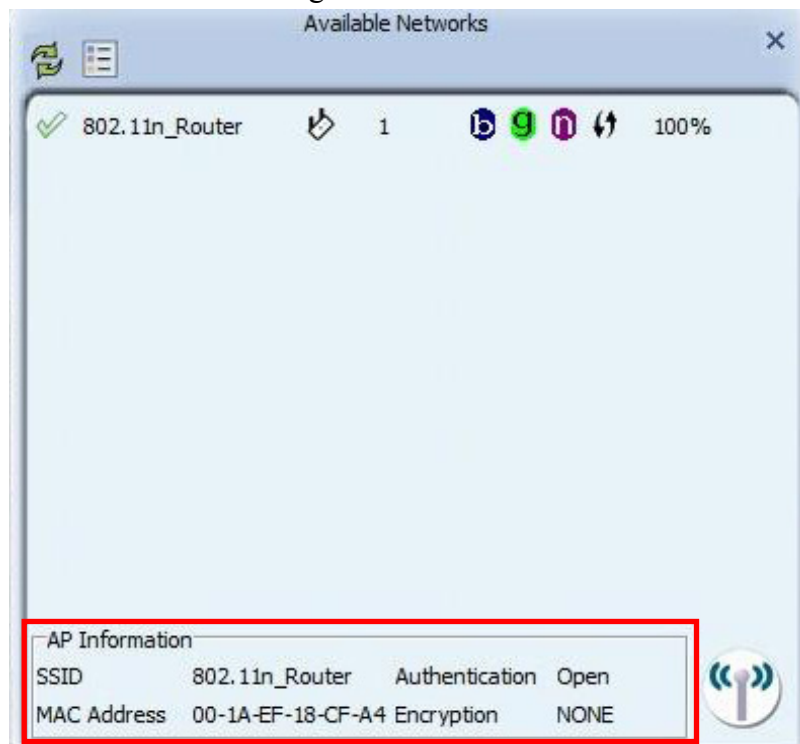


Figure 2-3-1-2 General information about the Access Point

5.4 Advanced

5.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

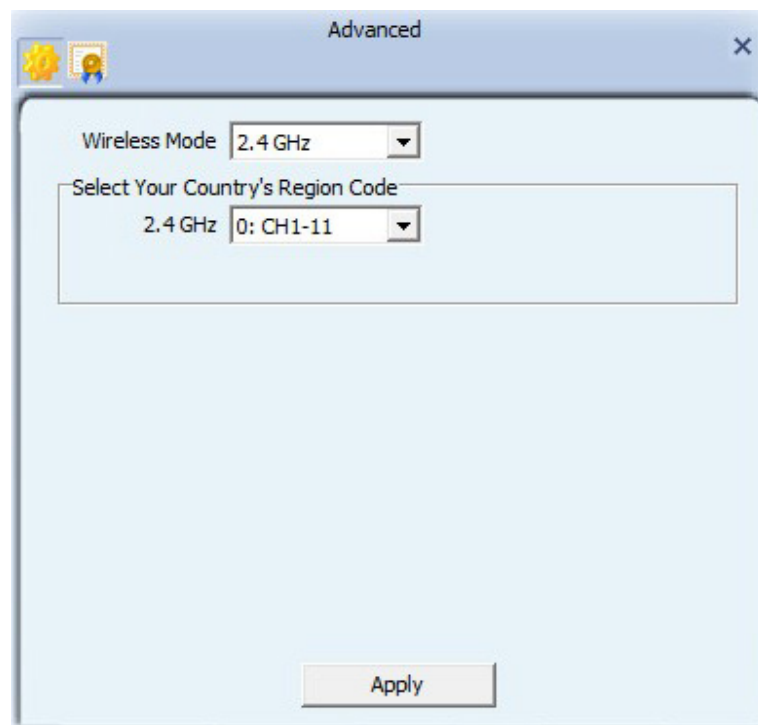


Figure 2-4 Advance function

- Wireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported. (2.4G/5GHz options are depend on different products)
- Wireless Protection: Users can choose from Auto, on, and off. (This is not supported by 802.11n adapters.)

Auto: STA will dynamically change as AP announcement.

On: The frames are always sent with protection.

Off: The frames are always sent without protection.

