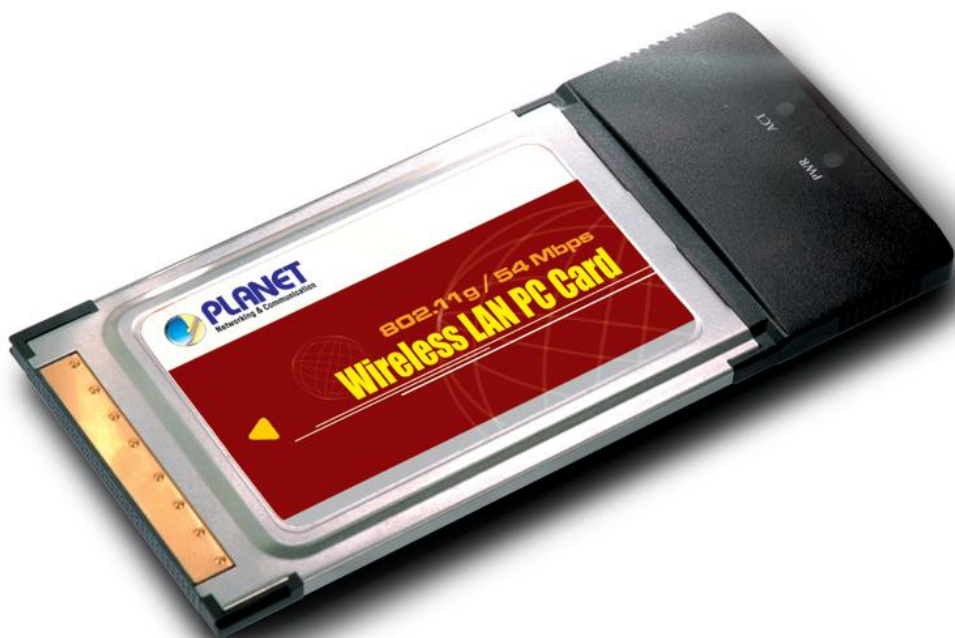




**54Mbps standard 11g
PCMCIA Wireless LAN Adapter**

WL-3564

User Manual



Copyright

Copyright © 2005 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To ensure continued compliance. (Example-use only shielded interface cables when connecting to 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 the 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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Potential restrictive use

France: Only channels 10,11,12 and 13

Revision

User's Manual for PLANET 54Mbps standard 11g PCMCIA Wireless LAN Adapter

Model: WL-3564

Rev: 1.0 (March, 2005)

Part No. EM-WL3564

Table of Contents

CHAPTER 1 INTRODUCTION.....	1
1.1 FEATURES.....	1
1.2 APPLICATIONS.....	2
1.2.1 <i>Infrastructure</i>	2
1.2.2 <i>Ad-Hoc</i>	2
1.2.3 <i>General Application</i>	2
1.3 SPECIFICATION.....	3
1.4 PACKAGE CONTENTS.....	4
1.5 MINIMUM SYSTEM REQUIREMENTS.....	4
1.6 INSTALLATION CONSIDERATIONS.....	4
CHAPTER 2 INSTALLATION PROCEDURE.....	5
2.1 CONFIGURATION UTILITY INSTALLATION.....	5
2.2 DRIVER INSTALLATION.....	6
CHAPTER 3 CONFIGURATION UTILITY.....	9
3.1 LINK INFO.....	10
3.2 CONFIGURATION.....	11
3.3 ENCRYPTION.....	12
3.4 SITE SURVEY.....	15
3.5 ABOUT.....	16
APPENDIX.....	17
GLOSSARY.....	19

Chapter 1 Introduction

Complying with the newly approved 802.11g standard, WL-3564 provides a faster wireless connection for laptop users who want to access network resources. The gadget delivers data at speeds up to 54Mbps, 5 times data rate than 802.11b. It can operate in Infrastructure mode or Ad-hoc mode based on your needs.

WL-3564 provides 360 degrees' coverage of wireless access by employing a build-in dipole antenna. Support of 64 and 128-bit WEP encryption plus WPA (Wi-Fi Protected Access) high-level encryption keeps your wireless network from unauthorized access and ensures secure data transfer.

WL-3564 is backward compatible with 802.11b products, allowing interoperability with any Wi-Fi certified wireless 802.11b/g products, so both 11b and 11g clients can reside on the same network. Support of most operating systems such as Windows98SE/Me/2000/XP/Server 2003 offers greater scalability and usability, making the device a perfect choice for users who are getting tired of running cables or in constant need of wireless access.

1.1 Features

- I 2.4GHz ISM band, unlicensed operation
- I A fast Wireless connection without the hassles and cost of running cables
- I IEEE 802.11b/g standard compliant
- I Up to 54Mbps data rate
- I Utilization of Direct Sequence Spread Spectrum plus OFDM modulation to provide a robust, interference-resistant solution in a multi-user environment
- I Support of 64/128-bit WEP encryption and WPA (Wi-Fi Protected Access) high-level encryption
- I Support of Ad-Hoc / Infrastructure mode
- I Seamless integration with IEEE 802.3 Ethernet through any other IEEE 802.11b/g compliant Access points
- I Support of most popular operating systems including Windows 98SE/Me/2000/XP/Server 2003
- I Support of Power Save mode
- I Plug-and-Play installation

1.2 Applications

1.2.1 Infrastructure

The difference between Infrastructure network and Ad-hoc network is that the former requires an Access point. For old buildings, open areas, or frequently changing environments, just install the WL-3564 on your laptop, and you thus can get connected to the wired Ethernet through a wireless Access Point. SOHO users can then access the Internet and share all kinds of data with the other wired or wireless clients within the coverage of wireless signals. For enterprise users, the installation of multiple Access Points to enlarge the coverage of wireless signals can provide wireless users with seamless network access.

