ZyXEL G-360

802.11g Wireless PCI Adapter

User's Guide

Version 2.0

December 2004

ZyXEL
Unleash Networking Power

Copyright

Copyright ©2004 by ZyXEL Communications Corporation

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents' rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

NOTE

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization (RMA) number. Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online at www.zyxel.com for free future product updates and information.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry.

Federal Communications Commission (FCC) Interference Statement[1]

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

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 commercial environment. 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.

If this equipment does cause harmful interference to radio/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 the 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/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
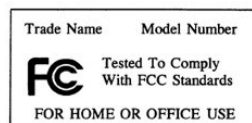
This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Caution

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

Certifications

Refer to the product page at www.zyxel.com.

Trade Name   Model Number

FC Tested To Comply
    With FCC Standards

FOR HOME OR OFFICE USE

---

[1] Refer to the *Quick Start Guide* for model specific FCC statement(s) and the procedure to view the product's certification(s).

Customer Support

When contacting your Customer Support Representative, please have the following information ready:

- ➢ Product model and serial number.
- ➢ Warranty Information.
- ➢ Date you received your product.
- ➢ Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[2] / FAX[2]	WEB SITE / FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw / sales@zyxel.com.tw	+886-3-578-3942 / +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com / sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 / +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de / sales@zyxel.de	+49-2405-6909-0 / +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 / +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es / sales@zyxel.es	+34 902 195 420 / +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk / sales@zyxel.dk	+45 39 55 07 00 / +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no / sales@zyxel.no	+47 22 80 61 80 / +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway

---

[2] "+" is the (prefix) number you enter to make an international telephone call.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[2] FAX[2]	WEB SITE FTP SITE	REGULAR MAIL
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on the purchase of your new ZyXEL G-360!

About This User's Guide

This manual provides information about the ZyXEL Wireless LAN Utility.

Syntax Conventions

- "Type" or "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.

- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.

- Window and command choices are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font.

- The ZyXEL G-360 802.11g Wireless PCI Adapter is referred to as the G-360 in this guide.

- The ZyXEL Wireless LAN Utility may be referred to as the ZyXEL WLAN Utility or, simply, as the ZyXEL Utility in this guide.

Related Documentation

➢ Support Disk

Refer to the included CD for support documents and device drivers.

➢ Quick Start Guide

Our Quick Start Guide is designed to help you get your ZyXEL G-360 up and running right away. It contains a detailed easy-to-follow connection diagram and information on installing your ZyXEL G-360.

➢ ZyXEL Glossary and Web Site

Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Graphics Icons Key

Wireless Access Point	Computer	Notebook computer
Server	Modem	Wireless Signal
Telephone	Switch	Router

Chapter 1
Getting Started

This chapter introduces the G-360 and prepares you to use the ZyXEL Utility.

1.1 About Your G-360

The G-360 is an IEEE 802.11g compliant wireless LAN adapter. With the G-360, you can enjoy the wireless mobility within the coverage area.

The following lists the main features of your G-360.

- Your G-360 can communicate with other IEEE 802.11b/g compliant wireless devices.
- Automatic rate selection.
- Proprietary transmission rates of 22Mbps for 802.11b standard and up to 125 Mbps for 802.11g standard when connected to the ZyXEL g+ access point or wireless router
- 64-bit, 128-bit and 256-bit WEP (Wired Equivalent Privacy) data encryption for network security
- Supports IEEE802.1x and WPA (Wi-Fi Protected Access)
- Low CPU utilization allowing more computer system resources for other programs
- A built-in antenna
- Driver support for Windows 98 Second Edition, Windows Me, Windows 2000 and Windows X

Actual speeds attained also depend on the distance from the AP, noise, etc.

1.2 G-360 Hardware and Utility Installation

Follow the instructions in the *Quick Start Guide* to install the ZyXEL Utility and make hardware connections.

1.3 Configuration Methods

To configure your G-360, use one of the following applications:

➢ Wireless Zero Configuration (WZC) (recommended for Windows XP)

➢ ZyXEL Utility

➢ Odyssey Client Manager

DO NOT use the Windows XP configuration tool or the Odyssey Client Manager and the ZyXEL Utility at the same time.

Refer to the Funk Odyssey Client documentation for more information.

1.4   Windows XP Users Only

You must disable WZC if you want to use the ZyXEL utility. Refer to the appendices on how to deactivate WZC or how to use WZC to manage the G-360.

1.5   Accessing the ZyXEL Utility

After you install and start the ZyXEL Utility, an icon for the ZyXEL Utility appears in the system tray.

When the ZyXEL Utility system tray icon displays, the G-360 is installed properly.

Figure 1-1 ZyXEL Utility: System Tray Icon

The color of the ZyXEL Utility system tray icon indicates the status of the G-360. Refer to the following table for details.

Table 1-1 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The G-360 is not connected to a wireless network or is searching for an available wireless network.
Green	The G-360 is connected to a wireless network.

Double click on the ZyXEL Wireless LAN Utility icon in the system tray to open the ZyXEL Utility. The ZyXEL Utility screens are similar in all supported Microsoft Windows operating systems. Screens for Windows Me are shown.

Click the 🛈 icon (located in the top right corner) to display the on-line help window.

Chapter 2
Wireless LAN Network

This chapter provides background information on wireless LAN network.

2.1 Overview

This section describes the wireless LAN network terms and applications.

2.1.1 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

2.1.2 Channel

A radio frequency used by a wireless device is called a channel.

2.1.3 Transmission Rate (Transfer Rate)

The G-360 provides various transmission (data) rate options for you to select. Options include **Fully Auto**, **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **11 Mbps**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, **54 Mbps** and **125 Mbps**. In most networking scenarios, the factory default **Fully Auto** setting proves the most efficient. This setting allows your G-360 to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the G-360 automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the G-360 gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

You can select any of the above options. If you wish to balance speed versus reliability, select **54 Mbps** in a networking environment where you are certain that all wireless devices can communicate at the highest transmission (data) rate. **1 Mbps** or **2 Mbps** are used often in networking environments where the range of the wireless connection is more important than speed.

> **Your G-360 can transmit at the proprietary transmission rates of** 22Mbps **or up to** 125 Mbps **when connected to the ZyXEL g+ AP or wireless router. Actual speeds attained also depend on the distance from the AP, noise, etc.**

2.1.4 Wireless Network Application

Wireless LAN works in either of the two modes: ad-hoc and infrastructure.

To connect to a wired network within a coverage area using Access Points (APs), set the G-360 operation mode to **Infrastructure (BSS)**. An AP acts as a bridge between the wireless stations and the wired network. In case you do not wish to connect to a wired network, but prefer to set up a small independent wireless workgroup without an AP, use the **Ad-hoc (IBSS)** (Independent Basic Service Set) mode.

Ad-Hoc (IBSS)

Ad-hoc mode does not require an AP or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

Figure 2-1 IBSS Example

To set up an ad-hoc network, configure all wireless stations in ad-hoc network type and use the same SSID and channel.

Infrastructure (BSS)

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

Figure 2-2 BSS Example

A series of overlapping BSS and a network medium, such as an Ethernet forms an Extended Service Set (ESS) or infrastructure network. All communication is done through the AP, which relays data packets to

other wireless stations or devices connected to the wired network. Wireless stations can then access resource, such as the printer, on the wired network.

Figure 2-3 Infrastructure Network Example

2.1.5 Roaming

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization or other factors.

The following figure depicts a roaming example. When wireless station **B** moves to position **X**, the G-360 in wireless station **B** automatically switches the channel to the one used by access point **2** in order to stay connected to the network.

Figure 2-4 Roaming Example

2.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communication between wireless stations and the wired network.

The figure below shows the possible wireless security levels on your G-360. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Figure 2-5 Wireless LAN Security Levels

Configure the wireless LAN security using the **Profile Security Settings** screen. If you do not enable any wireless security on your G-360, the G-360's wireless communications are accessible to any wireless networking device that is in the coverage area.

2.2.1 Data Encryption with WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the G-360 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your G-360.

- Automatic WEP key generation based on a "password phrase" called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
  For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four autom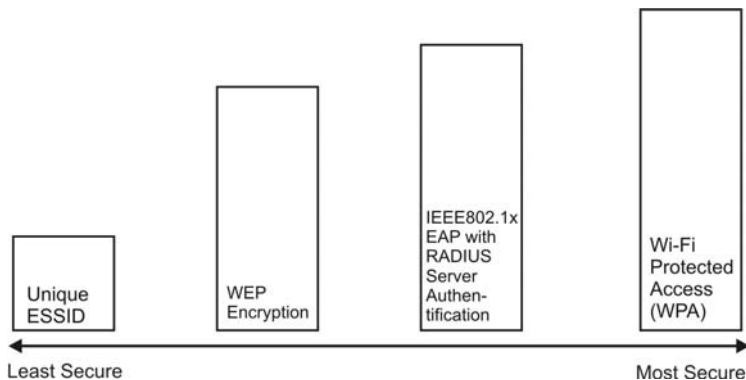atically generated WEP keys from the **Security Settings** screen of the ZyXEL Utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

Your G-360 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys and only one key is used as the default key at any one time.

2.2.2 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE802.1x. The G-360 supports EAP-TLS, EAP-TTLS and EAP-PEAP. Refer to the *Types of EAP Authentication* appendix for descriptions.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

2.2.3 WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

Therefore, if you don't have an external RADIUS server, you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

2.2.4 WPA-PSK Application Example

A WPA-PSK application looks as follows.

Step 1.   First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

Step 2.   The AP checks each client's password and (only) allows it to join the network if it matches its password.

Step 3.   The AP derives and distributes keys to the wireless clients.

Step 4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.
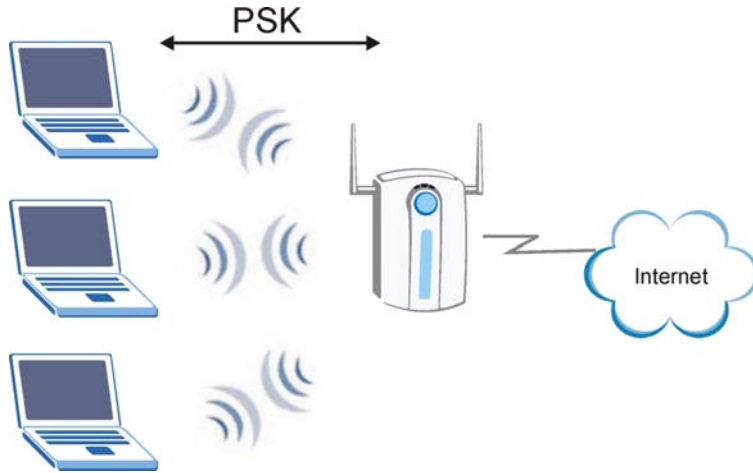

Figure 2-6 WPA-PSK Authentication

2.2.5 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

Step 1. The AP passes the wireless client's authentication request to the RADIUS server.

Step 2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

Step 3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.
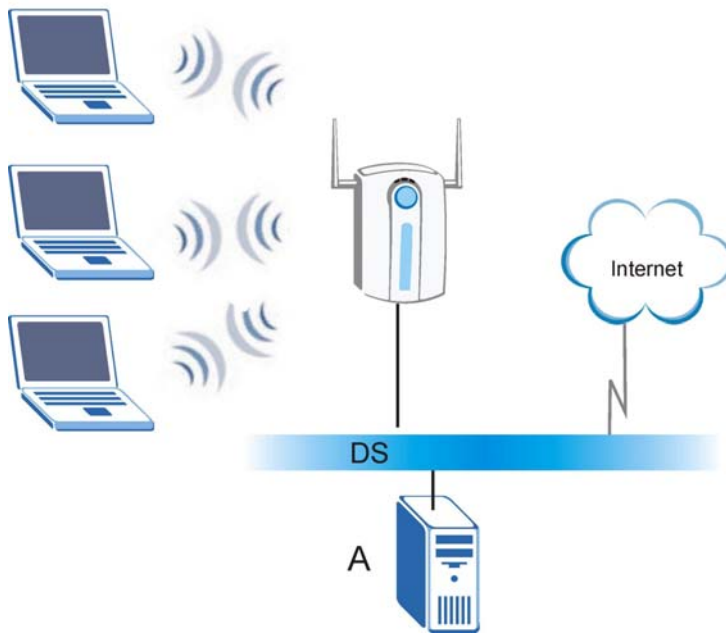
Figure 2-7 WPA with RADIUS Application Example

2.3 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the G-360 will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS Threshold** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS Threshold** size.

