# IEEE 802.11a/b/g Wireless USB 2.0 Adapter



User's Manual Version: 1.2

# **Table of Contents**

1	INTRO	DUCTION	4
	1.1 F	EATURES & BENEFITS	4
	1.2 P/	ACKAGE CONTENTS	5
	1.3 U	ISB ADAPTER DESCRIPTION	5
	1.4 S <sup>v</sup>	YSTEM REQUIREMENTS	5
	1.5 AI	PPLICATIONS	6
	1.6 N	IETWORK CONFIGURATION	
2	INSTAL	LL DRIVERS & CLIENT UTILITY	9
	2.1 Bi	EFORE YOU BEGIN	9
	2.2 IN	ISTALLING THE DRIVERS	9
3	USING	THE CLIENT UTILITY	15
	3.1 C	URRENT STATUS	15
	3.2 Pi	ROFILE MANAGEMENT	16
	3.2.1	Scan for available networks	17
	3.2.2	Create a New Profile	18
	3.2.3	Security	19
	3.2.3	3.1 Security Disabled	19
	3.2.3	3.2 WPA – ILS, IILS	19
	3.2.3	$3.3  \text{WPA} = \text{PEAP} (\text{EAP-GTG}) \dots \dots$	
	3.2.0	3.5 WPA - I ΕΔΡ	25
	323	3.6 WPA – Passphrase	23
	3.2.3	3.7 802.1x – TLS. TTLS.	
	3.2.3	3.8 802.1x – PEAP (EAP-GTC)	30
	3.2.3	3.9 802.1x – PEAP (EAP-MSCHAP-V2)	32
	3.2.3	3.10 802.1x – LEAP	34
	3.2.3	3.11 Pre-Shared Key (Static WEP)	36
	3.2.4	Advanced Settings	37
	3.2.4	4.1 Infrastructure Settings	37
	3.2.4	4.2 Ad Hoc Settings	38
	3.3 D	NARIE / DIGARIE RARIO	39
	3.4 EI	NABLE / DISABLE RADIU	41 /3
	3.6 D	NSPLAY SETTINGS	
4	UNINS	TALL THE DRIVERS & CLIENT UTILITY	
Δ			
~			
A	PPENDIX B – FCC INTERFERENCE STATEMENT49		

# Revision History

Version	Date	Notes
1.0	June 20, 2005	Initial Version
1.1	Oct. 12, 2005	Utility Upgrading
1.2	Oct. 14, 2005	Spec Updating

# 1 Introduction

This is a wireless USB 2.0 adapter that supports dual-band 802.11a/b/g (2.4GHz & 5GHz) 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 108Mbps in	Capable of handling heavy data payloads
Super A/G mode	such as MPEG video streaming.
High Output Power up to 25 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 draft IEEE 802.11h and j	Extended tuning range (2.300-2.500 &
standard	4.900-5.850 GHz) for worldwide use
	Dynamic Frequency Selection/Transmit
	Power Control (DFS/TPC) for international
	operation
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.

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.



# 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 2000/XP 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.

802.11 WLAN Client Installatio	on Program	
Setup Type Select the setup type that best suits		
	Click the type of setup you prefer. Install Client Utilities and Driver (recommended) Install Driver Only	Description Choose this option to install the driver and client utilities. This is the recommended option.
	< <u>B</u> ack <u>N</u> e	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 🛛 🕅
2	The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?

7. Click on the Yes button to continue.

802.11 WLAN Client Installation	i Program	
Choose Destination Location Select the folder where the installation	n program will install the files.	
	The installation program will install the client utilities in the following location:	
	CDestination Folder	_1
	C:\Program Files\802.11 WLAN Browse	
	< Back Next > Cancel	٦

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.