The Infrastructure mode is appropriate for enterprise-scale wireless access to a central database or provides various wireless applications for mobile users.

Infrastructure mode also supports roaming capabilities for mobile users. More than one BSS can be configured as an Extended Service Set (ESS). The continuous network allows users to roam freely within an ESS. All wireless clients using WL-3564 or other IEEE 802.11b compliant wireless adapters within one ESS must be configured with the same ESS ID and use the same radio channel.

Before adopting an ESS with roaming capability, choosing an available radio channel with less interference is highly recommended. Proper Access Point positioning combined with a clear radio channel will greatly enhance performance.

1.2.2 Ad-Hoc

Need a wireless networking comprising of several desktops or laptops without any access point? Configuring all the wireless adapters to operate in Ad-Hoc mode will be the easiest and cost-effective way to meet your requirements.

An Ad-hoc mode is a wireless network type in which a group of computers equipped with WL-3564 or other wireless adapters are connected as an independent wireless LAN. All computers operating in this mode must be configured to share the same radio channel.

In this kind of network, new devices can be quickly added; however, users can only communicate with other wireless LAN computers that are in this wireless LAN workgroup within range.

1.2.3 General Application

WL-3564 offers a fast, reliable, and cost-effective solution for wireless access to the various network scenarios:

1. Remote access to corporate network for information

Emails, file transfer, or terminal service.

2. Difficult-to-wire environments

Old or historical buildings, public occasions, venues and open area where it is difficult to wire.

3. Frequently changing environments

Factories, retailers, and offices that frequently change locations and rearrange the workplace.

4. Temporary LANs for special projects or peak time

Events, exhibitions, construction sites or some important occasions that require temporary network access.

5. SOHO (Small Office and Home Office) users

SOHO users in need of a easy-to-install and wide coverage networking

1.3 Specification

Product	IEEE 802.11g Wireless PCMCIA Adapter
Model Name	WL-3564
Attached Interface	PC CardBus 32-bit compliant
LED Indicators	PWR, ACT
Operating Frequency / Channel	2.412~2.462GHz (FCC, US/Canada) / 11 Channels 2.412~2.472GHz (ETSI, Europe) / 13 Channels 2.412~2.484GHz (TELEC, Japan) / 14 Channels
Emission type	Direct Sequence Spread Spectrum (DSSS) Technology
RF Modulation	OFDM with CCK, BPSK, QPSK, 16QAM, 64QAM
RF Output Power	15dBm
Data Rate	802.11b: 1, 2, 5.5, 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
Antenna	Built-in Patch Antenna
Sensitivity	54Mbps: Typical -73dBm @ 10% PER 11Mbps: Typical -85dBm @ 8% PER
Working Mode	Infrastructure, Ad-Hoc
Power Consumption	TX: 3.3v, 530mA, RX: 3.3v, 240mA Standby: 3.3v, 30mA
Dimension (mm)	117 x 54 x 6 mm
Humidity	10 ~ 95%, non-condensing (Operating and storage)
Temperature	0 ~ 40°C (Operating), -10 ~ 70°C (Storage)
Management	Bundled utility or Windows XP/Server2003 Wireless Zero Configuration utility
Electromagnetic Compatibility	FCC, CE

1.4 Package Contents

Before installation, please check the items of your package. The package should include the following items:

1 x WL-3564

1 x Quick Installation Guide

1 x Drivers and User's Manual CD

If any of the above items is missing, contact your supplier as soon as possible.

1.5 Minimum System Requirements

Before installation, please check the following requirements:

Operating System: Windows 98SE/Me/2000/XP/Server 2003

Desktop PC with a CD-ROM drive

One vacant PCMCIA slot

1.6 Installation Considerations

- I Beware of the walls and ceilings. Each wall or ceiling can reduce your wireless cover range from 3-90 feet. Properly position your Access Points, Residential Gateways, and computers so that the number of walls or ceilings residing between Access Points and clients is minimized.
- I Building materials make a difference - A solid metal door or aluminum studs may have a negative effect on signal coverage range. Try to properly position Access Points and computers with wireless adapters so that there would be less obstacles existing between them.
- I Keep your wireless LAN devices away from microwaves, cordless phones and child incubators. It is likely that the latter will cause interferences to affect the operation of your wireless LAN devices.

Chapter 2 Installation Procedure

Before you proceed with the installation, it is necessary that you have enough information about the *Wireless PCMCIA Card*. Follow the procedure described below to install the WL-3564 under Windows 98SE/Me/2000/XP/Server 2003.

Note: *If you had installed another Wireless Card before, please uninstall the existed drivers and utilities first. If this is the first time to install this device, please refer to the following steps to complete the installation.*

