

IEEE 802.11b/g Wireless USB 2.0 Adapter



ALL0283 User's Manual Version: 2.0

Table of Contents

1	INTR	RODUCT		4
	1.1	FEATUR	ES & BENEFITS	. 4
	1.2		E CONTENTS	
	1.3	USB AD	DAPTER DESCRIPTION	5
	1.4		I REQUIREMENTS	-
	1.5		NTIONS	
	1.6	NETWOR	RK CONFIGURATION	. 7
2	INST	ALL DR	IVERS & CLIENT UTILITY	9
	2.1		You Begin	
	2.2	INSTALL	ING THE DRIVERS	9
3	USIN	IG THE	CLIENT UTILITY	15
	3.1		NT STATUS	
	3.2	Profile	E MANAGEMENT	16
	3.2.1		n for available networks	
	3.2.2		te a New Profile	
	3.2.3		ırity	
	-	2.3.1	Security Disabled	
		2.3.2	WPA / WPA2 – TLS, TTLS	
		2.3.3 2.3.4	WPA / WPA2 – PEAP (EAP-GTC)	22
		2.3.4 2.3.5	WPA / WPA2 – PEAP (EAP-WSCHAP-V2)	24 26
	-	2.3.5	WPA / WPA2 – Passphrase	
	-	2.3.7	802.1x – TLS, TTLS	
	_	2.3.8	802.1x – PEAP (EAP-GTC)	
	_	2.3.9	802.1x – PEAP (EAP-MSCHAP-V2)	32
		2.3.10	802.1x – LEAP	
	3.:	2.3.11	Pre-Shared Key (Static WEP)	
	3.2.4	1 Adva	anced Settings	37
	3.	2.4.1	Infrastructure Settings	
	-	2.4.2	Ad Hoc Settings	
	3.3		STICS	
	3.4		/ DISABLE RADIO	
	3.5		TRAY ICON	
	3.6		SETTINGS	
4			THE DRIVERS & CLIENT UTILITY	
AF	PPENDI	X A – SF	PECIFICATIONS	47
AF	PPENDI	X B – F0	CC INTERFERENCE STATEMENT	48

Revision History

Version	Date	Notes
1.0	June 9, 2005	Initial Version
1.1	Oct. 12, 2005	Utility Upgrading
1.2	Oct 14, 2005	Spec updating
2.0	May 16, 2006	Security spec updating

1 Introduction

This is a wireless USB 2.0 adapter that supports the IEEE 802.11b/g (2.4GHz) radio operation. It provides a high-speed wireless connection with data rate up to 108Mbps.

To protect your wireless connectivity, the high-speed wireless USB adapter can encrypt all wireless transmissions through 64/128/152-bit WEP data encryption and also supports WPA. Dynamic Frequency Selection (DFS) puts your network on the cleanest channel in your location. With the high-speed wireless USB adapter, you will experience the best wireless connectivity available.

This chapter describes the features & benefits, package contents, applications, and network configuration.

Features	Benefits
High Speed Data Rate up to 108 Mbps in	Capable of handling heavy data payloads
Super G mode	such as MPEG video streaming.
High Output Power up to 23 dBm	More high power can advance the distance.
Advanced Encryption Standard (AES),	Powerful data security.
Temporal Key Integrity Protocol (TKIP) and	
Wired Equivalent Private (WEP)	
IEEE802.1x Client Support	Enhances authentication and security.
Support for 802.11e standard	Wireless Multimedia Enhancements Quality of
	Service support (QoS)
Advanced Power Management	Low power consumption in power saving
	mode up to 98%.
Support eXtended Range technology	eXtended Range technology give Wi-Fi
	products twice the range of existing designs

1.1 Features & Benefits

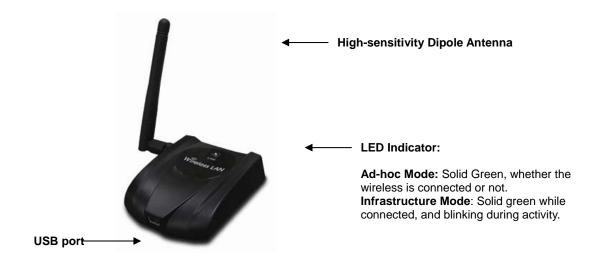
1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- > One Wireless LAN USB Adapter
- One USB Cable
- > One CD-ROM with User's Manual Included

1.3 USB Adapter Description

The USB adapter is a standard USB adapter that fits into any USB interface. The USB adapter has a LED indicator and an external high-sensitivity dipole antenna.



1.4 System Requirements

The following are the minimum system requirements in order to use the USB adapter.

- > PC/AT compatible computer with a USB interface.
- > Windows 2000/XP operating system.
- 20 MB of free disk space for installing the USB adapter driver and utility program.

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) Difficult-to-wire environments

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) Temporary workgroups

Consider situations in parks, athletic arenas, exhibition centers, disasterrecovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) The ability to access real-time information Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) Frequently changed environments Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) Small Office and Home Office (SOHO) networks SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

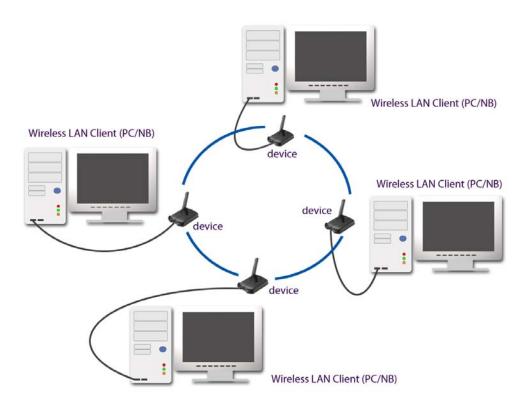
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1.6 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.