802.11 WLAN Client Installation	Program	
Select Program Folder Select a program folder.		
	The installation program will add program icons to the Program Folder listed below. You may type - new folder name or select one from the Existing Folders list. Program Folder: IEEE WLAN USB Existing Folders: DVgate Plus InterVideo WinDVD 5 Memory Stick Utility Microsoft Office mobile PhoneTools Network Smart Capture Performance Balancer PowerPanel Sony Notebook Setup SoundMAX Trend Micro PC-cillin WinRAR	
	< <u>B</u> ack <u>N</u> ext > Cancel	1

9. Select a program folder for the Start menu, or use the default setting: **802.11 WLAN**. Click on the **Next** button to continue.

302.11 WLAN Client Installation Program	×
802.11 WLAN Client Installation Program	
IMPORTANT: Please Read!	
On Windows XP, you can configure your 802.11 Wireless LAN Client Adapter through the 802.11 Client Utility (ACU) or a third party supplicant. Because third party tools may not provide all of the functionality available in ACU, 802.11 recommends that you use 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 ACU or a third party supplicant to configure your client adapter.	
NOTE: If you select a third party supplicant, some of the ACU features will not be available. To activate those features, you must install ACU.	
nstallShield	
< Back Next > 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.

802.11 WLAN Client Installation Program	
Choose Configuration Tool	
Which tool will you use to configure your client adapter?	
802.11 WLAN NIC utility and Supplicant.	
<ul> <li>Third Party Supplicant</li> </ul>	
InstallShield	Next > 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.

802.11	WLAN Client Installation Program
♪	The installation program installs the driver automatically when the client adapter is inserted. Insert the adapter now if it is not yet inserted, cancel the Found New Hardware Wizard if it appears, and proceed with the installation. Click OK to continue.
	ОК

- 12. At this point, carefully insert the device into the USB port 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.



- 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.

lar dwa	re Installation
	The software you are installing for this hardware:
<u> </u>	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.

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 USB adapter **Client Utility** in the Windows Program group called **802.11 WLAN**.

To run the Client Utility click **Start > Programs > WLAN DUAL 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 802.11 WLAN Client Utility**.



# 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 802.11 WL	AN Client Utility -	Current Profile: wlan		
<u>Action</u> Options	Help			
Current Status	Profile Management	Diagnostics		
	Profile Name:	wlan		Total 802.11
	Link Status:	Associated		AG .
	Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
	Network Type:	Infrastructure	Current Channel:	11
Serve	r Based Authentication:	None	Data Encryption:	None
	Signal Strength:	*****		Excellent
				Advanced

□ **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.

- **State:** 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, 5GHz 54Mbps or 5GHz 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.



# 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 Managemer	t Diagnostics	
Default		New
wian		Modify
		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name 1 (SSID1):	WLAN	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	

# 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.

Network Name (SSID HotSpot	) ©3	Super XR	Signa	al Strength 1 dB	Channel 1	Wireless Mode
i mistest	<b>6</b> 77		11 7	dB	5	2.4 GHz 54 Mbps
😵 WLAN			<b>ul</b> 11	l dB	11	2.4 GHz 11 Mbps

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 Managemen	( Diagnostics	
Default		New
🐚 wlan		Modify
		Remove
		Activate
Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name 1 (SSID1):	WLAN	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

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

rofile M	anagement		?
General	Security Advanced		
	Profile Settings Profile Name: Client Name:	profile1 FAE-9PHBRXC24JH	
	Network Names SSID1:	wireless	
	SSID2:		
	SSID3:		
		ОК	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.

Set Security Options	
WPA EAP Type: LEAP	~
○ WPA Passphrase	
0 802.1x 802.1x EAP Type: LEAP	~
Pre-Shared Key (Static WEP)	
<ul> <li>None</li> </ul>	
Configure	d Cells

# 3.2.3.2 WPA – TLS, TTLS

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** 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.

Set Security Options			
⊙ WPA	WPA EAP Type:	EAP-TLS	~
○ WPA Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
O Pre-Shared Key (Static WEP)	UUZ. IN LAI Type.		
🔿 None			
Configure		Allow Association to Mixed Cell	s

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

<any></any>	<u>&gt;</u>
User Information for EA	P-TTLS Authentication
User Name:	james
Password:	
Confirm Password:	

□ **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 **Advanced** button.