- TX Rate: Manually select the transfer rate. The default setting is auto. (802.11n wireless cards do not allow the user to select the TX Rate.)
- Enable TX Burst: Ralink's proprietary frame burst mode.
- Enable TCP Window Size: Optimize the TCP window size to allow for greater throughput.
- Fast Roaming at-: enables fast roaming, which is set by the transmit power.
- Select Your Country Region Code: There are eight countries to choose from in the country channel list. (11A ListBox only shows for 5G adapters.)
- Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.
- Apply the above changes.

5.4.2 Certificate Management

The Certificate Management configuration page as shown in Figure 2-4-2.

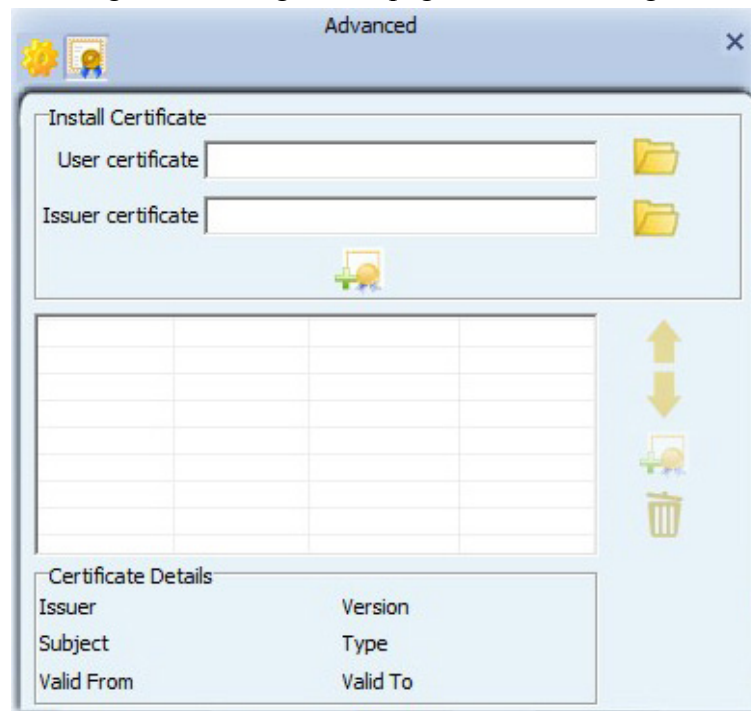


Figure 2-4-2 Certificate Management function

5.5 Link Information

5.5.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-5-1.

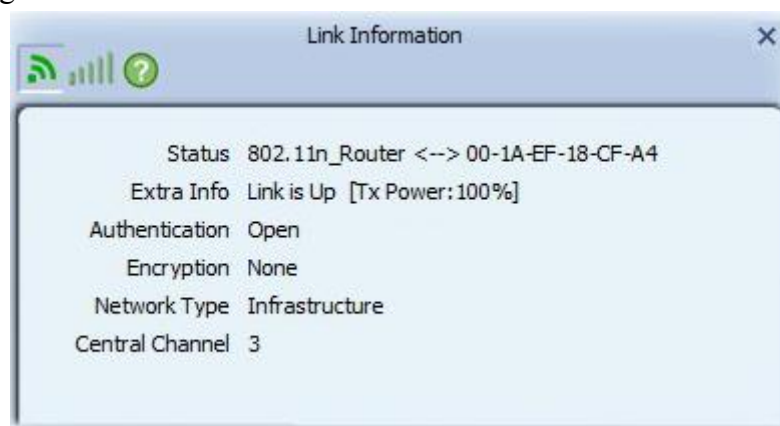


Figure 2-5-1 Link Status function

- **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.

5.5.2 Throughput

The throughput page displays detailed information about the current connection as shown in Figure 2-5-2.

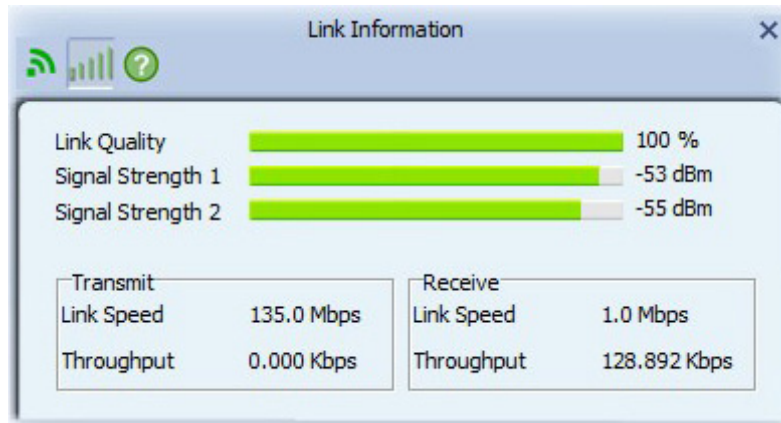


Figure 2-5-2 Throughput function

- 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.

