ZyXEL AG-320

802.11a/g Wireless CardBus Card

User's Guide

Version 1.00
Edition 1
9/2006

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

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Radiation Exposure Statement

- The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

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

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

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This product has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

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.

ZyXEL Limited Warranty

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

Note

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

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

Online Registration

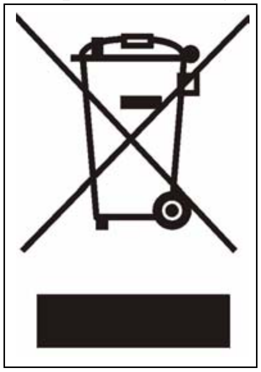
Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Safety Warnings

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

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.

This product is recyclable. Dispose of it properly.



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	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	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
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	

METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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		
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	

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyXEL AG-320 802.11a/g Wireless CardBus Card.

Your AG-320 is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your AG-320 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 Web Site

  Please go to http://www.zyxel.com for product news, firmware, updated documents, and other support materials.

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 right angle bracket For example, “In Windows, click **Start** > **Settings** > **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The ZyXEL AG-320 802.11a/g Wireless CardBus Card may be referred to as the AG-320 or “the device” in this user’s guide.

Graphics Icons Key

Wireless Access Point 	Computer 	Notebook Computer
Server 	Modem or Router 	Wireless Signal
Internet Cloud 		

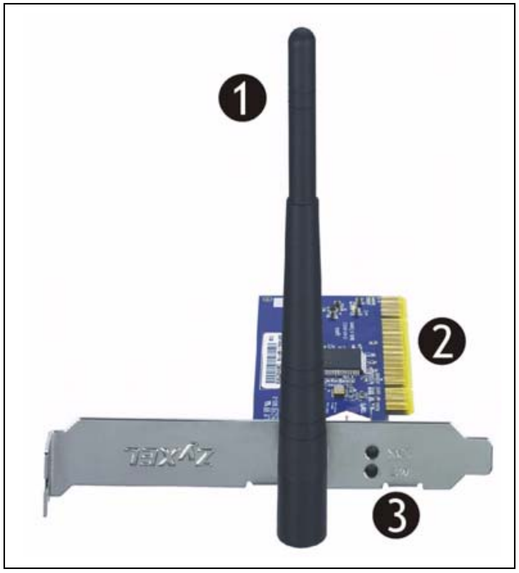
CHAPTER 1 Getting Started

This chapter introduces the AG-320 and prepares you to use the ZyXEL utility.

1.1 About Your AG-320

The AG-320 is an IEEE 802.11a/b/g compliant wireless LAN adapter. You can also use the ZyXEL utility to turn your AG-320 into an access point (AP). The ZyXEL utility is a tool that helps you configure your AG-320. See the appendix for detailed product specifications.

Figure 1 The AG-320



The following table describes the AG-320.

Table 1 External View

LABEL	DESCRIPTION
1	Removable antenna (5dBi, R-SMA connector)
2	PCI contacts
3	LEDs (lights)

The following table describes the operation of the **LINK** and **ACT** LEDs on the rear of the device.

Table 2 AG-320 LEDs

LED	STATE	DESCRIPTION
LINK	On	The AG-320 is receiving power.
	Off	The AG-320 is not receiving power.
ACT	Blinking	The AG-320 is sending or receiving data.
	Off	The AG-320 is not sending or receiving data.

1.2 Application Overview

This section describes some network applications for the AG-320.

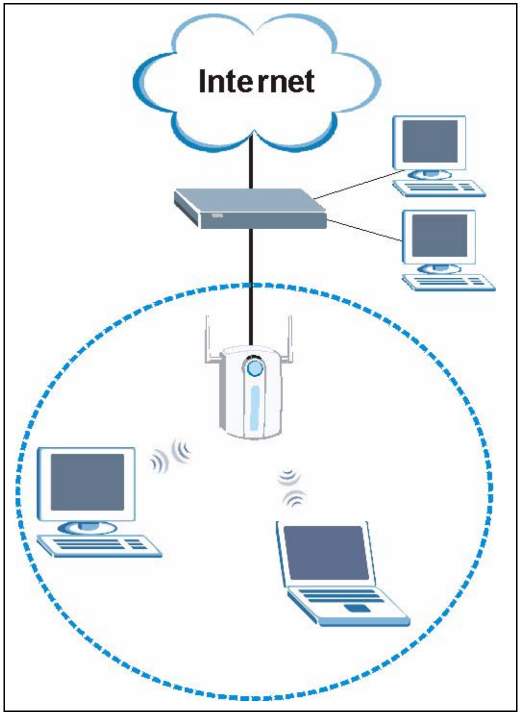
1.2.1 Station Mode

The AG-320 is in wireless station mode by default. When the AG-320 works as a wireless station (wireless client), you can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

1.2.1.1 Infrastructure

To connect to a network via an access point (AP), set the AG-320 network type to **Infrastructure** using the **Profile** screen. Through the AP, you can access the Internet or the wired network behind the AP.

Figure 2 Application: Infrastructure

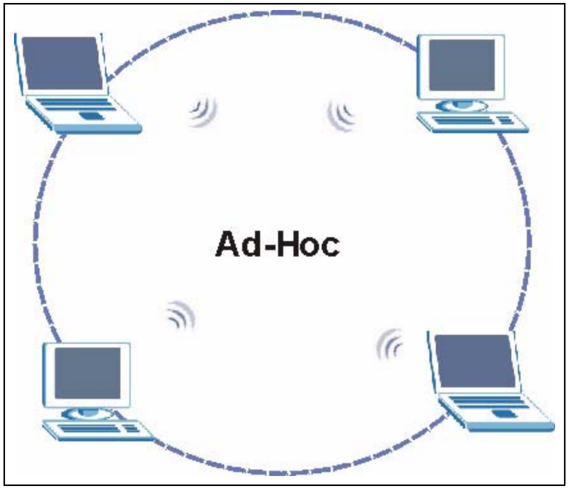


1.2.1.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc**.

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

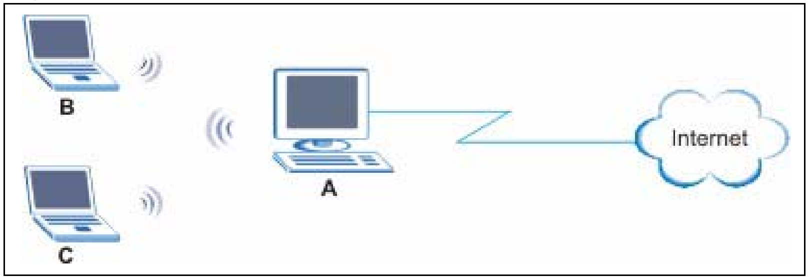
Figure 3 Application: Ad-Hoc



1.2.2 Access Point Mode

You can also set the AG-320 to access point mode. In access point mode, your AG-320 allows you to set up your wireless networks without using a dedicated AP. The following figure shows a network example.

Figure 4 Application: Access Point Mode



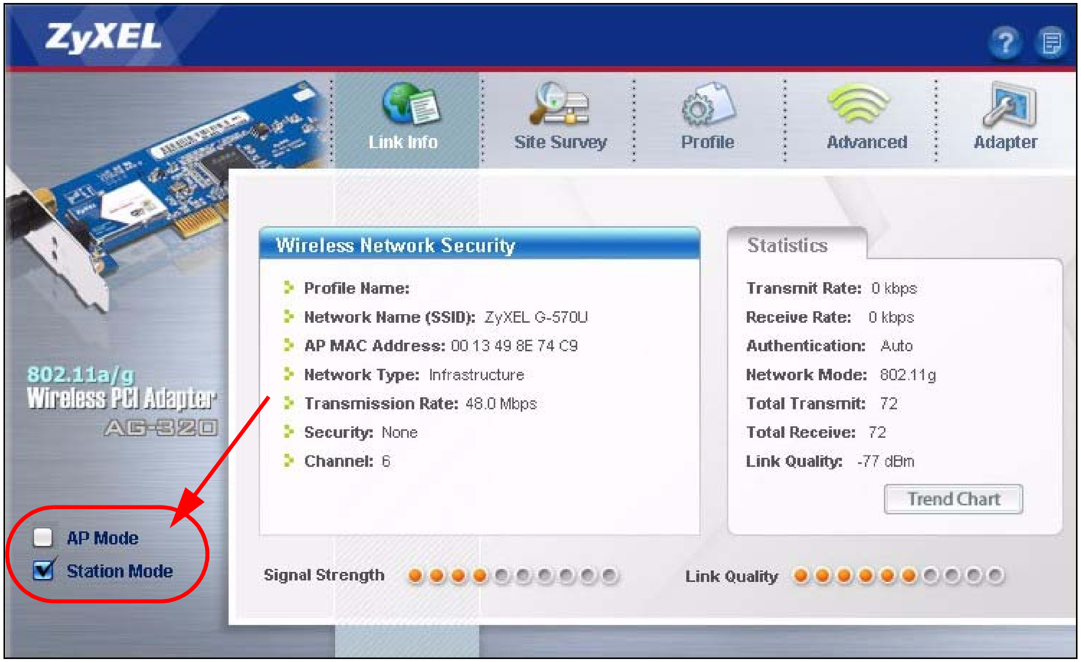
In the example, the AG-320 is installed on computer **A** and set to operate in access point mode. Computer **A** provides an Internet connection to the wireless LAN, so wireless stations **B** and **C** can access the Internet.

Note: With WZC, you cannot use the AG-320 as an access point.

1.2.3 Changing AG-320 Mode

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

Figure 5 ZyXEL Utility: Change Modes



Wireless Network Security

- Profile Name:
- Network Name (SSID): ZyXEL G-570U
- AP MAC Address: 00 13 49 8E 74 C9
- Network Type: Infrastructure
- Transmission Rate: 48.0 Mbps
- Security: None
- Channel: 6

Statistics

Transmit Rate: 0 kbps
Receive Rate: 0 kbps
Authentication: Auto
Network Mode: 802.11g
Total Transmit: 72
Total Receive: 72
Link Quality: -77 dBm

□ AP Mode
☑ Station Mode

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

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

The current mode is indicated by the color of the check box.

1.3 AG-320 Hardware and Utility Installation

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

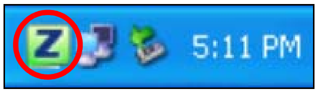
1.3.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, and insert the AG-320, an icon for the ZyXEL utility appears in the system tray.

Note: The ZyXEL utility system tray icon displays only when the AG-320 is installed properly.

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

Figure 6 ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the AG-320. Refer to the following table for details.

Table 3 ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The AG-320 is operating in wireless station mode but is not connected to a wireless network.
Green	The AG-320 is operating in wireless station mode and connected to a wireless network.
Pale Blue	The AG-320 is operating in access point mode.

Configuration Methods

To configure your AG-320, use one of the following applications:

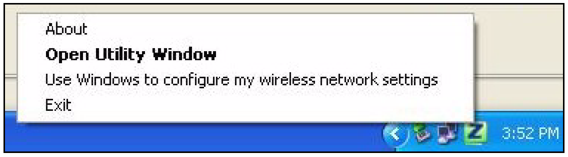
- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool)
- ZyXEL Utility (required when you want to use the AG-320 as an access point)

1.3.2 Enabling WZC

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

If you want to use WZC to configure the AG-320, 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 7 Enable WZC



About

Open Utility Window

Use Windows to configure my wireless network settings

Exit

Refer to the appendices for information on how to use WZC to manage the AG-320.

To re-activate the ZyXEL utility, double-click the (Z) icon on your desktop or click **Start**, **(All) Programs**, **ZyXEL AG-320 Utility**, **ZyXEL AG-320 Utility GUI**.

1.3.3 Accessing the ZyXEL Utility

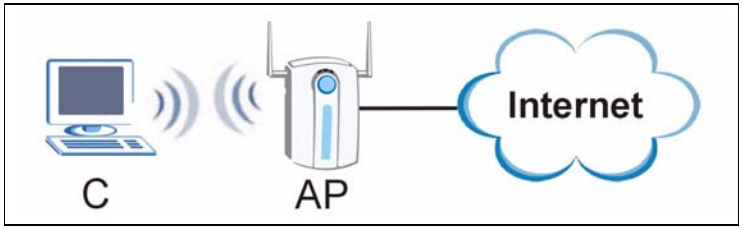
Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility. The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User’s Guide.

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 diagrams. The wireless client is labeled **C** and the access point is labeled **AP**.

