ZyXEL G-220 v2

802.11g Wireless USB Adapter

User's Guide

Version 1.00
1/2006
Edition 1

ZyXEL

Copyright

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 patent 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

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

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

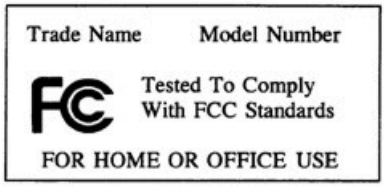
1. The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Certifications

1 Go to www.zyxel.com.

2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.



注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). 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 your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

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

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (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
CZECH REPUBLIC	info@cz.zyxel.com info@cz.zyxel.com	+420-241-091-350 +420-241-091-359	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
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 2860 Soeborg Denmark
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
FRANCE	info@zyxel.fr	+33-4-72-52-97-97 +33-4-72-52-19-20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
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
HUNGARY	support@zyxel.hu info@zyxel.hu	+36-1-3361649 +36-1-3259100	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
KAZAKHSTAN	http://zyxel.kz/support sales@zyxel.kz	+7-3272-590-698 +7-3272-590-689	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
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.
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

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
POLAND	info@pl.zyxel.com	+48-22-5286603 +48-22-5206701	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
RUSSIA	http://zyxel.ru/support sales@zyxel.ru	+7-095-542-89-29 +7-095-542-89-25	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
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
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
UKRAINE	support@ua.zyxel.com sales@ua.zyxel.com	+380-44-247-69-78 +380-44-494-49-32	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
UNITED KINGDOM	support@zyxel.co.uk sales@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only) +44-1344 303034	www.zyxel.co.uk ftp.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyXEL G-220 v2 802.11g Wireless USB Adapter.

Your ZyXEL G-220 v2 is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL G-220 v2 for its various applications.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. They contain hardware installation/connection information.

- ZyXEL Glossary and Web Site

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

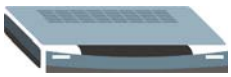
User Guide Feedback

Help us help you. E-mail all User 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.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choice.
- Mouse action sequences are denoted using a comma. For example, "In Windows, click **Start**, **Settings** and then **Control Panel**" means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The ZyXEL G-220 v2 802.11g Wireless USB Adapter may be referred to as the ZyXEL G-220 v2 in this user's guide.

Graphics Icons Key

Wireless Access Point 	Computer 	Notebook Computer 
Server 	Modem 	Wireless Signal 
Telephone 	Switch 	Router 
Internet Cloud 		

CHAPTER 1
Getting Started

This chapter introduces the ZyXEL G-220 v2 and prepares you to use the ZyXEL Utility.

1.1 About Your ZyXEL G-220 v2

The ZyXEL G-220 v2 is an IEEE 802.11g compliant wireless LAN adapter.

The following lists the main features of your ZyXEL G-220 v2. See the product specifications in the appendix for detailed features.

- Automatic rate selection.
- Security: WEP (Wired Equivalent Privacy), IEEE 802.1x, WPA-PSK, WPA (Wi-Fi Protected Access), WPA2-PSK and WPA2
- Proprietary SoftAP feature turns your ZyXEL G-220 v2 into an access point (AP).
- A built-in antenna
- Driver and utility support for Windows 98 Second Edition, Windows ME, Windows 2000 and Windows XP.

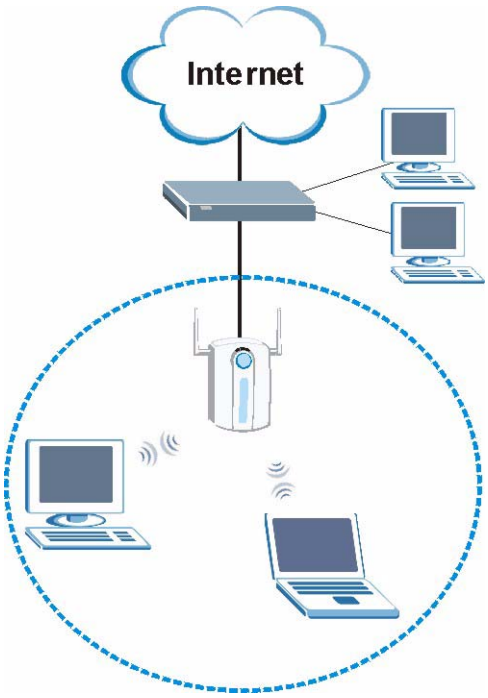
1.1.1 Application Overview

This section describes some network applications for the ZyXEL G-220 v2.

1.1.1.1 Infrastructure

To connect to a network via an Access Point (AP), set the ZyXEL G-220 v2 network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

Figure 1 Application: Infrastructure

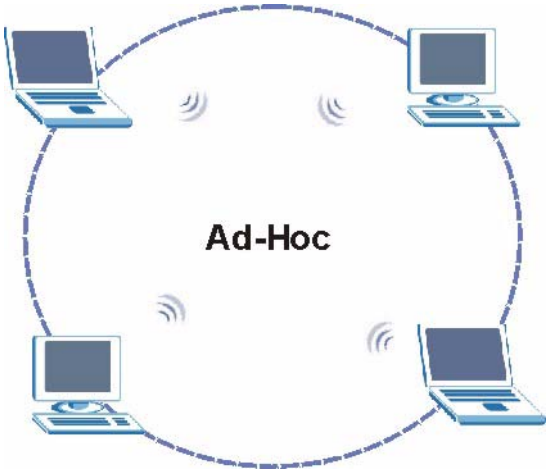


1.1.1.2 Ad-Hoc

In case you prefer to set up a small independent wireless workgroup without an AP, use the Ad-Hoc mode.

Ad-hoc mode does not require an AP or a wired network. Two or more wireless clients communicate directly to each other.

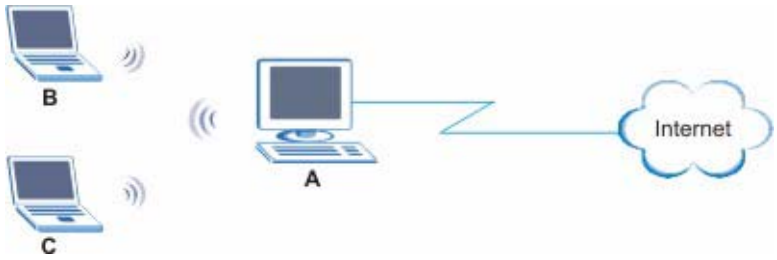
Figure 2 Application: Ad-Hoc



1.1.1.3 Access Point Mode

You can set the ZyXEL G-220 v2 in access point mode. The following figure shows a network example.

Figure 3 Application: Access Point Mode



In the example, the ZyXEL G-220 v2 is installed on computer **A** and set to operate in access point mode. Computer **A** shares Internet connection to the wireless LAN, so wireless stations **B** and **C** can access the Internet.

1.2 ZyXEL G-220 v2 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 ZyXEL G-220 v2, use one of the following applications:

- Wireless Zero Configuration (WZC) (recommended for Windows XP)
- ZyXEL Utility (required when you want to use the ZyXEL G-220 v2 as an access point)
- Odyssey Client Manager (not supplied)

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

Refer to the Odyssey Client Manager documentation for more information.

1.4 Windows XP Users Only

Note: When you use the ZyXEL Utility, it automatically disables the Windows XP wireless configuration tool.

Refer to the appendices on how to use WZC to manage the ZyXEL G-220 v2.

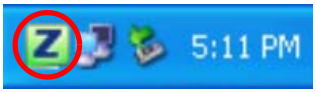
1.5 Accessing the ZyXEL Utility

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

Note: When the ZyXEL Utility system tray icon displays, the ZyXEL G-220 v2 is installed properly.

When you use the ZyXEL Utility, it automatically disables the Windows XP wireless configuration tool.

Figure 4 ZyXEL Utility: System Tray Icon



The color of the ZyXEL Utility system tray icon indicates the status of the ZyXEL G-220 v2. Refer to the following table for details.

Table 1 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The ZyXEL G-220 v2 is operating in wireless station mode but is not connected to a wireless network.
Green	The ZyXEL G-220 v2 is operating in wireless station mode and connected to a wireless network.
Pale Blue	The ZyXEL G-220 v2 is operating in access point mode.

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 Microsoft Windows versions. Screens for Windows XP are shown.

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

1.6 Connecting to a Wireless LAN

This section shows you how to associate with a network using the ZyXEL Utility. You can either manually connect to a network or configure a profile to have the ZyXEL G-220 v2 automatically connect to a specific network. Otherwise, configure nothing and leave the ZyXEL G-220 v2 to automatically scan for and connect to any other available network without security.

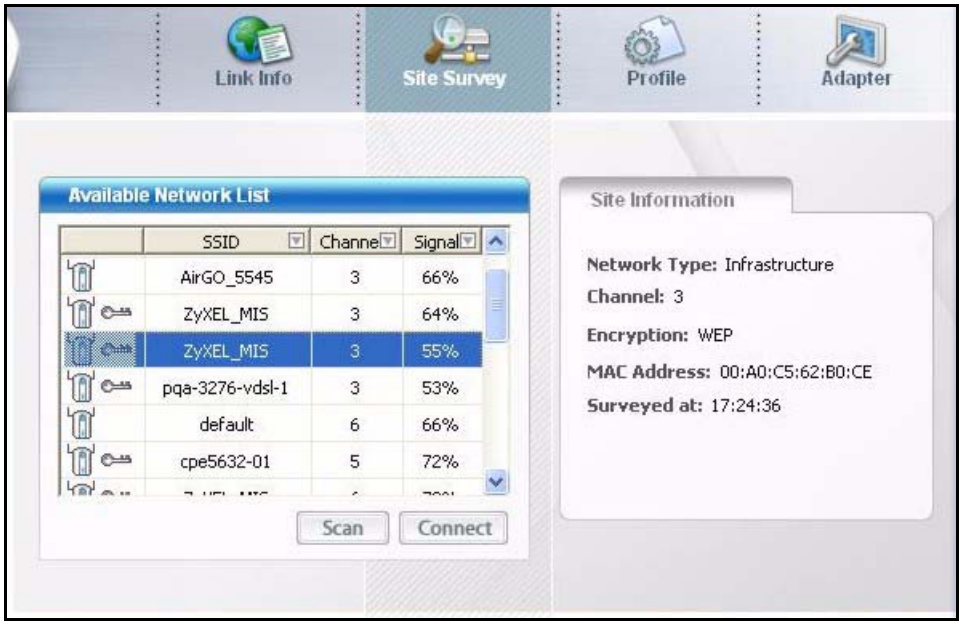
See the next chapters for detailed field descriptions.

1.6.1 Site Survey

After you install the ZyXEL Utility and then insert the ZyXEL G-220 v2, follow the steps below to connect to a network using the **Site Survey** screen.

1. Make sure a wireless network is available and within range.
2. Open the ZyXEL Utility and click the **Site Survey** tab to open the screen as shown next.
3. Click **Scan** to search for available wireless networks.

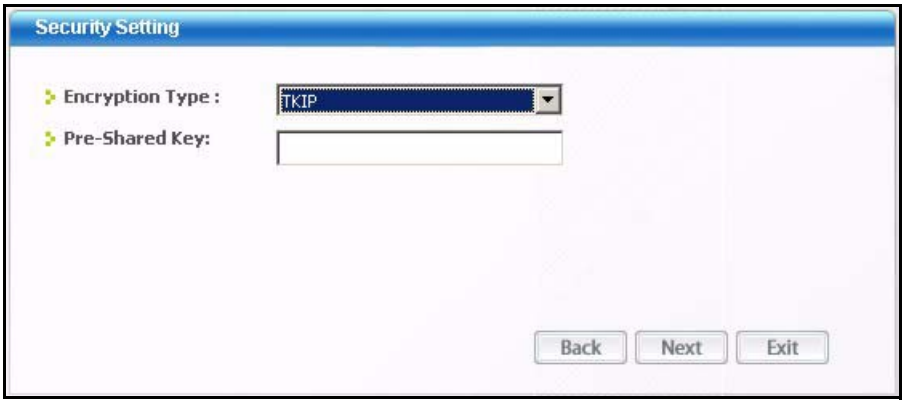
Figure 5 ZyXEL Utility: Site Survey



4. To join a network, either click an SSID in the table and then click **Connect** or double-click an SSID.
5. If the wireless security is activated for the selected wireless network, the **Security Setting** screen displays. This screen varies according to the network's encryption method. Configure the same security settings as the associated network.

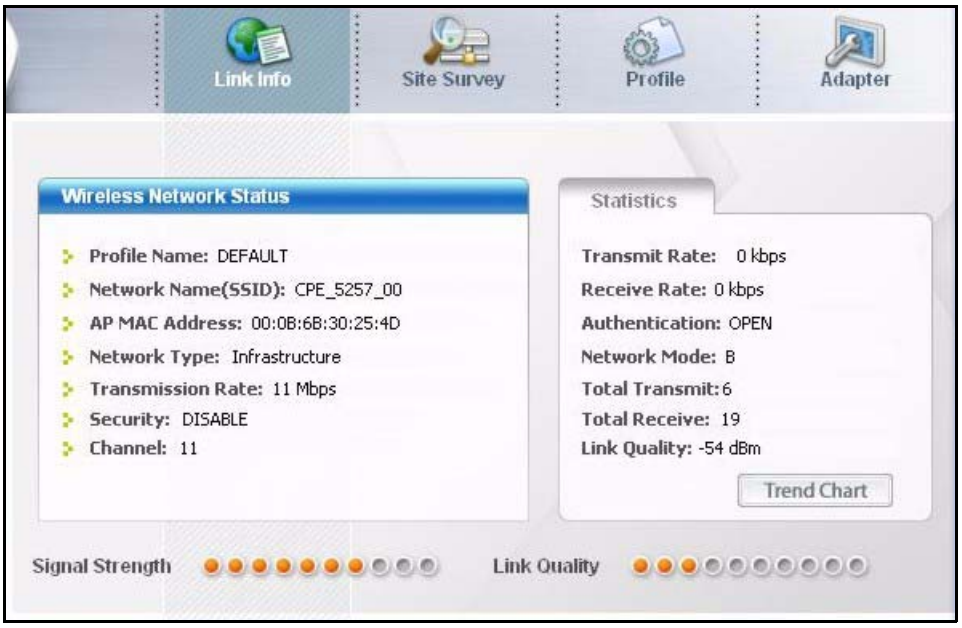
Note: If the selected network is unavailable or the security settings are not correct, the ZyXEL G-220 v2 cannot connect to a network.

Figure 6 ZyXEL Utility: Security Setting



6 Verify that you have successfully connected to the selected network and check the network information in the **Link Info** screen. If the ZyXEL G-220 v2 is not connected to a network, the fields in this screen are blank.

Figure 7 ZyXEL Utility: Link Info



1.7 ZyXEL G-220 v2 Modes

You can set your ZyXEL G-220 v2 to operate in either wireless station or access point (AP) modes.

In wireless station mode, your ZyXEL G-220 v2 must connect to a peer wireless station or an AP to take part in your wireless network.

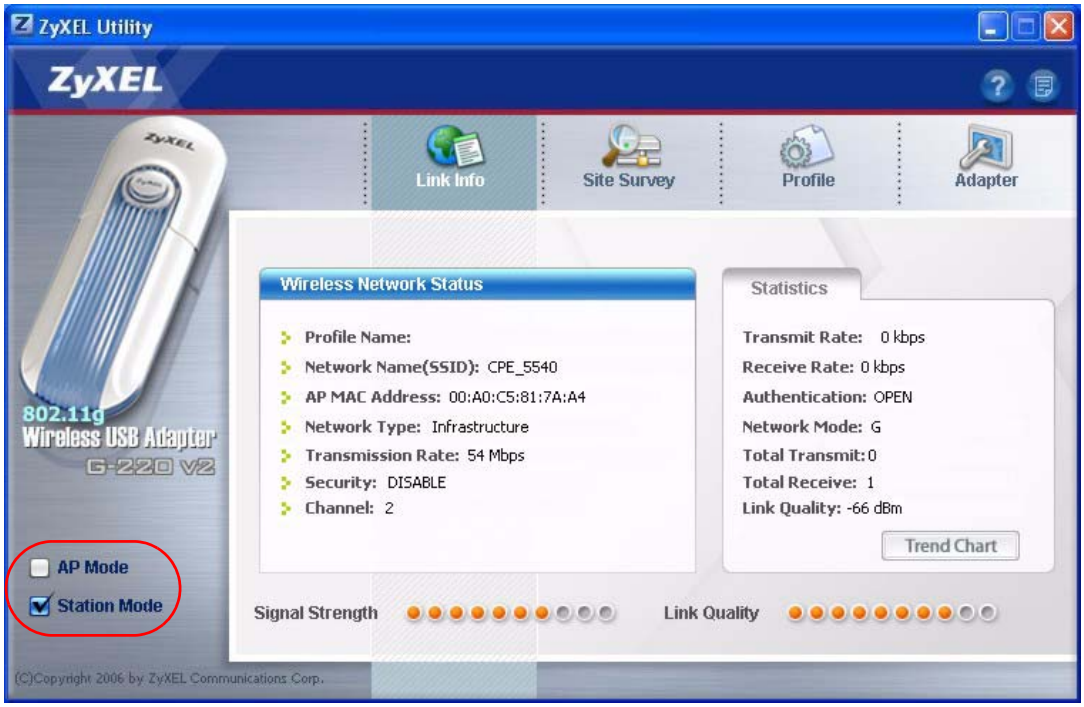
In access point mode, your ZyXEL G-220 v2 functions as an access point. This allows you to set up your wireless network without using a dedicated AP device. Up to 16 wireless stations can associate to the ZyXEL G-220 v2 to form a wireless network. Refer to Section 1.7.1 on page 25 and Chapter 4 on page 53 for more information.

