802.11g WLAN CardBus Card
With Smart Antenna

User Guide

Copyright

Version 1.0 (July, 2005)

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

Federal Communication Commission Interference 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.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

U-MEDIA declares that WCB-321A, (FCC ID: SI5WCB321A) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Table of Contents

Getting Started with the WCB-321A

Congratulations on purchasing the WCB-321A! The quick start guide included with your WCB-321A tells you how to install the Wireless Client Utility and how to operate the Wireless feature of the WCB-321A.

This manual provides information for setting up and configuring the WCB-321A. This manual is intended for both home users and professionals. It is not required to read some of the more technical information in this manual (such as in “Wireless LAN Networking” on page 13 and “Configuring Wireless Security” on page 29) to operate and enjoy the WCB-321A. It is included for your reference only.

The following conventions are used in this manual:

 NOTE	THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.
 TIP	THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.
 CAUTION	THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE YOUR SECURITY.
 IMPORTANT	LIKE NOTES AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED.

This section covers the following topics:

- Overview of the Wireless Client Utility
- Working with Profiles
- Checking for Available Access Points
- Disabling the Wireless Client Utility

Overview of the Wireless Client Utility

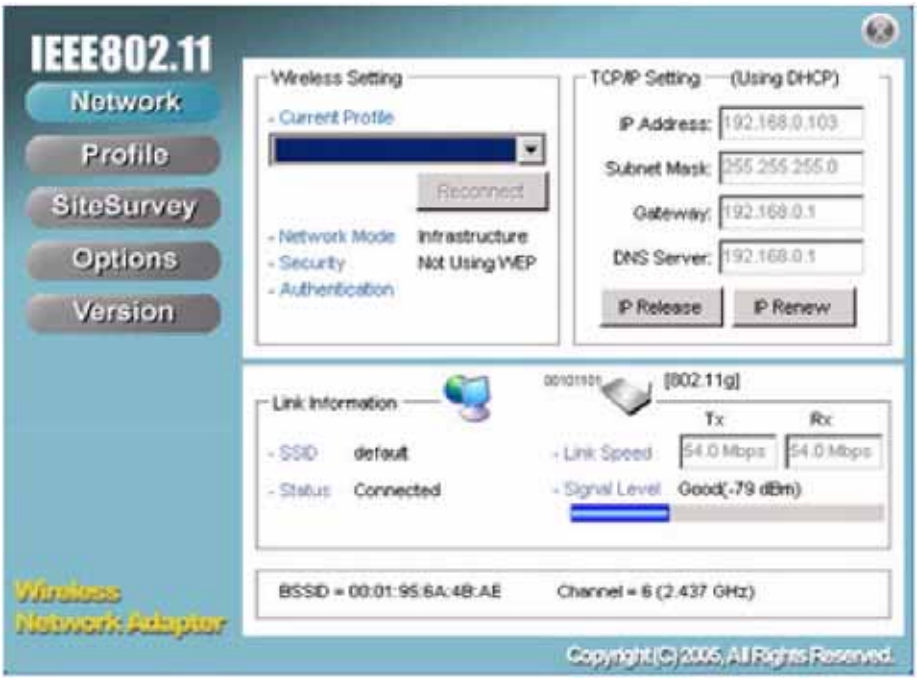
The Wireless Client Utility is included on the CD that shipped with the WCB-321A. Install the utility as described in the Quick Start Guide before attaching the WCB-321A to your computer.

IMPORTANT

BE SURE TO INSTALL THE WIRELESS CLIENT UTILITY BEFORE YOU ATTACH THE WCB-321A TO YOUR COMPUTER. ATTACHING THE WCB-321A BEFORE THE UTILITY IS INSTALLED COULD CAUSE THE INSTALLATION TO FAIL.

When the WCB-321A is installed, it is configured to automatically load when you start your computer. The utility icon displays in the system tray at the bottom-right corner of your screen.

Double-click the WCB-321A icon in the system tray, the following **Network** screen opens:



There are five screens in the utility.

- **The Network Screen**
- **The Profile Screen**
- **The SiteSurvey Screen**
- **The Options Screen**
- **The Version Screen**

The **Link Information** pane provides information on your current connection. This same pane is shows at the bottom of all screens so you are always aware of your connection status. l


NOTE

WHEN THE WCB-321A IS NOT CONNECTED TO YOUR COMPUTER, MOST SETTINGS IN THE WIRELESS CLIENT UTILITY ARE UNAVAILABLE. SETTINGS OR BUTTONS THAT ARE NOT AVAILABLE ARE GRAYED OUT.

Working with Profiles

A profile is a record of the configuration you use to connect to a particular access point. Without profiles, you would have to reconfigure the WCB-321A each time you change access points. Using the **Profile** screen you can configure the WCB-321A to access your home network and your office network. Each configuration is saved as a profile. Then when you go from the office to your home you just select the appropriate profile.

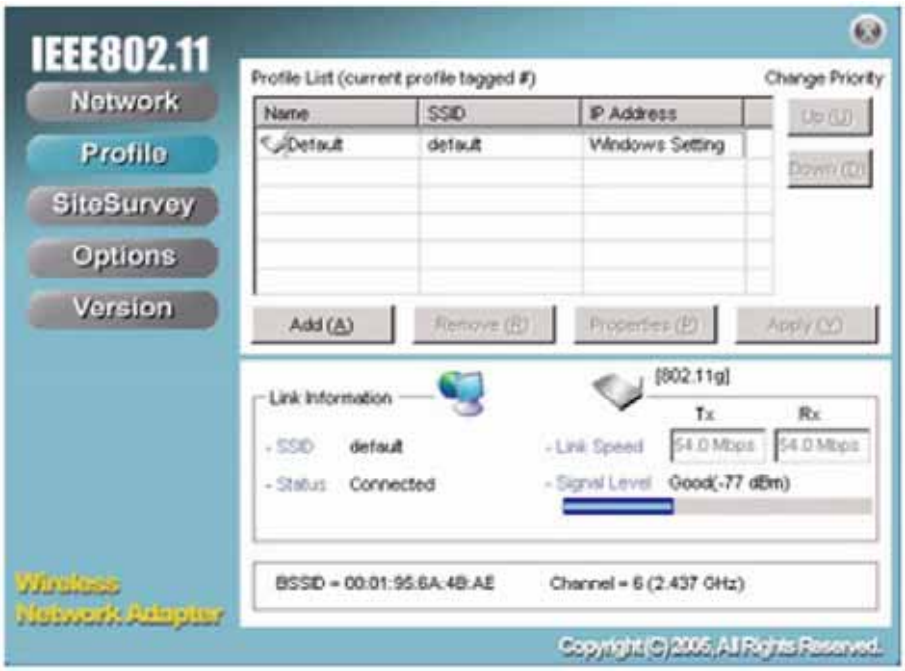

NOTE

YOU CAN CHANGE PROFILES WITHOUT REBOOTING YOUR COMPUTER. (PERHAPS WHEN WALKING FROM ONE ACCESS POINT TO ANOTHER WITHIN YOUR OFFICE.) IF YOU USE WINDOWS CONTROL PANEL TO CONFIGURE YOUR CONNECTIONS, YOU MUST REBOOT THE COMPUTER WHEN CHANGING ACCESS POINTS.

CREATING A PROFILE

Refer to the following to add a profile.

1. Click **Profile.**

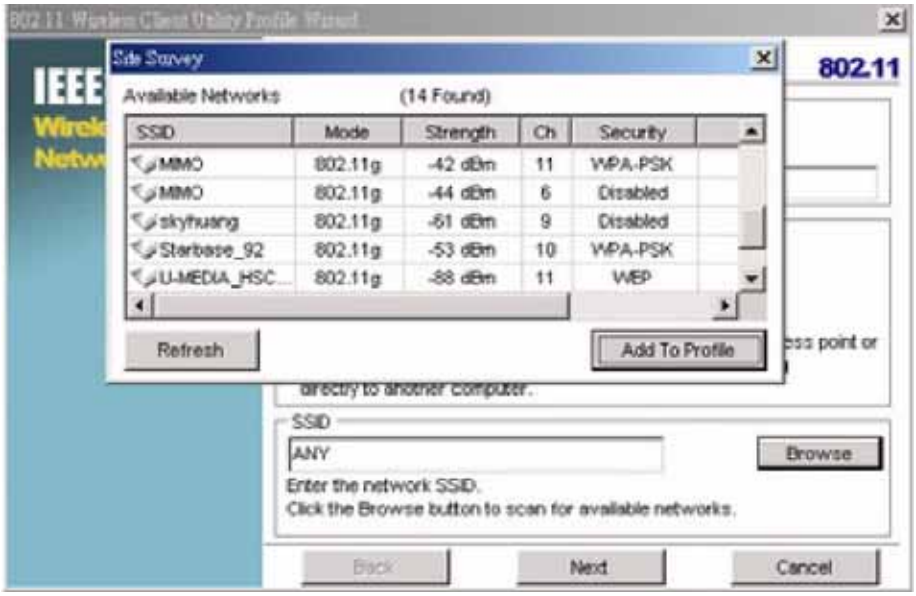


2. Click **Add.** The Wireless Client Utility Profile Wizard opens.

3. Type a descriptive name for the profile such as **Home** or **CoffeShop.**

4. Click the drop-down arrow at Network Mode and select **Infrastructure** or **Ad-Hoc.** Choose **Infrastructure** when connecting to an access point or wireless router. You will need to know the SSID of the access point.
   Choose **Ad-Hoc** when connecting directly to another computer without using an access point. You can type anything for the SSID as long as the same SSID is used on the computer you are connecting to.