Advanced Configuration	? 🛛
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 – 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** radio button, and then select **PEAP (EAP-GTC)** from the dropdown list.

Set Security Options		
() WPA	WPA EAP Type:	PEAP (EAP-GTC)
🔿 WPA Passphrase		EAP-TLS EAP-TTLS
○ 802.1×	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)
🔿 Pre-Shared Key (Static WEF	9	LEAP
○ None		
Configure		Allow Association to Mixed Cells

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

<pre>Irusted Rool <any></any></pre>	: Certification Authorities	~
User Name:	ismec	
Set Passwo	rd	
🔿 Toke	n	
	-	

- □ **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 **Advanced** button.

Advanced Configuration	? 🛛
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.

# 3.2.3.4 WPA – 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 radio button, and then select PEAP (EAP-MSCHAP-V2) from the drop-down list.

Set Security Options		
⊙ WPA	WPA EAP Type:	PEAP (EAP-MSCHAP V2)
🔿 WPA Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC)
O 802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)
O Pre-Shared Key (Static WEP)		
O None		
Configure		Allow Association to Mixed Cells

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

ne PEAP (EAP-MSCHAP	V2) Configuration	?
Trusted Root Certification	Authorities	
<any></any>		~
User Information for PEA User Name: Password:	P (EAP-MSCHAP V2) Authentication james	
Confirm Password:	•••••	
	Advanced OK	Cancel

- □ **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	Advan	iced	buttor
----------	-----	-------	------	--------

Advanced Configuration		? 🔀
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.

## 3.2.3.5 WPA – 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 WPA radio button, and then select LEAP from the drop-down list.

Set Security Options		
⊙ WPA	WPA EAP Type:	LEAP
O WPA Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC)
○ 802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)
O Pre-Shared Key (Static WEF	9	LEAP
O None		
Configure		Allow Association to Mixed Cells

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

LEAP Settings	? 🛛
LEAP username and passwo	rd settings
Use Temporary Use	er Name and Password
( Manually	Prompt for LEAP User Name and Password
🕞 Use Saved User Na	me and Password
User Name:	
Password:	
Confirm Password:	
Domain:	
V Include W V No Netwo	indows Logon Domain with User Name rk Connection Unless User Is Logged In tication Timeout Value (in seconds) 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 – Passphrase

file M	anagem	ent			?
eneral	Security	Advanced			
S	et Security	Options			
	0	WPA	WPA EAP Type:	LEAP	
	۲	WPA Passphrase			
	0	802.1x	802.1x EAP Type:	LEAP	
	0	Pre-Shared Key (Stati	c WEP)		
	0	None			
		Configure		Allow Association to Mixed Cells	
				ОК	Cance

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

Define WPA Pre-Shared Key	? 🛛
Enter a WPA Passphrase between 8 and 64 characters long.	
	- 18 I
ОК	Cancel

□ Enter a WPA 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.

neral Security	Advanced			
Set Security	Options			
C	WPA	WPA EAP Type:	LEAP	~
C	WPA Passphrase			
۲	802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
0	Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
0	None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP	
	Configure		Allow Association to Mixed	Cells

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.

<any></any>		•
User Information for E	AP-TTLS Authentication	
User Nam	e: james	
Passwor	d:	
Confirm Passwor	d:	

- □ **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 **Advanced** button.

Advanced Configuration		? 🔀
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.

General Security A	dvanced			
Set Security Op	otions			
OW				
	PA	WPA EAP Type:	LEAP	~
Ow	PA Passphrase			
() 80	2.1x	802.1x EAP Type:	PEAP (EAP-GTC)	~
O Pr	e-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
O No	one		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
	Configure		Allow Association to Mixed (	Cells

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

Define PEAP (E/	AP-GTC) Configuration	? 🔀
Trusted Root	Certification Authorities	
<any></any>		~
User Name:	james rd	
🔿 Toker 💽 Static	n : Password	
	Advanced OK	Cancel

- □ **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 **Advanced** button.

Advanced Configuration	2	3
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.