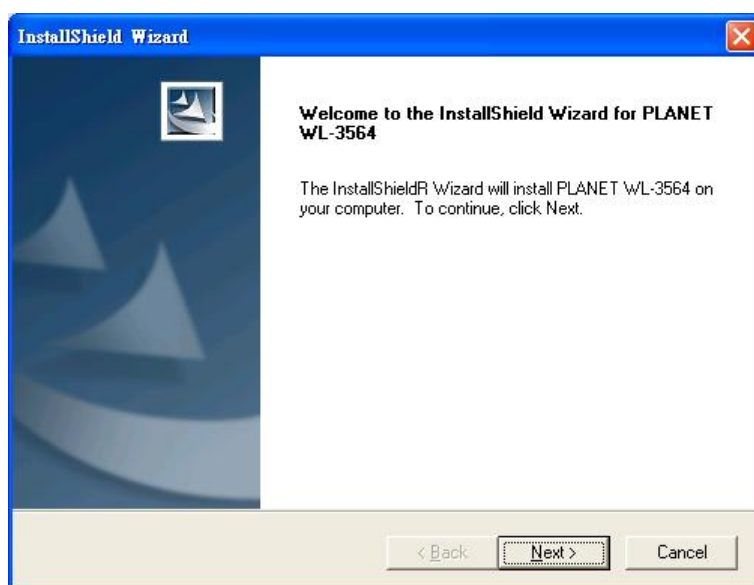
2.1 Configuration Utility Installation

Note: *The following installation operates under Window XP. The procedure also applies to Window 98SE/Me/2000/Server 2003..*

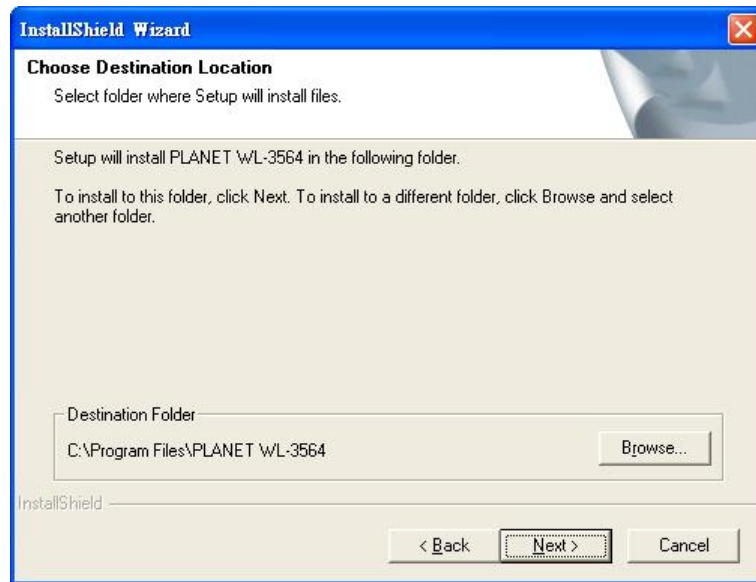
Please install the configuration utility before inserting WL-3564 into the PCMCIA slot of the computer.

1. Insert the bundled CD into the CD-ROM drive to launch the autorun program. Once completed, a menu screen will appear.
2. Click the “Configuration Utility” hyperlink in the WL-3564 field to initiate the installation procedure. You will see the below InstallShield Wizard window. Please click “Next” to continue.

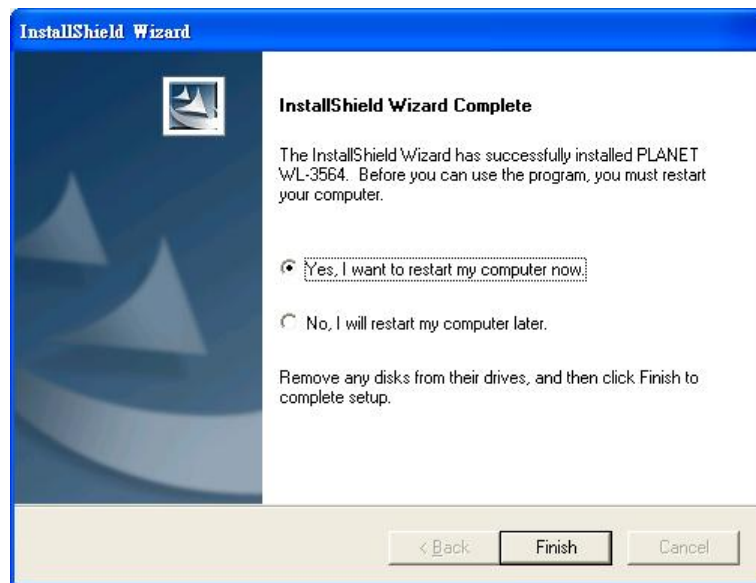
Note: *If the screen below does not appear, click “Start” at the taskbar. Then, select “Run” and type “E:\utility\WL-3564\setup.exe”, where E is your CD-ROM drive.*



3. You may click “Browse” to specify the Destination Folder. Or, you can keep the default setting and click “Next” to proceed.



4. Once the utility is installed, select “Yes” to restart your computer right away, or select “No” to restart later. Then, click “Finish” to go on.



2.2 Driver Installation

Note: The following installation operates under Window XP. The procedure also applies to Window 98SE/Me/2000/Server 2003. If your operating system is Windows 2000, please directly skip to step 3. If your operating system is Windows 98SE/ME, Windows will automatically detect the device and ask you to reboot (For Windows 98SE, the system installation CD will be required). Just click “Yes” to proceed.

