WLAN 802.11 A/B/G/N MINI-PCI WIRELESS RADIO MODULE USER MANUAL

MODEL: X52-HN

Version 1.0 – 27 August 2010

Copyright Statement

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates; uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated.

Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

If this device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Important Note:

This module is intended for an OEM integrator. The OEM integrator is still responsible for the FCC compliance requirement of the end product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

Users Manual Of The End Product

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Label On The End Product

The final end product must be labeled in a visible area with the following "Contains FCC ID: UWT-X52-HN". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label:

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Table of Contents

Copyright Statement **3**

FCC Statement **3**

Users Manual Of The End Product **4**

Label On The End Product **4**

1. Introduction **6**

1.1 System Requirements 6

2. Driver/Utility Installation / Uninstallation **7**

2.1 Installation 7
2.2 Additional Setup Processes 11
2.3 Uninstallation 11

3. Connecting to an Existing Network **15**

4. Additional Note for Windows XP **19**

5. Modifying a Wireless Network **24**

5.1 Infrastructure Mode and Ad Hoc Mode 24
5.2 Modifying a Wireless Network 25
5.3 Default Settings Windows XP Zero-Configuration 30

Appendix A: FAQ about WLAN **31**

1. Introduction

Thank you for purchasing the WLAN 802.11 a/b/g/n mini-card Module that provides the easiest way to wireless networking. This User Manual contains detailed instructions in the operation of this product. Please keep this manual for future reference.

1.1 System Requirements

A laptop PC containing:

- 50 MB of free hard disk space (minimum)
- 256 MB of RAM or later (recommended)
- 900 MHz processor or higher
- Microsoft® Win™ 2000/XP/Vista

2. Driver/Utility Installation / Uninstallation

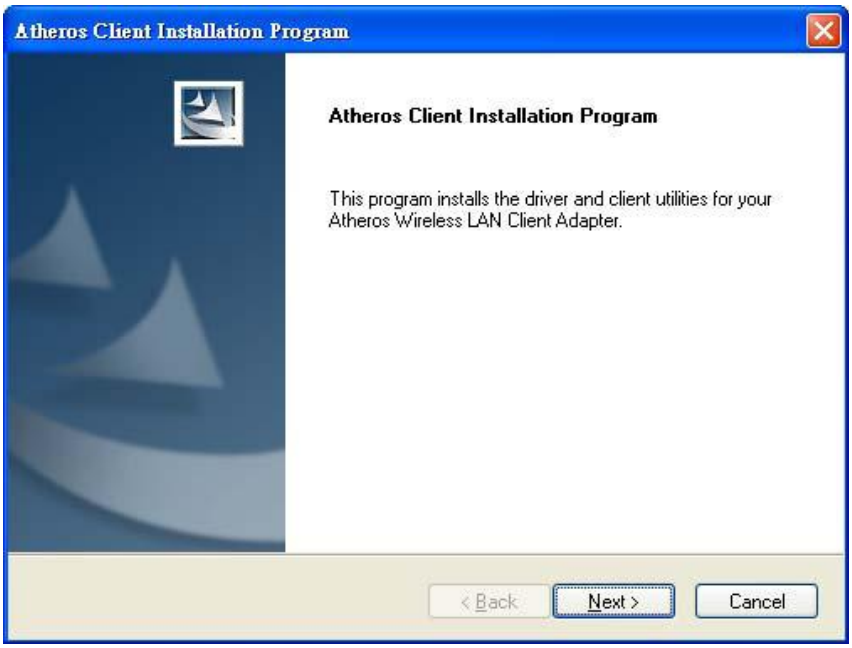
2.1 Installation

Note: The Installation Section in this User Manual describes the first-time installation for Windows. To re-install the driver, please first uninstall the previously installed driver. See Chapter 2.3 “Uninstallation” in this User Manual.

Follow the steps below to complete the driver/utility installation:

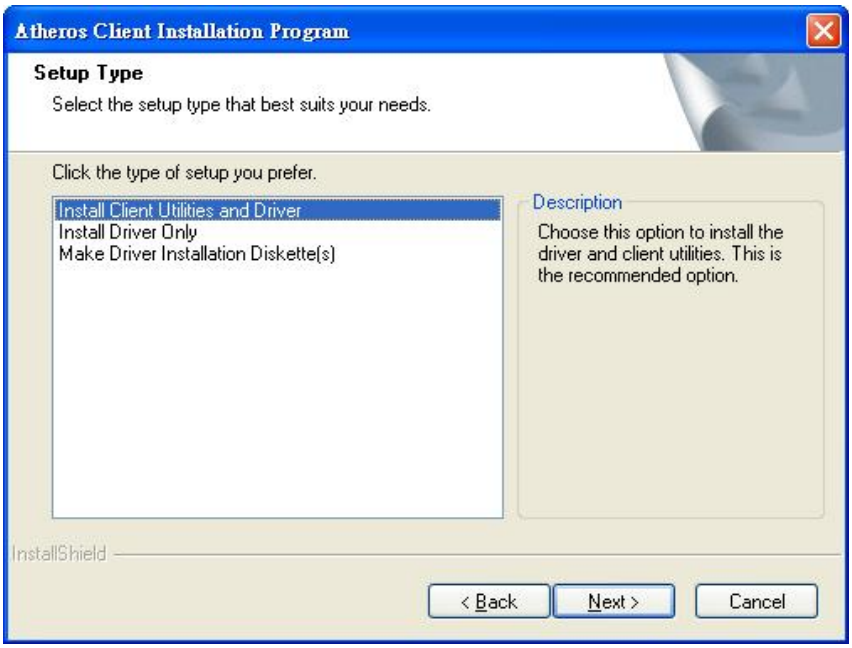
1. Install you card in your laptop and insert the **Installation Software CD** into the CD-Rom Drive.

2. Click **“Next”**.

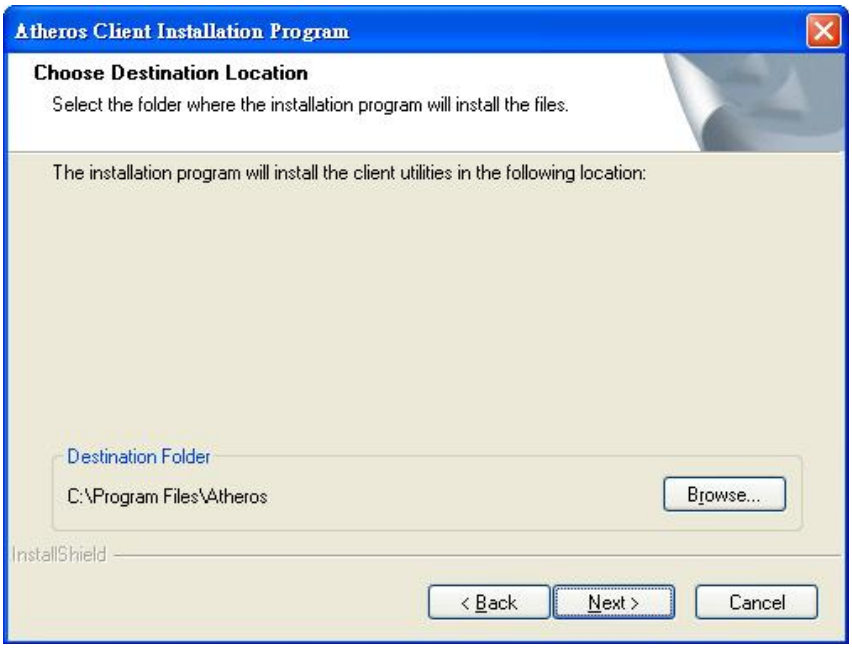


3. Read the **License Agreement** and choose **“I accept the items of the license agreement”**, then click **“Next”**.

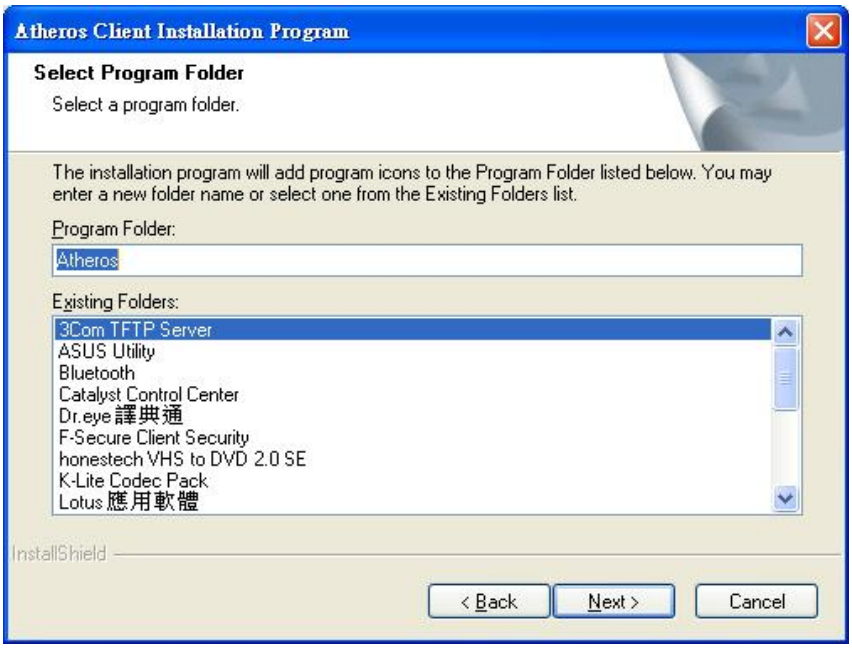
4. Choose this option to install the driver and client utilities, and click **"Next"**.