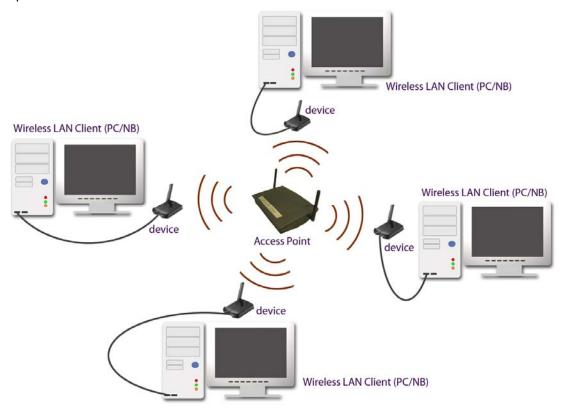
a) Ad-hoc (peer-to-peer) Mode



This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-topeer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.

b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



Version 2.0

2 Install Drivers & Client Utility

2.1 Before You Begin

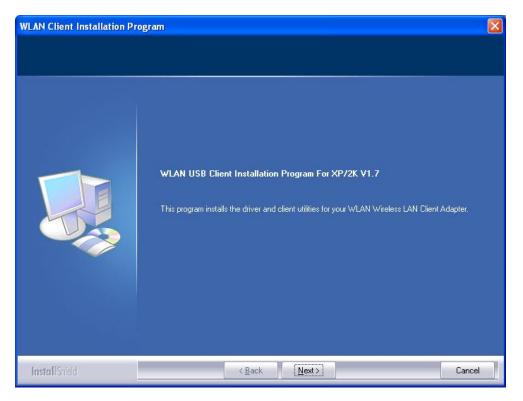
Before installing the new drivers of your USB adapter, you need to disable all of the Wireless LAN drivers that you have installed.

During the installation, Windows XP/2K/ME/98 may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS \OPTIONS\CABS directory.

2.2 Installing the Drivers

Follow the steps below in order to install the USB adapter drivers:

- 1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.
- 2. Once the setup begins you will see the **Install Shield Wizard**, as the image depicts below.



- Click on the **Next** button to continue.
 The Setup Wizard will then allow you to install the driver & utility or just the driver. Select the first option: Install Client Utilities and Driver.

WLAN Client Installation Progr	am	
Setup Type Select the setup type that best suit	s your needs.	
	Click the type of setup you prefer. Install Client Utilities and Driver Install Driver Only	Description Choose this option to install the driver and client utilities. This is the recommended option.
InstallShield	< <u>B</u> ack <u>N</u> ext >	Cancel

- 5. Click on the **Next** button to continue.
- 6. This message informs you that the system must be restarted after the installation is complete.

Questio	n 🛛 🔀
?	The option you have selected requires the system to be rebooted at the end of the operation. Do you wish to continue?

7. Click on the Yes button to continue.

WLAN Client Installation Pro	gram	
Choose Destination Location Select the folder where the insta	allation program will install the files.	
	The installation program will install the client utilities in the following location:	
	-Destination Folder- C:\Program Files\WLAN	
InstallShield	< Back Next> Canc	el

8. Click on the **Browse** button to select another drive or folder to install the drivers, and then click on the **Next** button. If you would like to use the default destination folder, click on the **Next** button.

WLAN Client Installation Prop	gram	\mathbf{X}
Select Program Folder Select a program folder.		
	The installation program will add program icons to the Program Folder listed below. You may enter a new folder name or select one from the Existing Folders list. Program Folder: VLAN Existing Folders: Actimistrative Tools Games Startup	
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel	

9. Select a program folder for the Start menu, or use the default setting: **WLAN**. Click on the **Next** button to continue.

WLAN Client Installation Program
WLAN USB Client Installation Program For XP/2K V1.7
IMPORTANT: Please Read!
On Windows XP, you can configure your WLAN Wireless LAN Client Adapter through the WLAN Client Utility (ACU) or a third-party supplicant. Because third-party tools may not provide all of the functionality available in the ACU, WLAN recommends that you use the ACU. (Please note that a patch from Microsoft might be required to use the Microsoft tool with WPA security.) On the next screen, select whether you want to use the ACU or a third-party tool to configure your client adapter. NOTE: If you select a third-party tool, some of the ACU features will not be available. To
activate those features, you must install the ACU.
< <u>Back</u> Cancel

10. The message depicted above informs you about configuring this device through the 802.11 Client Utility (ACU) or a third party supplicant. If you choose to use a third party supplicant, some of the ACU features will not be available. Click on the **Next** button to continue.

WLAN Client Installation Program		
Choose Configuration Tool		
	Which tool will you use to configure your client adapter?	
	 WLAN Client Utility (ACU) and Supplicant. 	
	Third-Party Supplicant	
InstallShield	< <u>B</u> ack <u>N</u> ext>	Cancel

11. Select one of the options. However, it is recommended to select the first option: **802.11 WLAN Client Utility and 802.1x Supplicant**. Click on the **Next** button to continue.



- 12. At this point, carefully insert the device into the PCMCIA slot of your computer, and click on the **OK** button.
- 13. Windows will automatically detect the device and display the Found New Hardware Wizard, as the image depicts below. It will ask you to connect to the Windows Update website, to search for software. Select No, not this time, and click on the Next button.