## 3.2.3.9 802.1x – 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.

ieneral Security Advanced			
Set Security Options			
○ WPA	WPA EAP Type:	LEAP	~
🔿 WPA Passphrase			
💿 802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
O Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
🔿 None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
Configure		LEAP	
			13
			-

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

fine PEAP (EAP-MSCHAP	V2) Configuration	?
Trusted Root Certification	Authorities	
<any></any>		~
Cuser Information for PEA User Name: Password: Confirm Password:	P (EAP-MSCHAP V2) Authentication james	
	Advanced OK	Cancel

- □ **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 **Advanced** button.

Advanced Configuration		? 🛛
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.

onie M	anagem	ent			
General	Security	Advanced			
S	et Security	Options			
	0	WPA	WPA EAP Type:	LEAP 👻	
	0	WPA Passphrase			
	۲	802.1x	802.1x EAP Type:	LEAP 👻	
-	0	Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS EEAP (EAP-GTC)	
	0	None		PEAP (EAP-MSCHAP V2)	
		Configure		Allow Association to Mixed Cells	
					-
				ОК	Cancel

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

LEAP Settings		? 🗙
LEAP username and passwo	rd settings	
OUse Temporary Use	er Name and Password	
O Manualiy I	Prompt for LEAP User Name and Password	
💿 Use Saved User Na	me and Password	-
User Name:		
Password:		
Confirm Password:		
Domain:		
✓ Include W ✓ No Netwo LEAP Authen	indows Logon Domain with User Name rk Connection Unless User Is Logged In tication Timeout Value (in seconds) 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.

Set Security Options			
() WPA	WPA EAP Type:	PEAP (EAP-GTC)	~
🔿 WPA Passphrase			
O 802.1×	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
💿 Pre-Shared Key (St	atic WEP)		
🔿 None			
Configure		Allow Association to Mixed	Cells

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

cryption Keys Transmit WEP Ke Key 64 120	
Transmit WEP Ke 64 120	
NED K	y Size:
V/ED Kault	3 152
	0
WEP Key 2: O	0
WEP Key 3: O	0
	0

- □ **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 Management			? 🛛
General Security Advanced			
- Wireless Mode	Power Save Mode:	Normal	×
☑ 5 GHz 54 Mbps	Network Type:	Infrastructure	*
🗹 2.4 GHz 54 Mbps	802.11b Preamble:	💿 Short & Long	🔵 Long Only
✓ 2.4 GHz 11 Mbps	- Wireless Mode Whe	n Starting Ad Hoc Netw	ork
Super A/G	○ 5 GHz 54 Mb ○ 5 GHz 108 M ○ 2.4 GHz 54/1	ps bps Channel: 1 Mbps	Auto
802.11 Authentication Mode	L	Pr	referred APs
		価	定 取消

- □ **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 or Off setting.
- Network Type: Select Infrastructure from the drop-down list.
- □ **802.11 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

rofile Management		?
General Security Advanced		
Wireless Mode	Power Save Mode:	Off
▼ 5 GHz 54 Mbps	Network Type:	Ad Hoc 💌
🔽 2.4 GH2 54 Mbps	802.11b Preamble:	💿 Short & Long 🛛 Long Only
🔽 2.4 GHz 11 Mbps	- Wireless Mode When	n Starting Ad Hoc Network
Super A/G	<ul> <li>● 5 GHz 54 Mbj</li> <li>● 5 GHz 108 Mi</li> <li>● 2.4 GHz 54/11</li> </ul>	ps bps Channel: Auto S 1 Mbps
802.11 Authentication Mode		Preferred APs
		確定 取消

- □ **Wireless Mode:** Place a check in the preferred frequency and data rates.
- Network Type: Select Ad hoc from the drop-down list.
- **802.11 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.

