M-302

802.11g Wireless MIMO PCI card

User's Guide

Version 2.00
Edition 1
4/2006

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.

Certifications

Federal Communications Commission (FCC) Interference Statement

This 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:

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

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 Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://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.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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

Note

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

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization 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.

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	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.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 M-302 802.11g Wireless MIMO PCI card.

The M-302 uses Multiple-in, Multiple-Out (MIMO) twin antenna technology to provide superior wireless performance.

Your M-302 is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your M-302 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. It contains 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.

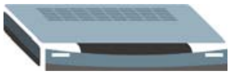
User Guide Feedback

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 M-302 802.11g Wireless MIMO PCI card may be referred to as the M-302 in this user’s guide.

Graphics Icons Key

Wireless Access Point 	Computer 	Notebook Computer
Server 	Modem 	Wireless Signal
Internet Cloud 	Printer 	

CHAPTER 1 Getting Started

This chapter introduces the M-302 and prepares you to use the ZyXEL utility. The ZyXEL utility is a tool that helps you configure your M-302. See the appendix for detailed product specifications.

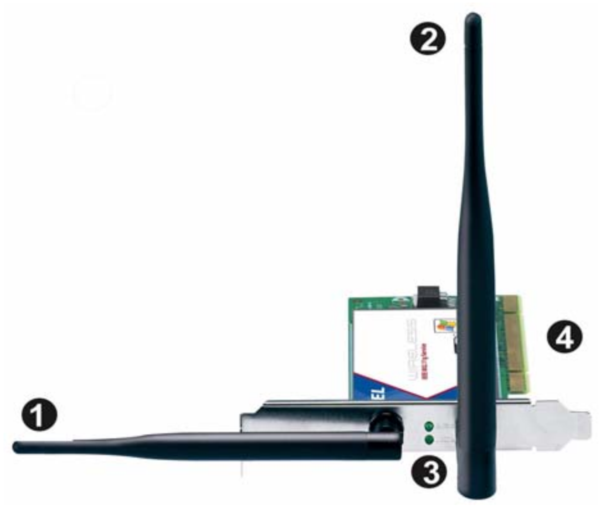
1.1 About Your M-302

The M-302 is an IEEE 802.11b/g compliant wireless Local Area Network (LAN) adapter. Fitting directly into an open PCI slot in your desktop computer's motherboard, the M-302 allows you to access wireless networks at speeds of up to 108Mbps (with the **Super G** function enabled). You can either set the network type to **Infrastructure** and connect to an access point (AP) or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

The following lists the main features of your M-302. See the product specifications in the appendix for detailed features.

- Multiple-In, Multiple-Out (MIMO) wireless technology.
- Automatic data rate selection.
- Security: WEP (Wired Equivalent Privacy), IEEE 802.1x, WPA-PSK and WPA (Wi-Fi Protected Access)
- A fixed antenna.
- Driver and utility support for Windows 2000 and Windows XP.

Figure 1 The M-302



The following table describes the M-302.

Table 1 External View

LABEL	DESCRIPTION
1	Removable antenna (5dBi, R-SMA connector)
2	Fixed antenna
3	Power (PWR) and Link (LNK) lights
4	PCI contacts

The following table describes the operation of the Power (**PWR**) and Link (**LNK**) lights on the rear of the device.

Table 2 Light Description

STATUS	PWR LIGHT	LNK LIGHT
Power off	The light is off.	The light is off.
Power on	The light blinks slowly.	The light is off.
Power on, device disabled	The light is on.	The light is off.
Searching for wireless network	Both lights blink in series	
Connected to wireless network (no traffic)	Both lights blink together slowly	
Connected to wireless network (traffic)	Both lights blink together rapidly	

1.1.1 Application Overview

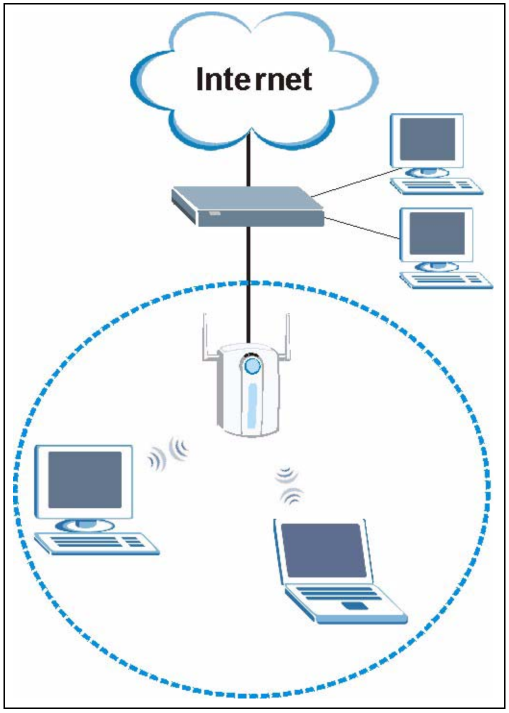
This section describes some network applications for the M-302.

1.1.1.1 Infrastructure

To connect to a network via an Access Point (AP), set the M-302 network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

Note: For more information on switching between Infrastructure and Ad-Hoc modes, refer to Section 4.4 on page 44.

Figure 2 Application: Infrastructure

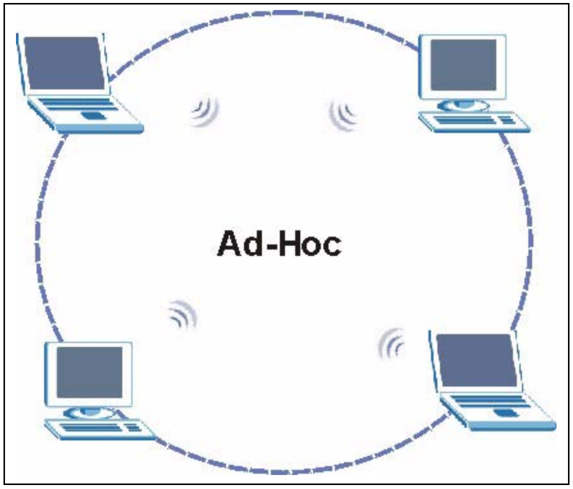


1.1.1.2 Ad-Hoc

If you want to set up a small independent wireless workgroup without an AP, use **Ad-Hoc** mode.

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

Figure 3 Application: Ad-Hoc



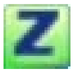
1.2 M-302 Hardware and Utility Installation

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

1.3 ZyXEL Utility Icon

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

Figure 4 ZyXEL utility: System Tray Icon



Note: The ZyXEL utility system tray icon displays only when the M-302 is installed properly.

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

The color of the ZyXEL utility system tray icon indicates the status of the M-302. Refer to the following table for details.

Table 3 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The M-302 is not connected to a wireless network or is searching for an available wireless network.
Green	The M-302 is connected to a wireless network.

1.4 Configuration Methods

To configure your M-302, use one of the following applications:

- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool)
- ZyXEL Utility (This guide shows you how to configure the M-302 using the ZyXEL utility)
- Odyssey Client Manager (not supplied)

  Refer to the Odyssey Client Manager documentation for more information.

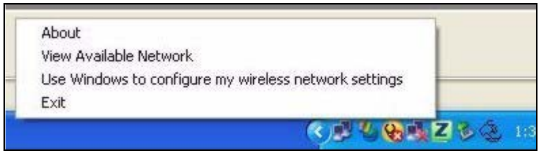
Note: Do NOT use WZC or the Odyssey Client Manager at the same time you use the ZyXEL utility.

1.5 Enabling WZC

Note: When you use the ZyXEL utility, it automatically disables WZC.

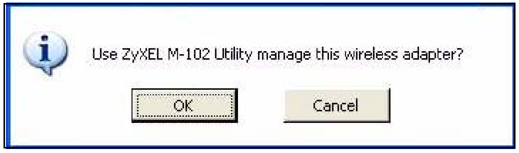
If you want to use WZC to configure the M-302, you need to disable the ZyXEL utility by right-clicking the utility icon (Z) in the system tray and selecting **Use Windows to configure my wireless network settings**.

Figure 5 Enable WZC



To reactivate the ZyXEL utility, double-click the Z icon and click **OK**.

Figure 6 Enable ZyXEL Utility



Use ZyXEL M-102 Utility manage this wireless adapter?

Refer to the appendices on how to use WZC to manage the M-302.

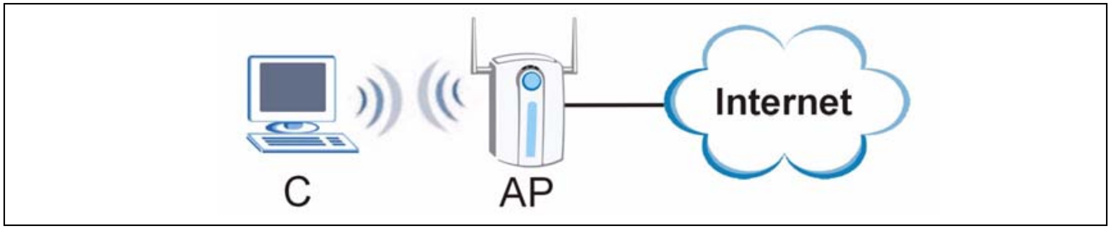
1.5.1 Accessing the ZyXEL Utility

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 in this User's Guide.

Note: Click the ? icon (located in the top right corner) to display the online help window.

CHAPTER 2
Tutorial

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



There are three ways to connect the wireless client to a network.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This tutorial shows you how to manually connect to a network, and how to configure a profile.

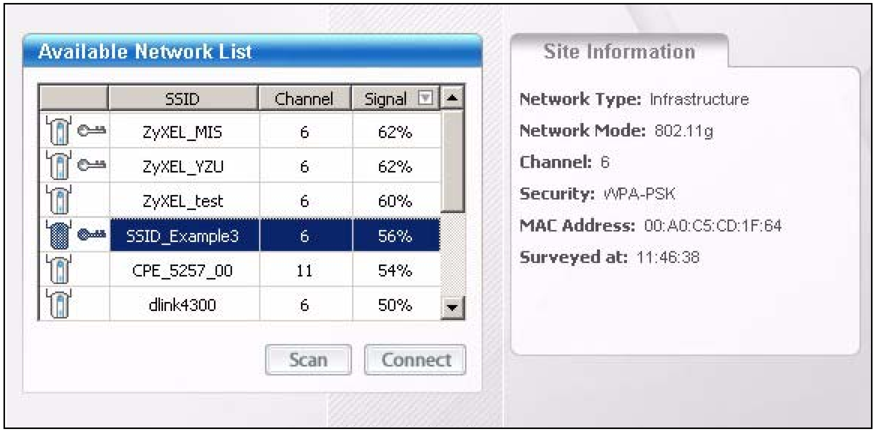
2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) configured for WPA-PSK security. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the Site Survey screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

Figure 7 ZyXEL Utility: Site Survey



Available Network List

	SSID	Channel	Signal
🔑	ZyXEL_MIS	6	62%
🔑	ZyXEL_YZU	6	62%
	ZyXEL_test	6	60%
🔑	SSID_Example3	6	56%
	CPE_5257_00	11	54%
	dlink4300	6	50%

Site Information

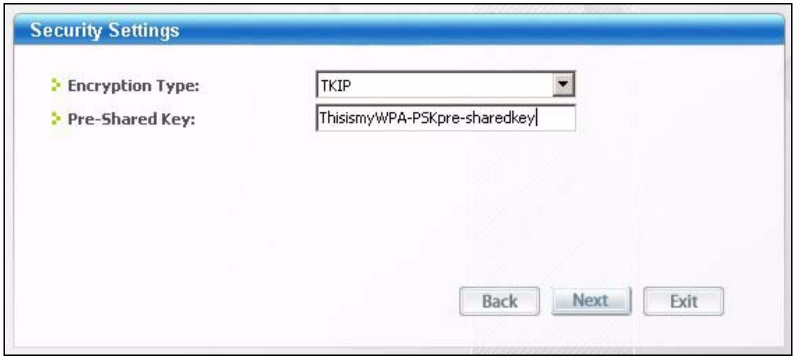
Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WPA-PSK
MAC Address: 00:A0:C5:CD:1F:64
Surveyed at: 11:46:38

2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer.