Note: With WZC, you cannot use the ZyXEL G-220 v2 as an access point.

1.7.1 Change ZyXEL G-220 v2 Mode

To change between the modes, select either the **Station Mode** or **AP Mode** option in any ZyXEL Utility screens.

Figure 8 ZyXEL Utility: Change Modes



Note: Wait for about five seconds for the ZyXEL Utility to complete the mode change.

The current mode is indicated by the color of the radio button.

1.8 ZyXEL Utility Screen Summary

This sections describes the ZyXEL Utility screens.

Figure 9 Menu Summary: Station Mode

Figure 10 Menu Summary: AP Mode

The following table describes the menus.

Table 2 ZyXEL Utility: Menu Screen Summary

TAB	DESCRIPTION
Station Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Site Survey	Use this screen to • scan for a wireless network • configure wireless security (if activated on the selected network). • connect to a wireless network.
Profile	Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings.
Adaptor	Use this screen to configure a transfer rate, enable power saving and use OTIST (One-Touch Intelligent Security Technology).
AP Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Configuration	Use this screen to configure wireless LAN settings.
MAC Filter	Use this screen to configure which computer(s) you want access to the wireless LAN through the ZyXEL G-220 v2.

CHAPTER 2
Wireless LAN Network

This chapter provides background information on wireless LAN network.

2.1 Wireless LAN 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 (Tx Rate)

The ZyXEL G-220 v2 provides various transmission (data) rate options for you to select. Options include **Fully Auto**, **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **6 Mbps**, **9 Mbps**, **11 Mbps**, **12 Mbps**, **18 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps** and **54 Mbps**. In most networking scenarios, the factory default **Fully Auto** setting proves the most efficient. This setting allows your ZyXEL G-220 v2 to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the ZyXEL G-220 v2 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 ZyXEL G-220 v2 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.

Note: With USB1.0/1.1, the ZyXEL G-220 v2 can only transmit at up to 11Mbps.

2.2 Wireless LAN Security Overview

Wireless LAN security is vital to your network to protect wireless communications.

Configure the wireless LAN security using the **Configuration** or the **Profile Security Setting** screen. If you do not enable any wireless security on your ZyXEL G-220 v2, the ZyXEL G-220 v2'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 ZyXEL G-220 v2 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 ZyXEL G-220 v2.

- 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 automatically generated WEP keys from the **Security Setting** 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 ZyXEL G-220 v2 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.

2.2.2.1 EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x 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 IEEE 802.1x. The ZyXEL G-220 v2 supports EAP-TLS and EAP-PEAP. Refer to Appendix E on page 89 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(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

2.2.3.1 Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP).

2.2.3.2 User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

2.2.4 WPA(2)-PSK Application Example

A WPA(2)s-PSK application looks as follows.

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 or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP and wireless clients use the pre-shared key to generate a common PMK.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

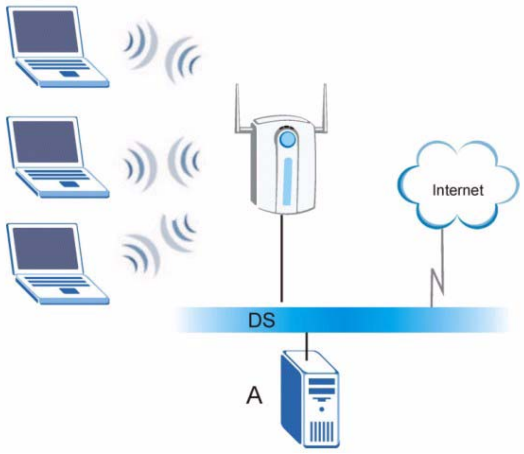
Figure 11 WPA-PSK Authentication

2.2.5 WPA(2) 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(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
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 12 WPA(2) with RADIUS Application Example



2.3 Encryption Type

The IEEE 802.11b/g standard describes a simple encryption method between the wireless stations and AP. Three encryption types are defined: **Auto**, **Open System** and **Shared Key**.

- **Open System** 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.
- **Shared Key** 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.
- **Auto** authentication mode allows the ZyXEL G-220 v2 to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

2.4 Preamble Type

Preamble is used to signal that data is coming to the receiver.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Auto** to have the ZyXEL G-220 v2 automatically use short preamble when all access point/wireless stations support it, otherwise the ZyXEL G-220 v2 uses long preamble.

Note: The ZyXEL G-220 v2 and the access point/wireless stations MUST use the same preamble mode in order to communicate.

2.5 Introduction to OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as "AP" here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

2.5.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

We use the Prestige 334WT in this guide as an example. Screens may vary slightly for your ZyXEL devices.

Note: The AP and wireless client(s) MUST use the same **Setup key**.

2.5.1.1 AP

On the Prestige 334WT, you can enable OTIST using the **Reset** button or the web configurator. If you use the **Reset** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

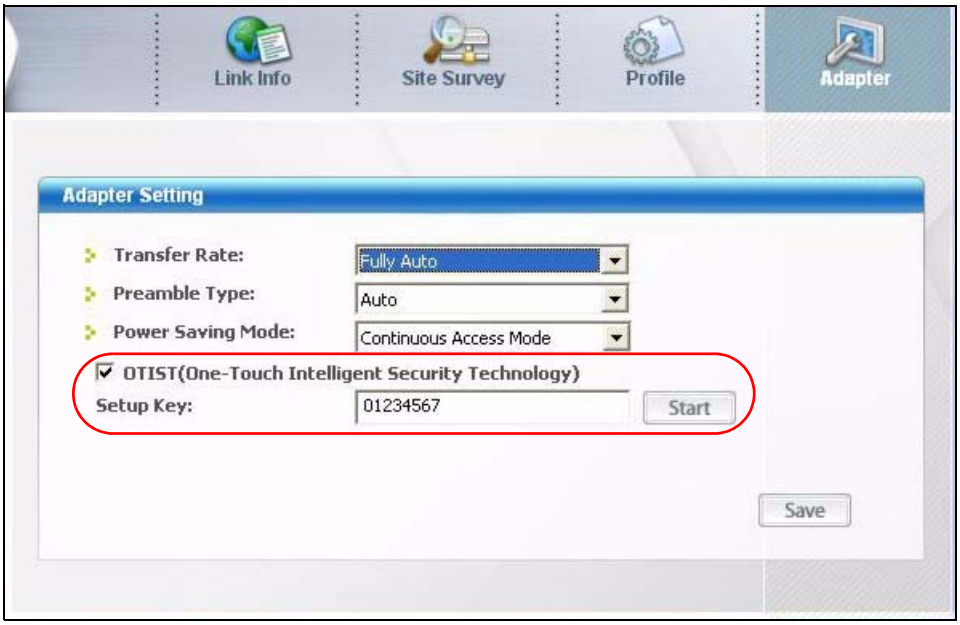
Hold in the **Reset** button for one or two seconds.

Note: If you hold in the **Reset** button too long, the device will reset to the factory defaults!

In the web configurator, go to the **Wireless LAN** main screen and then select **OTIST**. To change the **Setup key**, enter zero to eight printable characters. To have OTIST automatically generate a WPA-PSK key, select the **Yes** check box. If you manually configured a WEP key or a WPA-PSK key and you also selected this check box, then the key you manually configured is used.

2.5.1.2 Wireless Client

Start the ZyXEL Utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP's and click **Save**.



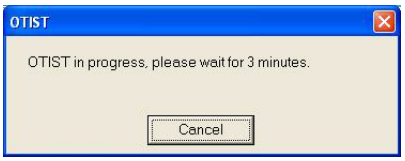
2.5.2 Starting OTIST

Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

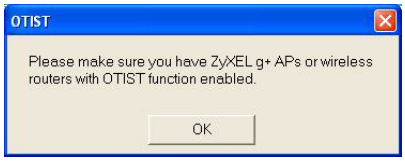
See the user's guide for more information.

1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.

2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.



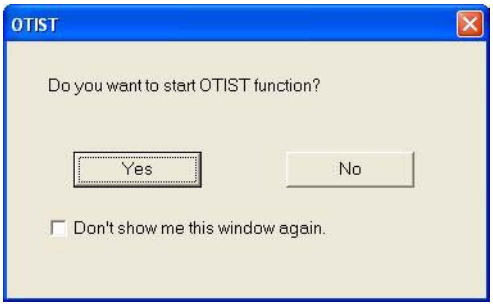
- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.



- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

2.5.3 Notes on OTIST

1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.



2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **Reset** button (for one or two seconds) for the AP to transfer settings.

4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).

5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL the wireless clients again.

CHAPTER 3
Wireless Station Mode Configuration

This chapter shows you how to configure your ZyXEL G-220 v2 in wireless station mode.

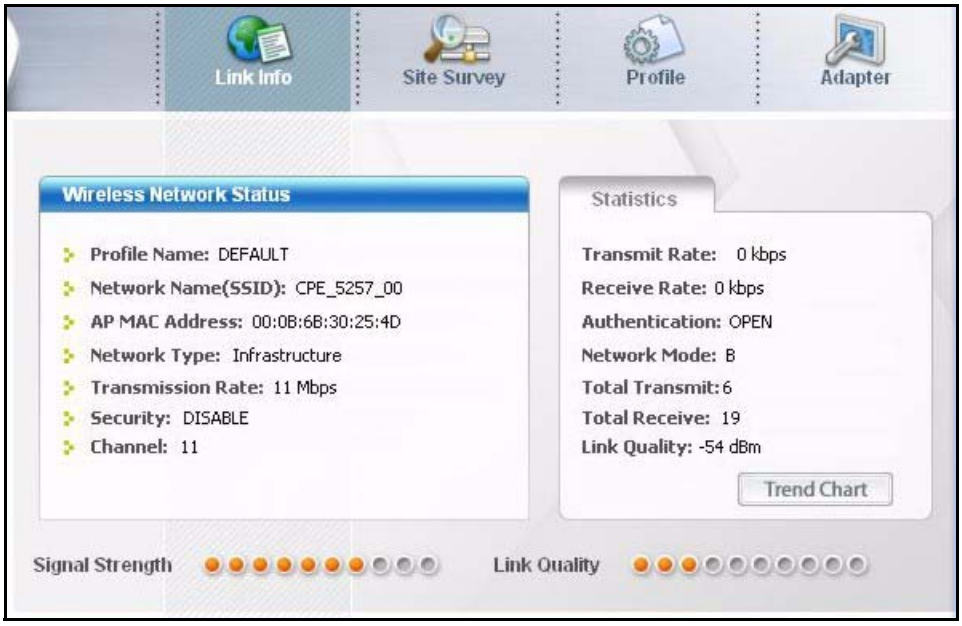
3.1 Wireless Station Mode Overview

To set your ZyXEL G-220 v2 in wireless station mode, refer to Section 1.7.1 on page 25.

3.2 The Link Info Screen

When the ZyXEL Utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your ZyXEL G-220 v2.

Figure 13 Station Mode: Link Info



The following table describes the labels in this screen.

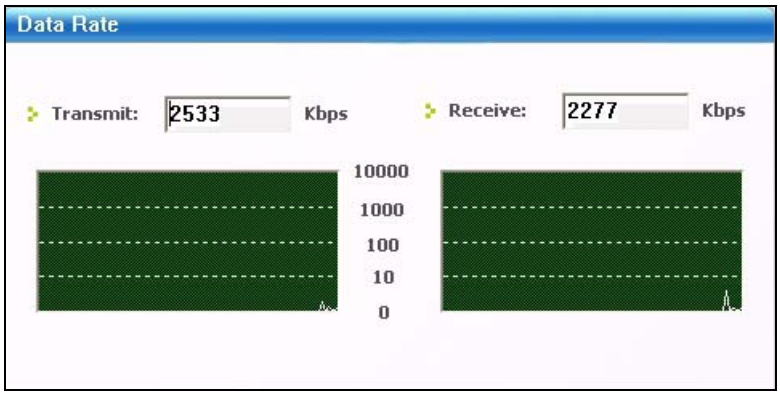
Table 3 Station Mode: Link Info

LABEL	DESCRIPTION
AP Mode Station Mode	Use the radio button to set the ZyXEL G-220 v2 to operate in wireless station or access point mode. Refer to Section 1.7.1 on page 25 for more information.
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 ZyXEL G-220 v2 is associated.
AP MAC Address	This field displays the MAC address of the wireless device to which the ZyXEL G-220 v2 is associated.
Network Type	This field displays the network type (**Infrastructure(BSS)** or **Ad Hoc**) of the wireless network.
Transmission Rate	This field displays the current transmission rate of the ZyXEL G-220 v2 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP** (WEP or 802.1x), **TKIP** (WPA/WPA-PSK/WPA2/WPA2-PSK), **AES** (WPA/WPA-PSK/WPA2/WPA2-PSK)) or inactive (**DISABLE**).
Channel	This field displays the radio channel the ZyXEL G-220 v2 is currently using.
Status	This field displays the authentication type of the wireless network.
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 ZyXEL G-220 v2.
Wireless Mode	This field displays the wireless standard (**B** or **G**) of the wireless device.
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 ZyXEL G-220 v2.
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.

3.2.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to display a screen as shown below. Use this screen to view real-time data traffic statistics.

Figure 14 Station Mode: Link Info: Trend Chart



The following table describes the labels in this screen.

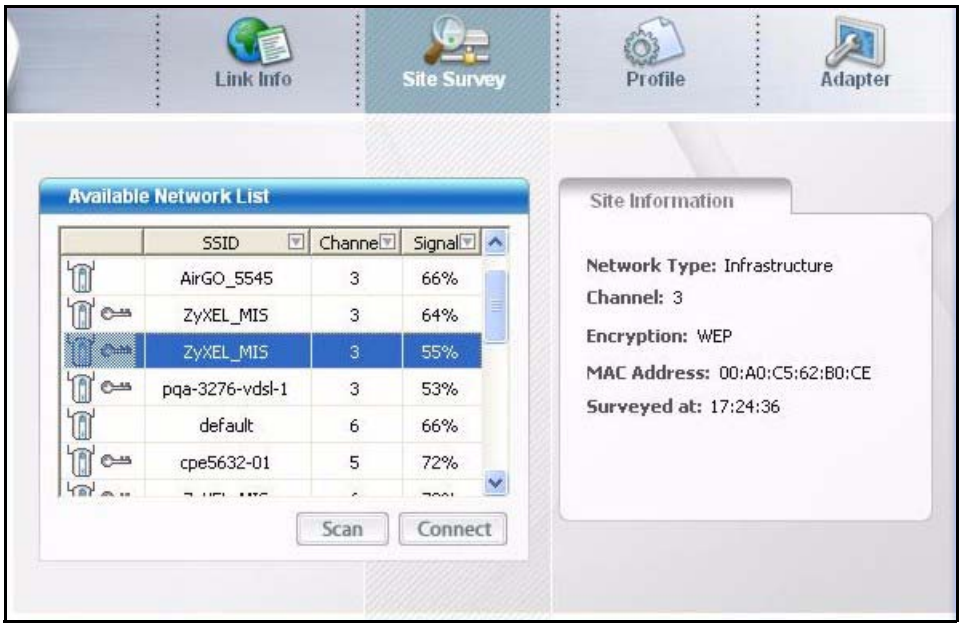
Table 4 Station Mode: Link Info: Trend Chart

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).

3.3 The Site Survey Screen

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

Figure 15 Station Mode: Site Survey



The following table describes the labels in this screen.

Table 5 Station Mode: Site Survey

LABEL	DESCRIPTION
Available Network List	Click a column heading to sort the entries.
	 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** (WEP or 802.1x), **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**) 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.