802.11 WLAN Client Utility - Current Profile: wlan ion Options Help	
urrent Status Profile Management Diagnostics	
Transmit Multicast Packets: 6 Broadcast Packets: 345 Unicast Packets: 3885	Adapter Information Advanced Statistics
Receive	
Broadcast Packets: 66429	
Total Bytes: 8134792	

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 Information	? 🗙
Card Name:	WLAN USB 2.0 Wireless Network Adapter
MAC Address:	00-02-6F-13-14-FA
Driver:	C:\WINDOWS\system32\DRIVERS\ar5523.sys
Driver Version:	1.0.0.114
Driver Date:	06 Oct 2004 16:52:28
Client Name:	S006275NB
	OK

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

4299 231 1931 0 4299 0 2993	RTS Frames: CTS Frames: No CTS Frames: Retried RTS Frames: Retried Data Frames: Authentication Time-Out:	0 0 0 231 0 231
4299 231 1931 1299 4299 0 2993	RTS Frames: CTS Frames: No CTS Frames: Retried RTS Frames: Retried Data Frames: Authentication Time-Out:	0 0 0 231 0
231 1931 0 1299 1299 0 2993	CTS Frames: No CTS Frames: Retried RTS Frames: Retried Data Frames: Authentication Time-Out:	0 0 231 0
1931 0 1299 1299 0 2993	No CTS Frames: Retried RTS Frames: Retried Data Frames: Authentication Time-Out:	0 231 0
0 \$299 0 ?993	Retried RTS Frames: Retried Data Frames: Authentication Time-Out:	0 231 0
4299 0 2993	Retried Data Frames: Authentication Time-Out:	231
0 2993	Authentication Time-Out:	0
0 2993	Authentication Time-Out:	0
2993		
	Authentication Rejects:	U
0	Association Time-Out:	0
449	Association Rejects:	0
0	Standard MIC OK:	0
7	Standard MIC Errors:	0
0	CKIP MIC OK:	0
0	CKIP MIC Errors:	0
1	1449 0 7 0 0	<ul> <li>1449 Association Rejects:</li> <li>0 Standard MIC OK:</li> <li>7 Standard MIC Errors:</li> <li>0 CKIP MIC OK:</li> <li>0 CKIP MIC Errors:</li> </ul>

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

Click on the **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 802.11 WLAN C	lient Utility - (	Current Profile: wla	n	
Action Options Help				
Disable <u>R</u> adio	anagement D			
Disable <u>T</u> ray Icon	_			C-000000
Manual LEAP Login	Profile Name:	wlan		Saper
<u>R</u> eauthenticate	Link Status:	Associated		AG.
E <u>x</u> it				
	Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
	Network Type:	Infrastructure	Current Channel:	11
Server Base	d Authentication:	None	Data Encryption:	None
ž	Signal Strength:			Excellent
				Advanced
L				

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

urrent Status	Profile Management	Diagnostics	
	Profile Name:	Diagnosilos	Total 802
802.	11 WLAN Client Uti	lity	
-			
(i	WLAN USB 2.0 Wir	the following network card(s) havi eless Network Adapter	e been successfully disabled:
(i	The RF signals for WLAN USB 2.0 Wir Signal Strength:	the following network card(s) have eless Network Adapter	e been successfully disabled: No Link

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

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

tion Options Help			
Enable <u>R</u> adio	anagement D	iagnostics	
Manual LEAP Login	Profile Name:		Total 802.11
<u>R</u> eauthenticate	Link Status:		AG.
Exit	Wireless Mode:	IP	Address:
	Network Type:	Current	Channel:
Server Based	d Authentication:	Data Er	ncryption:
	Signal Strength:		No Link
	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".

🔥 802.11 WLAN Client Utility - Current Profile: wlan	X
Action Options Help	
Current Status Profile Management Diagnostics	
Profile Name: wlan	2.11
802.11 WLAN Client Utility	TH
The RF signals for the following network card(s) have been successfully enabled: WLAN USB 2.0 Wireless Network Adapter	
Signal Strength: No Link	
Advanced	

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**.