2.4 RTS/CTS Threshold

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.
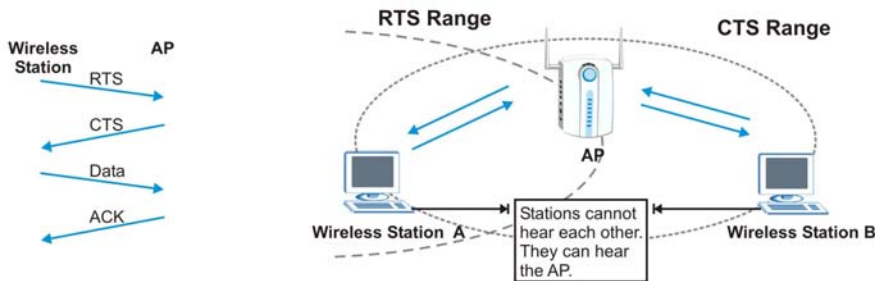
Figure 2-8 RTS Threshold

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS Threshold is designed to prevent collisions due to hidden nodes. An **RTS/CTS Threshold** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS Threshold** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS Threshold** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS Threshold** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS Threshold** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS Threshold** size.

> **Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance.**

2.5 Authentication Type

The IEEE 802.11b standard describes a simple authentication method between the wireless stations and AP. Two authentication modes are defined: **Open** and **Share**.

Open authentication mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP do *not* share a secret key. Thus the wireless stations can associate with any AP and listen to any data transmitted plaintext.

Share authentication mode involves a shared secret key to authenticate the wireless station to the AP. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP.

2.6   OTIST (One-Touch Intelligent Security Technology)

OTIST allows your ZyXEL g+ access point (AP) or wireless router to set the wireless adapter to use the same wireless settings as the ZyXEL g+ AP or wireless router.

The wireless adapter must also support OTIST and have OTIST enabled.

The following are the wireless settings that the ZyXEL g+ AP or wireless router assigns to the wireless adapter if OTIST is enabled on both devices and the OTIST setup keys are the same.

➢ SSID

➢ Security (WEP or WPA-PSK)

Chapter 3
Using the ZyXEL Utility

This chapter shows you how to configure the G-360 using the ZyXEL Utility.

3.1 The Link Info Screen

When the ZyXEL Utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your G-360.
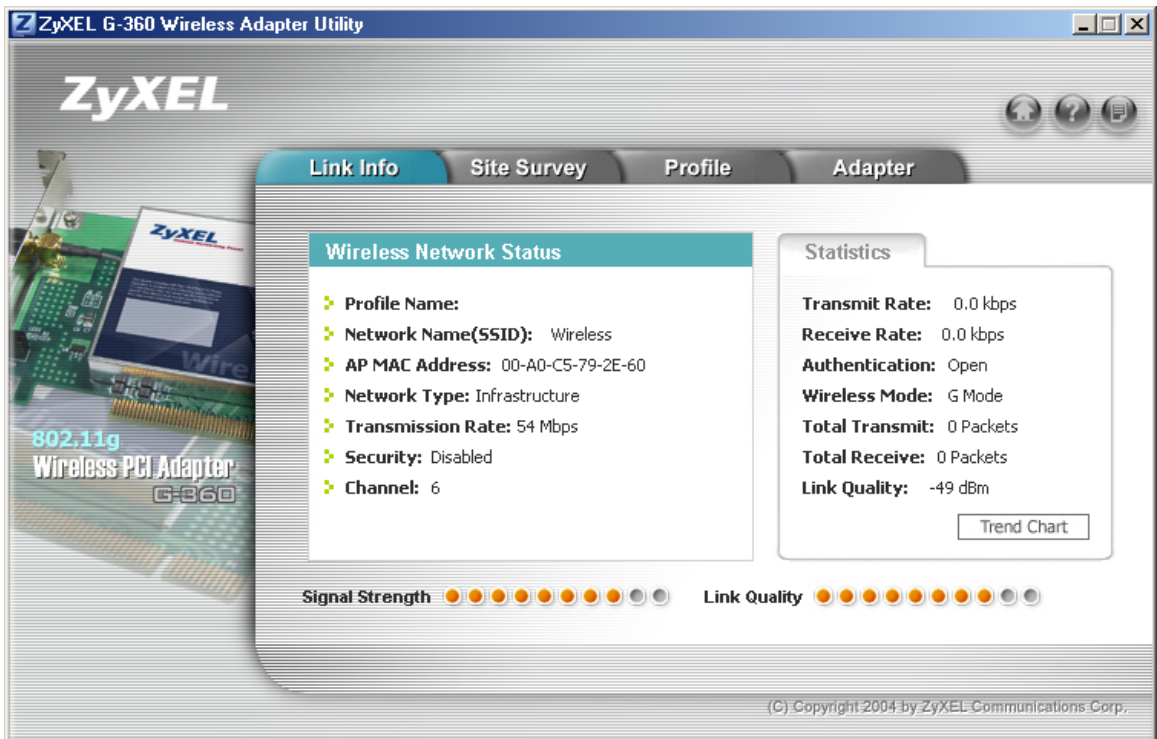

Figure 3-1 Link Info

The following table describes the labels in this screen.

Table 3-1 Link Info

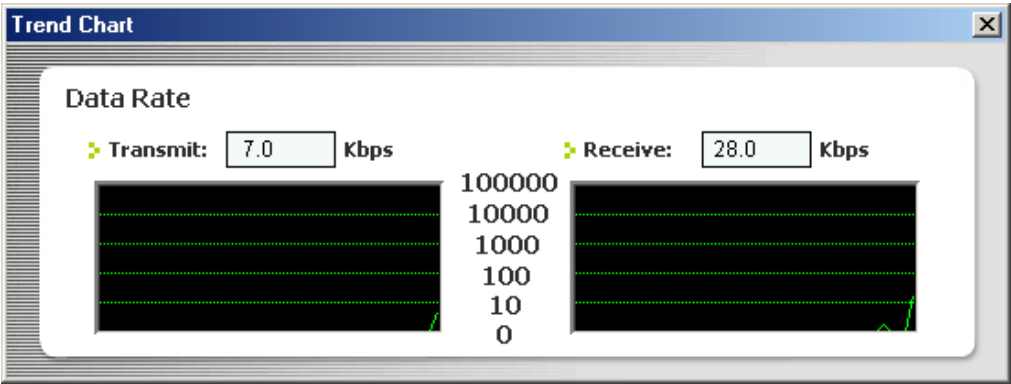| LABEL	DESCRIPTION
Wireless Network Status	
Profile Name	This is the name of the profile you are currently using.
Network Name (SSID)	The SSID identifies the Service Set to which a wireless station is associated. This field displays the name of the wireless device to which the G-360 is associated.
AP MAC Address	This field displays the MAC address of the wireless device to which the G-360 is associated.
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless network.
Transmission Rate	This field displays the current transmission rate of the G-360 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA-RADIUS** or **WPA**) or inactive (**Disabled**).
Channel	This field displays the radio channel the G-360 is currently using.
Statistics	
Transmit Rate	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive Rate	This field displays the current data receiving rate in kilobits per second (Kbps).
Authentication	This field displays the authentication method of the G-360.
Wireless Mode	This field indicates the wireless standard (802.11b or 802.11g) of the wireless device. This field displays **G Mode**, **B Mode** or **Mixed Mode**.
Total Transmit	This field displays the total number of data frames transmitted.
Total Receive	This field displays the total number of data frames received.
Signal Strength	This field displays the signal strength of the G-360.
Trend Chart	Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps).
Signal Strength	The status bar shows the strength of the signal.
Link Quality	The status bar shows the quality of the signal.

3.1.1 Trend Chart

Figure 3-2 Link Info: Trend Chart

The following table describes the labels in this screen.

Table 3-2 Link Info: Trend Chart

LABEL	DESCRIPTION
Transmit	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive	This field displays the current data receiving rate in kilobits per second (Kbps).

3.2 The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.
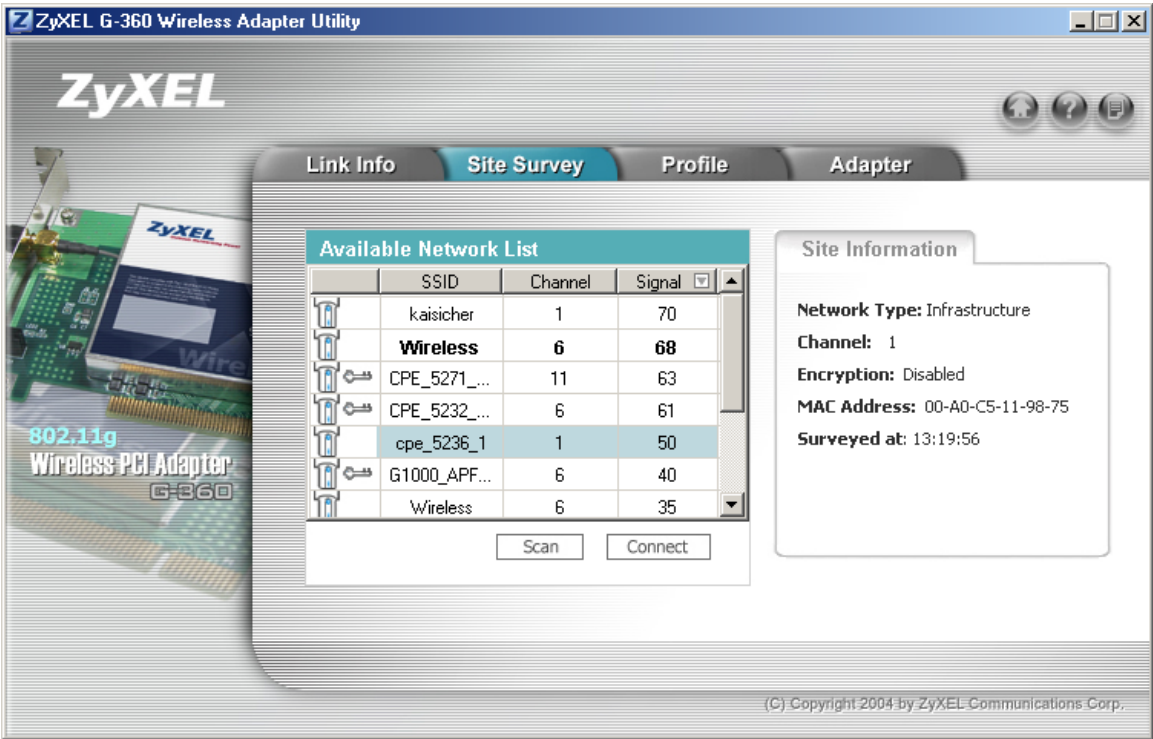
Figure 3-3 Site Survey

The following table describes the labels in this screen.

Table 3-3 Site Survey

LABEL	DESCRIPTION
Available Network List	
The device information in bold indicates the wireless network to which the G-360 is associated.	
Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.	

Table 3-3 Site Survey

LABEL	DESCRIPTION
📱🔑 , 📱 , 📶🔑 or 📶	📱🔑 denotes that the wireless device is in infrastructure mode and the wireless security is activated. 📱 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. 📶🔑 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. 📶 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set IDentifier) of each wireless device.
Channel	This field displays the channel number used by each wireless device.
Signal	This field displays the signal strength of each wireless device.
Scan	Click **Scan** to search for available wireless devices within transmission range.
Connect	Click **Connect** to associate to the selected wireless device.
Site Info Click an entry in the **Available Network List** table to display the information of the selected wireless device.	
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless device.
Channel	This field displays the channel number used by each wireless device.
Encryption	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA-RADIUS** or **WPA**) or inactive (**Disabled**).
MAC address	This field displays the MAC address of the wireless device.
Surveyed at	This field displays the time when the wireless device is scanned.

3.2.1 Connecting to a Network

Follow the steps below to connect to a network using the **Site Survey** screen.

Step 1.   Click **Scan** to search for all available wireless networks within range.

Step 2.   To join a network, either click an entry in the table to select a wireless network and then click **Connect** or double-click an entry.