Figure 8 Infrastructure Network



There are three ways to connect the wireless client (the AG-320 in station mode) 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 (see Section 2.1 on page 29).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see Section 2.2 on page 32).

This chapter also includes a simple example of how to configure the AG-320 as an AP using the ZyXEL utility. See Section 2.3 on page 34 for more information.

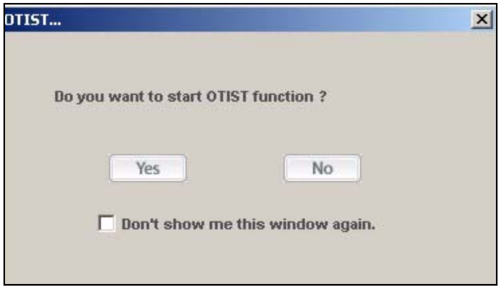
2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. 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 SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey" in the AP.

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. When the OTIST screen displays, click **No**. For information on the OTIST function, see Section 3.3 on page 41.

Figure 9 ZyXEL Utility: The OTIST Screen.



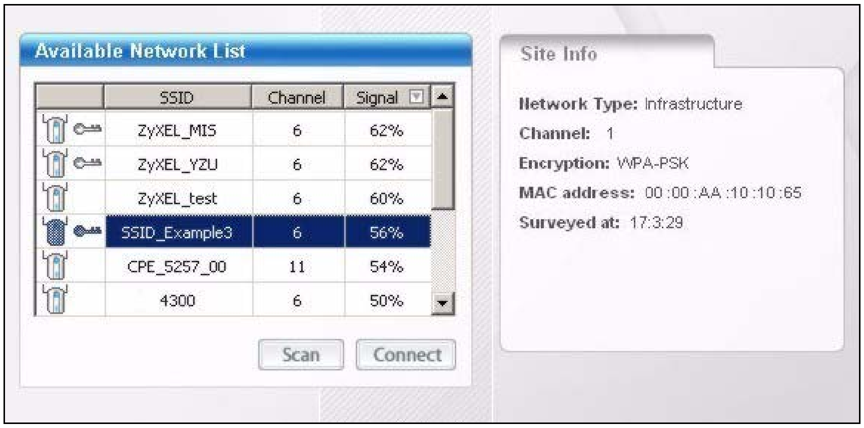
OTIST...

Do you want to start OTIST function ?

□ Don't show me this window again.

2 Click the **Site Survey** tab to open the screen as shown next.

Figure 10 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%
	4300	6	50%

Site Info

Network Type: Infrastructure

Channel: 1

Encryption: WPA-PSK

MAC address: 00:00:AA:10:10:65

Surveyed at: 17:3:29

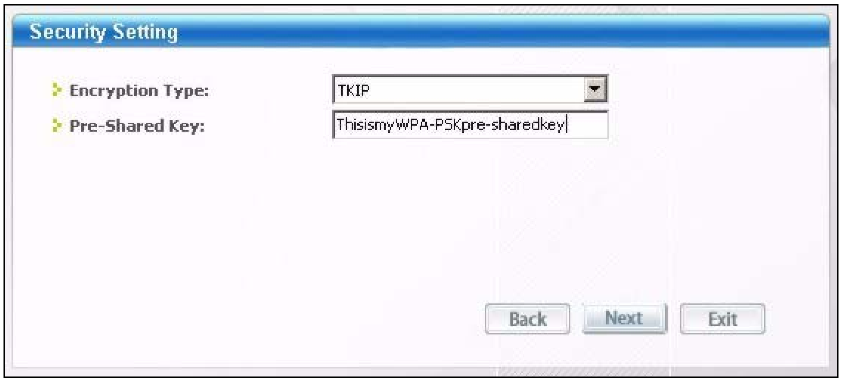
3 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See Table 7 on page 48 for detailed field descriptions.

4 To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (with a SSID of **SSID_Example3**, in this example).

5 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 11 ZyXEL Utility: Security Setting



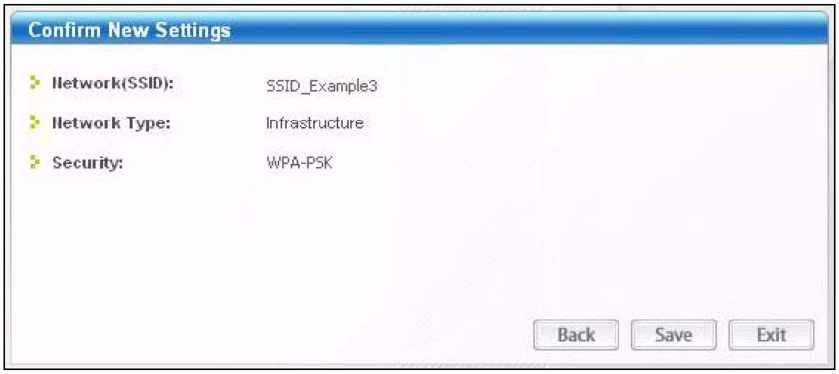
Security Setting

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

6 The **Confirm New Settings** window appears. Check your settings and click **Save** to continue.

Figure 12 ZyXEL Utility: Confirm New Settings



Confirm New Settings

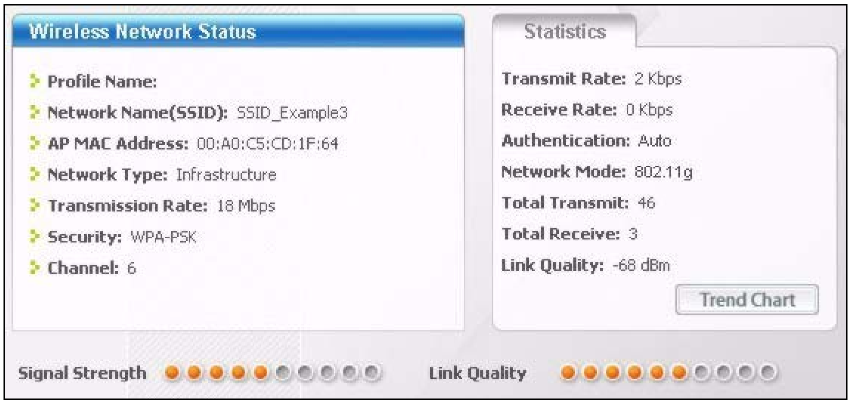
Network(SSID): SSID_Example3

Network Type: Infrastructure

Security: WPA-PSK

7 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. See Table 5 on page 46 for detailed field descriptions.

Figure 13 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: Auto

Network Mode: 802.11g

Total Transmit: 46

Total Receive: 3

Link Quality: -68 dBm

8 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 if necessary.

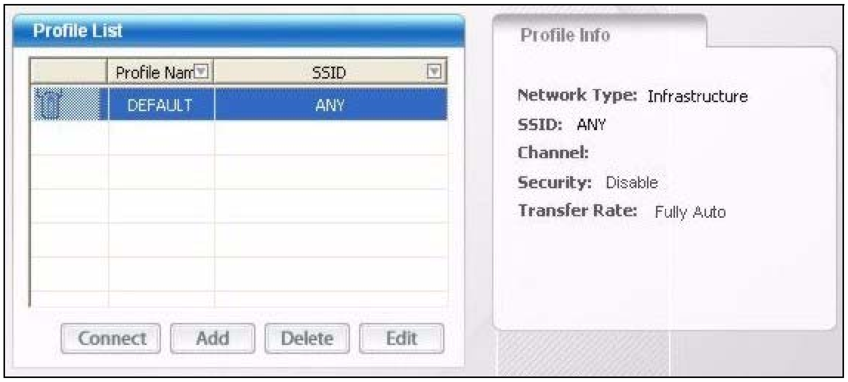
2.2 Creating and Using a Profile

A profile lets you automatically 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 SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey” in the AP. You have chosen the profile name “PN_Example3”.

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

Figure 14 ZyXEL Utility: Profile

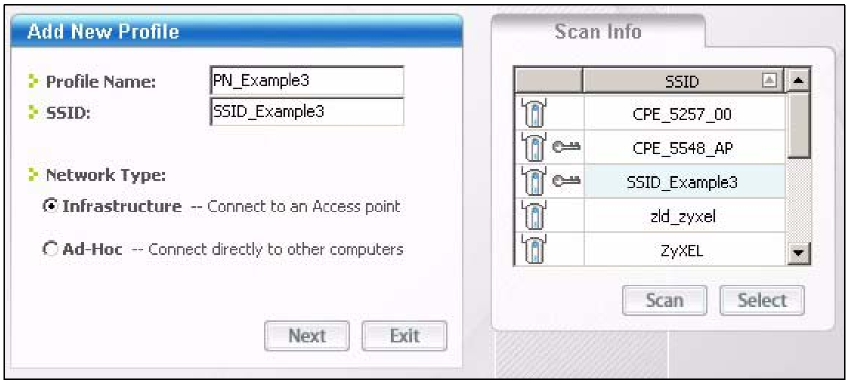


	Profile Nam	SSID
	DEFAULT	ANY

Network Type: Infrastructure
SSID: ANY
Channel:
Security: Disable
Transfer Rate: Fully Auto

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 15 ZyXEL Utility: Add New Profile



Profile Name: PN_Example3
SSID: SSID_Example3

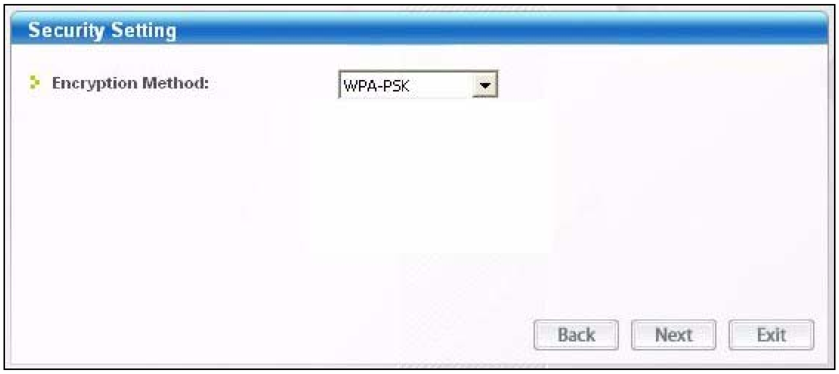
Network Type:
● Infrastructure -- Connect to an Access point
○ Ad-Hoc -- Connect directly to other computers

	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 **Infrastructure** 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).

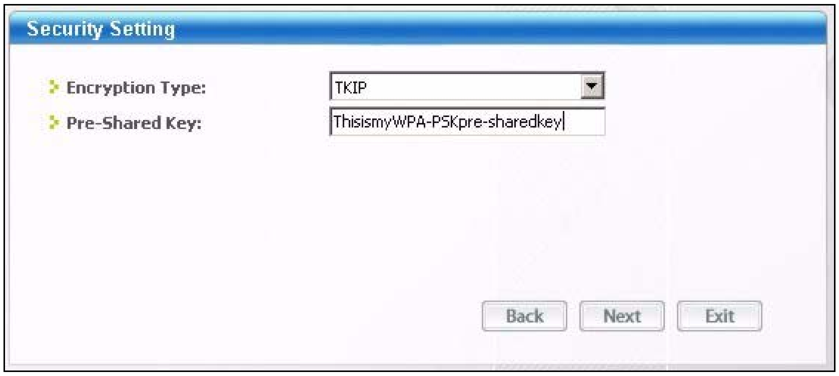
Figure 16 ZyXEL Utility: Profile Security


Security Setting

Encryption Method: 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 17 ZyXEL Utility: Profile Encryption

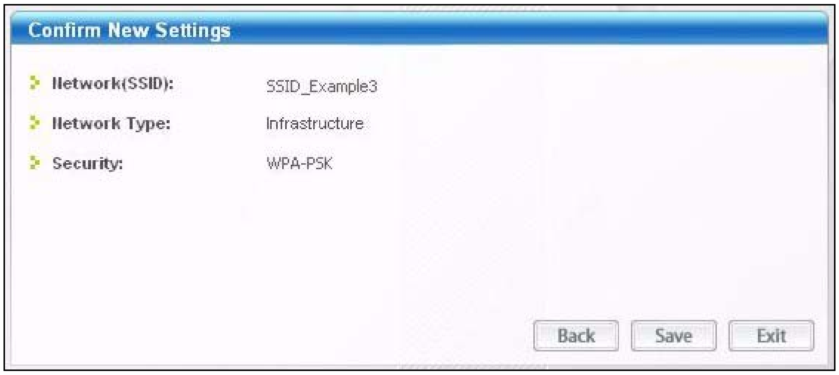

Security Setting

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

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

Figure 18 ZyXEL Utility: Profile Confirm New Settings


Confirm New Settings

Network(SSID): SSID_Example3

Network Type: Infrastructure

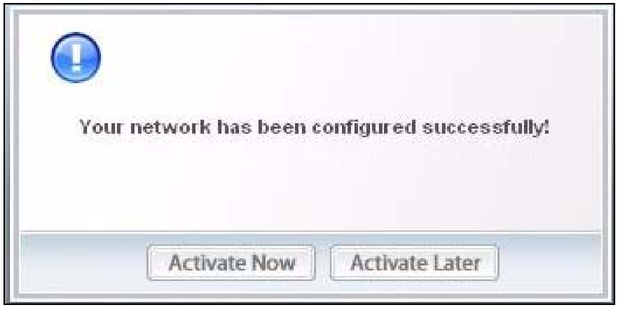
Security: WPA-PSK

7 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 19 ZyXEL Utility: Profile Activate



Your network has been configured successfully!