Found New Hardware Wizard		
	Welcome to the Found New Hardware Wizard Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission). Read our privacy policy Can Windows connect to Windows Update to search for software? Yes, this time only Yes, now and every time I connect a device No, not this time Click Next to continue.	
	< Back Next > Cancel	

- 14. Once again the **Found New Hardware** Wizard will ask you to install software. Click on the **Cancel** button to continue.
- 15. If you are using Windows XP, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

Har dwa	re Installation
1	The software you are installing for this hardware: WLAN USB 2.0 Wireless Adapter Bootloader Download has not passed Windows Logo testing to verify its compatibility with Windows XP. (<u>Tell me why this testing is important.</u>) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
	Continue Anyway STOP Installation

16. Once again, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

Hardware Installation		
	The software you are installing for this hardware: WLAN USB 2.0 Wireless Network Adapter has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.	
	Continue Anyway STOP Installation	

17. A message will then appear indicating that the installation process is complete Click on the **OK** button to reboot the system.

3 Using the Client Utility

After a successful installation you will see the Cardbus adapter **Client Utility** in the Windows Program group called **802.11 WLAN.**

To run the Client Utility click **Start > Programs > IEEE WLAN USB**. You will then see the Client Utility icon in the system tray of your computer.

To open the Client Utility, right click on the icon in the system tray, and then select **Open WLAN Client Utility**.

Client Utility Exit Open WLAN Client Utility... Disable Radio Show Connection Status Select Profile

o 🔊 🖞 👘

3.1 Current Status

The **Current Status** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.

A WLAN Clie	nt Utility - Currer	nt Profile: Default	? 🛛
Action Options	Help		
Current Status	Profile Management	Diagnostics	
	Profile Name:	Default	Total 80211
	Link Status:	Associated	G N
	Wireless Mode:	2.4 GHz 54 Mbps	IP Address: 192.168.1.204
	Network Type:	Infrastructure	Current Channel: 8
Server	Based Authentication:	None	Data Encryption: None
	Signal Strength:		Excellent
			Advanced
L			

- Profile Name: Displays the name of this profile. One device can have many profiles, but only one profile can be loaded at a time.
 Note: The profile name and network name (SSID) are not the same.
- Link Status: This indicates the state of the client, associated or not associated.
- Wireless Mode: Displays the 802.11 mode such as: 2.4GHz 11 Mbps, 2.4GHz 54 Mbps, 2.4GHz 108Mbps.
- Network Type: Displays the type of network, such as: Infrastructure or Ad-hoc.
- Server Based Authentication: Displays information about the authentication method.
- > IP address: Displays the IP address of this device.
- Current Channel: Displays the channel at which this device is connected.
- > Current Channel: Displays the type of encryption used.
- > Signal Strength: Displays the strength of the signal.

Click on the **Advanced** button to view more details about the current status. This window includes information such as: network name (SSID), AP MAC address, power save mode, power levels, signal strength, noise level, channel, frequency, and channel set (country). Click on the **OK** button to close the window.

Network Name (SSID):	RD5_3Com	Current Signal Strength:	-57 dBm
Server Based Authentication:	None	Current Noise Level:	-96 dBm
Data Encryption:	None	Up Time:	00:08:35
Authentication Type:		802.11b Preamble:	Short & Long
Message Integrity Check:	None	Current Receive Rate:	12.0 Mbps
QoS:	None	Current Transmit Rate:	48.0 Mbps
		Channel:	8
		Frequency:	2.447 GHz
Associated AP MAC Address:	00-14-7C-53-C5-C4	Channel Set:	United States
Power Save Mode:	Normal		

3.2 Profile Management

The second tab displayed is the **Profile Management** tab. This tab is used to create a new profile, modify an existing profile, remove an existing profile, and activate an existing profile.

Options Help ent Status Profile Manage	ment Diagnostics	
	Diagnostics	
Default wlan		<u>N</u> ew
wan		Modify
		Remo <u>v</u> e
		Activate
)etails		
Network Type:	Infrastructure	Import
Security Mode:	Pre Shared Key	
Network Name 1 (SSID1)	SENAOWL	Export
Network Name 2 (SSID2)	: <empty></empty>	S <u>c</u> an
Network Name 3 (SSID3)	<pre><empty></empty></pre>	<u>50</u> an

3.2.1 Scan for available networks

Click on the **Scan** button to view a list of available infrastructure and ad-hoc networks. This table lists the network name, encryption key if required, signal strength, channel, and wireless mode.

🔞 Super XR	Signal Strength	Channel	Wireles 🔷
a 1	1 50 dB	8	2.4 GHz
a 1	1 21 dB	1	2.4 GHz
a 1]] 8 dB	10	2.4 GHz
1	1 35 dB	7	2.4 GHz
10 I	1] 15 dB	11	2.4 GHz
	1 25 dB	2	2.4 GHz
	1 2 2 2 2 3 3 2 5 4 C	4	2.4 GHz
	1 36 dB	5	2.4 GHz
	1 35 dB	8	2.4 GHz
	חו דר 🗈	C	_ <u></u>
		 3 11 21 dB 3 11 8 dB 11 35 dB 35 dB 15 dB 12 dB 132 dB 136 dB 11 36 dB 11 35 dB 	 and 21 dB and 8 dB and 35 dB and 15 dB and 15 dB and 25 dB and 25 dB and 32 dB and 36 dB 5 and 35 dB

If you would like to associate with a specific network, select the network name (SSID) and then click on the **Activate** button. You will then get connected to the network if you have the correct permission keys.

3.2.2 Create a New Profile

Multiple profiles can be created for different Network Names (SSIDs). This allows a user to quickly associate with another network, instead of entering the credentials each time.

Options Help ent Status Profile Manageme	ent Diagnostics	
Default		<u>N</u> ew
w lan		Modify
		Remoye
		Activate
etails		
Network Type:	Infrastructure	Import
Security Mode:	Pre Shared Key	
Network Name 1 (SSID1):	SENAOWL	<u>Export</u>
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	Julia Sugar

Click on the **New** button to create a new profile. You will then see the **General** tab of the profile management window.

ofile Management	?
eneral Security Advance	d
Profile Settings Profile Name:	Wian
Client Name:	SW
Network Names	
SSID1:	SENAOWL
SSID2:	
SSID3:	
	OK Cancel

- Profile Name: Enter a name for this profile; this can be any name that you may associate with your network. This feature comes in handy when you need to work at several locations where there are different network settings. Using this you can configure a different profile for each of your networks.
- > Client Name: Enter any name to describe the profile.
- SSID1: Enter the SSID of the network. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- Click on the **OK** button to continue.