Step 3.   If the wireless security is activated for the selected wireless network, the **Security Settings** screen displays. You must set the related fields in the **Security Settings** screen to the same

security settings as the associated AP. Refer to *Section 3.2.2* for more information. Otherwise click the close (❌) button and connect to another wireless network without data encryption.

Step 4.   Verify that you have successfully connected to the selected network and check the network information in the **Link Info** screen.

3.2.2 Security Settings

When you configure the G-360 to connect to a network with wireless security activated and the security settings are disabled on the G-360, the screen varies according to the encryption method used by the selected network.
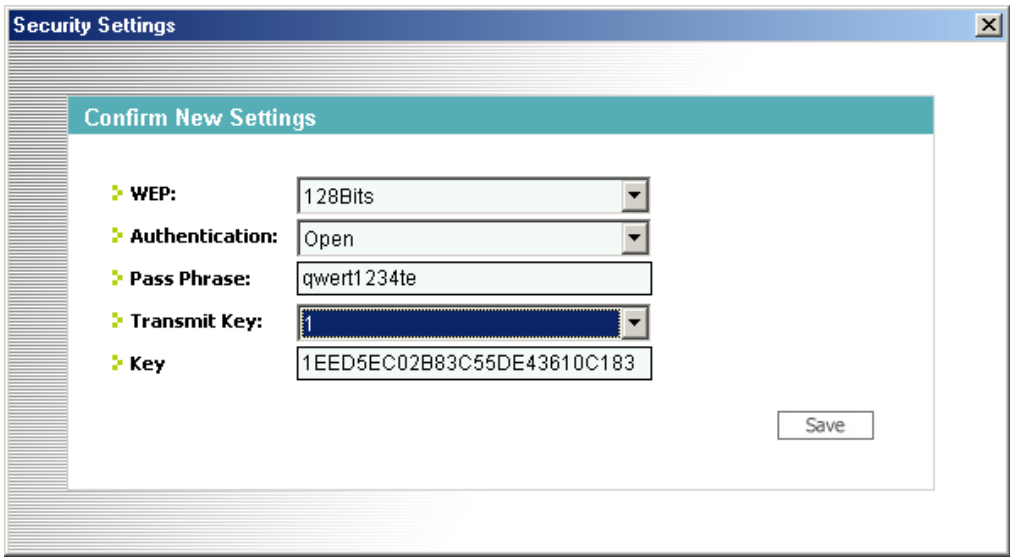
WEP Encryption

Figure 3-4 Site Survey: Security Settings: WEP

The following table describes the labels in this screen.

Table 3-4 Site Survey: Security Settings: WEP

LABEL	DESCRIPTION
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields.
Authentication	Select an authentication method. Choices are **Share** and **Open**. Refer to *Section 2.5* for more information.

Table 3-4 Site Survey: Security Settings: WEP

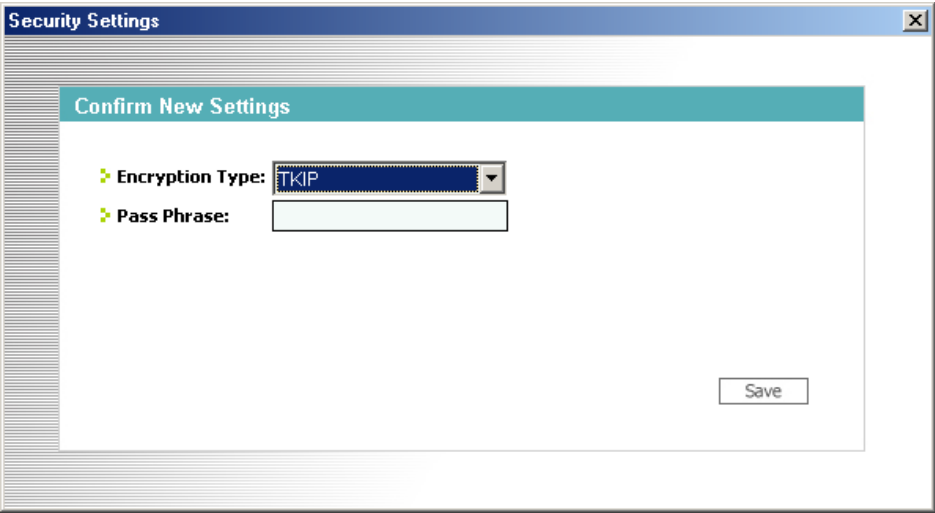| LABEL	DESCRIPTION
Pass Phrase	As you enter the passphrase, the G-360 automatically generates four different WEP keys. Only one key displays in the key field below at one time. Refer to *Section 2.2.1* for more information.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.

Key x (where x is a number between 1 and 4)	If you want to manually set the WEP keys, enter the WEP key in the field provided.
	If you select **64 Bits** in the **WEP** field.
	    ♦ Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type
	or
	    ♦ Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type.
	
	If you select **128 Bits** in the **WEP** field,
	    ♦ Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type
	or
	    ♦ Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type.
	
	If you select **256 Bits** in the **WEP** field,
	    ♦ Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 000011112222333344445555666677778888999AAAABBBBCCCC000011) for HEX key type
	or
	    ♦ Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) for ASCII key type.
	
	The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.
	ASCII WEP keys are case sensitive.

Save	Click **Save** to save the changes back to G-360 and display the **Link Info** screen. Otherwise, click the close (X) button to discard changes and go back to the **Site Survey** screen.

WPA-PSK

Figure 3-5 Site Survey: Security Settings: WPA-PSK

The following table describes the labels in this screen.

Table 3-5 Site Survey: Security Settings: WPA-PSK

FIELD	DESCRIPTION
Encryption Type	WPA uses Temporal Key Integrity Protocol (TKIP) to improve data encryption.
Pass Phrase	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a passphrase from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Save	Click **Save** to save the changes back to G-360 and display the **Link Info** screen. Otherwise, click the close (✕) button to discard changes and go back to the **Site Survey** screen.

WPA

Figure 3-6 Site Survey: Security Settings: WPA

The following table describes the labels not previously discussed

Table 3-6 Site Survey: Security Settings: WPA

FIELD	DESCRIPTION
Authentication Type	Select an authentication method from the drop down list. Options are **EAP-TLS**, **EAP-TTLS** and **EAP-PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **EAP-TLS** in the **Authentication Type** field. Enter the password associated with the user name above.

Table 3-6 Site Survey: Security Settings: WPA

FIELD	DESCRIPTION
Certificate	This field is only available when you select **EAP-TLS** in the **Authentication Type** field.
	Specify the location and name of a certificate in the **Certificate** field or click **Browse** to locate it.
	You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Browse	This field is only available when you select **EAP-TLS** in the **Authentication Type** field.
	Click this button to display the **Select Certificate** screen, select a certificate and click **OK**.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
TTLS Protocol	This field is only available when you select **EAP-TTLS** in the **Authentication Type** field.
	Use the drop-down list box to select a TTLS protocol. Options are **PAP**, **CHAP**, **MS CHAP**, **MS CHAP v2** and **EAP**.
PEAP Inner EAP	This field is only available when you select **EAP-PEAP** in the **Authentication Type** field.
	Use the drop-down list box to select a PEAP protocol. Options are **EAP-GTC** and **MS CHAP v2**.
Save	Click **Save** to save the changes back to G-360 and display the **Link Info** screen.
	Otherwise, click the close (✕) button to discard changes and go back to the **Site Survey** screen.

802.1x

The following section describes how to configure IEEE802.1x security with various authentication methods.

Figure 3-7 Site Survey: Security Settings: 802.1x

The following table describes the labels not previously discussed

Table 3-7 Site Survey: Security Settings: 802.1x

FIELD	DESCRIPTION
Authentication Type	Select an authentication method from the drop down list. Options are **EAP-TLS**, **EAP-TTLS** and **EAP-PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **EAP-TLS** in the **Authentication Type** field. Enter the password associated with the user name above.
Certificate	This field is only available when you select **EAP-TLS** in the **Authentication Type** field. Specify the location and name of a certificate in the **Certificate** field or click **Browse** to locate it. **You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.**

Table 3-7 Site Survey: Security Settings: 802.1x

FIELD	DESCRIPTION
Browse	This field is only available when you select **EAP-TLS** in the **Authentication Type** field.
	Click this button to display the **Select Certificate** screen, select a certificate and click **OK**.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
TTLS Protocol	This field is only available when you select **EAP-TTLS** in the **Authentication Type** field.
	Use the drop-down list box to select a TTLS protocol. Options are **PAP**, **CHAP**, **MS CHAP**, **MS CHAP v2** and **EAP**.
PEAP Inner EAP	This field is only available when you select **EAP-PEAP** in the **Authentication Type** field.
	Use the drop-down list box to select a PEAP protocol. Options are **EAP-GTC** and **MS CHAP v2**.
Save	Click **Save** to save the changes back to G-360 and display the **Link Info** screen. Otherwise, click the close (❌) button to discard changes and go back to the **Site Survey** screen.

3.3   The Profile Screen

Click the **Profile** tab in the ZyXEL Utility program to display the **Profile** screen as shown next.

The profile function allows you to save the wireless network settings in this screen, or use one of the pre-configured network profiles.
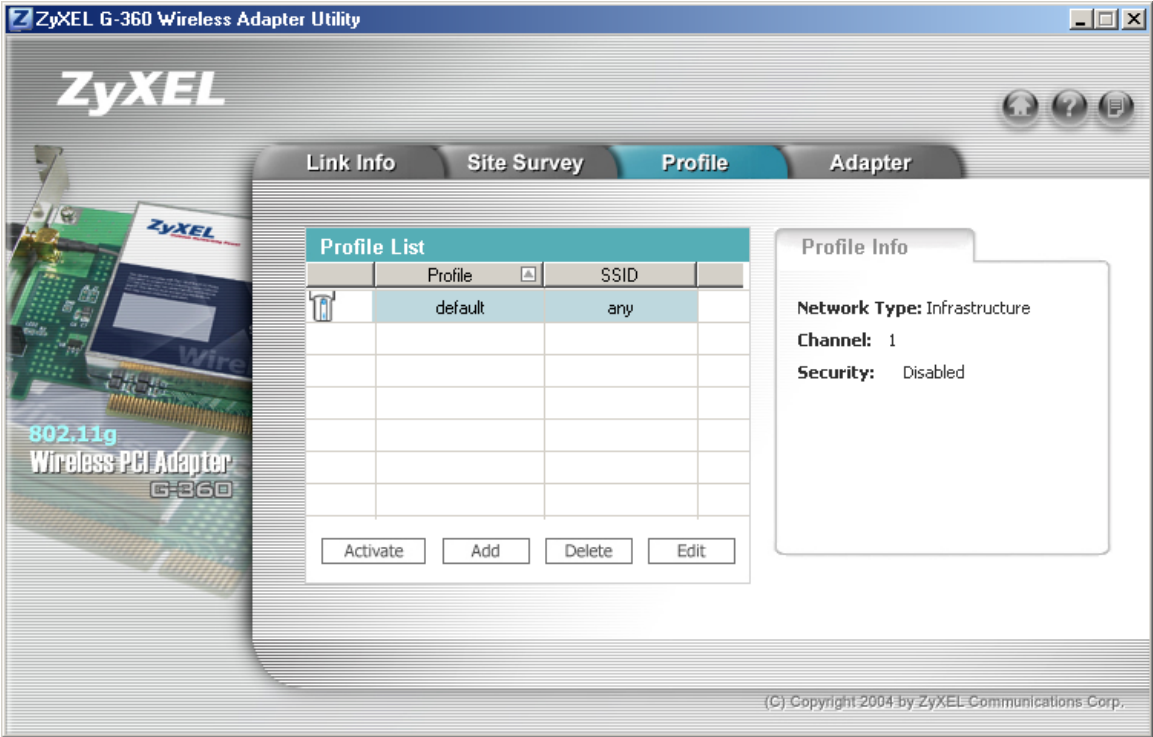
Figure 3-8 Profile

The following table describes the labels in this screen.

Table 3-8 Profile

LABEL	DESCRIPTION
Profile List	
Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.	

