Connect - To connect to one of the networks on the list, select the wireless network**,** and click the **Connect** button. If the wireless network has WEP encryption enabled, you will see the screen shown in Figure 8-5.

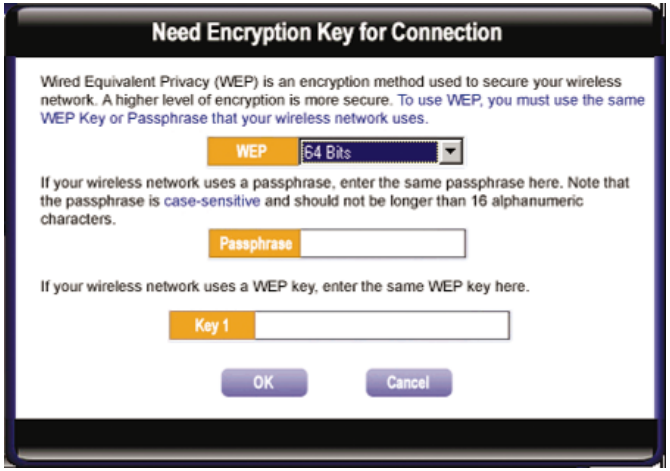

Figure 8-5

In the *WEP* drop-down box, select the type of WEP encryption used by the wireless network: **64-bit**, **128-bit**, or **152-bit** WEP.

If the wireless network uses a passphrase, enter the passphrase in the *Passphrase* field. If the wireless network uses a WEP key, enter the WEP key in the *Key 1* field.

Click the **OK** button to complete the network connection and return to the *Site Survey* screen, or click the **Cancel** button to cancel the network connection and return to the *Site Survey* screen.

On the *Site Survey* screen, click the **X** (Close) button in the upper right corner to exit the WLAN Monitor.

Profiles

The *Profiles* screen lets you save different configuration profiles for different network setups. You can also import or export profiles. The default profile holds the initial configuration saved when you ran the Setup Wizard.

Figure 8-6

Profile - Name of the connection profile.
SSID - The wireless network's unique name, as set in the connection profile.

Profile Information
Network Type - The mode of the wireless network currently in use.
Transfer Rate - The data transfer rate of the current connection. (In *Auto* mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)
Channel - The channel to which the wireless network devices are set.
WEP - The status of the WEP encryption security feature.

Connect - To connect to a wireless network using a specific profile, select the profile**,** and click the **Connect** button.

Edit - Select a profile, and click the **Edit** button to change an existing profile.

New - Click the **New** button to create a new profile. See the next section, "Creating a New Profile," for detailed instructions.

Import - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file, and click the **Open** button.

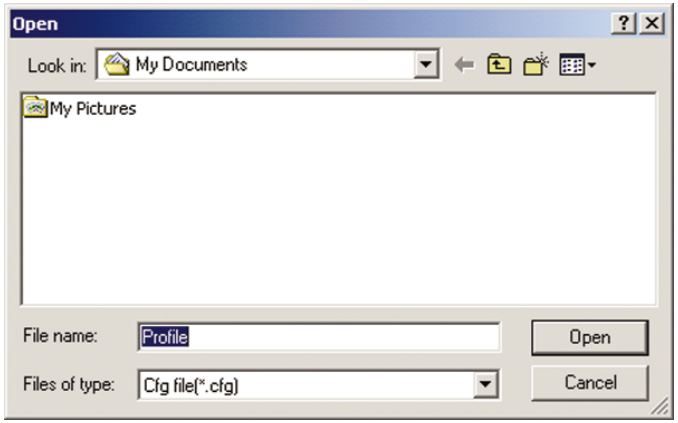

Figure 8-7

Export - To save the profile(s) in a different location, click the **Export** button. Direct Windows to the appropriate folder, and click the **Save** button.