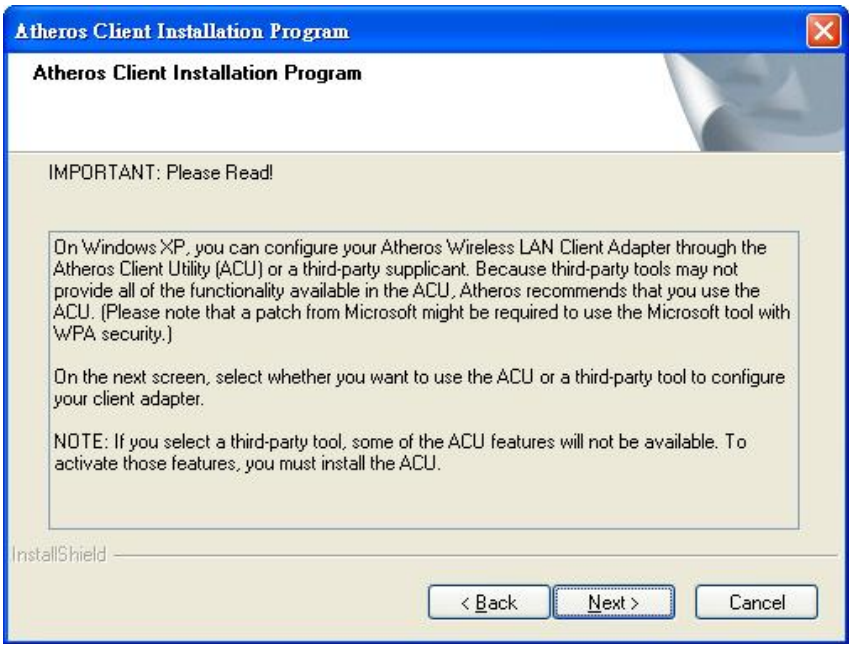
5. Click **"Next"** to continue or click **"Browse"** to choose a destination folder.



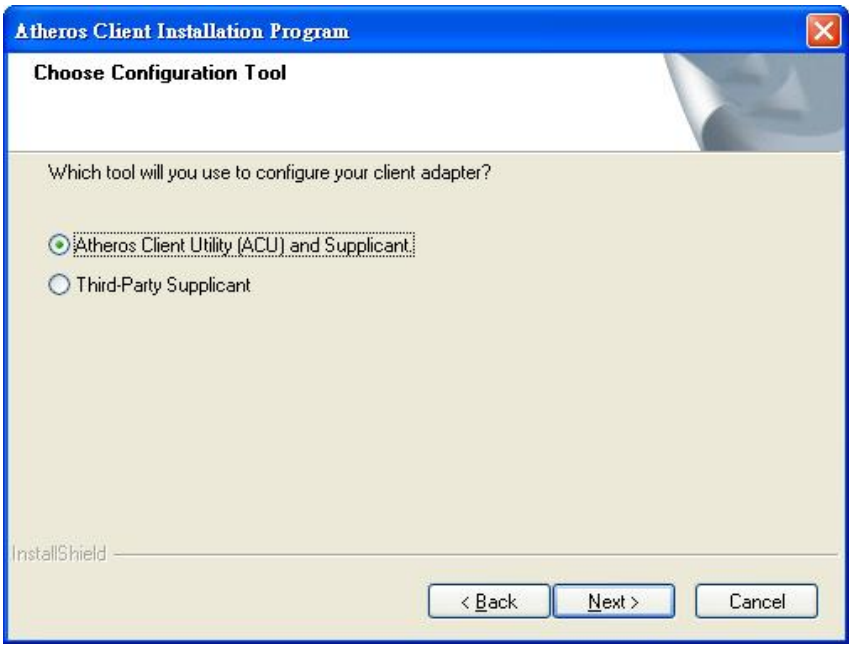
6. Click **"Next"** to continue or change the name of the program folder.



7. Click **"Next"**.



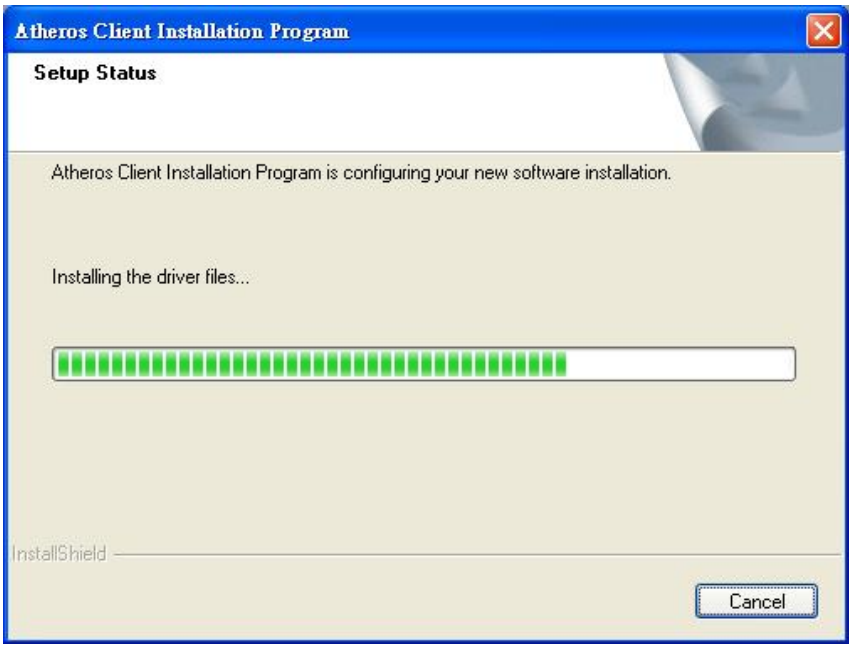
8. Choose the configuration tool for your client card and click **"Next"** to continue.



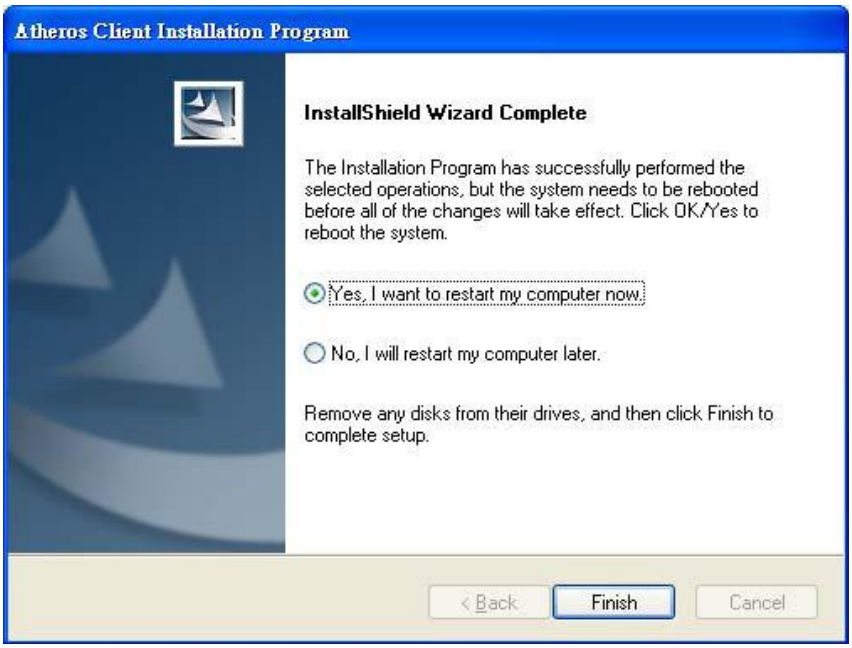
9. Click **"Yes"** to continue.