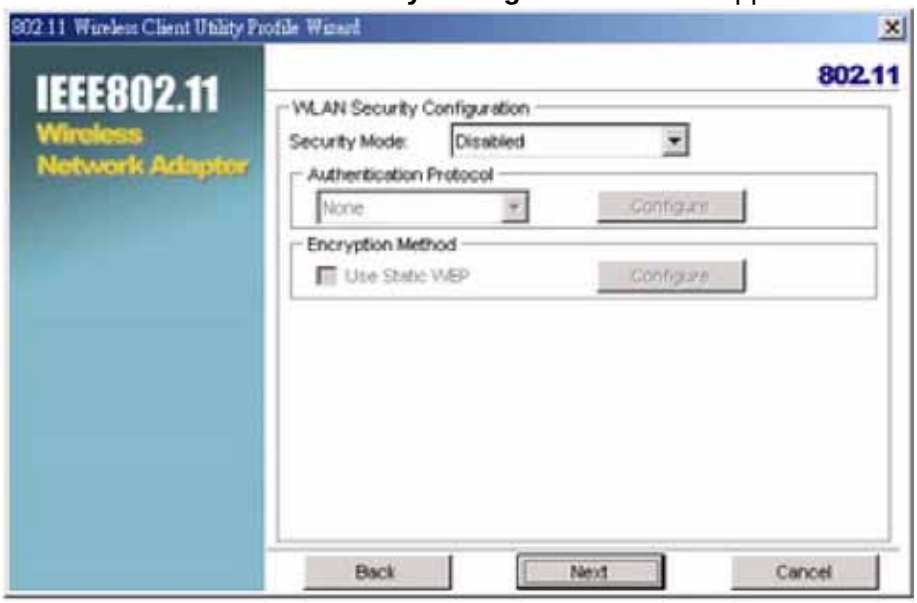
5. In the **SSID** pane click **Browse.** The utility performs a site survey and displays the results.



The SSID (Service Set IDentifier) is the name assigned to a wireless Wi-Fi network. All devices must use this case-sensitive name, which is a text string up to 32 bytes long, in order to communicate.

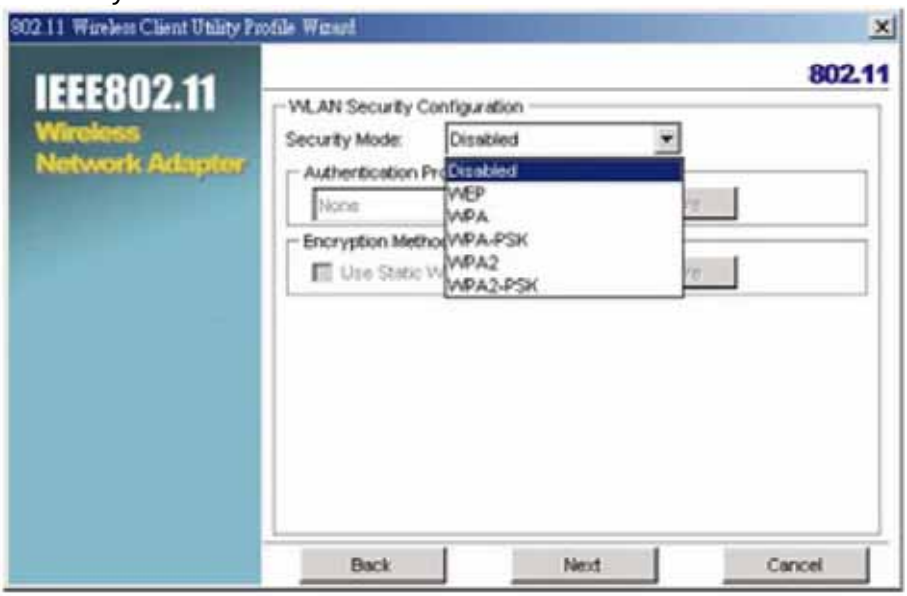
6. Select the SSID you want to connect to and click **Add To Profile.**

7. Click **Next.** The **WLAN Security Configuration** screen appears.



This screen reflects the security settings detected in the access point you want to connect to. Security settings vary in complexity and you may have to consult your network administrator for this information. See “Configuring Wireless Security” for more information.

8. Select the Security Mode from the drop-down list and then select the appropriate settings for the security mode.



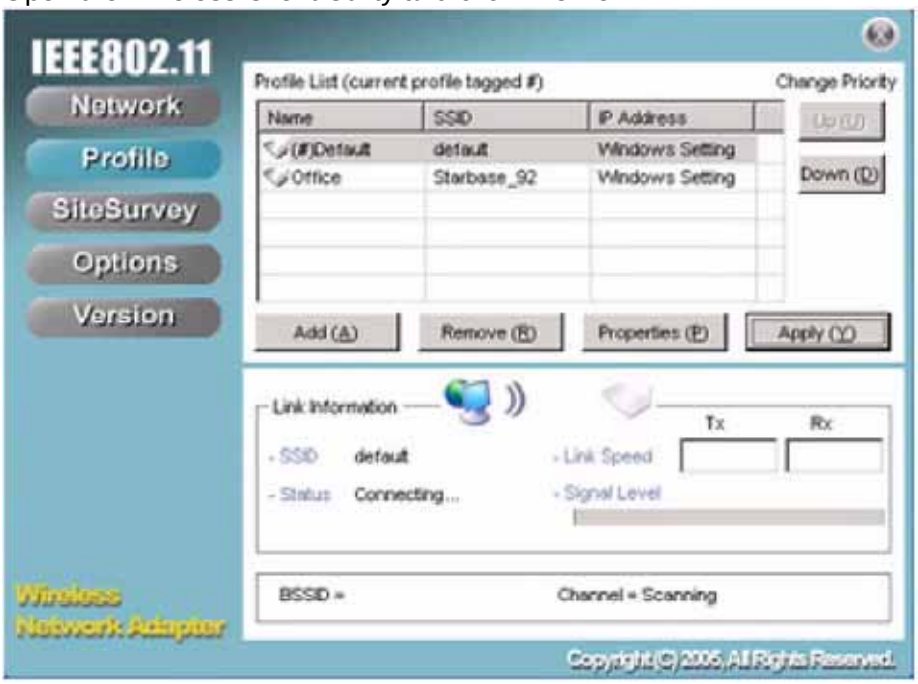
9. Click **Next.**

10. Click **Save** to complete the wizard and save the new profile. (If you do not want to activate the profile, uncheck the **Apply this profile now** checkbox.)

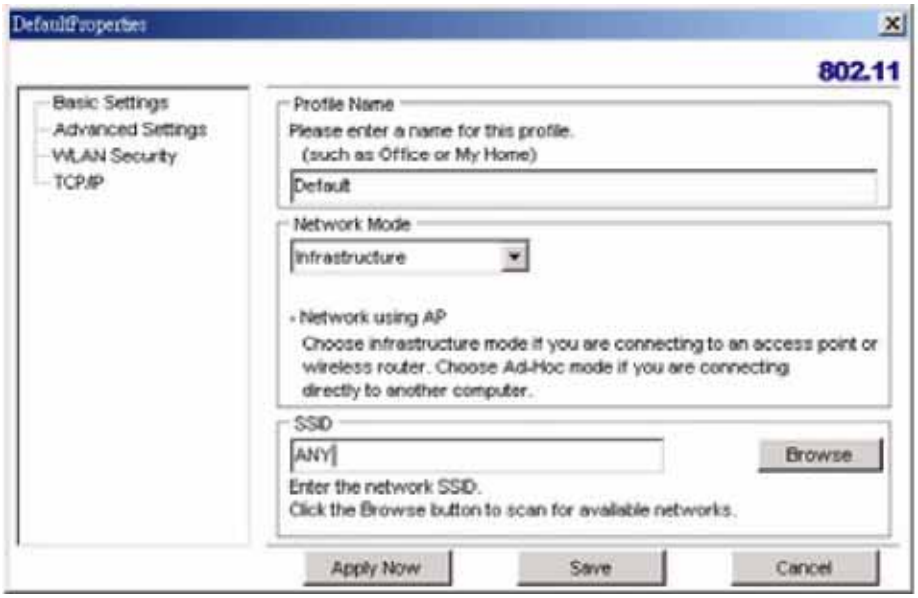
MODIFYING PROFILES

You may need to modify settings for a profile, for example, if you purchase a new router, or if your office administrator provides you with new security settings. Refer to the following to modify a profile.

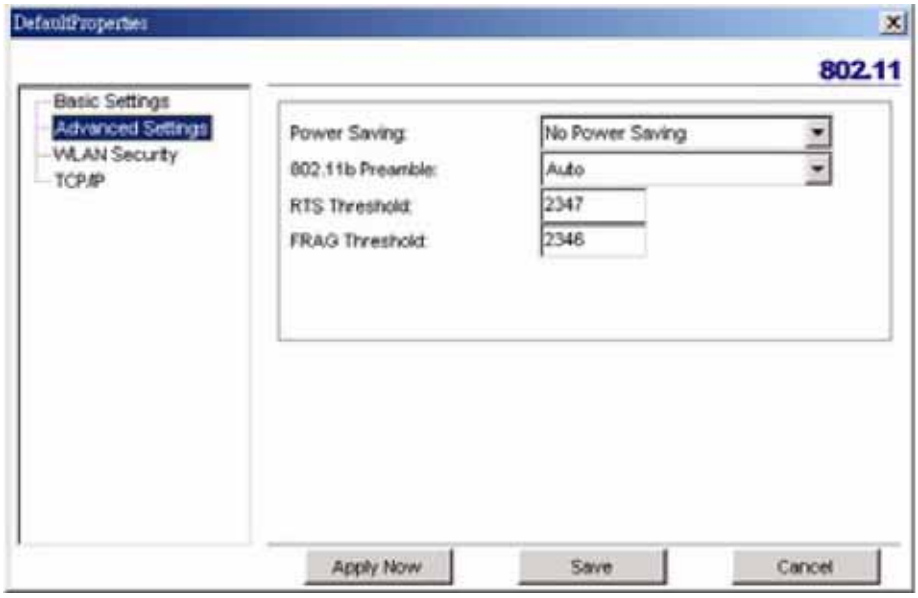
1. Open the Wireless Client Utility and click **Profile.**



2. Select the profile you want to modify and click **Properties.**



3. Make the changes you want to the **Basic Settings** and click **Advanced Settings.**



Unless you have a thorough understanding of wireless networking, it is recommended that you leave these settings at the defaults.