1. Power off your computer. Insert WL-3564 into a vacant PCMCIA slot and turn on the computer.

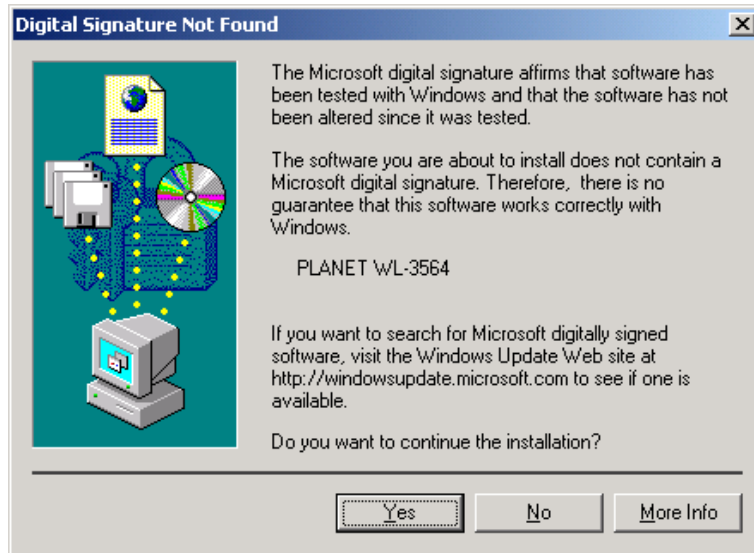
- Windows will automatically detect the device. Choose “Install the software automatically (Recommended)”. Then click “Next” to continue.



- A screen will appear to inform you that the PCMCIA adapter does not pass Windows Logo testing (WHQL). Click “Continue Anyway” to proceed since the card has been tested thoroughly to verify the compatibility.




Note: If your operating system is Windows 2000, the below window will pop up. Please click “Yes” to continue.

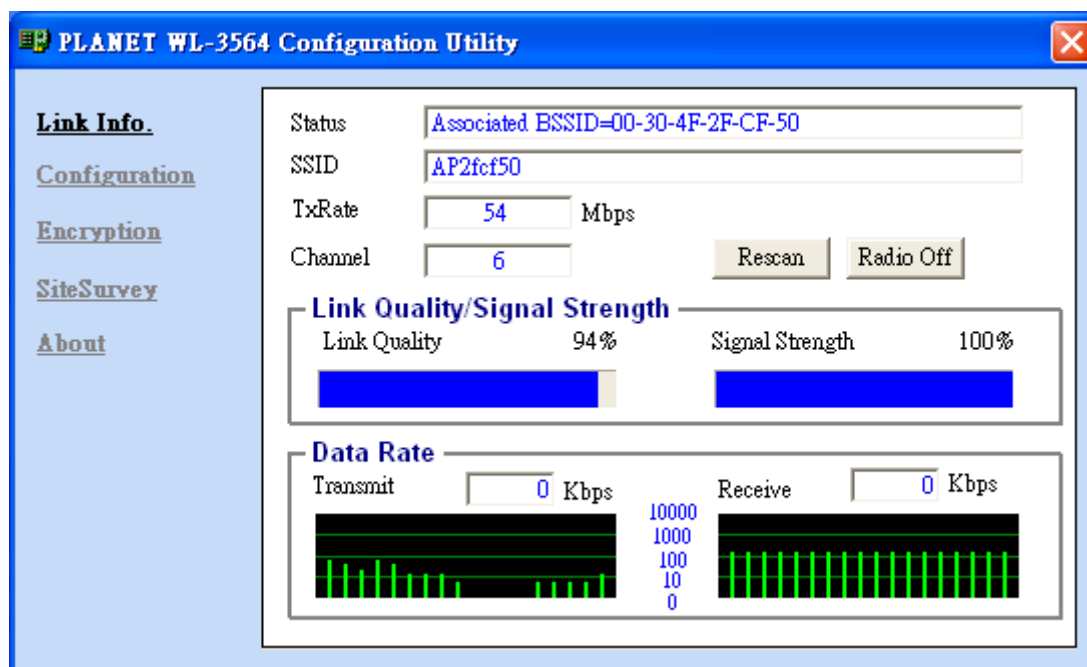



4. When the driver is installed, click "Finish" to complete the installation procedure.



Chapter 3 Configuration Utility

The Configuration Utility is a powerful tool that helps you to configure WL-3564 easily and monitor the status of wireless communication. By double-clicking  in the system tray, the dialog box will appear as follows:

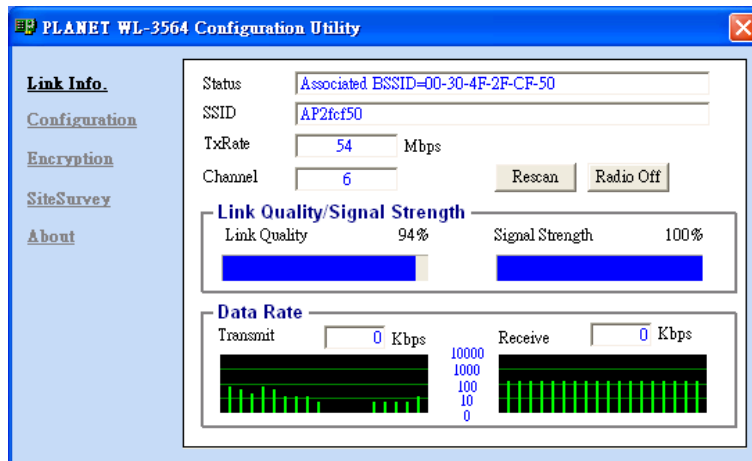


Note: It is highly recommended to use PLANET utility tool to configure WL-3564 rather than Windows XP/Server 2003 Wireless Zero Config Service. Windows XP/ Server 2003 Wireless Zero Config Service will take over the management task of the wireless adapte. Make sure to disable the Wireless Zero Config Service provided by Windows XP/ Server 2003 before launching PLANET utility. To complete this, firstly, restart your computer, and click the Windows XP/ Server 2003 networking icon in the system tray, and then click “Advanced” in “Wireless Network Connection” window. Uncheck “Use Windows to configure my wireless network settings” and click “OK” to exit (If your operating system is Windows 98SE/Me/2000, this step can be skipped). At last, double-click the utility icon  in the system tray to use the configuration utility.