3.3.1 Connecting to a WLAN Network

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

1. Click **Scan** to search for all available wireless networks within range.
2. To join a network, click an entry in the table to select a wireless network and then click **Connect** or double-click an entry.
3. If the wireless security is activated for the selected wireless network, the **Security Setting** screen displays. You must set the related fields in the **Security Setting** screen to the same security settings as the associated wireless device. Refer to Section 3.3.2 on page 39 for more information.

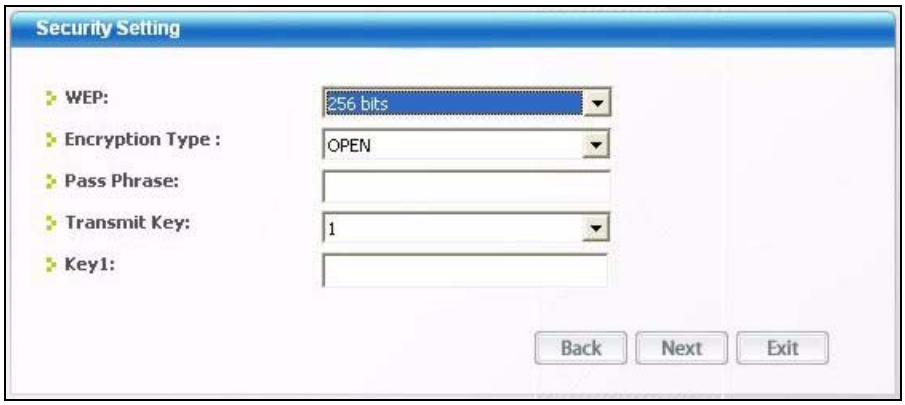
   Otherwise click the **Exit** button and connect to another wireless network without data encryption.
4. Verify that you have successfully connected to the selected network and check the network information in the **Link Info** screen.

3.3.2 Security Settings

When you configure the ZyXEL G-220 v2 to connect to a network with wireless security activated and the security settings are disabled on the ZyXEL G-220 v2, the screen varies according to the encryption method used by the selected network.

3.3.2.1 WEP Encryption

Figure 16 Station Mode: Security Settings: WEP



The following table describes the labels in this screen.

Table 6 Station Mode: Security Settings: WEP

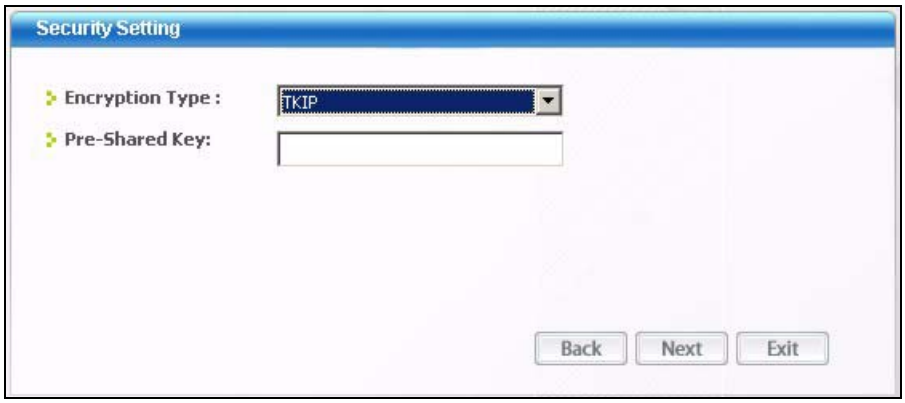
LABEL	DESCRIPTION
Security Settings	
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields. Select **Disable** to deactivate WEP encryption.
Encryption Type	Select an encryption type. Choices are **SHARED** and **OPEN**. Refer to Section 2.3 on page 31 for more information.
Pass Phrase	Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the ZyXEL G-220 v2 automatically generates four different WEP keys and displays it in the key field below. Refer to Section 2.2.1 on page 28 for more information. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.

Table 6 Station Mode: Security Settings: WEP (continued)

LABEL	DESCRIPTION
Key x (where x is a number between 1 and 4)	Select this option if you want to manually enter 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, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey11112222333334444555566 78) for ASCII key type. **Note:** 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.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen. Refer to Section 3.3.3 on page 43.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

3.3.2.2 WPA-PSK/WPA2-PSK

Figure 17 Station Mode: Security Settings: WPA-PSK/WPA2-PSK



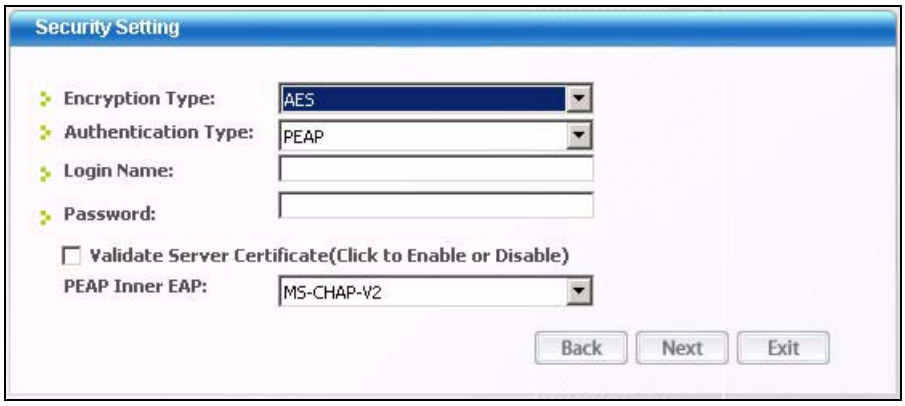
The following table describes the labels in this screen.

Table 7 Station Mode: Security Settings: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 2.2.3 on page 29 for more information.
Pre-Shared Key	Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen. Refer to Section 3.3.3 on page 43.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

3.3.2.3 WPA/WPA2

Figure 18 Station Mode: Security Settings: WPA/WPA2



The following table describes the labels in this screen.

Table 8 Station Mode: Security Settings: WPA/WPA2

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 2.2.3 on page 29 for more information.
Authentication Type	Select an authentication method from the drop down list. Options are **TLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.

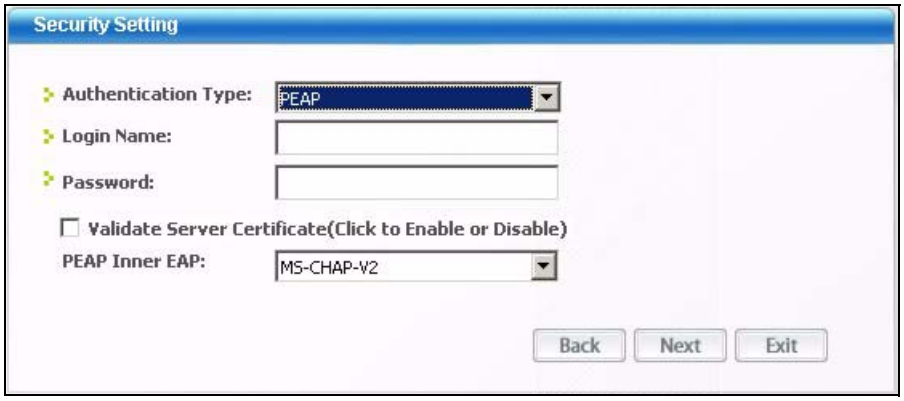
Table 8 Station Mode: Security Settings: WPA/WPA2

LABEL	DESCRIPTION
Password	This field is not available when you select **TLS** in the **Authentication Type** field. Enter the password associated with the user name above.
Certificate	This field is only available when you select **TLS** in the **Authentication Type** field. Select a certificate from the drop-down list box. **Note:** 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.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. The PEAP protocol is **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen. Refer to Section 3.3.3 on page 43.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

3.3.2.4 IEEE 802.1x

Configure IEEE 802.1x security with various authentication methods in this screen.

Figure 19 Station Mode: Security Settings: 802.1x



The following table describes the labels in this screen.

Table 9 Station Mode: Security Settings: 802.1x

LABEL	DESCRIPTION
Authentication Type	Select an authentication method from the drop down list. Options are **TLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.

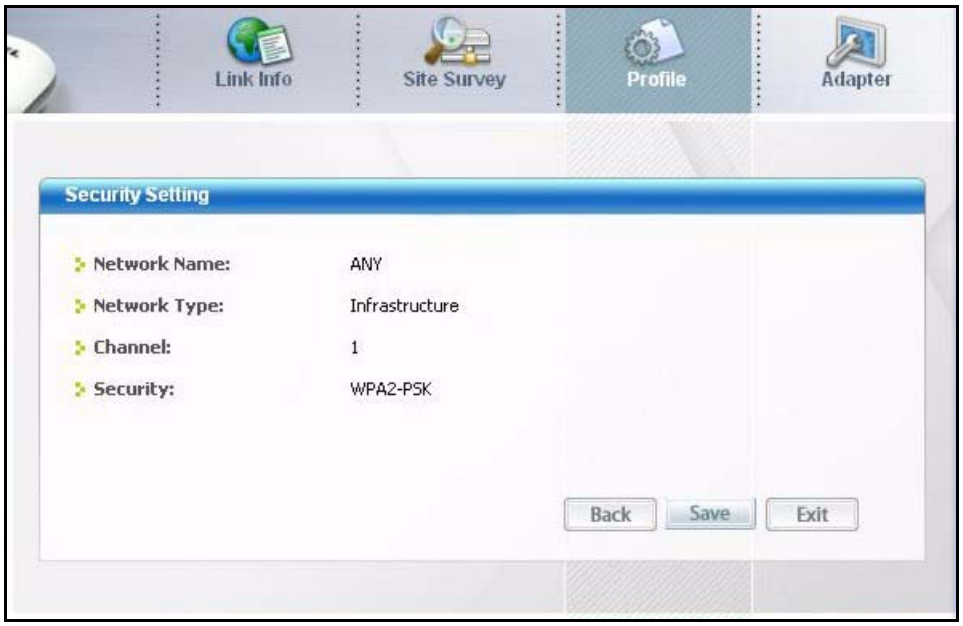
Table 9 Station Mode: Security Settings: 802.1x

LABEL	DESCRIPTION
Password	This field is not available when you select **TLS** in the **Authentication Type** field. Enter the password associated with the user name above.
Certificate	This field is only available when you select **TLS** in the **Authentication Type** field. Select a certificate from the drop-down list box. **Note:** 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.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. The PEAP protocol is **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen. Refer to Section 3.3.3 on page 43.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

3.3.3 Confirm Save Screen

Use the **Confirm Save** screen to confirm and save the security settings.

Figure 20 Confirm Save Screen



The following table describes the labels in this screen.

Table 10 Confirm Save Screen

LABEL	DESCRIPTION
Security Setting	
Network Name	This field displays the **SSID** previously entered.
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 the profile.
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x**) or inactive (**Disabled**).
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save the changes back to the ZyXEL G-220 v2 and display the **Link Info** screen.
Exit	Click **Exit** to discard changes and return to the **Site Survey** screen.

3.4 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the ZyXEL G-220 v2, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the ZyXEL G-220 v2 cannot connect to a network.

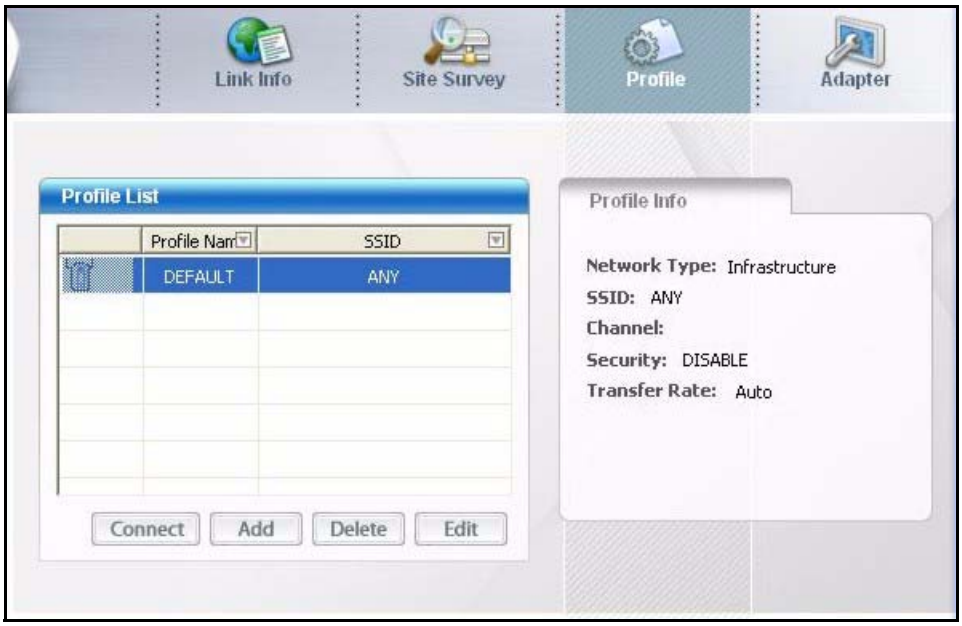
If you do not configure and activate a profile, each time you start the ZyXEL G-220 v2, the ZyXEL G-220 v2 uses the default profile to connect to any available network with security disabled.

The default profile is a profile that allows you to connect to any SSID without security.

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 21 Station Mode: Profile



The following table describes the labels in this screen.

Table 11 Station Mode: Profile

LABEL	DESCRIPTION
Profile List	Click a column heading to sort the entries.
, , 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.
SSID	This field displays the SSID (Service Set IDentifier) of the profile.
Channel	This field displays the channel number used by the profile.

Table 11 Station Mode: Profile (continued)

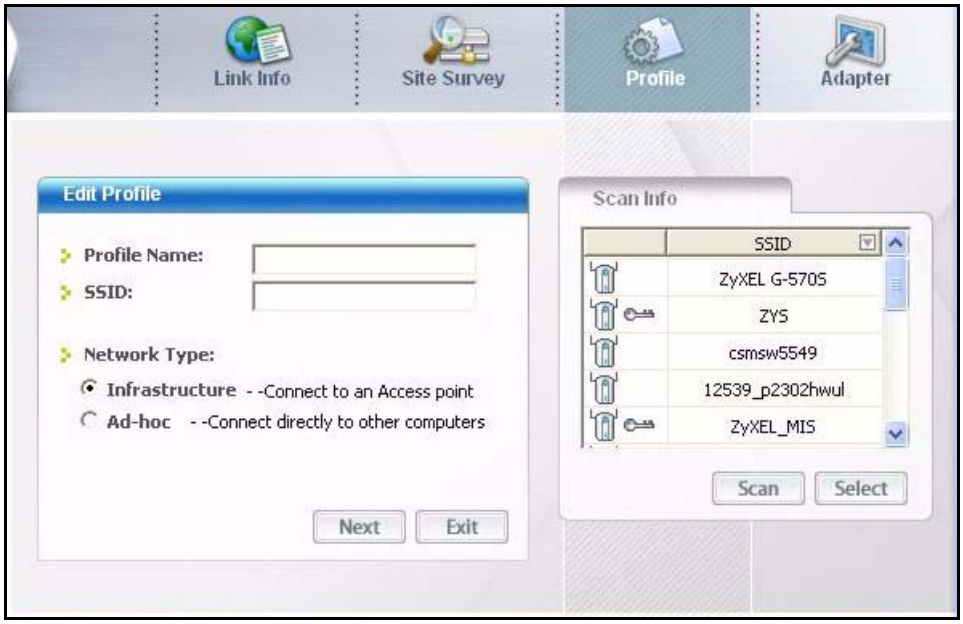
LABEL	DESCRIPTION
Security	This field shows whether data encryption is activated (**WEP** (WEP or 802.1x), **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**) or inactive (**DISABLE**).
Transmission Rate	This field displays the transmission speed of the selected profile in megabits per second (Mbps).

3.4.1 Adding a New Profile

Follow the steps below to add a new profile.

1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next. Click **Next** to continue.

Figure 22 Station Mode: Profile: Add a New Profile



The following table describes the labels in this screen.

Table 12 Station Mode: Profile: Add a New Profile

LABEL	DESCRIPTION
Add New Profile	
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 of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the ZyXEL G-220 v2 associate to any AP 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.
Next	Click **Next** to go to the next screen.