3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 8 ZyXEL Utility: Security Settings

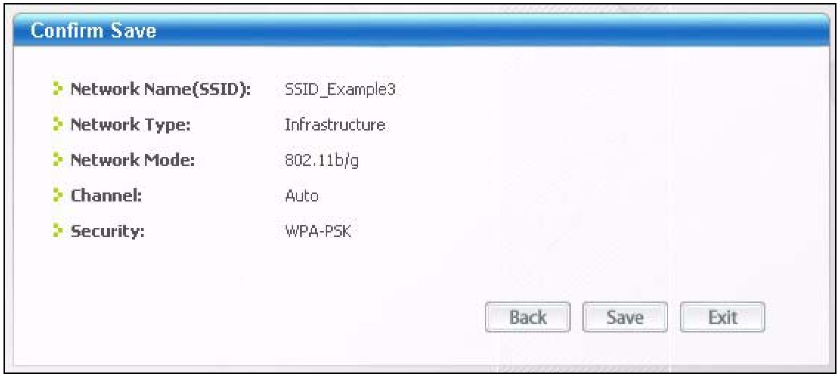


Security Settings

Encryption Type: TKIP
Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 9 ZyXEL Utility: Confirm Save

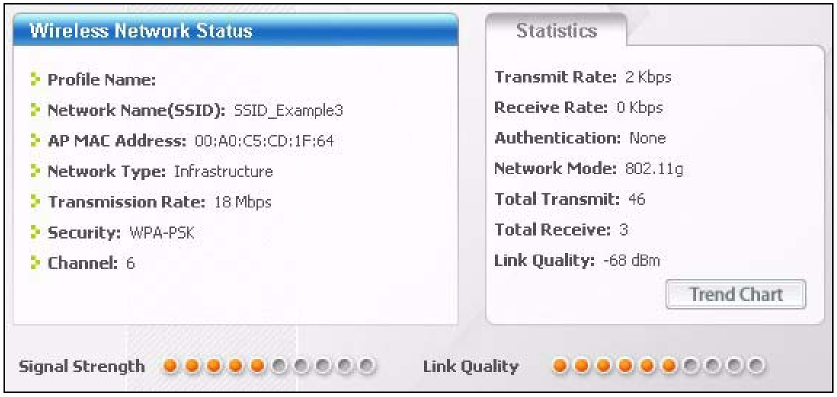


Confirm Save

- Network Name(SSID): SSID_Example3
- Network Type: Infrastructure
- Network Mode: 802.11b/g
- Channel: Auto
- Security: WPA-PSK

5 The ZyXEL Utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL Utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 10 ZyXEL Utility: Link Info



Wireless Network Status

- Profile Name:
- Network Name(SSID): SSID_Example3
- AP MAC Address: 00:A0:C5:CD:1F:64
- Network Type: Infrastructure
- Transmission Rate: 18 Mbps
- Security: WPA-PSK
- Channel: 6

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: None
Network Mode: 802.11g
Total Transmit: 46
Total Receive: 3
Link Quality: -68 dBm

6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other Web site in the address bar. If you are able to access the Web site, your wireless connection is successfully configured.

If you cannot access the Web site, check the Troubleshooting section of this User's Guide or contact your network administrator.

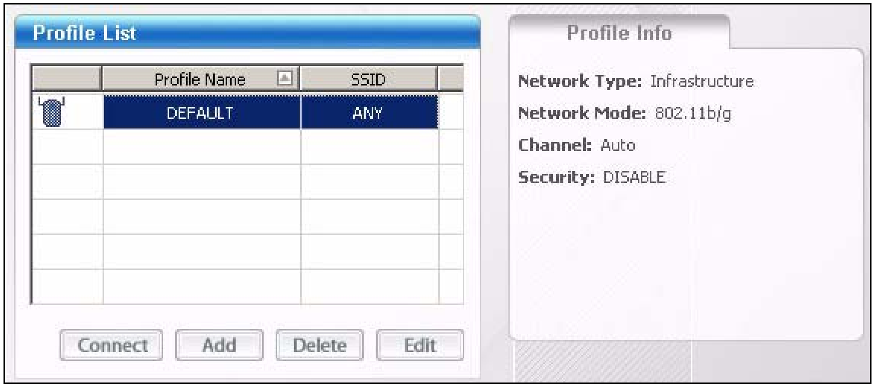
2.2 Creating and Using a Profile

A profile lets your wireless client connect to the same wireless network every time you use the ZyXEL Utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the AP’s SSID is “SSID_Example3” and its pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the Profile Name “PN_Example3”

1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 11 ZyXEL Utility: Profile



Profile List

Profile Name	SSID
DEFAULT	ANY

Profile Info

Network Type: Infrastructure

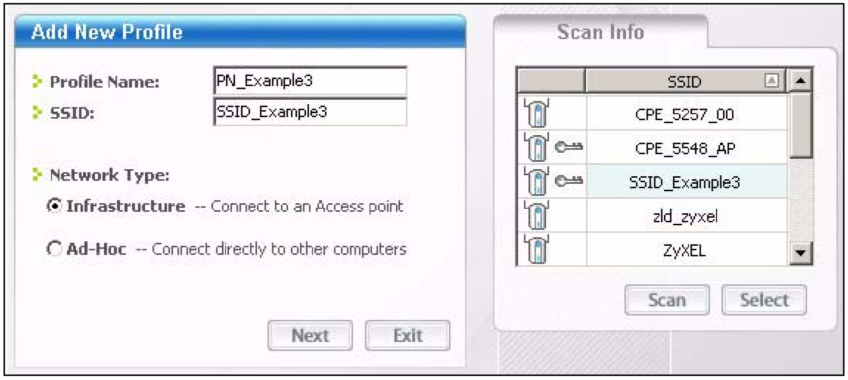
Network Mode: 802.11b/g

Channel: Auto

Security: DISABLE

2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

Figure 12 ZyXEL Utility: Add New Profile



Add New Profile

Profile Name: PN_Example3

SSID: SSID_Example3

Network Type:

● Infrastructure -- Connect to an Access point

○ Ad-Hoc -- Connect directly to other computers

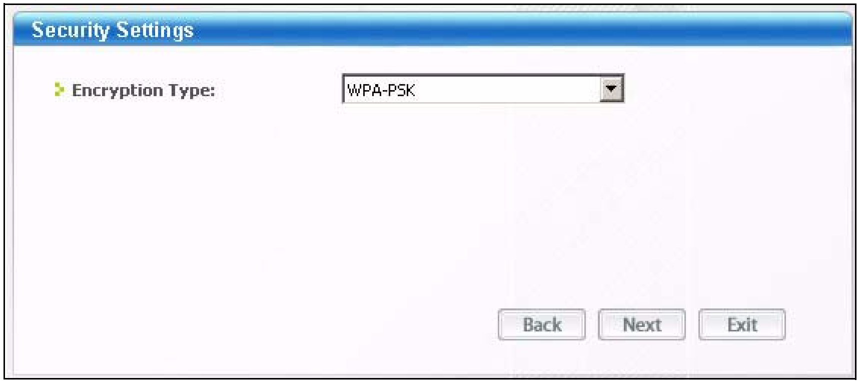
Scan Info

SSID
CPE_5257_00
CPE_5548_AP
SSID_Example3
zld_zyxel
ZyXEL

3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select the **Infrastructure** button and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

Figure 13 ZyXEL Utility: Profile Security

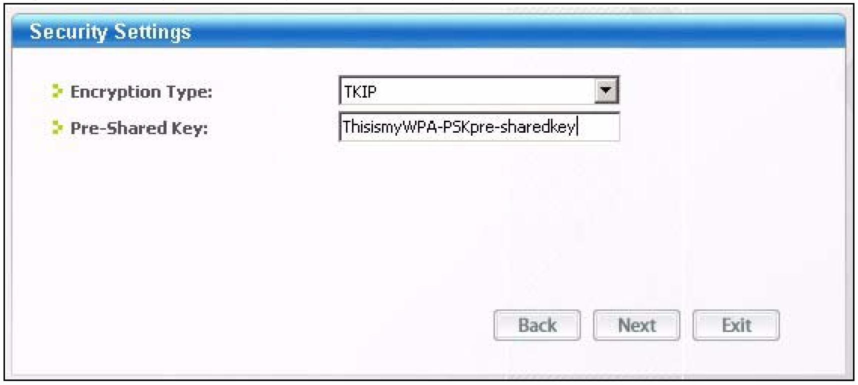


Security Settings

Encryption Type: WPA-PSK

5 This screen varies depending on the encryption method you selected in the previous screen. In this example, enter the pre-shared key and leave the encryption type at the default setting.

Figure 14 ZyXEL Utility: Profile Encryption



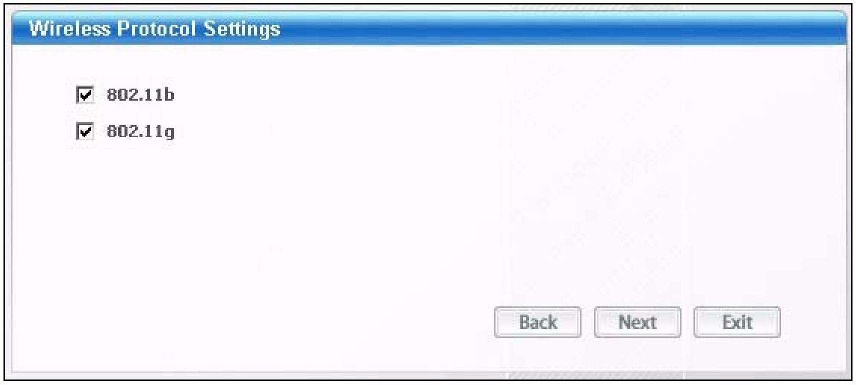
Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 In the next screen, leave both boxes checked.

Figure 15 ZyXEL Utility: Wireless Protocol Settings.



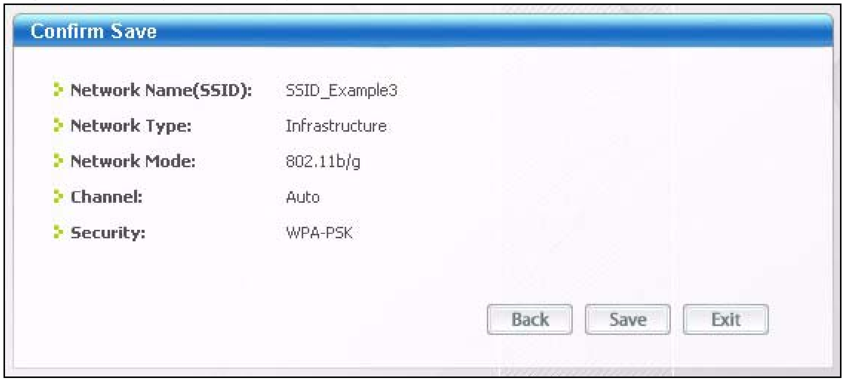
Wireless Protocol Settings

☑ 802.11b

☑ 802.11g

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

Figure 16 ZyXEL Utility: Save Profile



Confirm Save

Network Name(SSID): SSID_Example3

Network Type: Infrastructure

Network Mode: 802.11b/g

Channel: Auto

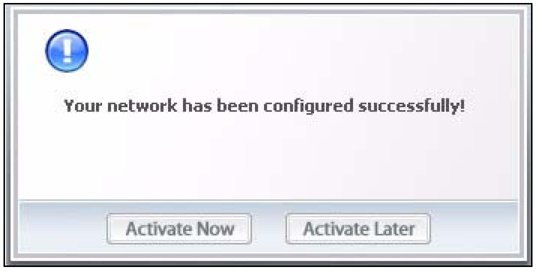
Security: WPA-PSK

8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

Figure 17 ZyXEL Utility: Profile Success



Your network has been configured successfully!

9 When you activate the new profile, the ZyXEL Utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL Utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10Open your Internet browser, enter http://www.zyxel.com or the URL of any other Web site in the address bar and press ENTER. If you are able to access the Web site, your new profile is successfully configured.