Table 3-8 Profile

LABEL	DESCRIPTION
, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated. denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
Profile Name	This is the name of the pre-configured profile.
SSID	This is the SSID of the wireless network to which the selected profile associate.
Connect	To use a previously saved network profile, select a pre-configured profile name in the table and click **Connect**.
Add	To add a new profile into the table, click **Add**.
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.
Profile Info The following fields display detail information of the selected profile in the **Profile List** table.	
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the profile.
Channel	This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA-RADIUS** or **WPA**) or inactive (**Disabled**).

3.3.1 Adding a New Profile

Follow the steps below to add a new profile.

Step 1.   Click **Add** in the **Profile** screen to display the screen as shown next. Click **Next** to continue.
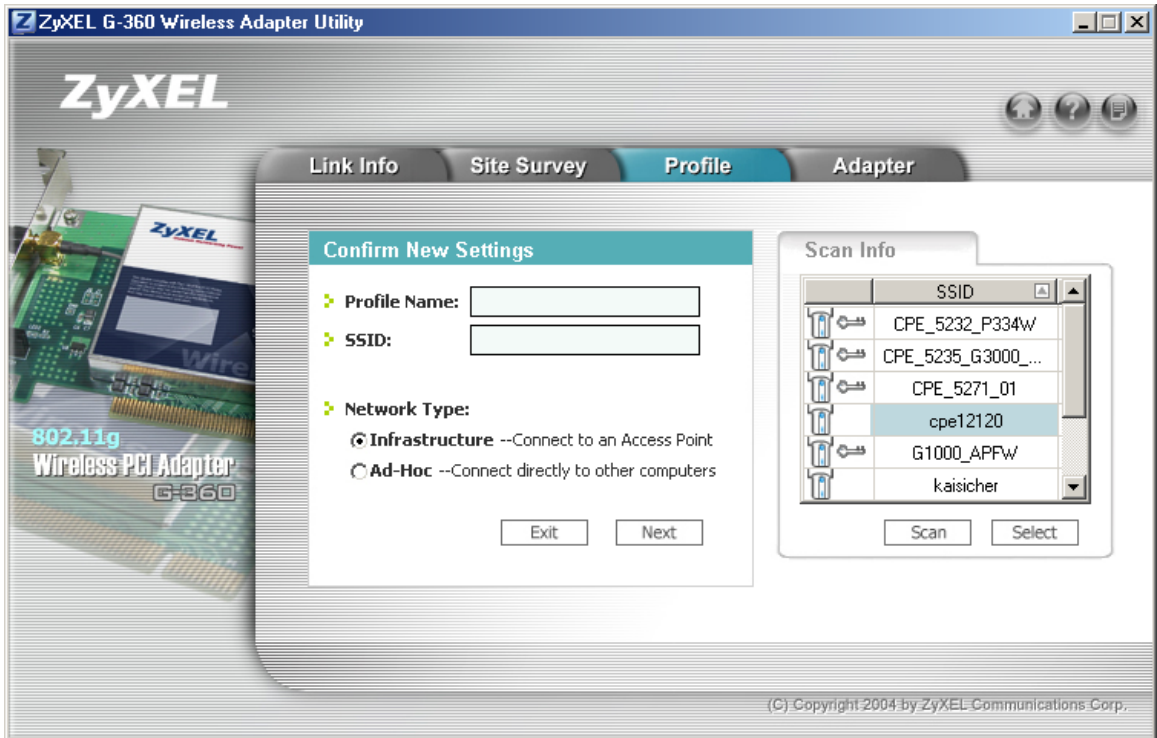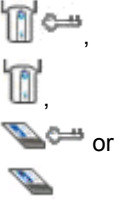
Figure 3-9 Profile: Add a New Profile

The following table describes the labels in this screen.

Table 3-9 Profile: Add a New Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID (Service Set IDentifier) of the AP or the peer ad-hoc computer to which you want to associate in this field. To associate to an ad-hoc network, you must enter the same SSID as the peer ad-hoc computer.
	Otherwise, leave this field blank or enter **any** to have the G-360 associate to or roam between any infrastructure wireless networks.
Network Type	Select the **Infrastructure** radio button to associate to an AP.
	Select the **Ad-Hoc** radio button to associate to a peer computer.

Table 3-9 Profile: Add a New Profile

LABEL	DESCRIPTION
Next	Click **Next** to go to the next screen.
Exit	Click **Exit** to go back to the previous screen without saving.
Scan Info	This table displays the information of the available wireless networks within the transmission range.

, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated.
	
	  denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.
	
	  denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.
	
	  denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.

SSID	This field displays the SSID (Service Set IDentifier) of each wireless device.
Scan	Click **Scan** to search for available wireless devices within transmission range.
Select	Select an available wireless device in the table and click **Select** to add it to this profile. Whenever you activate this profile, the G-360 associates to the selected wireless network only.

Step 2. If you select the **Infrastructure** network type in the previous screen, skip to *Step 3*. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a channel number and click **Next** to continue.
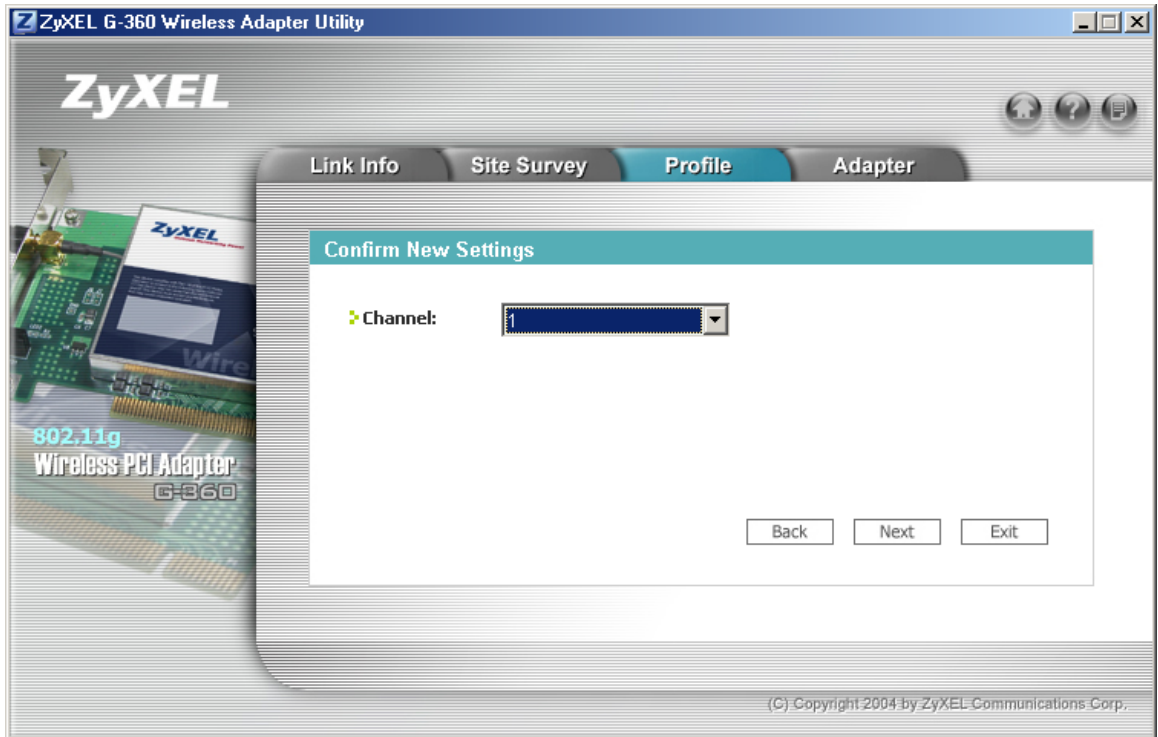
Figure 3-10 Profile: Select a Channel

The following table describes the labels in this screen.

Table 3-10 Profile: Select a Channel

LABEL	DESCRIPTION
Channel	Select a channel number from the drop-down list box. To associate to an ad-hoc network, you must use the same channel as the peer computer.

Step 3. If you select **Infrastructure** network type in the first screen, select **WEP**, **WPA-PSK**, **WPA** or **802.1x** from the drop-down list box to enable data encryption. If you select **Ad-Hoc** network type in the first screen, you can only use **WEP** encryption method. Otherwise, select **Disabled** to allow the G-360 to communicate with the access points or other peer wireless computers without any data encryption and skip to *Step 5*.
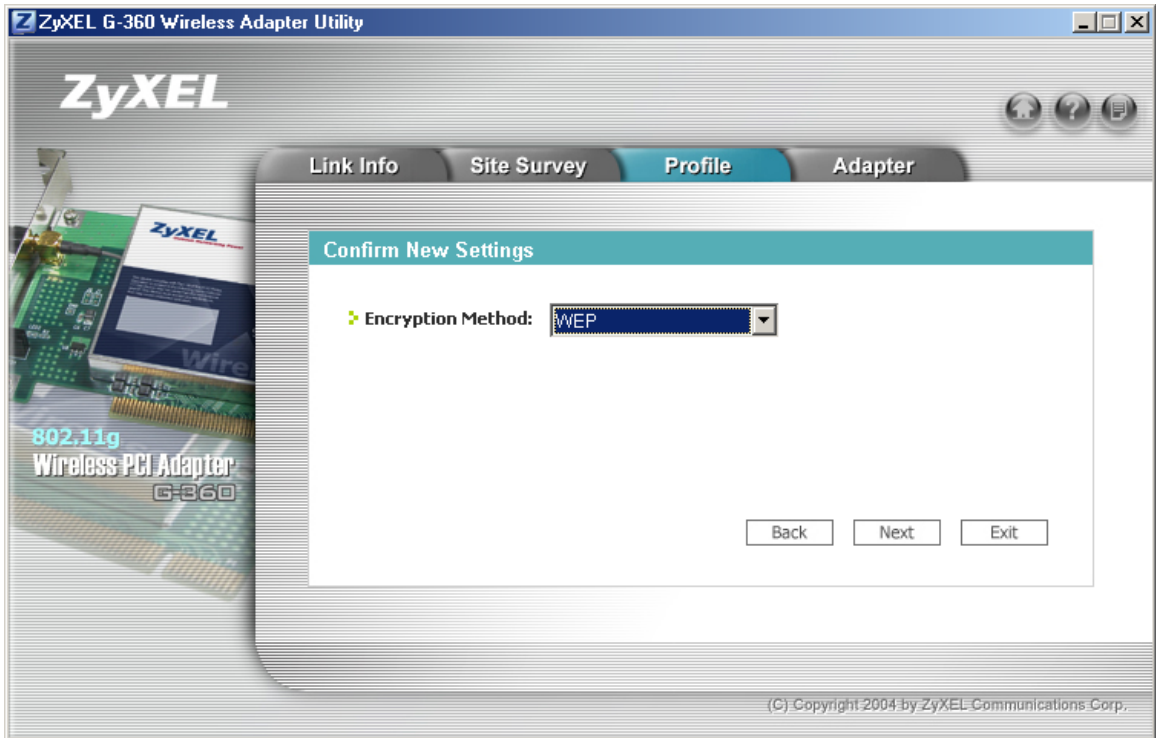
Figure 3-11 Profile: Wireless Settings

Step 4. The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless computers as they are on the G-360. Refer to *Section 3.2.2* for detailed information on wireless security configuration.

Figure 3-12 Profile: Security Settings

Step 5. This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

Figure 3-13 Profile: Confirm New Settings

Step 6. To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button.

Once you activate a profile, the ZyXEL Utility will use that profile the next time it is started.

