

LBU02

User's Manual

Revision: R00
(December 2001)

TRADEMARKS

All brand and product names are trademarks or registered trademarks of their respective companies.

NOTE

Information in this manual is subject to change without notice.



Table of Contents

- Regulations Information iii
- Safety Precautions 3

- 1 Introduction 5**
 - 1.1 Product Description 1
 - 1.2 Product View 3

- 2 Setting Up 5**
 - 2.1 System Requirements 5
 - 2.2 Installing the Driver and Utility 5
 - For Windows 98/2000/Me/XP 5
 - For Linux 8
 - 2.3 Connecting the WLAN USB Dongle 8
 - 2.4 Site Selection 9

- 3 Using Configuration & Monitor Application Utility 11**
 - 3.1 Getting Started 11
 - 3.2 Monitor 12
 - 3.3 Statistics 14
 - 3.4 Site Survey 15
 - 3.5 Encryption 16
 - 3.6 Advanced 17

- 4 Troubleshooting 19**
 - 4.1 Preliminary Checklist 19
 - 4.2 Installation Problem 19
 - 4.3 Configuration Problem 20
 - 4.4 Access Point Problem (*Infrastructure Mode*) 20
 - 4.5 Communication Problem 20
 - 4.6 LAN Problem 21

4.7 Software Problem	21
A Appendix	23
A.1 Specifications	23
A.2 Uninstalling the Utility and Driver	24
Configuration & Monitor Application Utility	24
WLAN USB Dongle	24
Glossary	25

Regulations Information

Federal Communications 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 or more 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 ensure continued compliance, use only shielded interface cables when connecting to the computer or peripheral devices. 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.

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 a minimum distance of 20 cm between the radiator and your body.
- This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

Safety Precautions

- Be sure to read and follow all warning notices and instructions.
- In order to extend the life of the device it is advised to store it in a protective casing whenever carrying the computing device on travel and not operating the device.
- Never use abrasive materials or rinse the device with liquids.
- At all times, it will be the responsibility of the end-user to ensure that an outdoor antenna installation complies with local radio regulations.
- Do not service the product by yourself. Refer all servicing to qualified service personnel.

Exposure to Radio Frequency Signal

Your wireless device is a low power radio transmitter and receiver. When it is ON, it receives and also sends out Radio Frequency (RF) signals. International agencies have set standards and recommendations for the protection of public exposure to RF electromagnetic energy. The design of your wireless device complies with these standards when used normally. In order to limit Radio Frequency (RF) exposure, the following rules should be applied:

- While installing the antenna in the location, please do not turn on power of the device.
- While the device is working (linking), please do not touch or move the antenna. Contact with the antenna affects link quality and may cause the wireless device to operate at a higher power level than otherwise needed.
- Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use.

1 Introduction

This chapter introduces the features and functions of the product.

1.1 Product Description

Congratulations on purchasing this USB (Universal Serial Bus) Dongle Wireless Local Area Network (WLAN) device.

Your WLAN USB Dongle's 11 Mbps data rate provides an equivalent Ethernet speed to access corporate networks or the Internet in a wireless environment. When installed, the WLAN USB Dongle is able to communicate with any 802.11b-compliant product, allowing you to work anywhere in the coverage area, enjoying its convenience and mobility.

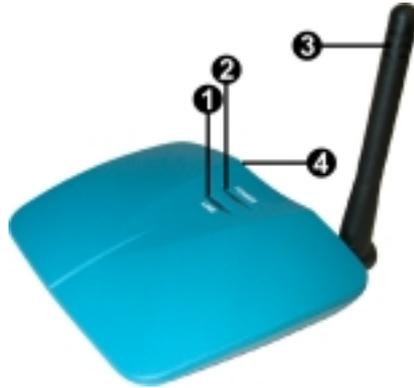
Your WLAN USB Dongle features:

- IEEE 802.11b and Wi-Fi-compliant 11 Mbps WLAN access solution
- Direct Sequence Spread Spectrum (DSSS) standard
- Wired Equivalent Privacy (WEP) 128-bit data encryption
- Frequency range at 2.4 GHz ISM band
- Automatic data rate selection at 11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps (automatic data rate fallback under noisy environment)
- USB interface Plug-and-Play
- High sensitivity and output power

Typical applications include:

- IEEE 802.11b-compliant WLAN radio
- Notebook computer wireless modem
- Point-to-Point data
- Wireless home networking
- Small Office Home Office (SOHO) wireless application

1.2 Product View



Ref	Component	Description
①	Wireless Connection Indicator	Glows green when the WLAN USB Dongle has successfully linked with an Access Point (<i>Infrastructure</i> mode) or with another wireless station (<i>Ad-Hoc</i> mode).
②	Power Indicator	Glows red when the WLAN USB Dongle is connected to your computer and is deriving power from it.
③	Integrated Antenna	Allows the WLAN USB Dongle to receive and transmit wireless data.
④	USB Port	Use a USB cord to connect the WLAN USB Dongle to a computer.

2 Setting Up

This chapter tells you how to setup the device for use.

2.1 System Requirements

To use the device, you need:

- Operating system: Windows 98, Windows Me, Windows 2000, Windows XP, or Linux 2.2.x
- Available USB port on your computing device
- CD-ROM Drive

