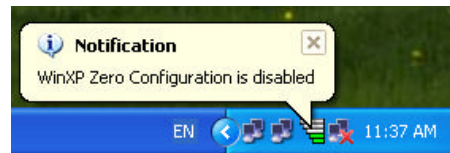
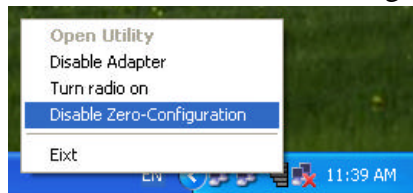


Additional Note for Windows XP

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

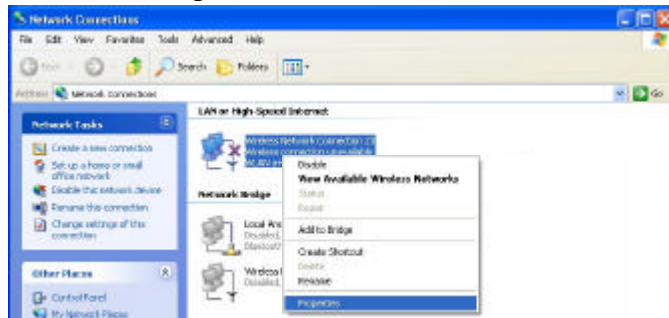
Option 1:

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”.

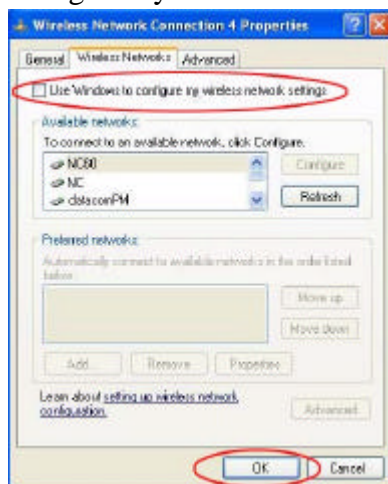


Option 2:

1. Go to “Control Panel” and double click “Network Connections”.
2. Right-click “Wireless Network Connection” of “WLAN a+b+g mini-PCI Module”, and select “Properties”.

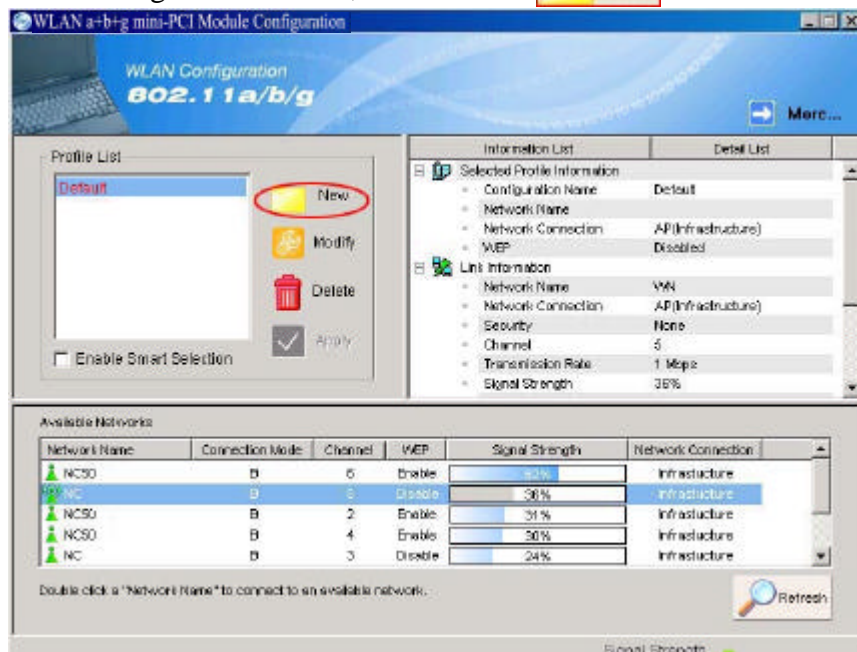


3. Select “Wireless Networks” tab, and uncheck the check box of “Use Windows to configure my wireless network settings”, and then click “OK”.