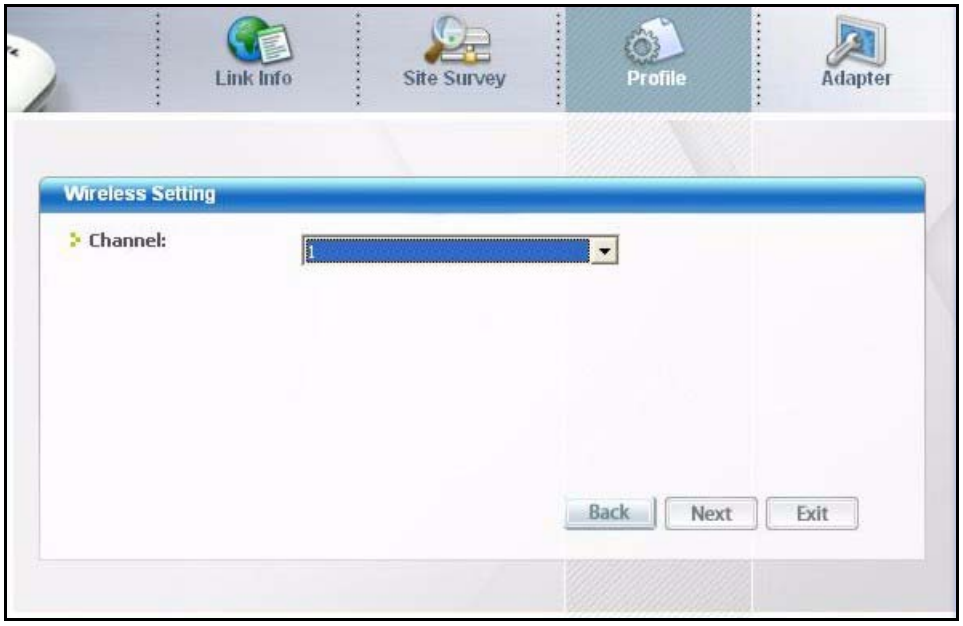
Table 12 Station Mode: Profile: Add a New Profile (continued)

LABEL	DESCRIPTION
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 ZyXEL G-220 v2 associates to the selected wireless network only.

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.

Note: To associate to an ad-hoc network, you must use the same channel as the peer computer.

Figure 23 Station Mode: Profile: Select a Channel



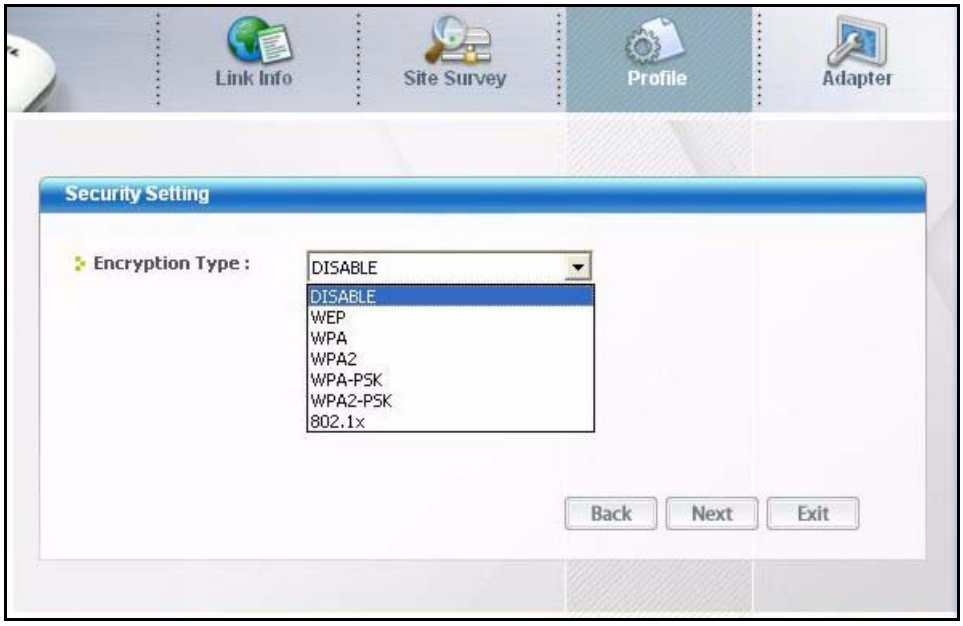
The following table describes the labels in this screen.

Table 13 Station Mode: Profile: Select a Channel

LABEL	DESCRIPTION
Wireless Settings	
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.

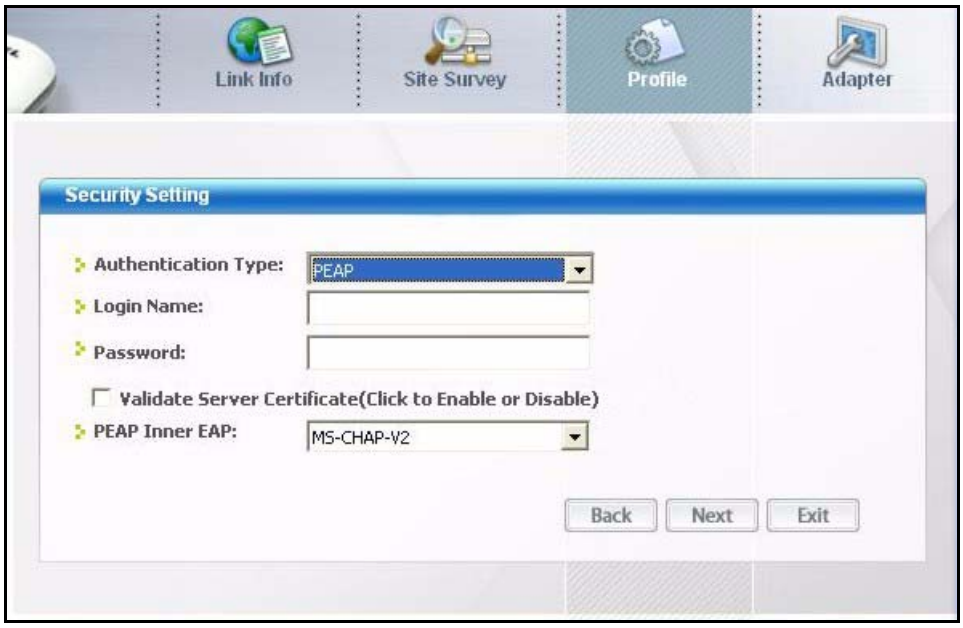
3 If you select **Infrastructure** network type in the first screen, select **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x** from the drop-down list box to enable data encryption. If you select **Ad-Hoc** network type in the first screen, you can only use **WEP** encryption method. Otherwise, select **DISABLE** to allow the ZyXEL G-220 v2 to communicate with the access points or other peer wireless computers without any data encryption and skip to step 5.

Figure 24 Station Mode: Profile: Wireless Settings



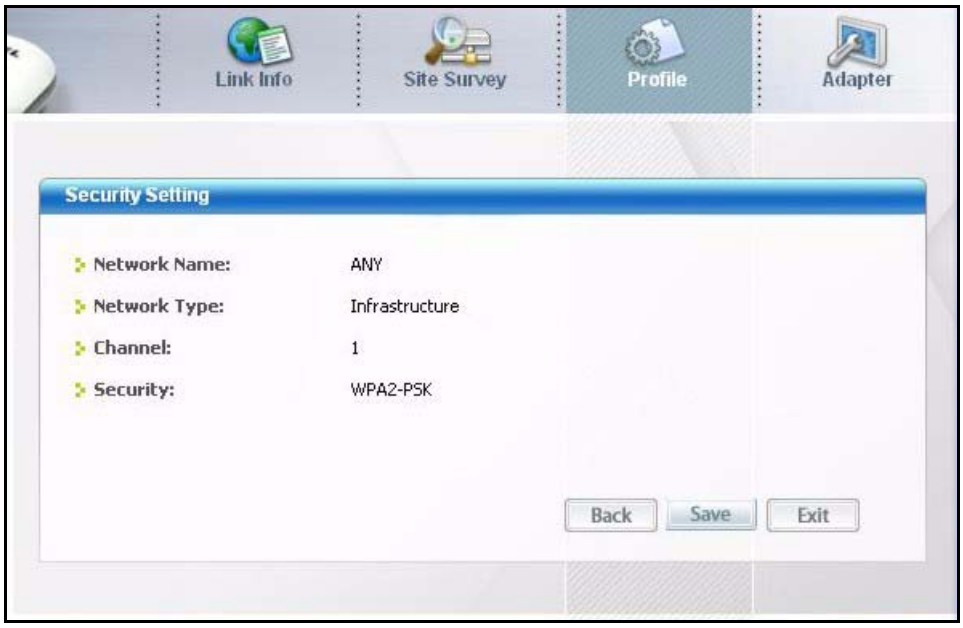
4 The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless computers as they are on the ZyXEL G-220 v2. Refer to Section 3.3.2 on page 39 for detailed information on wireless security configuration.

Figure 25 Station Mode: Profile: Security Settings



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 26 Station Mode: Profile: Confirm New Settings



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

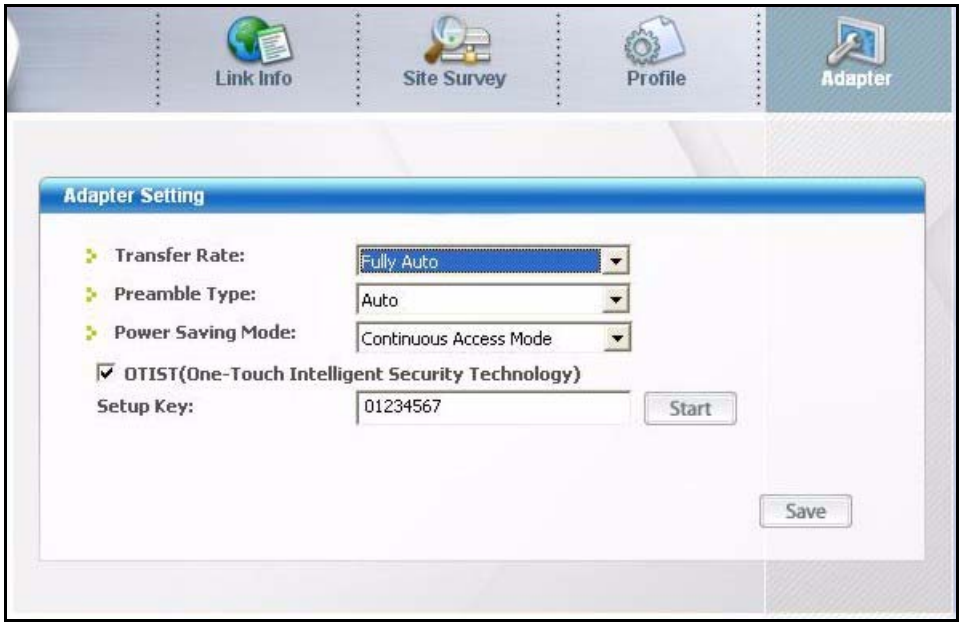
Note: Once you activate a profile, the ZyXEL Utility will use that profile the next time it is started.

Figure 27 Station Mode: Profile: Activate the Profile

3.5 The Adapter Screen

To set the advanced features on the ZyXEL G-220 v2, click the **Adapter** tab.

Figure 28 Station Mode: Adapter



The following table describes the labels in this screen.

Table 14 Station Mode: Adapter

LABEL	DESCRIPTION
Adapter Setting	
Transmission Rate	Select a transmission speed from the drop-down list box. Choose from **Fully Auto** (default), **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **6 Mbps**, **9 Mbps**, **11 Mbps**, **12 Mbps**, **18 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, and **54 Mbps**.
Preamble Type	Select a preamble type. Choices are **Long**, **Short** and **Auto**.The default setting is **Auto**. Refer to Section 2.4 on page 31 for more information

Table 14 Station Mode: Adapter (continued)

LABEL	DESCRIPTION
Power Saving Mode	Select **Maximum Power Save** or **Fast Power Save** to save power (especially for notebook computers). This forces the ZyXEL G-220 v2 to go to sleep mode when it is not transmitting data. When you select **Continuous Access Mode**, the ZyXEL G-220 v2 will never go to sleep mode.
OTIST (One-Touch Intelligent Security Technology)	Select this check box to enable OTIST.
Setup Key	Enter the same setup key (up to eight printable characters) as the ZyXEL AP or wireless router to which you want to associate. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key on the ZyXEL 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 AP or wireless router set your ZyXEL G-220 v2 to use the same wireless settings as the ZyXEL AP or wireless router. You must also activate and start OTIST on the ZyXEL AP or wireless router at the same time. The process takes three minutes to complete
Save	Click **Save** to save the changes back to the ZyXEL G-220 v2 and return to the **Link Info** screen.

CHAPTER 4
Access Point Mode Configuration

This chapter shows you how to configure your ZyXEL G-220 v2 in access point mode.

4.1 Access Point Mode Introduction

To set your ZyXEL G-220 v2 as an Access Point (AP), refer to Section 1.7.1 on page 25.

In access point mode, your ZyXEL G-220 v2 functions as an access point. This allows you to set up your wireless networks without using a dedicated AP device. Up to 16 wireless stations can associate to the ZyXEL G-220 v2.

4.1.1 Additional Setup Requirements

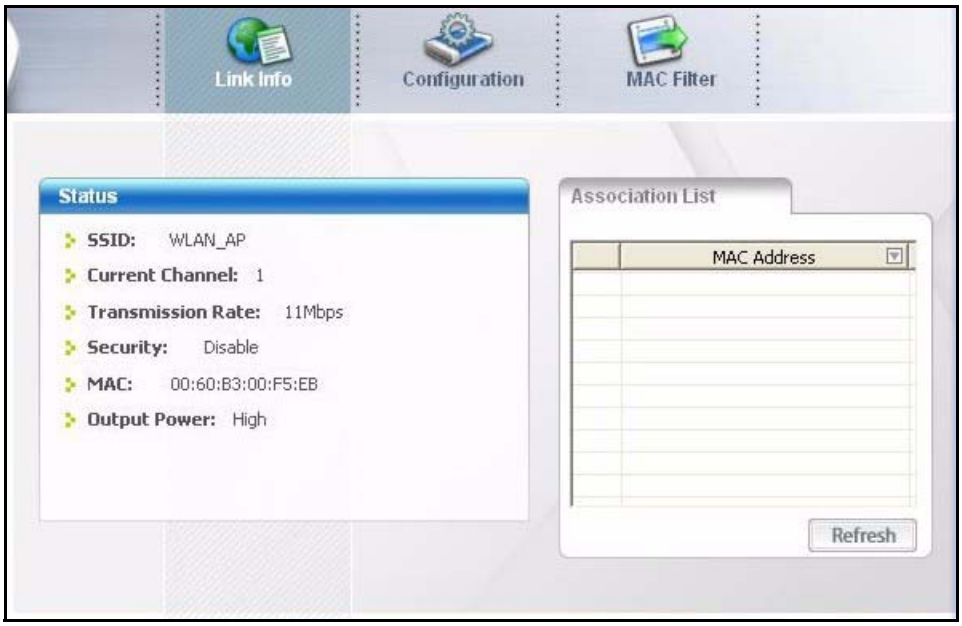
To bridge your wired and wireless network using the ZyXEL G-220 v2, the following requirements must be met:

1. The ZyXEL G-220 v2 must be installed on a computer connected to the wired network.
2. Either bridge the two interfaces (wireless and wired) on the computer (using the **Configuration** screen of the ZyXEL utility in Windows XP) or configure network sharing (refer to Appendix B on page 67 for an example).
3. Set the wireless station's IP address to be in the same subnet as the computer in which the ZyXEL G-220 v2 is installed. Refer to Appendix F on page 95.

4.2 The Link Info Screen

Select the **AP Mode** radio button and wait for about five seconds to display the screen as shown.

Figure 29 Access Point Mode: Link Info



The following table describes the labels in this screen.

Table 15 Access Point Mode: Link Info

LABEL	DESCRIPTION
Status	
SSID	This field displays the name that identifies your ZyXEL G-220 v2 in the wireless LAN network.
Current Channel	This field displays the radio channel the ZyXEL G-220 v2 is currently using.
Transmission Rate	This field displays the current transmission rate of the ZyXEL G-220 v2 in megabits per second (Mbps).
Security	This field shows whether data encryption is activated (**WEP**) or inactive (**Disable**).
MAC	This field displays the MAC address of the ZyXEL G-220 v2.
Output Power	This field shows the strength of the ZyXEL G-220 v2's antenna gain or transmission power.
Association List	This table lists up to 16 wireless clients that are currently connected to the ZyXEL G-220 v2.
	 denotes a wireless client without WEP security.  denotes a wireless client with WEP security enabled.
MAC Address	This field displays the MAC addresses of a wireless client that is currently connected to the ZyXEL G-220 v2.
Refresh	Click **Refresh** to update this screen.

4.3 The Configuration Screen

Click **Configuration** in the **ZyXEL Utility** screen to display the screen as shown.

Figure 30 Access Point Mode: Configuration

The following table describes the labels in this screen.