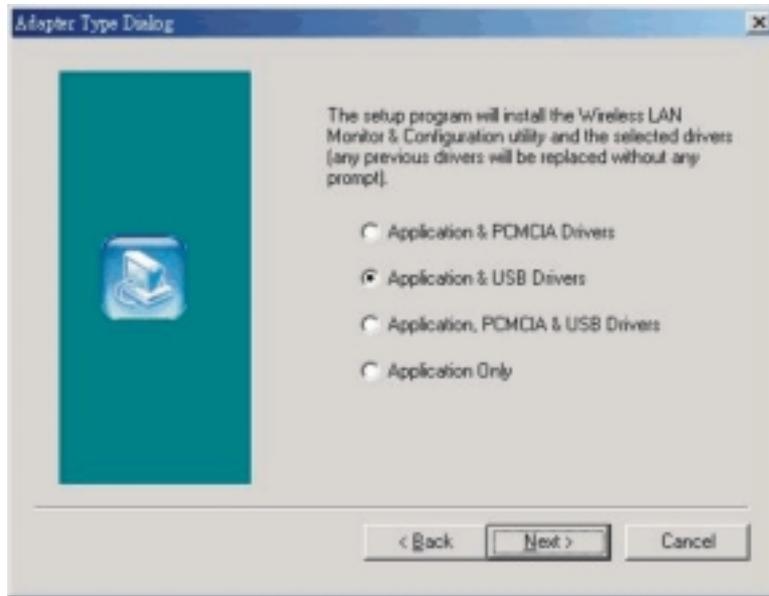
2.2 Installing the Driver and Utility

For Windows 98/2000/Me/XP

CAUTION: Do not connect your WLAN USB Dongle to the computer at this stage until you are required to do so.

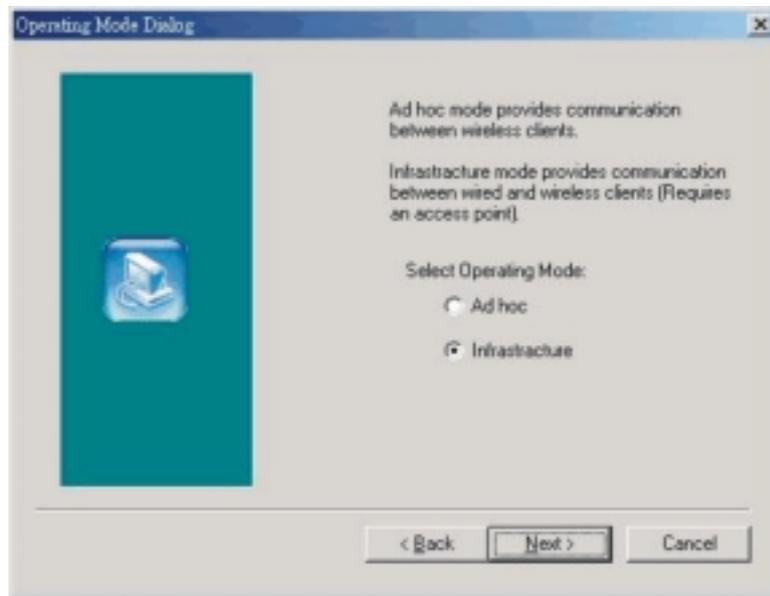
NOTE: When using Windows 2000 and before proceeding, make sure you have logged on as "Administrator."

1. Insert the driver CD into the CD-ROM drive and double-click the file `SETUP.EXE` under the `Windows/Setup` directory.
2. Follow the onscreen instructions to continue.
3. When the next screen appears, select the option "Application & USB Drivers" to install the utility (Configuration and Monitor Application) and the WLAN USB Dongle driver.



NOTE: If the WLAN USB Dongle driver have been previously installed and have not been uninstalled prior to this latest installation, the new driver will overwrite the old one without prompting you.

4. After you have confirmed the driver's "Destination Location" as well as the "Program Folders," choose the mode of operation whether *Ad-Hoc* or *Infrastructure* on the **Operating Mode Dialog** window.



- **Ad-Hoc Mode**

In *Ad-Hoc* mode the wireless stations can communicate directly with each other.

When selecting the *Ad-Hoc* mode you need to specify the ESSID and the Channel parameters.

- ESSID: All stations participating in the *Ad-Hoc* network should have the same ESSID.
- Channel: Select the 14 channels available for use.

- **Infrastructure Mode**

In *Infrastructure* mode the use of an Access Point (AP) is necessary for wireless stations to communicate with each other.

When selecting the *Infrastructure* mode you need to specify the ESSID.

- ESSID: Specify the ESSID of the AP to which the wireless station will be associated with.

NOTE: You can still change the Operating Mode afterwards using the Configuration & Monitor Application utility.

5. After you have made your selection, click **Next** and a window listing your installation setting appears. If the settings are correct, click **Next** to continue. In case you made a mistake, click **Back** to make the correction and follow the onscreen instructions to exit the installation.

NOTE: For Windows 2000, select *Yes* when the "Digital Signature Not Found" window appears.

6. Re-boot your system after completing the installation.

NOTE: To uninstall the driver and utility, refer to the section "Uninstalling the Driver and Utility" on the Appendix.

7. Upon re-booting your system, the Configuration & Monitor Application utility icon should appear on your Window's system tray.

For Linux

Module Parameters

In order to reconfigure the WLAN USB Dongle, use one of the applications that comes with the driver:

- **fvnet** (command line utility) or
- **xvnet** (graphical interface for the X windows)

For more information on using the **fvnet** and **xvnet** applications, refer to the relevant Linux system manual pages (`man xvnet` or `man fvnet`).

NOTE: If nothing happens the first time you plug in your WLAN USB Dongle, then run `# insmod vnetusb`.

2.3 Connecting the WLAN USB Dongle

NOTE: Make sure that the WLAN USB Dongle's driver as well as the Configuration & Monitor Application utility has been properly installed (see previous section).

Connect one end of the included USB cord to the WLAN USB Dongle's USB port and the other end to the USB port of your computer.



NOTE: If you have never installed the driver of the USB port of your system, then Windows would automatically detect the new hardware and may prompt you to install it. Have the Windows installation CD ready (in case you are prompted for it) and follow the onscreen instructions to install the driver.

Your WLAN USB Dongle should start searching for wireless signals from an AP (*Infrastructure* mode) or another wireless station (*Ad-Hoc* mode).