8 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.

9 Make sure the selected AP in the active profile is connected to the Internet. Open 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.

10 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.

2.3 Configuring the AG-320 as an AP

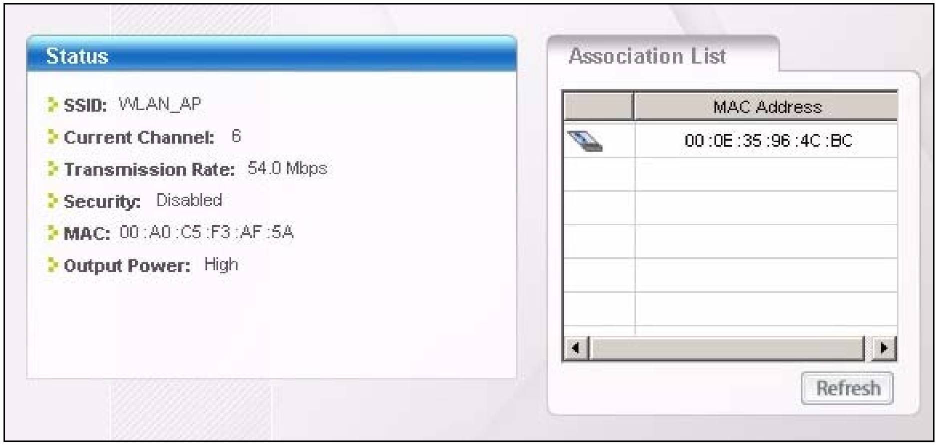
In access point mode, your AG-320 allows you to set up your wireless network without using a dedicated AP. Refer to Section 1.2.3 on page 26 and Chapter 5 on page 63 for more information.

Note: With WZC, you cannot use the AG-320 as an access point.

After you install the ZyXEL utility and then insert the AG-320, follow the steps below to set up your AG-320 as an AP.

1 Select **AP Mode** in any utility screen and wait for five seconds. The screen changes and displays as next. Under **Status**, you can view the current settings on the AG-320. In the **Association List**, you can see if any wireless clients have connected to your AG-320.

Figure 20 ZyXEL Utility: AP: Link Info



SSID: WLAN_AP

Current Channel: 6

Transmission Rate: 54.0 Mbps

Security: Disabled

MAC: 00 :A0 :C5 :F3 :AF :5A

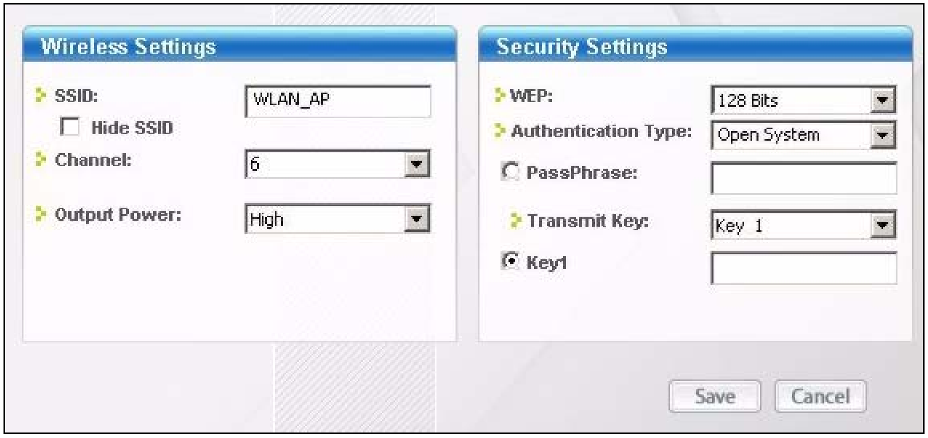
Output Power: High

	MAC Address
	00 :0E :35 :96 :4C :BC

2 If you want to change the SSID and enable wireless security for your AG-320, click the **Configuration** tab and refer to Section 5.3 on page 65 for detailed field descriptions.

Note: You can use only WEP when the AG-320 is in AP mode.

Figure 21 ZyXEL Utility: AP: Configuration



SSID: WLAN_AP

☐ Hide SSID

Channel: 6

Output Power: High

WEP: 128 Bits

Authentication Type: Open System

○ PassPhrase:

Transmit Key: Key 1

● Key1

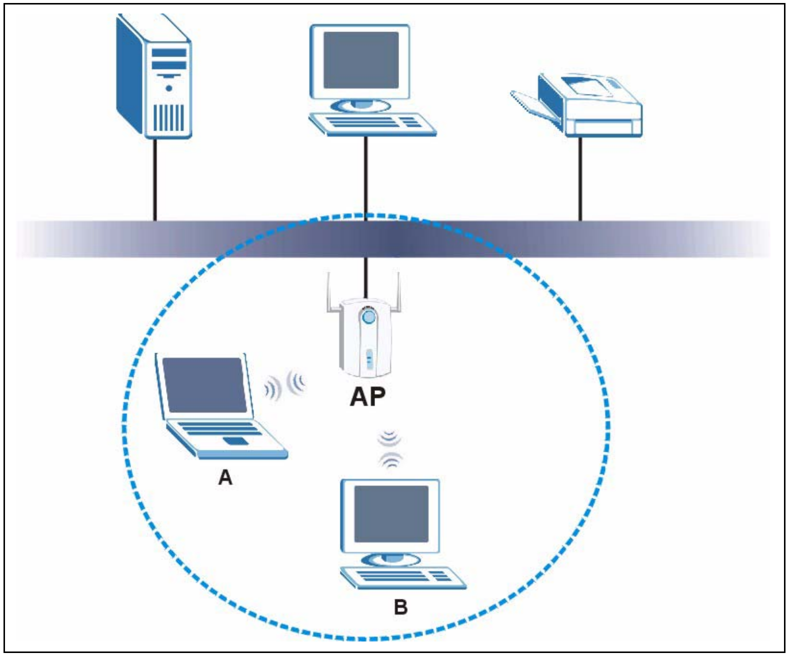
CHAPTER 3
Wireless LAN Network

This chapter provides background information on wireless LAN network.

3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 3 on page 25 for an Ad Hoc network example.

Figure 22 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 **Configuration** or the **Profile Security Setting** screen. If you do not enable any wireless security on your AG-320, the AG-320's wireless communications are accessible to any wireless networking device that is in the coverage area.

Note: You can use only WEP encryption if you set the AG-320 to Ad-hoc mode.

See the appendices for more detailed information about wireless security.

3.2.1 Hide SSID

Normally, the AG-320 in AP mode acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AG-320 in AP mode does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

3.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the AG-320 in AP mode which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

3.2.3 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. 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.

3.2.3.1 WEP

3.2.3.1.1 Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AG-320 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 AG-320.

- Automatic WEP key generation based on a "password phrase" called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

  For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Setting** or the **Configuration** 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 AG-320 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.

3.2.3.1.2 Authentication Type

The IEEE 802.11a/b/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. 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 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 AG-320 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.

3.2.3.2 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.

3.2.3.2.1 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 AG-320 supports EAP-TLS and EAP-PEAP. Refer to Appendix D on page 93 for descriptions.

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

3.2.3.3 WPA and WPA2

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

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

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

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

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

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

3.3 Introduction to OTIST

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

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

3.3.1 Enabling OTIST

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

We use the P-334U in this guide as the example AP. Screens may vary slightly for your ZyXEL devices.

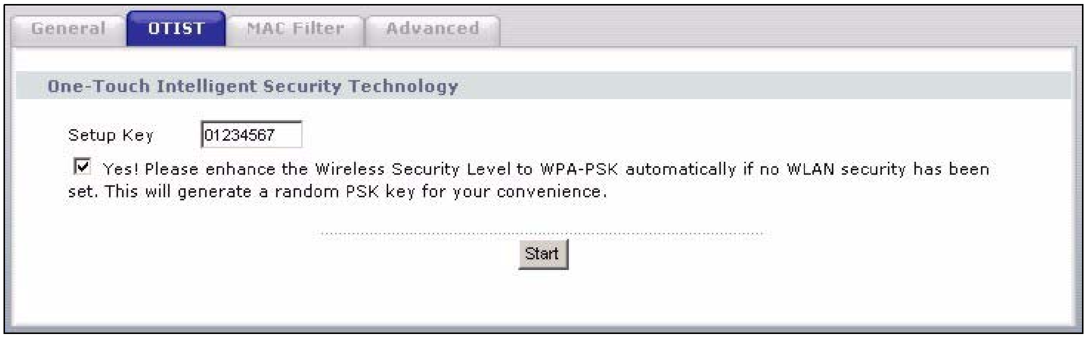
Note: The AP and wireless client(s) MUST use the same **Setup key**.

3.3.1.1 AP

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

Hold in the **OTIST** button for about two seconds.

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



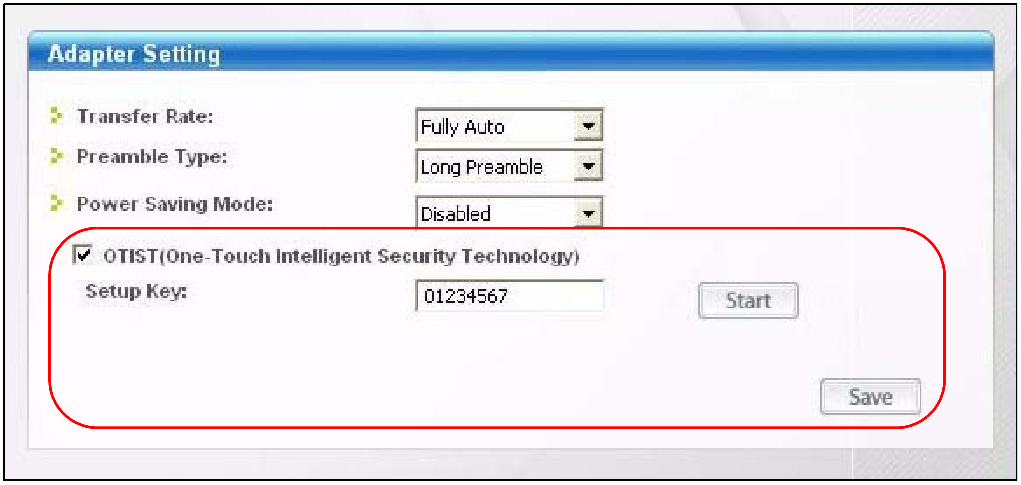
One-Touch Intelligent Security Technology

Setup Key: 01234567

☑ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.

3.3.1.2 Wireless Client

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



Transfer Rate: Fully Auto

Preamble Type: Long Preamble

Power Saving Mode: Disabled

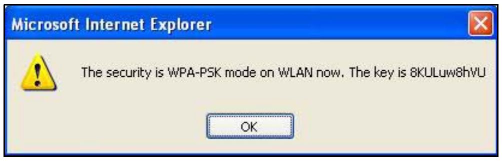
☑ OTIST(One-Touch Intelligent Security Technology)

Setup Key: 01234567

3.3.2 Starting OTIST

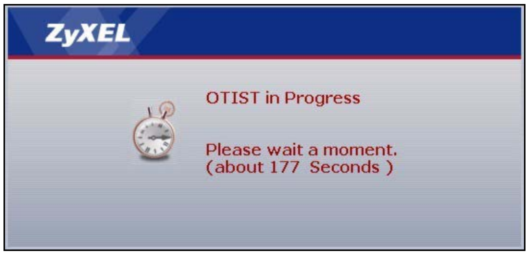
Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

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



The security is WPA-PSK mode on WLAN now. The key is 8KULuw8hVU

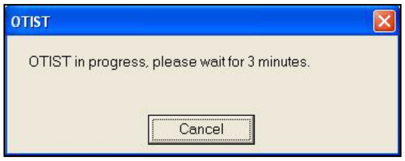
2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.