10. Click **"OK"** to continue.

11. Installing process.



12. Reboot your computer.



2.2 Additional Setup Processes

During software installation procedure, each operating system may prompt different specific options:

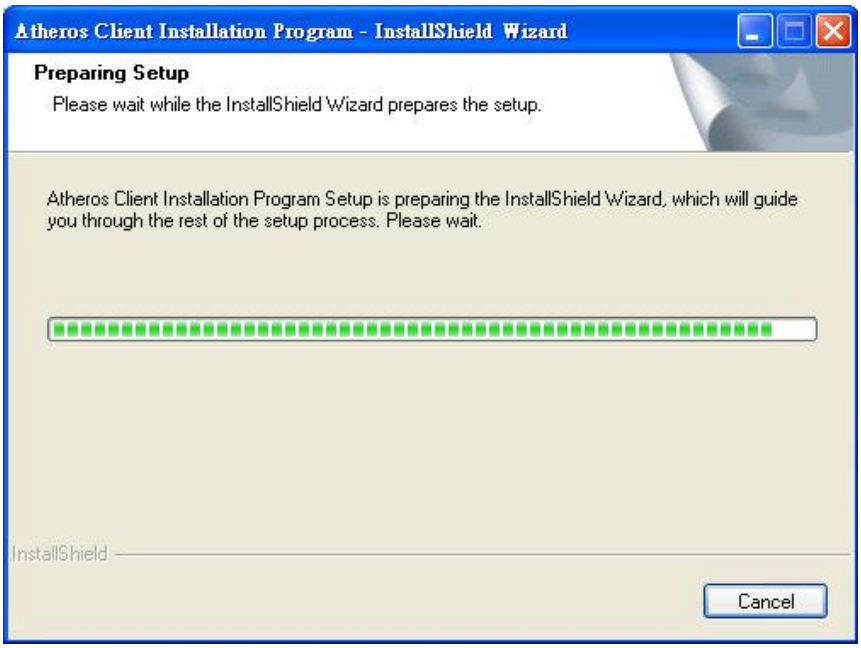
1. **Windows 2000/XP/Vista:** Select “Install the software automatically” when the window with this option appears, and then click “Next” to continue installation.

2.3 Uninstallation

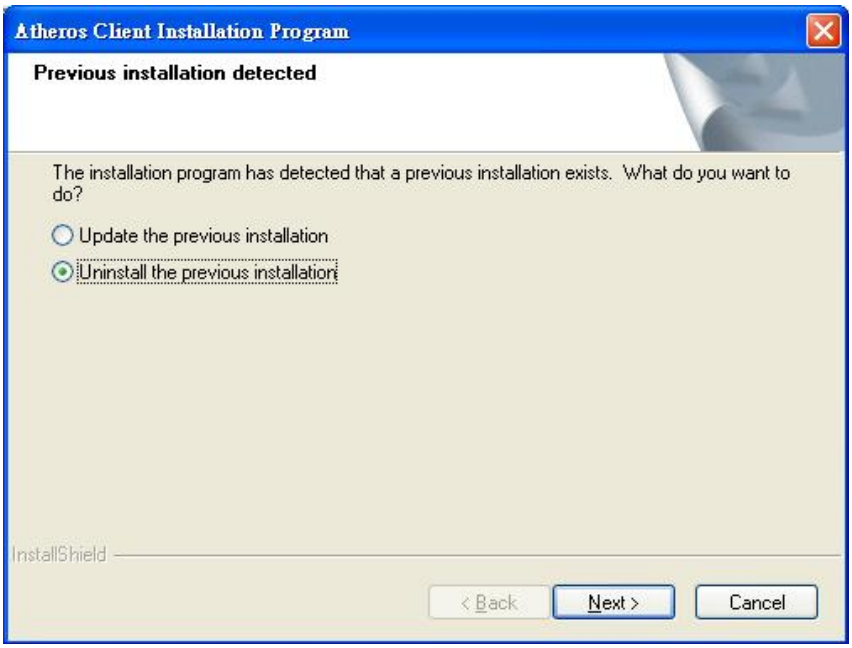
Note: Before uninstallation, please close all running programs.

1. Click Start>Programs>Control Panel >Install/uninstall program>Atheros client installation program>.

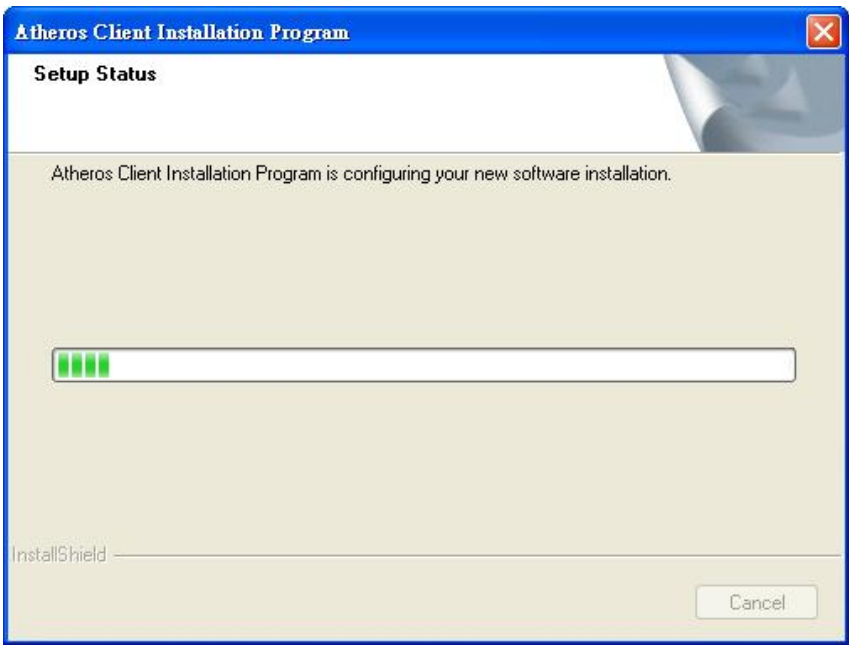
2. Choose **"Remove"**. Click **"Next"**.