Table 16 Access Point Mode: Configuration

LABEL	DESCRIPTION
Wireless Settings	
SSID	The SSID identifies the service set to which a wireless station is associated. Wireless stations associating to the access point (the ZyXEL G-220 v2) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
Channel	Set the operating frequency/channel depending on your geographical region.
Output Power	Set this field if you need to conserve power consumption (especially for notebook computers). This control changes the strength of the ZyXEL G-220 v2's antenna gain or transmission power. Antenna gain, measured in dBm (decibel relative units compared to milliwatts), is the increase in coverage. Higher antenna gain improves the range of the signal for better communications. Select **High** to set the ZyXEL G-220 v2's antenna to transmit at 17-dBm. Select **Medium-High** to set the ZyXEL G-220 v2's antenna to transmit at 15-dBm. Select **Medium-Low** to set the ZyXEL G-220 v2's antenna to transmit at 13-dBm. Select **Low** to set the ZyXEL G-220 v2's antenna to transmit at 11-dBm. This allows for the least power consumption.
Bridge	This field is only applicable in Windows XP. Select the check box and an Ethernet adapter (network interface card (NIC)) on your computer from the drop-down list box. This allows you to connect your wireless network to the specified wired network.
Security Settings	

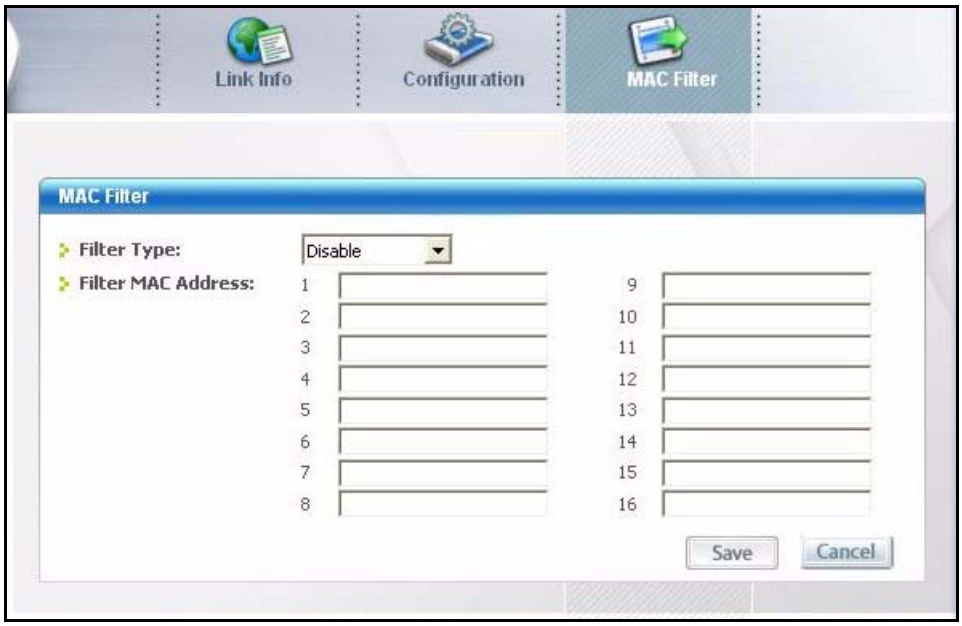
Table 16 Access Point Mode: Configuration (continued)

LABEL	DESCRIPTION
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields. Select **Disable** to deactivate the WEP encryption.
Authentication Type	Select an authentication method. Choices are **Auto**, **Shared Key** and **Open System**. Refer to Section 2.3 on page 31 for more information.
Pass Phrase	When you select the radio button, enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the ZyXEL G-220 v2 automatically generates four different WEP key and displays it in the key field below. Refer to Section 2.2.1 on page 27 for more information. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
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)	Select this option if you want to manually enter 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, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey1111222233334444555566 78) for ASCII key type. **Note:** 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.
Cancel	Click **Cancel** to discard the changes.

4.4 The MAC Filter Screen

The **MAC Filter** screen allows you to configure the ZyXEL G-220 v2 to give exclusive access to (Accept) devices or exclude devices from (Reject) connecting to the ZyXEL G-220 v2. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the device(s) to configure this screen.

Figure 31 Access Point Mode: MAC Filter



The following table describes the labels in this screen.

Table 17 Access Point Mode: MAC Filter

LABEL	DESCRIPTION
Filter Type	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Disable** to deactivate the MAC filter feature. Select **Reject** to block access to the ZyXEL G-220 v2, MAC addresses not listed will be allowed to access the ZyXEL G-220 v2. Select **Accept** to permit access to the ZyXEL G-220 v2, MAC addresses not listed will be denied access to the ZyXEL G-220 v2.
Filter MAC Address 1-16	Specify the MAC address(es) of the wireless station(s) that is allowed or denied association to the ZyXEL G-220 v2. Enter six pairs of hexadecimal digits (separated by colons) in the range of "A-F", "a-f" and "0-9" (for example, 00:A0:C5:00:00:02). If you enter an invalid MAC address, once you click **Save** to save the values, a warning screen will be displayed.
Save	Click **Save** to save the changes back to the ZyXEL G-220 v2.
Cancel	Click **Cancel** to discard the changes.

CHAPTER 5
Maintenance

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

5.1 The About Screen

The **About** screen displays related version numbers of the ZyXEL G-220 v2. To display the screen as shown below, click the about ( ) button.

Figure 32 About

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

Table 18 About

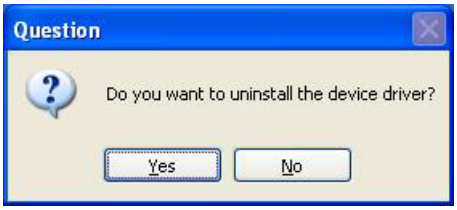
LABEL	DESCRIPTION
Driver Version	This field displays the version number of the ZyXEL G-220 v2 driver.
Utility Version	This field displays the version number of the ZyXEL Utility.

5.2 Uninstalling the ZyXEL Utility

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

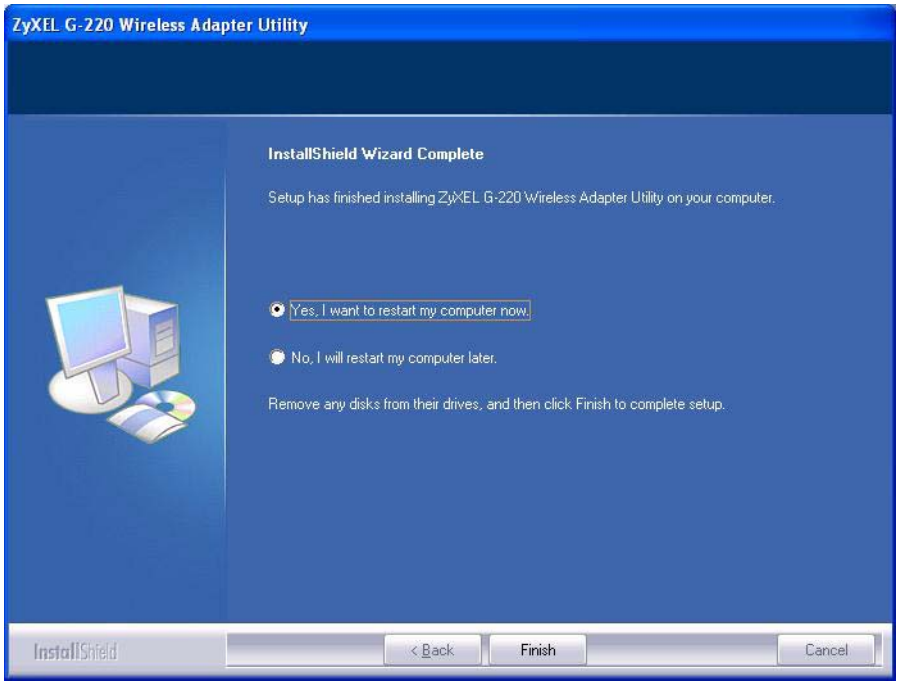
1. Click **Start**, **(All) Programs**, **ZyXEL G-220 v2 Wireless Adapter Utility**, **Uninstall ZyXEL G-220 v2 Wireless Adapter Utility**.
2. When prompted, click **OK** or **Yes** to remove the driver and the utility software.

Figure 33 Uninstall: Confirm



3 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

Figure 34 Uninstall: Finish



5.3 Upgrading the ZyXEL Utility

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

To perform the upgrade, follow the steps below.

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

2 Follow the steps in Section 5.2 on page 59 to remove the current ZyXEL Utility from your computer.

3 Restart your computer when prompted.

4 Disconnect the ZyXEL G-220 v2 from your computer.

5 Double-click on the setup program for the new utility to start the ZyXEL Utility installation.

6 Insert the ZyXEL G-220 v2 and check the version numbers in the **About** screen to make sure the new utility is installed properly.

CHAPTER 6
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.

6.1 Problems Starting the ZyXEL Utility Program

Table 19 Troubleshooting Starting ZyXEL Utility Program

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Wireless LAN Utility	Make sure the ZyXEL G-220 v2 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 ZyXEL G-220 v2 under **Network Adapter**. (Steps may vary depending on the version of Windows). Install the ZyXEL G-220 v2 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.

6.2 Problem Connecting to an Access Point

Table 20 Troubleshooting Access Point Connection Problem

PROBLEM	CORRECTIVE ACTION
When using the Windows XP configuration tool, cannot scan for or connect to any access points.	The ZyXEL G-220 v2 might still be operating in access point mode. This results when you set the ZyXEL G-220 v2 to operate in access point mode using the ZyXEL Utility, close the ZyXEL Utility and then use the Windows XP configuration tool. Before you use the Windows XP configuration tool, make sure you set the ZyXEL G-220 v2 to operate in station mode before you close and exit the ZyXEL Utility.

6.3 Problem with the Link Status

Table 21 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.

6.4 Problems Communicating With Other Computers

Table 22 Troubleshooting Communication Problem

PROBLEM	CORRECTIVE ACTION
In wireless station mode, the computer with the ZyXEL G-220 v2 installed cannot communicate with the other computer(s).	In Infrastructure Mode • Make sure that the AP and the associated computers are turned on and working properly. • Make sure the ZyXEL G-220 v2 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 Setting** screen. In Ad-Hoc (IBSS) Mode • Verify that the peer computer(s) is turned on. • Make sure the ZyXEL G-220 v2 computer and the peer computer(s) are using the same SSID and channel. • Make sure that the computer and the peer computer(s) share the same security settings. • Change the wireless clients to use another radio channel if interference is high.
In access point mode, the wireless station(s) cannot associate to the ZyXEL G-220 v2.	Verify that the computer with the ZyXEL G-220 v2 installed is turned on. Make sure the wireless station(s) uses the same SSID as the ZyXEL G-220 v2. Make sure the wireless station(s) uses the same security settings. Verify that the wireless station(s) is not blocked in the **MAC Filter** screen.

APPENDIX A
Product Specifications

Table 23 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	ZyXEL G-220 v2 802.11g Wireless USB Adapter
Interface	USB 2.0 compatible
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	2.412-2.484GHz
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: 11, 5.5, 2, 1Mbps IEEE 802.11g: 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
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power	IEEE 802.11g: TX: 450mA RX: 345mA IEEE 802.11b: TX: 450mA RX: 345mA
Voltage	5V
Weight	25.8 g
Dimension	(W) 95 mm × (D) 30 mm × (H) 16 mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Frequency	2.4 ~ 2.484GHz (Industrial Scientific Medical Band)
Channels	1~11 Channels (USA, Canada) 1~13 Channels (Europe)
Data Rate	IEEE 802.11g (OFDM): 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps

Table 23 Product Specifications (continued)

Modulation	IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (OFDM) IEEE 802.11b: 11, 5.5 Mbps (CCK), 2 Mbps (DQPSK), 1 Mbps (DBPSK)
Output Power	17 dBm (typical) at 11Mbps CCK, QPSK, BPSK 15 dBm (typical) at 54Mbps OFDM
RX Sensitivity	IEEE 802.11g (OFDM): 54 Mbps: < -72 dBm IEEE 802.11b (CCK): 11 Mbps: < -85 dBm
SOFTWARE SPECIFICATIONS	
Device Drivers	Microsoft Windows 98 Second Edition, Windows ME, Windows 2000, Windows XP
Roaming	IEEE 802.11b/g compliant
WEP	Supports 64-bit, 128-bit and 256-bit WEP encryption

APPENDIX B
Access Point Mode Setup Example

This example uses the network sharing feature in Windows 2000 to bridge the wired and wireless network when you set the ZyXEL G-220 v2 in access point (AP) mode.

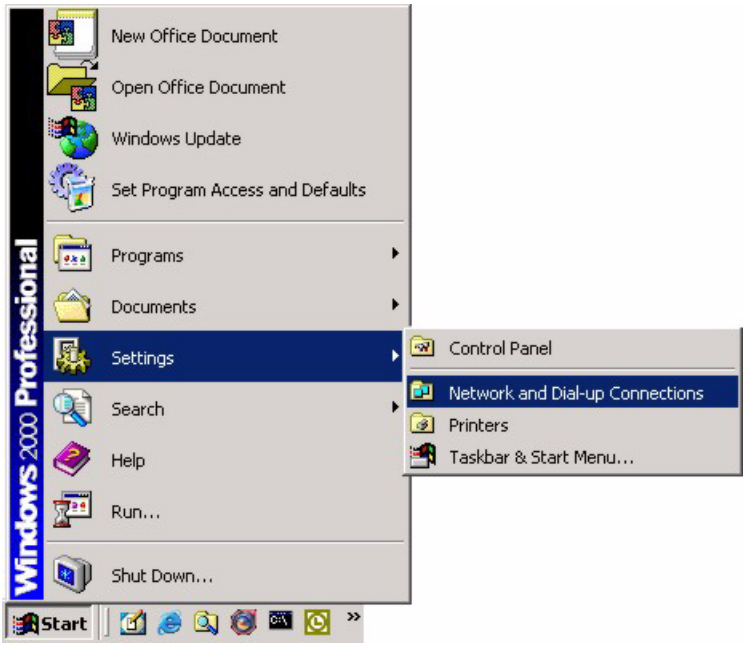
Refer to Chapter 4, "Access Point Mode Configuration," on page 53 for setup methods and requirements.

Steps may vary depending on your Windows version. You may need to install additional software in Windows 98 Second Edition and Windows ME.

Configuring the Computer on Which You Install the ZyXEL G-220 v2

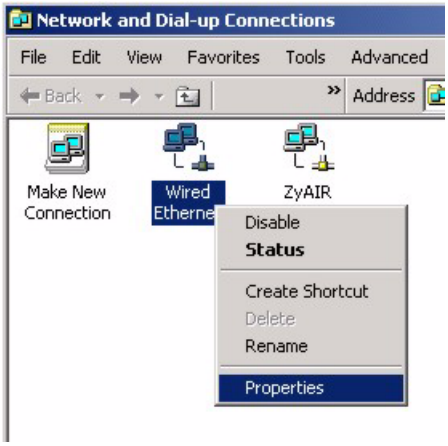
1. Refer to Section 1.7.1 "Change ZyXEL G-220 v2 Mode" on page 25 to set the ZyXEL G-220 v2 to operate in AP mode.
2. Click **Start**, **Settings**, **Network and Dial-up Connections** (or click **Start**, **Settings**, **Control Panel** and double-click **Network and Dial-up Connections**).

Figure 35 Windows 2000: Start



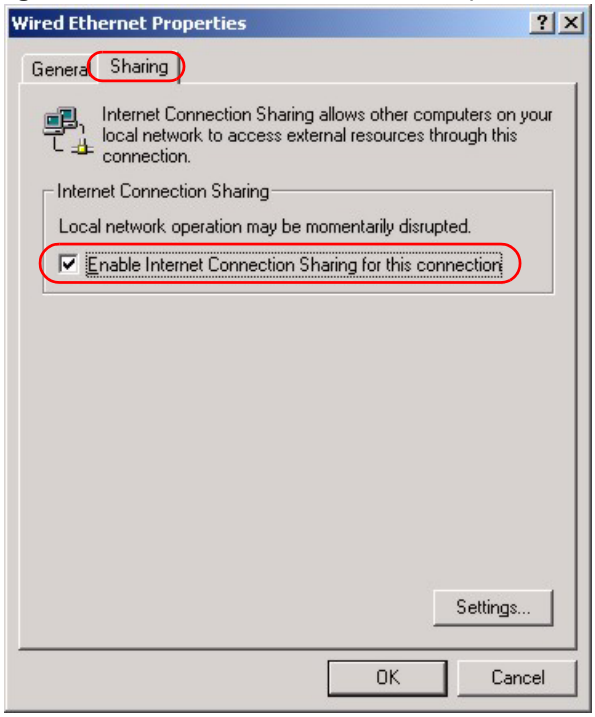
3. Right-click on the icon for your wired Ethernet adapter and click **Properties**.