If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

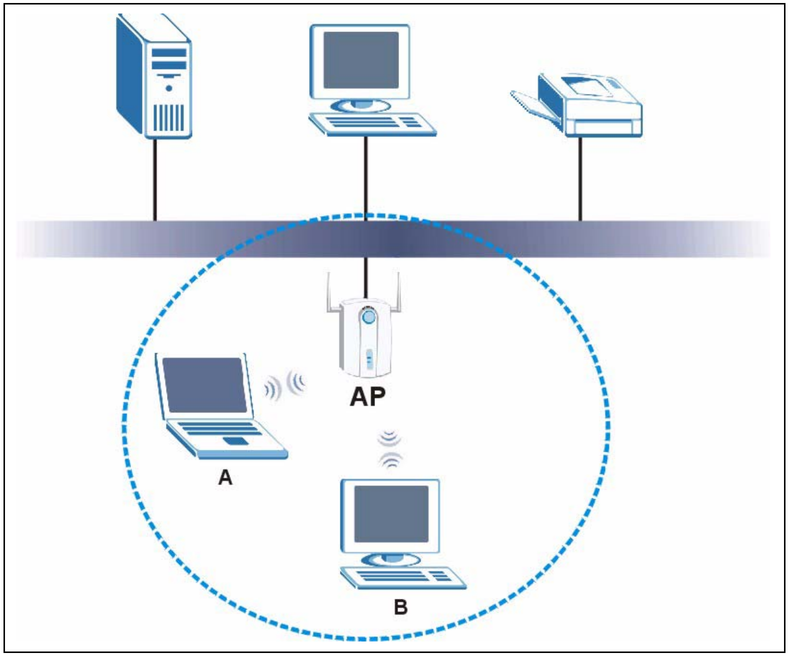
CHAPTER 3 Wireless LAN Network

This chapter provides background information on wireless LAN networks.

3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 3 on page 21 for an Ad Hoc network example.

Figure 18 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

3.2 Wireless LAN Security

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

Configure the wireless LAN security using the **Profile Security Settings** screen. If you do not enable any wireless security on your M-302, the M-302's wireless communications are accessible to any wireless networking device that is in the coverage area.See the appendices for more detailed information about wireless security.

3.2.1 User Authentication and Encryption

User authentication is when every user must log in to the wireless network before they can use it. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

3.2.1.1 WEP

3.2.1.1.1 Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the M-302 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 M-302.

- 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 Settings screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

  Your M-302 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.

3.2.1.1.2 Authentication Type

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication 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 or peer computer do not share a secret key (WEP key). Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- Shared Key mode involves a shared secret key (WEP key) to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- Auto authentication mode allows the M-302 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.

3.2.1.2 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.

3.2.1.2.1 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 M-302 supports EAP-TLS, EAP-TTLS and EAP-PEAP. Refer to the appendix on wireless security for more details.

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 a digital ID) can be used to authenticate users, and a CA issues certificates and guarantees the identity of each certificate owner.

3.2.1.3 WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP. Refer to the appendix on wireless security for more details.

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

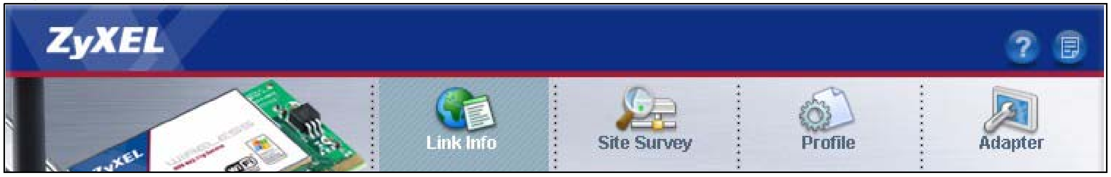
CHAPTER 4
ZyXEL Utility Configuration

This chapter shows you how to configure your M-302.

4.1 ZyXEL Utility Screen

This section describes the ZyXEL utility screens.

Figure 19 ZyXEL Utility: Menu Screen



The following table describes the menus.

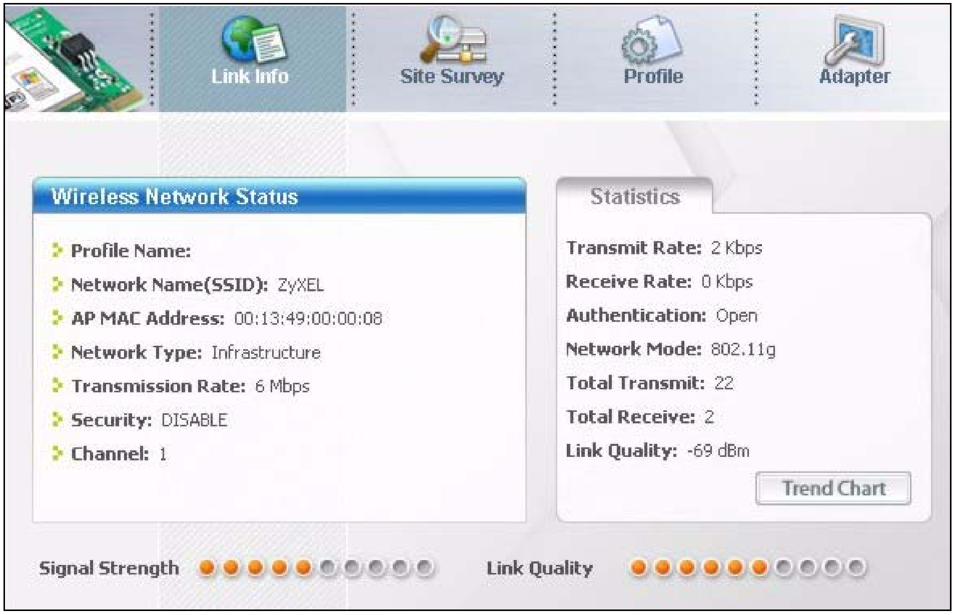
Table 4 ZyXEL Utility: Menu Screen

TAB	DESCRIPTION
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.
Adapter	Use this screen to configure a transfer rate and enable power saving.

4.2 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your M-302.

Figure 20 Link Info



Wireless Network Status

- Profile Name:
- Network Name(SSID): ZyXEL
- AP MAC Address: 00:13:49:00:00:08
- Network Type: Infrastructure
- Transmission Rate: 6 Mbps
- Security: DISABLE
- Channel: 1

Statistics

Transmit Rate: 2 Kbps
Receive Rate: 0 Kbps
Authentication: Open
Network Mode: 802.11g
Total Transmit: 22
Total Receive: 2
Link Quality: -69 dBm

Signal Strength ●●●●●○○○○○ Link Quality ●●●●●●○○○○

The following table describes the labels in this screen.

Table 5 Link Info

LABEL	DESCRIPTION
Wireless Network Status	
Profile Name	This is the name of the profile you are currently using.
Network Name (SSID)	The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the M-302 is associated.
AP MAC Address	This field displays the MAC address of the AP or peer computer to which the M-302 is associated.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless network.
Transmission Rate	This field displays the current transmission rate of the M-302 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP** (WEP or 802.1x), **TKIP** (WPA/WPA-PSK), **AES** (WPA/WPA-PSK)) or inactive (**Disable**).
Channel	This field displays the radio channel the M-302 is currently using.
Statistics	
Transmit Rate	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive Rate	This field displays the current data receiving rate in kilobits per second (Kbps).
Authentication	This field displays the authentication method of the M-302.
Network Mode	This field displays the network standard (**802.11b** or **802.11g**) of the AP or peer computer.
Total Transmit	This field displays the total number of data frames transmitted.
Total Receive	This field displays the total number of data frames received.
Link Quality	This field displays the quality of the signal of the M-302.

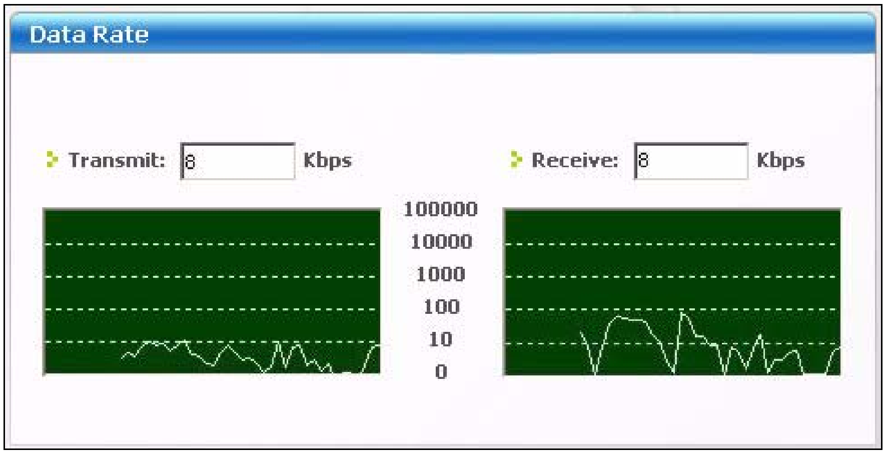
Table 5 Link Info (continued)

LABEL	DESCRIPTION
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. The signal strength depends mainly on the antenna output power and the distance between the M-302 and the AP or peer computer.
Link Quality	The status bar shows the quality of the wireless connection. This refers to the percentage of packets delivered successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength.

4.2.1 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 21 Link Info: Trend Chart



Data Rate

Transmit: 8 Kbps

Receive: 8 Kbps

The following table describes the labels in this screen.

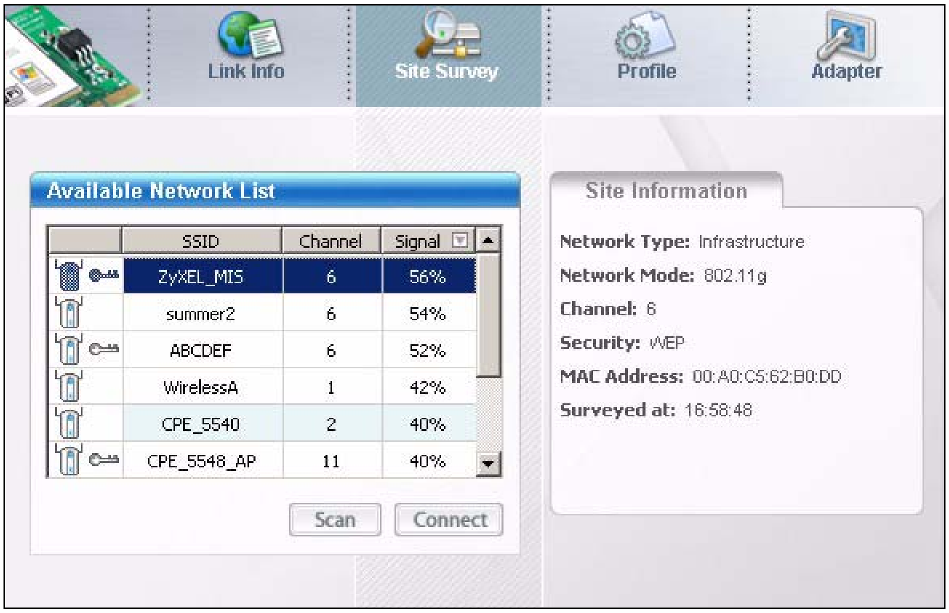
Table 6 Link Info: Trend Chart

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).

4.3 The Site Survey Screen

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

Figure 22 Site Survey



Available Network List

	SSID	Channel	Signal
	ZyXEL_MIS	6	56%
	summer2	6	54%
	ABCDEF	6	52%
	WirelessA	1	42%
	CPE_5540	2	40%
	CPE_5548_AP	11	40%

Site Information

Network Type: Infrastructure
Network Mode: 802.11g
Channel: 6
Security: WEP
MAC Address: 00:A0:C5:62:B0:DD
Surveyed at: 16:58:48

The following table describes the labels in this screen.

Table 7 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 Information	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.	
Network Mode	This fields displays the network standard (**802.11g** or **802.11b**) of the wireless device.	
Channel	This field displays the channel number used by each wireless device.	