4. Click **WLAN Security.** (Refer to "Configuring Wireless Security" for more details on security settings.)

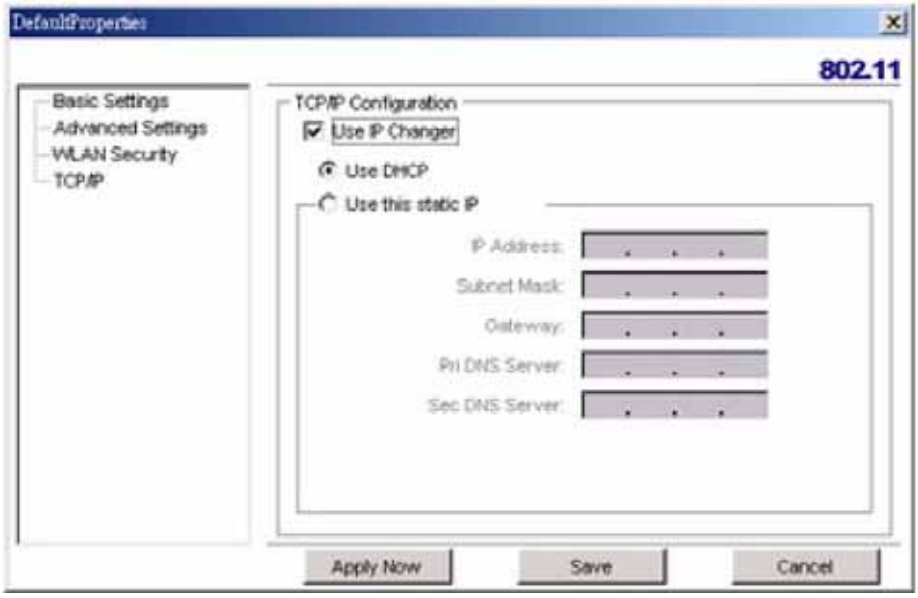
Click the drop-down arrow at Security Mode to choose from the following settings:
Disabled (No Encryption)
All data sent between the access point and the client is left unencrypted and may be viewed by other wireless devices.
WEP (Wired Equivalent Privacy)
Encrypts all traffic sent between the access point and the client using a shared key. When using WEP encryption, only access points and PCs using the same WEP Key can communicate with each other.

WPA/WPA2
WPA encrypts all traffic between the access point and the client using either TKIP or AES encryption. Depending on the authentication protocol selected, each client must authenticate using their own unique username, password, and security certificate.

WPA-PSK/WPA2-PSK
WPA-PSK or WPA2-PSK is a compromise between WPA/WPA2 and WEP. Like WEP, it uses a pre-shared key that every user of the network must have in order to send and receive data. Like WPA, it uses either TKIP or AES.

IMPORTANT	IT IS RECOMMEDED THAT YOU USE WPA/WPA2 OR WPA-PSK/WPA2-PSK WHENEVER POSSIBLE. WPA (WI-FI PROTECTED ACCESS) PROVIDES STRONGER ENCRYPTION THAN THE EARLIER WEP (WIRED EQUIVALENT PRIVACY) METHOD. WPA2 PROVIDES EVEN STRONGER ENCRYPTION, AUTHENTICATION AND KEY MANAGEMENT.

5. Make the changes you want and click **TCP/IP Config.**



Select the **Use IP Changer** checkbox. This allows you to bypass your existing wireless TCP/ IP settings and configure TCP/IP settings for each profile.
Use DHCP
DHCP (Dynamic Host Configuration Protocol) automatically assign IP addresses. Check this radio button if your router is set to DHCP.
Use static IP below
Check this radio button if you have to enter a static IP address.

Checking for Available Access Points

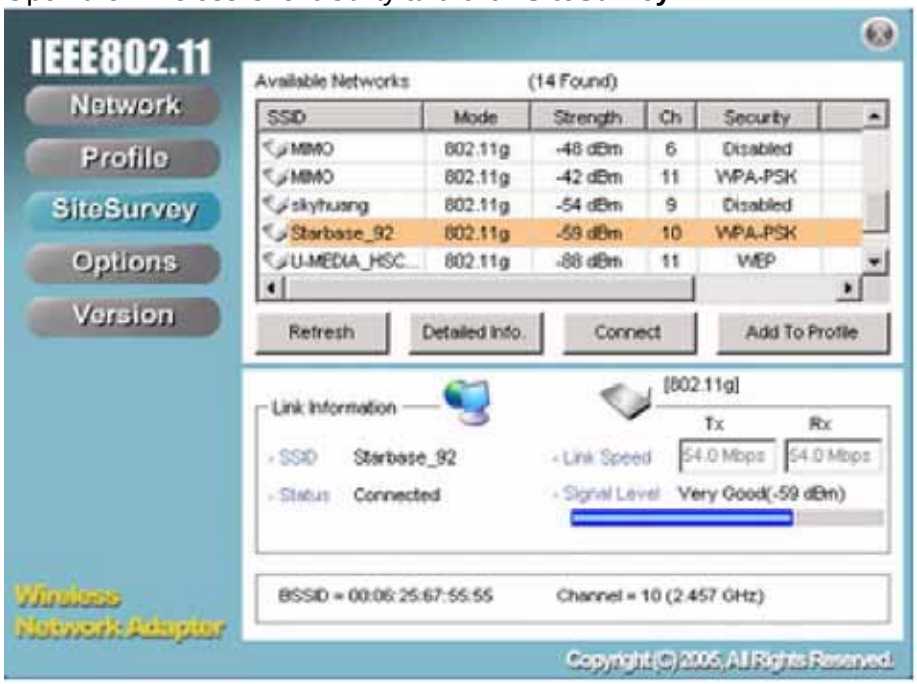
The number of access points or hot spots for public use is constantly increasing in major cities. Many Web sites report on the locations of hot spots. Check the following Web sites for updated information for your location.

- http://intel.jiwire.com
- www.hotspot-locations.com
- www.hotspotlist.com
- www.wififreespot.com
- www.wifinder.com
- www.wi-fizone.org

If you think you are in the vicinity of an access point, you can use the SiteSurvey screen to list the ones available.

To scan for access points using the WCB-321A, refer to the following.

1. Open the Wireless Client Utility and click **SiteSurvey.**



2. Available wireless networks are listed. Click **Refresh** anytime to update the list.

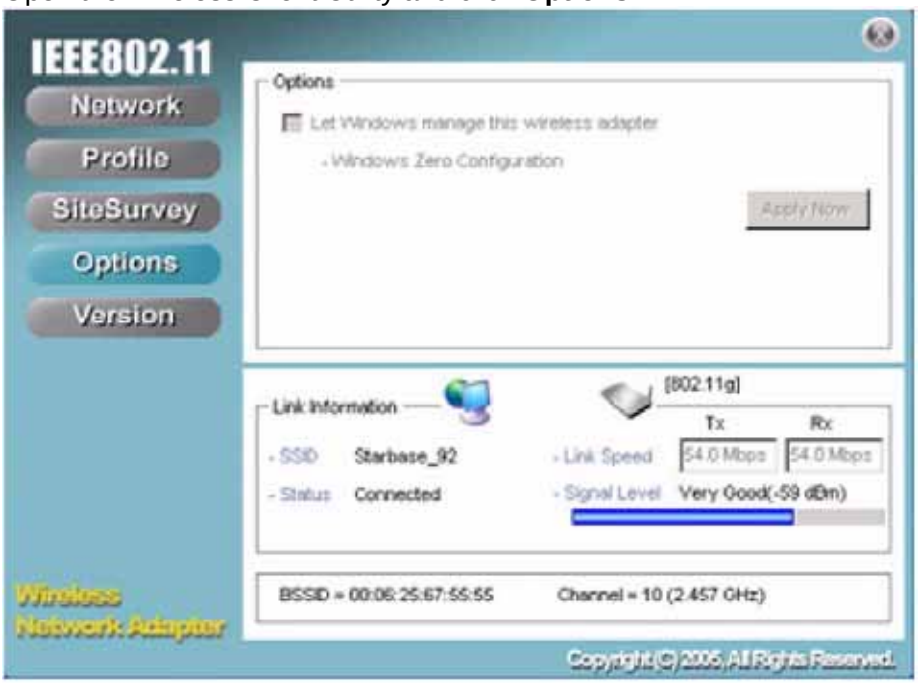
3. Select the network you want and click **Connect.** Or click **Add To Profile** if you want to connect later.

For details about any of the listed access points, select it from the list and click **Detailed Info** to see the following screen. (You can also double-click an access point to view the **Detailed Info** screen.

Disabling the Wireless Client Utility

You may need to have Windows manage your wireless network settings. In that case, you should disable the Wireless Client Utility. To disable the Wireless Client Utility refer to the following.

1. Open the Wireless Client Utility and click **Options.**



2. Select the **Let Windows manage this wireless adapter check box** and click **Apply Now.**

Wireless LAN Networking

This section provides background information on wireless LAN networking technology. Consult the "Glossary" for definitions of the terminology used in this section.

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

Transmission Rate (Transfer Rate)

The WCB-321A provides various transmission (data) rate options for you to select. Options include Fully Auto, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps and 108Mbps. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your WCB-321A to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the WCB-321A automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the WCB-321A gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

Types of Wireless Networks

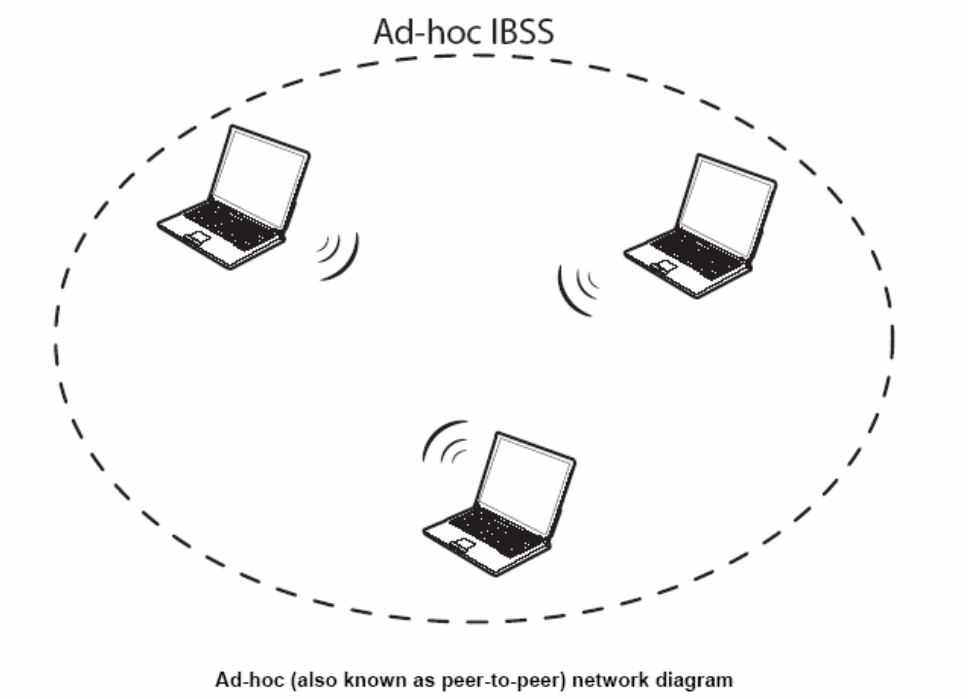
Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the WCB-321A operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