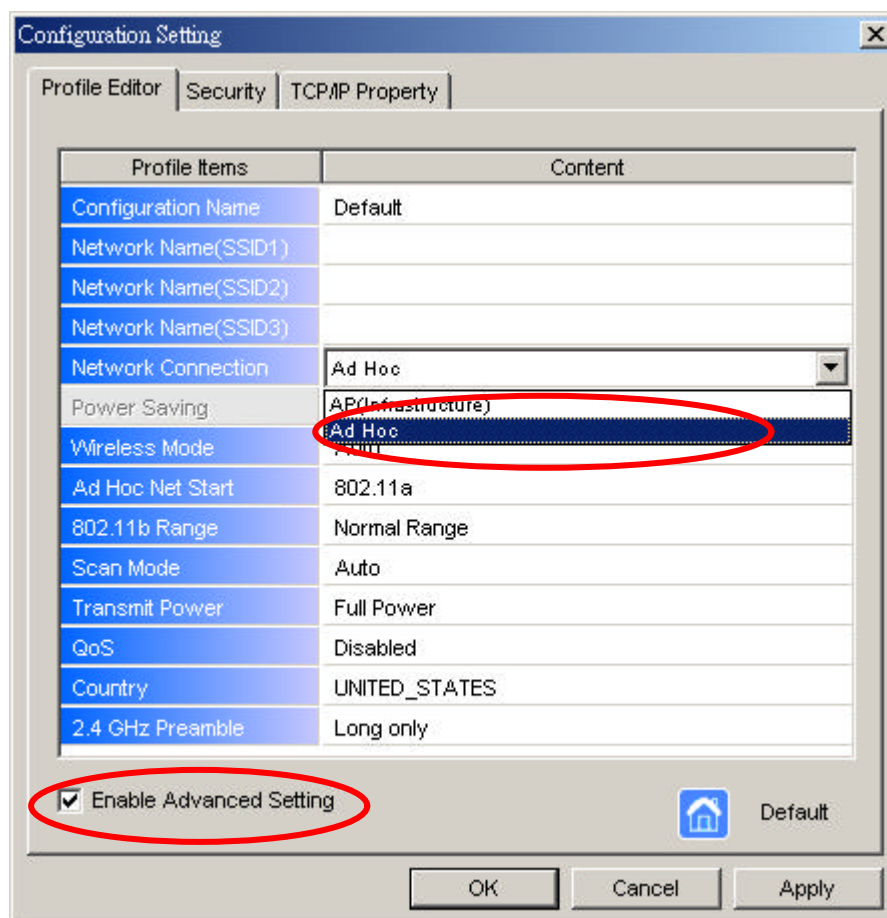


4. Creating an Ad Hoc New Network

1. In the Configuration window, click New 



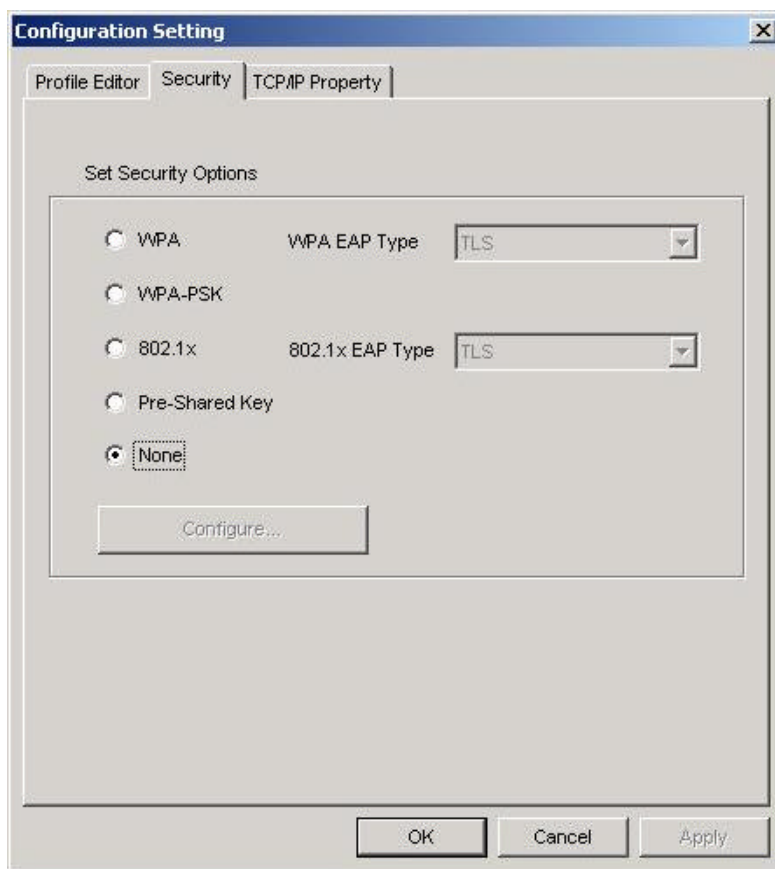
2. Select the "Profile Editor" tab.



3. Choose the check box of **Enable Advanced Setting** to edit all settings.
4. If joining or creating an Ad-Hoc network, choose **Ad Hoc**.
5. If the correct country is not selected, select the country where the computer is located.