Table 7 Site Survey

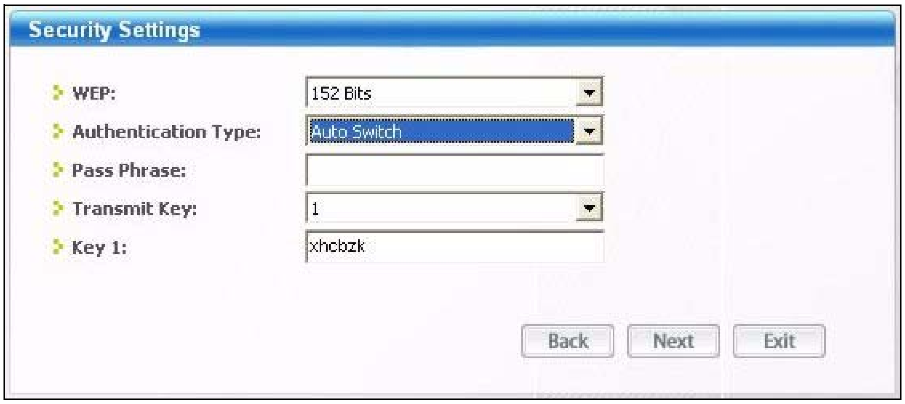
LABEL	DESCRIPTION
Security	This field shows whether data encryption is activated. If WPA is activated, **WPA** displays. If WPA-PSK is activated, **WPA-PSK** displays. If WEP or 802.11x is activated, **WEP** displays. If security is inactive, **Disable** displays.
MAC Address	This field displays the MAC address of the wireless device.
Surveyed at	This field displays the time when the wireless device is scanned.

4.3.1 Security Settings

When you configure the M-302 to connect to a network with wireless security activated and the security settings are disabled on the M-302, the screen varies according to the encryption method used by the selected network.

4.3.1.1 WEP Encryption

Figure 23 Security Settings: WEP



Security Settings

WEP: 152 Bits

Authentication Type: Auto Switch

Pass Phrase:

Transmit Key: 1

Key 1: xhcbzk

The following table describes the labels in this screen.

Table 8 Security Settings: WEP

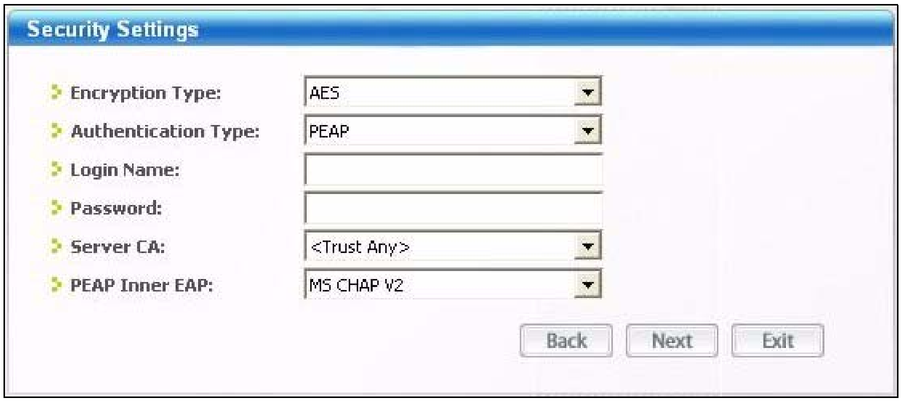
LABEL	DESCRIPTION
WEP	Select **64 Bits**, **128 Bits** or **152 Bits** to activate WEP encryption and then fill in the related fields.
Authentication Type	Select authentication type. Choices are **Auto Switch**, **Open** and **Shared**. Refer to Section 3.2.1.1.2 on page 33 for more information.
Pass Phrase	Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the M-302 automatically generates four different WEP keys and displays it in the key field below. Refer to Section 3.2.1 on page 32 for more information. At the time of writing, you cannot use passphrase to generate 152-bit WEP keys.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.

Table 8 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 **152 Bits** in the **WEP** field, Enter either 32 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCCDDEEFF) for HEX key type or Enter 16 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678901) 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 other network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.2 WPA

Figure 24 Security Settings: WPA



Security Settings

Encryption Type: AES

Authentication Type: PEAP

Login Name:

Password:

Server CA: <Trust Any>

PEAP Inner EAP: MS CHAP V2

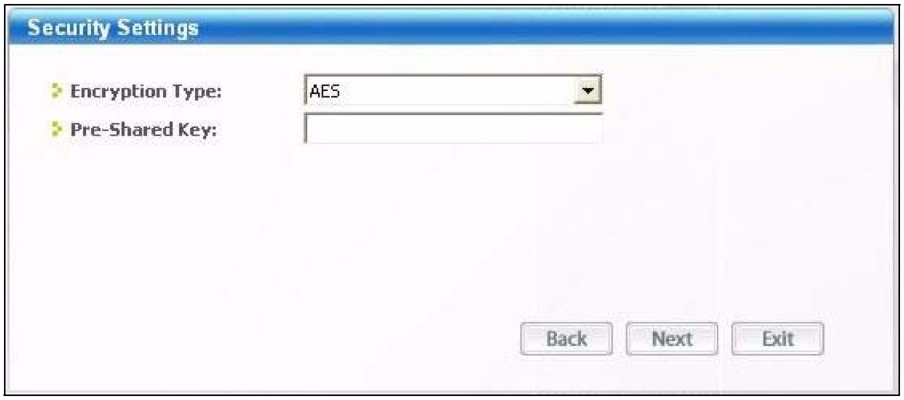
The following table describes the labels in this screen.

Table 9 Security Settings: WPA

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.1.3 on page 33 for more information.
Authentication Type	Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **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 used by the authentication server to authenticate the M-302. **Note:** You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA).
Server CA	Select a certificate authority (CA) that you trust and accept any certificates signed by that CA. Otherwise, select **Trust Any** to accept certificates from any CA.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. Select a PEAP protocol. Options are **GTC** and **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to other network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.3 WPA-PSK

Figure 25 Security Settings: WPA-PSK



Security Settings

Encryption Type: AES

Pre-Shared Key:

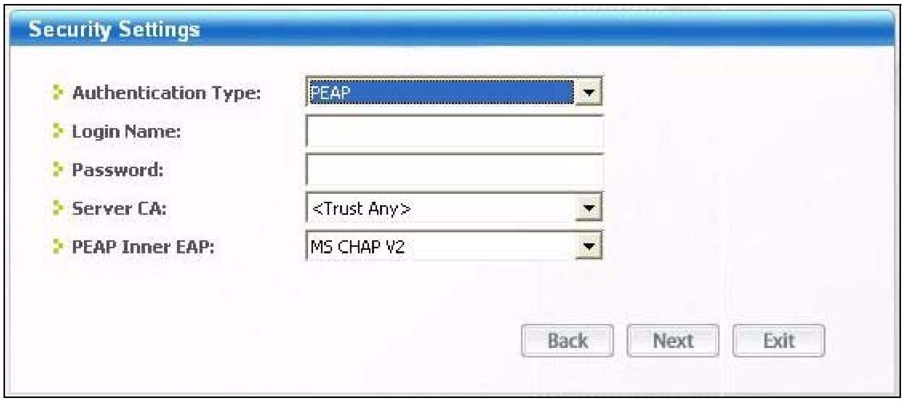
The following table describes the labels in this screen.

Table 10 Security Settings: WPA-PSK

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.1.3 on page 33 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).
Back	Click **Back** to go to the **Site Survey** screen to select and connect to other network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.4 IEEE 802.1x

Figure 26 Security Settings: 802.1x



Security Settings

Authentication Type: PEAP

Login Name:

Password:

Server CA: <Trust Any>

PEAP Inner EAP: MS CHAP V2

The following table describes the labels in this screen.

Table 11 Security Settings: 802.1x

LABEL	DESCRIPTION
Authentication Type	The type of authentication you use depends on the authentication server or AP. Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password	This field is not available when you select **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 used by the authentication server to authenticate the M-302. **Note:** You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA).

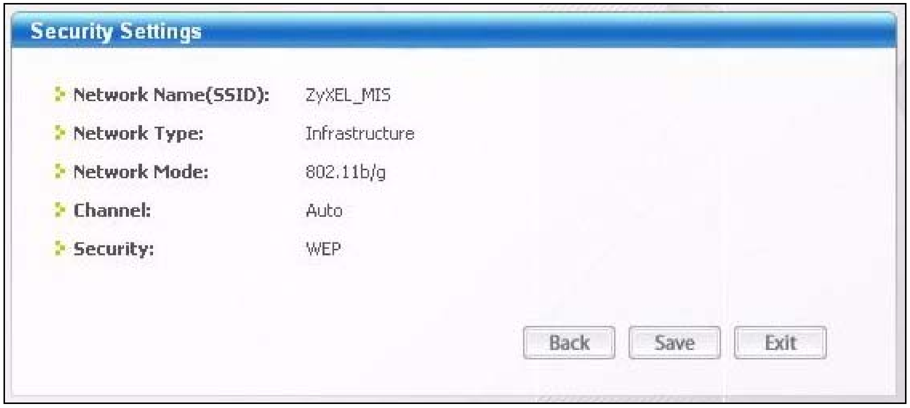
Table 11 Security Settings: 802.1x

LABEL	DESCRIPTION
Server CA	Select a certificate authority (CA) that you trust and accept any certificates signed by that CA. Otherwise, select **Trust Any** to accept certificates from any CA.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. Select a PEAP protocol. Options are **GTC** and **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to other network.
Next	Click **Next** to confirm your selections and advance to the **Confirm Save** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.2 Confirm Save Screen

Use this screen to confirm and save the security settings.

Figure 27 Confirm Save Screen



Security Settings

Network Name(SSID): ZyXEL_MIS
Network Type: Infrastructure
Network Mode: 802.11b/g
Channel: Auto
Security: WEP

The following table describes the labels in this screen.

Table 12 Confirm Save Screen

LABEL	DESCRIPTION
Network Name (SSID)	This field displays the **SSID** previously entered.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless device.
Network Mode	This fields displays the network standard (**802.11g**, **802.11b** or **802.11b/g**) 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**, **802.1x**, **WPA** or **WPA-PSK**) or inactive (**DISABLE**).
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save the changes back to the M-302 and display the **Link Info** screen.
Exit	Click **Exit** to discard changes and return to the **Site Survey** screen.

4.4 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 M-302 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 M-302 will remain disconnected.

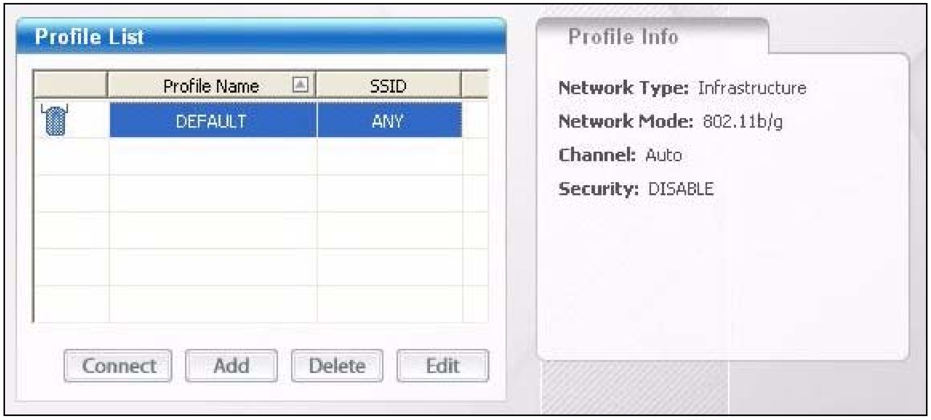
If you do not configure and activate a profile, each time you start the M-302 it uses the default profile to connect to any available network with security disabled.

The default profile allows you to connect to any wireless network 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 28 Profile Screen



Profile List

	Profile Name	SSID
	DEFAULT	ANY

Profile Info

Network Type: Infrastructure
Network Mode: 802.11b/g
Channel: Auto
Security: DISABLE

The following table describes the labels in this screen.

Table 13 Profile Screen

LABEL	DESCRIPTION	
Profile 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.
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 associates.	
Connect	To use and activate a previously saved network profile, select a pre-configured profile name in the table and click **Connect**.	