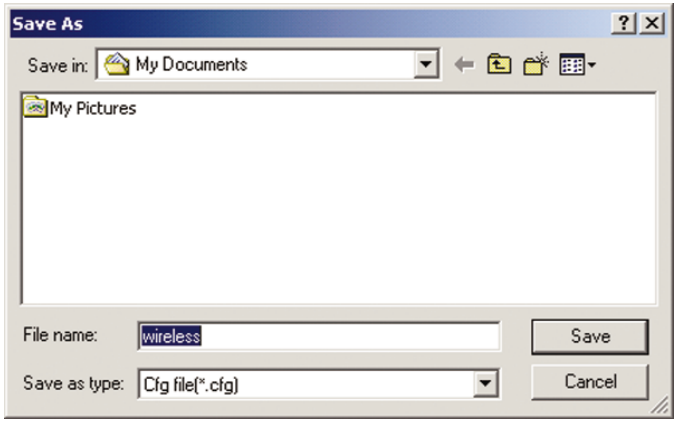

Figure 8-8

Note: If you want to export more than one profile, you have to export them one at a time.

Delete - Click the **Delete** button to delete a profile.

Click the **X** (Close) button in the upper right corner to exit the WLAN Monitor.

Creating a New Profile

1. On the *Profiles* screen, click the **New** button to create a new profile.

Figure 8-9

2. The *Choose a network type* screen shows a choice of two wireless modes (see Figure 8-10). In the *Current Profile* field, enter the name of the new profile. Click the **Infrastructure Mode** radio button if you want your wireless computers to communicate with computers on your wired network via a wireless access point. Click the **Ad-Hoc Mode** radio button if you want multiple wireless computers to communicate directly with each other. Complete the *SSID* field. Click the **Next** button to continue or the **Back** button to return to the previous screen.

   Current Profile - Enter the name of this profile here.

   Infrastructure Mode - This mode allows wireless and wired networks to communicate through an access point.

   Ad-Hoc Mode - This mode allows wireless-equipped computers to communicate directly with each other. No access point is used.

   SSID - The SSID is the unique name shared by all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all devices in your wireless network.

Figure 8-10

3. If you chose Infrastructure Mode, go to ***Step 4*** now. If you chose Ad-Hoc Mode, select the correct operating channel for your network. Click the **Next** button, and go to ***Step 4***. Click the **Back** button to change any settings.

   Channel - The channel you choose should match the channel set on the other devices in your wireless network.

Figure 8-11

4. The *Network Settings* screen will appear.

   If your network has a DHCP server, click the radio button next to **Obtain an IP address automatically (DHCP)**. Click the **Next** button to continue, or click the **Back** button to return to the previous screen. Then go to ***Step 5***.

   If your network does not have a DHCP server, click the radio button next to **Specify the IP address**. Enter an **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS** appropriate for your network. Enter each address in this format: **xxx.xxx.xxx.xxx** (the x's represent the numbers that make up each address). You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, then leave these fields alone. Click the **Next** button to continue, or click the **Back** button to return to the previous screen. Then go to ***Step 5***.

   IP Address - This IP Address must be unique to your network.

   Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

   Default Gateway - Enter the IP address of your network's Gateway here.

   DNS - Enter the DNS addresses of your Ethernet (wired) network here.