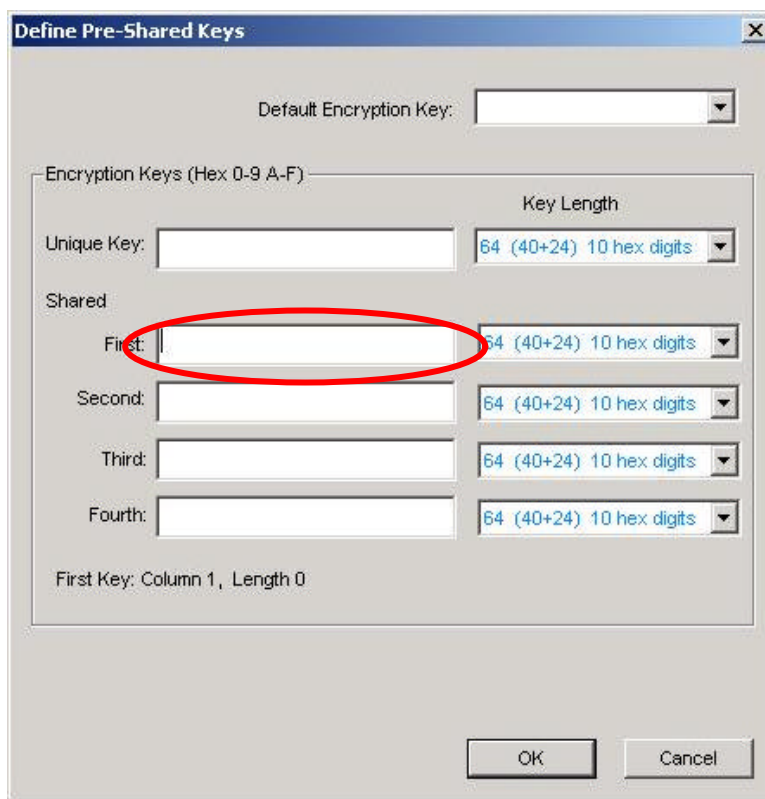
ALERT! Different countries have different regulations that affect which channels can be used. You should always choose the country where you are physically located to avoid using an illegal channel.

6. Click **OK** (or **Apply** if using the other tabs) to save the settings.
For details of each setting, refer to [Modifying a Wireless Network on page 20](#).
7. Click the **Security** tab. If not using security, select **None**.