Figure 36 Windows 2000: Network and Dial-up Connections



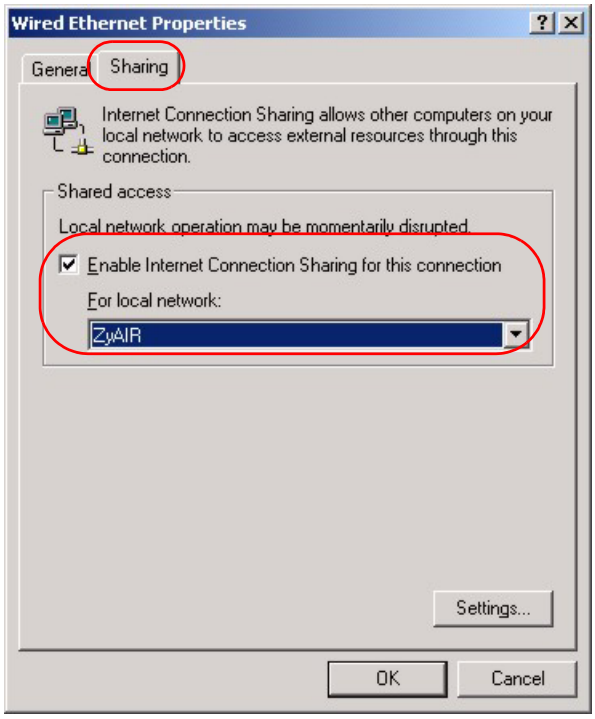
4 A **Properties** screen displays. Click the **Sharing** tab and select **Enable Internet Connection Sharing for this connection**. Click **OK**.

Figure 37 Windows 2000: Network Properties



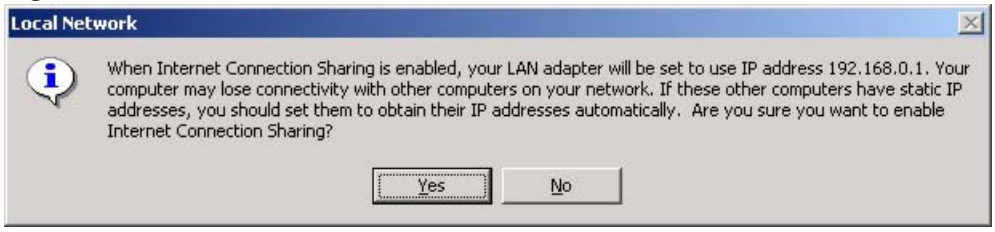
If there is more than one network adapter on the computer, select **Enable Internet Connection Sharing for this connection** and select the network adapter to which you want to share network access.

Figure 38 WIndows 2000: Network Properties: Select Network Adapter



5 A notice screen displays. Click **Yes**.

Figure 39 Windows 2000: Local Network



Configuring the Wireless Station Computer

Refer to Appendix F, "Setting up Your Computer's IP Address," on page 95 for more information on how to set up the wireless station computer(s) IP address.

APPENDIX C
Disable Windows XP Wireless LAN Configuration Tool

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

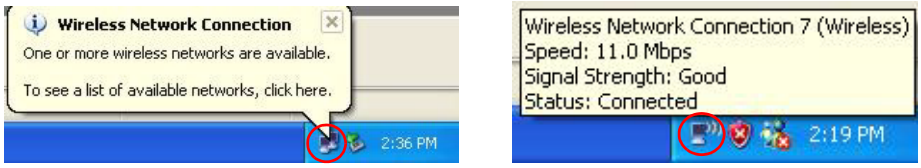
Follow the steps below to disable the configuration tool in Windows XP after you install the ZyXEL Utility. The screen varies depending on the version of Windows XP service pack.

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.

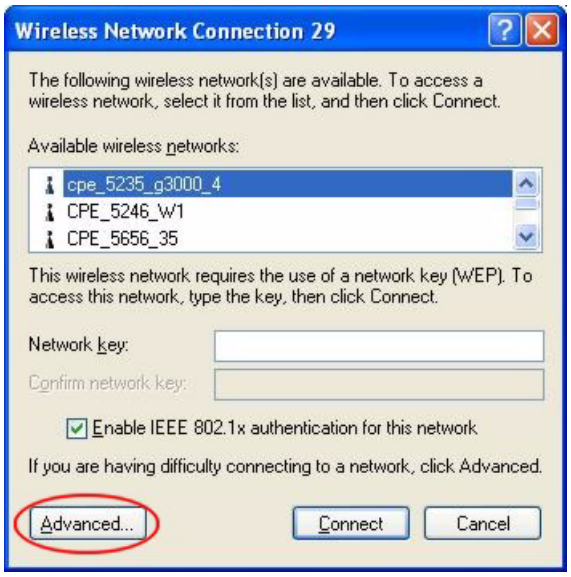
1 Double-click the network icon for wireless connections in the system tray.

Figure 40 Windows XP: System Tray Icon



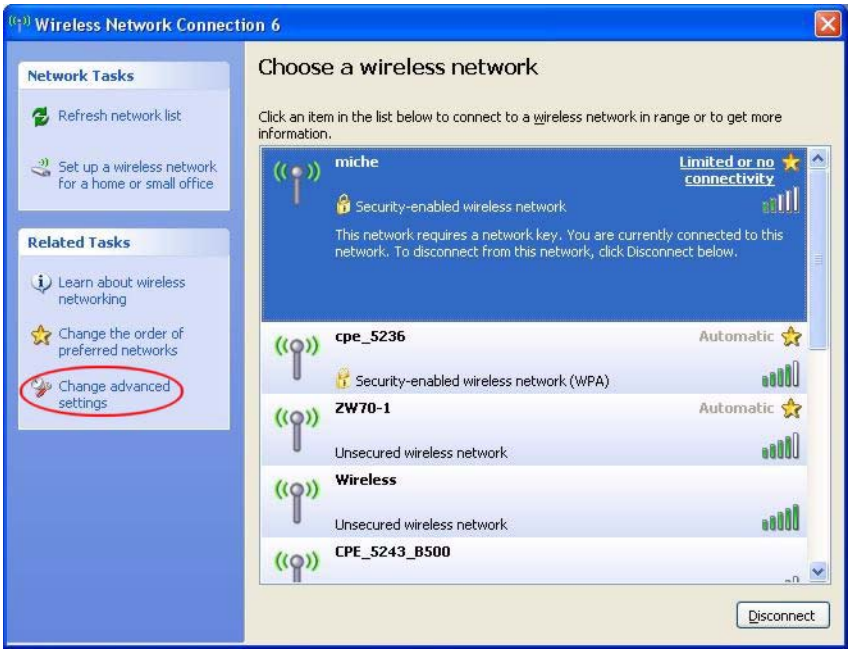
2 Windows XP SP1: When a **Wireless Network Connection** window displays, click **Advanced…**.

Figure 41 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.

Figure 42 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**.

Figure 43 Windows XP SP1: Wireless Network Connection Properties

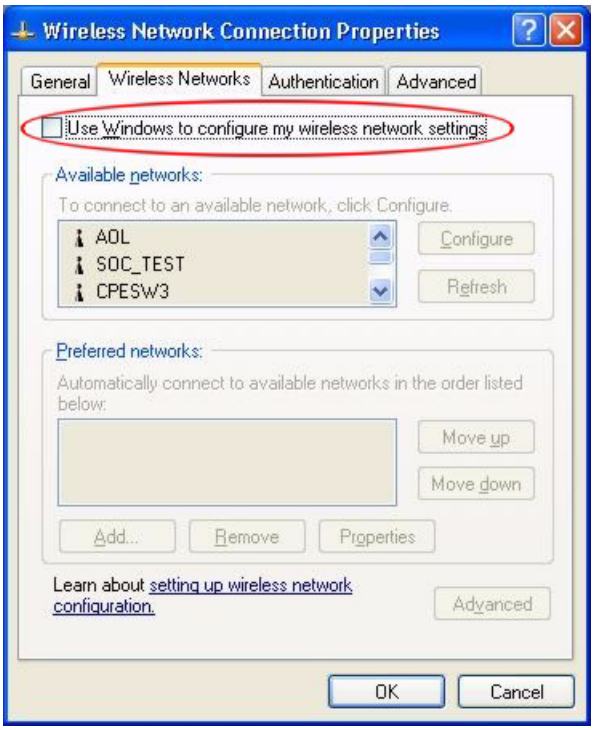
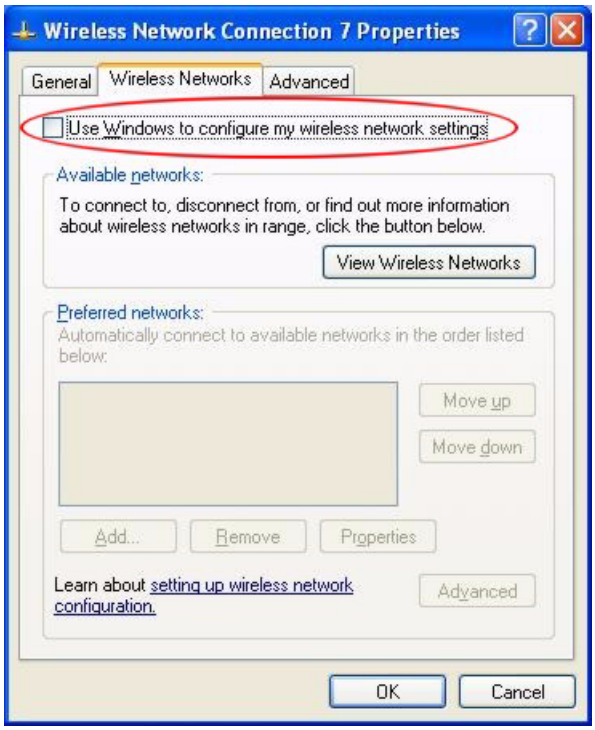


Figure 44 Windows XP SP2: Wireless Network Connection Properties



Via the Control Panel

1. If the icon for the wireless network connection is not in the system tray, click **Start**, **Control Panel** and double-click **Network Connections**.
2. Double-click on the icon for wireless network connection to display a status window as shown below.
3. Click **Properties** and click the **Wireless Networks** tab.

Figure 45 Windows XP SP1: Wireless Network Connection Status

Figure 46 Windows XP SP2: Wireless Network Connection Status

4 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**.

Figure 47 Windows XP SP1: Wireless Network Connection Properties

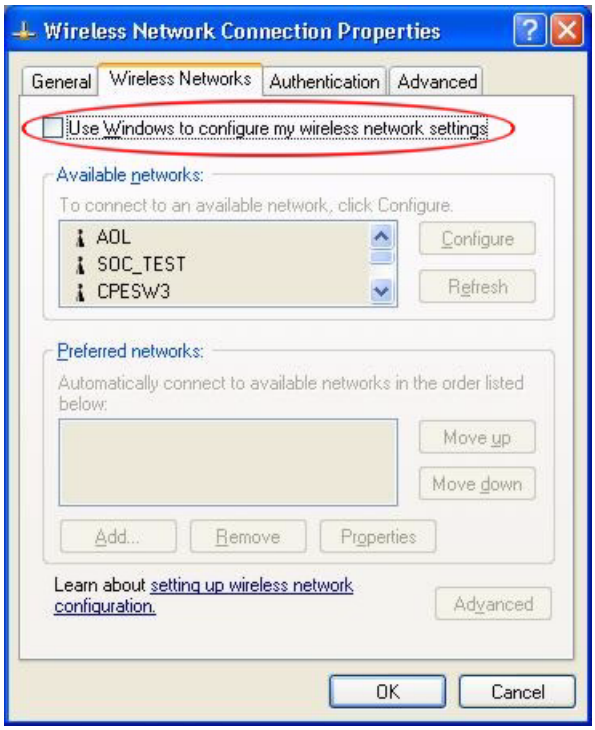
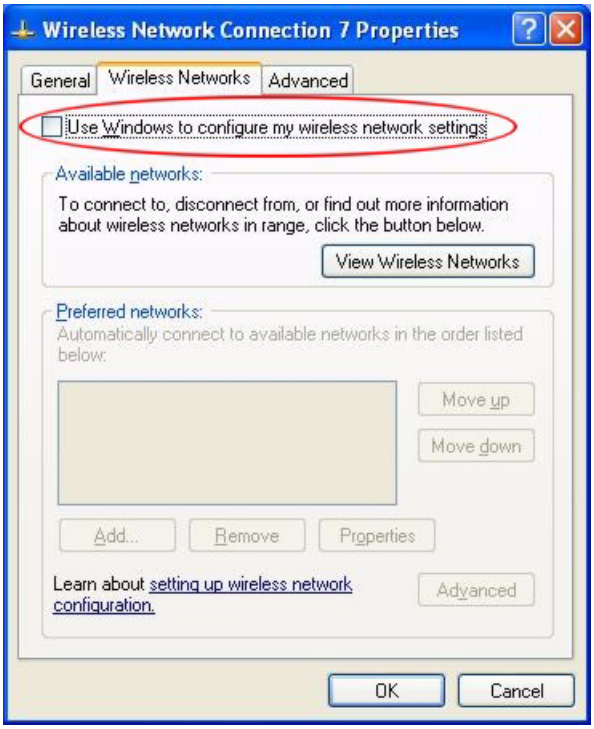


Figure 48 Windows XP SP2: Wireless Network Connection Properties



APPENDIX D
Management with Wireless Zero Configuration

This appendix shows you how to manage your ZyXEL G-220 v2 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.

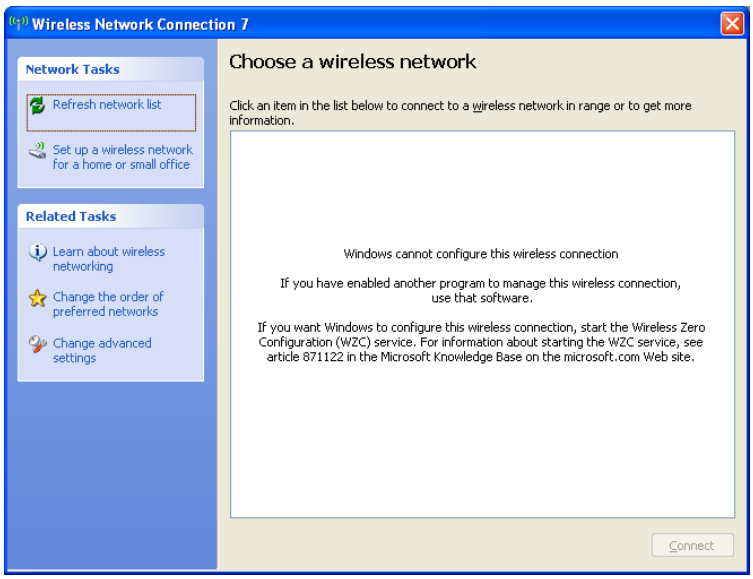
Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon ( ) in most screens, move the cursor to the item that you want the information about and click to view the help.

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 C on page 71.

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

Figure 49 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.

Figure 50 Windows XP SP2: System Tray Icon

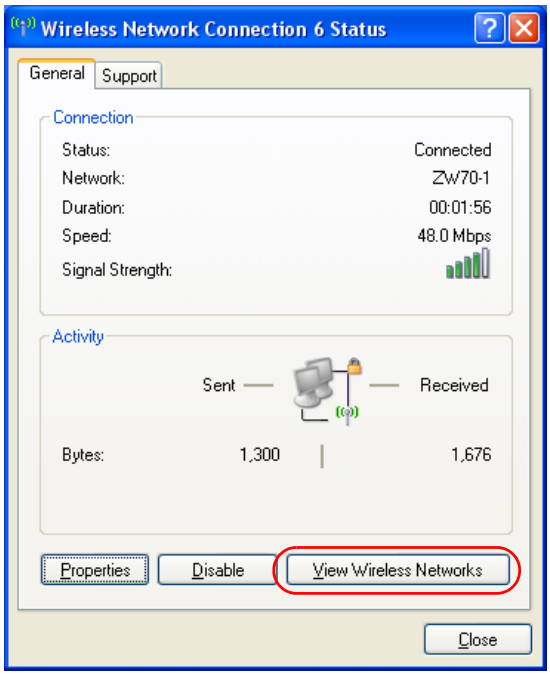
The type of the wireless network icon in Windows XP SP2 indicates the status of the ZyXEL G-220 v2. Refer to the following table for details.

Table 24 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The ZyXEL G-220 v2 is connected to a wireless network.
	The ZyXEL G-220 v2 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 ZyXEL G-220 v2 is not connected to a wireless network.

