User Manual

USB Wireless 802.11 a/b/g Adaptor

V 1.0

Information in this document is subject to change without notice.

Microsoft, Encarta, MSN, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products.

PART NUMBER WUBA180AG

TABLE OF CONTENTS

1 Introduction

Your PC comes with a built-in USB Wireless 802.11a/b/g adaptor which allows it to function as a Wireless Local Area Network (WLAN) connecting with other wireless product(s). This product is an IEEE 802.11a/b/g Compliant device. It features automatic rate selection and advanced security features like WEP, 802.1x, WPA/WPA2 with TKIP and AES for stronger data encryption.

Inventory Checklist

Included with your HP PC should be the following items for your Wireless USB Adaptor:

- Documentation CD (Contains *Quick Installation Guide* and full User Manual)
- A high gain omni directional antenna as well as an attachment pad (See Chapter 2 for installation instructions)

Note*: Not all PC Configurations ship with this external omni-directional antenna. If your PC did not come with an antenna in a plastic packet then there is a built-in internal antenna already installed in your PC. In such case please skip chapter 2 of this manual as your PC does not need an external antenna.*

Supported Security

In order to secure your network from passive or active intrusion, key

features are enabled on **Windows Vista** ® **Wireless Auto Configuration**:

- WPA Personal/Enterprise security
- WPA2 Personal/Enterprise Security
- WEP Encryption

Please see Chapter 3 for information on security settings for your USB Wireless adaptor.

2 Security Setting

Security can be set up using WEP (Wired Equivalency Protocol), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2) or 802.1X (with EAP-TLS and PEAP authentication method). It is important to set up matching security types between devices. Be certain to check the type of security on your other wireless device(s) in order to decide which type of security needs to be set up on your PC.

WEP security was the original security standard provided for wireless 802.11 devices. WPA or WPA2 security which offers more advanced encryption technology is a more recent standard of security available.The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA.

IEEE 802.1X reduces the security vulnerabilities that are associated with connections to IEEE 802.11 wireless networks. Unlike open system or shared key authentication(specified in IEEE802.11), IEEE 802.1X enforces verification of user-based credentials for a wireless computer or user before allowing access to the wireless network and, depending on the authentication method used, dynamically determines encryption keys for wireless communication. If you connect to an IEEE 802.11 wireless local area network (WLAN) without IEEE 802.1X authentication enabled, the data that you send is more vulnerable to attacks.

3 Windows Vista® Wireless Auto Configuration

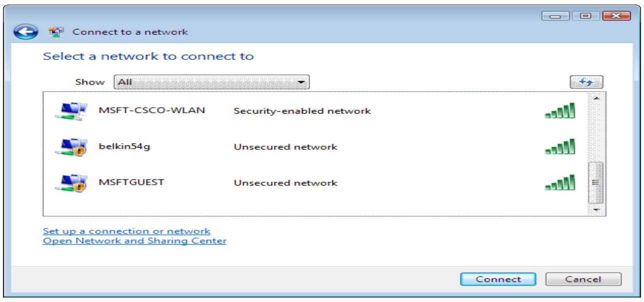
It is necessary to complete the steps in Chapter 2, Antenna Attachment prior to using Windows Vista Wireless Network Configuration.

If you have already established a wireless network with access to the internet and you would like to wirelessly connect this HP PC to your wireless network, use Windows Vista Auto Configuration.