AD-HOC (IBSS) NETWORK

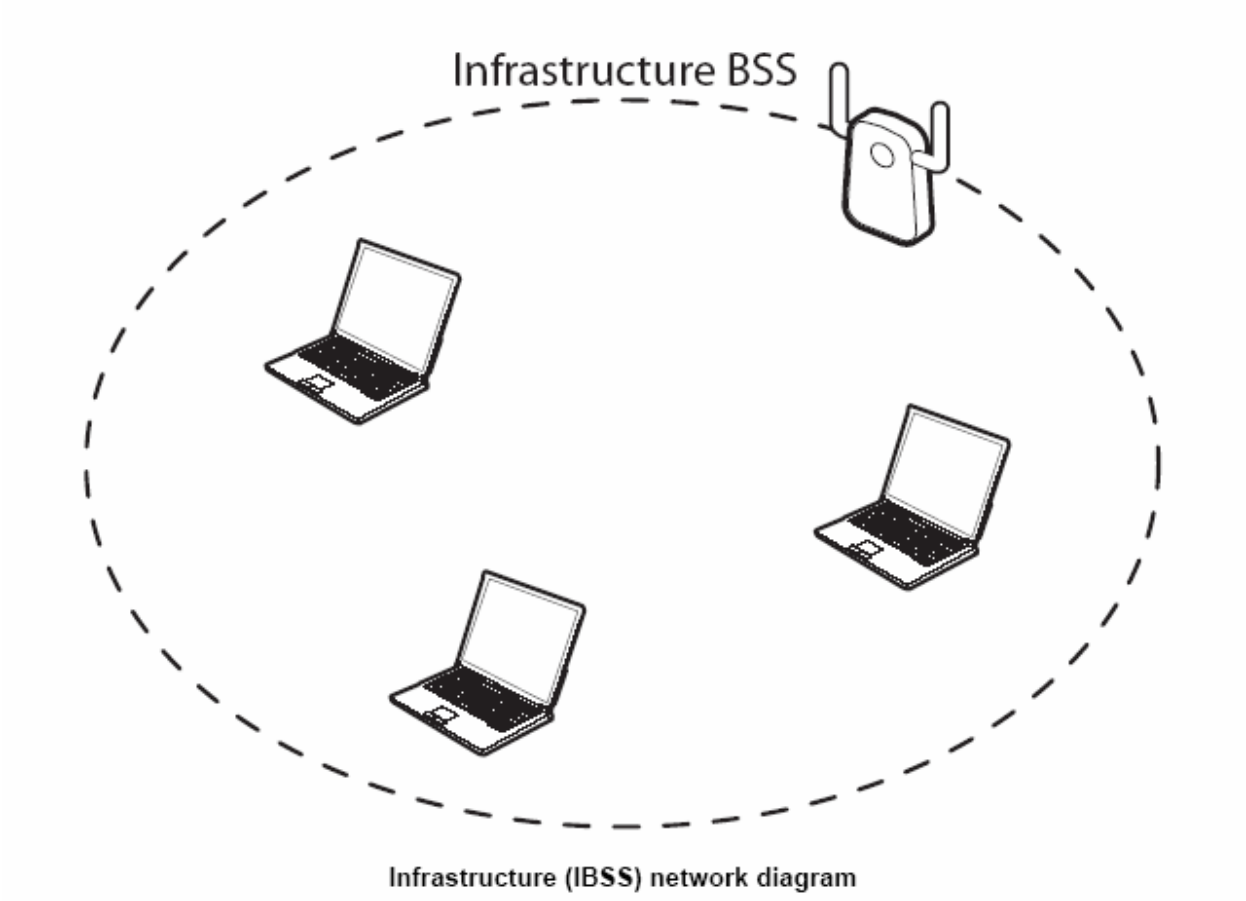
Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each station.



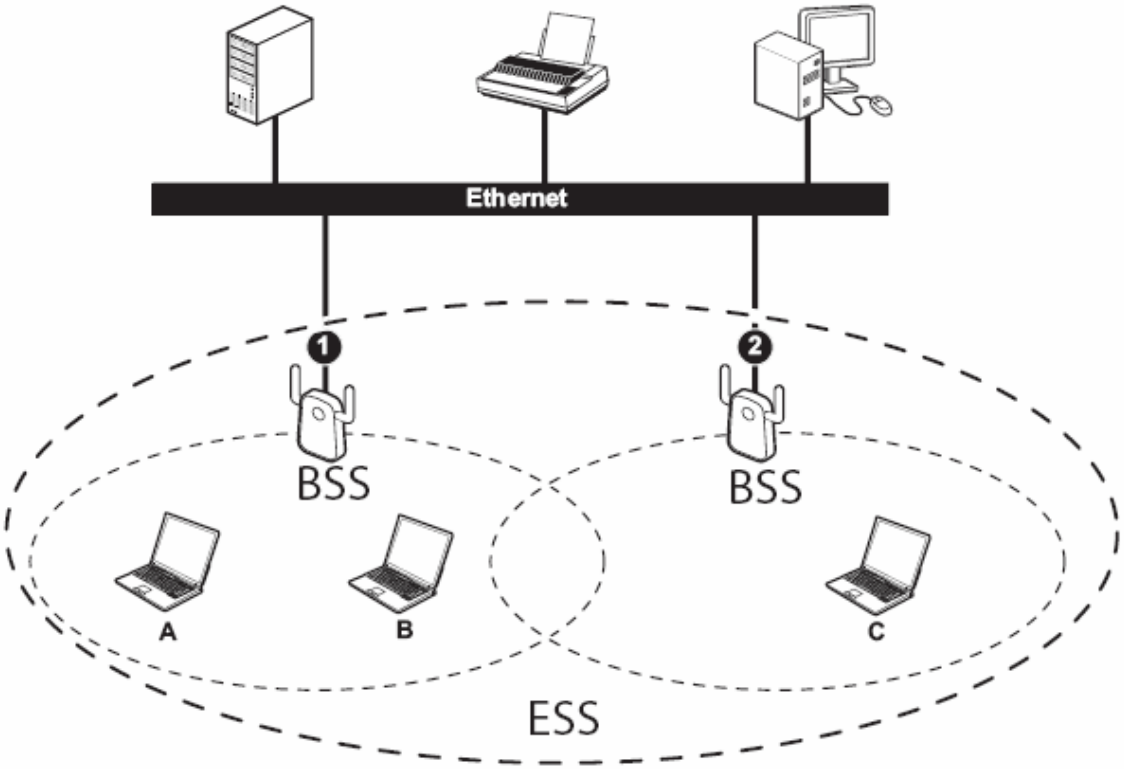
Ad-hoc (also known as peer-to-peer) network diagram

When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).



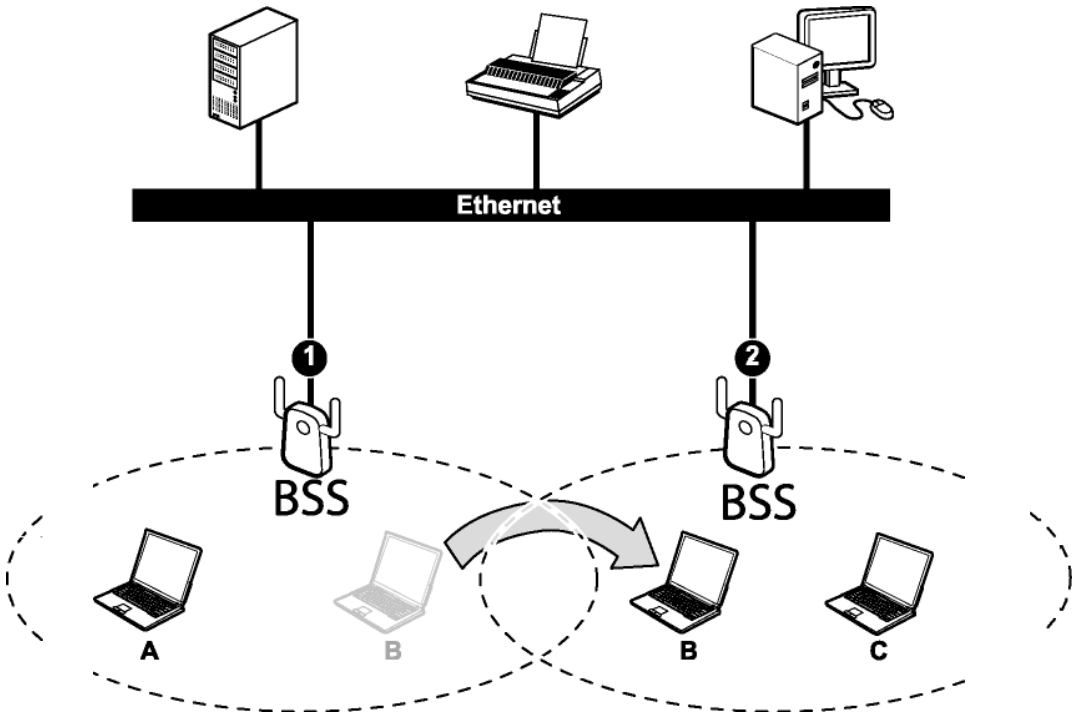
Infrastructure (IBSS) network diagram

In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



Infrastructure (ESS) network diagram

In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the WCB-321A automatically switches to the channel used in BSS (2).



Roaming in an ESS network diagram

WIRELESS LAN SECURITY

Because wireless networks are not as secure as wired networks, its vital that security settings are clearly understood and applied.