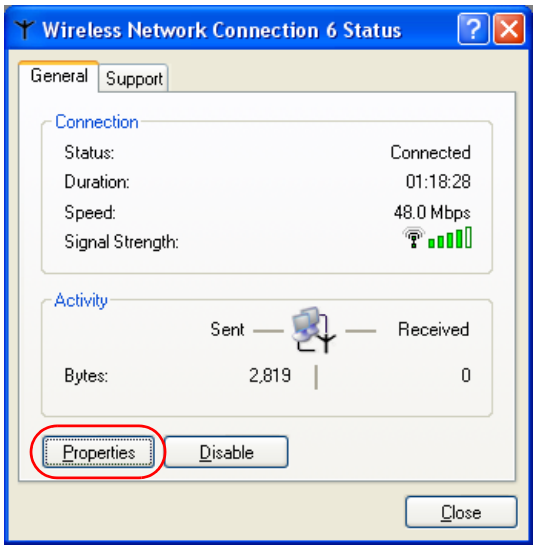
2 Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

Figure 51 Windows XP SP2: Wireless Network Connection Status



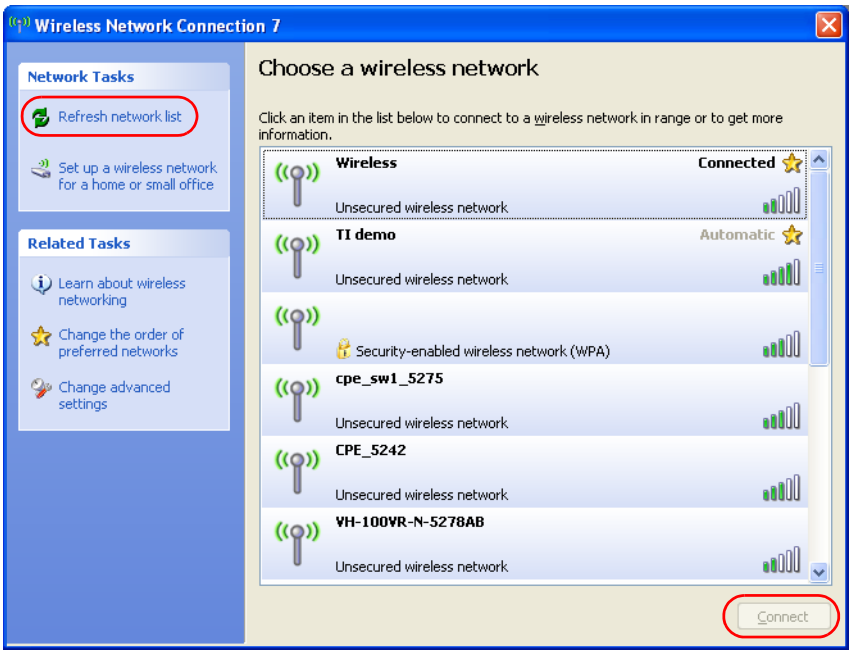
Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

Figure 52 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.

Figure 53 Windows XP SP2: Wireless Network Connection



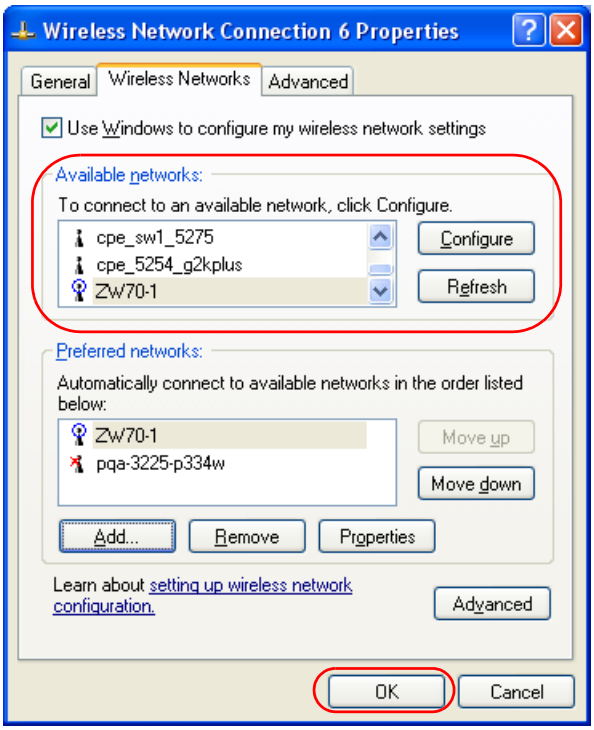
The following table describes the icons in the wireless network list.

Table 25 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
	This denotes that 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 ZyXEL G-220 v2 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.

Figure 54 Windows XP SP1: Wireless Network Connection Properties



4 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 and click **Connect**. Refer to the section about security settings 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.

Figure 55 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

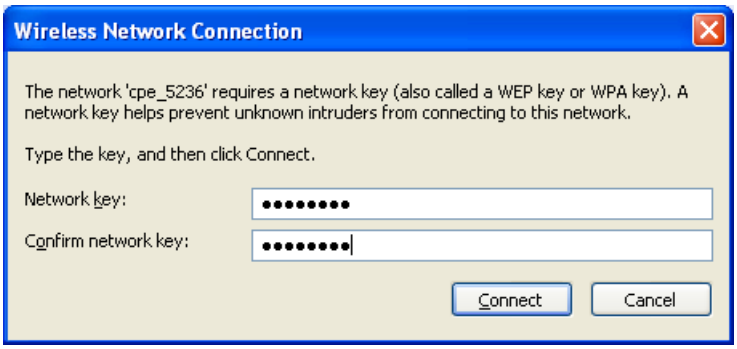


Figure 56 Windows XP SP2: Wireless Network Connection: No Security

5 Verify that you have successfully connected to the selected network and check the 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.

Table 26 Windows XP: Wireless Networks

ICON	DESCRIPTION
	This denotes the wireless network is an available wireless network.
	This denotes the ZyXEL G-220 v2 is associated to the wireless network.
	This denotes the wireless network is not available.

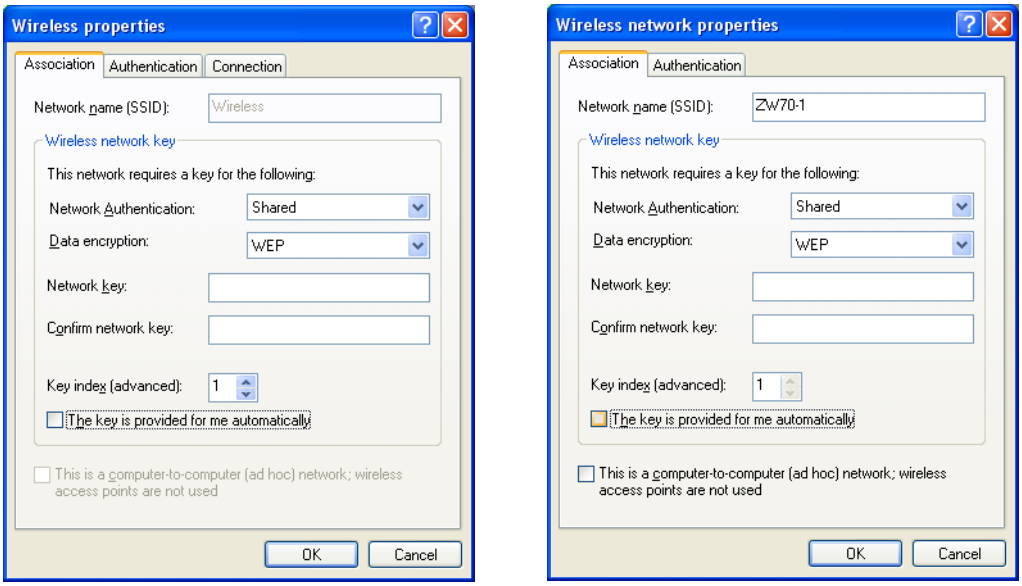
Security Settings

When you configure the ZyXEL G-220 v2 to connect to a secure network but the security settings are not yet enabled on the ZyXEL G-220 v2, 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.

Figure 57 Windows XP: Wireless (network) properties: Association



The following table describes the labels in this screen.

Table 27 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.
Data Encryption	This field automatically shows the encryption type (**TKIP**, **WEP** or **Disable**) used by the selected network.
Network Key	Enter the 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 ZyXEL G-220 v2 a key.

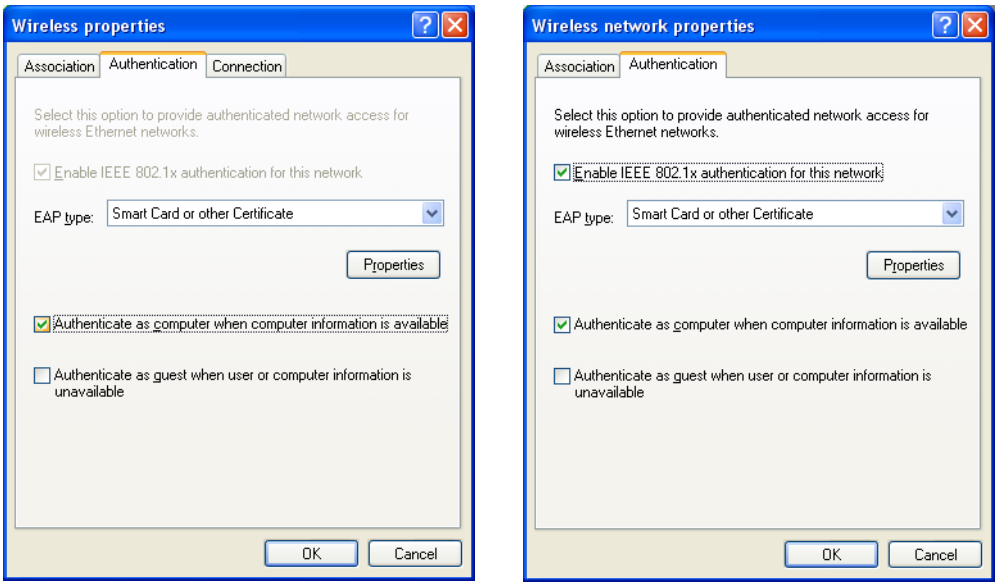
Table 27 Windows XP: Wireless (network) properties: Association (continued)

LABEL	DESCRIPTION
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.

Figure 58 Windows XP: Wireless (network) properties: Authentication



The following table describes the labels in this screen.

Table 28 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.

Table 28 Windows XP: Wireless (network) properties: Authentication (continued)

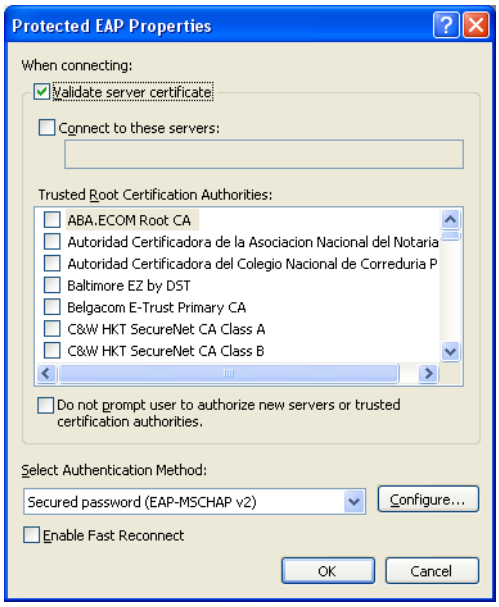
LABEL	DESCRIPTION
Authenticate as computer when computer information is available	Select this check box to have the computer send its information to the network for authentication when a user is not logged on.
Authenticate as guest when user or computer information is unavailable	Select this check box 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 leave 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

Figure 59 Windows XP: Protected EAP Properties



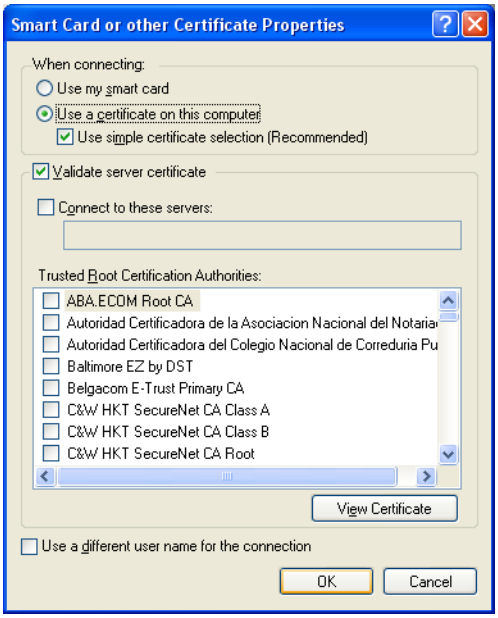
The following table describes the labels in this screen.

Table 29 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. **Note:** 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 verify 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

Figure 60 Windows XP: Smart Card or other Certificate Properties



The following table describes the labels in this screen.

Table 30 Windows XP: Smart Card or other Certificate Properties

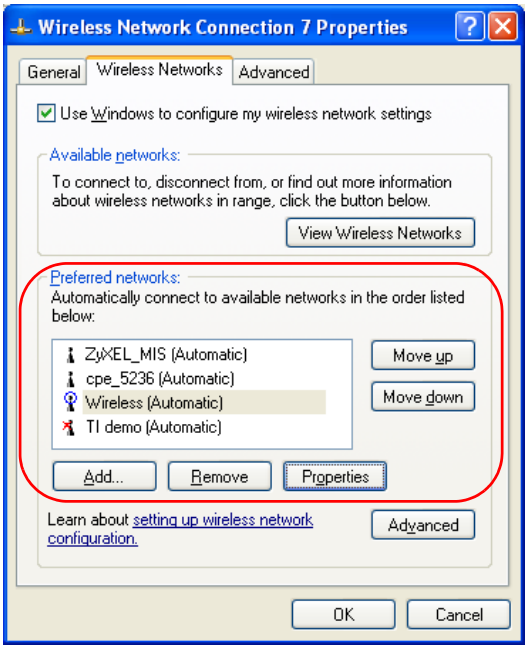
LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication 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.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. **Note:** 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.

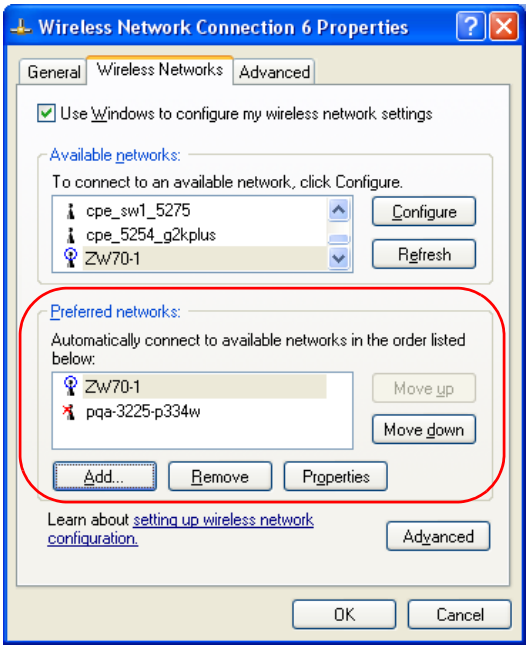
1 Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see Figure 53 on page 79). The screen displays as shown.

Figure 61 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.

Figure 62 Windows XP SP1: Wireless Networks: Preferred Networks



2 Whenever the ZyXEL G-220 v2 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 E
Types of EAP Authentication

This appendix discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information. Your wireless LAN device may not support all authentication types.

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 IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

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 authentication types.

Table 31 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

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include 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.

WPA and WPA2 regularly change and rotate 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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. 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), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a sucessful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WPA(2)-PSK Application Example

A WPA(2)s-PSK application looks as follows.