ZyXEL

OTIST in Progress

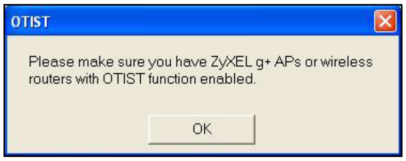
Please wait a moment.
(about 177 Seconds)



OTIST

OTIST in progress, please wait for 3 minutes.

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



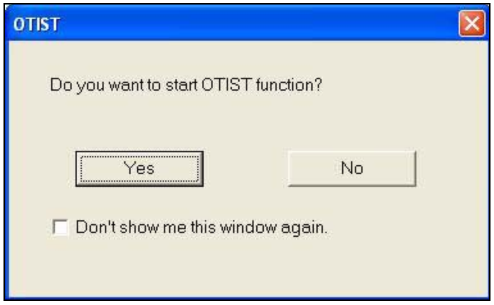
OTIST

Please make sure you have ZyXEL g+ APs or wireless routers with OTIST function enabled.

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

3.3.3 Notes on OTIST

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



OTIST

Do you want to start OTIST function?

□ Don't show me this window again.

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

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

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

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

CHAPTER 4 Wireless Station Mode Configuration

This chapter shows you how to use the ZyXEL utility to configure your AG-320 in wireless station mode. See Chapter 5 on page 63 for how to configure the AG-320 in access point mode.

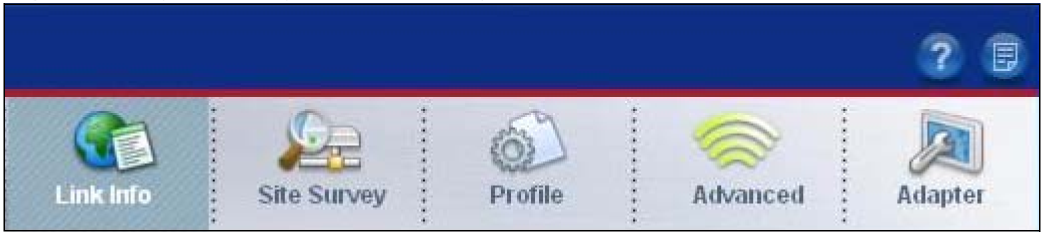
4.1 Wireless Station Mode Overview

To set your AG-320 in wireless station mode, select **Station Mode** in any utility screen (refer to Section 1.2.3 on page 26).

4.1.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens when the AG-320 is in station mode.

Figure 23 ZyXEL Utility Menu Summary: Station Mode



The following table describes the menus.

Table 4 ZyXEL Utility Menu Summary: Station Mode

TAB	DESCRIPTION
Station Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Site Survey	Use this screen to • scan for a wireless network • configure wireless security (if activated on the selected network). • connect to a wireless network.
Profile	Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings.

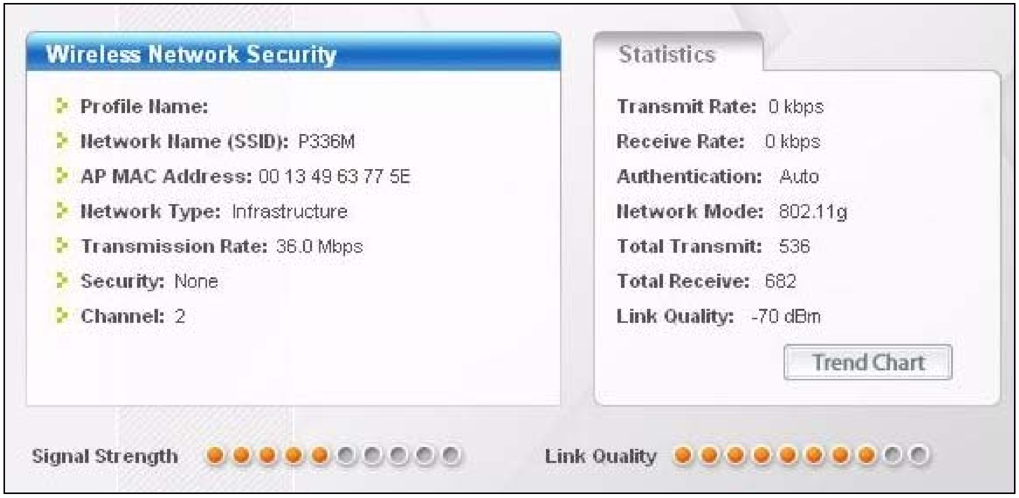
Table 4 ZyXEL Utility Menu Summary: Station Mode

TAB	DESCRIPTION
Advanced	Use this screen to configure the wireless LAN mode.
Adapter	Use this screen to configure a transfer rate, enable power saving and use OTIST (One-Touch Intelligent Security Technology).

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 AG-320.

Figure 24 Station Mode: Link Info



Wireless Network Security

Profile Name:
Network Name (SSID): P336M
AP MAC Address: 00 13 49 63 77 5E
Network Type: Infrastructure
Transmission Rate: 36.0 Mbps
Security: None
Channel: 2

Statistics

Transmit Rate: 0 kbps
Receive Rate: 0 kbps
Authentication: Auto
Network Mode: 802.11g
Total Transmit: 536
Total Receive: 682
Link Quality: -70 dBm

The following table describes the labels in this screen.

Table 5 Station mode: 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 AG-320 is associated.
AP MAC Address	This field displays the MAC address of the AP or peer computer to which the AG-320 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 AG-320 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP** (WEP or 802.1x), **TKIP** (WPA/WPA-PSK/WPA2/WPA2-PSK), **AES** (WPA/WPA-PSK/WPA2/WPA2-PSK)) or inactive (**None**).

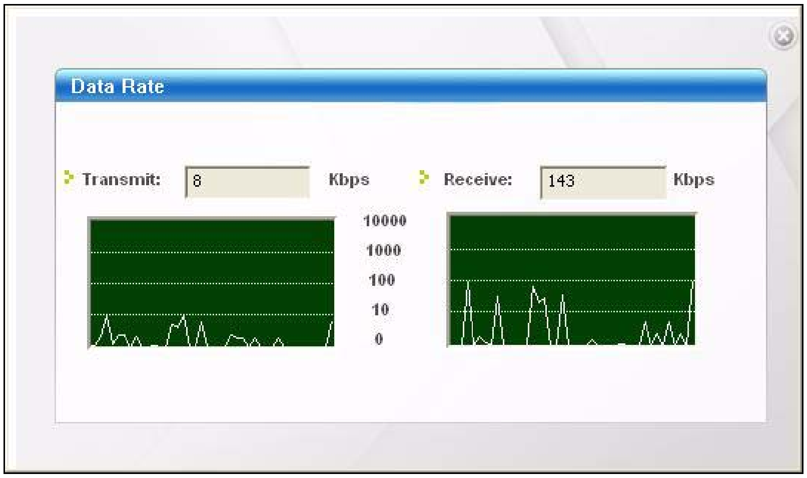
Table 5 Station mode: Link Info (continued)

LABEL	DESCRIPTION
Channel	This field displays the radio channel the AG-320 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 AG-320.
Network Mode	This field displays the wireless standard (**802.11a**, **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 signal strength of the AG-320.
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 is mainly depending on the antenna output power and the distance between your AG-320 and the AP or peer computer.
Link Quality	The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted 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 25 Station Mode: Link Info: Trend Chart



Data Rate

Transmit: 8 Kbps

Receive: 143 Kbps

The following table describes the labels in this screen.

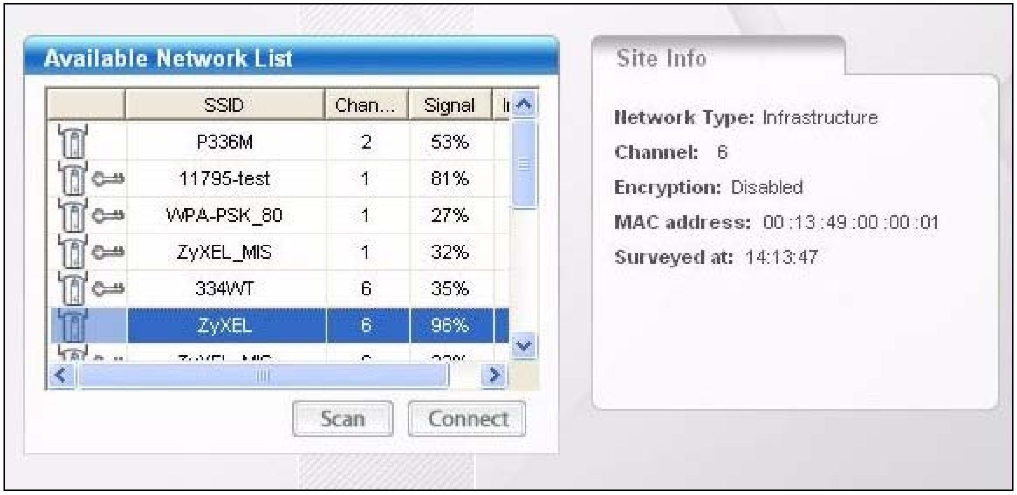
Table 6 Station Mode: Link Info: Trend Chart

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

4.3 The Site Survey Screen

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

Figure 26 Station Mode: Site Survey



	SSID	Chan...	Signal
	P336M	2	53%
	11795-test	1	81%
	WPA-PSK_80	1	27%
	ZyXEL_MIS	1	32%
	334WT	6	35%
	ZyXEL	6	96%

Network Type: Infrastructure
Channel: 6
Encryption: Disabled
MAC address: 00:13:49:00:00:01
Surveyed at: 14:13:47

The following table describes the labels in this screen.

Table 7 Station Mode: Site Survey

LABEL	DESCRIPTION
Available Network List	Click a column heading to sort the entries.
, , or	denotes that the wireless device is in infrastructure mode and the wireless security is activated. denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
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.

Table 7 Station Mode: Site Survey (continued)

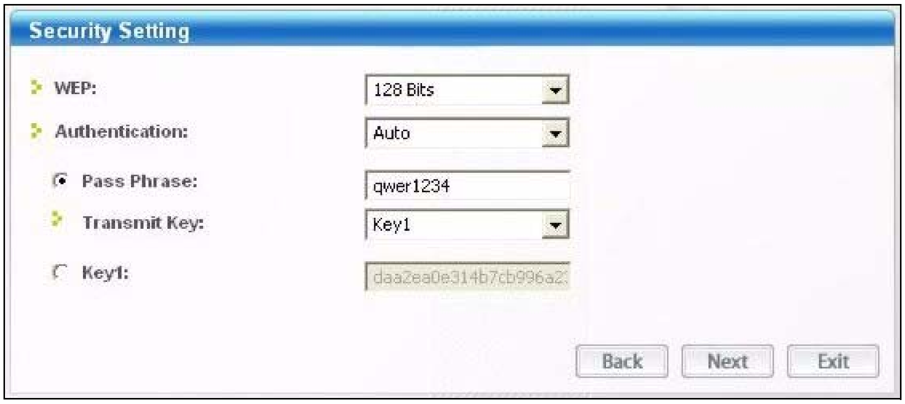
LABEL	DESCRIPTION
Connect	Click **Connect** to associate to the selected wireless device.
Site Info	Click an entry in the **Available Network List** table to display the information of the selected wireless device.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless device.
Channel	This field displays the channel number used by each wireless device.
Encryption	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA**, **802.1x**, **WPA2**, **WPA2-PSK**) or inactive (**Disabled**).
MAC address	This field displays the MAC address of the wireless device.
Surveyed at	This field displays the time when the wireless device is scanned.

4.3.1 Security Settings

When you configure the AG-320 to connect to a network with wireless security activated and the security settings are disabled on the AG-320, the screen varies according to the encryption method used by the selected network.

4.3.1.1 WEP Encryption

Figure 27 Station Mode: Security Setting: WEP



Security Setting

WEP: 128 Bits

Authentication: Auto

● Pass Phrase: qwer1234

Transmit Key: Key1

○ Key1: daa2ea0e314b7cb996a2

The following table describes the labels in this screen.