3.1 Link Info.

The default page is as below after you launch the configuration utility. It displays the current link status of WL-3564. You may press the “Radio off” button if you want your wireless PCMCIA adapter to stop working. After the wireless PCMCIA adapter stops working, the “Radio off” button will be renamed to “Radio on”. Click it if you would like to get your wireless PCMCIA adapter back to work. If you have connected to a certain Access Point, pressing “Rescan” button enables the wireless PCMCIA adapter to rebuild the link with the Access Point.

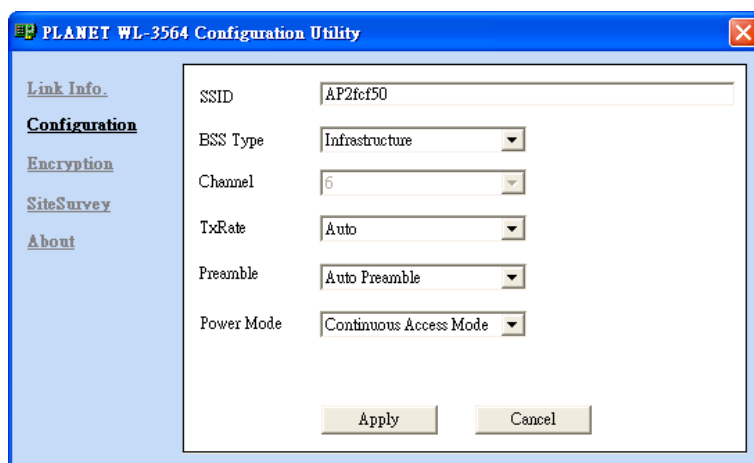


1. **Status:** It shows the BSSID associated with, which can be used to identify the wireless network.
2. **SSID:** It shows the current SSID, which must be the same for the wireless client and AP in order to establish the link.
3. **TxRate:** It shows the current data rate for transmission.
4. **Channel:** It shows the current channel for communication.
5. **Link Quality:** It shows the link quality of WL-3564 with the Access Point when operating in Infrastructure mode.
6. **Signal Strength:** It shows the signal strength of the wireless connection between WL-3564 and the Access Point.

7. Data Rate: It shows the statistics of data transfer based on the number of packets transmitted and received.

3.2 Configuration

In this page, you can configure the settings of the Access Point you want to connect to or you have connected to. After making the configuration, please click “Apply” to make it work or “Cancel” to give up.



- 1. SSID:** It must be identical for each wireless clients and devices in the same wireless work.
- 2. BSS Type:** There are two types available for selection:
 - (1) Ad-hoc:** This mode allows clients to communicate directly with each other without the use of an Access Point.
 - (2) Infrastructure:** This mode requires the presence of an Access Point, via which all wireless communication is conducted.
- 3. Channel:** It shows the current channel on which the AP is operating. In Infrastructure mode, this value is fixed, while in Ad-hoc mode it can be changed.
- 4. Tx Rate:** It shows the data transfer rate. If Auto mode is selected, the device will choose the best data transfer rate automatically.
- 5. Preamble (Auto/Long/Short):** There are 3 options: Auto, Short, and Long Preamble.

Preamble is a sequence of bits transmitted at 1Mbps that allows the PHY circuitry to reach steady-state demodulation and synchronization of bit clock and frame start. It is the first Suffield of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). The Short Preamble minimizes overhead and thus improves throughput performance. However, the Short Preamble is supported only by IEEE 802.11b (High-Rate) standard and not by IEEE 802.11. That means the stations using Short Preamble cannot communicate with the peers using Long Preamble. If Auto Preamble is selected, the device will automatically choose the appropriate preamble type to communicate with the Access Point.
- 6. Power Mode:** It shows Power Management modes. There are 3 options: Continuous Access Mode (CAM), Maximum Power Save, and Fast Power Save.

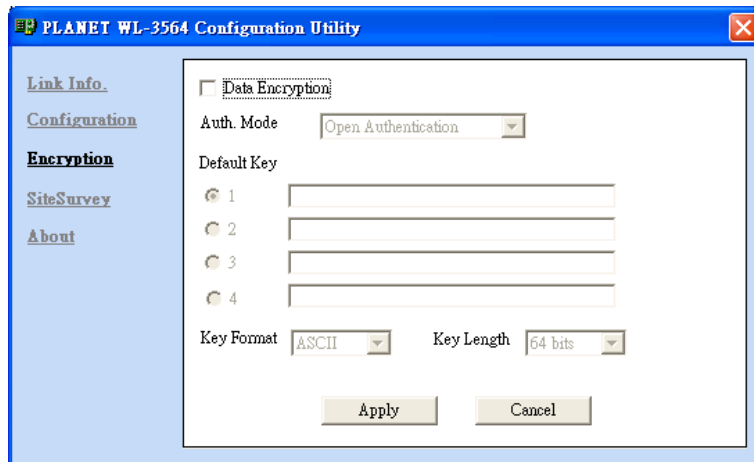
(1) Continuous Access Mode: The adapter will be always operating with full power, consuming the most power.

(2) Maximum Save Mode: The adapter will enter power saving mode when it is idle and only revives when there is data transmission, consuming the minimum power.

(3) Fast Power Save: The adapter will transfer and receive data once in each 5 seconds, consuming the moderate level of power.

3.3 Encryption

In this option, you can enable and select one of the security methods to protect your wireless connection. WL-3564 has provided WEP (Open Authentication, Shared Authentication), WPA and WPA-PSK functions for your network security. Please choose one of them and refer to the below for the detail settings.