Table 13 Profile Screen (continued)

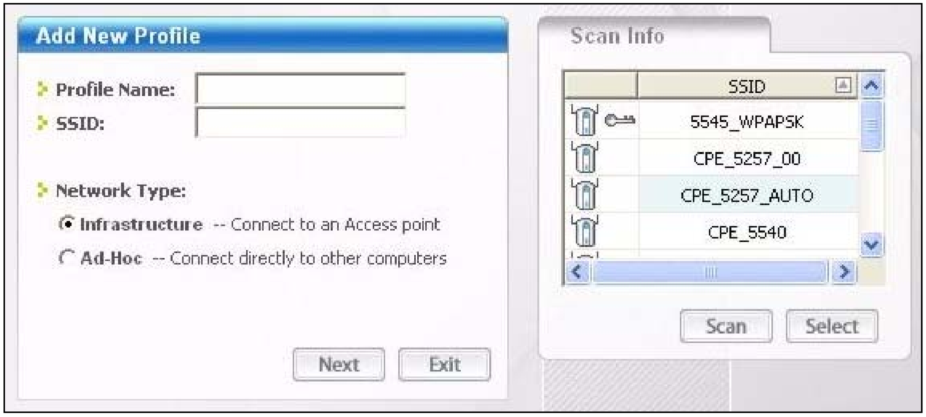
LABEL	DESCRIPTION
Add	To add a new profile into the table, click **Add**.
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.
Profile 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.
Network Mode	This fields displays the network standard (**802.11g**, **802.11b** or **802.11b/g**) 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**, **802.1x**, **WPA-PSK**, **WPA**) or inactive (**Disable**).

4.4.1 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 29 Profile: Add New Profile



Add New Profile

Profile Name:

SSID:

Network Type:

● Infrastructure -- Connect to an Access point

○ Ad-Hoc -- Connect directly to other computers

Scan Info

	SSID
	5545_WPAPSK
	CPE_5257_00
	CPE_5257_AUTO
	CPE_5540

The following table describes the labels in this screen.

Table 14 Profile: Add New Profile

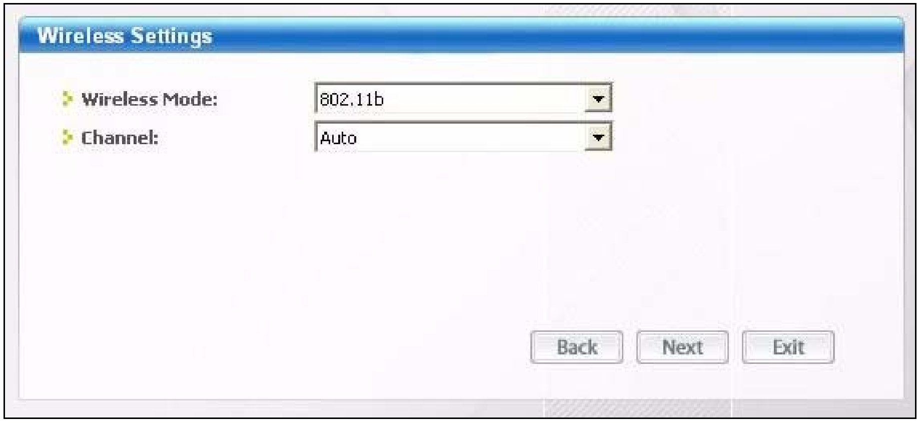
LABEL	DESCRIPTION
Add New Profile	
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the M-302 associate to or roam between any infrastructure wireless networks.

Table 14 Profile: Add New Profile (continued)

LABEL	DESCRIPTION
Network Type	Select **Infrastructure** to associate to an AP. Select **Ad-Hoc** to associate to a peer computer
Next	Click **Next** to go to the next screen.
Exit	Click **Exit** to go back to the previous screen without saving.
Scan Info	This table displays the information of the available wireless networks within the transmission range.
	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 AP or peer 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 M-302 associates to the selected wireless network only.

2 If you selected the **Infrastructure** network type in the previous screen, skip to step 3. If you selected the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a channel number and click **Next** to continue.

Figure 30 Profile: Wireless Setting: Select a Channel



Wireless Settings

Wireless Mode: 802.11b

Channel: Auto

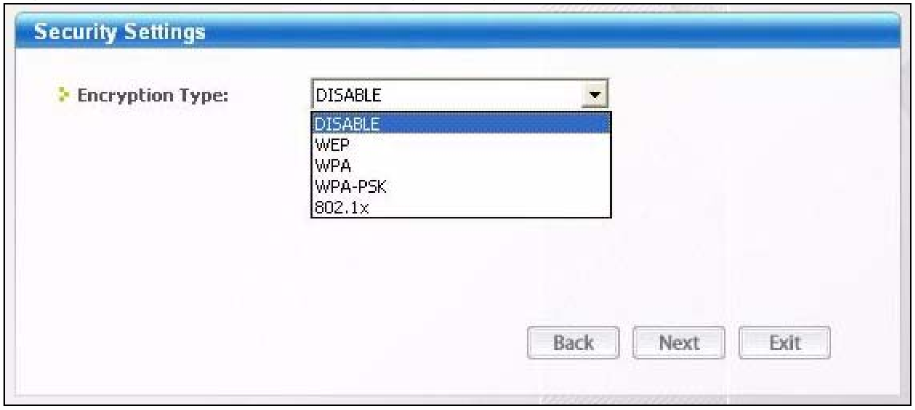
The following table describes the labels in this screen.

Table 15 Profile: Wireless Setting: Select a Channel

LABEL	DESCRIPTION
Wireless Settings	
Wireless Mode	When configuring for an Ad-Hoc network 802.11b mode is used.
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.
Back	Click **Back** to return to the **Add New Profile** screen.
Next	Click **Next** to confirm your selection and advance to the **Encryption Type** screen.
Exit	Click **Exit** to discard changes and return to the **Add New Profile** screen.

3 If you selected **Infrastructure** network type in the first screen, select **WEP**, **WPA**, **WPA-PSK** or **802.1x** from the drop-down list box to enable data encryption. If you selected **Ad-Hoc** network type in the first screen, you can only use **WEP** encryption method. Otherwise, select **DISABLE** to allow the M-302 to communicate with the access points or other peer wireless computers without any data encryption and skip to step 5.

Figure 31 Profile: Security Setting: Encryption Type

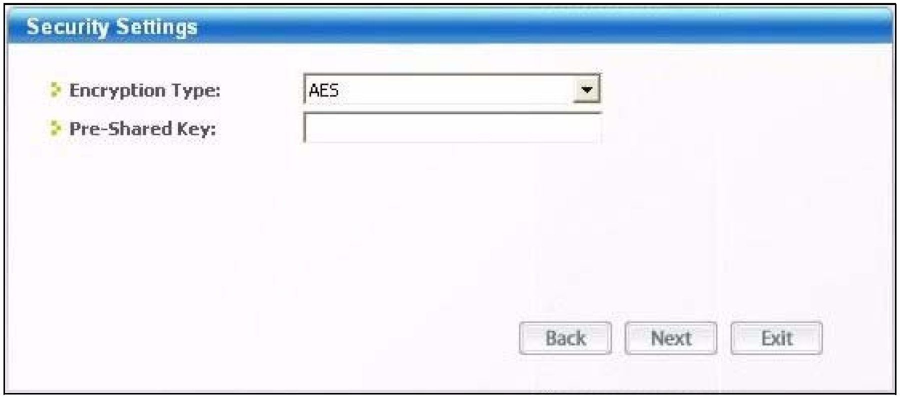


Security Settings

Encryption Type: DISABLE

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 M-302.

Figure 32 Profile: Security Setting



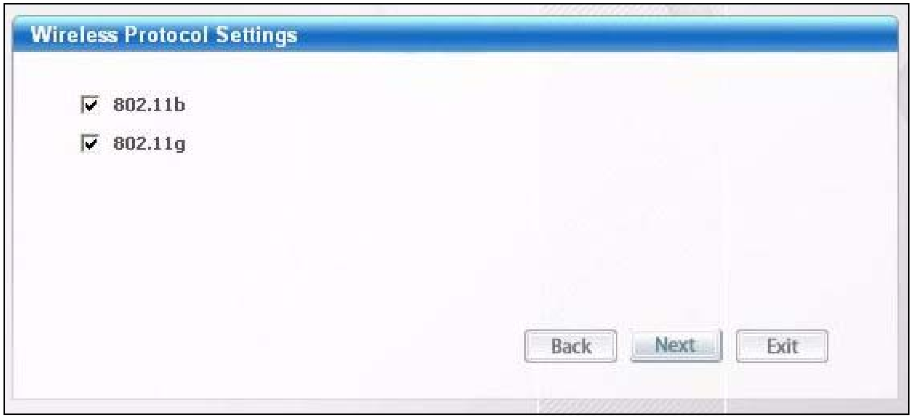
Security Settings

Encryption Type: AES

Pre-Shared Key:

5 If you selected **Ad-Hoc** network type in the first screen, skip to the next step. If you selected **Infrastructure** network type, specify a wireless protocol. Select **802.11b** to have the M-302 connect to an IEEE 802.11b wireless device. Select **802.11g** to have the M-302 connect to an IEEE 802.11g wireless device. Select both to have the M-302 connect to either an IEEE 802.11g or IEEE 802.11b wireless device.

Figure 33 Profile: Wireless Protocol



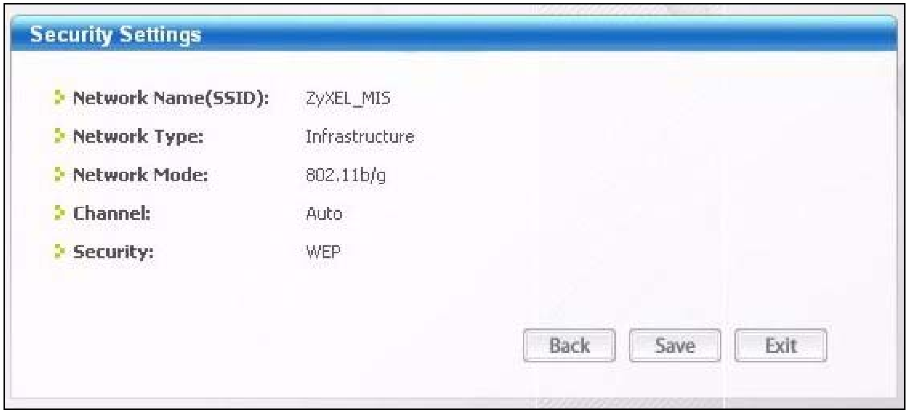
Wireless Protocol Settings

☑ 802.11b

☑ 802.11g

6 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 34 Profile: Confirm New Settings



Security Settings

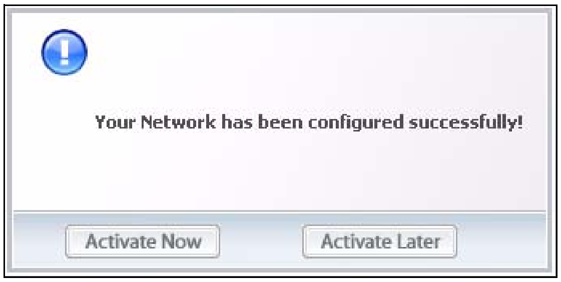
Network Name(SSID):	ZyXEL_MIS
Network Type:	Infrastructure
Network Mode:	802.11b/g
Channel:	Auto
Security:	WEP

7 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.

You can activate only one profile at a time.