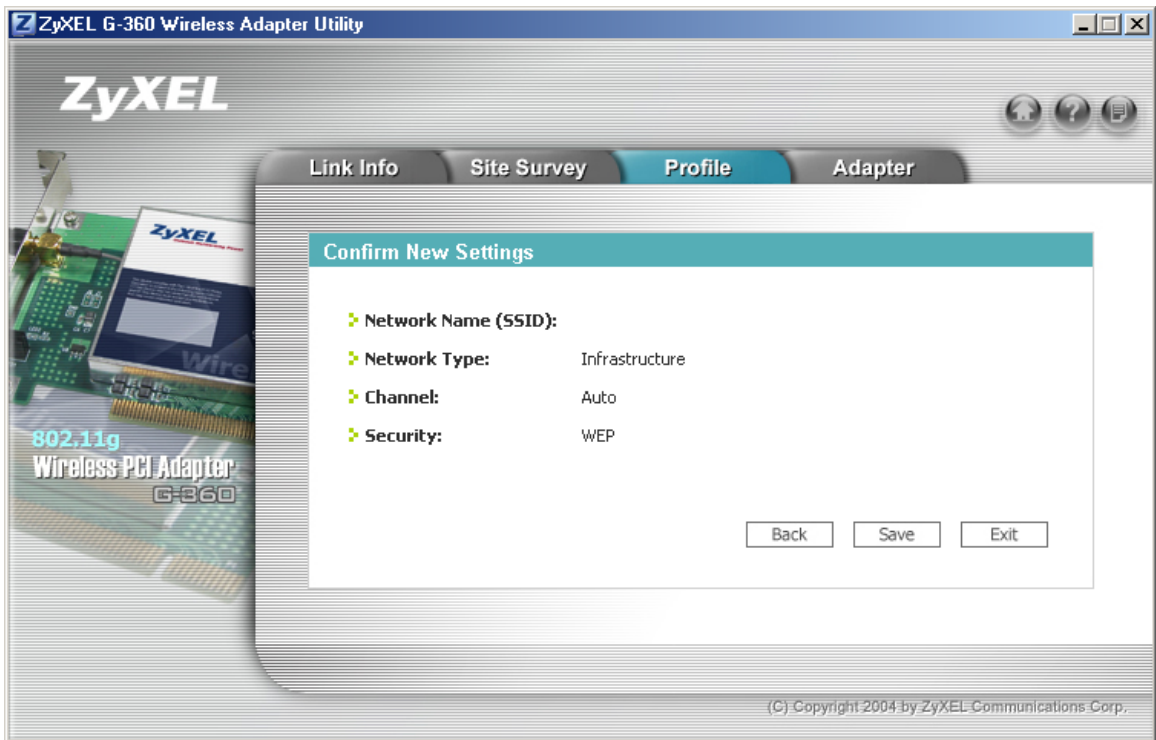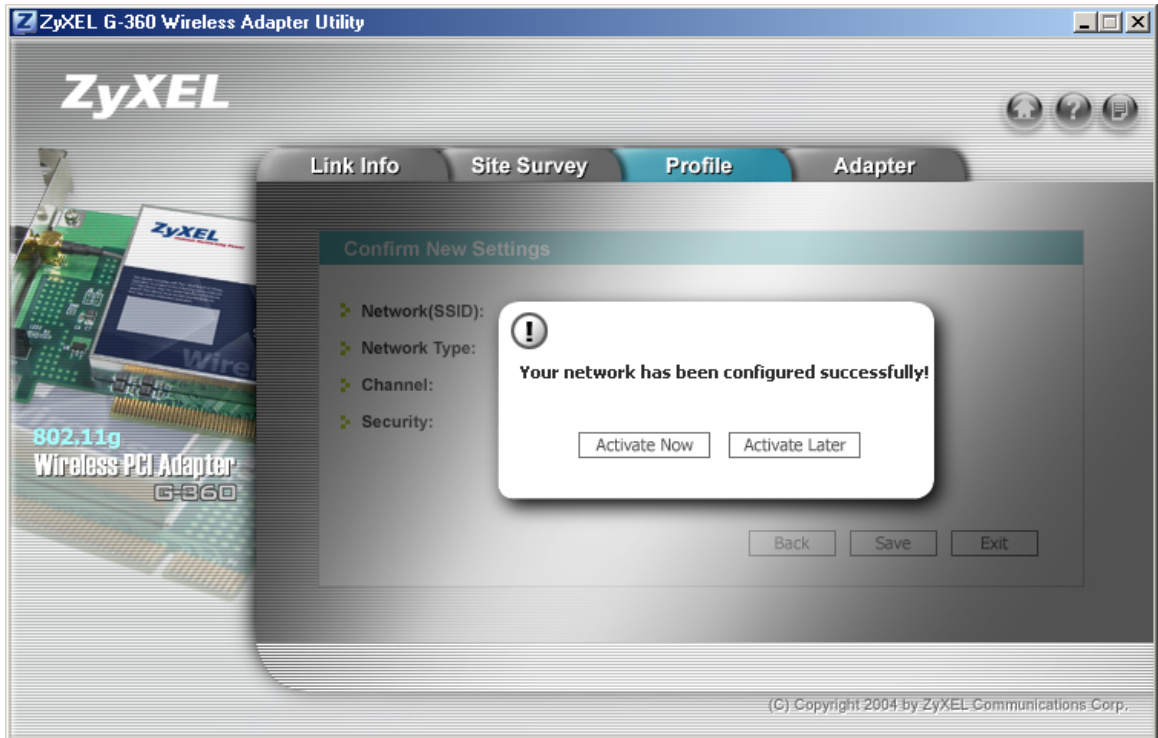**Figure 3-14 Profile: Activate the Profile**

3.4   The Adapter Screen
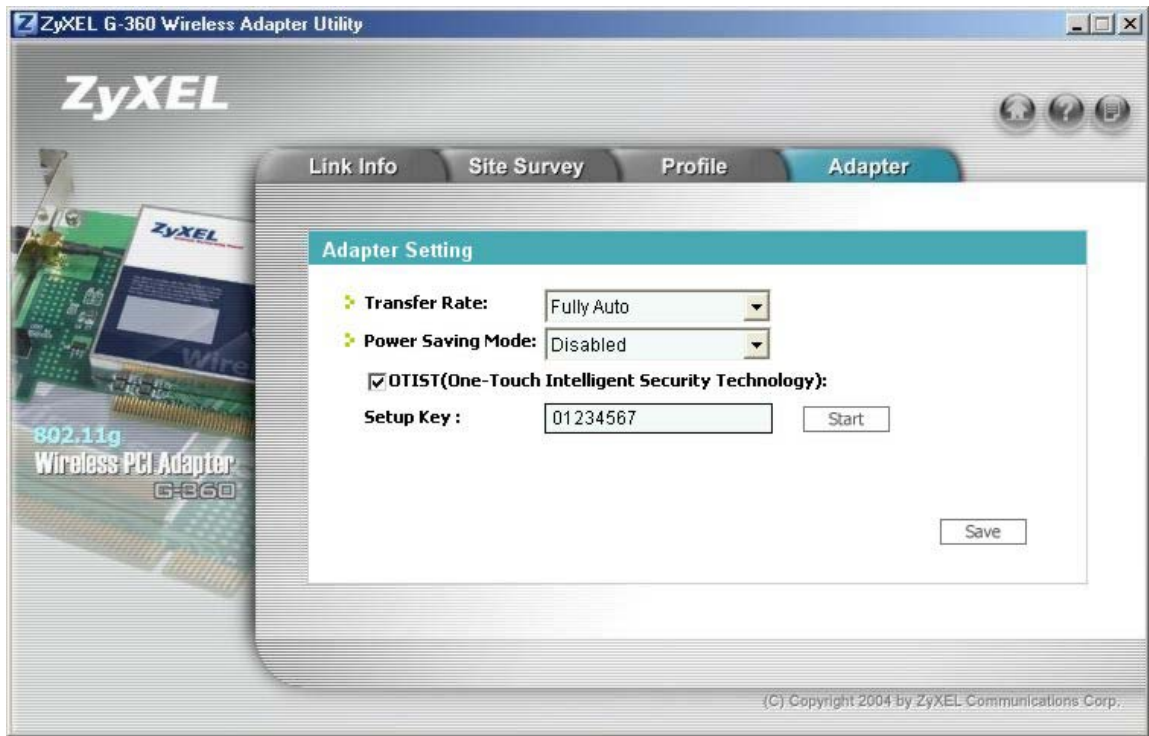
To set advanced features on the G-360, click the **Adapter** tab.

Figure 3-15 Adapter

The following table describes the labels in this screen.

Table 3-11 Adapter

LABEL	DESCRIPTION
Adapter Setting	
Transfer Rate	Select a transmission speed from the drop-down list box. Choose from **Fully Auto** (default), **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **11 Mbps**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, **54 Mbps** and **125 Mbps**.
	Your G-360 can transmit at the proprietary transmission rates of 22Mbps or up to 125 Mbps when connected to the ZyXEL g+ AP or wireless router. Actual speeds attained also depend on the distance from the AP, noise, etc.
Power Saving Mode	Select **Enabled** to save power (especially for notebook computers). This forces the G-360 to go to sleep mode when it is not transmitting data.
	When you select **Disabled**, the G-360 will never go to sleep mode.

Table 3-11 Adapter

LABEL	DESCRIPTION
OTIST (One-Touch Intelligent Security Technology)	Select this check box to enable OTIST.
Setup Key	Enter the same setup key (of exactly eight ASCII characters) as the ZyXEL g+ AP or wireless router to which you want to associate. The default OTIST setup key is "01234567". **If you change the OTIST setup key on the ZyXEL g+ AP or wireless router, you must also make the same change here.**
Start	Click **Start** to encrypt the wireless security data using the setup key and have the ZyXEL g+ AP or wireless router set your G-360 to use the same wireless settings as the ZyXEL g+ AP or wireless router. You must also activate and start OTIST on the ZyXEL g+ AP or wireless router at the same time. See the *User's Guide* of your ZyXEL g+ AP or wireless router or the guide on OTIST for more details.
Save	Click **Save** to save the changes back to G-360.

Chapter 4
Maintenance

This chapter describes how to uninstall or upgrade the ZyXEL Utility.

4.1   The About Screen

The **About** screen displays related version numbers of the G-360. To display the screen as shown next, click the about ( ) button.

Figure 4-1 About

The following table describes the read-only fields in this screen.

Table 4-1 About

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the ZyXEL driver.
Utility Version	This field displays the version number of the ZyXEL Utility.

4.2 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL Utility from your computer.

Step 1. Click **Start**, **Programs**, **G-360 Wireless Adapter**, **Uninstall**.

Step 2. When prompted, click **OK** to remove the driver and the utility software.

Confirm Uninstallation   ⊠

Do you want to uninstall the device driver, application and all its components?
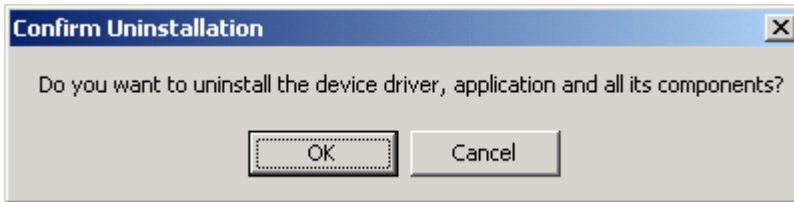
OK   Cancel

Figure 4-2 Confirm Uninstall

Step 3. Click **Finish** to complete uninstalling the software. Restart your computer if prompted.

4.3 Upgrading the ZyXEL Utility

Before you uninstall the ZyXEL Utility, take note of the current network configuration.

To perform the upgrade, follow the steps below.

Step 1. Download the latest version of the utility from the ZyXEL web site and save the file on your computer.

Step 2. Follow the steps in *Section 4.2* to remove the current ZyXEL Utility from your computer.

Step 3. Restart your computer when prompted.

Step 4. After restarting, refer to the procedure in the *Quick Start Guide* to install the new utility.

Step 5. Check the version numbers in the **About** screen to make sure the new utility is installed properly.

Chapter 5
Troubleshooting

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

5.1   Problems Starting the ZyXEL Utility Program

Table 5-1 Troubleshooting Starting ZyXEL Utility Program

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Wireless LAN Utility	Make sure the G-360 is properly inserted and the LED(s) is on. Refer to the *Quick Start Guide* for the LED descriptions.
	Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the G-360 under **Network Adapter**. (Steps may vary depending on the version of Windows).
	Install the G-360 in another computer. If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.
The ZyXEL Utility icon does not display.	If you install the Funk Odyssey Client software on the computer, uninstall (remove) both the Funk Odyssey Client software and ZyXEL utility, and then install the ZyXEL utility again after restarting the computer.
	If you use the Windows XP configuration tool and the ZyXEL Utility to configure the G-360 at the same time, the ZyXEL Utility icon does not display. You need to disable the Windows XP configuration tool (refer to Appendix A for more information).

5.2   Problem with the Link Status

Table 5-2 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	Search and connect to another AP with a better link quality using the **Site Survey** screen.
	Move your computer closer to the AP or the peer computer(s) within the transmission range.
	There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.