8. If security is used, select **Pre-Shared Key** and click on the **Configure** button.

9. Enter an encryption key in the **Shared: First** field.



The screenshot shows a dialog box titled "Define Pre-Shared Keys". At the top, there is a "Default Encryption Key:" label followed by a text input field. Below this is a section titled "Encryption Keys (Hex 0-9 A-F)". Inside this section, there is a "Unique Key:" label with a text input field and a "Key Length" dropdown menu. The "Key Length" dropdown is set to "64 (40+24) 10 hex digits". Below the "Unique Key" section, there is a "Shared" section. The "Shared" section has four rows, each with a label ("First:", "Second:", "Third:", "Fourth:") and a text input field. The "First:" text input field is circled in red. To the right of each text input field is a "Key Length" dropdown menu, all of which are set to "64 (40+24) 10 hex digits". At the bottom of the dialog box, there are "OK" and "Cancel" buttons. A status bar at the bottom left says "First Key: Column 1, Length 0".

10. Click **OK** (or **Apply** if using the other tabs) to save the settings. The new **Network Name** is listed in the **Profile List**.

The driver does not allow channel selection in Ad-Hoc mode. Instead, the driver starts with an initial channel then checks channel status. If the channel is busy, the driver automatically uses a different channel.

For details of each setting, please see chapter 5.

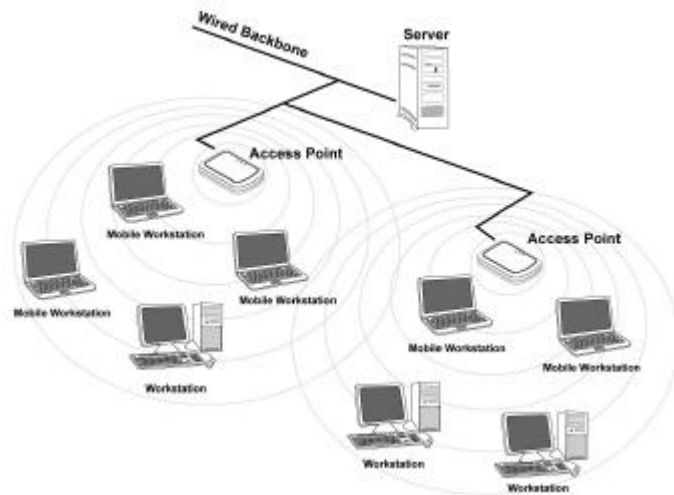
5. Modifying a Wireless Network

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**.

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).

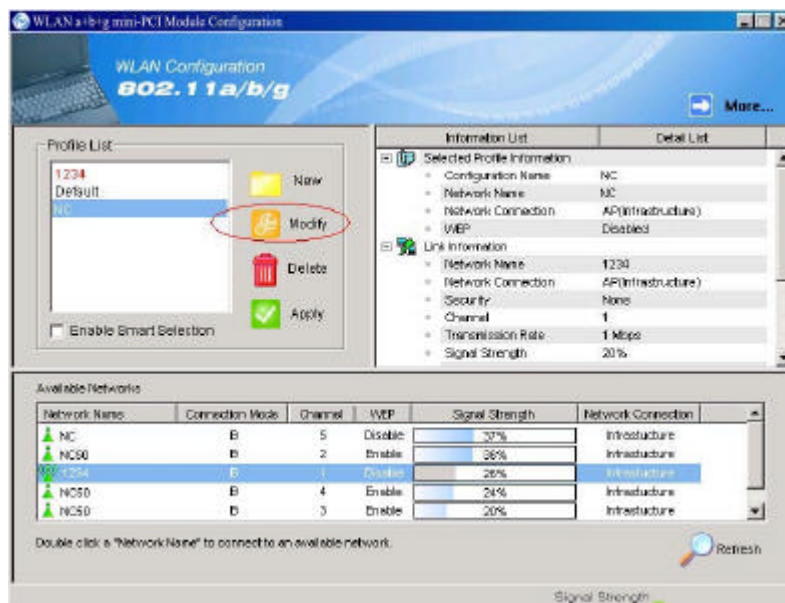


5.2 Modifying a Wireless Network

1. Open “WLAN a+b+g mini-PCI Module 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 Editor** tab and edit the settings. Click **OK** to save the modifications.