Launching Microsoft Windows Vista ® Wireless Network Configuration

To launch Windows Vista Wireless Network Configuration:

1. Click **Start**, and then **Connect to** from the Windows Vista desktop.



Connect to a network

Select a network to connect to

Show: All

MSFT-CSCO-WLAN	Security-enabled network	
belkin54g	Unsecured network	
MSFTGUEST	Unsecured network	

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Figure: 4.1 The connect to a network dialog box

2. In **Show,** please select on **Wireless** for wireless connections only.

> ***Note***: *Your Network name will appear in the above window. Any other listed available wireless networks represent the wireless networks established within range of your PC. These will vary and may not provide secured access to the internet.*

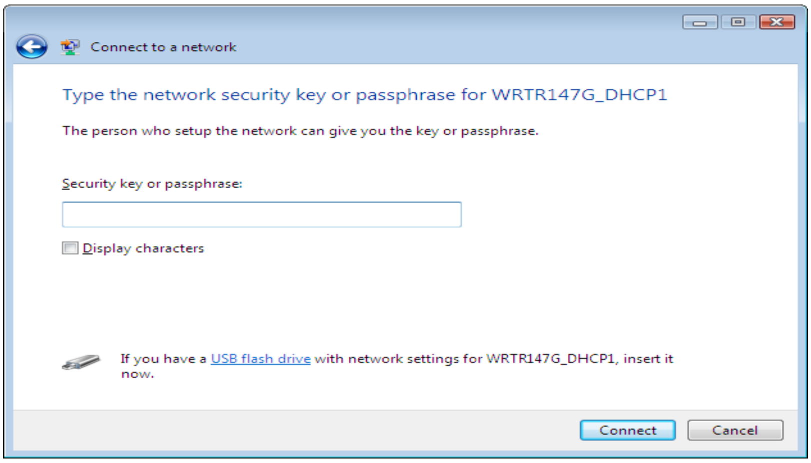
Setting the Network Key Automatically

The PC will begin functioning in Station Mode (as a Client) with your Wireless LAN Network as soon as the Network Key is set-up.

Note: If you do not have an existing wireless network you will need to set up your Wireless Router/ Access Point prior to using your PC in Station Mode.

1. Find the Network Key (WEP Key or WPA Key) for your Wireless Network.
2. Launch the Connect to a Network dialog box. (See above for instructions)
3. Select the Wireless Network of your choice by clicking on its name and the entire block will become highlighted.
4. Select **Connect** in the lower right corner.

   The Entering Network Key dialog box will appear as shown below.



Connect to a network

Type the network security key or passphrase for WRTR147G_DHCP1

The person who setup the network can give you the key or passphrase.

Security key or passphrase:

□ Display characters

If you have a USB flash drive with network settings for WRTR147G_DHCP1, insert it now.

Figure: 4.2 Wireless Network Connection dialog box

5. Enter your Network Key (WEP Key or WPA Key) or Passphrase for your Wireless Network.

6. **Display characters** Specifies whether you want to view the value typed in **Security Key/Passphrase**.

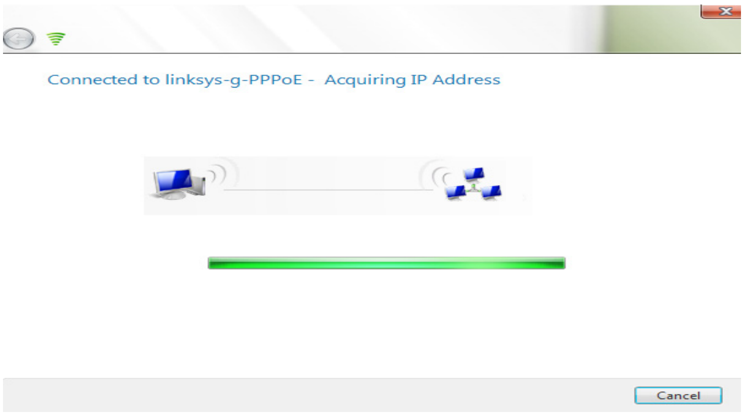
***Note**: If your network is using WEP encryption, then a HEX or an ASCII format is necessary when entering your Network Key:*

- HEX: 10 characters in HEX notation for 40 bit or 26 characters for 128 bit encryption.
- ASCII: 5 characters for 40 bit or 13 characters for 128 bit encryption.

If your network is using WPA it is necessary to enter an 8 – 63 character alphanumeric key-phrase.
The Network Key will accept any of these as it supports both WEP and WPA.