5.5.3 Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to understand. Figure 2-5-1 shows the detailed page layout.

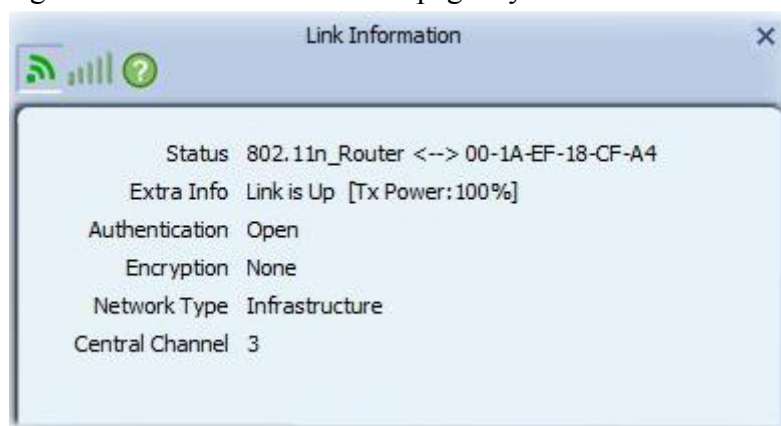
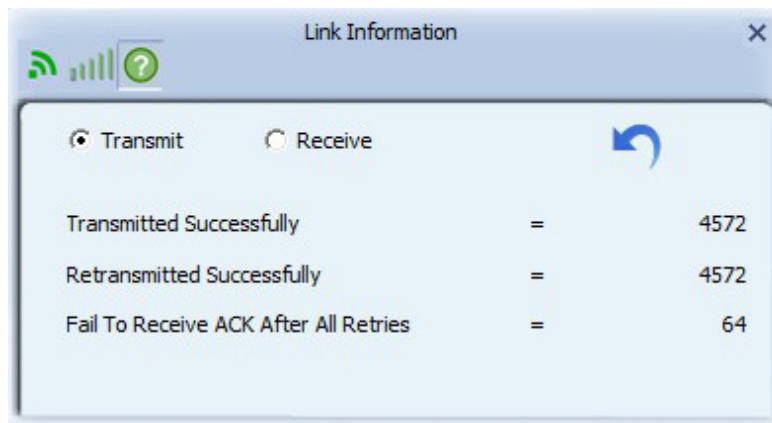


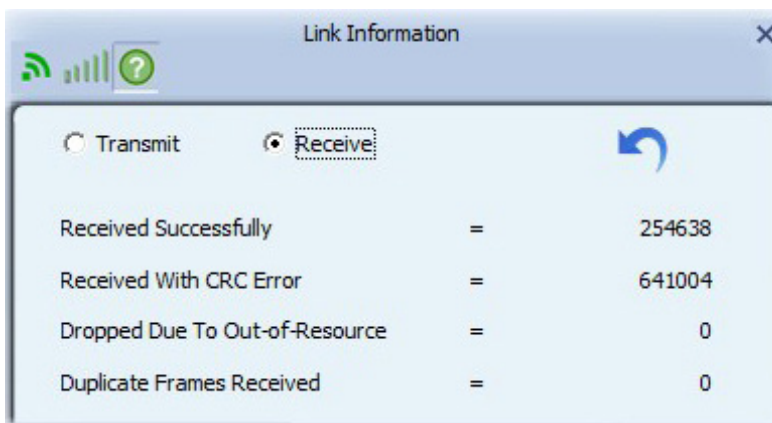
Figure 2-5-1 Statistics function

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: Failed to receive CTS after sending RTS.
- Frames Retransmitted Successfully: Successfully retransmitted frames numbers.
- Reset counters to zero.

Receive Statistics:



- Frames Received Successfully: The number of frames successfully received.
- Frames Received With CRC Error: The number of frames received with a CRC error.
- Frames Dropped Due to Out-of-Resource: The number of frames dropped due to a resource issue.
- Duplicate Frames Received: The number of duplicate frames received.
- Reset all the counters to zero.

5.6 About

5.6.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-10.



Figure 2-10 About function

Connect to Ralink's website: [Ralink Technology, Corp.](http://www.ralink.com)

Display Configuration Utility, Driver, and EEPROM version information.