The screenshot shows a 'Configuration Setting' dialog box with three tabs: 'Profile Editor', 'Security', and 'TCP/IP Property'. The 'Profile Editor' tab is active, displaying a table of configuration items and their current values. Below the table, there is a checkbox for 'Enable Advanced Setting' which is checked, a 'Default' button with a house icon, and 'OK', 'Cancel', and 'Apply' buttons at the bottom.

Profile Items	Content
Configuration Name	Default
Network Name(SSID1)	
Network Name(SSID2)	
Network Name(SSID3)	
Network Connection	AP(Infrastructure)
Power Saving	Normal
Wireless Mode	Auto
Ad Hoc Net Start	802.11a
802.11b Range	Normal Range
Scan Mode	Auto
Transmit Power	Full Power
QoS	Disabled
Country	UNITED_STATES
2.4 GHz Preamble	Short and Long

☒ Enable Advanced Setting

 Default

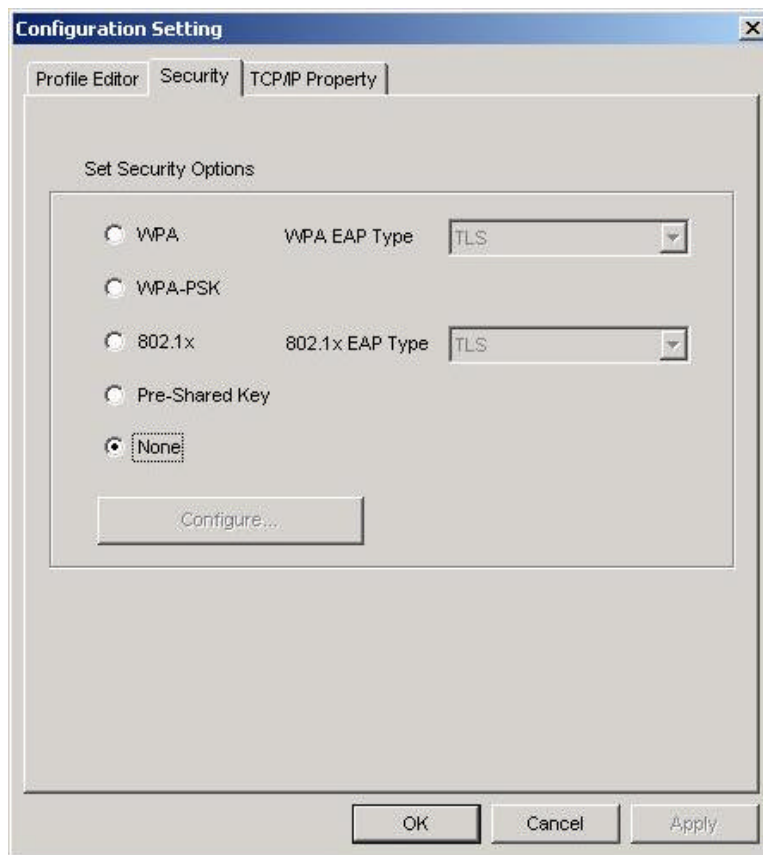
OK Cancel Apply

- **Configuration Name:** This name identifies the configuration. This name should be unique.
- **Network Name (SSID1) (SSID2) (SSID3):** The name of the wireless network. This name cannot be longer than 32 characters. If the field is set to be “ANY” or is left blank, your computer will connect to an AP with the best signal strength.
- **Network Connection:** Specifies the mode of the network. Two options are “Infrastructure” and “Ad Hoc”.
- **Power Saving:** Minimizes power consumption while maintaining network connectivity and high data transfer performance. In **Ad Hoc** mode, **Power Savings** function cannot be enabled. The power management options are:
 - **Off:** PC Card is powered up at all times.
 - **Normal:** PC Card sleeps less often and stays asleep for a shorter period.
 - **Maximum:** PC Card sleeps more frequently and stays asleep as much as possible.
- **Wireless Mode:** Three options are “802.11b”, “802.11a”, “802.11g”