3. Choose **"Uninstall the previous installation"** and click **"Next"** to start **Uninstall**.

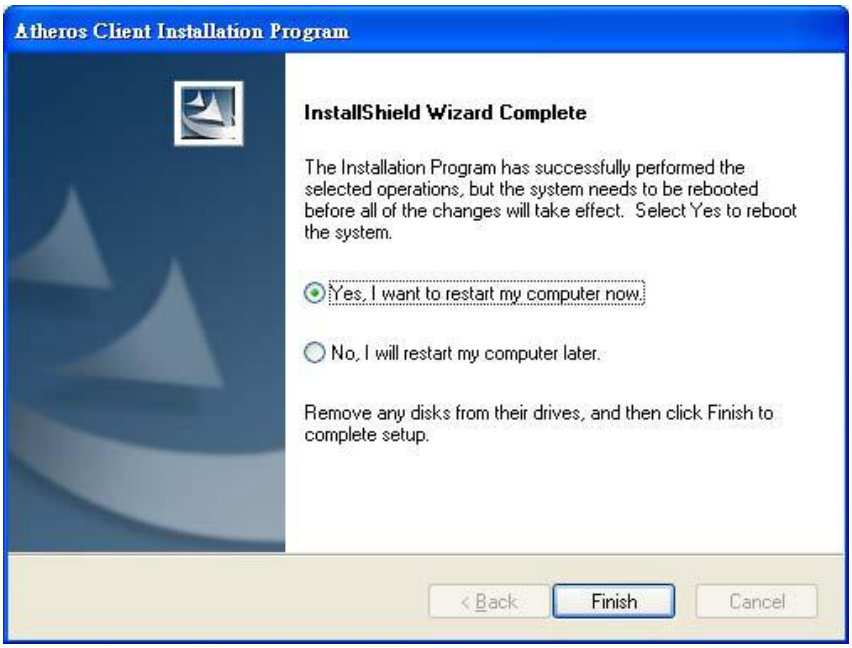


4. Click **"OK" or "Yes"** to start **Uninstall**.



5. Click **“Yes” to remove the profiles and click “No” to remove your profiles.**

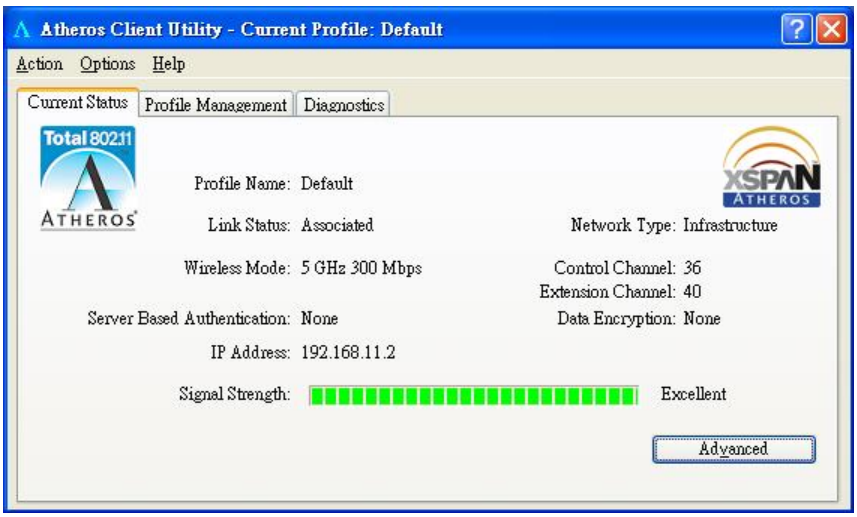
6. Click **"Finish"** and reboot your computer. The **Uninstall** is now completed.



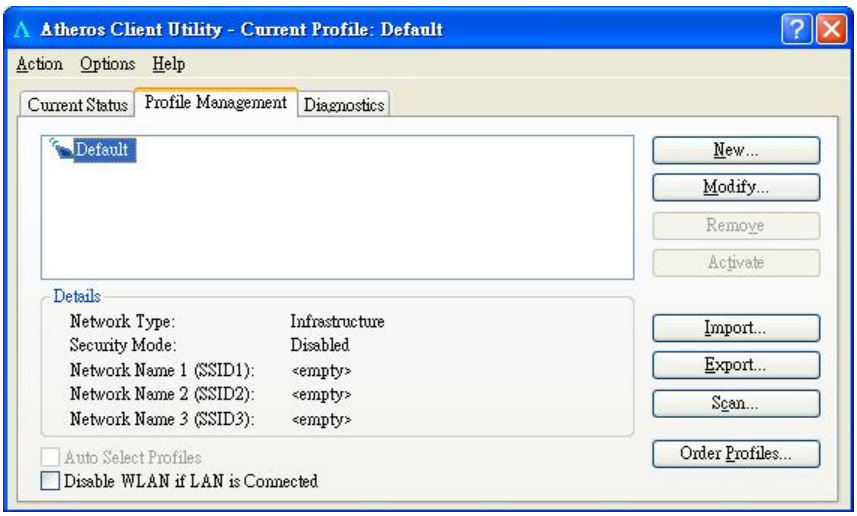
3. Connecting to an Existing Network

1. Double click the shortcut icon of Atheros Client Utility on the desktop, and the Configuration window appears.

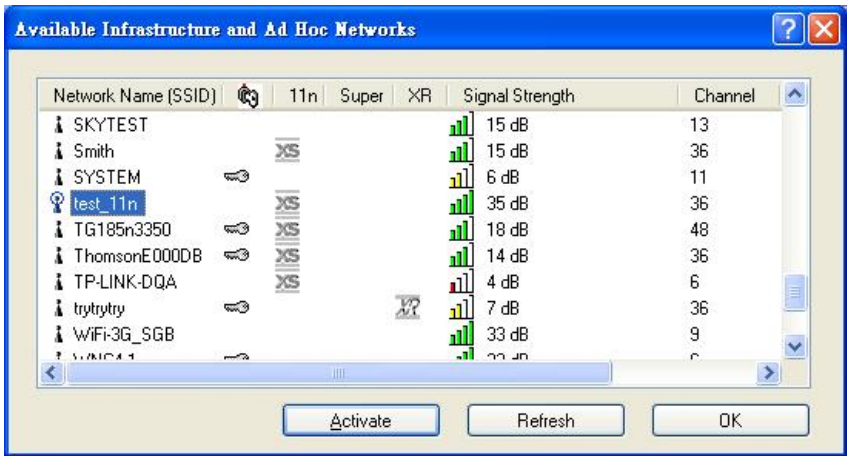
2. Click “Profile Management” tab.



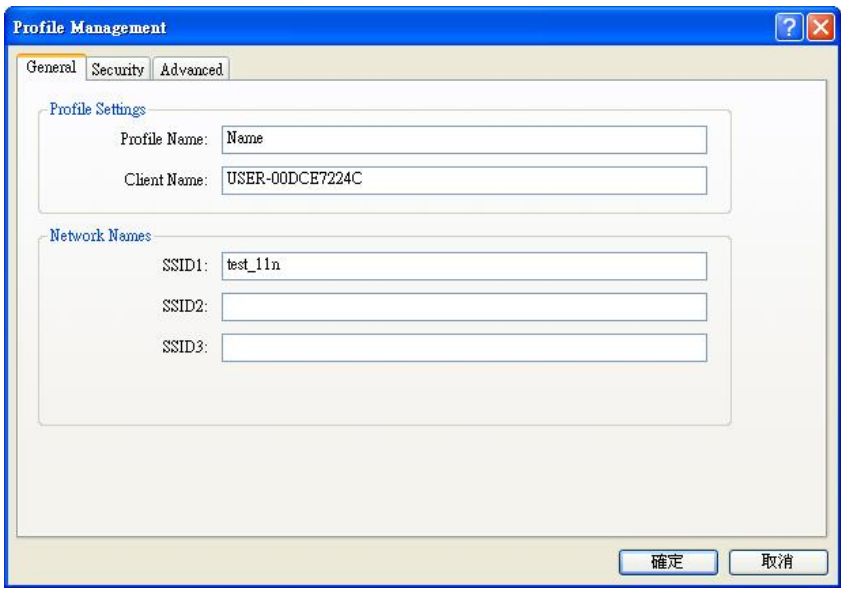
3. Click “Scan”.



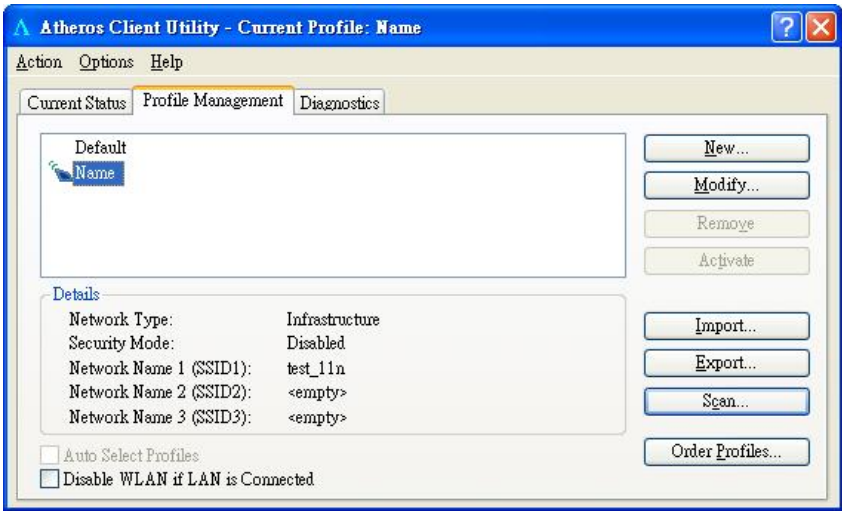
4. Choose which AP you want to link and click “Activate”.