Table 8 Station Mode: Security Setting: WEP

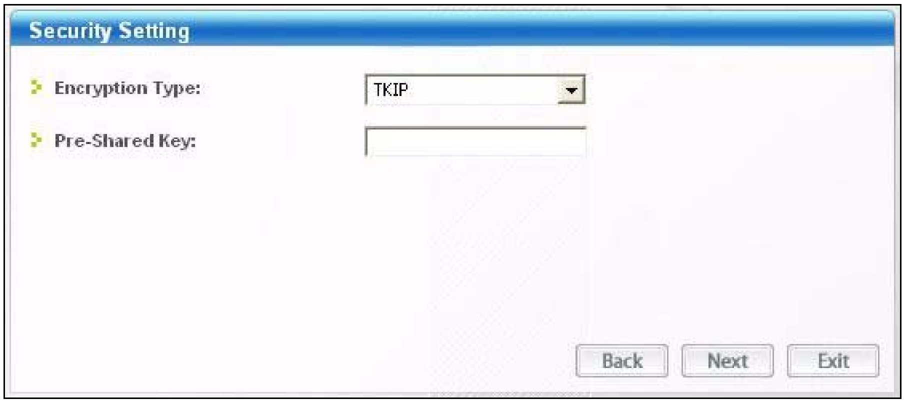
LABEL	DESCRIPTION
Security Setting	
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields.
Encryption Type	Select an authentication method. Choices are **Auto**, **Open System** and **Shared Key**. Refer to Section 3.2.3.1.2 on page 39 for more information.

Table 8 Station Mode: Security Setting: WEP (continued)

LABEL	DESCRIPTION
Pass Phrase	Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the AG-320 automatically generates four different WEP keys and displays it in the key field below. Refer to Section 3.2.3.1.1 on page 39 for more information. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.
Key x (where x is a number between 1 and 4)	Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided. If you select **64 Bits** in the **WEP** field. Enter either 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 11AA22BB33) for HEX key type. or Enter 5 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey) for ASCII key type. If you select **128 Bits** in the **WEP** field, Enter either 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type. If you select **256 Bits** in the **WEP** field, Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) for ASCII key type. **Note:** The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm New Settings** screen. Refer to Section 4.3.2 on page 53.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.2 WPA-PSK/WPA2-PSK

Figure 28 Station Mode: Security Setting: WPA-PSK/WPA2-PSK



Security Setting

Encryption Type: TKIP

Pre-Shared Key:

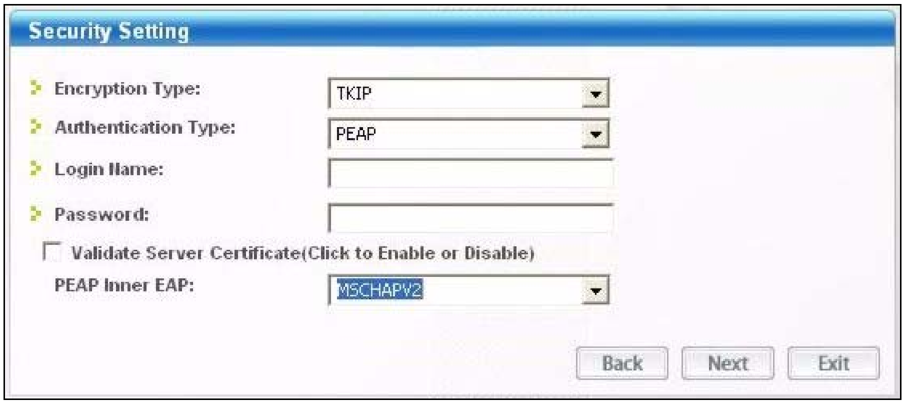
The following table describes the labels in this screen.

Table 9 Station Mode: Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.3.3 on page 40 for more information.
Pre-Shared Key	Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm New Settings** screen. Refer to Section 4.3.2 on page 53.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.3 WPA/WPA2

Figure 29 Station Mode: Security Setting: WPA/WPA2



Security Setting

Encryption Type: TKIP

Authentication Type: PEAP

Login Name:

Password:

□ Validate Server Certificate(Click to Enable or Disable)

PEAP Inner EAP: MSCHAPV2

The following table describes the labels in this screen.

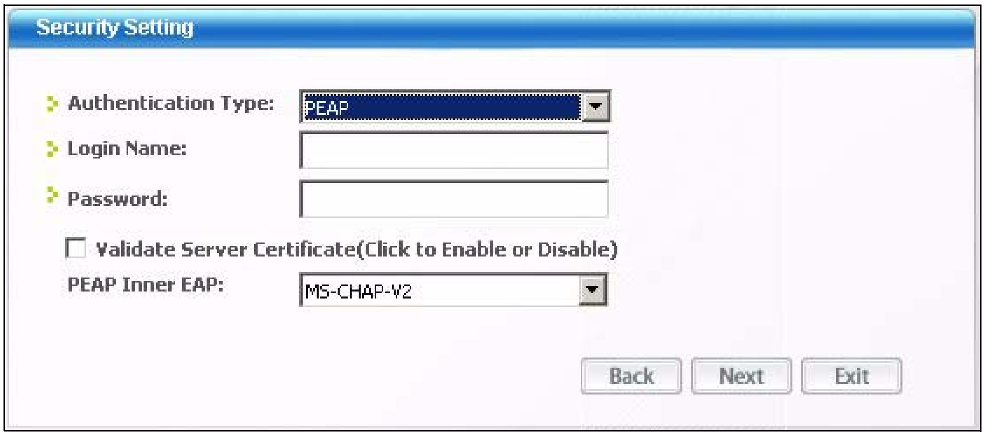
Table 10 Station Mode: Security Setting: WPA/WPA2

LABEL	DESCRIPTION
Encryption Type	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.3.3 on page 40 for more information.
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
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 AG-320. **Note:** You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm New Settings** screen. Refer to Section 4.3.2 on page 53.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.4 802.1x

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

Figure 30 Station Mode: Security Setting: 802.1x



Security Setting

Authentication Type: PEAP

Login Name:

Password:

□ Validate Server Certificate(Click to Enable or Disable)

PEAP Inner EAP: MS-CHAP-V2

The following table describes the labels in this screen.

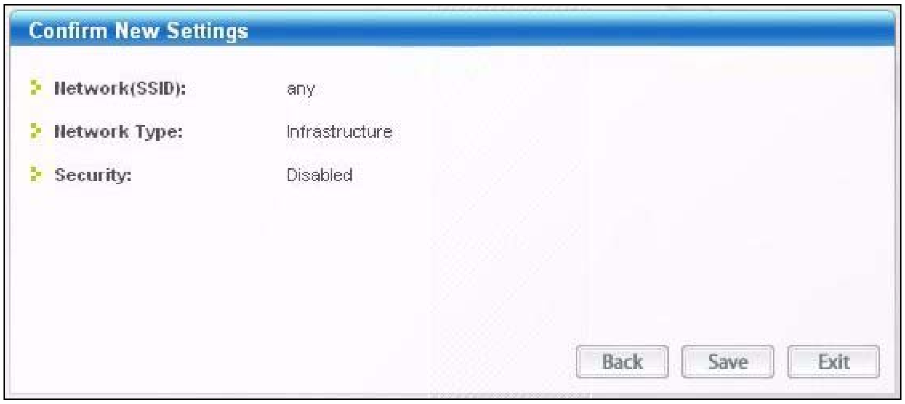
Table 11 Station Mode: Security Setting: 802.1x

LABEL	DESCRIPTION
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS** and **PEAP**.
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
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 AG-320. **Note:** You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the **Confirm New Settings** screen. Refer to Section 4.3.2 on page 53.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.2 Confirm New Settings

Use this screen to confirm and save the security settings.

Figure 31 Station Mode: Confirm New Settings



Confirm New Settings

- Network(SSID): any
- Network Type: Infrastructure
- Security: Disabled

The following table describes the labels in this screen.

Table 12 Station Mode: Confirm New Settings

LABEL	DESCRIPTION
Network (SSID)	This field displays the **SSID** previously entered.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless device.
Security	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA**, **802.1x**, **WPA2**, **WPA2-PSK**) or inactive (**Disabled**).
Channel	This field displays the channel number used by the profile.
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save the changes to the AG-320 and display the **Link Info** screen.
Exit	Click **Exit** to discard changes and return to the **Site Survey** screen.

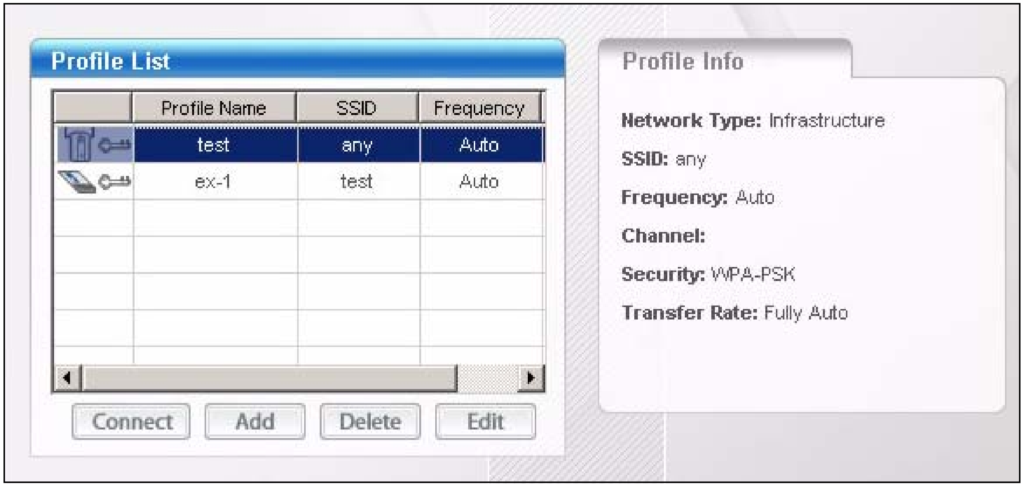
4.4 The Profile Screen

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 AG-320, 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 AG-320 cannot connect to a network.

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 32 Station Mode: Profile



Profile List

	Profile Name	SSID	Frequency
📶🔑	test	any	Auto
💳🔑	ex-1	test	Auto

Profile Info

Network Type: Infrastructure

SSID: any

Frequency: Auto

Channel:

Security: WPA-PSK

Transfer Rate: Fully Auto

The following table describes the labels in this screen.

Table 13 Station Mode: Profile

LABEL	DESCRIPTION
Profile List	Click a column heading to sort the entries.
📶🔑 , 📶 , 💳🔑 or 💳 .	📶🔑 denotes that the wireless device is in infrastructure mode and the wireless security is activated. 📶 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. 💳🔑 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. 💳 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
Profile Name	This is the name of the pre-configured profile.
SSID	This is the SSID of the wireless network to which the selected profile associate.
Frequency	This is the wireless LAN mode 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**.
Add	To add a new profile into the table, click **Add**.
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.
Profile Info	The following fields display detail information of the selected profile in the **Profile List** table.
Network Type	This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the profile.
SSID	This field displays the SSID (Service Set IDentifier) of the profile.
Frequency	This field displays the wireless LAN mode of the profile.
Channel	This field displays the channel number used by the profile.

Table 13 Station Mode: Profile (continued)

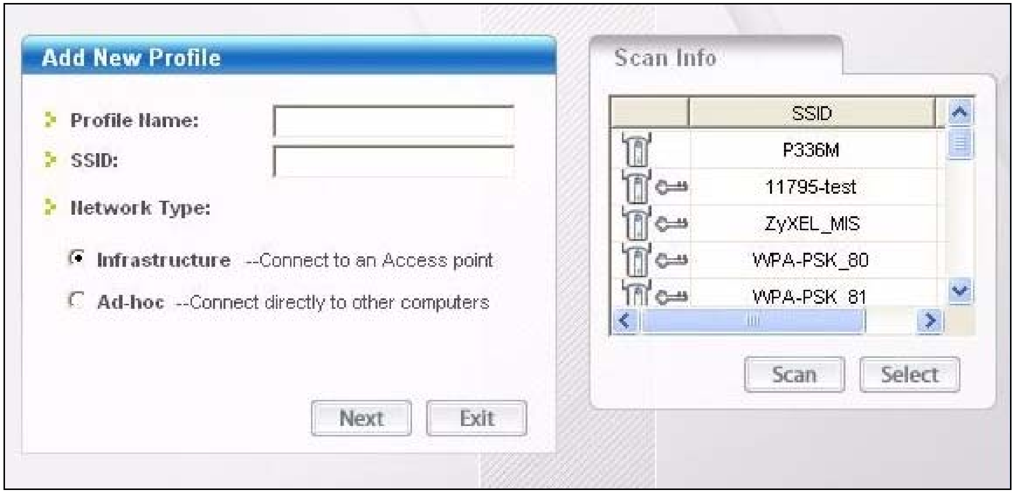
LABEL	DESCRIPTION
Security	This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**) or inactive (**Disable**).
Transfer Rate	This field displays the transmission speed of the selected profile in megabits per second (Mbps).