- **Ad Hoc Net Start:** Specifies a band to establish an Ad Hoc network if no matching SSID is found. three options are available: 802.11b, 802.11a, and 802.11g.
- **802.11b Range:** Options are **Normal Range** and **Extended Range**. This function can let user to determine the transfer range in 802.11b mode. Extended Range can prolong the transfer range with a lower data transmitting rate.
- **Scan Mode:** Options are **Active Scan**, **Passive Scan** and **Auto**. In Active Scan, the driver sends out the probe request frames from each channel and collects the response frames from the responding. In Passive Scan, the driver scan each requested channel, listening the beacons on each channel.
- **Transmit Power:** This setting allows you to change the output power of the PC Card to increase or decrease the coverage area, but can not exceed the authorized max. power output.
- **QoS:** Disables or enables the PC Card to cooperate in a network using QoS (Quality of Service).
- **Country:** Select the country where this PC Card will operate.
ALERT! Different countries have different regulations that affect which channels can be used. You should always choose the country where you are physically located to avoid using an illegal channel. (When this product sells to US, client will disable the other frequency of outside USA)
- **2.4 GHz Preamble:** Allows Ad-Hoc compatibility with other 2.4 GHz devices. Two options are **Short and Long** and **Long only**. Use **Long Only** when configuring the client for an 802.11b RoamAbout AP wireless network.

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

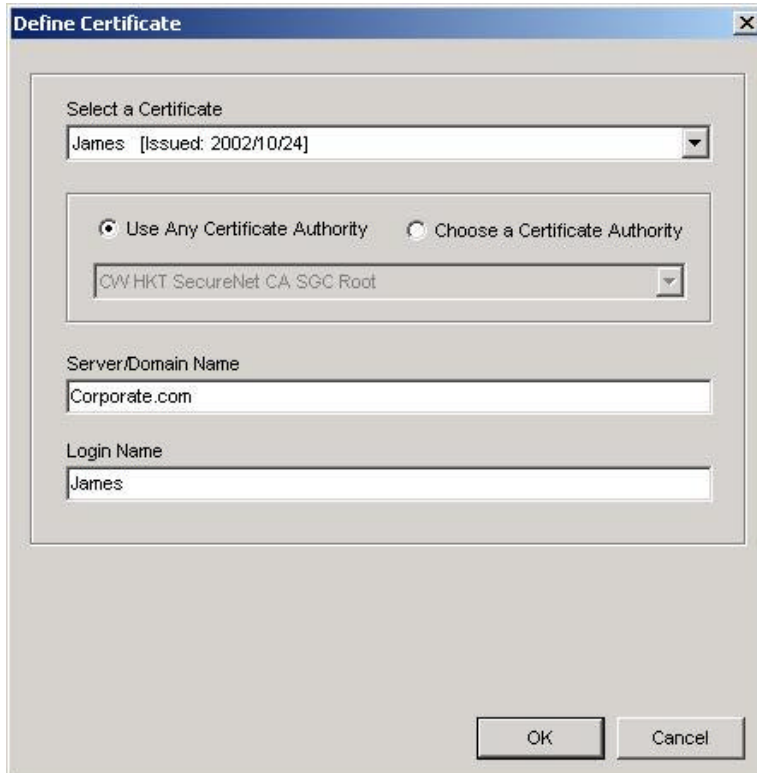
Note! Check with your Network Administrator for the security features supported by your AP.



- **WPA:** Enables the use of WiFi protected Access (WPA). This option requires IT administration.
 - a) Select **WPA** to open the WPA EAP drop-down menu. The options includes TLS and PEAP.
 - b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.
- **WPA-PSK:** Enables the WPA-Pre Shared Key (PSK). Click on the **Configure** button and complete the configuration information in the WPA Passphrase dialog.
- **802.1x:** Enables 802.1x security. This option requires IT administration.
 - a) Select **802.1x** to open the 802.1x EAP drop-down menu. The options include TLS and PEAP.
 - b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.