Disable <u>R</u> adio		Diagnostics		
Disable <u>T</u> ray Icon	_			Total 802
Manual LEAP Login	Profile Name:	wlan		Supe
Reauthenticate	Link Status:	Associated		'AG
E <u>x</u> it	Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
	Network Type:	Infrastructure	Current Channel:	11
Server Base	d Authentication:	None	Data Encryption:	None
	Signal Strength:			Excellent
				Advanced

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 802.11 WLAN Client Utility -	Current Profile: wla	In	
Action Options Help			
Currer Display Settings	)iagnostics		
Profile Name:	wlan		Total 802.11
Link Status:	Associated		AG .
Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
Network Type:	Infrastructure	Current Channel:	11
Server Based Authentication:	None	Data Encryption:	None
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%	<mark>⊙</mark> dBm	
Refresh Interval (seconds):	-	3 🗘	
Data Display:	O Relative	Cumulative	
		K 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**.

6	-	Currently installed programs:	Show up <u>d</u> ates	Sort by: Name	2
C <u>h</u> ange or Remove Programs		$\Lambda$ 802.11 WLAN Client Installation Program	n v1.00	Size Used Last Used On	0.36MB rarely 11/8/2005
Add New	_	To change this program or remove it from your	computer, click Change/Remove.	Char	ige/Remove
Programs		🕎 Acronis True Image 15 ATI - Software Uninstall Utility		Size	: 18.02MB

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.

Questio	n 😿
2	The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?
	Yes No

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 re	move the s	elected application an	d all of its features?

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	1 🛛
?	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.

802.11 WLAN Client Installation Program	
⚠	The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

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

# Appendix A – Specifications

#### **Data Rates**

**802.11a:** 6, 9, 12, 18, 24, 36, 48, 54, 72, 96 & 108 (Super A) Mbps

**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, IEEE802.11a, IEEE802.11g, IEEE802.11b, draft IEEE 802.11e, f, h, and i standards, IEEE802.1x

#### **Regulation Certifications**

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

#### **Operating Voltage**

5 V ± 0.25V

#### Status LEDs

RF link activity

#### **Drivers**

Windows 2000/XP

#### **RF** Information

#### **Frequency Band**

**802.11a:** 5.15~5.25GHz, 5.25~5.35GHz, 5.725~5.850GHz **802.11b/g:** 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**

802.11a/g: 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, 2 for Spain, 4 for France

### **Receive Sensitivity (Typical)**

- 5.15~5.35GHz
   6Mbps@ -90dBm;
   54Mbps@ -74dBm
- 5.47~5.725GHz
   6Mbps@ -90dBm;
   54Mbps@ -73dBm
- 5.75~5.85GHz
   6Mbps@ -89dBm;
   54Mbps@ -72dBm
- 2.412~2.472G(IEEE802.11g)
   6Mbps@ -91dBm;

#### 54Mbps@ -76dBm

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

#### Available transmit power (Typical)

### FCC (Typical)

- 5.15~5.24 GHz
   17 dBm @6Mbps
   17 dBm @54Mbps
- 5.26~5.35 GHz
   20 dBm @6Mbps
   17 dBm @54Mbps
- 5.725 ~ 5.850GHz
  - 19 dBm @6Mbps
  - 15 dBm @54Mbps
- 2.412~2.462GHz(IEEE802.11g)
   24 dBm @ 6 ~ 24 Mbps
   21 dBm @ 36 Mbps
   20 dBm @ 48 Mbps
   19 dBm @ 54 Mbps
- 2.412~2.462GHz(IEEE802.11b)
   25 dBm @1~11Mbps

#### **ETSI (Typical)**

- 5.15~5.35 GHz
   20 dBm @6Mbps
   17 dBm @54Mbps
- 5.47 ~ 5.725GHz
   19 dBm @6Mbps
   16 dBm @54Mbps
- 5.725 ~ 5.825GHz
   18 dBm @6Mbps
   15 dBm @54Mbps
- 2.412~2.472G(IEEE802.11g)
   20 dBm @ 6 ~ 24 Mbps
   20 dBm @ 36 Mbps
  - 20 dBm @ 30 Mbps 20 dBm @ 48 Mbps 19 dBm @ 54 Mbps
- 2.412~2.472G(IEEE802.11b)
- 20 dBm @1~11Mbps

### Antenna

Dipole antenna

### 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 2.0/1.1

### 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.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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