4.4.1 Adding a New Profile

Follow the steps below to add a new profile.

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

Figure 33 Station Mode: Profile: Add a New Profile


Add New Profile
Profile Name:
SSID:
Network Type:
Infrastructure --Connect to an Access point
Ad-hoc --Connect directly to other computers
Next
Exit
Scan Info
Scan
Select

● Infrastructure --Connect to an Access point
○ Ad-hoc --Connect directly to other computers

	SSID
	P336M
	11795-test
	ZyXEL_MIS
	WPA-PSK_80
	WPA-PSK_81

The following table describes the labels in this screen.

Table 14 Station Mode: Profile: Add a New Profile

LABEL	DESCRIPTION
Add New Profile	
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the AG-320 associate to any AP or roam between any infrastructure wireless networks.
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.

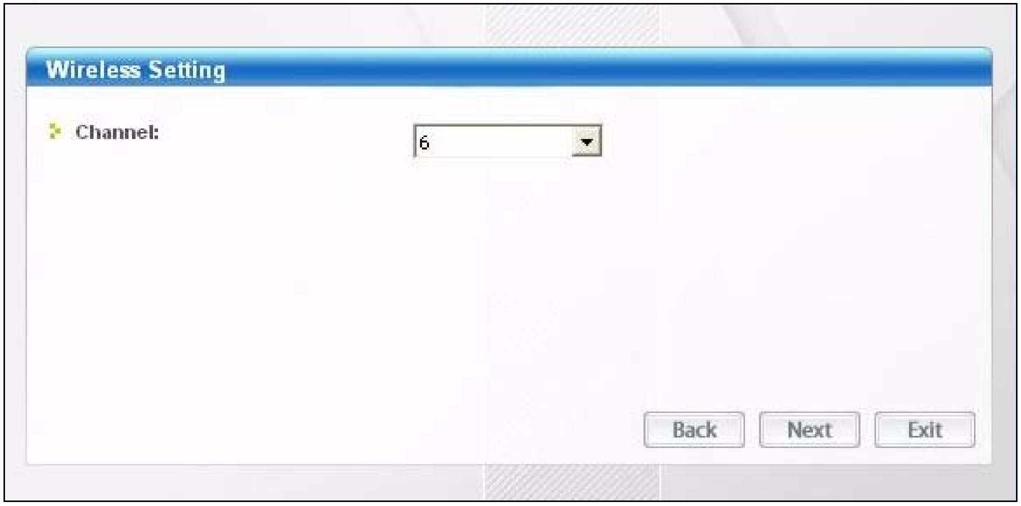
Table 14 Station Mode: Profile: Add a New Profile (continued)

LABEL	DESCRIPTION
📡🔑 , 📡 , 💳🔑 or 💳	📡🔑 denotes that the wireless device is in infrastructure mode and the wireless security is activated. 📡 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. 💳🔑 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. 💳 denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.
SSID	This field displays the SSID (Service Set IDentifier) of each 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 AG-320 associates to the selected wireless network only.

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

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

Figure 34 Station Mode: Profile: Select a Channel



Wireless Setting

Channel: 6

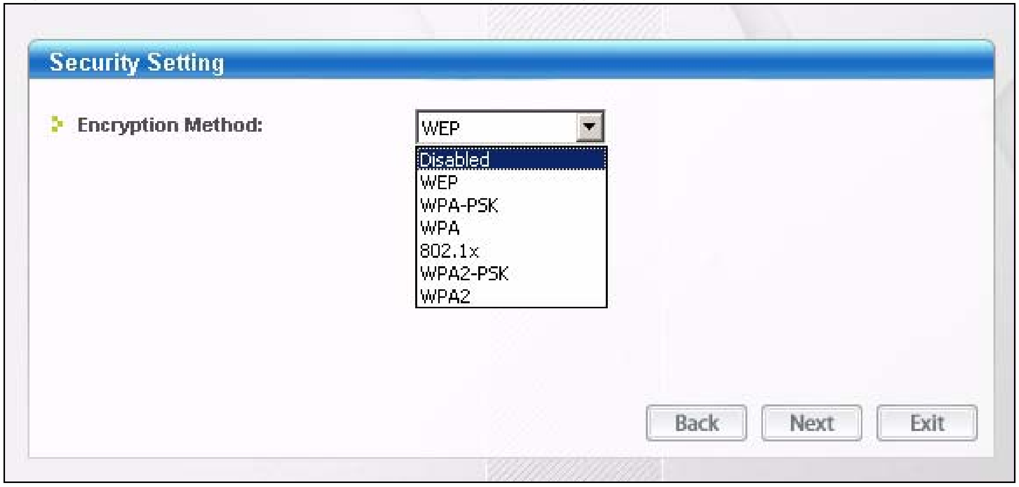
The following table describes the labels in this screen.

Table 15 Station Mode: Profile: Select a Channel

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

- If you select **Infrastructure** network type in the first screen, select **WEP**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2** or **802.1x** from the drop-down list box to enable data encryption. If you select **Ad-Hoc** network type in the first screen, you can only use **WEP** encryption method. Otherwise, select **Disabled** to allow the AG-320 to communicate with the access points or other peer wireless computers without any data encryption and skip to step 5.

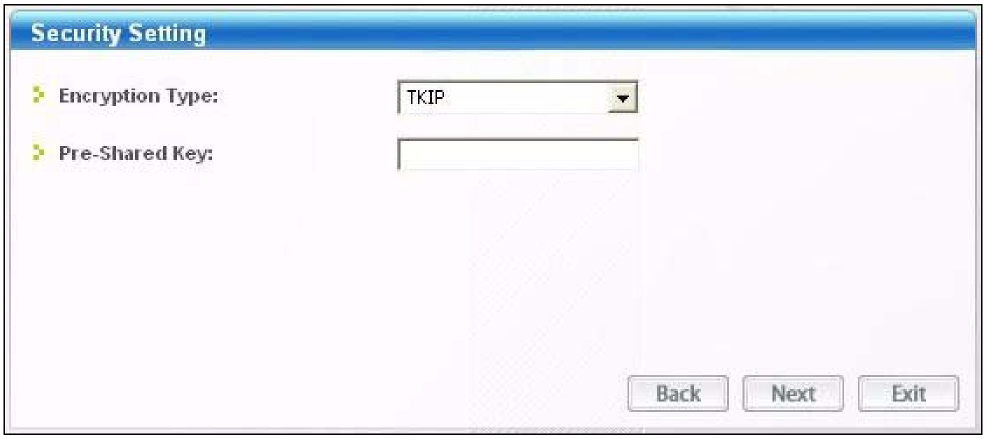
Figure 35 Station Mode: Profile: Security Settings



Encryption Method: WEP

- 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 AG-320. Refer to Section 4.3.1 on page 49 for detailed information on wireless security configuration.

Figure 36 Station Mode: Profile: Security Settings

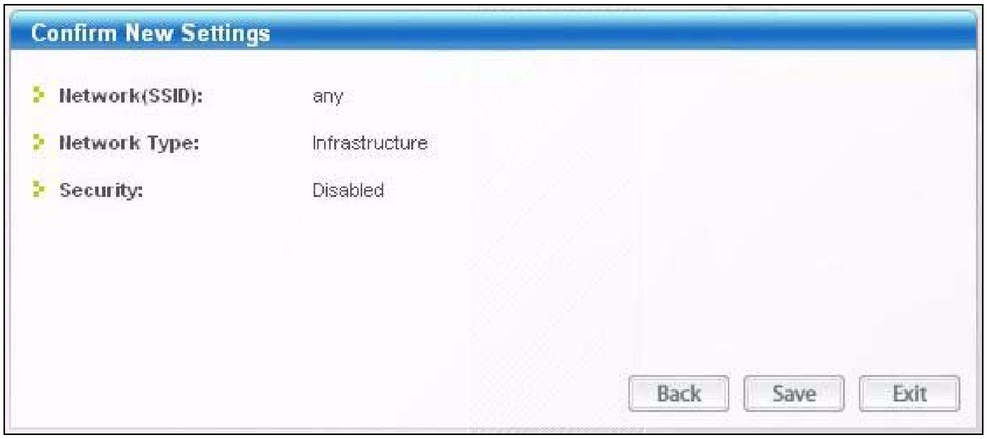


Encryption Type: TKIP

Pre-Shared Key:

- 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 37 Station Mode: Profile: Confirm New Settings



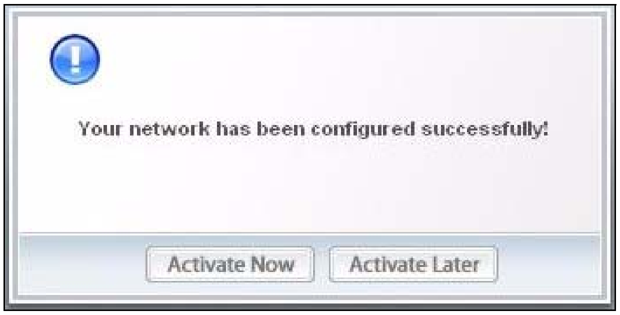
Confirm New Settings

- Network(SSID): any
- Network Type: Infrastructure
- Security: Disabled

- To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

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

Figure 38 Station Mode: Profile: Activate the Profile



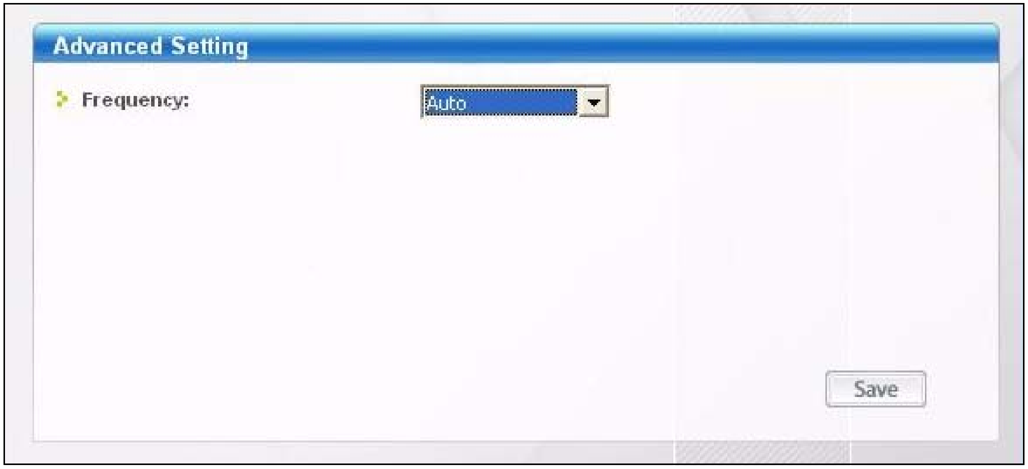
Your network has been configured successfully!

4.5 The Advanced Screen

To set the wireless LAN mode of the AG-320, click the **Advanced** tab.

Select **Auto** to have the AG-320 connect to either an IEEE 802.11a or an IEEE 802.11b/g wireless device. If you select **802.11a**, the AG-320 can connect to an IEEE 802.11a wireless device only. If you select **802.11b+g**, the AG-320 can connect to an IEEE 802.11b or g wireless device only. Click **Save** to save the changes to the AG-320.