5.3   Problems Communicating With Other Computers

Table 5-3 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The G-360 computer cannot communicate with the other computer.	Make sure you are connected to the network.
A. **Infrastructure**	Make sure that the AP and the associated computers are turned on and working properly.
	Make sure the G-360 computer and the associated AP use the same SSID.
	Change the AP and the associated wireless clients to use another radio channel if interference is high.
	Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Settings** screen.
B. **Ad-Hoc (IBSS)**	Verify that the peer computer(s) is turned on.
	Make sure the G-360 computer and the peer computer(s) are using the same SS ID and channel.
	Make sure that the computer and the peer computer(s) share the same security option and key.
	Change the wireless clients to use another radio channel if interference is high.

Appendix A
Disable Windows XP Wireless LAN Configuration Tool

Windows XP includes a configuration tool (also known as Wireless Zero Configuration (WZC)) for wireless devices.

Follow the steps below to disable the configuration tool in Windows XP after you install the ZyXEL Utility. The screen varies depending on the version of Windows XP service pack.

Via the Wireless Network System Tray Icon

If the network icon for wireless connections is not present in the system tray, see the next section.

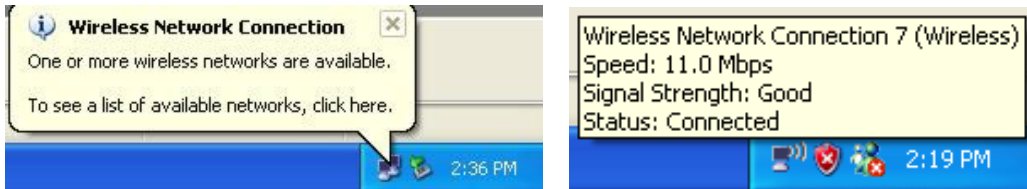1.   Double-click the network icon for wireless connections in the system tray.

Diagram 1 Windows XP: System Tray Icon

2. Windows XP SP1: When a **Wireless Network Connection** window displays, click **Advanced…**.
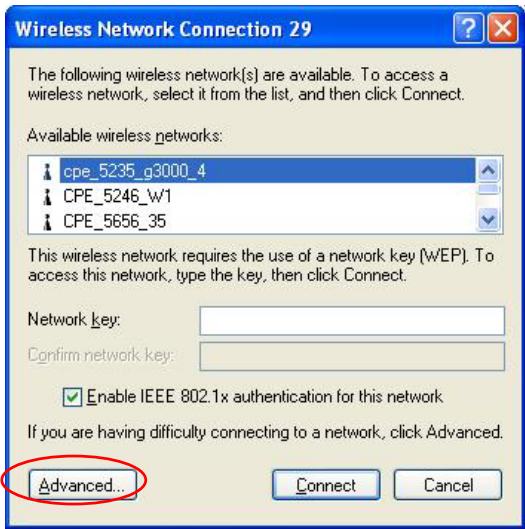

Diagram 2 Windows XP SP1: Wireless Network Connection

Windows XP SP2: When a **Wireless Network Connection** window displays, click **Change advanced settings** under **Related Tasks** and then the **Wireless Networks** tab.
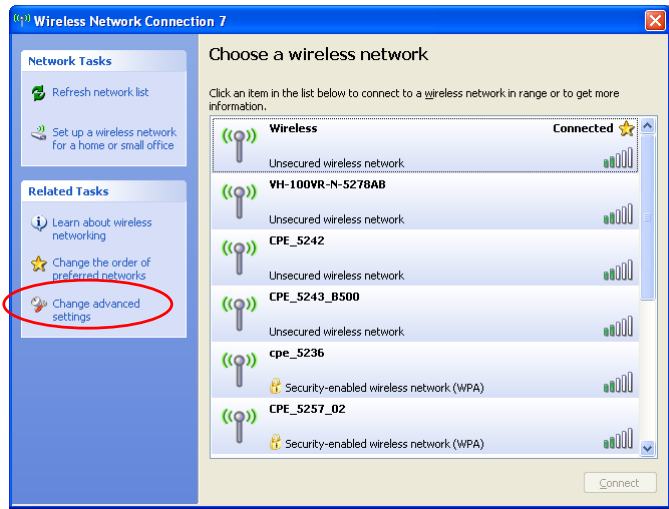

Diagram 3 Windows XP SP2: Wireless Network Connection

3. In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is *not* selected. Click **OK**.
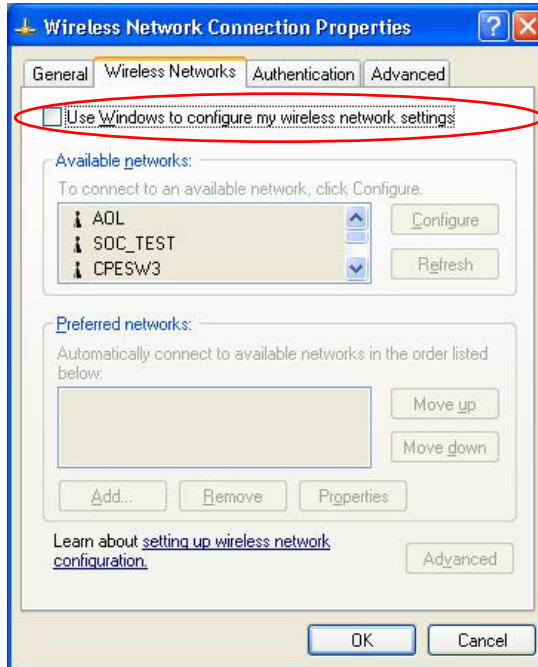

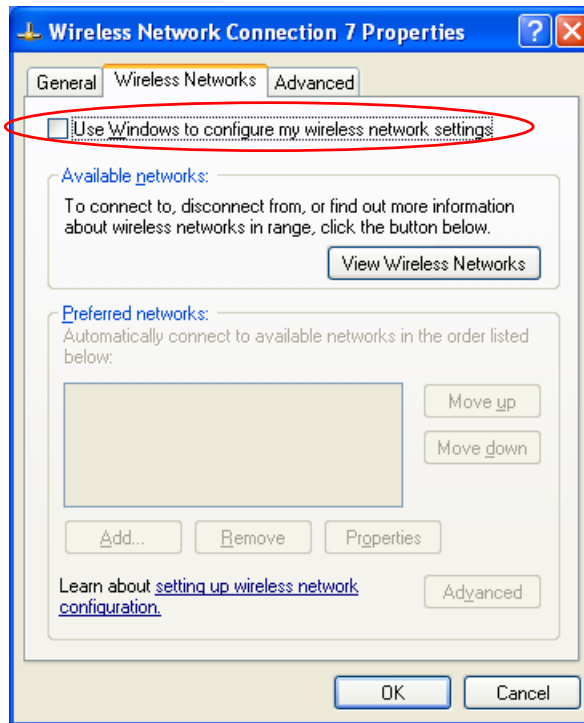**Diagram 4 Windows XP SP1: Wireless Network Connection Properties**

Diagram 5 Windows XP SP2: Wireless Network Connection Properties

Via the Control Panel

4. If the icon for the wireless network connection is not in the system tray, click **Start**, **Control Panel** and double-click **Network Connections**.

5. Double-click on the icon for wireless network connection to display a status window as shown below.

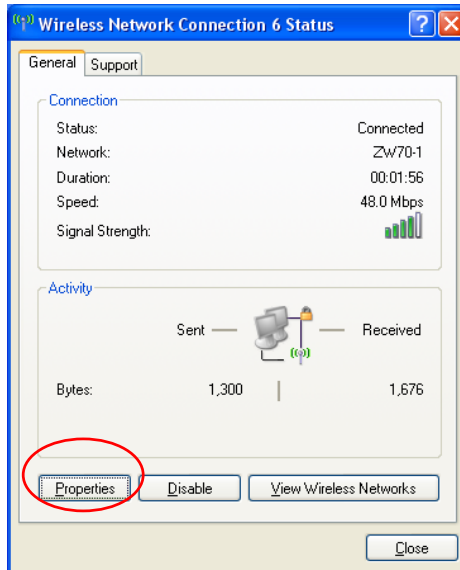**Diagram 6 Windows XP SP1: Wireless Network Connection Status**

Diagram 7 Windows XP SP2: Wireless Network Connection Status

6. Click **Properties** and click the **Wireless Networks** tab.

7. In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is *not* selected. Click **OK**.
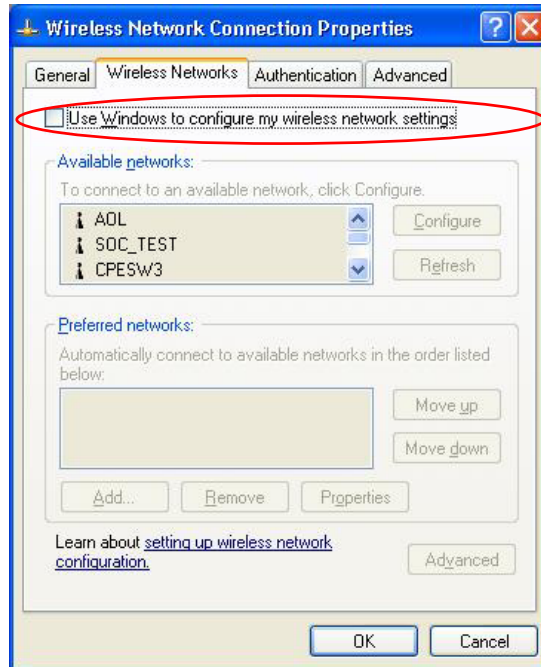

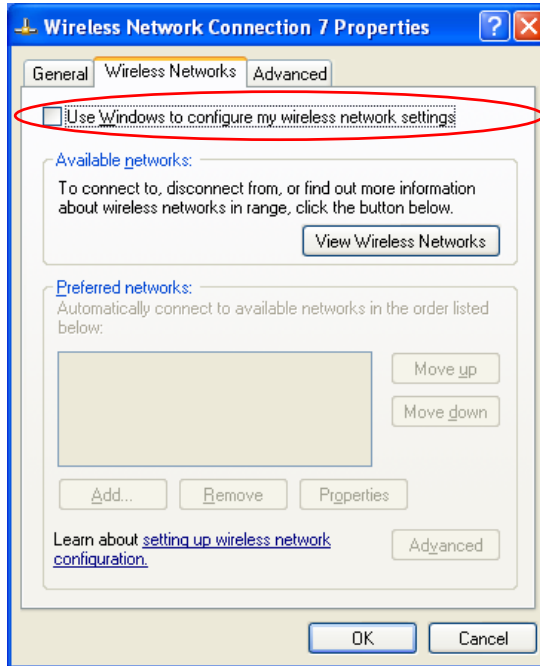**Diagram 8 Windows XP SP1: Wireless Network Connection Properties**

Diagram 9 Windows XP SP2: Wireless Network Connection Properties

Appendix B
Management with Wireless Zero Configuration

This appendix shows you how to manage your G-360 using the Windows XP wireless zero configuration tool.

Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon (🔼) in most screens, move the cursor to the item that you want the information about and click to view the help.

Activating Wireless Zero Configuration

Make sure the **Use Windows to configure my wireless network settings** check box is selected in the **Wireless Network Connection Properties** screen. Refer to *Appendix A*.

If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.
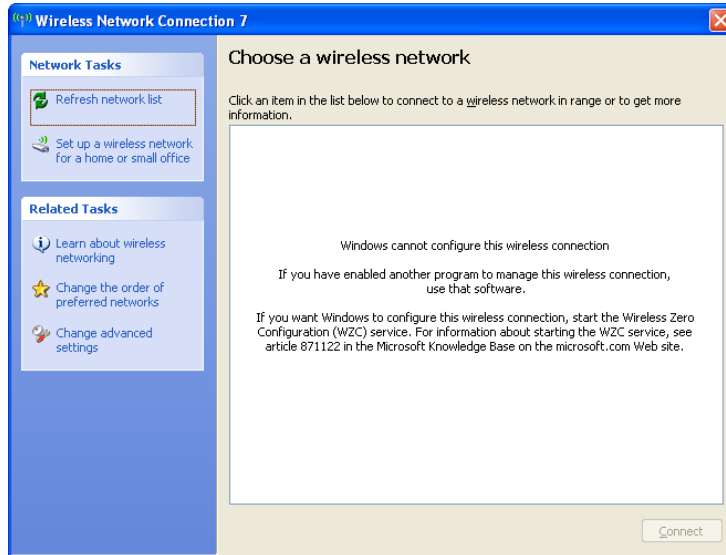

Diagram 10 Windows XP SP2: WZC Not Available

Connecting to a Wireless Network

1. Double-click the network icon for wireless connections in the system tray to open the **Wireless Network Connection Status** screen.