3.2.3 Security

The next tab displayed is the **Security** tab. Here you can configure the authentication and encryption method that is used on your network. There are five types of security methods available: none, WPA, WPA-PSK, 802.1x, Pre-shared WEP key. The configuration steps for each method are described below.

3.2.3.1 Security Disabled

If your network does not require any security methods, then select **None** in the security tab, and then click on the **OK** button.

Profile Management			? 🛛
General Security Adv.	anced		
Set Security Options			
O WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	~
O WPA/WPA2 Pa	assphrase		
O 802.1x	802.1x EAP Type:	LEAP	~
O Pre-Shared Key	(Static WEP)		
None None			
Configure	Group Policy Delay: 0 0 sec	lixed Cells	
		C	OK Cancel

3.2.3.2 WPA / WPA2- TLS, TTLS

WPA2 (Wi-Fi Protected Access 2) provides network administrators with a high level of assurance that only authorized users can access the network. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with.

Select the **WPA/WPA2** radio button, and then select **EAP – TLS** or **EAP – TTLS** from the drop-down list. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

Profile Management			? 🛛
General Security Advanced			
Set Security Options			
SWPA/WPA2	WPA/WPA2 EAP Type:	NOR NEWS	
○ WPA/WPA2 Passphrase		EAP-TLS EAP-TTLS	
○ 802.1×	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
O Pre-Shared Key (Static WEP)		LEAP EAP-FAST	
◯ None			1
Configure		tan terretar	
Group Policy Delay:	Allow Association to M	ixed Lells	
			Cancel

Click on the **Configure** button to configure the TTLS settings.

Define EAP-TTLS Configuration	? 🛛
Use Machine Information For Domain Logon Trusted Root Certification Authorities	
<any></any>	~
User Information for EAP-TTLS Authentication User Name: iames Password: Confirm Password:	
Settings OK Car	ncel

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- > Confirm Password: Re-type the password.

Click on the Settings button.

Configuration Settings	? 🛛
Specific Server or Domain:	
Login Name:	james
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.3 WPA/WPA2 – PEAP (EAP-GTC)

PEAP (EAP-GTC) was standardized along with EAP in RFC 2284. EAP-GTC allows the exchange of clear text authentication credentials across the network. The GTC method does provide a way to move a simple username and password from client to server using an EAP method, so it can be used to provide an authentication method. Naturally, if EAP-GTC is used to transport reusable passwords, it must be used inside a tunnel for protection and server authentication. EAP-GTC can be used with both TTLS and PEAP.

Select the **WPA/WPA2** radio button, and then select **PEAP (EAP-GTC)** from the drop-down list.

WHAWHAL WHAWHAL WPA/WPA2 Passphrase EAP-TLS 802.1x 802.1x EAP Type: Pre-Shared Key (Static WEP) EAP-TAST	Set Security Options		
WPA/WPA2 Passphrase EAP-TTLS EAP-TTLS B02.1x B02.1x B02.1x EAP Type: Pre-Shared Key (Static WEP) None Configure	⊙ WPA/WPA2	WPA/WPA2 EAP Type:	Contraction and a second se
802.1x 802.1x EAP Type: PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP EAP-FAST None None	○ WPA/WPA2 Passphrase		
Pre-Shared Key (Static WEP) EAP-FAST None Configure	○ 802 1×	802.1x EAP Type:	PEAP (EAP-GTC)
			LEAP
Configure			EAP-FAST
Configure	() None		
Allow Association to Mixed Cells	Configure	Allow Association to M	ixed Cells
Group Policy Delay: 60 🗢 sec	Group Policy Delay:	60 🗢 sec	

Click on the **Configure** button to configure the PEAP (EAP-GTC) settings.

Define PEAP (EAP-GTC) C	onfiguration	? 🔀
Use Machine Information F	or Domain Logon	
Trusted Root Certification Auth		
<any></any>		~
- Set Password		
🔿 Token		
Static Password		
- User Information for PEAP (G		
User Name:	james	
Password:		
Confirm Password:		
	Settings	ancel

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Set Password: Select Token or Static Password radio button. The default setting is Static Password.

Click on the Settings button.

Configuration Settings	2 🛛
Specific Server or Domain:	
Login Name:	james

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the OK button to return to the previous window. Once again, click on

the **OK** button to return to the Profile Management window.

3.2.3.4 WPA/WPA2 – PEAP (EAP-MSCHAP-V2)

The PEAP (EAP-MSCHAP V2) authentication type is based on EAPTLS authentication, but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key, which is derived from the device and RADIUS server, to encrypt data.

Select the **WPA/WPA2** radio button, and then select **PEAP (EAP-MSCHAP-V2)** from the drop-down list.

⊙ WPA/WPA2	WPA/WPA2 EAP Type:	PEAP (EAP-MSCHAP V2)	~
○ WPA/WPA2 Passphrase		EAP-TLS EAP-TTLS	
○ 802.1x	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
O Pre-Shared Key (Static WEP)		LEAP EAP-FAST	
O None			
Configure	- AB	tool early	
Group Policy Dela	Allow Association to M Allow Association to M	ixed Lelis	

Click on the **Configure** button to configure the PEAP (EAP-MSCHAP-V2) settings.