Figure 39 Station Mode: Advanced



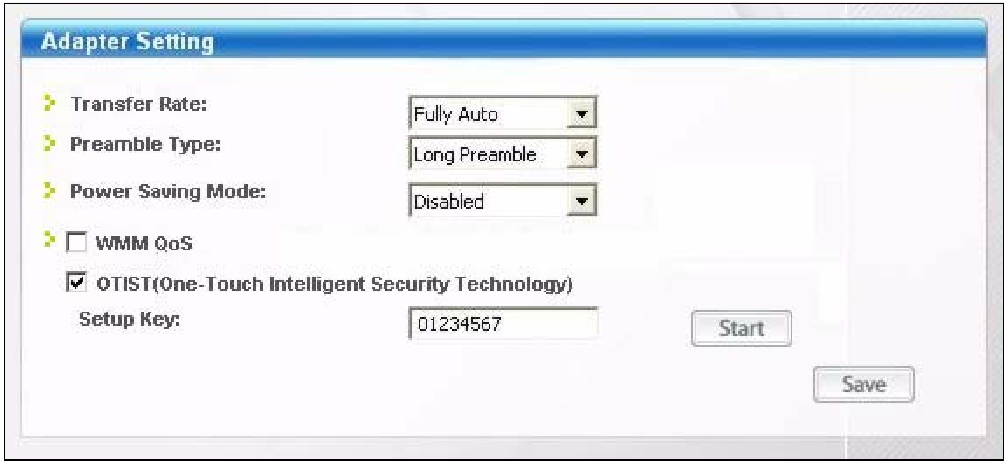
Advanced Setting

Frequency: Auto

4.6 The Adapter Screen

To set the other advanced features on the AG-320, click the **Adapter** tab.

Figure 40 Station Mode: Adapter



Adapter Setting

Transfer Rate: Fully Auto

Preamble Type: Long Preamble

Power Saving Mode: Disabled

□ WMM QoS

☑ OTIST(One-Touch Intelligent Security Technology)

Setup Key: 01234567

The following table describes the labels in this screen.

Table 16 Adapter

LABEL	DESCRIPTION
Adapter Setting	
Transfer Rate	In most networking scenarios, the factory default **Fully Auto** setting is the most efficient and allows your AG-320 to operate at the highest possible transmission (data) rate. If you want to select a specific transmission rate, select one that the AP or peer wireless device supports.

Table 16 Adapter (continued)

LABEL	DESCRIPTION
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 AG-320 automatically use short preamble when all access point or wireless stations support it; otherwise the AG-320 uses long preamble. **Note:** The AG-320 and the access point or wireless stations MUST use the same preamble mode in order to communicate.
Power Saving Mode	Select **Enabled** to save power (especially for notebook computers). This forces the AG-320 to go to sleep mode when it is not transmitting data. When you select **Disabled**, the AG-320 will never go to sleep mode.
WMM QoS	Select this check box to enable WMM (Wi-Fi MultiMedia) QoS (Quality of Service). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services. To do this, you must enable WMM QoS on both the AP and wireless clients.
OTIST (One-Touch Intelligent Security Technology)	Select this check box to enable OTIST.
Setup Key	Enter the same setup key (up to eight printable characters) as the ZyXEL AP or wireless router to which you want to associate. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key on the ZyXEL AP or wireless router, you must also make the same change here.
Start	Click **Start** to encrypt the wireless security data using the setup key and have the ZyXEL AP or wireless router set your AG-320 to use the same wireless settings as the ZyXEL AP or wireless router. You must also activate and start OTIST on the ZyXEL AP or wireless router all within three minutes. See Section 3.3 on page 41 for more information.
Save	Click **Save** to save the changes to the AG-320 and return to the **Link Info** screen.

CHAPTER 5
Access Point Mode Configuration

This chapter shows you how to configure your AG-320 in access point mode.

5.1 Access Point Mode Introduction

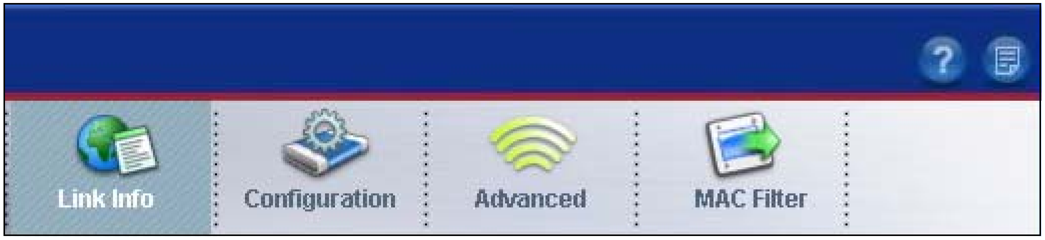
To set your AG-320 as an Access Point (AP), select **AP Mode** in any utility screen (refer to Section 1.2.3 on page 26).

In access point mode, your AG-320 functions as an access point. This allows you to set up your wireless networks without using a dedicated AP.

5.1.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens when the AG-320 is in AP mode.

Figure 41 ZyXEL Utility Menu Summary: AP Mode



The following table describes the menus.

Table 17 ZyXEL Utility Menu Summary: AP Mode

TAB	DESCRIPTION
AP Mode	
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Configuration	Use this screen to configure wireless LAN settings.
Advanced	Use this screen to configure the wireless LAN mode.
MAC Filter	Use this screen to configure which computer(s) you want access to the wireless LAN through the AG-320.

5.1.2 Additional Setup Requirements

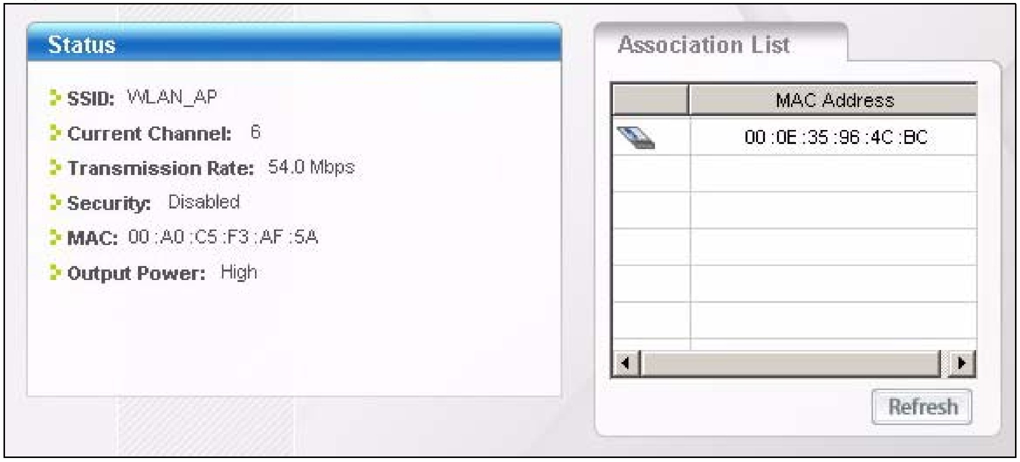
To bridge your wired and wireless network using the AG-320, the following requirements must be met:

1. The AG-320 must be installed on a computer connected to the wired network.
2. Either configure network sharing (refer to Appendix B on page 75 for an example) or bridge the two interfaces (wireless and wired) on the computer.
3. Set the wireless station's IP address to be dynamic if you want the wireless stations to access the wired network or the Internet through the AG-320. Refer to Appendix E on page 99 for how to configure your computer's IP address.

5.2 The Link Info Screen

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

Figure 42 Access Point Mode: Link Info



Status

- SSID: WLAN_AP
- Current Channel: 6
- Transmission Rate: 54.0 Mbps
- Security: Disabled
- MAC: 00 :A0 :C5 :F3 :AF :5A
- Output Power: High

Association List

	MAC Address
	00 :0E :35 :96 :4C :BC

The following table describes the labels in this screen.

Table 18 Access Point Mode: Link Info

LABEL	DESCRIPTION
Status	
SSID	This field displays the name that identifies your AG-320 in the wireless LAN network.
Current Channel	This field displays the radio channel the AG-320 is currently using.
Transmission Rate	This field displays the current transmission rate of the AG-320 in megabits per second (Mbps).
Security	This field shows whether data encryption is active (**WEP**) or inactive (**Disabled**).
MAC	This field displays the MAC address of the AG-320.
Output Power	This field shows the strength of the AG-320's antenna gain or transmission power.

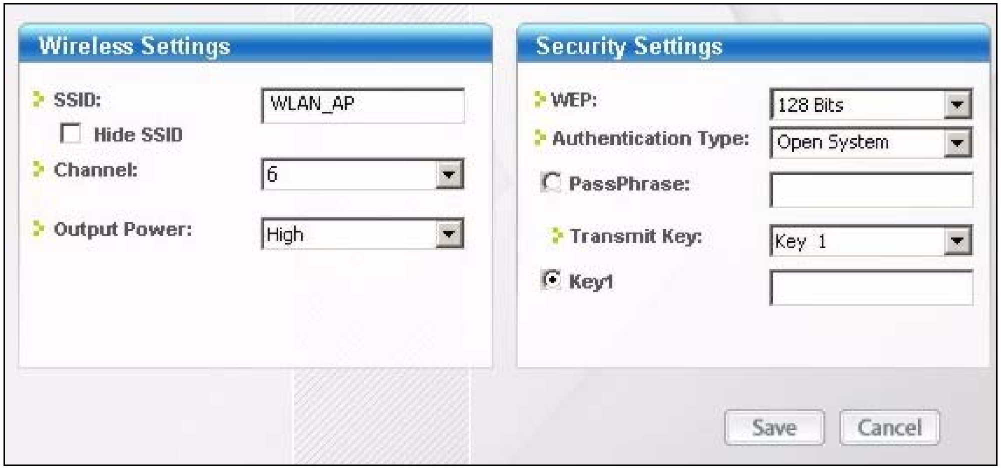
Table 18 Access Point Mode: Link Info (continued)

LABEL	DESCRIPTION
Association List	This table lists up to 16 wireless clients that are currently connected to the AG-320.
or	denotes a wireless client without WEP security. denotes a wireless client with WEP security enabled.
MAC Address	This field displays the MAC addresses of a wireless client that is currently connected to the AG-320.
Refresh	Click **Refresh** to update this screen.

5.3 The Configuration Screen

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

Figure 43 Access Point Mode: Configuration



Wireless Settings

SSID: WLAN_AP

□ Hide SSID

Channel: 6

Output Power: High

Security Settings

WEP: 128 Bits

Authentication Type: Open System

○ PassPhrase:

Transmit Key: Key 1

● Key1

The following table describes the labels in this screen.

Table 19 Access Point Mode: Configuration

LABEL	DESCRIPTION
Wireless Settings	
SSID	The SSID identifies the wireless network to which a wireless station is associated. Wireless stations associating to the access point (the AG-320) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID so an intruder cannot obtain the SSID through scanning using a site survey tool.
Channel	Set the operating frequency/channel depending on your geographical region.

Table 19 Access Point Mode: Configuration (continued)

LABEL	DESCRIPTION
Output Power	Set this field if you need to conserve power consumption (especially for notebook computers). This control changes the strength of the AG-320's antenna gain or transmission power. Antenna gain, measured in dBm (decibel relative units compared to milliwatts), is the increase in coverage. Higher antenna gain improves the range of the signal for better communications. Select **High** to set the AG-320's antenna to transmit at 17-dBm. Select **Medium-High** to set the AG-320's antenna to transmit at 15-dBm. Select **Medium-Low** to set the AG-320's antenna to transmit at 13-dBm. Select **Low** to set the AG-320's antenna to transmit at 11-dBm. This allows for the least power consumption.
Security Settings	
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields. Select **Disable** to deactivate the WEP encryption.
Authentication Type	Select an authentication method. Choices are **Auto**, **Shared Key** and **Open System**. Refer to Section 3.2.3.1.2 on page 39 for more information.
Pass Phrase	When you select the radio button, enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the AG-320 automatically generates four different WEP key and displays it in the key field below. Refer to Section 3.2.3.1 on page 39 for more information. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.
Key x (where x is a number between 1 and 4)	Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided. If you select **64 Bits** in the **WEP** field. Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type or Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type. If you select **128 Bits** in the **WEP** field, Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. If you select **256 Bits** in the **WEP** field, Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) 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.

Table 19 Access Point Mode: Configuration (continued)

LABEL	DESCRIPTION
Save	Click **Save** to save the changes.
Cancel	Click **Cancel** to discard the changes.