5. Give a Profile name for the SSID and Click “OK”.

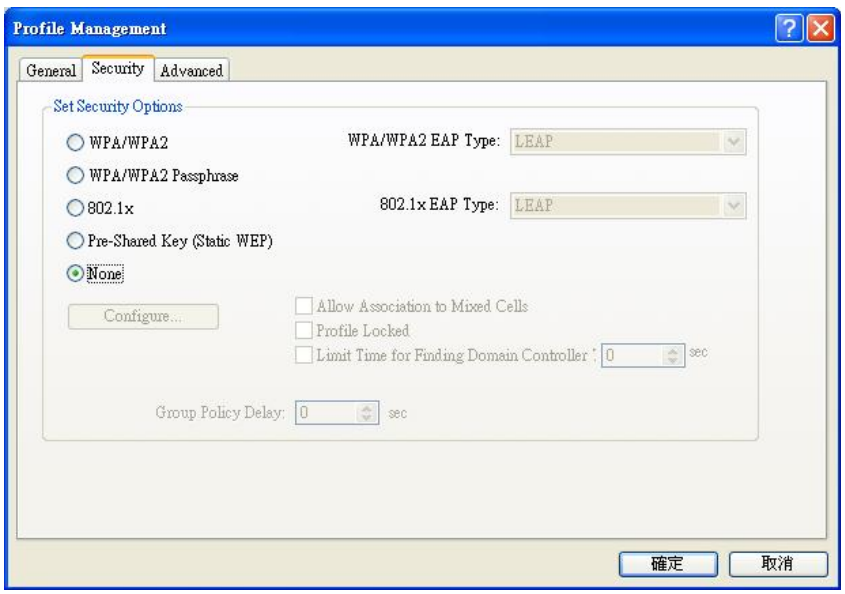


6. Give a Profile name for the SSID and Click “OK”.

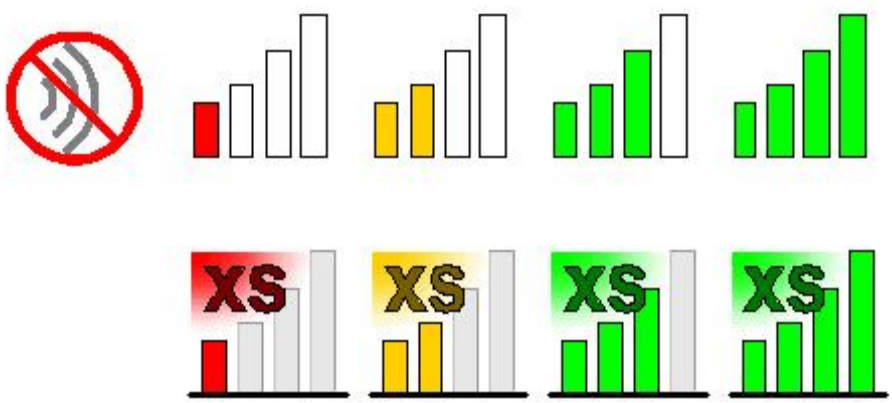


Note: To automatically connect to the network with the strongest signal, select Enable Smart Selection. Any displays in Profile List.

7. If the chosen network has security enabled, the Security tab displays. Select the security option used by the network. Contact the network administrator for the correct settings. About the security setting process, please refer to Chapter 5.



8. Once connected, you can check the signal strength from the following icon in the Windows System Tray.



4. Additional Note for Windows XP

In Windows XP, it is recommended that you use the WLAN a/b/g/n mini-card Module Configuration Utility. Before using the Utility, please follow the steps below to disable the Windows XP Zero Configuration:

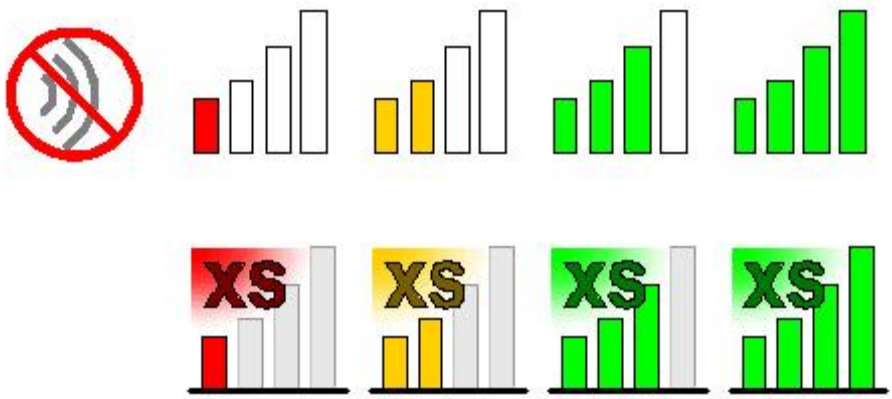
Option 1:

1. Double click the shortcut icon to open the Utility.

2. From the Windows System Tray, you should see the signal icon. Right-click it and select “Disable Zero-Configuration”.

3. Tray icon.

The tray icon appears at the bottom of the screen, and shows the signal strength using colors.



Hold the mouse cursor over the tray icon to display the current configuration profile name and association, as well as transmit and receive speed and the wireless adapter name and IP address.

Right-click on the tray icon to:

Help	Open the online help.
Open Atheros Client Utility	Launch the Atheros Client Utility (ACU). Use the ACU to configure the profile or view status and Statistics information.
Client Managed Test	Run the Client Managed Test Utility.
Preferences	Set the startup options and menu options for the ACU. Check whether the program should start automatically when Windows starts, and check the menu items that should appear on the popup menu.
Enable/Disable Radio	Enable or disable the RF Signal.
Manual LEAP Login	Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.
Reauthenticate	Reauthenticate to the access point.
Select Profile	Click a configuration profile name to switch to it. If no configuration profile exists for a connection, add a profile first.
Show Connection Status	Display the Connection Status window. This window

displays information about the connection:

Active Profile	Displays the name of the active configuration profile.
Auto Profile Selection	Shows whether auto profile selection is enabled
Connection Status	Displays whether the adapter is connected to a wireless network.
Link Quality	Lists the quality of the link connection.
SSID	Displays the SSID of the associated network.
Access Point Name	Shows the name of the access point the wireless adapter is connected to.
Access Point IP Address	Shows the IP address of the access point the wireless adapter is connected to.
Current Receive Rate	Shows the current receive rate in Mbps.
Current Transmit Rate	Shows the current transmit rate in Mbps.
Client Adapter IP Address	Displays the IP address of the wireless adapter

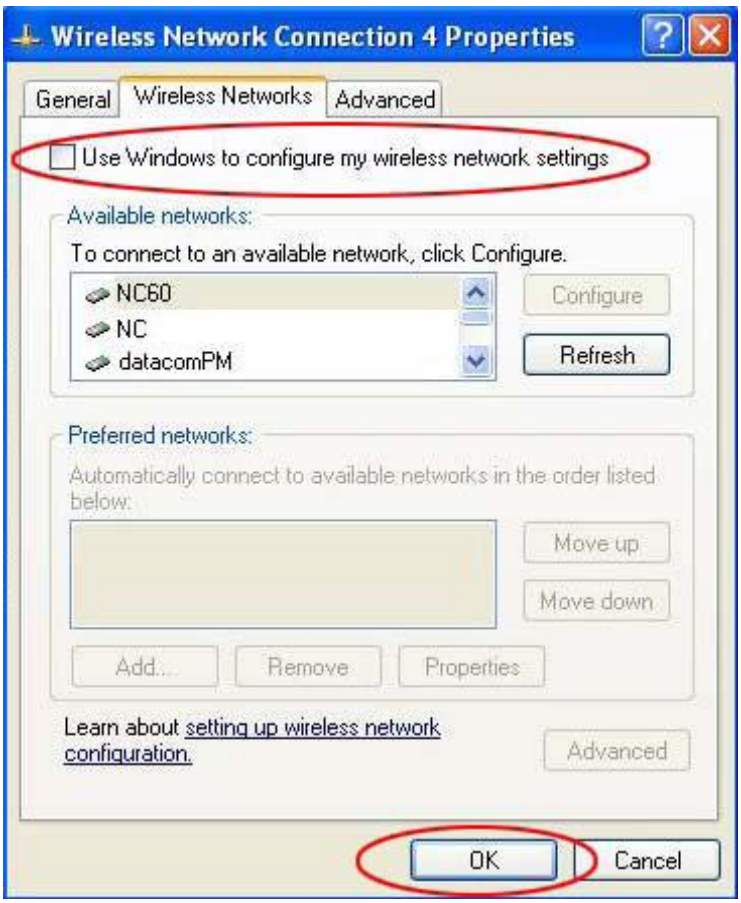
Exit Exit the Atheros Client Utility application.