Display Wireless NIC MAC address.

5.7 WPS

5.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.



Figure 2-7-1 WPS function

- 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 supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.
- WPS AP List: Displays the SSID of the surrounding APs with WPS IE from the last scan result.
- PBC: Start to add to AP using PBC configuration method.
- 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.
- Auto: Starts to add to AP by using to select the AP automatically in PIN method.

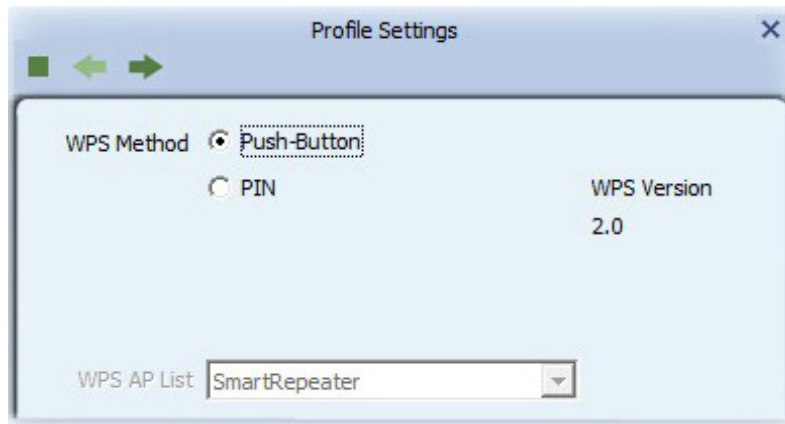


Figure 2-7-1-1 WPS Profile

- PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to re-generate a new PIN Code.
- Config Mode: The station serving as an Enrollee or an external Registrar.

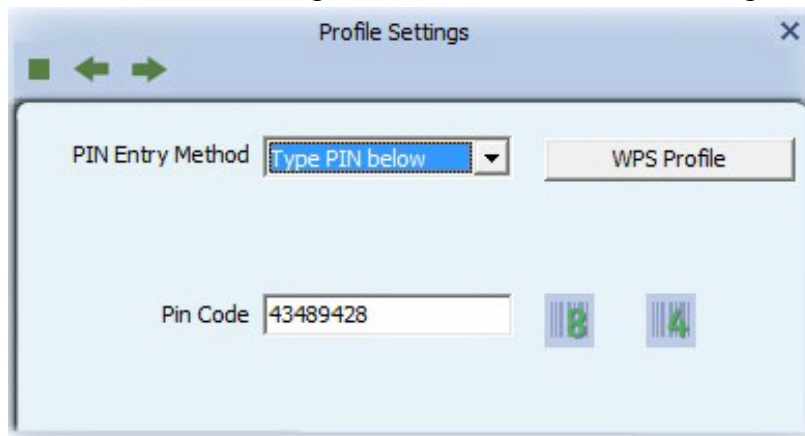


Figure 2-7-1-2 WPS PIN function

After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

- Progress Bar: Displays the rate of progress from Start to Connected.
- Status Bar: Displays the current WPS Status.

6. Security

6.1 Auth.\ Encry. Setting – WEP/TKIP/AES

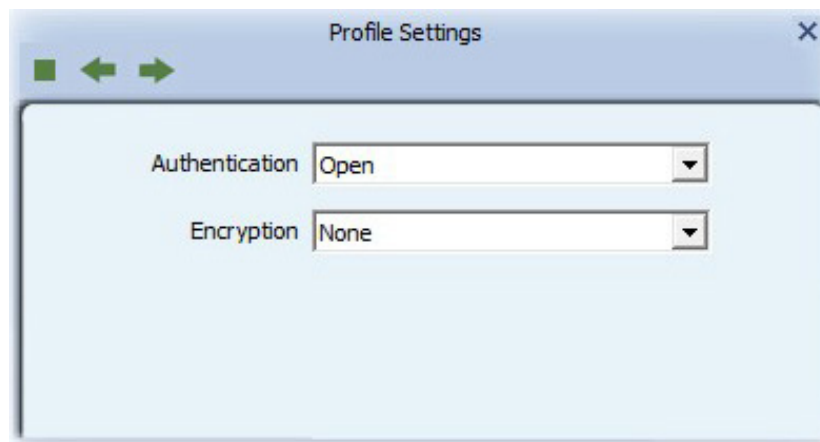


Figure 3-1 Auth.\Encry. Settings in the Profile Page

- Authentication Type: There are 7 authentication modes supported by RaUI. They are Open, Shared, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1x, WAPI-PSK and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the available encryption types are none and WEP. For Shared and 802.1x authentication mode, the selection of available encryption is WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available. For WAPI-PSK and WAPI-CA authentication mode, only SMS4 encryption is available.