Define PEAP (EAP-MSCHAP	PV2) Configuration	? 🔀
Use Machine Information F Trusted Root Certification Auth		
<any></any>		~
User Information for PEAP (E User Name:	AP-MSCHAP V2) Authentication	
Password:	•••••	
Confirm Password:		
S	ettings OK Cano	;el

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the Settings button.

Configuration Settings	? 🔀
Specific Server or Domain: Login Name:	james
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN.

Select the WPA/WPA2 radio button, and select LEAP from the drop-down list.

EAP-TLS		
EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	802.1x EAP Type:	○ WPA/WPA2 Passphrase ○ 802.1x
LEAP EAP-FAST	2)	O Pre-Shared Key (Static WB
		◯ None
ixed Cells	Allow Association to Mi	Configure
	licy Delay: 60 ᅌ sec	Group P
ixed Cells	A CONTRACTOR OF A CONTRACTOR O	

Click on the **Configure** button to configure the LEAP settings.

Isername and Password Settings	
O Use Temporary User Name and Password	
 Automatically Prompt for User Name and Password Manually Prompt for User Name and Password 	
OUse Saved User Name and Password	
User Name:	
Password:	
Confirm Password:	
Domain:	
✓ Include Windows Logon Domain with User Name	
✓ No Network Connection Unless User Is Logged In	
Authentication Timeout Value (in seconds)	90
OK	Cancel

- Use Temporary User Name and Password: Select this radio button for a temporary user name and password. This will manually prompt for the user name and password.
- Use Saved User Name Password: Select this radio button if the user name and password will be saved in this profile.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the OK button to return to the previous window

3.2.3.6 WPA/WPA2 – Passphrase

WPA/WPA2 Passphrase 802.1x EAP Type: LEAP 9 Pre-Shared Key (Static WEP) 9 None Configure Allow Association to Mixed Cells	WPA/WPA2 Passphrase 802.1x EAP Type: LEAP Pre-Shared Key (Static WEP) None Configure	Set Security Options		
802.1x 802.1x EAP Type: LEAP Pre-Shared Key (Static WEP) None Configure Allow Association to Mixed Cells	802.1x 802.1x EAP Type: LEAP Pre-Shared Key (Static WEP) None Configure Allow Association to Mixed Cells	O WPA/WPA2	WPA/WPA2 EAP Type: LEAP	~
) Pre-Shared Key (Static WEP)) None Configure	Pre-Shared Key (Static WEP) None Configure Allow Association to Mixed Cells	WPA/WPA2 Passphrase		
None Configure Allow Association to Mixed Cells	Configure	◯ 802.1x	802.1x EAP Type: LEAP	v

Select the **WPA/WPA2 Passphrase** radio button and then click on the **Configure** button.

Define WPA/WPA2 Pre-Shared Key	? 🔀
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters)	
ОК	Cancel

► Enter a WPA/WPA2 passphrase. For ASCII text, enter 8-63 characters,

for hexadecimal enter 64 characters).

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.7 802.1x – TLS, TTLS

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

○ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	Y
🔿 WPA/WPA2 Passphrase			
	802.1x EAP Type:	EAP-TTLS	~
O Pre-Shared Key (Static WEF	2)	EAP-TLS EAP-TTLS	
◯ None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
		LEAP	
Configure	Allow Association to M	EAP-FAST Host Based EAP	
Group Pol	icy Delay: 60 😂 sec		

Select the **802.1x** radio button, and then select **EAP – TLS** or **EAP – TTLS** from the drop-down list. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

Click on the **Configure** button to configure the TTLS settings.

Define EAP-TTLS Configuration	? 🗙
Use Machine Information For Domain Logon Trusted Root Certification Authorities	
<any></any>	~
User Information for EAP-TTLS Authentication User Name: iames Password: Confirm Password:	
Settings OK Can	cel

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- > Confirm Password: Re-type the password.

Click on the Settings button.

Configuration Settings	? 🔀
Specific Server or Domain: Login Name:	james
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.8 802.1x – PEAP (EAP-GTC)

PEAP (EAP-GTC) was standardized along with EAP in RFC 2284. EAP-GTC allows the exchange of clear text authentication credentials across the network. The GTC method does provide a way to move a simple username and password from client to server using an EAP method, so it can be used to provide an authentication method. Naturally, if EAP-GTC is used to transport reusable passwords, it must be used inside a tunnel for protection and server authentication. EAP-GTC can be used with both TTLS and PEAP.

Select the **802.1x** radio button, and then select **PEAP (EAP-GTC)** from the dropdown list.

) WPA/WPA2) WPA/WPA2 Passphrase	WPA/WPA2 EAP Type:	LEAP	*
802.1x) Pre-Shared Key (Static WEP)) None Configure Group Policy Delay:	802.1x EAP Type:	EAP-TLS EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP	~

Click on the **Configure** button to configure the PEAP (EAP-GTC) settings.

Define PEAP (EAP-GTC) C	onfiguration	? 🔀
Use Machine Information F	or Domain Logon	
Trusted Root Certification Auth		
<any></any>		~
- Set Password		
🔿 Token		
 Static Password 		
User Information for PEAP (G		
User Name:	james	
Password:		
Confirm Password:		
	Settings OK Ca	ancel

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Set Password: Select Token or Static Password radio button. The default setting is Static Password.

Click on the Settings button.

Configuration Settings	? 🛛
Specific Server or Domain: Login Name:	
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the OK button to return to the previous window. Once again, click on

the **OK** button to return to the Profile Management window.

3.2.3.9 802.1x – PEAP (EAP-MSCHAP-V2)

The PEAP (EAP-MSCHAP V2) authentication type is based on EAPTLS authentication, but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key, which is derived from the device and RADIUS server, to encrypt data.

Select the **802.1x** radio button, and then select **PEAP (EAP-MSCHAP-V2)** from the drop-down list.