Option 2:

1. Go to “Control Panel” and double click “Network Connections”.

2. Right-click “Wireless Network Connection” of “WLAN a/b/g/n mini-card Module”, and select “Properties”.

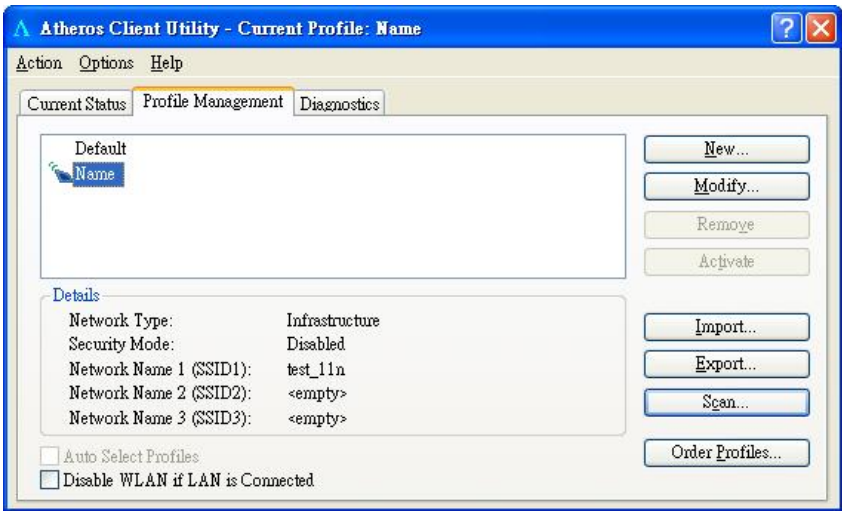
3. Select “Wireless Networks” tab, and uncheck the check box of “Use Windows to configure my wireless network settings”, and then click “OK”.



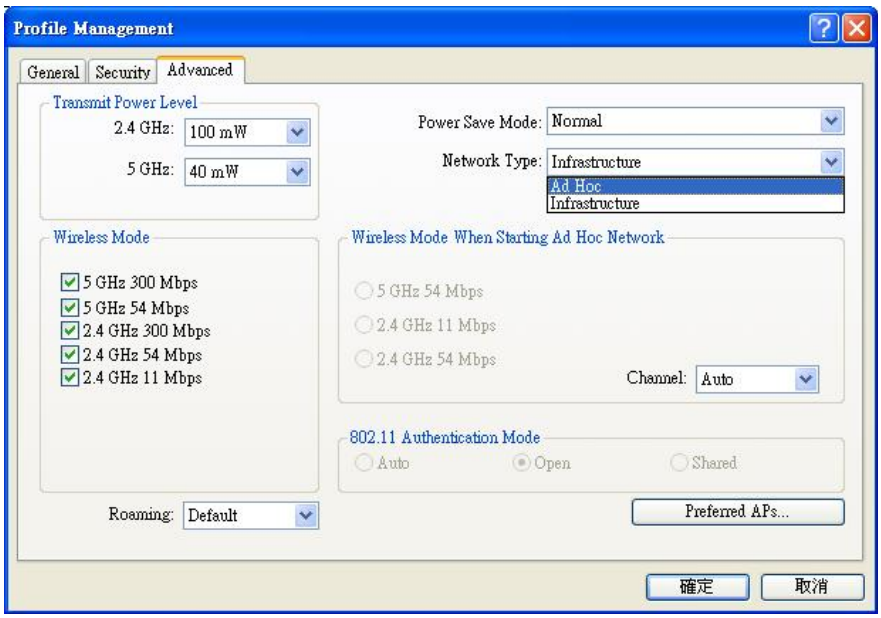
4. Creating an Ad Hoc New Network

NOTE: Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and does not have radar detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.

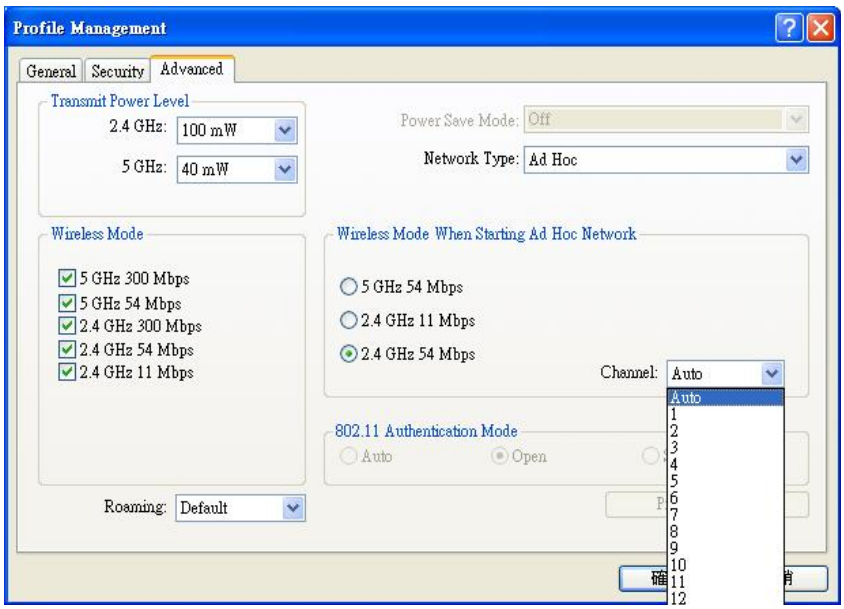
1. In the **Profile Management** tab, click **New**.



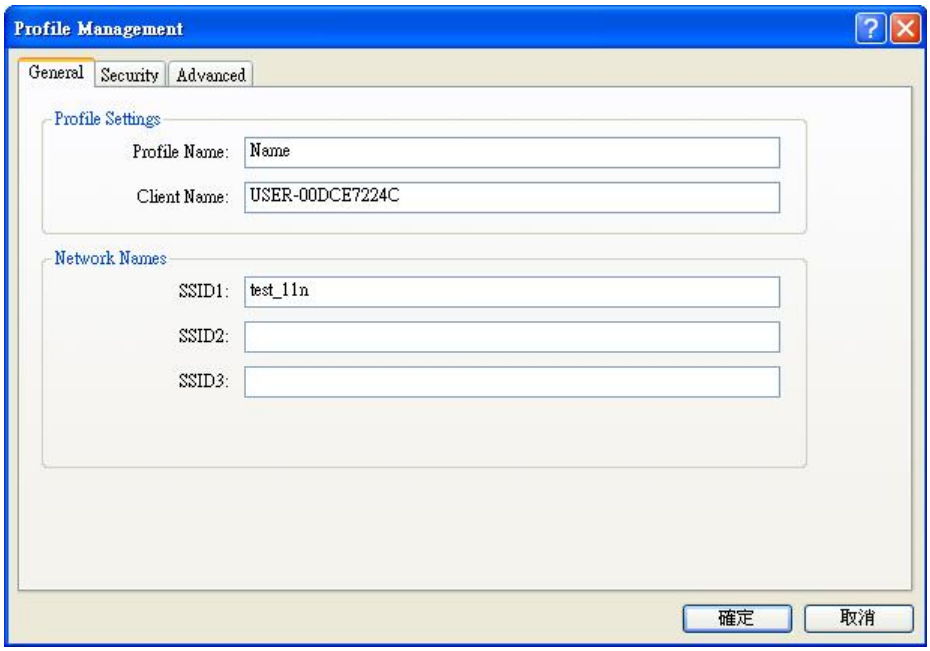
2. In the **Profile Management** window, click **Advance** tab and choose **“Ad Hoc”** in the Network Type function**.**



3. Select the “Channel” tab and click “**OK**”.



4. Give a Profile name for the SSID and Click "**OK**" to save the settings.



5. Click the **Security** tab. If not using security, select **None**. Please refer to the chapter 5 for the security setting.