2.4 Site Selection

The following are the tested typical outdoor operating range:

- 250 M at 11 Mbps (high speed)
- 350 M at 5.5 Mbps (medium speed)
- 400 M at 2 Mbps (standard speed)
- 500 M at 1 Mbps (low speed)

The range of the wireless signal is related to the *Transmit Rate* of the wireless communication (*Tx Rate* on the **Monitor** utility of the **Configuration & Monitor Application** utility). Communications at lower transmit range may travel larger distances.

NOTE: The range values listed above are typical distances measured. These values may provide a rule of thumb and may vary according to the actual radio conditions at the location where the WLAN USB Dongle will be installed.

- The range of your wireless devices can be affected when the antennas are placed near metal surfaces and solid high-density materials.
- Range is also impacted due to “obstacles” in the signal path of the radio that may either absorb or reflect the radio signal.

If you intend to use the WLAN USB Dongle as part of an outdoor antenna installation, the range of the outdoor antenna installation will be related to clearance of the radio signal path.

The typical conditions when used indoors in “office environments” can be described as follows:

- In **Open Office environments**, antennas can “see” each other, i.e., there are no physical obstructions between them. This describes the ideal indoor antenna installation.
- In **Semi-open Office environments**, workspace is divided by shoulder-height, hollow wall elements; antenna are at desktop level. This describes the typical indoor antenna installation.
- In **Closed Office environments**, workspace is separated by floor-to-floor ceiling brick walls. This type of indoor antenna installation is not applicable to your WLAN USB Dongle.

3 Using the Configuration & Monitor Application Utility

3.1 Getting Started

In special circumstances, you may need to change configuration settings depending on how you would like to manage your wireless network. The Configuration & Monitor Application utility enables you to make configuration changes and perform user-level diagnostics on your WLAN USB Dongle as well as monitor the status of communication.

To use the Configuration & Monitor Application utility:

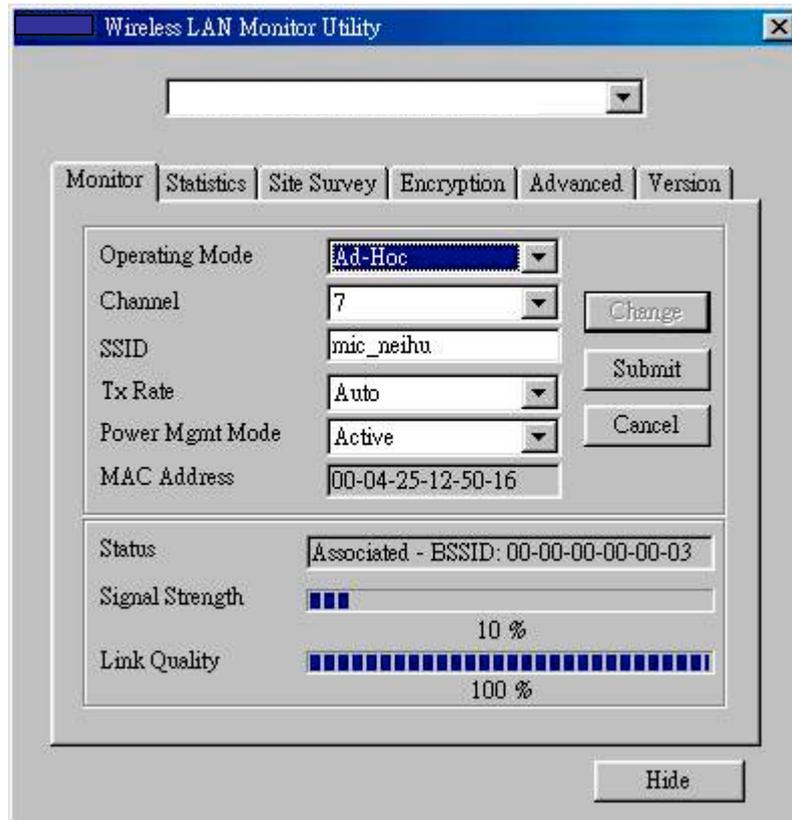
1. Make sure that the Configuration & Monitor Application utility has been installed properly (see Chapter 2).
2. The Configuration & Monitor Application utility appears as an icon on the Windows' system tray. Double-click on this icon.

NOTES:

- When the station is in *Infrastructure* mode and not associated with an AP, color of the icon is red.
- When the station is in *Infrastructure* mode and associated with an AP, color of icon is blue.
- When the station is in *Ad-Hoc* mode, color of icon is always blue.
- When the station is in *Ad-Hoc* mode and the WLAN USB Dongle is resetting and initializing, color of icon is red.

3. When the Configuration & Monitor Application utility appears onscreen, make sure that “USB Dongle” is selected on the very top of the window.

3.2 Monitor



The following configuration parameters are shown:

- **Operating Mode**
Allows you to choose between *Ad-Hoc* or *Infrastructure* mode. In *Ad-Hoc* mode the wireless stations can communicate directly with each other. In *Infrastructure* mode the use of an Access Point (AP) is necessary for wireless stations to communicate with each other.
- **Channel**
This item is available only if *Ad-Hoc* mode was selected in the previous field. Select the 14 channels available for use.

- **SSID**
When using the wireless station in an *Ad-Hoc* mode then all participating stations should have the same SSID. When using the wireless station in an *Infrastructure* mode the SSID must be the same as the SSID of the AP it is associated with.
- **TxRate**
Your WLAN USB Dongle provides various transmission (data) rate options for you to select. In most networking scenarios, the option *Auto* will prove the most efficient. This setting allows your WLAN USB Dongle to operate at the maximum transmission rate. When the communication quality drops below a certain level, the WLAN USB Dongle will automatically switch to a lower transmission rate. Transmission at lower data speeds are usually more reliable. However, when the communication quality improves again, the WLAN USB Dongle will gradually increase the transmission rate again until it reaches the highest available transmission rate. If you wish to balance speed versus reliability, you can select any of the available options.
- **Power Mgmt Mode**
Allows you to minimize power consumption and conserve the battery life of your computer.
- **MAC Address**
On a Local Area Network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. On an Ethernet LAN, it is the same as your Ethernet address.