CAUTION

DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTTINGS FOR A NETWORK WITHOUT AUTHORIZATION AND WITHOUT CLEARLY UNDERSTANDING THE SETTINGS YOU ARE APPLING. WITH POOR SECURITY SETTINGS, SENSITIVE DATA YOU SEND CAN BE SEEN BY OTHERS.

The list below shows the possible wireless security levels on your WCB-321A starting with the most secure. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. EAP requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or the LAN to provide authentication service for wireless stations.

1. Wi-Fi Protected Access (WPA)
2. IEEE802.1X EAP with RADIUS Server authentication
3. WEP Encryption
4. Unique ESSID

To check wireless LAN security settings for a connection, open the Wireless Client Utility and select the **Profile** screen. Select the connection you want and click Properties. See “Modifying Profiles” on page 6.

DATA ENCRYPTION WITH WEP

The WEP (Wired Equivalent Privacy) security protocol is an encryption method designed to try to make wireless networks as secure as wired networks. WEP encryption scrambles all data packets transmitted between the WCB-321A and the access point or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your WCB-321A.

- Automatic WEP key generation based on a password phrase called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
- For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the wireless utility and entering them manually as the WEP keys in the other WLAN adapter(s).

The WCB-321A allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.

THE WCB-321A SUPPORTS UP TO FOUR 64-BIT, 128-BIT, AND 152-BIT WEP KEYS. THE 152-BIT WEP MUST COMPLY WITH THE WEP SETTING OF YOUR ACCESS POINT OR ROUTER.

Exploring the Wireless Client Utility Screens

This section covers the following topics:

The Network Screen

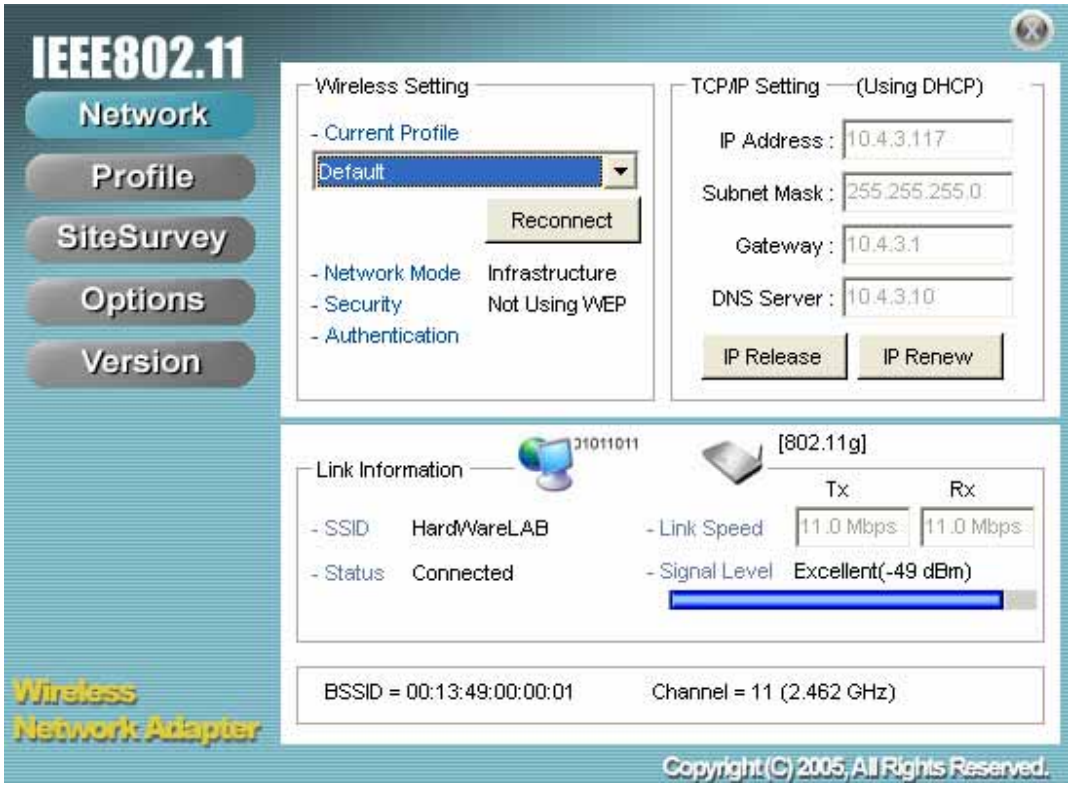
The Wireless Client Utility is included on the CD that shipped with the WCB-321A. Install the utility as described in the Quick Start Guide before attaching the WCB-321A to your computer.

IMPORTANT

BE SURE TO INSTALL THE WIRELESS CLIENT UTILITY BEFORE YOU ATTACH THE WCB-321A TO YOUR COMPUTER. ATTACHING THE WCB-321A BEFORE THE UTILITY IS INSTALLED COULD CAUSE THE INSTALLATION TO FAIL.

When the WCB-321A is installed, it is configured to automatically load when you start your computer. The utility icon displays in the system tray at the bottom-right corner of your screen.

Double-click the WCB-321A icon in the system tray, the following **Network** screen opens:



WIRELESS SETTING

The Wireless Setting pane settings are described below

Current Profile	Shows the current profile you have selected. If you have not added a profile, only **Default** shows. The settings shown in the Network screen are for the current profile. Click the dropdown arrow to select another profile.
Reconnect (button)	Press to reconnect to the current access point.
Network Mode	Shows the current network mode. Infrastructure or ad-hoc mode. (See **Note** below for more information.)
Security	Shows the security status.
Authentication	Shows the authentication required.(See "Configuring Wireless Security")

NOTE

WIRELESS SYSTEMS WORK IN INFRASTRUCTURE MODE OR PEER-TO-PEER MODE. IN INFRASTRUCTURE MODE, WIRELESS DEVICES COMMUNICATE TO A WIRED LAN VIA ACCESS POINTS. IN AD-HOC MODE (ALSO KNOWN AS PEERTO-PEER MODE), WIRELESS DEVICES COMMUNICATE WITH EACH OTHER DIRECTLY AND DO NOT USE AN ACCESS POINT.

TCP/IP SETTING

The TCP/IP Setting pane settings are described below.

IP Address	Shows the current network IP address.
Subnet Mask	Shows the current subnet mask status.
Gateway	Shows the current gateway.
DNS Server	Shows the current network DNS address.
IP Release (button)	Click to release the current TCP/IP settings.
IP Renew (button)	Click to renew the TCP/IP settings.

LINK INFORMATION

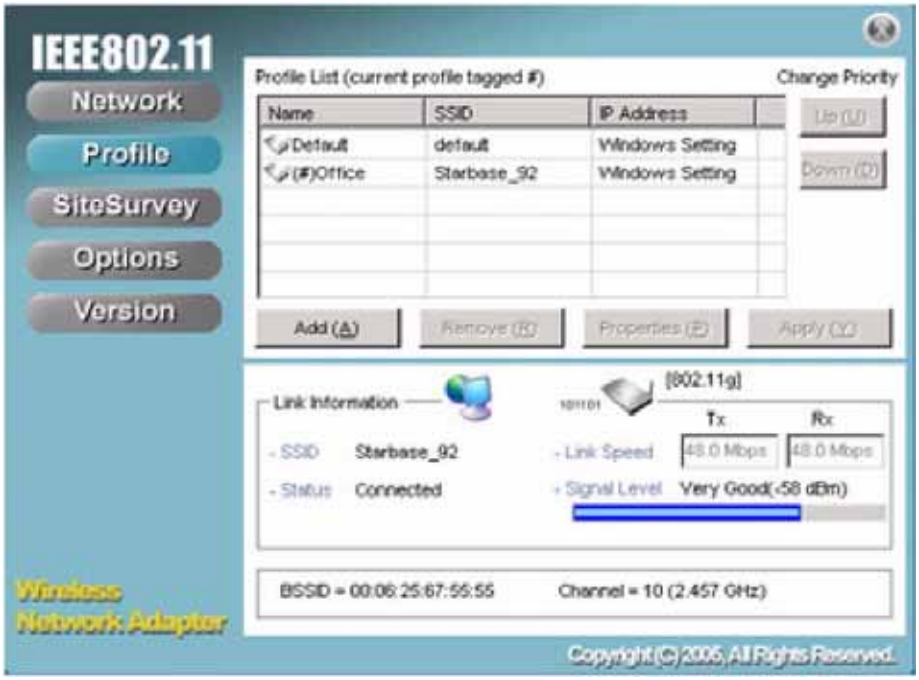
The Link Information pane settings are described below. The Link Information pane shows the network status.

SSID	Shows the current SSID (Service Set IDentifier). This is the name assigned to a wireless Wi-Fi network. All devices must use this case-sensitive name in order to communicate.
Status	Shows the current connection status.
Link Speed	Shows the speed of the current connection. Tx is the transmit speed; Rx the receive speed.
Signal Level	Shows the signal strength of the current connection. (See **Tip** below for more information.)
BSSID	Shows the ID of the current BSS. (See **Note** below for more information.)
Channel	Shows the network channel.

TIP	THE LINK INFORMATION PANEL IS SHOWN IN ALL SCREENS SO YOU CAN ALWAYS SEE THE STATUS OF YOUR CURRENT CONNECTION. MONITOR THIS SETTING AS YOU MOVE AROUND TO ATTAIN A SUITABLE SIGNAL..
NOTE	WIRELESS SYSTEMS WORK IN INFRASTRUCTURE MODE OR AD-HOC (PEER-TO-PEER) MODE. IN INFRASTRUCTURE MODE, WIRELESS DEVICES COMMUNICATE TO A WIRED LAN VIA ACCESS POINTS. EACH ACCESS POINT AND ITS WIRELESS DEVICES ARE KNOWN AS A BASIC SERVICE SET (BSS). IN AD-HOC MODE (ALSO KNOWN AS PEER-TO-PEER MODE), WIRELESS DEVICES COMMUNICATE WITH EACH OTHER DIRECTLY AND DO NOT USE AN ACCESS POINT. THIS IS AN INDEPENDENT BSS (IBSS).

The Profile Screen

A profile is a record of the configuration you use to connect to a particular access point. Without profiles, you would have to reconfigure the WCB-321A each time you change access points. Using the **Profile** screen you can configure the WCB-321A to access your home network and your office network. Each configuration is saved as a profile.