Diagram 11 Windows XP SP2: System Tray Icon

The type of the wireless network icon in Windows XP SP2 indicates the status of the G-360. Refer to the following table for details.

Chart 1 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The G-360 is connected to a wireless network.
	The G-360 is in the process of connecting to a wireless network.
	The connection to a wireless network is limited because the network did not assign a network address to the computer.
	The G-360 is not connected to a wireless network.

2. Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.
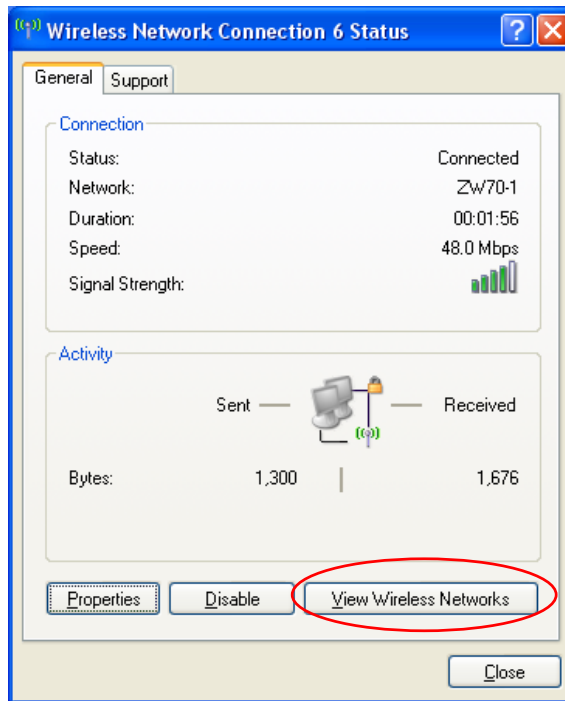
Diagram 12 Windows XP SP2: Wireless Network Connection Status

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.
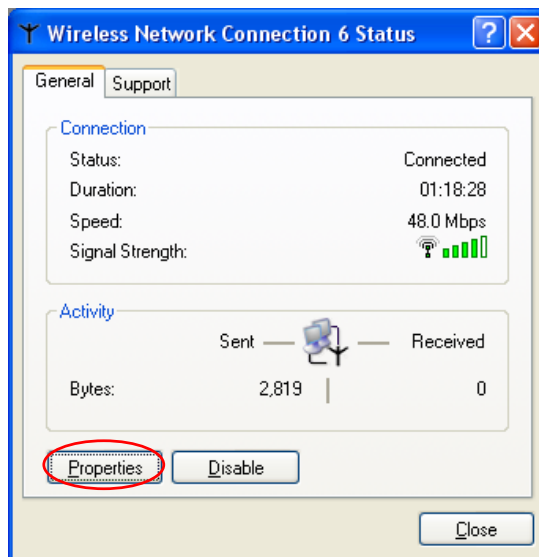
Diagram 13 Windows XP SP1: Wireless Network Connection Status

3. Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.
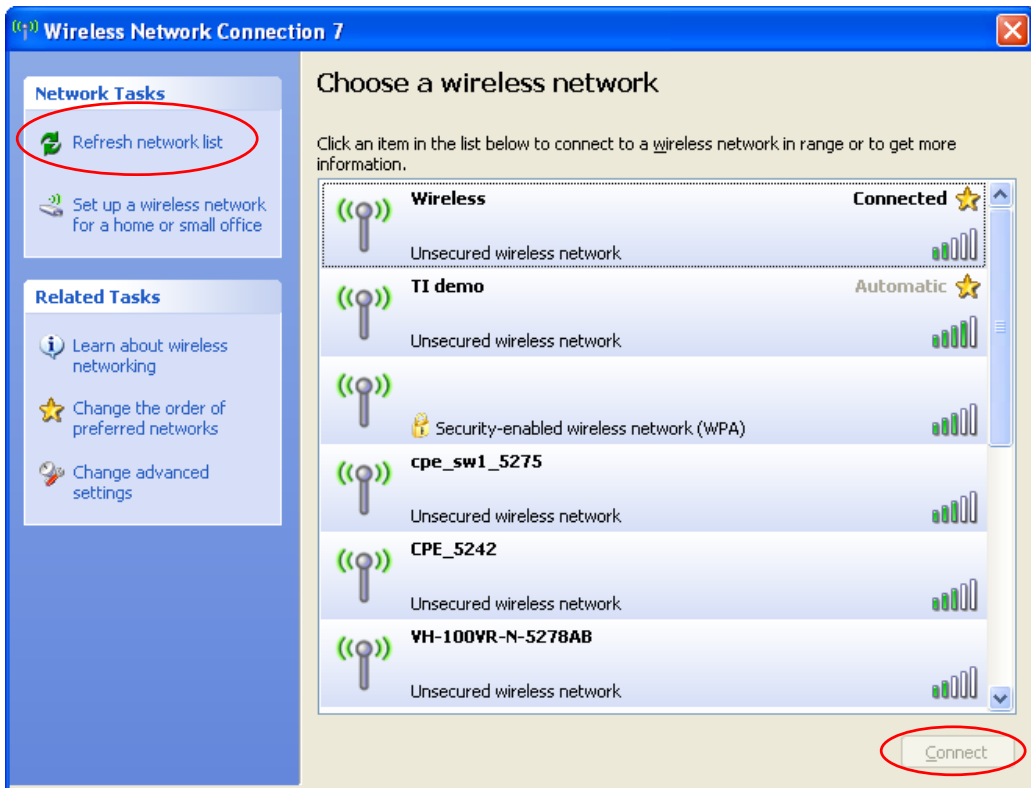
Diagram 14 Windows XP SP2: Wireless Network Connection

The following table describes the icons in the wireless network list.

Chart 2 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
🔒	This denotes that the wireless security is activated for the wireless network.
⭐	This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the G-360 tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks for detailed information.
📶	This denotes the signal strength of the wireless network. Move your cursor to the icon to see details on the signal strength.

Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred networks** table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.
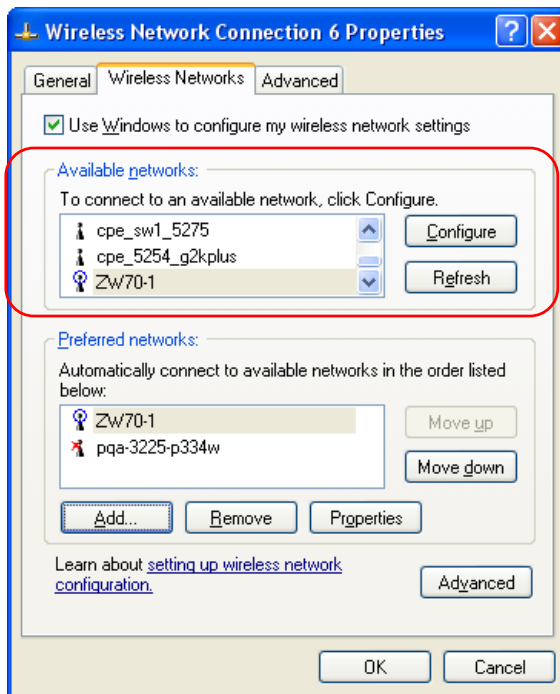

Diagram 15 Windows XP SP1: Wireless Network Connection Properties

4. Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP. Refer to *Section 0* for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption. If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.
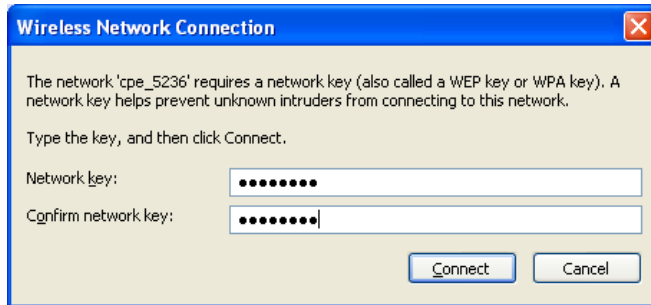
Diagram 16 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

Diagram 17 Windows XP SP2: Wireless Network Connection: No Security

5. Verify that you have successfully connected to the selected network and check connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

Chart 3 Windows XP: Wireless Networks

ICON	DESCRIPTION
🏃	This denotes the wireless network is an available wireless network.
🖳	This denotes the G-360 is associated to the wireless network.
🏃	This denotes the wireless network is not available.

Security Settings

When you configure the G-360 to connect to a secure network but the security settings are not yet enabled on the G-360, you will see different screens according to the authentication and encryption methods used by the selected network.

Association

Select a network in the **Preferred networks** list and click **Properties** to view or configure security.
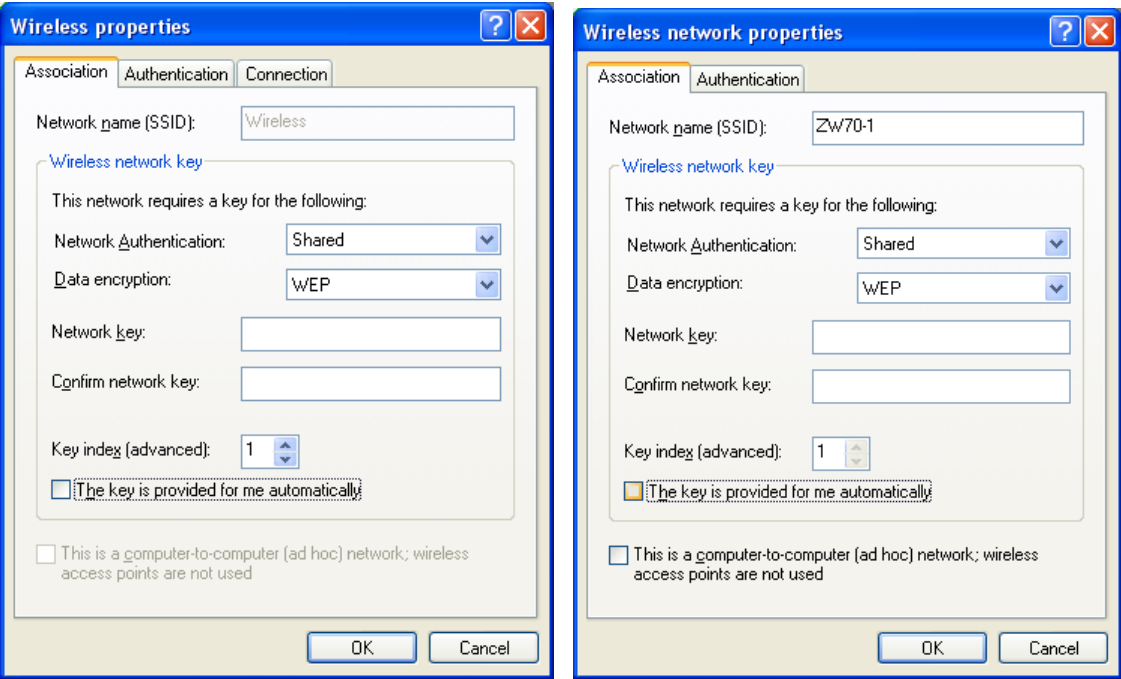

Diagram 18 Windows XP: Wireless (network) properties: Association

The following table describes the labels in this screen.

Chart 4 Windows XP: Wireless (network) properties: Association

LABEL	DESCRIPTION
Network name (SSID)	This field displays the SSID (Service Set IDentifier) of each wireless network.
Network Authentication	This field automatically shows the authentication method (**Share**, **Open**, **WPA** or **WPA-PSK**) used by the selected network. Refer to *Section 2.5* for more information.
Data Encryption	This field automatically shows the encryption type (**TKIP**, **WEP** or **Disable**) used by the selected network.