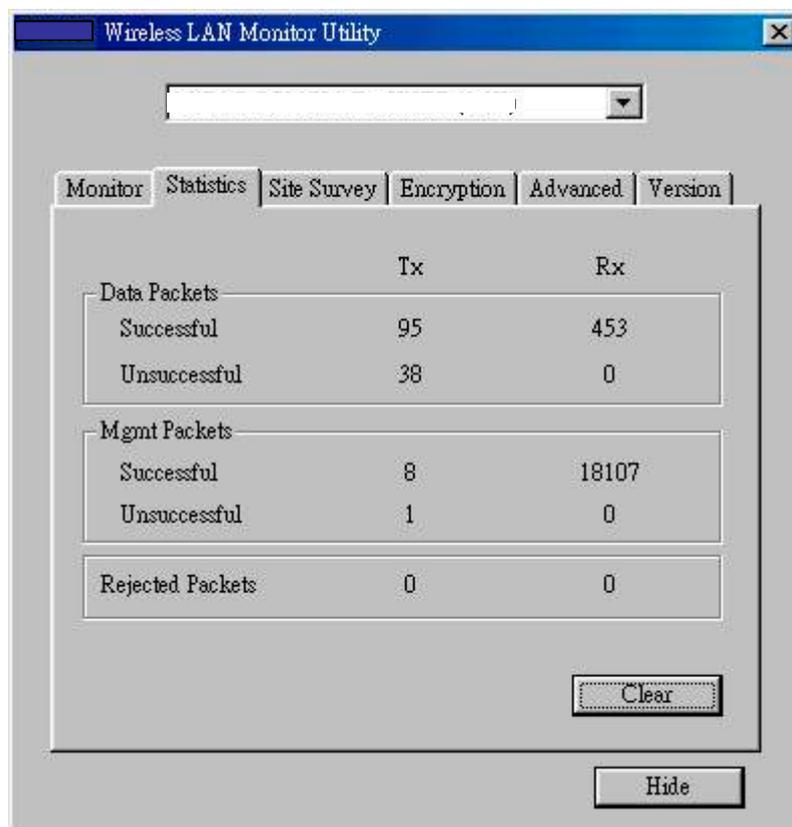
The communication status is also shown:

- **BSSID**
Basic Service Set Identifier of the AP to which the WLAN USB Dongle is associated.
- **Signal Strength**
Signal level when receiving the last responding packet. Signal strength is calculated as the percentage of its signal level measurement relative to the full signal level.

- **Link Quality**
Shows the point-to-point data transmission quality between your WLAN USB Dongle and another WLAN station (*Ad-Hoc* mode) or the transmission quality between your WLAN USB Dongle and the AP it is associated with (*Infrastructure* mode).

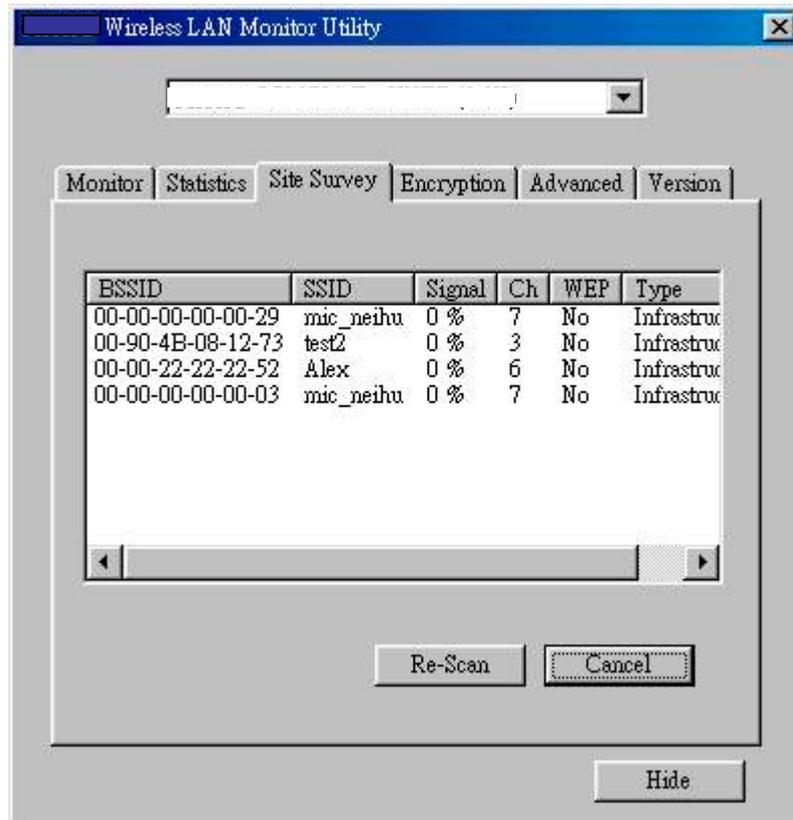
To change the configuration parameters press **Change**, make your changes then click **Submit** to save your changes.

3.3 Statistics



The **Statistics** utility allows you to view the statistic (Packets) information (Data Packets, Mgmt Packets, and Rejected Packets). To renew or update the list of statistics, press **Clear**.