7. Click **Connect.**

The Wireless Network Connecting dialog box appears as you are being connected.

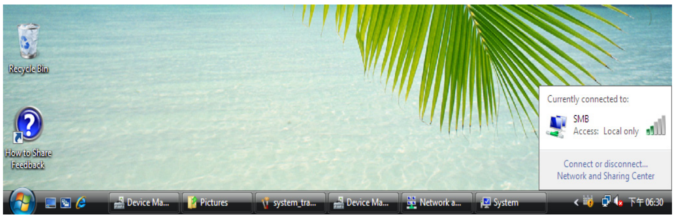


Connected to linksys-g-PPPoE - Acquiring IP Address

Figure: 4.3 Connecting to Wireless

After connection to a wireless network is established, a Wireless

Network LAN icon, as shown below will appear in the system tray.



Currently connected to:

SMB
Access: Local only

Connect or disconnect...
Network and Sharing Center

Figure: 4.4 Wireless Network LAN Icon

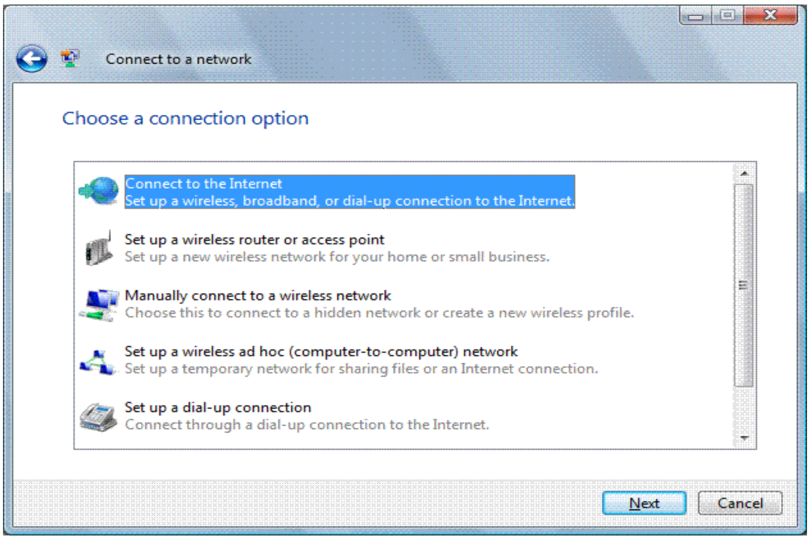
Setting the Wireless Network Connection Manually

After launching the application (See Section See "Launching Microsoft Windows Vista Wireless Network Configuration" on page 7), you may click **Set up a connection or network** at the lower left corner to set up your wireless network connection manually.(See Figure 5.1 above)

Before manually setting up the Network name and Network Key on your HP PC you must identify this information on your current wireless network:

- Your unique network name to distinguish it from other wireless networks(SSID)
- Security WEP Key
- Security WPA-PSK Key or WPA-Enterprise authentication
- Security WPA2-PSK Key or WPA2-Enterprise authentication
- 802.1x : also known as the dynamic WEP

The **Choose a Connection Option** shows up when you click to setup a connection or network:



Connect to a network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

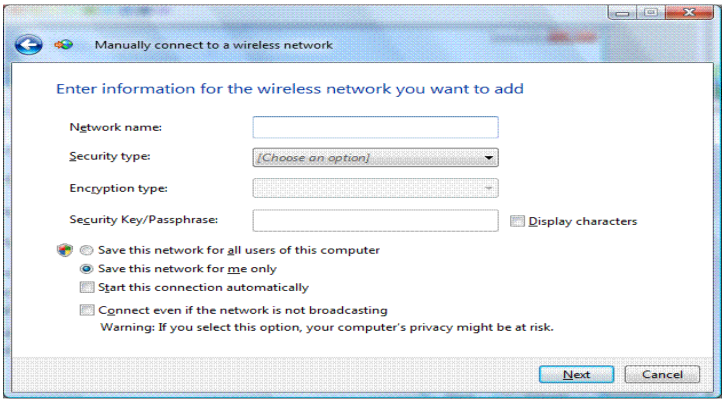
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.

Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Figure: 4.5 Choose a connection dialog box

1. To manually configure the wireless settings for a wireless network, click **Manually connect to a wireless network**, and then click **Next**. Windows Vista displays the following page.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: [Choose an option]

Encryption type:

Security Key/Passphrase:

□ Display characters

○ Save this network for all users of this computer

● Save this network for me only

□ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

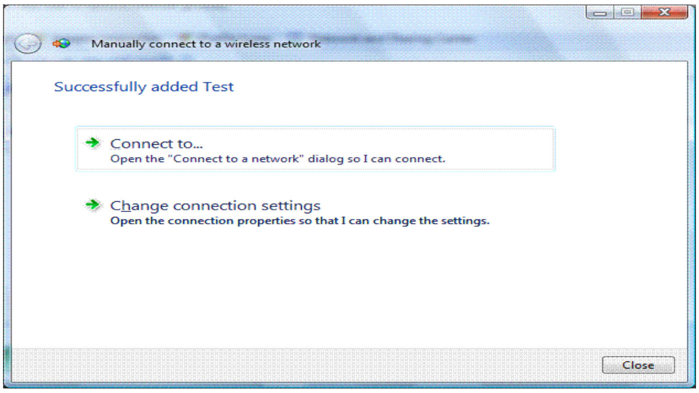
Figure: 4.6 Manually setup a wireless connection

On the **Enter information for the wireless network you want to add** page, configure the following:

1. **Network name** Type the name of the wireless network
2. **Security type** Select the method used to authenticate a connection to the wireless network. The choices are the following:
   - Your unique network name to distinguish it from other wireless networks(SSID)
   - Security WEP Key
   - Security WPA-PSK Key or WPA-Enterprise authentication
   - Security WPA2-PSK Key or WPA2-Enterprise authentication
   - 802.1x : also known as the dynamic WEP
3. **Encryption type** Select the method used to encrypt data frames sent over the wireless network. The choices depend on the selected security type.The choices are the following:
   - When the **No authentication (Open)** security type is selected, **None** is selected.
   - When the **WEP** security type is selected, **WEP** is selected
   - When the **WPA/WPA2-Personal** security type is selected, you can select **TKIP** or **AES**
   - When the **WPA/WPA2-Enterprise** security type is selected, you can select **TKIP** or **AES**

- When the **WEP (802.1x)** security type is selected, **WEP** is selected
- **Security Key/Passphrase** Type the WEP key (if you selected the **WEP** security type), the WPA preshared key (if you selected the **WPA-Personal** security type), or the WPA2 preshared key (if you selected the **WPA2-Personal** security type)
- **Display characters** Specifies whether you want to view the value typed in **Security Key/Passphrase**
- **Save this network for all users of this computer/Save this network for me only** Specifies that this wireless network profile will be in the list of networks for other users of the computer or only the current user. If specified only for the current user, the wireless network will be disconnected when the user logs off or switches to another user
- **Start this connection automatically** Specifies whether Windows Vista will automatically connect to this wireless network. If you clear this checkbox, you must manually connect to the wireless network from the **Connect to a network** dialog box
- **Connect even if the network is not broadcasting** Specifies whether Windows should attempt to connect even if the wireless network is not broadcasting its name. This will cause Windows Vista to send Probe Request frames to locate the wireless network. These probe request frames can be used by malicious users to determine the name of the non-broadcast network