General Security Advanced			
Set Security Options			
○ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	~
O WPA/WPA2 Passphrase			
	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
O Pre-Shared Key (Static W	EP)	EAP-TLS EAP-TTLS PEAP (EAP-GTC)	
O None		PEAP (EAP-MSCHAP V2)	
Configure	Allow Association to M		
Group F	'olicy Delay: 🚺 🤤 sec		

Click on the **Configure** button to configure the PEAP (EAP-MSCHAP-V2) settings.

Define PEAP (EAP-MSCHAP	PV2) Configuration	? 🔀
Use Machine Information F Trusted Root Certification Auth		
<any></any>		~
User Information for PEAP (EU)	AP-MSCHAP V2) Authentication	
Password:	•••••	
Confirm Password:		
S	ettings OK Canc	el

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the Settings button.

Configuration Settings	? 🔀
Specific Server or Domain:	
Login Name:	james
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.10 802.1x - LEAP

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN.

Select the **802.1x** radio button, and then select **LEAP** from the drop-down list.

eneral Security A	dvanced			
Set Security Optio	ns			
○ WPA/WPA2		WPA/WPA2 EAP Type	E LEAP	~
○ WPA/WPA2	Passphrase			
		802.1x EAP Type	LEAP	~
O Pre-Shared K	(ey (Static WEP)		EAP-TLS EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2	9
Configure.		Allow Association to I	LEAP	
	Group Policy Delay:	60 😂 sec		

Click on the **Configure** button to configure the LEAP settings.

LEAP Settings	
💿 Use Saved User Nam	e and Password
User Name:	
Password:	
Confirm Password:	
Domain:	
🗹 No Network Connec	gon Domain with User Name tion Unless User Is Logged In uthentication Timeout Value (in seconds) 90 📚
	OK Cancel

- Use Temporary User Name and Password: Select this radio button for a temporary user name and password. This will manually prompt for the user name and password.
- Use Saved User Name Password: Select this radio button if the user name and password will be saved in this profile.
- **User Name:** Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- > Confirm Password: Re-type the password.

Click on the **OK** button to return to the previous window

3.2.3.11 Pre-Shared Key (Static WEP)

You may select 64, 128 or 152 bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase.

ofile Management			?
eneral Security Advanced			
Set Security Options			
○ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	~
○ WPA/WPA2 Passphrase			
◯ 802.1x	802.1x EAP Type:	LEAP	~
Pre-Shared Key (Static WEF)	η		
O None			
Configure	Allow Association to M		
Group Poli		ixed Cells	
		c	OK Cancel

Select the **Pre-Shared Key (Static WEP)** radio button and click on the **Configure** button.

	?
ASCII Text (all keyboard characters)	
	·
	0
	0
	0
○ ○	0
ОК С	ancel
	WEP Key S 64 128

- Key Entry: Select Hexadecimal or ASCII depending on the WEP key that is used.
- > WEP Key Size: Select 64, 128, or 152 bit WEP key size.
- > Transmit Key: Enter the WEP key in the four WEP key text boxes.

Click on the OK button to return to the previous window

3.2.4 Advanced Settings

Click on the **Advanced** tab in the Profile Management section. Here you can configure the transmit power level, wireless mode, power save mode, and network type.

3.2.4.1 Infrastructure Settings

Profile Managemer	it				? 🔀
General Security A	Advanced				
Power Save Mode:	Normal	~			
Network Type:	Infrastructure	~			
802.11b Preamble:	Short & Long	O Long Only]		
Wireless Mode	bps	Wireless Mode W	'hen Starting Ad Ho	o Network	
🗹 2.4 GHz 11 M	bps	0 2.4 GHz 11 M	lbps		
Super G	nge (XR) TM	0 2.4 GHz 54 M	lbps	Channel: Auto	~
QoS		802.11 Authentic Auto	ation Mode	O Shared	
				Preferred APs.	
				ОК	Cancel

- ➤ Wireless Mode: Place a check in the preferred frequency and data rates.
- Power Save Mode: Select Maximum, Normal, or Off from the dropdown list. Selecting Maximum will save the most power; this is recommended if using a laptop running on battery. For other instances, use the Normal of Off setting.
- > Network Type: Select Infrastructure from the drop-down list.
- 802.11b Preamble: This setting should be the same as the access point. If you are not sure of that setting, select Short & Long.
- Preferred APs: Click on this button to add specific access points to this profile. Then enter the MAC addresses of the specific access points and then click on the OK button to return to the previous window.

Preferred Access Points	? 🛛
Specified Access Point MAC Addresses	
Access Point 1:	
Access Point 2:	
Access Point 3:	
Access Point 4:	
	OK Cancel

3.2.4.2 Ad Hoc Settings

Power Save Mode: Off		1	
Network Type: Ad Hoc		1	
802.11b Preamble: Short & Long	O Long Only]	
✓ Wireless Mode ✓ 2.4 GHz 54 Mbps ✓ 2.4 GHz 11 Mbps	Wireless Mode V	Vhen Starting Ad Ho Mbps	c Network
☑ SuperG ☑ eXtended Range (XR) TM	0 2.4 GHz 54 I	МЬря	Channel: Auto
QoS	- 802.11 Authentio	cation Mode	O Shared

- ► Wireless Mode: Place a check in the preferred frequency and data rates.
- > Network Type: Select Ad hoc from the drop-down list.
- ➤ 802.11b Preamble: This setting should be the same as the access point. If you are not sure of that setting, select Short & Long.