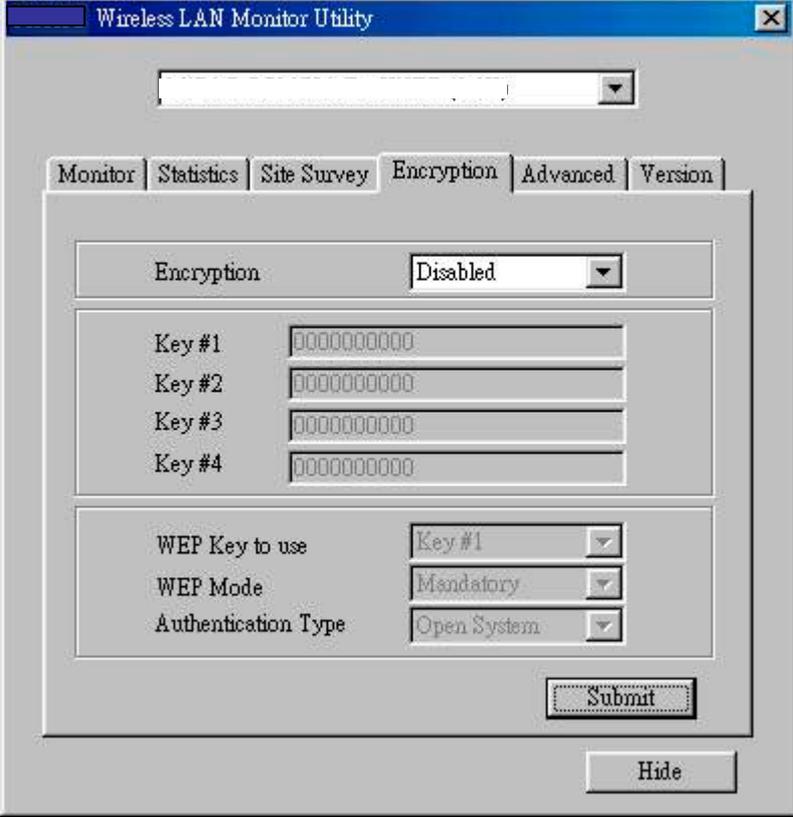
3.4 Site Survey



The **Site Survey** utility allows you to scan all the channels to locate all the APs (Access Points) within range of your WLAN USB Dongle. When an/various AP(s) are located, information regarding the BSSID and SSID, signal strength and channel where the AP operates, whether or not WEP encryption is used, and the operating mode is shown. Click **Re-Scan** to update the list.

To associate with any of the APs listed, double-click on your choice (on the BSSID field) and the utility will take you back to the **Monitor** utility showing you the parameters of the newly established connection.

3.5 Encryption



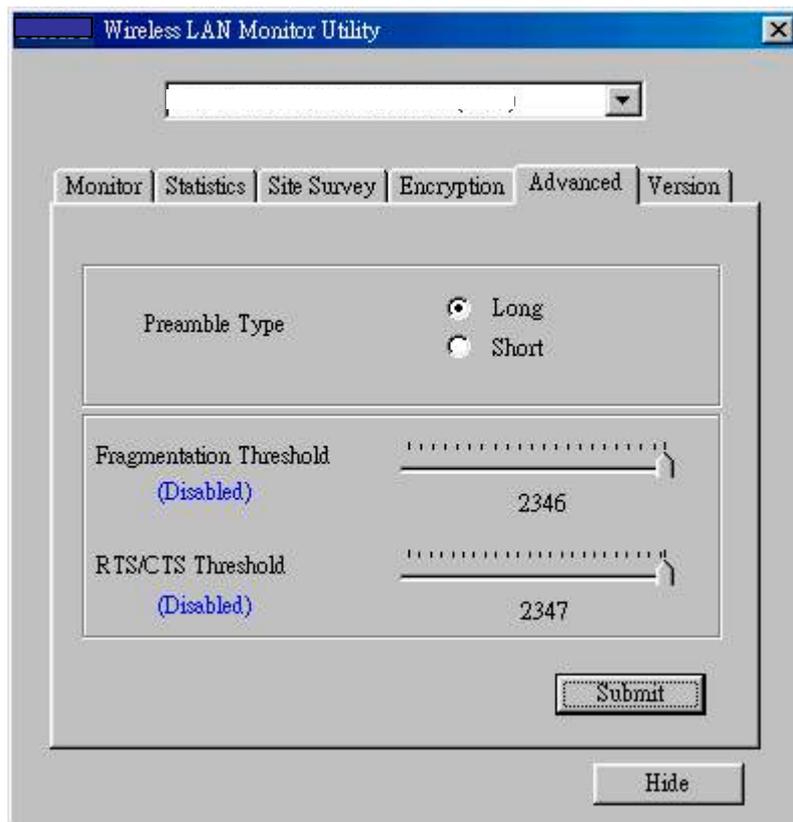
The screenshot shows the 'Encryption' tab of the 'Wireless LAN Monitor Utility' window. The window has a title bar with the text 'Wireless LAN Monitor Utility' and a close button. Below the title bar is a dropdown menu. The main content area has a tabbed interface with 'Encryption' selected. The 'Encryption' section has a dropdown menu set to 'Disabled'. Below this are four text input fields labeled 'Key #1', 'Key #2', 'Key #3', and 'Key #4', each containing a series of zeros. The 'WEP Key to use' section has a dropdown menu set to 'Key #1'. The 'WEP Mode' section has a dropdown menu set to 'Mandatory'. The 'Authentication Type' section has a dropdown menu set to 'Open System'. At the bottom right of the main content area are 'Submit' and 'Hide' buttons.

To prevent unauthorized wireless stations from accessing data transmitted over the network, the **Encryption** utility offers highly secure data encryption by allowing you to set four different WEP keys and specify which one to use. To set encryption:

1. Choose *Enabled* on the **Encryption** window.
2. Select any of the available WEP keys (**Key #1** to **#4**) on the **WEP Key to use** window. The WEP keys must be in HEX (hexadecimal) format in the range of *a* to *f*, *A* to *F*, and *0* to *9*.

3. Select the **WEP Mode** (*Mandatory* or *Optional*).
 - If *Mandatory* is selected, then not only must you use WEP encryption but also any other station you are communicating with must also use WEP encryption for a link to be established. This requirement is part of the IEEE 802.11b standard.
 - If *Optional* is selected, then your station can communicate with every other station regardless if they use WEP encryption or not.
4. Select the **Authentication Type** (*Open System* or *Shared Key*).
5. Press **Submit** for any changes to take effect.