5. Modifying a Wireless Network

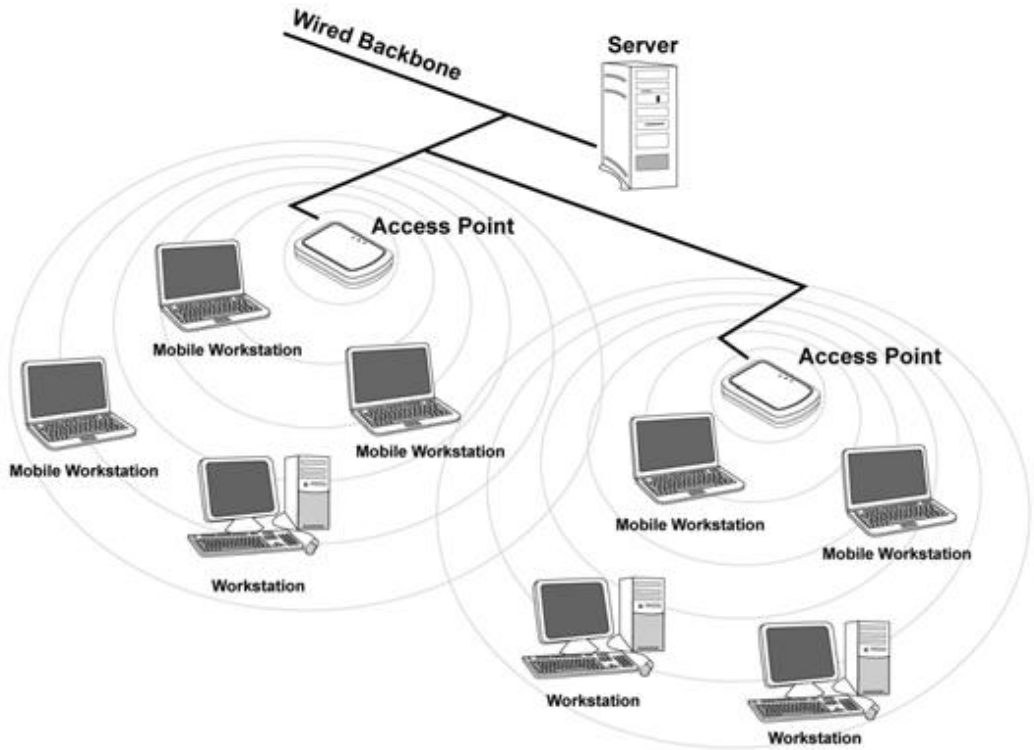
5.1 Infrastructure Mode and Ad Hoc Mode

You can set the Wireless Network Adapter to work in either **Infrastructure mode** or **Ad Hoc mode**.

NOTE: Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and do not have radar detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.

Infrastructure Mode

In infrastructure mode, devices communicate with each other by first going through an Access Point (AP). Wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations, it is referred to as a BSS (Basic Service Set).



Ad Hoc Mode

Ad-hoc mode is also called “peer-to-peer mode” or “Independent Basic Service Set (IBSS)”. In ad hoc mode, devices communicate directly with each other without using an Access Point (AP).

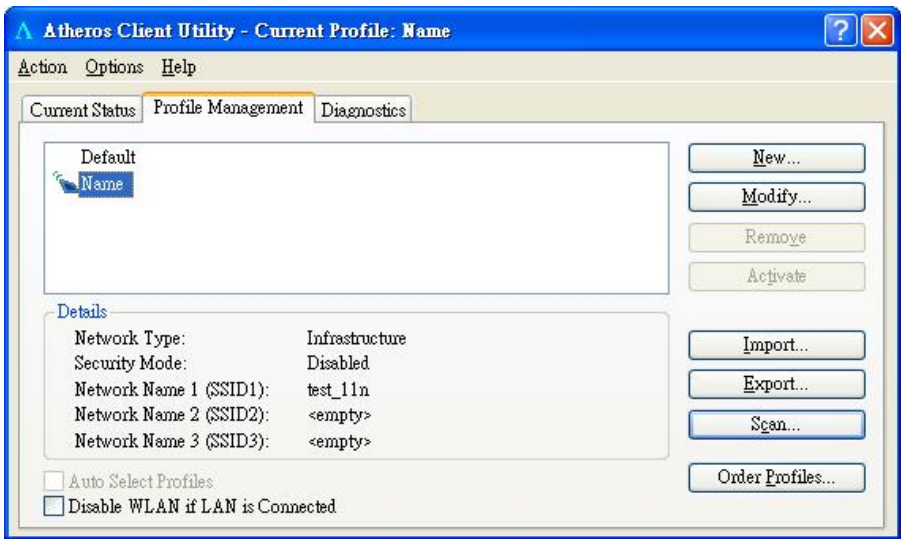
NOTE: Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and do not have radar detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.

5.2 Modifying a Wireless Network

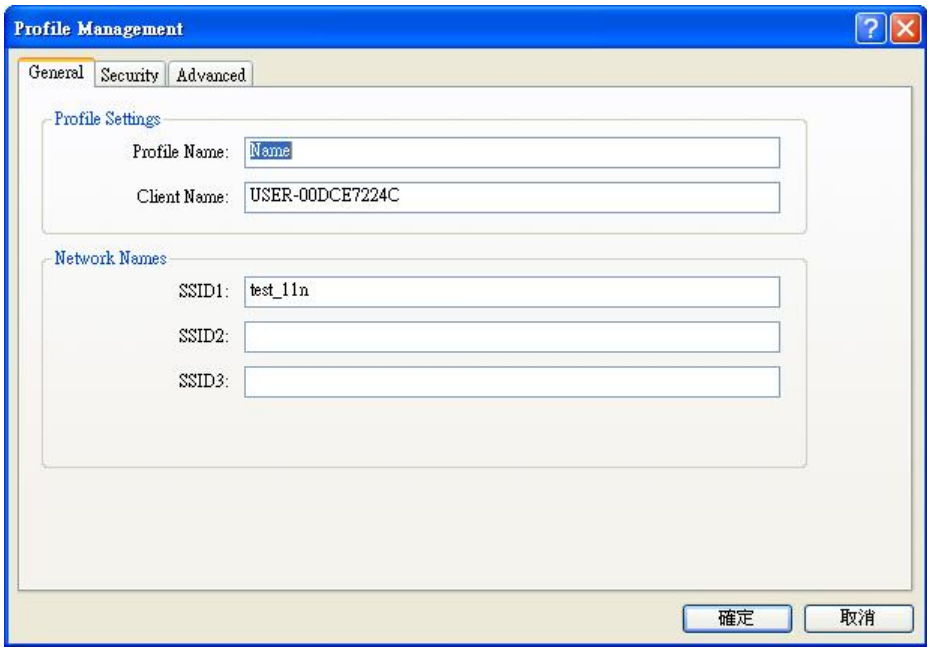
1. Open “WLAN a/b/g/n mini-cardModule Configuration” by double clicking the shortcut icon on the desktop.

Note! If there’s no network name listed in the “Profile List”, click Refresh button and double click a Network Name from Available Networks. The chosen Network Name is listed in the Profile List.

2. From the Profile List, select one Profile and click **Modify** button.



3. Select **Profile Modify** tab and edit the settings. Click **OK** to save the modifications.



Profile Name	Identifies the configuration profile. This name must be unique. Profile names are not case sensitive.
Client Name	Identifies the client machine.
Network Names (SSIDs)	The IEEE 802.11 wireless network name. This field has a maximum limit of 32 characters. Configure up to three SSIDs (SSID1, SSID2, and SSID3).

4. Select **Security** tab and choose the security mode.

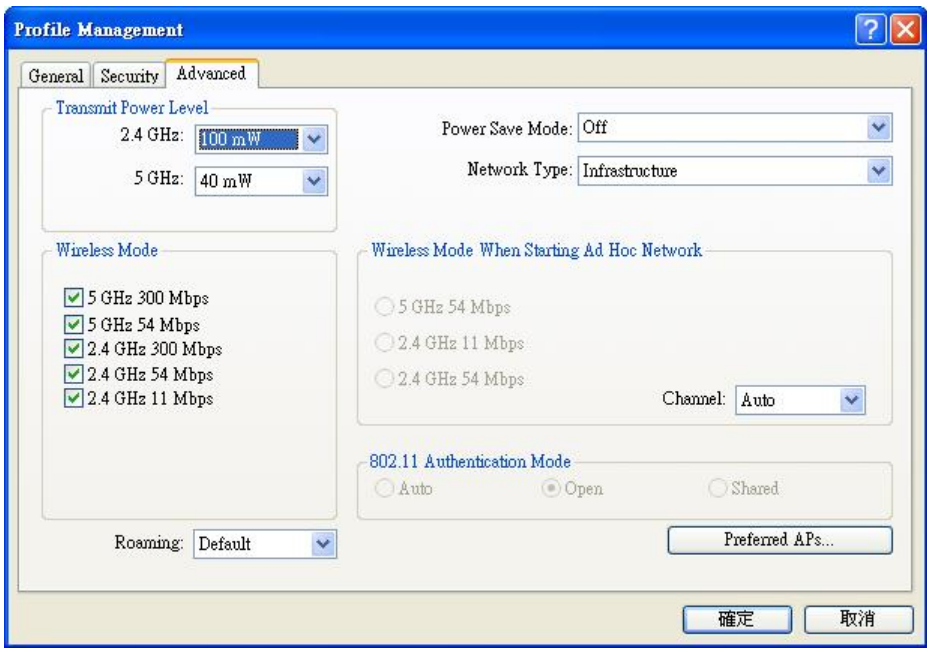
Note: ***Check with your Network Administrator for the security features supported by your AP.***