Click on the **OK** button to return to the previous window

3.3 Diagnostics

The third tab displayed is the **Diagnostics** tab. This tab displays the number of transmitted and received packets.

on Options Help		
rrent Status Profile Mana	gement Diagnostics	
Transmit		
Multicast Packets:	12	Adapter Information
Broadcast Packets:	1796	Advanced Statistics
Unicast Packets:	1298	Tha <u>T</u> arloog ortanismos
Total Bytes:	154059	
Receive		
Multicast Packets:	464	
Broadcast Packets:	4773	
Unicast Packets:	88	
Total Bytes:	706605	

Click on the **Adapter Information** button to view information about the Cardbus adapter such as: card name, MAC address, driver name, driver version, and driver date.

Adapter Informa	tion ? 🔀
Card Name:	WLAN USB 2.0 Wireless Network Adapter
MAC Address:	00-02-6F-3C-31-EB
Driver:	C:\WINDOWS\System32\DRIVERS\ar5523.sys
Driver Version:	1.5.0.102
Driver Date:	05 Jan 2006 16:56:08
Client Name:	SW
	(

Click on the **OK** button to return to the previous window

Click on the **Advanced Statistics** button to view detailed statistics about transmit and receive frames.

Transmit			
Frames Transmitted OK:	3208	RTS Frames:	1
Frames Retried:	215	CTS Frames:	1
Frames Dropped:	1569	No CTS Frames:	0
No ACK Frames:	96	Retried RTS Frames:	0
ACK Frames:	3208	Retried Data Frames:	215
Receive			
Beacons Received:	24376	Authentication Time-Out:	0
Frames Received OK:	7778	Authentication Rejects:	0
Frames Received with Errors:	39853	Association Time-Out:	0
CRC Errors:	4865	Association Rejects:	0
Encryption Errors:	98	Standard MIC OK:	0
Duplicate Frames:	36	Standard MIC Errors:	0
AP Mismatches:	0	CKIP MIC OK:	0
Data Rate Mismatches:	0	CKIP MIC Errors:	0

Click on the \mathbf{OK} button to return to the previous window

3.4 Enable / Disable Radio

To **disable** the radio, click on **Action** in the menu bar, and then click on **Disable Radio**.

A WLAN Client UI	tility - Curren	nt Profile: wlan	? 🛛
Action Options Help	<u> </u>		
Disable Radio Disable Tray Icon	Management	Diagnostics	
Exit	Profile Name:	wlan	Total 80211
	Link Status:	Associated	G
1	Wireless Mode:	2.4 GHz 11 Mbps	IP Address: 10.0.190.42
	Network Type:	Infrastructure	Current Channel: 1
Server Based	Authentication:	None	Data Encryption: WEP
	Signal Strength:		Excellent
			Advanced

You will then see a confirmation message "The RF signals for the following network card(s) have been successfully disabled".

WLAN Clie	ent Utility - Curren	t Profile: wlan	?
ction Option:	s Help		
Current Status	Profile Management	Diagnostics	
1.2	Profile Name:		Total 80211
	WLAN Client Utility		🔀 🔏 🔒
		following network card(s) have been	radicessially disabled.
Serve	WLAN USB 2.0 Wireles	ОК	
Serv o		ОК	учка споурчоп.

Click on the $\ensuremath{\text{OK}}$ button to continue.

To **enable** the radio, click on **Action** in the menu bar, and then click on **Enable Radio**.

A WLAN Client Utili	ty - Current Profile: wlan	? 🛛
Action Options Help		
Enable Radio Disable Tray Icon	fanagement Diagnostics	
Exit	Profile Name:	Total 80211
	Link Status: Not Associated	
Wi	reless Mode:	IP Address:
N	etwork Type:	Current Channel:
Server Based Au	ithentication:	Data Encryption:
Sig	nal Strength:	
F	Radio Status: Software Disabled	Advanced

You will then see a confirmation message "The RF signals for the following network card(s) have been successfully enabled".

🔥 WLAN Clie	nt Utility - Curren	t Profile: wlan	? 🗙
Action Options	Help		
Current Status	Profile Management	Diagnostics	
	Profile Name:		Total 80211
V	/LAN Client Utility	Personal and the second se	🛛 🖌 🔛
Serv a	The RF signals for the WLAN USB 2.0 Wireles	following network card(s) have been successfu ss Network Adapter	
	Signal Strength:		ī.
	Radio Status:	Software Disabled	Adyanced

Click on the **OK** button to continue.

3.5 Disable Tray Icon

To disable the tray icon, click on **Action** in the menu bar, and then click on **Disable Tray Icon**.

A WLAN Client U	Jtility - Currer	ıt Profile: wlan		? 🔀
Action Options He	elp			
Disable Radio Disable Tray Icon	Management	Diagnostics		
Exit	Profile Name:	wlan	Tota JGy	180211 H
	Link Status:	Associated		EXTERNO
	Wireless Mode:	2.4 GHz 11 Mbps	IP Address: 10.0.190.42	2
	Network Type:	Infrastructure	Current Channel: 1	
Server Base	ed Authentication:	None	Data Encryption: WEP	
	Signal Strength:		Excellent Advance	
			·	

You will then notice that the tray icon has disappeared from the system tray.

3.6 Display Settings

To change the display settings, click on **Options** in the menu bar, and then click on **Display Settings**.

A WLAN Client Utility - Curren	nt Profile: wlan	? 🛛
Action Options Help		
Currer Display Settings	Diagnostics	
Profile Name:	wlan	Total 80211 F
Link Status:	Associated	G DE
Wireless Mode:	2.4 GHz 11 Mbps	IP Address: 10.0.190.42
Network Type:	Infrastructure	Current Channel: 1
Server Based Authentication:	None	Data Encryption: WEP
Signal Strength:		Excellent
		Advanced

In this window you can change the Signal Strength Display Units from dBm to %, and increase or decrease the refresh interval rate, as well as displaying the data in a cumulative or relative fashion.