Figure 35 Profile: Activate the Profile

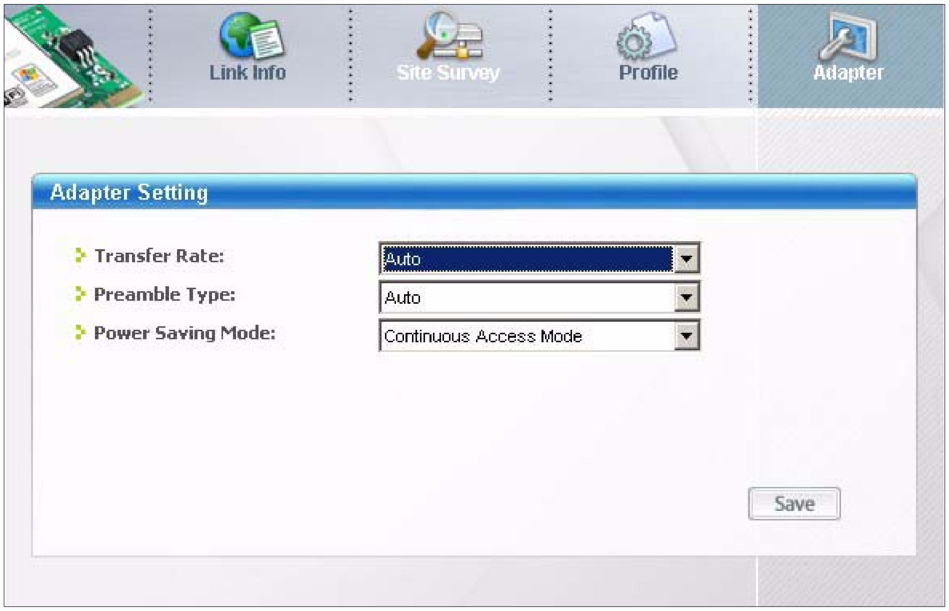


Your Network has been configured successfully!

4.5 The Adapter Screen

To set the advanced features on the M-302, click the **Adapter** tab.

Figure 36 Adapter Screen



Transfer Rate: Auto

Preamble Type: Auto

Power Saving Mode: Continuous Access Mode

The following table describes the labels in this screen.

Table 16 Adapter Screen

LABEL	DESCRIPTION
Adapter Setting	
Transfer Rate	In most networking scenarios, the factory default **Fully Auto** setting is the most efficient and allows your M-302 to operate at the highest possible transfer (data) rate. If you want to select a specific transfer rate, select one that the AP or peer wireless device supports. **Note:** Super G The **Super G** technology works with IEEE 802.11 a/b/g products. It doubles IEEE 802.11g performance by bonding two 54Mbps channels and allowing larger frames to be sent. Your M-302 can transmit at up to 108 Mbps when connected to an AP or wireless router with the **Super G** feature enabled.
Preamble Type	Preamble is used to signal that data is coming to the receiver. Select the preamble type that the AP uses. **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 **Auto** to have the M-302 automatically use short preamble when all access point or wireless stations support it; otherwise the M-302 uses long preamble. **Note:** The M-302 and the access point or wireless stations MUST use the same preamble mode in order to communicate.
Power Saving Mode	Select **Maximum Power Saving** or **Fast Power Saving** to save power (especially for notebook computers). This forces the M-302 to go to sleep mode when it is not transmitting data. When you select **Continuous Access Mode**, the M-302 will never go to sleep mode.
Save	Click **Save** to save the changes back to the M-302.

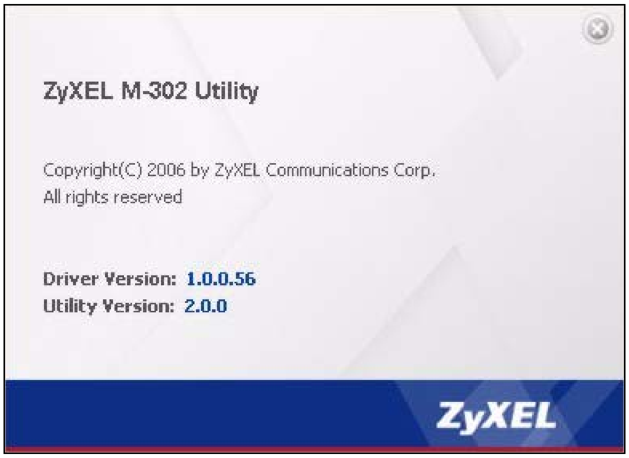
CHAPTER 5 Maintenance

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

5.1 The About Screen

The **About** screen displays driver and utility version numbers of the M-302. To display the screen as shown below, click the about (📄) button.

Figure 37 About Screen



ZyXEL M-302 Utility

Copyright(C) 2006 by ZyXEL Communications Corp.
All rights reserved

Driver Version: 1.0.0.56
Utility Version: 2.0.0

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

Table 17 About Screen

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the M-302 driver.
Utility Version	This field displays the version number of the ZyXEL utility.

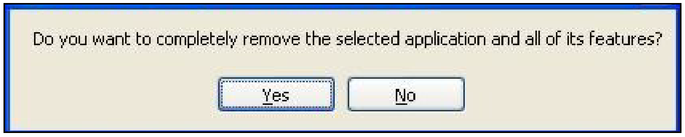
5.2 Uninstalling the ZyXEL Utility

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

1 Click **Start**, **(All) Programs**, **M-302 Utility**, **Uninstall M-302 Utility**.

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

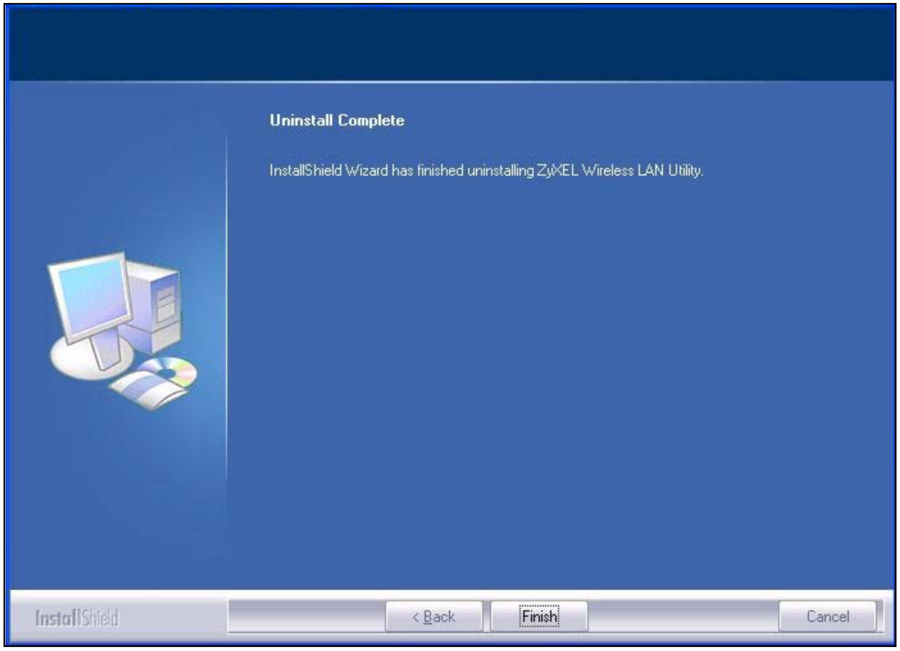
Figure 38 Uninstall: Confirm



Do you want to completely remove the selected application and all of its features?

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

Figure 39 Uninstall: Finish



Uninstall Complete

InstallShield Wizard has finished uninstalling ZyXEL Wireless LAN Utility.

5.3 Upgrading the ZyXEL Utility

Note: Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

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 Remove the current ZyXEL utility from your computer (see Section 5.2 on page 53*)*.

3 Restart your computer when prompted.

4 Disconnect the M-302 from your computer.

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

6 Insert the M-302 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 solve the problem.

6.1 Problems Starting the ZyXEL Utility

Table 18 Troubleshooting Starting the ZyXEL Utility

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Wireless LAN utility	Make sure the M-302 is properly inserted and the LED is on. 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 M-302 under **Network Adapter**. (Steps may vary depending on the version of Windows). Install the M-302 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 with the Link Quality

Table 19 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. Make sure there are not too many wireless stations connected to a wireless network.

6.3 Problems Communicating With Other Computers

Table 20 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The computer with the M-302 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 M-302 computer and the associated AP use the same SSID. • Change the AP and the associated wireless clients to use another radio channel if interference is high. • Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Settings** screen. • If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa. In Ad-Hoc Mode • Verify that the peer computer(s) is turned on. • Make sure the M-302 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. • If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa. • Change the wireless clients to use another radio channel if interference is high.

APPENDIX A
Product Specifications

Table 21 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	M-302 802.11g Wireless MIMO PCI card
Interface	3.3V 32-bit CardBus card
Standards	IEEE 802.11b IEEE 802.11g (Infrastructure mode only)
Network Architectures	Infrastructure Ad-Hoc
Security	64/128/152-bit WEP Encryption WPA/WPA-PSK IEEE 802.1x
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-25 ~ 70 degrees Centigrade
Operating Humidity	0 ~ 70% (non-condensing)
Storage Humidity	10 ~ 90% (non-condensing)
Power Consumption	TX: 620mA RX: 600mA
Voltage	3.3V
Weight	0.09 lbs / 40g
Dimensions	134mm X 119mm X 22mm (without antenna) 158mm X 205mm X22mm (with antenna)
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Frequency	USA (FCC) & Canada 11 Channels: 2.412GHz~2.462GHz Europe (ETSI) 13 Channels: 2.412GHz~2.472GHz Japan (TELEC) 13 Channels: 2.412GHz~2.483GHz
Data Rate	IEEE 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): 108 (Super G mode only), 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11b: 11, 5.5, 2, 1 Mbps
Modulation	11g: OFDM (64QAM, 16QAM, QPSK, BPSK) 11b: PBCC, Direct Sequence Spread Spectrum (DSSS), (CCK, DQPSK, DBPSK)
Output Power	11g: At 54Mbps 16dBm +/-1dBm (typical) 11b: At 11Mbps 18dBm +/-1dBm (typical)
RX Sensitivity	11g: At 54Mbps -74dBm +/- 1dBm (typical) 11b: At 11Mbps -84dBm +/- 1dBm (typical)
SOFTWARE SPECIFICATIONS	

Table 21 Product Specifications (continued)

Device Drivers	Windows 2000, Windows XP
Roaming	IEEE 802.11b/g compliant
WEP	64/128/152-bit WEP encryption

APPENDIX B
Management with Wireless Zero Configuration

This appendix shows you how to manage your ZyXEL wireless LAN adapter 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.

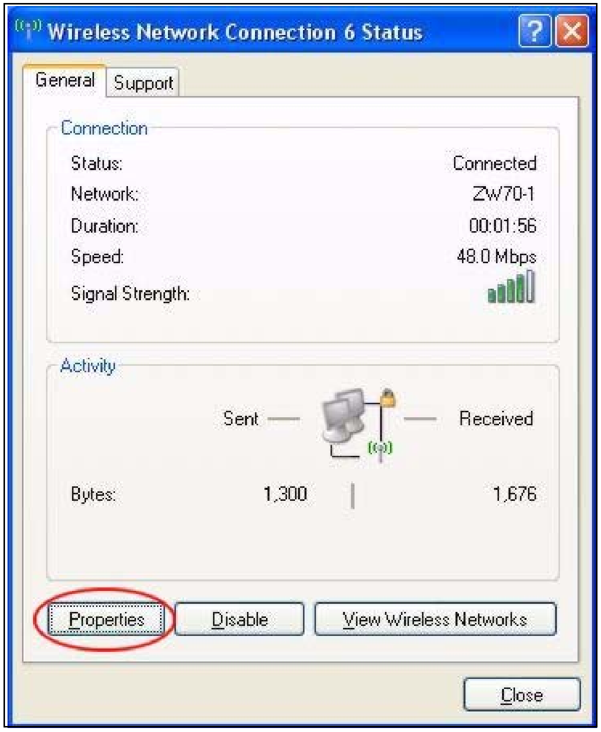
Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon (?) in most screens, move the cursor to the item that you want the information about and click to view the help.

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.