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 or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP and wireless clients use the pre-shared key to generate a common PMK.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

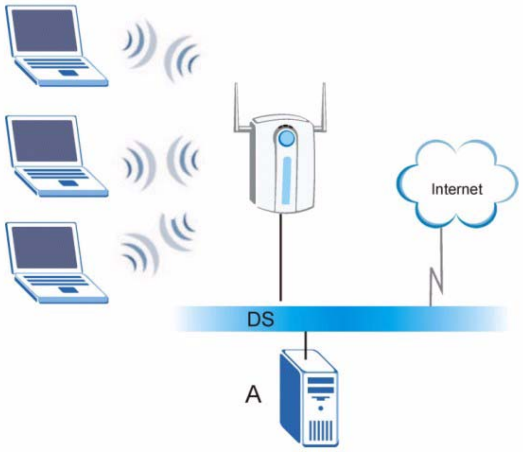
Figure 63 WPA-PSK Authentication

WPA(2) 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(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
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 64 WPA(2) with RADIUS Application Example



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 32 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

APPENDIX F
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

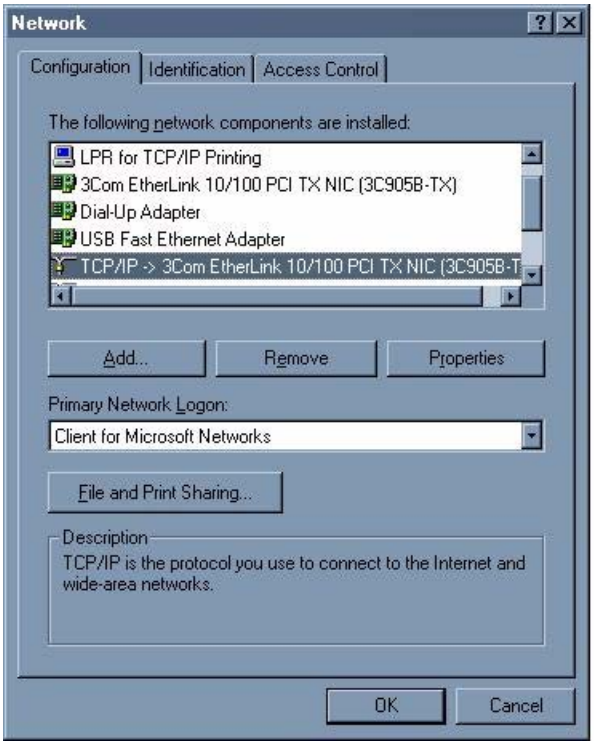
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL G-220 v2's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 65 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

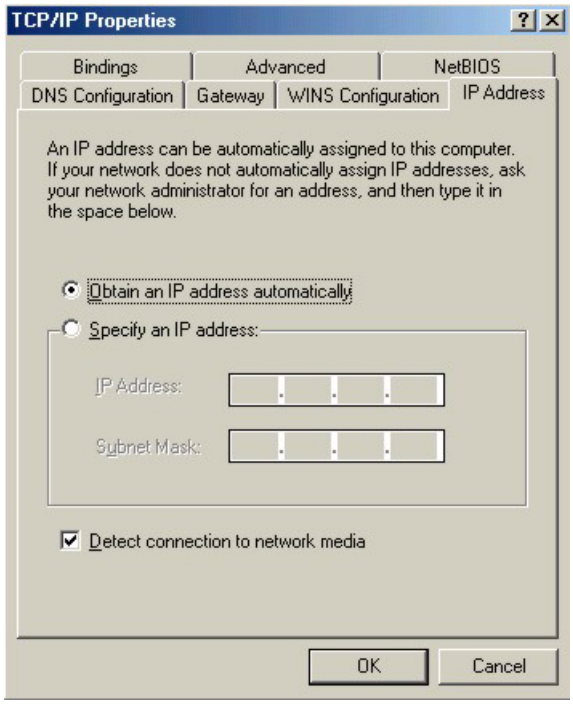
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

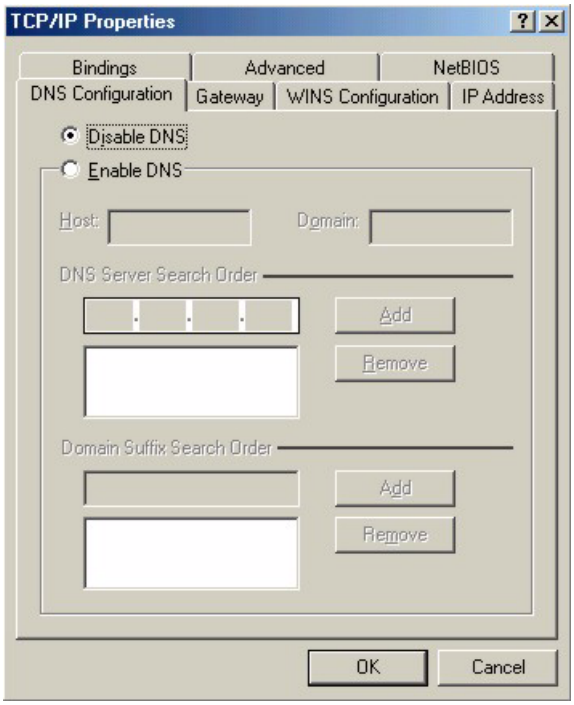
Figure 66 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 67 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyXEL G-220 v2 and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

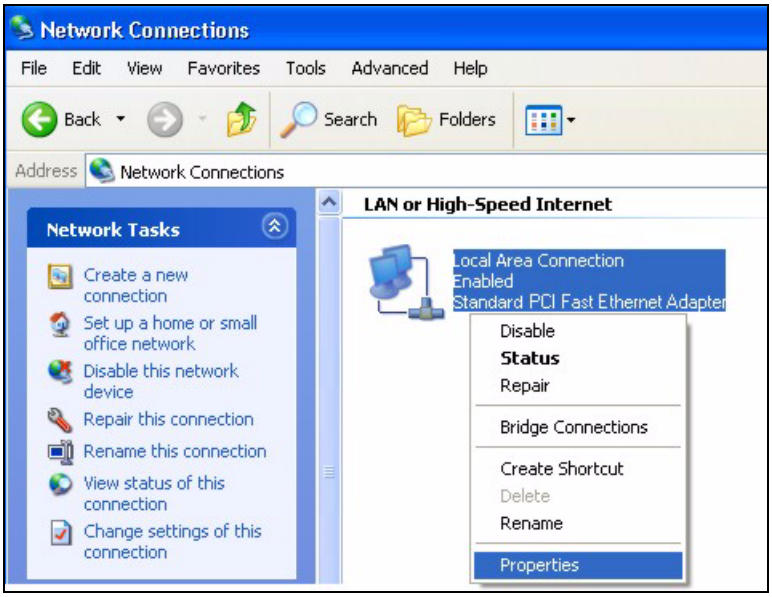
Figure 68 Windows XP: Start Menu

2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 69 Windows XP: Control Panel

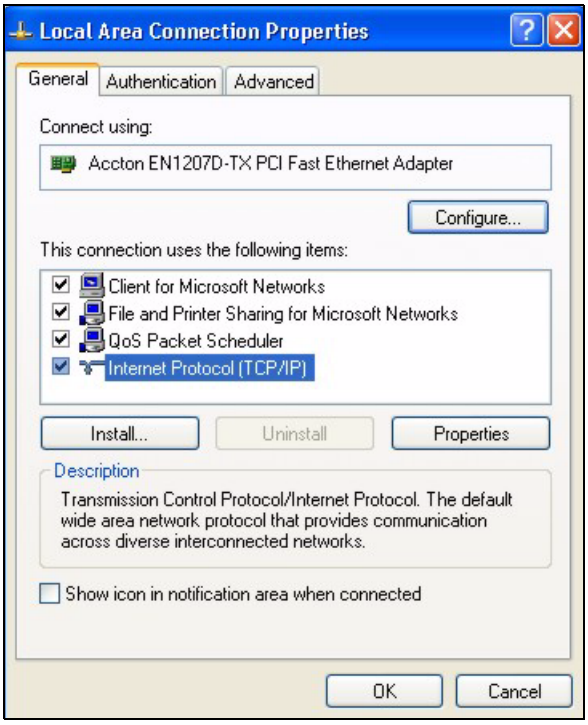
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 70 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 71 Windows XP: Local Area Connection Properties

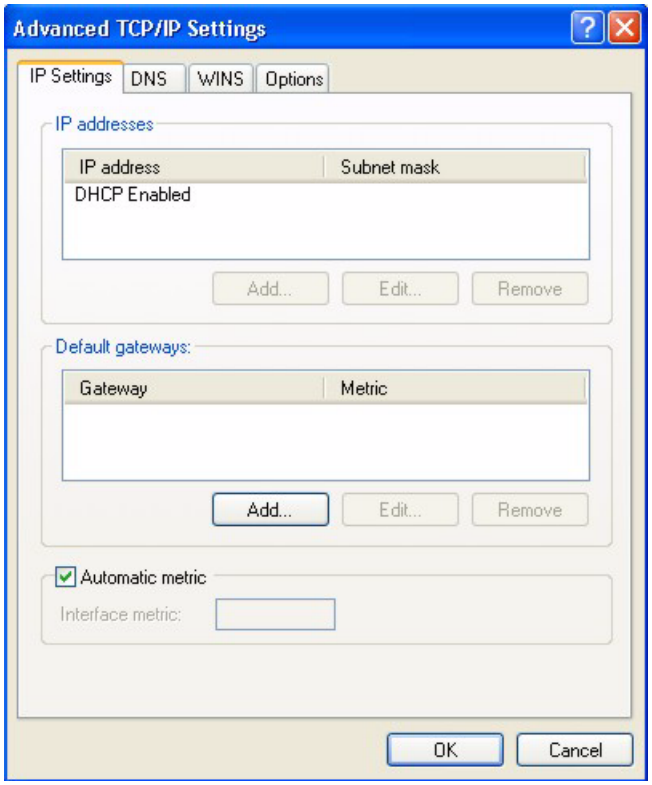


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 72 Windows XP: Advanced TCP/IP Settings



6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

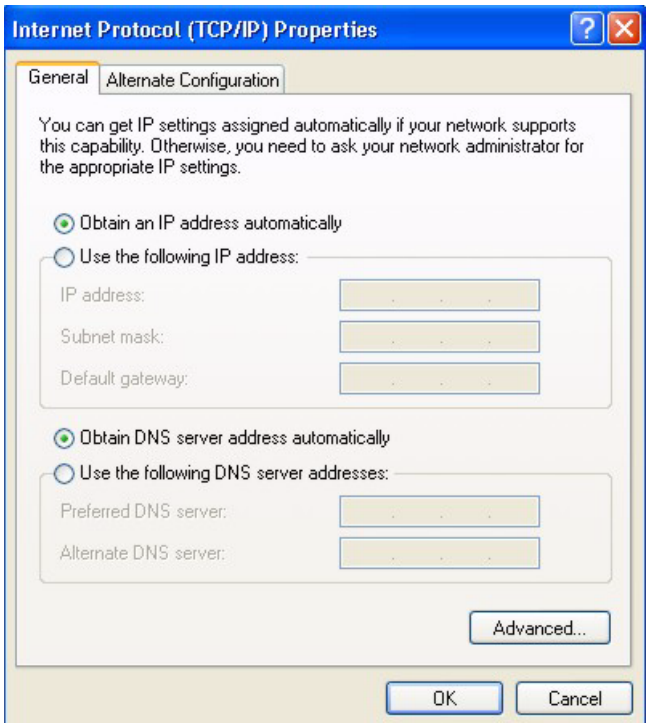
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 73 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your ZyXEL G-220 v2 and restart your computer (if prompted).

Verifying Settings

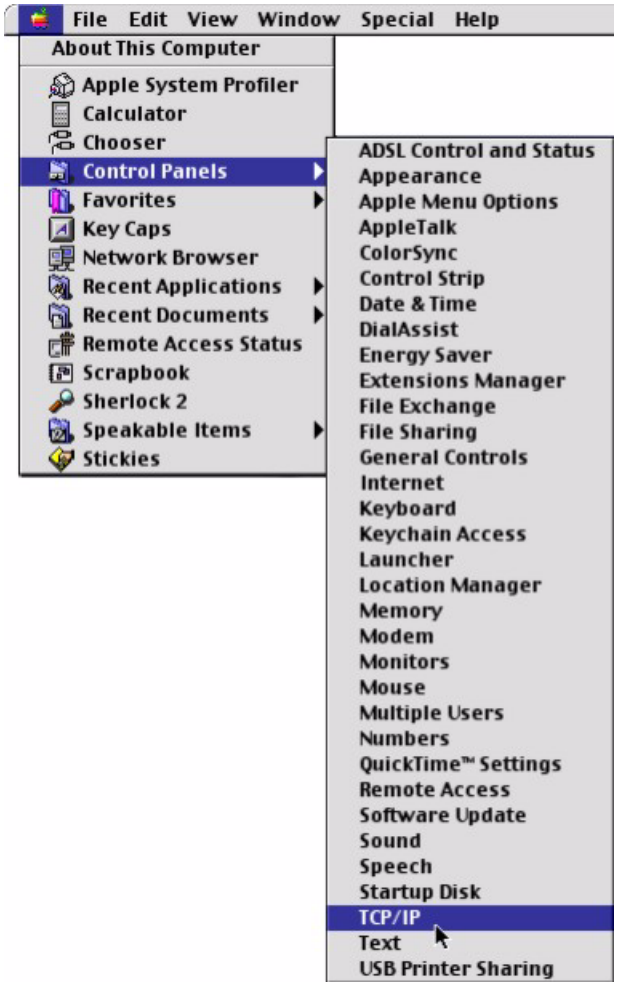
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

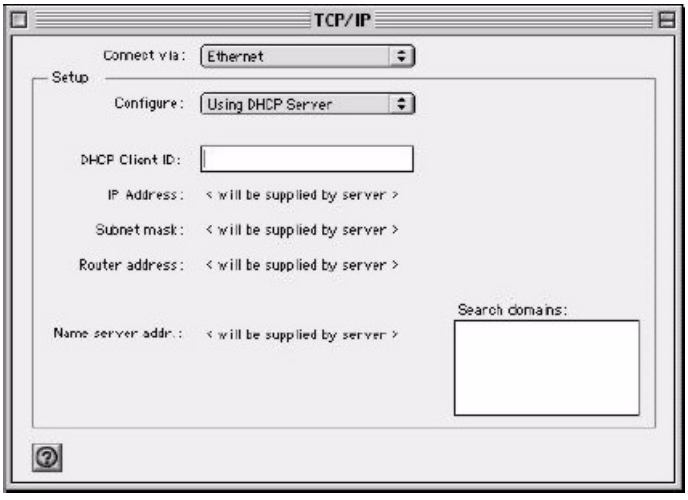
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 74 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 75 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL G-220 v2 in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL G-220 v2 and restart your computer (if prompted).

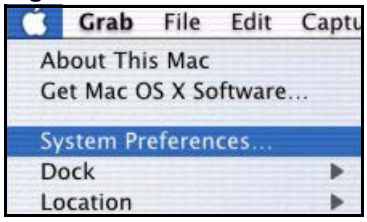
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 76 Macintosh OS X: Apple Menu

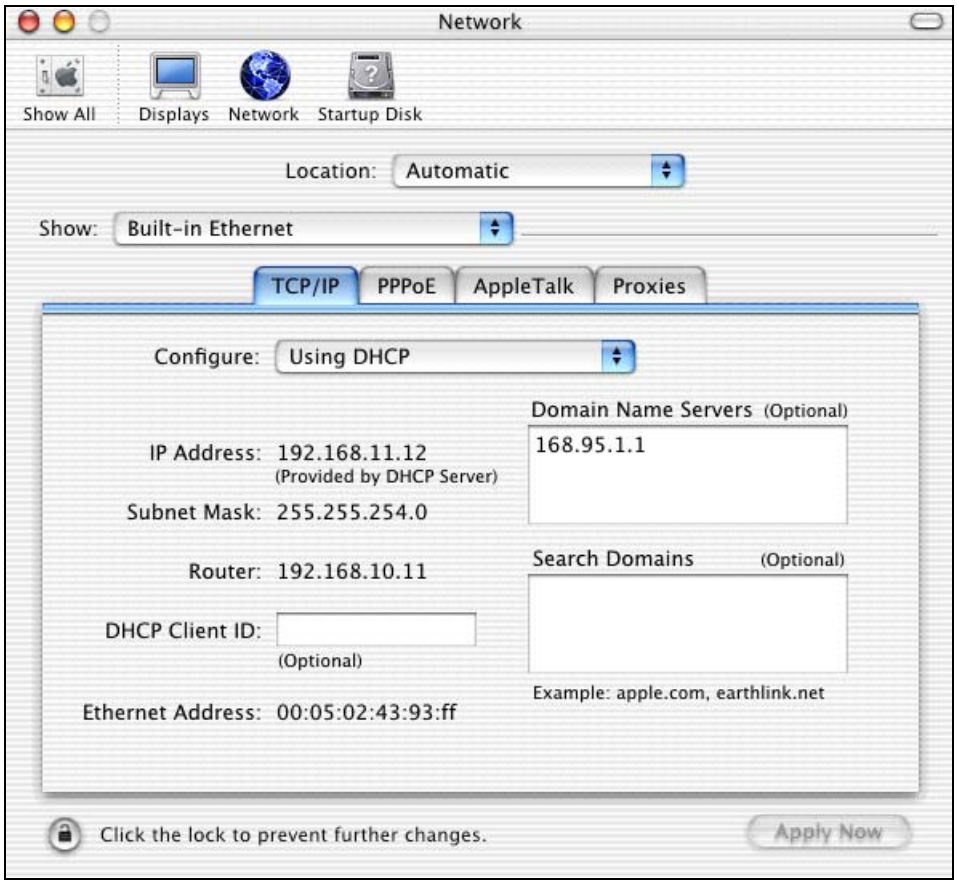


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 77 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL G-220 v2 in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL G-220 v2 and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Index

A

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z