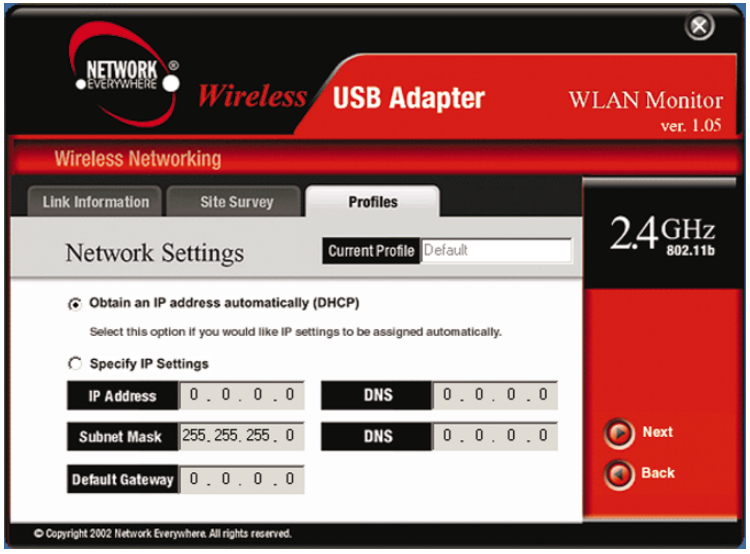

Figure 8-12

5. The *Security Settings* screen will appear. Enable or disable Wired Equivalent Privacy (WEP) encryption for your wireless network. If you enable WEP, enter a Passphrase or WEP key. Click the **Next** button to continue or the **Back** button to return to the previous screen.

   WEP (Disabled/64-bit WEP/128-bit WEP) - If you do not want to use WEP encryption, choose **Disabled**. To use WEP encryption (recommended to increase network security), select **64-bit** or **128-bit WEP** from the drop-down menu, and enter either a Passphrase or WEP key.

   Passphrase - Instead of manually entering WEP keys, you can enter a Passphrase, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your wireless network and is compatible with Network Everywhere wireless products only. (If you have any non-Network Everywhere wireless products, enter the WEP key(s) manually on those products.)

   Key 1 - This WEP key must match the WEP key of your wireless network. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Figure 8-13

6. The *Confirm New Settings* screen will appear. To save the new settings, click the **Next** button. To cancel the settings and return to the *Profiles* screen, click the **No** button. To edit the new settings, click the **Back** button.

Figure 8-14

7. The *Congratulations* screen will appear next. Click **Activate Now** to implement the new settings immediately and return to the *Link Information* screen. Click **Activate Later** to keep the current settings active and return to the *Profiles* screen.

Figure 8-15

You have successfully created a connection profile. Click the X (Close) button in the upper right corner to exit the WLAN Monitor.

Appendix A: Troubleshooting

Common Problems and Solutions

This chapter provides solutions to problems that may occur during the installation and operation of the Wireless USB Adapter. Read the descriptions below to solve your problems. If you can't find an answer here, check the Network Everywhere website at *www.networkeverywhere.com.*

1. My computer does not recognize the Wireless USB Adapter.
- Make sure that the Adapter is properly inserted into the USB port.
- Also, make sure that the USB Controller is enabled in the BIOS. Refer to your motherboard's user guide for more information.

2. The Wireless USB Adapter does not work properly.
- Reinsert the Adapter into the notebook or desktop's USB port.
- For Windows 98SE or Me, right-click **My Computer**, and select **Properties**. Select the **Device Manager** tab, and select the Adapter. You will find the Wireless USB Adapter if it has been installed successfully. If you see a yellow exclamation mark, the resources may be in conflict, and you must follow the steps below:
  - Uninstall the driver software from your PC.
  - Restart your PC and repeat the hardware and software installation as specified in this User Guide.

3. I cannot communicate with a wired computer linked via an access point in the infrastructure configuration.
- Make sure that the notebook or desktop PC is powered on.
- Make sure that the Adapter is configured with the same SSID and security options as the other computers in the infrastructure configuration.

Frequently Asked Questions

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play computer games with other members of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:
- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently

being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: Glossary

802.11b - One of the IEEE standards for wireless networking hardware. Products that adhere to a specific IEEE standard will work with each other, even if they are manufactured by different companies. The 802.11b standard specifies a maximum data transfer rate of 11Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

Ad-hoc Network - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

CTS (**C**lear **T**o **S**end) - An RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data.