1 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 40 Windows XP SP2: Wireless Network Connection Status

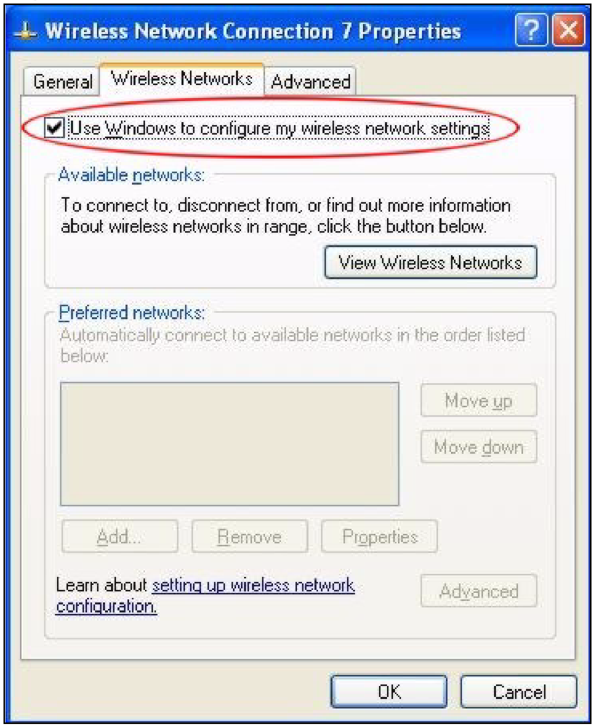


Status: Connected
Network: ZW70-1
Duration: 00:01:56
Speed: 48.0 Mbps
Signal Strength:

Bytes: 1,300 | 1,676

4 In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is selected. Click **OK**.

Figure 41 Windows XP SP2: Wireless Network Connection Properties



☑ Use Windows to configure my wireless network settings

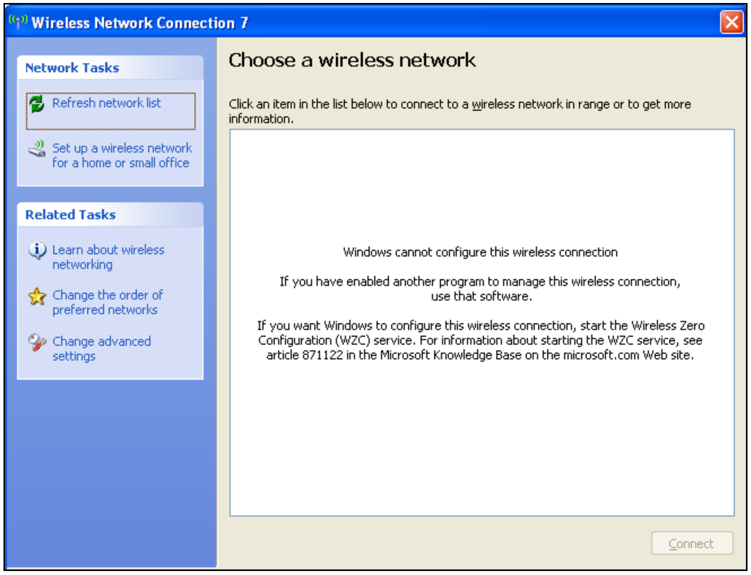
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

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

Figure 42 Windows XP SP2: WZC Not Available



Wireless Network Connection 7
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Windows cannot configure this wireless connection

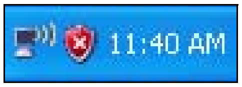
If you have enabled another program to manage this wireless connection, use that software.

If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.

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 43 Windows XP SP2: System Tray Icon



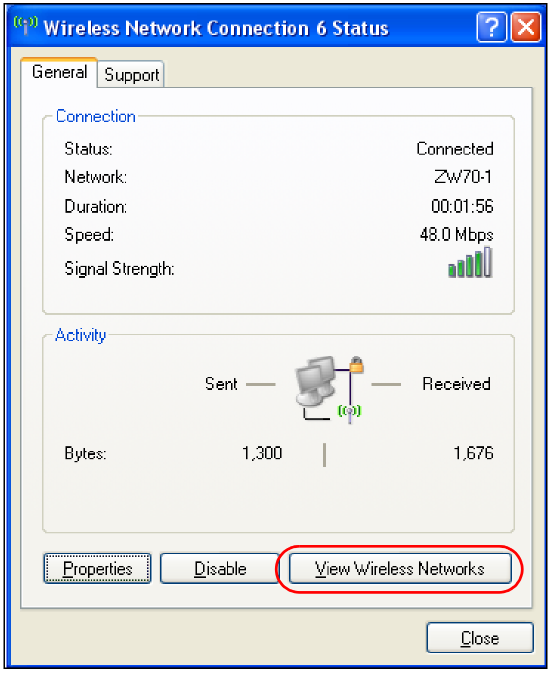
The type of the wireless network icon in Windows XP SP2 indicates the status of the ZyXEL wireless LAN adapter. Refer to the following table for details.

Table 22 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The ZyXEL wireless LAN adapter is connected to a wireless network.
	The ZyXEL wireless LAN adapter 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 wireless LAN adapter 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 44 Windows XP SP2: Wireless Network Connection Status



Connection

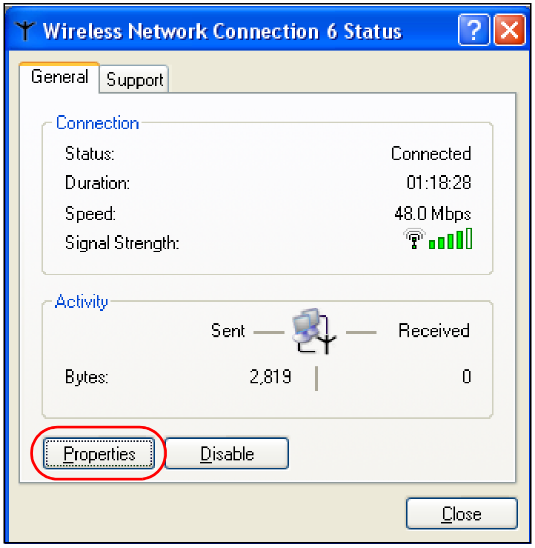
Status: Connected
Network: ZW70-1
Duration: 00:01:56
Speed: 48.0 Mbps
Signal Strength:

Activity

Sent — — Received
Bytes: 1,300 | 1,676

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 45 Windows XP SP1: Wireless Network Connection Status



Connection

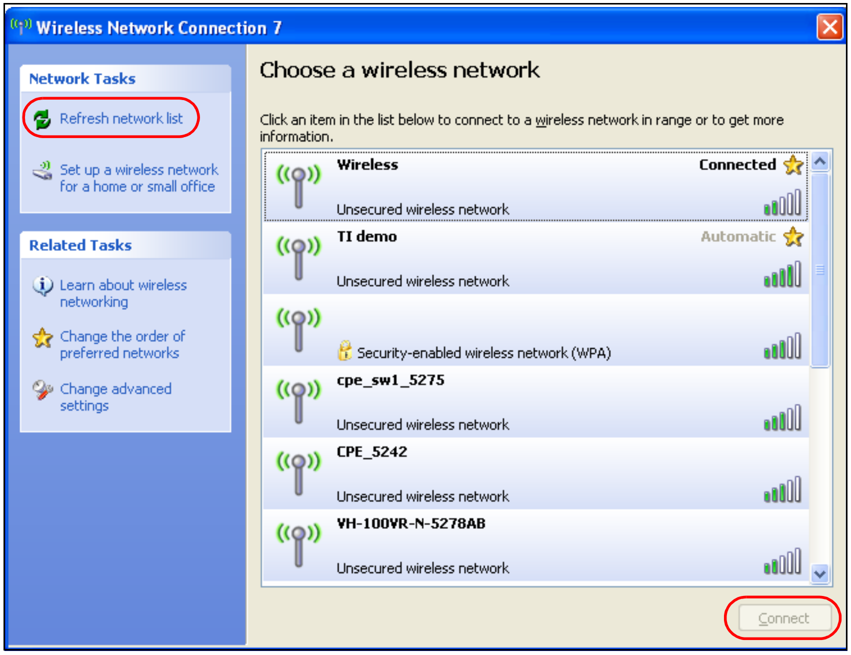
Status: Connected
Duration: 01:18:28
Speed: 48.0 Mbps
Signal Strength:

Activity

Sent — — Received
Bytes: 2,819 | 0

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 46 Windows XP SP2: Wireless Network Connection



Wireless Network Connection 7

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Wireless — Connected ★ — Unsecured wireless network

TI demo — Automatic ★ — Unsecured wireless network

Security-enabled wireless network (WPA)

cpe_sw1_5275 — Unsecured wireless network

CPE_5242 — Unsecured wireless network

VH-100VR-N-5278AB — Unsecured wireless network

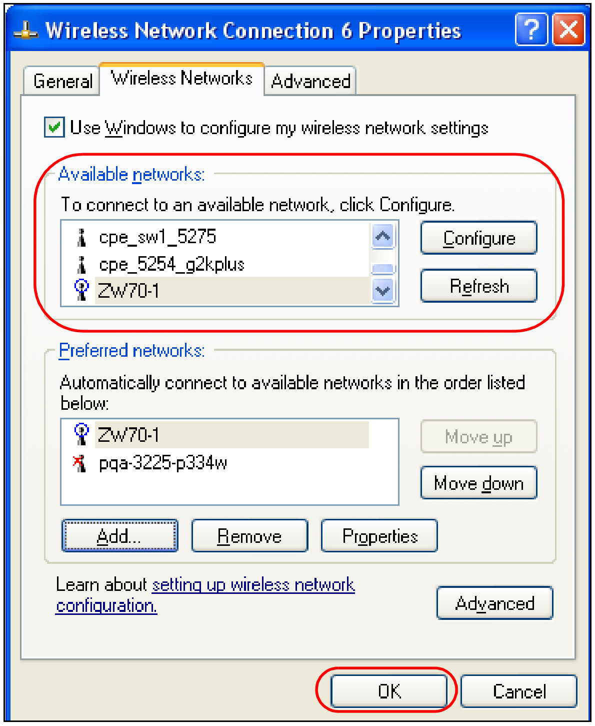
The following table describes the icons in the wireless network list.

Table 23 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 wireless LAN adapter 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 47 Windows XP SP1: Wireless Network Connection Properties



Wireless Network Connection 6 Properties

General | Wireless Networks | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

Preferred networks:

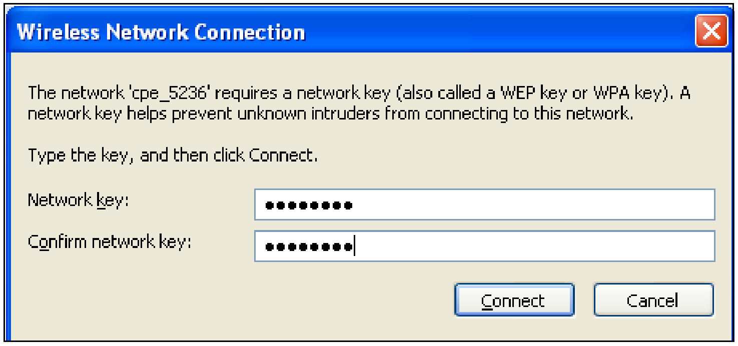
Automatically connect to available networks in the order listed below:

- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

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



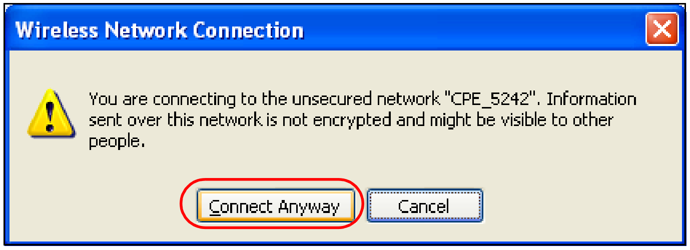
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Figure 49 Windows XP SP2: Wireless Network Connection: No Security



You are connecting to the unsecured network "CPE_5242". Information sent over this network is not encrypted and might be visible to other people.

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 24 Windows XP: Wireless Networks

ICON	DESCRIPTION
📶	This denotes the wireless network is an available wireless network.
📶	This denotes the ZyXEL wireless LAN adapter is associated to the wireless network.
✗	This denotes the wireless network is not available.