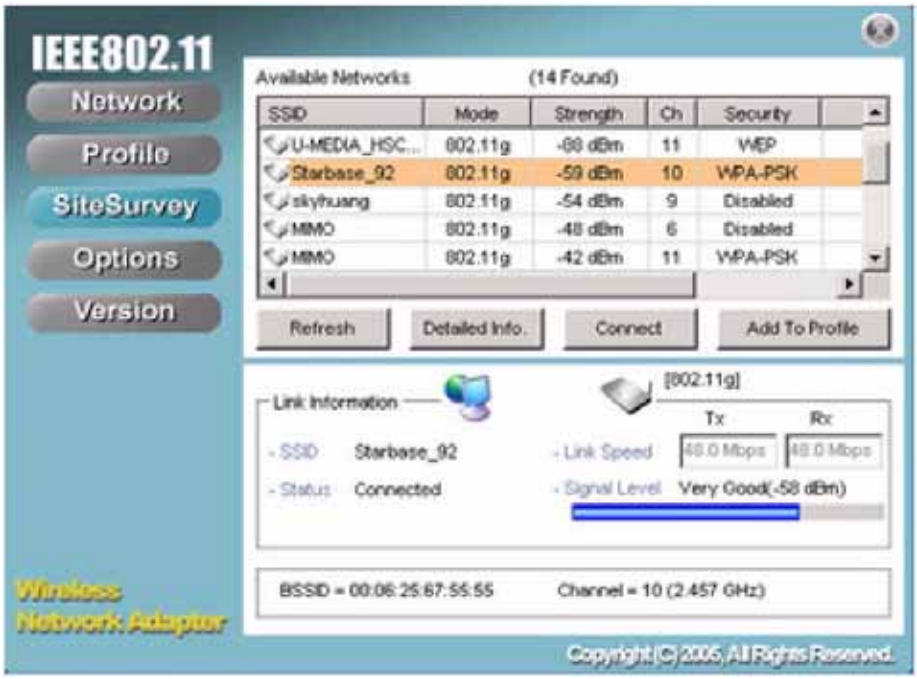
PROFILE LIST

The Profile List pane settings are described below.

Name	Shows the name of the profile that you assigned. If only default displays, no profiles have been added.
SSID	Shows the name (usually the equipment vendor's name) assigned to a wireless Wi-Fi network. (The keyword “ANY” means any available network.)
IP Address	Shows the IP address.
Add (button)	Click to add a profile.
Remove (button)	Click to remove the selected profile.
Properties (button)	Click to view properties for the selected profile.
Apply (button)	Click to apply changes after modifying settings.
Up (button)	Use the **Up/Down** buttons to move the selected profile to the top of the list or to the bottom. When in the Network screen, the WCB-321A attempts to connect to the network at the top of this list first.
Down (button)	

The SiteSurvey Screen

Use the SiteSurvey screen to scan for available networks in your vicinity.



AVAILABLE NETWORKS

The Available Networks pane settings are described below.

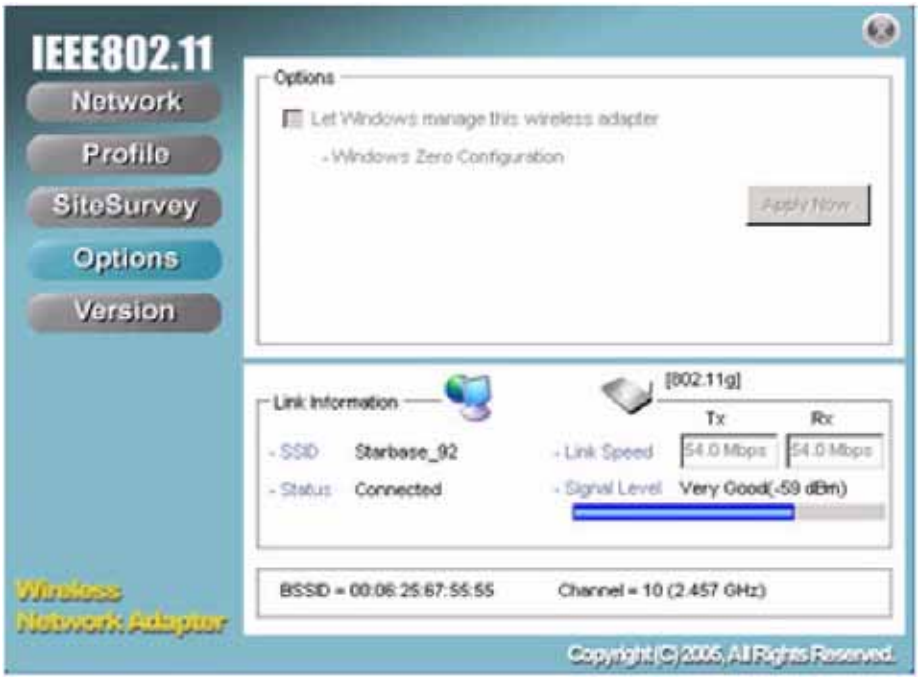
SSID	Shows the name (usually the equipment vendor's name) assigned to a wireless Wi-Fi network.
Mode	Shows the signal type (802.11b/g).
Strength	Shows the signal strength.
Ch	Shows the network channel.
Security	Shows the security status.
Refresh (button)	Click to refresh the list of currently available networks.
Detailed Info (button)	Click to view properties for the selected network. (See Detailed Info. Screen below.)
Connect (button)	Click to connect to the selected network. (The network is not added to the profile list.)
Add To Profile (button)	Click to add the network to the profile list.

DETAILED INFO. SCREEN

For details about any of the listed access points, select it from the list and click **Detailed Info** to see the following screen. (You can also double-click an access point to view the **Detailed Info** screen.

The Options Screen

By default, the Wireless Client Utility configures your wireless settings. Use this screen to disable the Wireless Client Utility.



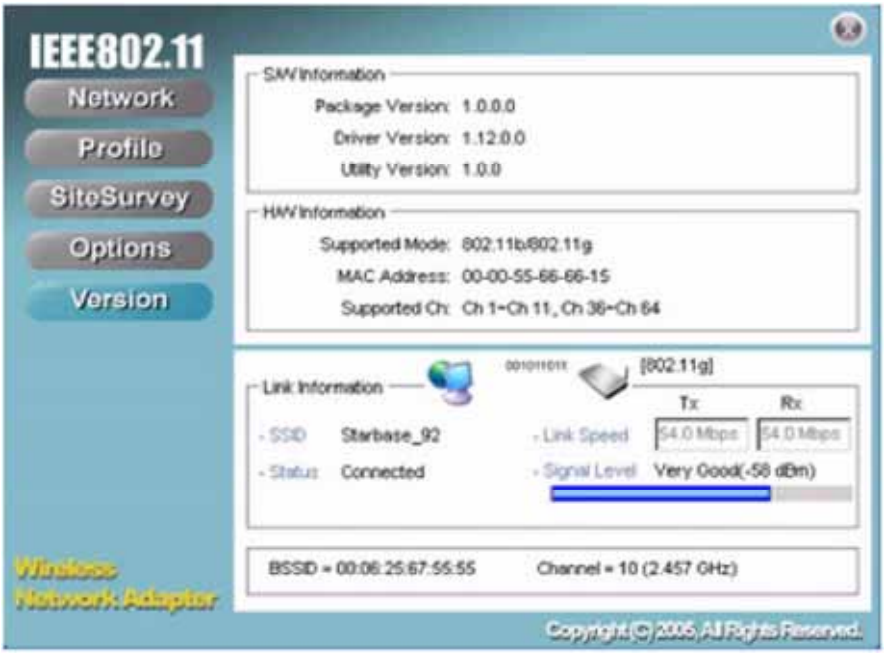
OPTIONS

The Options pane settings are described below.

Let Windows manage this wireless adapter (tick box)	When you check the Let Windows manage this wireless adapter checkbox, Windows Zero Configuration manages your wireless settings. The Wireless Client Utility still shows the link status of the adapter.
Apply Now (button)	Click to execute the changes.

The Version Screen

This screen displays the software and hardware information of the adapter. You cannot make changes to this screen.



NOTE

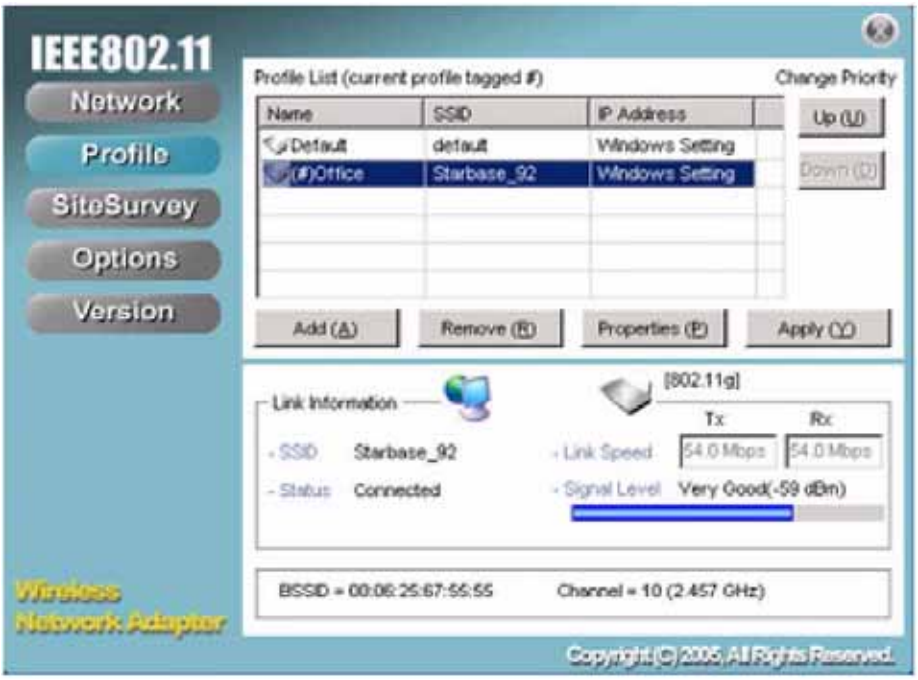
Reference the **Version** screen if you need to contact technical support. See "Maintenance".

Configuring Wireless Security

This chapter covers the configuration of security options in the 802.11 Wireless Client Utility.