1. Data Encryption: You can check this for enabling data encryption.

2. Authentication Mode: If Data Encryption is implemented, it will be required to choose the authentication mode. There are 4 options available:

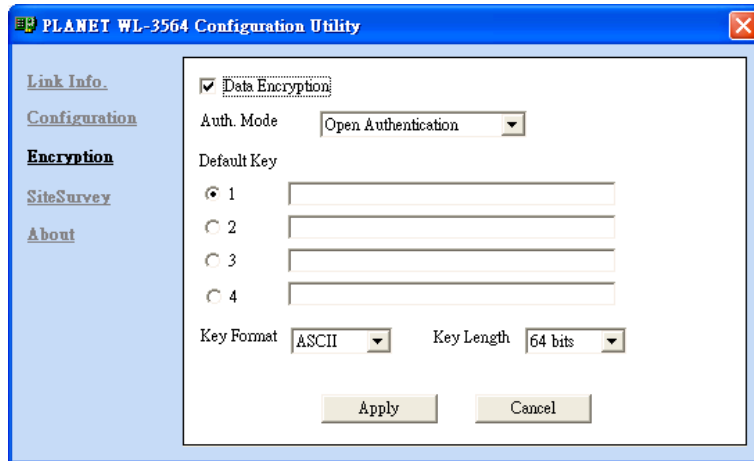
(1) Open Authentication: In this mode, wireless stations directly associate with the Access Point without any authentication (null authentication). You can decide whether to employ WEP data encryption.

(2) Shared Authentication: In this mode, wireless stations communicate with the Access Point with the identical WEP key settings for authentication and data encryption. It combines with WEP data encryption.

(3) WPA-PSK: In this mode, you can use a pre-shared key to AP authenticate and encrypt data during communication. It uses TKIP to change the encryption key frequently. This can improve security very much.

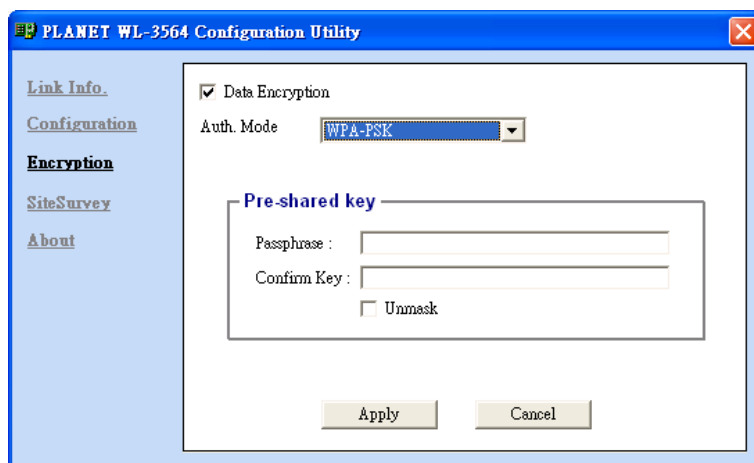
(4) WPA: Wi-Fi Protected Access (WPA) is an advanced security standard. You will need to obtain a Certificate Authority from the RADIUS server for authentication before connect to the wireless network which work with this WPA encryption.

3. **WEP Key options:** This will be configurable only when **Open Authentication** or **Shared Authentication** is selected in **Auth. Mode** option.



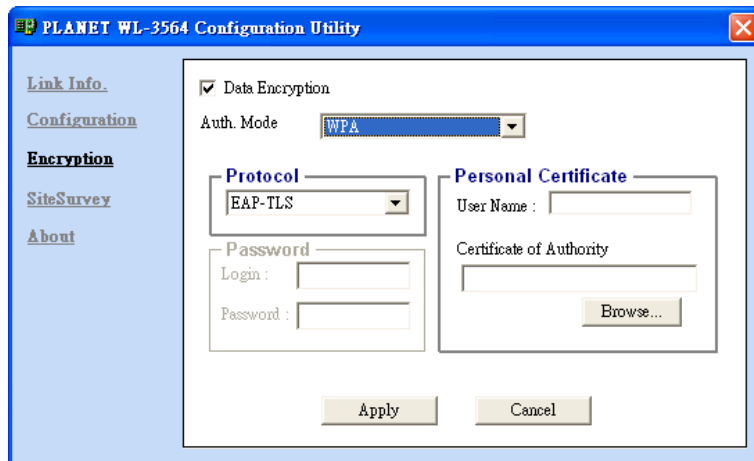
- (1)**Default Key:** There are 4 keys available for the WEP authentication/data encryption. Please select one of them to use.
- (2)**Network Key:** You can define the WEP (Wired Equivalent Privacy) Key values by yourself.
- (3)**Key Format:** You can decide on the WEP key format in **HEX** (Hexadecimal code, 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange, 0-9, a-z, A-Z) code.
- (4)**Key Length:** You can select 64 or 128 bits as the length of the WEP keys. Each category has 2 kinds of key length based on the key format you have selected: 64 bit (5 ASCII/ 10 HEX) and 128 bit (13 ASCII/ 26 HEX).

4. **WPA-PSK Pre-shared key option:** This will be configurable only when **WPA-PSK** is selected in **Auth. Mode** option.