4. Click Next and Windows Vista will display the following page:



Manually connect to a wireless network

Successfully added Test

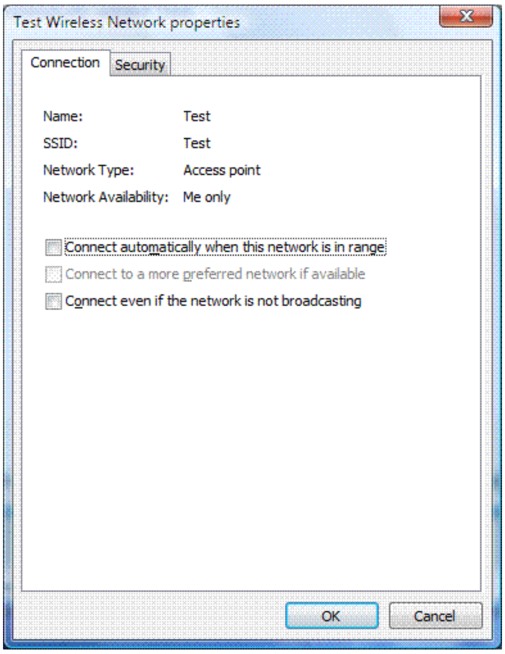
Connect to...
Open the "Connect to a network" dialog so I can connect.

Change connection settings
Open the connection properties so that I can change the settings.

Figure: 4.7 Adding or change the settings for a manually setup wireless connection

To connect to the wireless network that you just created, click **Connect to**, and then double-click the newly created wireless network in the **Connect to a network** dialog box.

To configure the properties of the wireless network you have just created, click **Change connection settings**. Windows Vista displays the following dialog box..



Test Wireless Network properties

Name: Test

SSID: Test

Network Type: Access point

Network Availability: Me only

□ Connect automatically when this network is in range

□ Connect to a more preferred network if available

□ Connect even if the network is not broadcasting

Figure: 4.8 Wireless Network Connection Properties dialog box

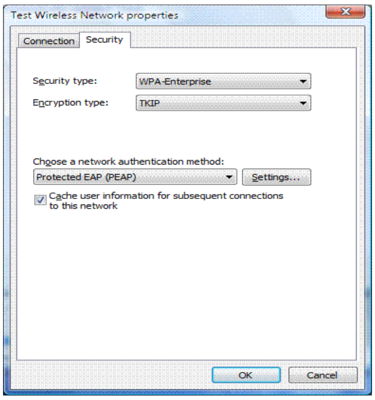
From the **Connection** tab, you can view the wireless network's name, SSID, network type (either **Access point** for infrastructure mode networks or **Computer-to-computer** for ad hoc mode networks), and availability. You can also configure the following:

- Connect automatically when this network is in range

Connect to a more preferred network if available

- Specifies whether Windows Vista will automatically disconnect from this wireless network if a more preferred wireless network comes within range.
- Connect even if the network is not broadcasting

The following figure shows the **Security** tab:



Security type: WPA-Enterprise

Encryption type: TKIP

Choose a network authentication method: Protected EAP (PEAP) Settings...

☑ Cache user information for subsequent connections to this network

Figure: 4.9 Wireless Network Security Properties dialog box

Based on the selected security type, you can configure either a network security key or specify and configure a network authentication method. If you specify **WPA-Enterprise**, **WPA2-Enterprise**, or **802.1x** as your security type, you must configure the following (as shown in the above figure):

- **Choose a network authentication method** Select an Extensible Authentication Protocol (EAP) method
- **Cache user information for subsequent connections to this network** Specifies that when the user logs off, the user credential data is removed from the registry. The result is that when the next user logs on, they will be prompted for their credentials (such as user name and password)

Glossary

- Access Point (AP)

  A hardware device (possibly a PC) that can act as a communication hub for wireless devices enabling them to connect to a wired LAN (Local Area Network) or to one another.

- ASCII (American Standard Code for Information Interchange)

  A code used for encryption that represents letters with numbers.

- Broadband Router

  A device which lets multiple client devices share a single internet connection (like DSL, Cable modem or T1). Generally Broadband Routers offer rudimentary network address translations and firewall features.

- Client

  A device that acquires networking services from another device like another PC or access point.