Chart 4 Windows XP: Wireless (network) properties: Association

LABEL	DESCRIPTION
Network Key	Enter the passphrase, pre-shared key or WEP key.
	The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.
Confirm network key	Enter the key again for confirmation.
Key index (advanced)	Select a default WEP key to use for data encryption.
	This field is available only when the network use **WEP** encryption method and the **The key is provided for me automatically** check box is not selected.
The key is provided for me automatically	If this check box is selected, the wireless AP assigns the G-360 a key.
This is a computer-to-computer (ad hoc) network; wireless access points are not used	If this check box is selected, you are connecting to another computer directly.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Authentication

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.
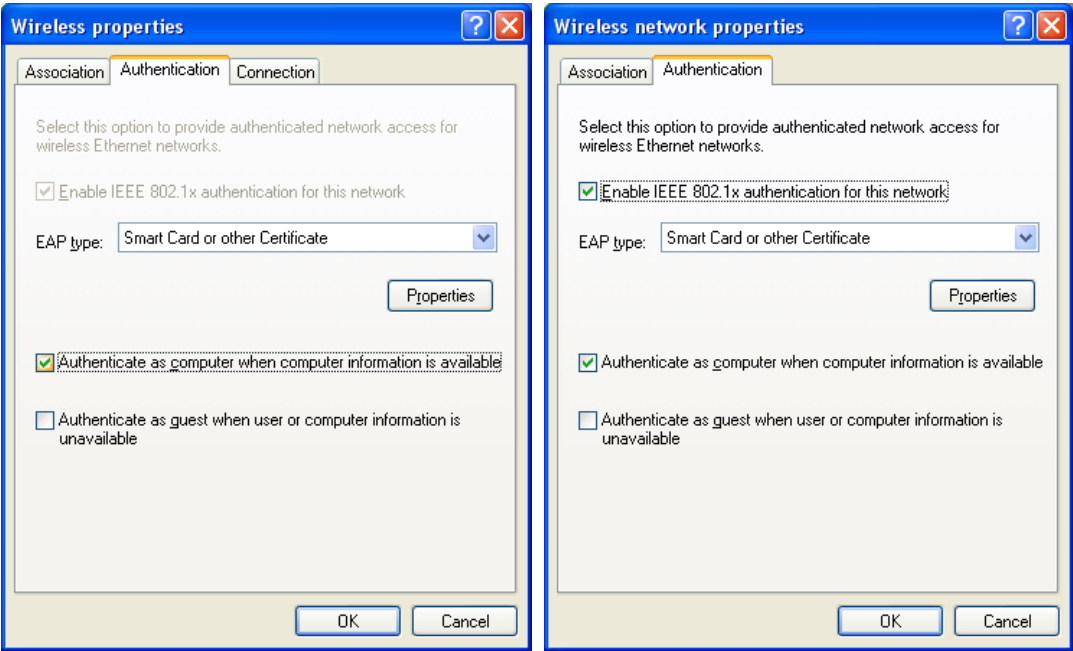
Diagram 19 Windows XP: Wireless (network) properties: Authentication

The following table describes the labels in this screen.

Chart 5 Windows XP: Wireless (network) properties: Authentication

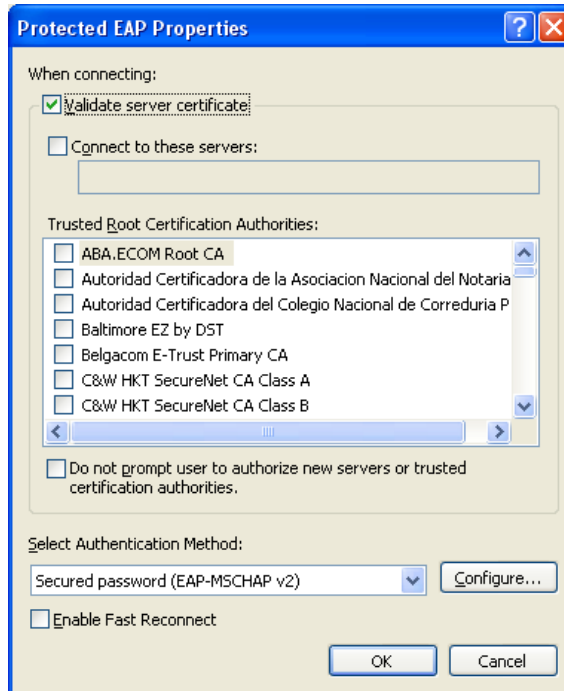| LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication. Options are **Protected EAP (PEAP)** and **Smart Card or other Certificate**.
Properties	Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the **EAP type** field.
Authenticate as computer when computer information is available	Select this check box to have the computer send its information to the network for authentication when a user is not logged on.

Chart 5 Windows XP: Wireless (network) properties: Authentication

LABEL	DESCRIPTION
Authenticate as guest when user or computer information is unavailable	Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to close this screen without saving any changes you may have made.

Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

Protected EAP Properties

Diagram 20 Windows XP: Protcted EAP Properties

The following table describes the labels in this screen.

Chart 6 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. **You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.**
Do not prompt user to authorize new server or trusted certification authorities.	Select this check box to authorize a new authentication server or trusted CA without prompting. This field is available only if you installed the Windows XP server pack 2.
Select Authentication Method:	Select an authentication method from the drop-down list box and click **Configure** to do settings.
Enable Fast Reconnect	Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

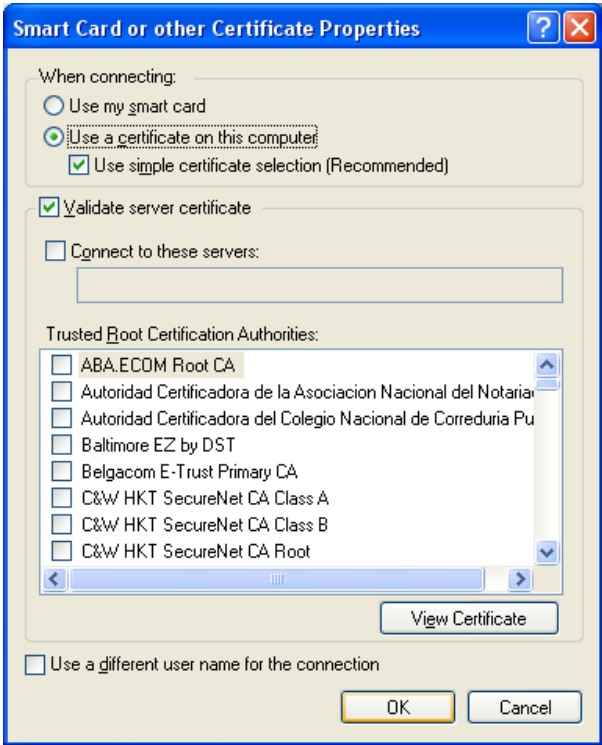*Smart Card or other Certificate Properties*

Diagram 21 Windows XP: Smart Card or other Certificate Properties

The following table describes the labels in this screen.

Chart 7 Windows XP: Smart Card or other Certificate Properties

LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.

Chart 7 Windows XP: Smart Card or other Certificate Properties

LABEL	DESCRIPTION
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. **You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.**
View Certificate	Click this button if you want to verify the selected certificate.
Use a different user name for the connection:	Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Ordering the Preferred Networks

Follow the steps below to manage your preferred networks.

6. Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see *Diagram 14*). The screen displays as shown.
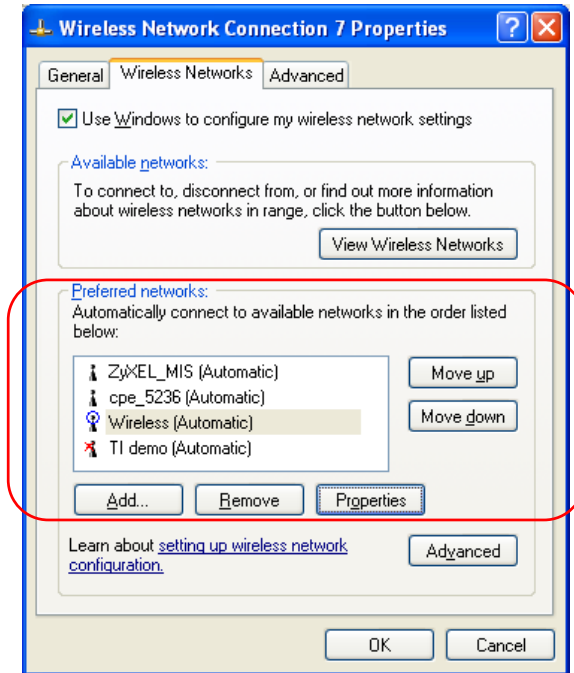
Diagram 22 Windows XP SP2: Wireless Networks: Preferred Networks

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.
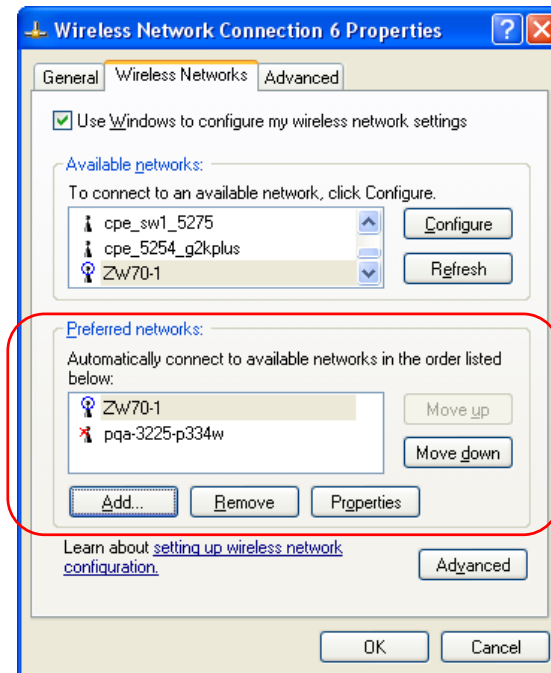
Diagram 23 Windows XP SP1: Wireless Networks: Preferred Networks

7. Whenever the G-360 tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change it's order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

Appendix C
Product Specifications

PHYSICAL SPECIFICATIONS	
Product Name	ZyXEL G-360 802.11g Wireless PCI Adapter
Type	3.3V 32-bit PCI V2.2
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	2.412-2.483GHz
Operating Channels	IEEE 802.11b: 11 Channels (North America) IEEE 802.11g: 11 Channels (North America) IEEE 802.11b: 13 Channels (Europe) IEEE 802.11g: 13 Channels (Europe)
Data Rate	IEEE 802.11b: 22* (B+ proprietary), 11, 5.5, 2, 1Mbps IEEE 802.11g: 125* (G+ proprietary), 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK) IEEE 802311b: PBCC, Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).
Security	64/128/256-bit WEP, WPA, WPA-PSK, 802.1x
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 65 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power Consumption	IEEE 802.11g: TX: 600mA RX: 450mA (max.) IEEE 802.11b: TX: 600mA RX: 450mA (max.)
Voltage	3.3V±5%

Weight	105 g
Dimension	120mm(L) x 13mm(H) x 84mm(W)

RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Frequency	2.4 ~ 2.483GHz (Industrial Scientific Medical Band)
Channels	1~11 Channels (USA, Canada) 1~13 Channels (Europe)
Data Rate	802.11g (OFDM): 6, 9, 12, 18, 24, 36, 48, 54, 125 Mbps 802.11b: 1, 2, 5.5, 11, 22 Mbps
Modulation	802.11g: OFDM with BPSK, QPSK and 16/64-QAM sub-carrier modulations 802.11b: PBCC, DSSS (DBPSK, DQPSK, CCK)
Output Power	17 dBm (typical) at 11Mbps DBPSK, DQPSK, CCK 14 dBm (typical) at 54Mbps OFDM
RX Sensitivity	802.11g (OFDM): 54 Mbps: < -68 dBm (typ.) < -69 dBM (max.) 802.11b (PBCC): 22 Mbps: < -83 dBm (typ.) < -88 dBM (max.)

SOFTWARE SPECIFICATIONS	
Device Drivers	Microsoft Windows 98(SE), Windows 2000, Windows XP, Windows ME
Roaming	802.11b/g compliant
WEP	Supports 64-bit, 128-bit and 256-bit encryption

ENVIRONMENTAL SPECIFICATIONS	
Temperature	Operating: 0° ~ 50° C Storage: -30° ~ 65° C
Relative Humidity	20% to 95% (non-condensing)

Appendix D
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of five authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

Appendix E
Index

Z