Configuring Security

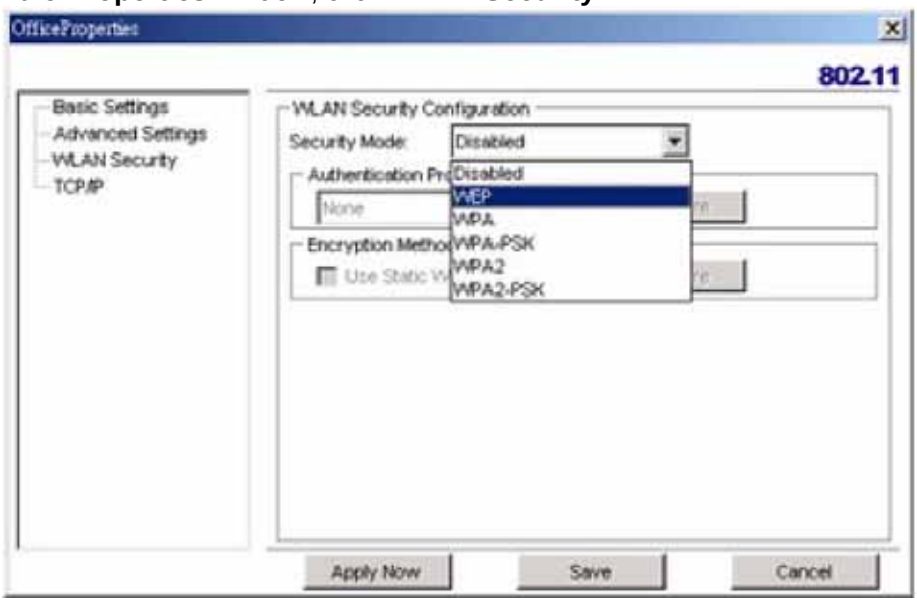
When you create a profile you need to configure the security settings with the information provided by the administrator. You modify security settings by selecting the profile and clicking **Properties.**



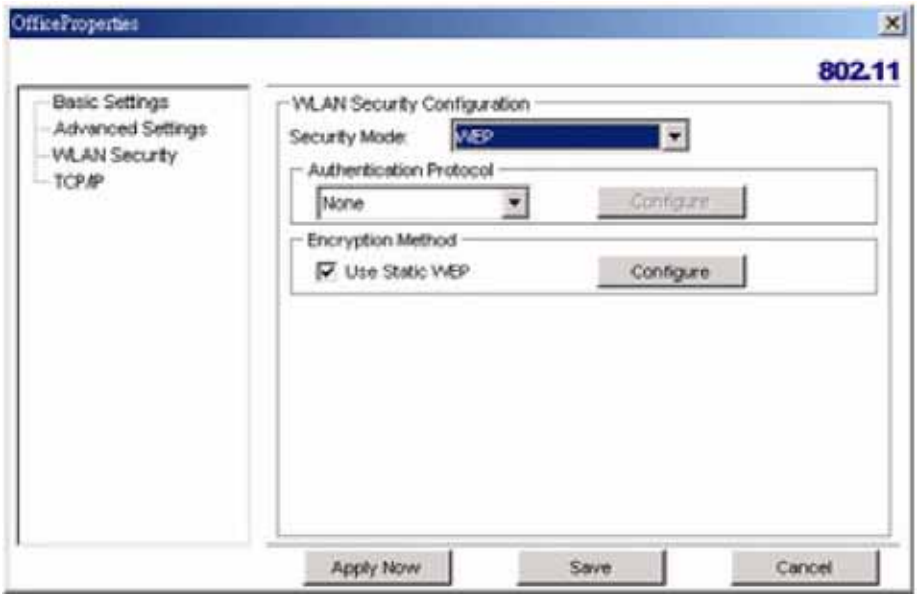
CONFIGURING WEP

Refer to the following to modify WEP settings.

1. In the **Properties** window, click **WLAN Security.**



2. Click the drop-down arrow at **Security Mode** and choose **WEP.**
3. Click the **Use Static WEP** checkbox.



4. Click **Configure.** The WEP Configuration screen appears.

WEP Method	Select the encryption to match your access point: 64, 128, or 256-bit. The encryption level must match the encryption level used by your access point.
Authentication	Options are Auto, Open System, and Shared. For most installations choose Auto.
Make Key using Pass-Phrase	A WEP Key is automatically generated as you type in any Passphrase of your choice. Use this feature when you have used a Passphrase to generate your WEP key on your access point.
Manual Input (ASCII)	Generate your own WEP Key (4 keys maximum) using ASCII characters.
Manual Input (HEX)	Generate your own WEP Key using hexadecimal characters.
Default Key	Four keys are used for decryption; you have to choose a default key from them for encryption. Make sure access point uses same WEP key.

CONFIGURING WPA & WPA2

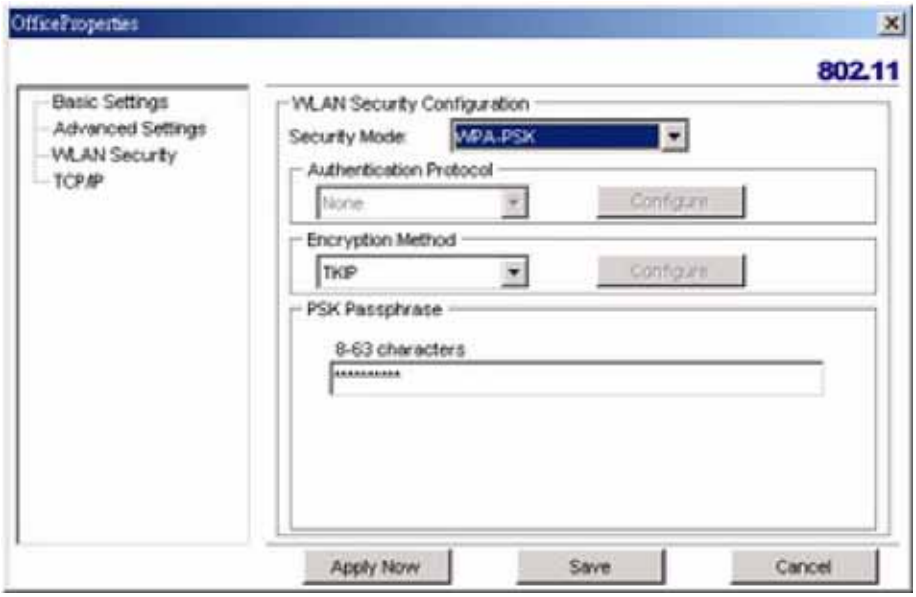
Refer to the following to configure WPA & WPA2.

1. Click the drop-down arrow at **Security Mode** and choose **WPA** or **WPA2.**
2. Click the drop-down arrow at **Encryption Method** and choose **TKIP** or **AES.**

To configure 802.1X (authentication protocol) for WPA or WPA2, see “Configuring 802.1X ” on page 34.

CONFIGURING WPA-PSK & WPA2-PSK

Refer to the following to configure WPA-PSK & WPA2-PSK.



1. Click the drop-down arrow at **Security Mode** and choose **WPA-PSK** or **WPA2-PSK.**
2. Click the drop-down arrow at **Encryption Method** and choose **TKIP** or **AES.** (Most access points use TKIP for WPA-PSK & AES for WPA2-PSK.)
3. At **PSK Passphrase** enter the same pass phrase used to configure the WPA-PSK or WPA2-PSK on your access point.

CONFIGURING 802.1X

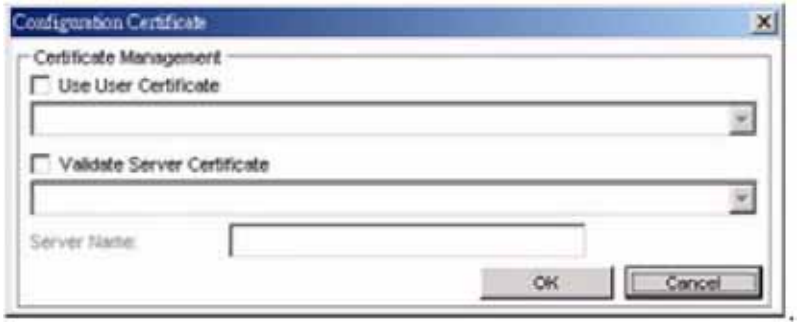
You need to know if your access point supports 802.1X and then apply the configuration here.

1. Choose the EAP method under **Authentication protocol.**
2. Options for **User Information** depend on the EAP method chosen.

CONFIGURING 802.1X – PEAP

Refer to the following to configure PEAP.

1. At **WPA** or **WPA2** security mode, click **Configure** button next to **Authentication Protocol.**
2. Select **Inner PEAP** protocol.
3. Click **Save** to finish and return to the previous screen.
4. Type in a unique **User ID** and **Password** under **User Information.**
5. If your network uses a user server certificate click **Configure Certificate** (see **Note** below). The following window appears:



Use user certificate	Check this box if your network requires user certification and then select the certificate from the drop-down menu.

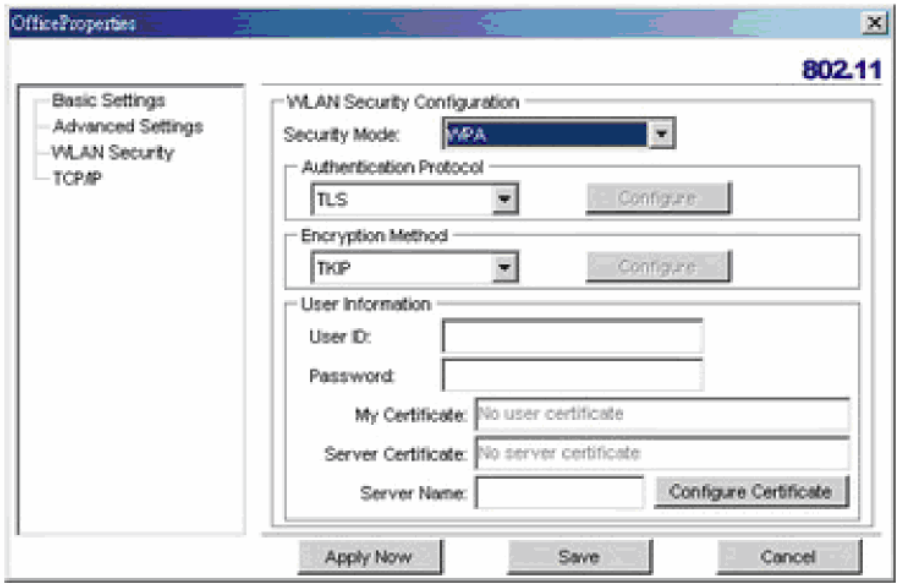
Validate server certificate	Check this box if your network requires server certification and then select the certificate authority from the drop-down menu.
Server name:	Type in the name of the server that is used for 802.1X authentication.
Server name should match exactly	Check this box if the server name should exactly match the name in the certificate.