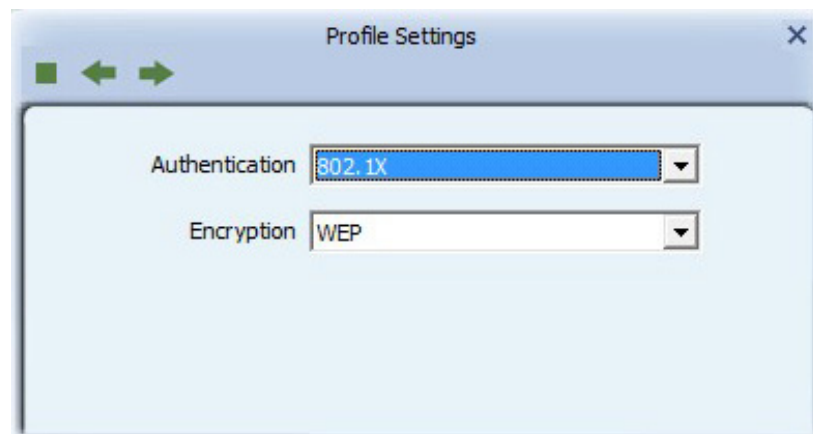


Figure 3-1-2 Authentication \ Encryption Settings in the Profile Page

- 8021X: This is introduced in the topic of [Section 3-2](#).

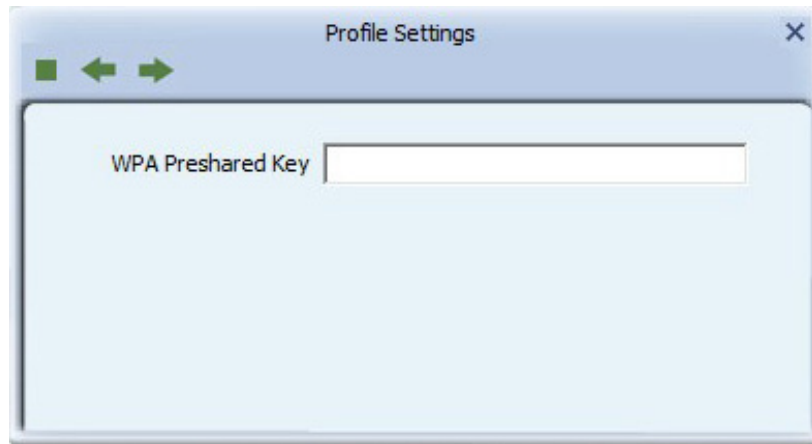


Figure 3-1-3 Pre-shared Key Configuration

- Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

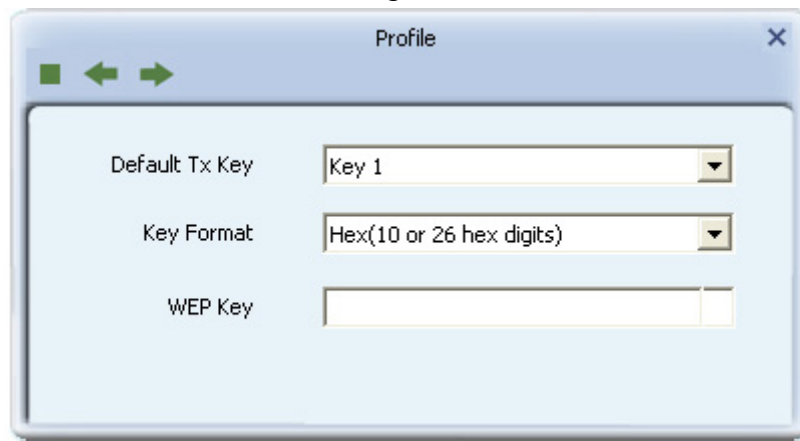
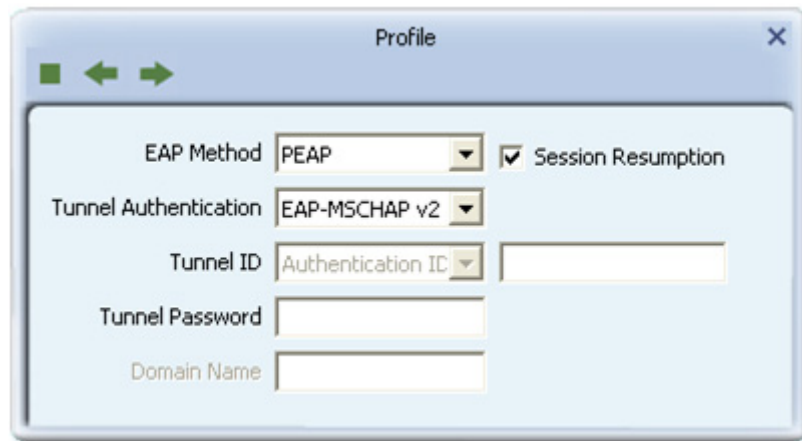