- DNS Server

  Domain Name System / Service / Server is a service available on the internet that translates domain names into IP addresses.

- Encryption

  The most efficient way to achieve data security online. Encryption is a method of coding data. Generally it is necessary to provide a secret key or password in order to receive decoded information when encrypted.

- Gateway

  A gate or entrance into a network. The ISP connecting a home to the internet is generally the gateway in a residence.

- HEX

  A numbering system used in encryption. HEX is a 16 symbol system consisting of the numbers 0 – 9 and A – F.

- IP Address

  An address that identifies devices on a TCP/IP network (eg; 192.168.0.2).

- ISP (Internet Service Provider)

  A company that provides access to the internet.

Continued

- MAC Address

  Media Access Control Address. On an 802.11 network the MAC address is used to identify each node of the network.

- Network Name

  See SSID.

- Network Key

  Network password.

- SSID (Service Set Identifier)

  The unique identifier attached to the header of packets sent over a Wireless Local Area Network (WLAN). The SSID differentiates Wireless LANs from one another. For this reason an SSID must be entered on each wireless device attempting to connect on the WLAN.

- Station

  See Client.

- WEP

  Wired Equivalency Protocol. WEP is an 802.11 encryption standard that provides security for wireless LANs.

- Wireless LAN

  A wireless version of Ethernet, the Wireless Local Area Network enables wireless internet access through your SoftAP™ or broadband router.

- Wireless Network

  See Wireless LAN.

- WPA

  Wi-Fi Protected Access. WPA is an addition to the security in the 802.11 standard. It is an enhancement to the original security implementation for 802.11 devices.

- WPA Personal AES

  (Advanced Encryption Standard). See WPA.

- WPA Personal TKIP

  (Temporal Key Integrity Protocol). See WPA.

Troubleshooting

Problems	Recommended Solutions
My WPA security settings are not working properly.	Verify that your Network Keys are entered correctly. If the problem persists......... Reconfigure your wireless network setting to WEP security.
I am unable to see my Network name in the Available wireless networks section of the Wireless Network Connection dialog box on my HP PC.	Verify your Network name and Security settings. If the problem persists............ Consult the users manual for your Wireless Gateway or Access Point.
I am having difficulty with my VPN connection.	Check your VPN server administrator/IT Department for wireless connection support and requirements.
Internet Gaming issues	For assistance with internet gaming issues please refer to Microsoft internet gaming site.

Regulatory Notices

Regulatory Notices

To identify this product refer to the part or model number on the product label

Federal Communication Commission Notices

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.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

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

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.

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only
IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna,
3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end product for any additional compliance requirements required with this module installed (for example PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions cannot be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID cannot be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: **MXF-U950711AG**".

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module. The end user manual shall include all required regulatory information/warning as show in this manual.

Canada (Industry Canada)

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and
2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 1.95 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

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

Product Specifications

Model Number WUBR180AG

Functional Criteria	
Data Rate	Up to 54 Mbps
Operating Range	802.11b/g: 30m (indoor), 200 m (outdoor)
Radio Signal	
Modulation	Orthogonal Frequency Division Multiplexing (OFDM)
Operating Frequency	USA (FCC), Canada (IC): 802.11b & 802.11g: 2.412~2.462 GHz 802.11a: 5.150~5.250 GHz, 5.725~5.850 GHz
Operating Channel	USA, Canada: 11 Channels (802.11b/g) Europe: 13 Channels (802.11b/g)
Physical Characteristics	
Power Consumption	TX: 350/305mA Max in 802.11b/g mode RX: 145 mA Max in 802.11b/g mode
Dimensions	4.5x 1.25 x1.25 in.
Polarization	Vertical

Model Number WUBR180AG

Connector	I-PEX Connector
Gain	802.11b/g: Peak gain: 1.95dBi
Radiation	Omni-directional
Frequency Band	2.4 ~ 2.5GHz, 4.9 ~ 5.9GHz

INDEX