6. Click **OK** to apply the settings.

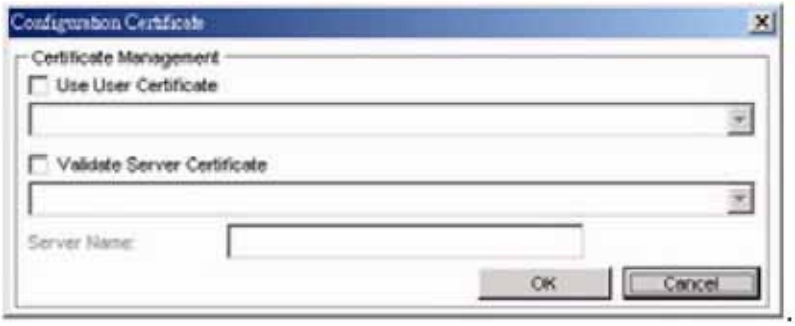
Server Certificates require a wired connection to the network so you Can obtain the certificate(s) from the certificate authority. Your network administrator can provide on certificate management.

.

CONFIGURING 802.1X – EAP-TLS



1. At **Security Mode** select **WPA** or **WPA2** from the drop-down menu.
2. At **Authentication Protocol** select **TLS** from the drop-down menu.
3. TLS requires both server and user certification. Click **Configure Certificate** (see **Note** below). The following window appears:



Use user certificate	Check this box if your network requires user certification and then select the certificate from the drop-down menu.
Validate server certificate	Check this box if your network requires server certification and then select the certificate authority from the drop-down menu.
Server name:	Type in the name of the server that is used for 802.1X authentication.
Server name should match exactly	Check this box if the server name should exactly match the name in the certificate.

5. Click **OK** to apply the settings.

Server Certificates require a wired connection to the network so you Can obtain the certificate(s) from the certificate authority. Your network administrator can provide on certificate management.

.

Glossary

For unfamiliar terms used below, look for entries elsewhere in the glossary.

AD-HOC (IBSS)

Ad-hoc mode does not require an AP or a wired network. A network that transmits wireless from computer to computer without the use of a base station (access point).

Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

CHANNEL

A radio frequency used by a wireless device is called a channel.

EAP AUTHENTICATION

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1X transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

ENCRYPTION

The reversible transformation of data from the original to a difficult-to-interpret format. Encryption is a mechanism for protecting confidentiality, integrity, and authenticity of data. It uses an encryption algorithm and one or more encryption keys.

FRAGMENTATION THRESHOLD

This is the maximum data fragment size that can be sent before the packet is fragmented into smaller packets.

IEEE 802.1X

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

INFRASTRUCTURE (BSS)

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

ROAMING

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization among other factors.

SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server.

USER AUTHENTICATION

WPA applies IEEE 802.1X and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. If you do not have an external RADIUS server, use WPA-PSK/WPA2-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, clients will be granted access to a WLAN.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the WCB-321A and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA/WPA2

Wi-Fi Protected Access (WPA) and WPA2 (future upgrade) is a subset of the IEEE 802.11 i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Appendix

This section provides maintenance and troubleshooting procedures. The following topics are discussed:

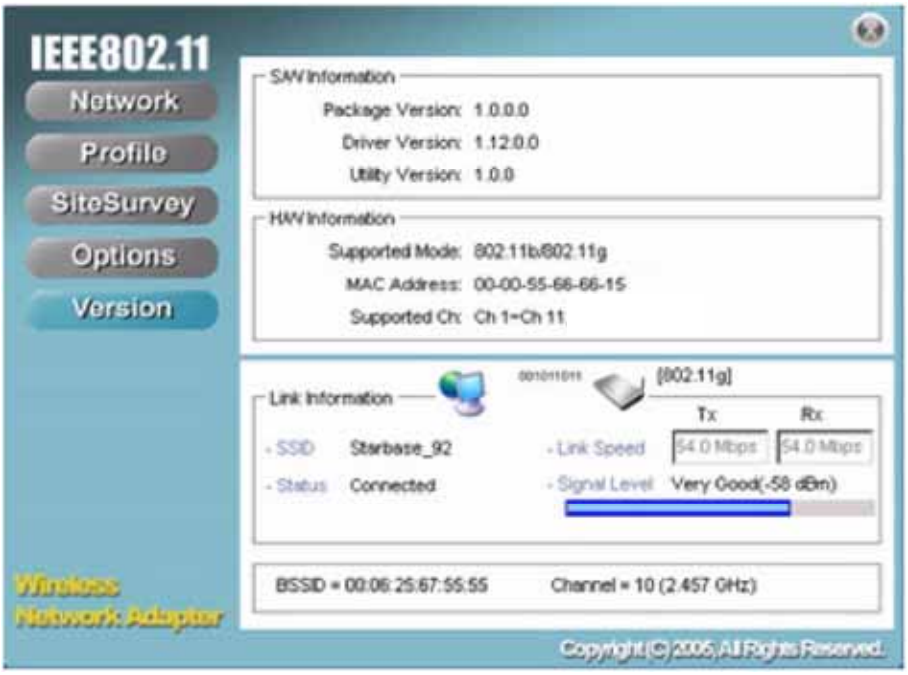
- See "Maintenance"
- See "Troubleshooting"

Maintenance

Installing a newer version of the Wireless Client Utility may improve the performance of the WCB-321A. Before installing the new version, you must uninstall the old one.

CHECKING THE WIRELESS CLIENT UTILITY VERSION

To check the current Wireless Client Utility, open the utility on the Version screen. In the **S/W Information** pane, note the **Utility Version** number.



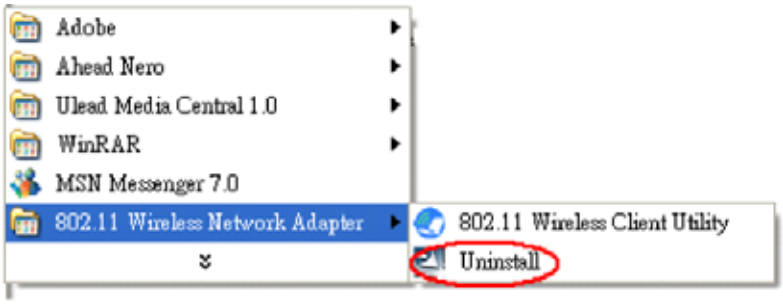
IMPORTANT

If you need to contact technical support, you will need to provide the S/W Information. Be sure to check the screen in the utility that is installed on your computer and not the screen shown in this manual.

UNINSTALLING THE WIRELESS CLIENT UTILITY

Refer to the following to uninstall (remove) the Wireless Client Utility from your computer.

1. Click **Start -> All Programs** (Windows 2000 **Programs) -> 802.11 Wireless Network Adapter -> Uninstall.**



2. When prompted, click **Yes** to remove the driver and utility software.

3. Click **Finish** to complete the uninstallation.
4. Reboot your computer if prompted.

UPGRADING THE WIRELESS CLIENT UTILITY

Contact your dealer or technical support for details on downloading the current Wireless Client Utility. Refer to the following to upgrade the Wireless Client Utility.

1. Double-click the Setup.exe file that you downloaded. The installation wizard screen opens.
2. Click **Next** to continue.
3. Click **Next** in the **Choose Destination Location** screen.
4. Click **Install** to begin the installation.
5. Click **Finish** to exit the wizard and complete the installation.

Troubleshooting

PROBLEMS STARTING THE 802.11 WIRELESS CLIENT UTILITY PROGRAM

PROBLEM	CORRECTIVE ACTION
Windows does not auto-detect the WCB-321A.	Make sure the WCB-321A power switch is turned off and properly inserted into the USB port and then restart your computer.
	Perform a hardware scan by clicking **Start, Settings, Control Panel** and then double-click **Add/Remove Hardware.** (Steps may vary depending on Windows version). Follow the on-screen instructions to search for the WCB-321A (Wireless 802.11 USB Network Adapter) and install the driver.
	Check for possible hardware conflicts. In Windows, click **Start, Settings, Control Panel, System, Hardware** and then click **Device Manager.** Verify the status of the WCB-321A (Wireless 802.11 USB Network Adapter) under **Network Adapter.** (Steps may vary depending on the Windows version).
	Install the WCB-321A in another computer. If the error persists, there may be a hardware problem. In this case, please contact your local dealer for support.

PROBLEMS WITH THE LINK STATUS

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time from the status bar.	Search and connect to another AP with a better link quality using the **Site Survey** screen. Change the channel used by your AP. Move your computer closer to the AP or the peer computer(s) within the transmission range. There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.

PROBLEMS WITH SECURITY SETTINGS

"Disconnected" (meaning authentication failure) Shown in the Status Bar	Make sure your AP/Router has the same setting as your client adapter and follow AP/Router's security settings.
LED PWR and LINK are on but cannot receive or sending data and connect to network	Make sure your AP/Router has the same setting as your client adapter and follow AP/Router's security settings.

Problems Communicating With Other Computers

PROBLEM	CORRECTIVE ACTION
The WCB-321A computer cannot communicate with the other computer.	Make sure you are connected to the network.

Infrastructure	Make sure that the AP and the associated computers are turned on and working properly. Make sure the WCB-321A computer and the associated AP use the same SSID. Change the AP and the associated wireless clients to use another radio channel if interference is high. Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Settings** screen.
Ad-Hoc (IBSS)	Verify that the peer computer(s) is turned on. Make sure the WCB-321A computer and the peer computer(s) are using the same SSID and channel. Make sure that the computer and the peer computer(s) share the same security option and key. Change the wireless clients to use another radio channel if interference is high.