- **Pre-Shared Key:** Enables the use of pre-shared keys that are defined on the AP and the station.
 - a) Select the **Pre-Shared Key** radio button.
 - b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.
- **None:** No security.

5. Define the Certificate.



The image shows a Windows-style dialog box titled "Define Certificate". It contains the following fields and controls:

- Select a Certificate:** A dropdown menu showing "James [Issued: 2002/10/24]".
- Use Any Certificate Authority:** A radio button that is selected.
- Choose a Certificate Authority:** A radio button that is unselected.
- Choose a Certificate Authority:** A dropdown menu showing "CW HKT SecureNet CA SGC Root".
- Server/Domain Name:** A text field containing "Corporate.com".
- Login Name:** A text field containing "James".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

- **Select a Certificate:** Select the Certificate to Authenticate to the RADIUS server from the drop-down menu.
- **Use any Certificate Authority:** The Default Setting. Select this radio button to use any Certificate Authority (CA) for authentication.
- **Choose a Certificate Authority:** Select this radio button to choose the desired Certificate Authority for authentication from the drop-down menu.
- **Server/Domain Name:** The the RADIUS server name or the domain name used for the network access.
- **Login Name:** The username used to log into the server or domain.
- **Define User Information (PEAP):** Click on the **Define User Information** button and complete the configuration information in the Define User Information dialog.

6. If selecting **WPA-PSK**, click on the **Configure** button to enter the PassPhrase. The PassPhrase must be a minimum of 8 printable ASCII characters. The PassPhrase should be at least 20 characters to make it more difficult for an attacker to decipher the key.
7. If selecting **Pre-Shared Key**, click on the **Configure** button to enter the Encryption Keys. When finished, click **OK**. For WEP key, please contact with MIS administrator.

Define Pre-Shared Keys

Default Encryption Key: [Dropdown]

Encryption Keys (Hex 0-9 A-F)

Key Length: [Dropdown]

Unique Key: [Text Field] [Key Length: 64 (40+24) 10 hex digits]

Shared

First: [Text Field] [Key Length: 64 (40+24) 10 hex digits]

Second: [Text Field] [Key Length: 64 (40+24) 10 hex digits]

Third: [Text Field] [Key Length: 64 (40+24) 10 hex digits]

Fourth: [Text Field] [Key Length: 64 (40+24) 10 hex digits]