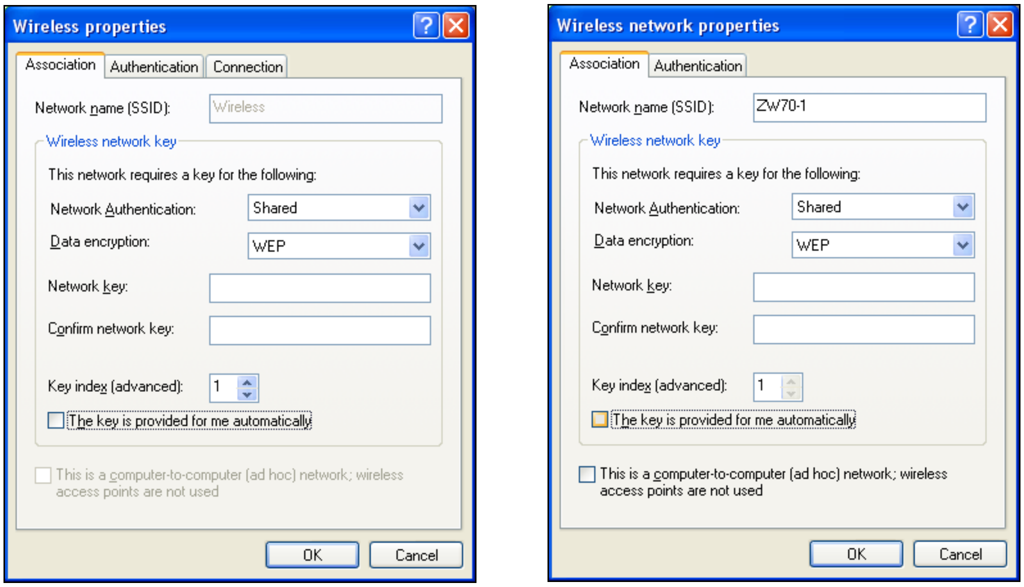
Security Settings

When you configure the ZyXEL wireless LAN adapter to connect to a secure network but the security settings are not yet enabled on the ZyXEL wireless LAN adapter, 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 50 Windows XP: Wireless (network) properties: Association



Wireless properties

Network name (SSID): Wireless

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network properties

Network name (SSID): ZW70-1

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

The following table describes the labels in this screen.

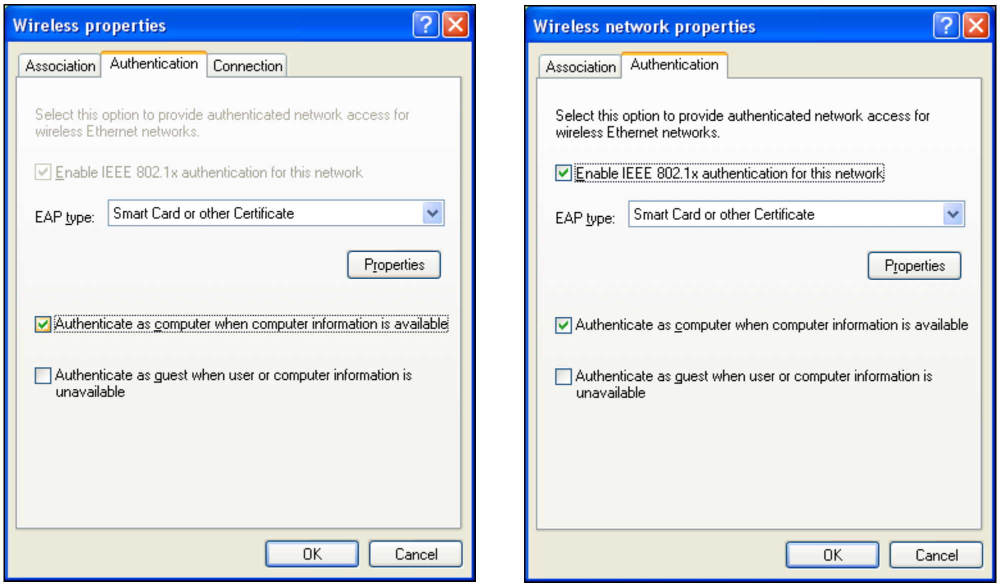
Table 25 Windows XP: Wireless (network) properties: Association

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 wireless LAN adapter a key.
This is a computer-to-computer (ad hoc) network; wireless access points are not used	If this check box is selected, you are connecting to another computer directly.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

Authentication

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

Figure 51 Windows XP: Wireless (network) properties: Authentication



Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

The following table describes the labels in this screen.

Table 26 Windows XP: Wireless (network) properties: Authentication

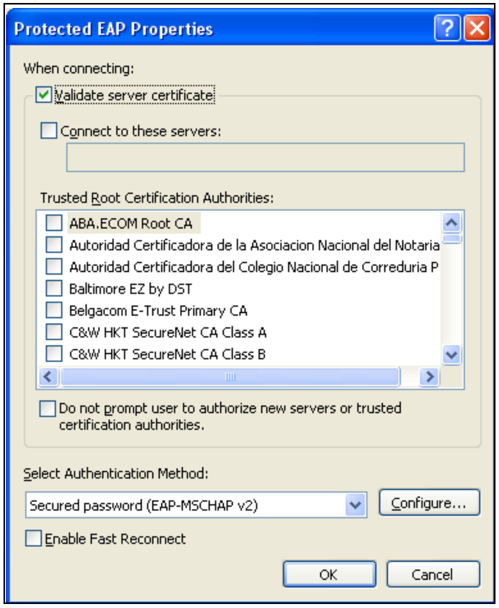
LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication.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



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria P
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

The following table describes the labels in this screen.

Table 27 Windows XP: Protected EAP Properties

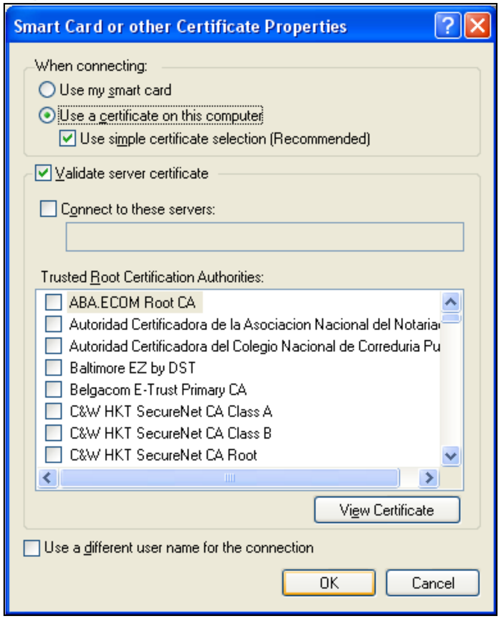
LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root 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.

Table 27 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
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 53 Windows XP: Smart Card or other Certificate Properties



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B
□ C&W HKT SecureNet CA Root

□ Use a different user name for the connection

The following table describes the labels in this screen.

Table 28 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.

Table 28 Windows XP: Smart Card or other Certificate Properties

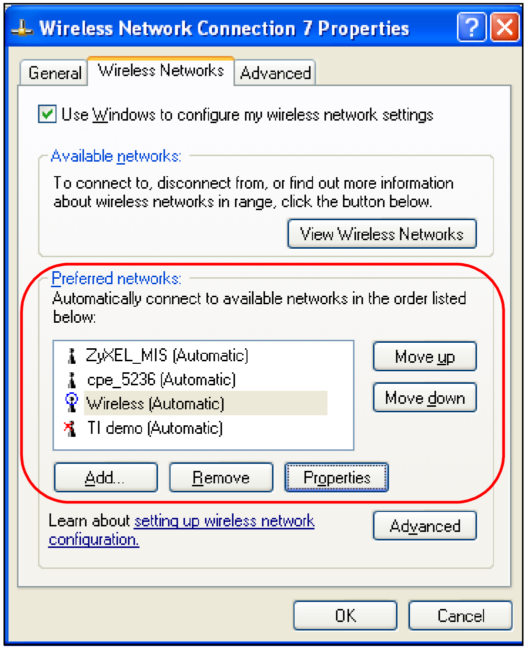
LABEL	DESCRIPTION
Use a different user name for the connection:	Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** 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 46 on page 63). The screen displays as shown.

Figure 54 Windows XP SP2: Wireless Networks: Preferred Networks



Wireless Network Connection 7 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

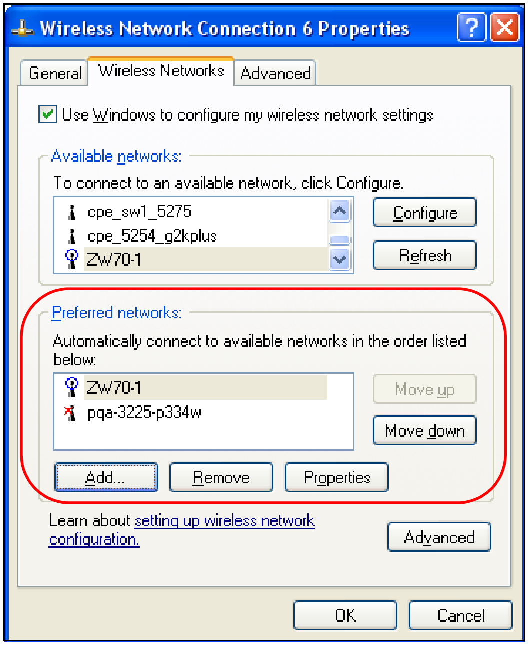
Automatically connect to available networks in the order listed below:

- ZyXEL_MIS (Automatic)
- cpe_5236 (Automatic)
- Wireless (Automatic)
- TI demo (Automatic)

Learn about setting up wireless network configuration.

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

Figure 55 Windows XP SP1: Wireless Networks: Preferred Networks



Wireless Network Connection 6 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

Preferred networks:

Automatically connect to available networks in the order listed below:

- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

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

APPENDIX C
Wireless Security

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

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.

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 a digital ID) can be used to authenticate users, and a CA issues certificates and guarantees the identity of each certificate owner.

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 29 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

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.

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

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

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA uses 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 regularly changes 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 and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs 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

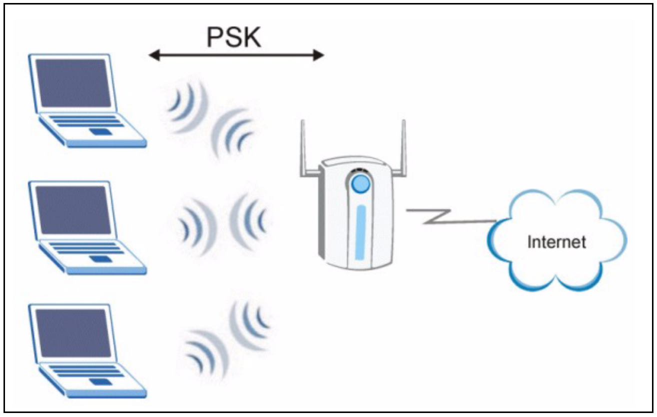
WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

WPA-PSK Application Example

A WPA-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 56 WPA-PSK Authentication

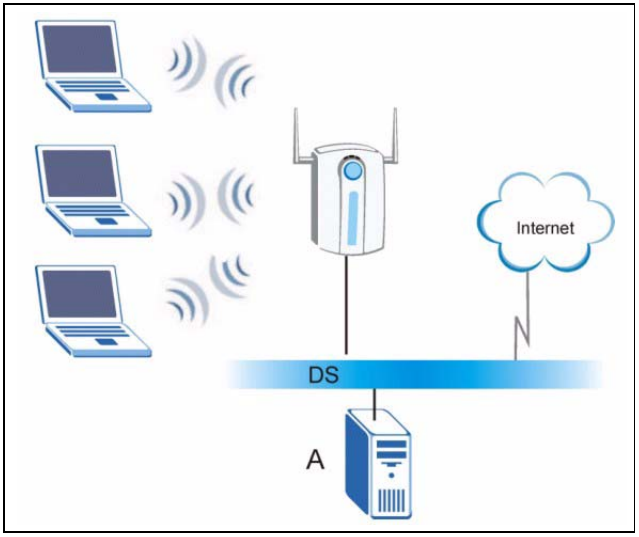


WPA with RADIUS Application Example

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

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 57 WPA 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 30 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

Index