3.6 Advanced



The **Advanced** utility allows you to change the following advanced configuration settings:

- **Preamble Type**

Before selecting *Short*, make sure that the other station(s) and AP supports this feature. The WLAN USB Dongle has an auto-detect feature that allows it to select the **Preamble Type** depending on the **Preamble Type** of the AP it is associated with.

- **Fragmentation Threshold**

Allows you to set the Fragmentation Threshold (threshold for the activation of the fragmentation mechanism). The Fragmentation function is used for improving the efficiency when high traffic flows along in the wireless network. If you often transmit large files in the wireless network, move the slide bar with your mouse and then use the right and left arrow keyboard keys to select an exact number. The figure shows the recommended configuration setting.

- **RTS/CTS Threshold**

Allows you to set the RTS Threshold (threshold for the activation of the RTS/CTS mechanism). Transmitter contending for the medium may not hear each other. RTS/CTS (Request-To-Send/Clear-To-Send) mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will not be enabled. To enable RTS/CTS Threshold, move the slide bar with your mouse and then use the right and left arrow keyboard keys to select an exact number. The figure shows the recommended configuration setting.

4 Troubleshooting

This chapter covers potential problems you may run into and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and solve the problem.

4.1 Preliminary Checklist

Here are helpful hints to follow before you take further actions when you encounter problems:

- Try to isolate which part of the computer's network connection is causing the problem.
- Make sure that the cable connections are correct and secure (from WLAN USB Dongle's USB port to the computer's USB port).
- Absence of, or conflict of the WLAN USB Dongle driver. Make sure that all device drivers are correctly installed (refer to chapter 2).

If a problem persists after you follow the instructions in this chapter, contact an authorized dealer for help.

4.2 Installation Problem

Problems encountered during installation.

- Reconnect one end of the USB cable to the WLAN USB Dongle and the other end to the computer again. The Power LED indicator on the WLAN USB Dongle should be ON (red) if the USB cable is properly connected.
- Check if the I/O and IRQ for the WLAN USB Dongle have conflict problems with other devices connected to your computer.

- For Windows 98 / 2000 / Me / XP operating system, make sure that the USB device driver is installed on your computer.

4.3 Configuration Problem

Problems encountered with the configuration.

- Use the **Monitor** utility of your **Configuration & Monitor Application** utility to check the *Link Quality* of your WLAN USB Dongle with the AP it is associated with (*Infrastructure* mode) or with other wireless station(s) (*Ad-Hoc* mode).
- Use the **Site Survey** utility of your **Configuration & Monitor Application** utility to check if there is high interference around the environment.

4.4 Access Point Problem (*Infrastructure* Mode)

Problems with settings for the Access Point.

- Make sure that the Access Point that your WLAN USB Dongle is associated with is powered on and all the LEDs are working properly.
- Reconfigure and reset the Access Point.
- Use the Web Manager / Telnet of the Access Point to check whether it is connected to the network.

4.5 Communication Problem

The WLAN USB Dongle cannot communicate with the computer in the Ethernet when *Infrastructure* mode is configured.

- Make sure that the Access Point your WLAN USB Dongle is associated with is powered on.
- Use the **Site Survey** utility of the **Configuration & Monitor Application** utility to verify if the operating radio *channel* is in good quality. Or, change the Access Point and all the wireless station(s) within the *BSSID* to another radio *channel*.

- Out-of-range situation, which prevents the WLAN USB Dongle from establishing a wireless connection with the network. Move the WLAN USB Dongle closer to the Access Point it is associated with.
- Make sure that your WLAN USB Dongle is configured with the same security option (encryption) to the Access Point.
- Make sure that the *BSSID* is the same as the Access Point for a roaming-disabled wireless station, or the *ESSID* is the same as the Access Point for a roaming-enabled wireless station.

4.6 LAN Problem

I cannot access the network.

- Make sure that the necessary driver(s) is correctly installed.
- Make sure that the network configuration is appropriate.
- Make sure that the user name or password is correct.
- You have moved out of range of the network.
- Turn off power management.

4.7 Software Problem

The Configuration & Monitor Application utility does not work correctly.

- Make sure that the **Configuration & Monitor Application** utility is correctly installed (refer to chapter 2).
- If you are sure the operation has stop, reset the computer.

A Appendix

A.1 Specifications

| **NOTE:** Specifications are subject to change without notice.

Parts	Specifications
Frequency Band	ISM Band 2400 to 2483.5 MHz (for USA and Canada) 2400 to 2483.5 MHz (for Europe) 2400 to 2497 MHz (for Japan)
Operating Channel	IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS) 11 Channels (for USA and Canada) 13 Channels (for Europe) 14 Channels (for Japan)
Modulation Technique	BPSK (low transmit rate) / QPSK (standard transmit rate) / CCK (high and medium transmit rate)
Data Rate	Up to 11 Mbit/s
Antenna	Single
Antenna Gain	1 dBi maximum
Radiation Power	16 dBm typical
Receiver Sensitivity	-80 dBm at 11 Mbps -82 dBm at 5.5 Mbps -87 dBm at 2 Mbps -90 dBm at 1 Mbps
Power Consumption	5 V, 320 mA TX, 230 mA RX
Dimension (W×H×D)	84×20×92 mm
Weight	48 g
Environment Temperature	Operating: 0°C (32°F) to 55°C (131°F) Storage: -20°C (-3.91°F) to 70°C (158.02°F)
Environment Humidity	Operating: 0% to 70% Storage: 0% to 95% (non-condensing)

Parts	Specifications
Regulation (compliant)	Wi-Fi compliant, FCC/CA, CE (Europe), DGT/BSMI
OS Support	Windows 98 / Me / 2000 / XP / Linux 2.2.x

A.2 Uninstalling the Utility and Driver

Configuration & Monitor Application Utility

1. Exit the Configuration & Monitor Application utility if it is currently active.
2. Select the “Uninstall Configuration & Monitor Application” option by clicking on **Start**, then **Programs**, then **802.11 Wireless LAN**.