Default Gateway - The router used to forward all traffic that is not addressed to a station within the local subnet.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.
DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DNS - The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DSSS (**D**irect-**S**equence **S**pread **S**pectrum) - DSSS generates a redundant bit pattern for all transmitted data. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN end-point), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

ESS (**E**xtended **S**ervice **S**et) - A set of more than two or more BSSs (multiple access points) forming a single network.

Firmware - Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

IEEE - The Institute of Electrical and Electronics Engineers. The IEEE describes itself as "the world's largest technical professional society—promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

Infrastructure Network - An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless

LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requester or the e-mail sender and can respond by sending another message using the IP address it received.

IPCONFIG - A utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility, under Windows NT and 2000, for configuring networks with static IP addresses.

ISP - An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as Web site building and virtual hosting.

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

MAC Address - The MAC (Media Access Control) address is your computer's unique hardware number.

mIRC - mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining and leaving channels.

Network Mask - Also known as the "Subnet Mask."

Plug-and-Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

Roaming - In an infrastructure mode wireless network, this refers to the ability to move out of one access point's range and into another and transparently reassociate and reauthenticate to the new access point. This reassociation and reauthentication should occur without user intervention and ideally without interruption to network connectivity. A typical scenario would be a location with multiple access points, where users can physically relocate from one area to another and easily maintain connectivity.

SSID (**S**ervice **S**et **I**dentifier) - An identification name that wireless devices use to make connections. In order for wireless devices to communicate, they must all be set to the same channel and they all must use the same SSID. For instance, if you are using an access point to connect two computers using wireless devices, the access point and each of the wireless devices must use the same SSID. Even if they are set to the same channel, they cannot communicate unless the SSID is the same.

Static IP Address - A permanent IP address that is assigned to a node in a TCP/IP network.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection-oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

UDP (**U**ser **D**atagram **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for effi-

cient delivery over the network. UDP is known as a “connection-less” protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

WEP (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11b standard.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining and managing IP addresses within a network. A commonly used utility under Windows 95, 98, and Me.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix C: Specifications

Standards	IEEE 802.11b, USB 1.1
Channels	11 Channels (USA)
Port	USB
Transmit (typical)	18 dBm
Receive Sensitivity (typical)	-84 dBm
Modulation	CCK, DQPSK, DBPSK
Network Protocols	TCP/IP
LEDs	Link, Power

Environmental

Dimensions	3.58" x 2.80" x 0.91" (91 mm x 71 mm x 23 mm)
Unit Weight	2.82 oz. (0.08 kg)
Power	Supplied by PC's USB port
Certifications	FCC Class B, Wi-Fi
Operating Temp.	32ºF to 131ºF (0ºC to 55ºC)
Storage Temp.	-13ºF to 158ºF (-25ºC to 70ºC)
Operating Humidity	0% to 70%, Non-Condensing
Storage Humidity	10% to 90%, Non-Condensing

Appendix D: Warranty Information

BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL NETWORK EVERYWHERE'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. NETWORK EVERYWHERE DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

NETWORK EVERYWHERE OFFERS CROSS SHIPMENTS, A FASTER PROCESS FOR PROCESSING AND RECEIVING YOUR REPLACEMENT. NETWORK EVERYWHERE PAYS FOR UPS GROUND ONLY. ALL CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES OF AMERICA AND CANADA SHALL BE HELD RESPONSIBLE FOR SHIPPING AND HANDLING CHARGES. PLEASE CALL NETWORK EVERYWHERE FOR MORE DETAILS.

Appendix E: Contact Information

For help with the installation or operation of the Wireless USB Adapter, contact Network Everywhere Technical Support at one of the phone numbers or Internet addresses below.

Technical Support	949-271-5470, M-F, 8:00 am to 5:00 pm (PST)
Fax	949-265-6655
E-mail	support@NetworkEverywhere.com
Web site	http://www.NetworkEverywhere.com

http://www.NetworkEverywhere.com

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: To assure continued compliance, 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 equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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