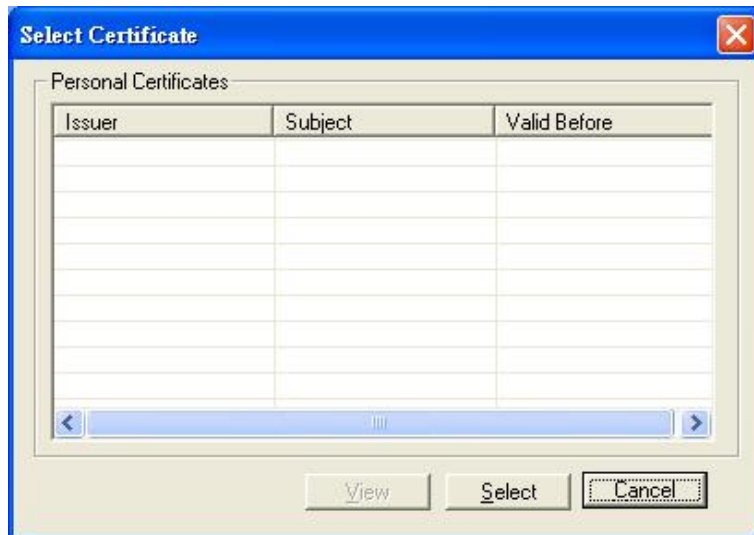
- (1)**Passphrase:** You have to input at least 8 character pass phrase as the pre-shared keys
- (2)**Confirm Key:** Please input the same pass phrase as above option.

5.WPA: This will be configurable only when WPA is selected in Auth. Mode option.



(1)**Protocol:** WPA function is support EAP-TLS protocol only now.

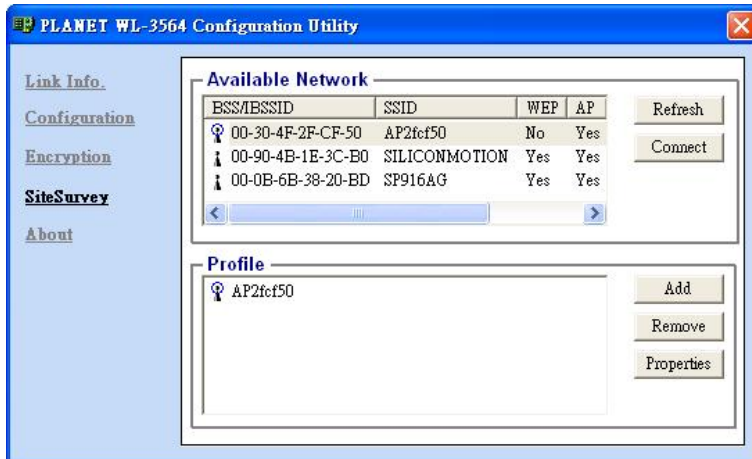
(2)**Personal Certificate:** Before enable WPA function. Please make sure you have obtain a valid Certificate. Please press “Browse...” button. You will see the installed Certificate in below dialog box. Please click the Certificate you want to use and press “Select”. Then you will back to the Encryption screen, please check the User Name and Certificate of Authority are correct. Press “Apply”.



Note: When you enable encryption, please ensure that you have configured the same authentication mode and settings as the wireless device you connect to. For example: Your Access Point is working in WPA-PSK authentication mode and key value (aaaaaaa), please ensure WL-3564 is using the same settings to communicate with this Access Point.

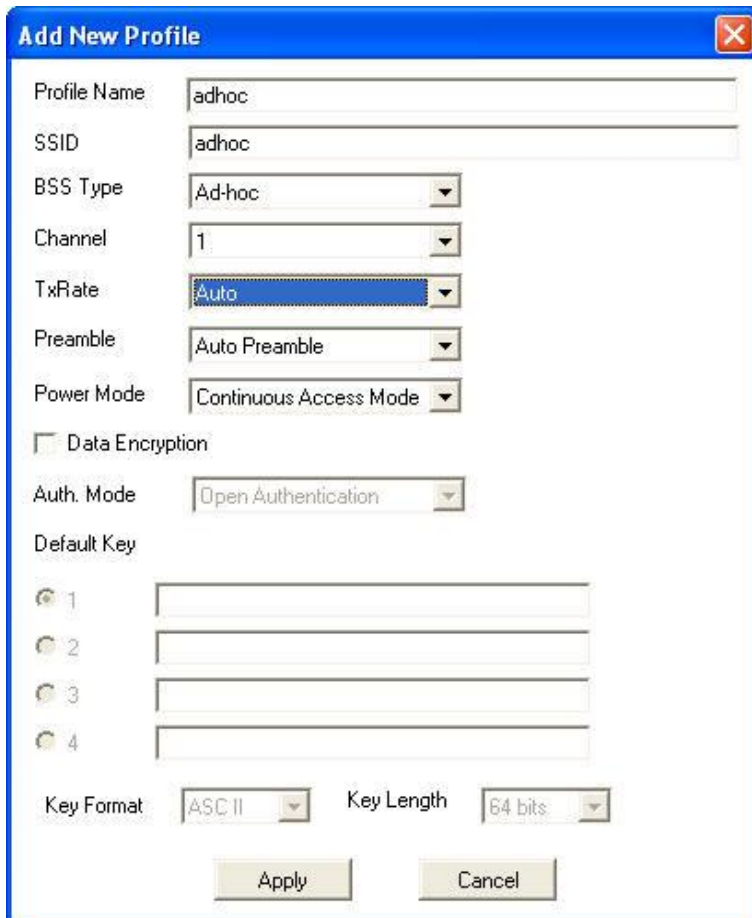
3.4 Site Survey

In this page, The **Available Network** list displays all available Access Points (Infrastructure mode) and adapters (Ad-hoc mode) within the signal coverage range for WL-3564 to connect to. Click “**Refresh**” to scan all available networks again. Select the SSID you want to connect and double-clicking the specified Access Point or clicking the “**Connect**” button. Then WL-3564 will connect to the device and create a profile for the selected device automatically.