Figure 3-1-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.
 1. Hexadecimal - 40bits: 10 Hex characters.
 2. Hexadecimal - 128bits: 32Hex characters.
 3. ASCII - 40bits: 5 ASCII characters.
 4. ASCII - 128bits: 13 ASCII characters.

6.2 802.1x Setting

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.



Authentication type:

- **PEAP:** Protect Extensible Authentication Protocol. PEAP transport securely authenticates 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.
- **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.
- **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.
- **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 supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. **For tunnel authentication, only support "Generic Token Card" authentication.**
- **LEAP:** Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
- **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. **(Only support XP)**

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

Tunnel Authentication:

- **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".
- **Tunnel Identity:** Identity for tunnel.

- Tunnel Password: Password for tunnel.

ID \ PASSWORD

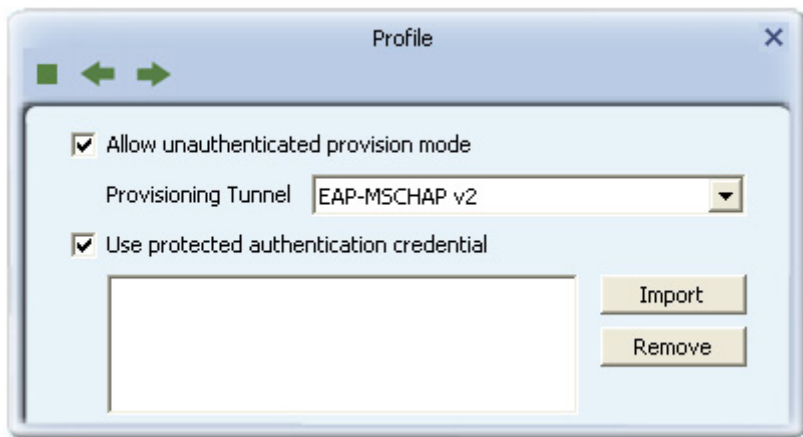
- Authentication ID/Password: The identity, password and domain name for server.
Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.
- Tunnel ID/Password: Identity and Password for the server..

Client Certification



Use Client certificate: Client certificate for server authentication.

EAP Fast



- 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.
- Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method.

Server Certification



- Certificate issuer: Select the server that issues the certificate.
- Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.
- Server name: Enter an authentication sever root.

7. Trouble Shooting

This chapter provides solutions to problems that may occur during the installation and operation of PCI Adapter. Read the descriptions below to solve your problems.

1. The PCI Adapter does not work properly.

Reinsert PCI Adapter into your PC's PCI slot. Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find PCI Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of PCI Adapter. If there is a yellow question mark, please check the following: Make sure that your PC has a free IRQ (Interrupt Request, a hardware interrupt on a PC.) Make sure that you have inserted the right adapter and installed the proper driver. If PCI Adapter does not function after attempting the above steps, remove it and do the following: Uninstall the driver software from your PC. Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2. I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.

Make sure that the PC to which PCI Adapter is associated is powered on. Make sure that PCI Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

3. What should I do when the computer with PCI Adapter installed is unable to connect to the wireless network and/or the Internet?

Check that the LED indicators for the broadband modem are indicating normal activity. If not, there may be a problem with the broadband connection. Check that the LED indicators on the wireless router are functioning properly. If not, check that the AC power and Ethernet cables are firmly connected. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points. In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it might be necessary to set up one client to establish a BSS (Basic Service Set) and wait briefly before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it. Check that the Network Connection for the wireless client is configured properly. If Security is enabled, make sure that the correct encryption keys are entered on both PCI Adapter and the access point.