Display Settings		? 🛛
Signal Strength Display Units:	0%	OB
Refresh Interval (seconds):		3 🗘
Data Display:	O Relative	 Cumulative
	ОК	Cancel

Click on the **OK** button to return to the previous window.

4 Uninstall the Drivers & Client Utility

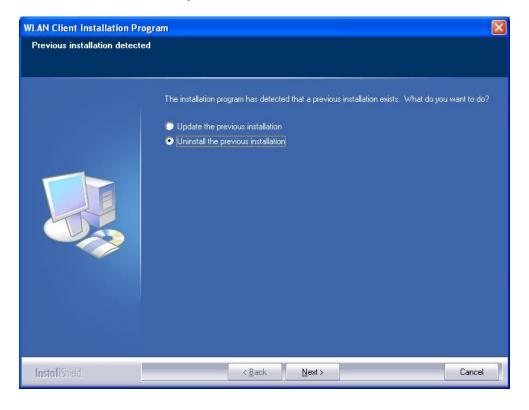
If the device installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the device and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the Drivers and Client Utility:

- 1. Click on Start > Settings > Control Panel > Add or Remove Programs
- 2. You will then see the following window. Select the Atheros Utility and then click on **Change/Remove**.

🐻 Add or R	emov	re Programs			
C <u>h</u> ange or Remove	*	子 Agere Systems AC'97 Modem	ort by:	Name	×
Programs		Windows XP Hotfix - KB822603 A WLAN USB Client Installation Program For XP/2K V1.7 Click here for support information.		Size Used	<u>0.51MB</u> frequently
Add <u>N</u> ew Programs		To change this program or remove it from your computer, click Change or Remove.		ast Used On Change	5/15/2006 Remove
5	~				

3. Click on Uninstall the previous installation radio button.



4. Click on the **Next** button to continue. You will then see the following message informing you that you must restart the system after installation.

Question	n 🛛 🛛 🔀
2	The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?

5. Click on the **Yes** button to continue. You will then see the following message asking you if you would like to remove the application.

Confirm Uninstall	
Do you want to completely remove the	selected application and all of its features?
	Cancel
	Cancer

6. Click on the **OK** button to continue. You will then see the following message asking you if you would like to remove the driver and all the existing profiles.

Question	n 🛛 🔛
?	Do you really wish to remove the device driver? This removes your profiles.

7. Click on the **Yes** button to continue. You must then restart your system to complete the Uninstallation.



8. Remove the device form your computer and then click on the **OK** button. The Uninstallation process is complete.

Appendix A – Specifications

Data Rates

802.11g: 6, 9, 12, 18, 24, 36, 48, 54, 72, 96 & 108 (Super G) Mbps

802.11b: 1, 2, 5.5, 11Mbps

Standards / Compliance IEEE802.11, IEEE802.11g, IEEE802.11b, draft IEEE 802.11e, and i standards, IEEE802.1x

Regulation Certifications

FCC Part 15/UL, ETSI 300/328/CE

Operating Voltage

 $5V \pm 0.25V$

Status LEDs

RF link activity

Drivers

Windows XP/2K/ME/98

RF Information

Frequency Band

U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations

Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology

802.11g: OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b: DSSS (DBPSK, DQPSK, CCK) Operating Channels

11 for North America, 14 for Japan, 13 for Europe

Receive Sensitivity (Typical)

- 2.412~2.472G(IEEE802.11g)
 6Mbps@ -91dBm;
 54Mbps@ -76dBm
- 2.412~2.472G(IEEE802.11b)
 11Mbps@ -91dBm;
 1Mbps@ -96dBm

Available transmit power

FCC

2.412~2.472G(IEEE802.11g)
 22 dBm @ 6 ~ 24 Mbps
 21 dBm @ 36 Mbps

20 dBm @ 48 Mbps 19 dBm @ 54 Mbps

2.412~2.472G(IEEE802.11b)
 22 dBm @1~11Mbps

ETSI

- 2.412~2.472G(IEEE802.11g)
 20 dBm @ 6 ~ 24 Mbps
 20 dBm @ 36 Mbps
 20 dBm @ 48 Mbps
 19 dBm @ 54 Mbps
- 2.412~2.472G(IEEE802.11b)
 20 dBm @1~11Mbps

Antenna

Detachable Dipole antenna (2dBi Gain)

Networking

Topology

Ad-Hoc, Infrastructure

Security

IEEE802.1x support for LEAP/PEAP WEP 64,128,152bit WPA (PSK,TKIP) WPA2 (AES)

Physical

Form Factor USB 2.0

Dimensions

75.2(L) mm x 53.9(W) mm x 14(H) mm

Weight

40 g/ 1.5oz

Environmental

Temperature Range

Operating: -0°C to 55°C Storage: -20°Cto 75°C

Humidity (non-condensing)

5%~95% Typical

Package Contents

One USB Adapter One USB Cable One CD-ROM with User's Manual and Drivers

Appendix B – FCC Interference Statement

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 equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

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.



Germering, 05.07.06

EC – Declaration of conformity

for

ALL0283 (802.11b/g USB Adaptor)



This equipment conforms with the requirements of the Council Directive **R&TTE 1999/5/EG** on the approximation of the laws of the member states relating to Radio and Telecommunication Terminal Equipment and the mutual recognition of their conformity.

The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL0283 (802.11b/g USB adaptor) conforms to the European Directives 73/23/EEC and 89/336/EEC.

This equipment meets the following conformance standards:

EMI: EN 50022 :1994 (A1 :1995, A2 :1997, Class B)

EMS: EN 55024 :1998 (A1 :2001, A2 :2003)

EN 60950:2000

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET Computersysteme GmbH Maistr. 2 82110 Germering

and can be downloaded from http://www.allnet.de/ce-certificates/ .