You can configure the profile with those buttons:

- (1)**Add:** Add a new profile. If you want to create a new Ad-Hoc network, you should add a new profile manually and set the BSS Type as “Ad-Hoc”.



(2)Remove: Delete the selected profile.

(3)Properties: View or modify the selected profile.

After clicking “Add” or “Properties”, the dialog box as below will appear for your configuration. You can refer to the above to configure the settings of the profile to meet your needs.

The screenshot shows a dialog box titled "Connect: WAP4030". It contains the following fields and options:

- Profile Name: WAP-4030
- SSID: WAP4030
- BSS Type: Infrastructure
- Channel: 6
- TxRate: Auto
- Preamble: Auto Preamble
- Power Mode: Continuous Access Mode
- Data Encryption
- Auth. Mode: Open Authentication
- Default Key: Four radio buttons labeled 1, 2, 3, and 4, each with an adjacent text input field.
- Key Format: ASCII
- Key Length: 64 bits
- Buttons: Apply and Cancel

3.5 About

This page displays the current firmware, driver and utility version of WL-3564.

The screenshot shows the "PLANET WL-3564 Configuration Utility" window. It features a sidebar with the following links: [Link Info](#), [Configuration](#), [Encryption](#), [SiteSurvey](#), and [About](#). The main content area displays "Version Information" with the following data:

Version Information	Value
Firmware Version	3.0.0.36
Driver Version	3.1.0.9
Utility Version	1.0b14

Appendix

This section provides some technological Q&A. Read the description below to know the IEEE802.11g standard.

ü **What is the IEEE 802.11g standard?**

The IEEE 802.11g Wireless LAN standard subcommittee has formulated a standard for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate with each other. It is backward compatible with 802.11b.

ü **Which IEEE 802.11 features are supported?**

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

ü **What is Ad-hoc?**

An Ad-hoc mode is a wireless network type, meaning a group of computers with WLAN adapters are connected as an independent wireless LAN. It is operating without the presence of the Access Point.

What is Infrastructure?

An Infrastructure is a wireless network type, meaning wireless stations communicate with each other via an Access Point.

ü **Can Wireless products support printer sharing?**

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows NT/2000/XP/Server 2003, or other networking operating systems to support the printer or file sharing.

ü **Would the information be intercepted while transmitting on air?**

WLAN features two-folded 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 series offer the encryption function (WEP) to enhance security and Access Control for users to set up depending on their needs.

ü **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 the 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 of retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

ü **What is Spread Spectrum?**

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication 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).

Glossary

Access Point: An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc: An independent wireless LAN network formed by a group of computers, each with a network adapter.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type: An indication of an authentication algorithm which can be supported by the Access Point and wireless stations:

1. Open System: Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.
2. Shared Key: Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key.

Backbone: The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth: The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Beacon: A beacon is a packet broadcast by the Access Point to keep the network synchronized. What is included in a beacon is the information such as wireless LAN service area, the IP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit: A binary digit, which is either 0 or 1 for value, is the smallest unit for data.

Browser: An application program that enables one to view the content and interact on the World Wide Web or Intranet.

BSS: BSS stands for "Basic Service Set". It is an Access Point and all the wireless stations associating with it.

Channel: The bandwidth where wireless Radio operates is divided into several segments, which we call them "Channels". Access Points and associated wireless stations reside in one of the channels.

CSMA/CA: In local area network, this is the CSMA technique that combines slotted time -division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid the occurrence of collisions a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection, which is a LAN media access method used in Ethernet. When a device wants to gain access to the network, it will see if the network is quiet (senses the carrier). If it is not, it waits for a random amount of time before retrying. If the network is

quiet and two devices access the media at exactly the same time, their signals collide. When the collision is detected, they both back off and wait for a random amount of time before retrying.

DHCP: Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network easily. Every computer must have an IP address in order to communicate with each other in a TCP/IP-based network. Without DHCP, each computer must be entered the IP address manually. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon connected to the network.

DSSS: 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.

Dynamic IP Address: An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption: A security method that uses a specific algorithm to alter the data transmitted, and thus prevent others from knowing the information transmitted.

ESS: ESS stands for "Extended Service Set". More than one BSS is configured to become an Extended Service Set. WLAN mobile users can roam between different BSSs in an ESS.

ESSID: The unique identifier that identifies the ESS. In infrastructure mode, the stations use the same ESSID as AP's to communicate.

Ethernet: A popular local area data communications network, originally developed by Xerox Corp., Ethernet operates in a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation: When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold: The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frames due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway: a device that interconnects networks with different, incompatible communication protocols.

HEX: Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE: The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of

standards that often become national and international standards.

Infrastructure: An infrastructure network is a wireless network type, meaning all wireless stations communicate with each other via the Access Point.

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 2.4GHz, in particular, is being made available worldwide.

MAC Address: Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting: Sending data to a group of nodes instead of a single destination.

Node: A network junction or connection point, typically a computer or workstation.

Packet: A unit of data routed between a source and a destination in a network.

PLCP: Physical layer convergence protocol

PPDU: PLCP protocol data unit

Preamble Type: During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU: PLCP service data unit

Roaming: A LAN mobile user moves around an ESS and enjoys a continuous connection to the distribution system.

RTS: Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold: Transmitters contending for the medium may not be aware of 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.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask: The method used for splitting IP networks into a series of sub-groups, 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/IP: Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e.

intranet or Internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from those with a TCP/IP program.

Throughput: The amount of data transferred successfully from one point to another in a given period of time.

WEP: Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking to the Access Point.