Set Security Options	The type of security mode the station is using. The options include the following: • WPA/WPA2/CCKM • WPA/WPA2 Passphrase • 802.1x • Pre-Shared Key (Static WEP) • None These options define the unique encryption key for network configuration security.
WPA/WPA2	Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA/WPA2 opens the WPA/WPA2 EAP drop-down menu. The options include: • EAP-FAST • EAP-TLS • EAP-TTLS • EAP-SIM • PEAP (EAP-GTC) • PEAP (EAP-MSCHAP V2)

	• LEAP
WPA/WPA2 Passphrase	Enables WPA/WPA2 Passphrase security. Click on the Configure button and fill in the WPA/WPA2 Passphrase.
802.1x	Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include: • EAP-FAST • EAP-TLS • EAP-TTLS • EAP-SIM • PEAP (EAP-GTC) • PEAP (EAP-MSCHAP V2) • LEAP If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.
Pre-Shared Key (Static WEP)	Enables the use of pre-shared keys that are defined on both the access point and the station. To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the Define Pre-Shared Keys window. If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.
None	No security (not recommended).
Allow Association to Mixed Cells	Check this check box if the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter. Otherwise, the client is unable to establish a connection with the access point.
Limit Time for Finding Domain Controller To	Check this check box and enter the number of seconds (up to 300) after which the authentication process times out when trying to find the domain controller. Entering zero is like unchecking this check box, which means no time limit is imposed for finding the domain controller. ***Note: The authentication process times out whenever the authentication timer times out or the time for finding the domain controller is reached.***
Group Policy Delay	Specify how much time elapses before the Windows logon process starts group policy. Group policy is a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network

authentication occurs. Valid ranges are from 0 to 65535 seconds. The value that you set goes into effect after you reboot your computer with this profile set as the active profile. This drop-down menu is active only if you chose EAP-based authentication.

6. Select **Advanced** tab.



Transmit Power Level

Selects the transmit power level for 80211b/g or 802.11a in mW. Actual transmit power may be limited by regulatory domain or hardware limitations. Also note that administrator has the privilege of locking these power levels, so that these values are pre-selected and not editable.

Power Save Mode

Specify:

• Maximum mode causes the access point to buffer incoming messages for the wireless adapter. The adapter periodically polls the access point to see if any messages are waiting.

• Normal uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets.

• Off turns power saving off, thus powering up the wireless adapter continuously for a short message response time.

Network Type

Specifies the network as either infrastructure (access point mode) or ad hoc.

Wireless Mode

Specifies 5 GHz 54Mbps, 5 GHz 300Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11Mbps, 2.4 GHz 300Mbps or Quality of Service operation in an access point network.

The wireless adapter must match the wireless mode of the access point it associates to.

Wireless Mode when Starting Ad Hoc Network

Specifies 5 GHz 54 Mbps, 5 GHz 108 Mbps, or 2.4 GHz **an** 54/11 Mbps to start an ad hoc network if no matching

network name is found after scanning all available modes.

This mode also allows selection of the channel the wireless adapter uses. The channels available depend on the regulatory domain. If the adapter finds no other ad hoc adapters, this selection specifies the which channel with the adapter starts the ad hoc network with.

The wireless adapter must match the wireless mode and channel of the clients it associates to.

802.11 Authentication Mode

Select what mode the wireless adapter uses to authenticate to an access point:

• Auto causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails.

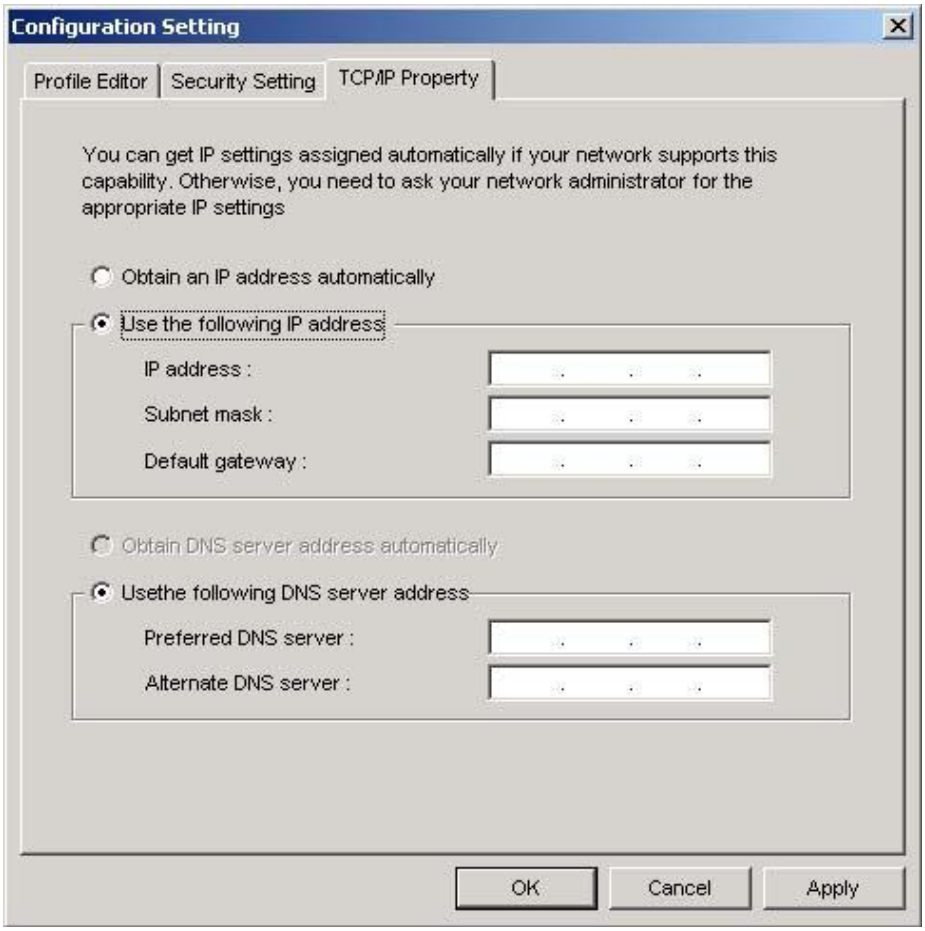
• Open enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.

• Shared only allows the adapter to associate with access points that have the same WEP key.

Roaming Strength

Select the roaming level to suit the roaming aggressiveness of the client. Five roaming levels ranging from **Very Low** to **Very High** allow for the best performance in different environments such as home or office.

7. Select “TCP/IP Property” tab. Enter the settings and click “OK” to save the settings.



- If the network uses DHCP server, choose **Obtain an IP address automatically**.
- If the network does not use DHCP server, choose **Use the following IP address** to set the relative settings. For the IP configuration information, please contact the network administrator.

5.3 Default Settings Windows XP Zero-Configuration

You may also choose the default parameters and directly proceed to Windows XP zero-configuration through the steps below:

1. Go to “Control Panel” and open “Network Connections”.

2. Right-click the Wireless Network Connection of “WLAN a/b/g/n mini-card Module”, and make sure this connection is **Enabled**.

3. Right-click the Wireless Network Connection of “WLAN a/b/g/n mini-card Module”, and then click “Properties”.

4. Select “Wireless Networks” tab and select “Use Windows to configure my wireless network settings” check box.

Note: Clear the check box of “Use Windows to configure my wireless network settings” will disable automatic wireless network configuration.

Appendix A: FAQ about WLAN

1. Can I run an application from a remote computer over the wireless network?

This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine whether it supports operation over a network.

2. Can I play computer games with other members of the wireless network?

Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

3. What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

4. What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

5. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

6. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

7. What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

8. What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and

quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone. As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.