NOTE: If during the uninstall process you receive an error message, insert the driver CD and try to uninstall again.

WLAN USB Dongle

For Windows 98 / Me / XP –

1. Select the “Network” icon by clicking on **Start**, then **Settings**, then **Control Panel**.
2. Select the “WLAN USB Dongle” from the list and click on **Remove**.
3. When the system prompts you to re-boot, select “Yes.”

For Windows 2000 –

1. Make sure that the WLAN USB Dongle is plugged into the USB port.
2. Select the WLAN USB Dongle under **Device Manager**.
3. Click on **Uninstall**.

Glossary

802.11	The IEEE standard that specifies WLAN MAC and PHY (Physical Layer) specifications.
802.11b	The IEEE standard that specifies Higher-Speed Physical Layer Extension in the 2.4 GHz band for 5.5 and 11 Mbps WLANs.
802.3	The IEEE standard that specifies carrier sense media access control and physical layer specifications for Ethernet LANs.
Access Control	The prevention of unauthorized usage of network resources by demanding that users supply a login name and password.
Access Point (AP)	Any entity that has station functionality and provides access to the distribution services, via the Wireless Medium (WM) for associated stations.
Ad-Hoc	An Ad-Hoc WLAN is a group of computers each with wireless adapters connected as an independent WLAN.
Authentication	In a multi-user or network operating system, the process by which the system validates a user's logon information. A user's name and password are compared against an authorized list, and if the system detects a match, access is granted to the extent specified in the permission list for that user.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Bandwidth	A frequency measurement, expressed in cycles per second (hertz) or bits per second (bps), of the amount of information that can flow through a channel. The higher the frequency, the higher the bandwidth.
Base Station	In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communication with the mobile radio telephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station, each base station in turn is interconnected with other cell's base stations.
Bit	(Binary Digit) – A single digit number in base-2, in other words, either a one or a zero. The smallest unit of computerized data.

Broadband	Of or relating to communications systems in which the medium of transmission (such as a wire or fiber-optic cable) carries multiple messages at a time, each message modulated on its own carrier frequency by means of modems. Broadband communication is found in wide area networks.
BSS	Basic Service Set. An AP associated with several wireless stations.
Byte	Abbreviated B. Short for binary term. A unit of data, today almost always consisting of 8 bits. A byte can represent a single character, such as a letter, a digit, or a punctuation mark. Because a byte represents only a small amount of information, amounts of computer memory and storage are usually given in kilobytes (1,024 bytes), megabytes (1,048,576 bytes), or gigabytes (1,073,741,824 bytes).
Cryptoanalysis	The act of analyzing (or breaking into) secure documents or systems that are protected with encryption.
Decryption	The act of restoring an encrypted file to its original state.
Directional Antenna	An antenna that concentrates transmission power into a direction thereby increasing coverage distance at the expense of coverage angle. Directional antenna types include yagi, patch and parabolic dish.
Direct Sequence Spread Spectrum	Abbreviated DSSS. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Encryption	The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula that determines how the file is decrypted.
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the AP must have the same ESSID.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
Gateway	A device that connects networks using different communications protocols so that information can be passed from one to the other. A gateway both transfers information and converts it to a form compatible with the protocols used by the receiving network.
Gigahertz (GHz)	One billion cycles per second. A unit of measure for frequency.
Hertz (Hz)	The unit of frequency measurement; one cycle (of a periodic event such as a waveform) per second. Frequencies of interest in computers and electronic devices are often measured in kilohertz (kHz = 1,000 Hz = 10 ³ Hz), megahertz (MHz = 1,000 kHz = 10 ⁶ Hz), gigahertz (GHz = 1,000 MHz = 10 ⁹ Hz), or terahertz (THz = 1,000 GHz = 10 ¹² Hz).

Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
HTTP	Acronym for HyperText Transfer Protocol. The client/server protocol used to access information on the World Wide Web.
IEEE 802 Standards	A set of standards developed by the IEEE to define methods of access and control on LANs. The IEEE 802 standards correspond to the physical and data-link layers of the ISO Open Systems Interconnection model, but they divide the data-link layer into two sublayers. The logical link control (LLC) sublayer applies to all IEEE 802 standards and covers station-to-station connections, generation of message frames, and error control. The MAC sublayer, dealing with network access and collision detection, differs from one IEEE 802 standard to another: IEEE 802.3 is used for bus networks that use CSMA/CD, both broadband and baseband, and the baseband version is based on the Ethernet standard. IEEE 802.4 is used for bus networks that use token passing, and IEEE 802.5 is used for ring networks that use token passing (token ring networks). In addition, IEEE 802.6 is an emerging standard for metropolitan area networks, which transmit data, voice, and video over distances of more than five kilometers.
internet	(Lower case I) Any time you connect two or more networks together, you have an internet.
Internet	(Upper case I) The worldwide collection of networks and gateways that use the TCP/IP suite of protocols to communicate with one another. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, consisting of thousands of commercial, government, educational, and other computer systems, that route data and messages. One or more Internet nodes can go off line without endangering the Internet as a whole or causing communications on the Internet to stop, because no single computer or network controls it. Currently, the Internet offers a range of services to users, such as FTP, email, the World Wide Web, Usenet news, Gopher, IRC, telnet, and others. Also called Net.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
ISP (Internet Service Providers)	ISPs provide connections into the Internet for home users and businesses. There are local, regional, national and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.