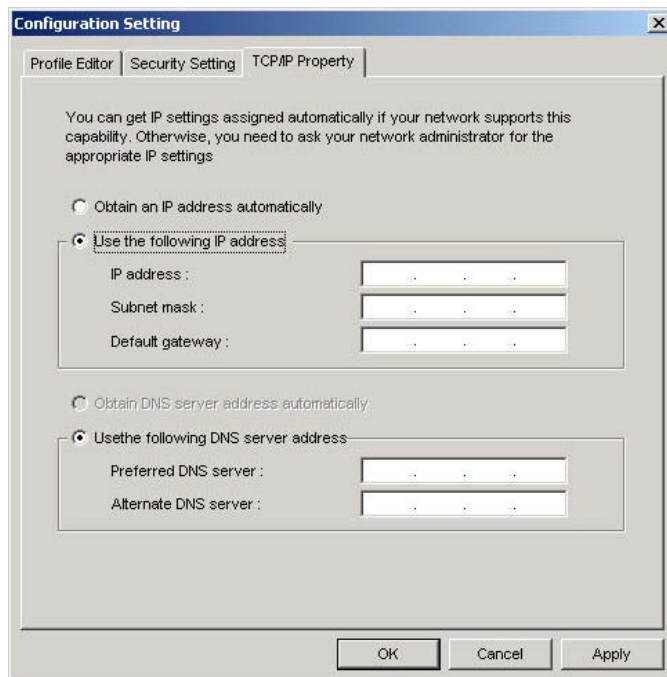
First Key: Column 1, Length 0

OK Cancel

- **Key Entry Method:** Determines the entry method for the key. Hexadecimal (0-9, A-F) or ASCII text (all keyboard characters).
- **Default Encryption Key:** Allows you to choose one encryption key (First, Second, Third, or Fourth) as the transmit key, which encrypts transmissions from the PC Card.
- **Unique Key:** Defines the per-session encryption key for the current network configuration. Not used in Ad-Hoc mode.
- **Shared Keys:** Use these fields to enter the wireless network's encryption keys. The keys must be in the correct position (First, Second, Third, or Fourth).
- **Key Length:** Defines the length of each encryption key.
 - o For 40/64 bit (enter 10 digits for hexadecimal or 5 characters for ASCII)
 - o For 104/128 bit (Enter 26 digits for hexadecimal or 13 characters for ASCII)

When the length is changed, the number of available characters in the field automatically changes. If a previously entered key is too long, the key is automatically truncated to fit. If the key length is increased again, the key does not update to the previous value.

8. Click **OK** to save the settings.
9. 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 mini-PCI Module”, and make sure this connection is **Enabled**.
3. Right-click the Wireless Network Connection of “WLAN a+b+g mini-PCI 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.

Appendix B: Specification

Item	Key specifications			
Frequency range	➤ U-NII: 5.15 ~ 5.35Ghz, 5.725 ~ 5.825Ghz 2.400 – 2.4835GHz,			
Modulation technique	➤ 802.11b/g DSSS (DBPSK, DQPSK, CCK) OFDM for data rate > 20 Mbps ➤ 802.11a OFDM(BPSK,QPSK, 16-QAM, 64-QAM)			
Channels support	➤ 802.11b/g US/Canada: 11 (1 ~ 11) ➤ 802.11a 1). US/Canada:12 non-overlapping channels (5.15 ~ 5.35GHz, 5.725 ~ 5.825GHz)			
Operation voltage	➤ 3.3V +/- 5%			
Power consumption		802.11a	802.11b	802.11g
	➤ Continuous Tx	490~510mA @18dBm	570~590mA @18dBm	610~640mA@18dBm
	➤ Continuous Rx	340~350mA	360~380mA	420~440mA
	➤ FTP Tx	420~440mA	510~530mA	530~545mA
	➤ FTP Rx	400~420mA	470~485mA	490~510mA
	➤ Standby mode	360~380mA	440~450mA	450~470mA
	➤ Power saving mode	50mA	50mA	50mA
	➤ RF Kill	40mA	40mA	40mA

Item		Key specifications
Operation distance	➤	802.11a Indoor:20m@72Mbps,25m@54Mbps,35m@48Mbps,40m@36Mbps
	➤	802.11b Outdoor:300m@11Mbps,465m@5.5Mbps,500m@2Mbps,515m@1Mbps Indoor: 60m@11Mbps,70m@5.5Mbps,83m@2Mbps,85m@1Mbps
	➤	802.11g Outdoor: 82m@54Mbps,100m@48Mbps,300m@36Mbps Indoor:20m@54Mbps,25m@48Mbps,35m@36Mbps
Operation System supported	➤	Windows [®] 98SE, ME, 2K, XP
Security	➤	64-bit,128-bit, 152-bit WEP Encryption
	➤	802.1x Authentication
	➤	AES-CCM & TKIP Encryption
Operation mode	➤	Infrastructure & Ad-hoc mode
Transfer data rate	➤	802.11b/g
	➤	11, 5.5, 2, 1 Mbps, auto-fallback, up to 54 Mbps
	➤	802.11a (Normal mode) 54, 48, 36, 24, 18, 12, 9, 6Mbps, auto-fallback
Operation temperature	➤	0° ~ 70° C
Storage temperature	➤	-20° ~ 80° C
Wi-Fi [®] Alliance	➤	WECA Compliant
WHL	➤	Microsoft [®] 2K, XP Complaint
FAA	➤	S/W audio On/Off support
Media access protocol	➤	CSMA/CA with ACK architecture 32-bit MAC
Embedded Antenna	➤	Embedded Dual Band Antenna