LAN (Local Area Network)	<p>Personal and other computers within a limited area that are linked by high-performance cables so that users can exchange information, share peripherals, and draw on programs and data stored in a dedicated computer called a file server.</p> <p>Ranging tremendously in size and complexity, LANs may link only a few personal computers to an expensive, shared peripheral, such as laser printer. More complex systems use central computers (file servers) and allow users to communicate with each other via electronic mail to share multi-user programs and to access shared databases.</p>
Linux	<p>A version of the UNIX System V Release 3.0 kernel developed for PCs with 80386 and higher-level microprocessors. Linux is distributed free with source code through BBSs and the Internet, although some companies distribute it as part of a commercial package with Linux-compatible utilities. The Linux kernel works with the GNU utilities.</p>
MAC (Media Access Control)	<p>On a LAN or other network, the MAC address is your computer's unique hardware number. (On an Ethernet LAN, it is the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.</p>
Megahertz (MHz)	<p>A measure of frequency equivalent to 1 million cycles per second.</p>
Modulation	<p>The conversion of a digital signal to its analog equivalent, especially for the purposes of transmitting signals using telephone lines and modems.</p>
Network	<p>Any time you connect two or more computers together so that they can share resources, you have a computer network. Connect two or more networks together and you have an internet.</p>
NIC (Network Interface Card)	<p>A board that provides network communication capabilities to and from a computer system. Also called an adapter.</p>
Node	<p>In LAN, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers, and shared peripherals. In common usage, however, the term node is synonymous with workstation.</p>
Packet	<p>A basic message unit for communication across a network. A packet usually includes routing information, data and (sometimes) error detection information.</p>
PCMCIA (Personal Computer Memory Card International Association)	<p>Develops standards for PC Cards, formerly known as PCMCIA Cards. They are available in three types that are about the same length and width as credit cards but range in thickness from 3.3 mm (Type I) to 5.0 mm (Type II) to 10.5 mm (Type III). These cards provide many functions, including memory storage and acting as landline modems and as WLAN.</p>
POP (Post Office Protocol)	<p>This is a common protocol used for sending, receiving and delivering mail messages.</p>

Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g., web servers normally listen on port 80.
Privacy	The concept that a user's data, such as stored files and email, is not to be examined by anyone else without that user's permission. A right to privacy is not generally recognized on the Internet. Federal law protects only email in transit or in temporary storage, and only against access by Federal agencies. Employers often claim a right to inspect any data on their systems. To obtain privacy, the user must take active measures such as encryption.
Protocol	A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
Public Key Encryption	An asymmetric scheme that uses a pair of keys for encryption: the public key encrypts data, and a corresponding secret key decrypts it. For digital signatures, the process is reversed: the sender uses the secret key to create a unique electronic number that can be read by anyone possessing the corresponding public key, which verifies that the message is truly from the sender.
Radio Frequency (RF)	The portion of the electromagnetic spectrum with frequencies between 3 kilohertz and 300 gigahertz. This corresponds to wavelengths between 30 kilometers and 0.3 millimeter.
Range	A linear measure of the distance that a transmitter can send a signal.
RFC (Request for Comments)	An RFC is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.

Roaming	A function that enables one to travel with his mobile end system (e.g., WLAN mobile station) throughout a domain (e.g., an ESS) while being continuously connected to the infrastructure.
Router	An intermediary device on a communications network that expedites message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. On an interconnected set of LANs using the same communications protocols, a router serves the somewhat different function of acting as a link between LANs, enabling messages to be sent from one to another.
RTS (Request-To-Send) Threshold	A signal sent, as from a computer to its modem, to request permission to transmit. Transmitter contending for the medium may not hear each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will not be enabled.
Server	<ol style="list-style-type: none"> 1. On a LAN, a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network. 2. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client.
SSL (Secure Sockets Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
Station (STA)	Any device that contains an IEEE 802.11 conformant Medium Access Control (MAC) and physical layer (PHY) interface to the Wireless Medium (WM).
Telnet	An Internet protocol that enables Internet users to log on to another computer linked to the Internet, including those that cannot directly communicate with the Internet's TCP/IP protocols. Telnet establishes a "plain vanilla" computer terminal called a network virtual terminal. This capability is frequently used to enable communications with bulletin board systems (BBSs) and mainframe computers. For example, you will often see hyperlinks to Telnet sessions while browsing the WWW. If you click such a hyperlink, your browser starts a Telnet helper program, and you see a text-only command window. In this window, you type commands and see the remote system's responses.

URL (Uniform Resource Locator)	An address for a resource on the Internet. URLs are used by Web browsers to locate Internet resources. A URL specifies the protocol to be used in accessing the resource (such as http: for a World Wide Web page or ftp: for an FTP site), the name of the server on which the resource resides (such as //www.whitehouse.gov), and, optionally, the path to a resource (such as an HTML document or a file on that server).
VPN (Virtual Private Network)	<ol style="list-style-type: none"> 1. A set of nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines. 2. A WAN formed of permanent virtual circuits (PVCs) on another network, especially a network using technologies such as ATM or frame relay.
WAN (Wide Area Network)	A network that uses high-speed, long-distance communications networks or satellites to connect computers over distances greater than those traversed by LANs – about 2 miles (3.22 km).
Wired Equivalent Privacy (WEP)	The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy.
Wireless Local Area Network (WLAN)	A flexible data communications system implemented as an extension to, or an alternative for a wired LAN. Using radio frequency (RF) technology, WLANs transmit and receive data over the air, minimizing the need for wired connections.
Wireless Medium (WM)	The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a WLAN.
WWW (World Wide Web)	The total set of interlinked hypertext documents residing on HTTP servers all around the world. Documents on the World Wide Web, called pages or Web pages, are written in HTML (Hypertext Markup Language), identified by URLs (Uniform Resource Locators) that specify the particular machine and pathname by which a file can be accessed, and transmitted from node to node to the end user under HTTP (Hypertext Transfer Protocol). Codes, called tags, embedded in an HTML document associate particular words and images in the document with URLs so that a user can access another file, which may be halfway around the world, at the press of a key or the click of a mouse. These files may contain text (in a variety of fonts and styles), graphics images, movie files, and sounds as well as Java applets, ActiveX controls, or other small embedded software programs that execute when the user activates them by clicking on a link. A user visiting a Web page also may be able to download files from an FTP site and send messages to other users via email by using links on the Web page. Also called w3, W3, Web.