5.4 The Advanced Screen

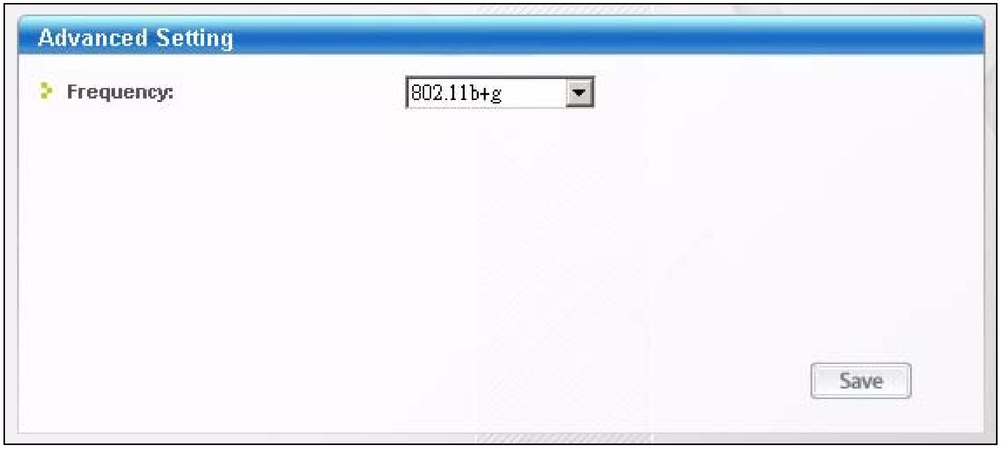
To set the wireless LAN mode of the AG-320, click the **Advanced** tab.

Select **802.11b** to allow only IEEE 802.11a compliant WLAN devices to associate with the AG-320.

Select **802.11b+g** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the AG-320. The transmission rate of your AG-320 might be reduced.

Click **Save** to save the changes to the AG-320.

Figure 44 Access Point Mode: Advanced



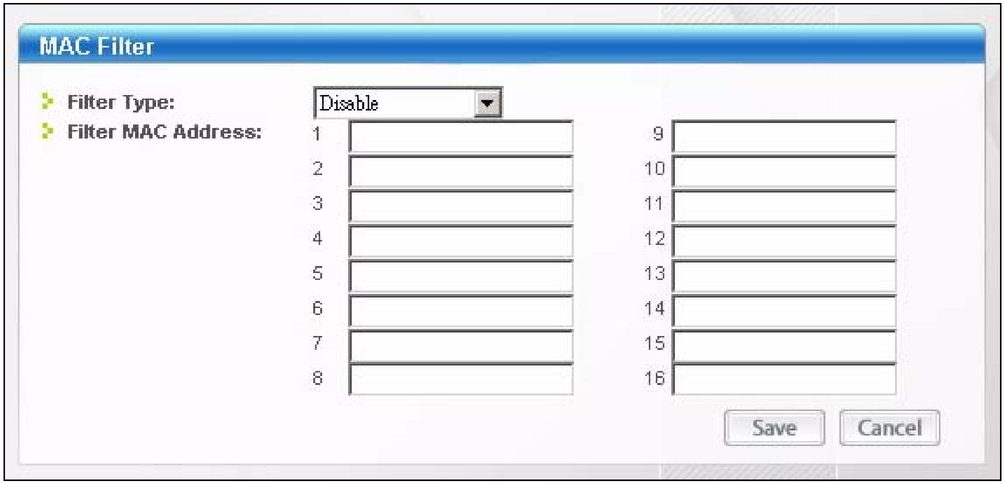
Advanced Setting

Frequency: 802.11b+g

5.5 The MAC Filter Screen

The **MAC Filter** screen allows you to configure the AG-320 to give exclusive access to (**Accept**) devices or exclude devices from (**Reject**) connecting to the AG-320. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the device(s) to configure this screen. See Section 3.2.2 on page 38 for more information.

Figure 45 Access Point Mode: MAC Filter



MAC Filter

Filter Type: Disable

Filter MAC Address: 1–16

The following table describes the labels in this screen.

Table 20 Access Point Mode: MAC Filter

LABEL	DESCRIPTION
Filter Type	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Disable** to deactivate the MAC filter feature. Select **Reject** to block access to the AG-320, MAC addresses not listed will be allowed to access the AG-320. Select **Accept** to permit access to the AG-320, MAC addresses not listed will be denied access to the AG-320.
Filter MAC Address 1-16	Specify the MAC address(es) of the wireless station(s) that is allowed or denied association to the AG-320. Enter six pairs of hexadecimal digits (separated by colons) in the range of “A-F”, “a-f” and “0-9” (for example, 00:A0:C5:00:00:02). If you enter an invalid MAC address, once you click **Save** to save the values, a warning screen will be displayed.
Save	Click **Save** to save the changes to the AG-320.
Cancel	Click **Cancel** to discard the changes.

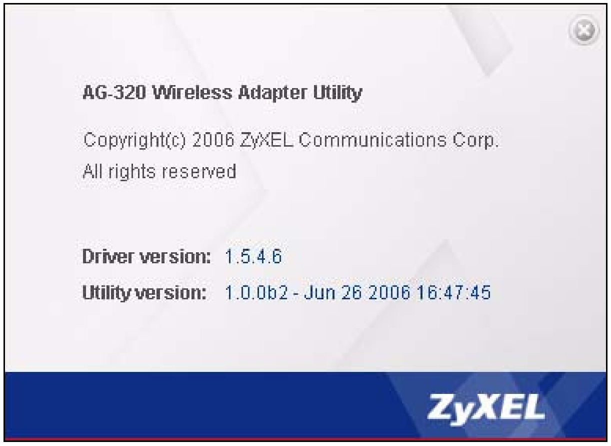
CHAPTER 6 Maintenance

This chapter describes the **About** screen and how to uninstall or upgrade the ZyXEL utility.

6.1 The About Screen

The **About** screen displays driver and utility version numbers of the AG-320. To display the screen as shown below, click the about (📄) button.

Figure 46 About



AG-320 Wireless Adapter Utility

Copyright(c) 2006 ZyXEL Communications Corp.
All rights reserved

Driver version: 1.5.4.6

Utility version: 1.0.0b2 - Jun 26 2006 16:47:45

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

Table 21 About

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the AG-320 driver.
Utility Version	This field displays the version number of the ZyXEL utility.

6.2 Uninstalling the ZyXEL Utility

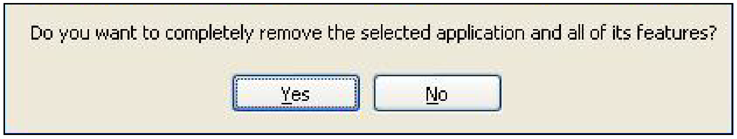
Note: Before you uninstall the ZyXEL utility, make a note of your current wireless configurations.

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

1 Click **Start**, **(All) Programs**, **ZyXEL AG-320 Utility**, **Uninstall ZyXEL AG-320 Software**.

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

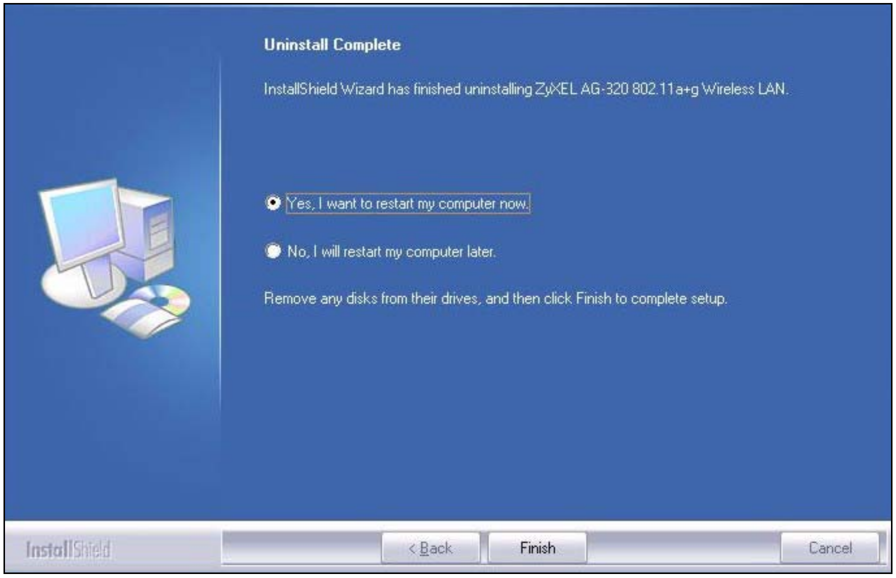
Figure 47 Uninstall: Confirm



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 48 Uninstall: Finish



Uninstall Complete

InstallShield Wizard has finished uninstalling ZyXEL AG-320 802.11a+g Wireless LAN.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

6.3 Upgrading the ZyXEL Utility

Note: Before you uninstall the ZyXEL utility, make a 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 Follow the steps in Section 6.2 on page 69 to remove the current ZyXEL utility from your computer.

3 Restart your computer when prompted.

4 Disconnect the AG-320 from your computer.

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

6 Insert the AG-320 and check the version numbers in the **About** screen to make sure the new utility is installed properly.

CHAPTER 7 Troubleshooting

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

7.1 Problems Starting the ZyXEL Utility

Table 22 Troubleshooting Problems Starting the ZyXEL Utility

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Wireless LAN utility	Make sure the AG-320 is properly inserted and the LED(s) is on. Refer to the Quick Start Guide for the LED descriptions. Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the AG-320 under **Network Adapter**. (Steps may vary depending on the version of Windows). Install the AG-320 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.

7.2 Problems Connecting to an Access Point

Table 23 Troubleshooting Access Point Connection Problems

PROBLEM	CORRECTIVE ACTION
When using the Windows XP configuration tool, cannot scan for or connect to any access points.	The AG-320 might still be operating in access point mode. This results when you set the AG-320 to operate in access point mode using the ZyXEL utility, close the ZyXEL utility and then use the Windows XP configuration tool. Before you use the Windows XP configuration tool, make sure you set the AG-320 to operate in station mode before you close and exit the ZyXEL utility.

7.3 Problems with the Link Quality

Table 24 Troubleshooting Link Quality Problems

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. Lower the output power of each AP. Make sure there are not too many wireless stations connected to a wireless network.

7.4 Problems Communicating With Other Computers

Table 25 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
In wireless station mode, the computer with the AG-320 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 AG-320 computer and the associated AP use the same SSID. • Change the AP and the associated wireless clients to use another radio channel if interference is high. • Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Setting** screen. • 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 (IBSS) Mode • Verify that the peer computer(s) is turned on. • Make sure the AG-320 computer and the peer computer(s) are using the same SSID and channel. • Make sure that the computer and the peer computer(s) share the same security settings. • Change the wireless clients to use another radio channel if interference is high.
In access point mode, the wireless station(s) cannot associate to the AG-320.	Verify that the computer with the AG-320 installed is turned on. Make sure the wireless station(s) uses the same SSID as the AG-320. Make sure the wireless station(s) uses the same security settings. Verify that the wireless station(s) is not blocked in the **MAC Filter** screen.

Appendix A
Product Specifications

Table 26 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	ZyXEL AG-320 802.11a/g Wireless CardBus Card
Interface	PCI Bus 2.2 standard
Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	IEEE 802.11a: 5.15~5.35GHz, 5.725~5.825GHz (North America and Taiwan) 5.15~5.35GHz, 5.47~5.725GHz (Europe) IEEE 802.11b: 2.412~2.462GHz (North America and Taiwan) 2.412~2.472GHz (Europe) IEEE 802.11g: 2.412~2.462GHz (North America and Taiwan) 2.412~2.472GHz (Europe)
Operating Channels	IEEE 802.11a: 12 Channels (North America and Taiwan) IEEE 802.11b: 11 Channels (North America and Taiwan) IEEE 802.11g: 11 Channels (North America and Taiwan) IEEE 802.11a: 19 Channels (Europe) IEEE 802.11b: 13 Channels (Europe) IEEE 802.11g: 13 Channels (Europe)
Data Rate	IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11b: 11, 5.5, 2, 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) IEEE 802311b: PBCC, Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK) IEEE 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Voltage	3.3V DC
Weight	46g ± 1g
Dimension	135 (L) mm 121 (W) mm 21.8 (H) mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11

Table 26 Product Specifications (continued)

Average Output Power	IEEE 802.11a: 13 dBm (typical) at 11Mbps CCK, QPSK, BPSK IEEE 802.11b: 18 dBm (typical) at 54Mbps OFDM IEEE 802.11g: 15 dBm (typical) at 11Mbps CCK, QPSK, BPSK
RX Sensitivity	54 Mbps (OFDM): < -70 dBm 11 Mbps (CCK): < -85 dBm
SOFTWARE SPECIFICATIONS	
Device Drivers	Microsoft Windows 98 Second Edition, Windows ME, Windows 2000, Windows XP
Security	64/128/256-bit WEP WPA WPA-PSK WPA2 WPA2-PSK IEEE 802.1x

APPENDIX B
Access Point Mode Setup Example

This example uses the network sharing feature in Windows 2000 to bridge the wired and wireless network when you set the AG-320 in access point (AP) mode.

Refer to Chapter 5 on page 63 for setup methods and requirements.

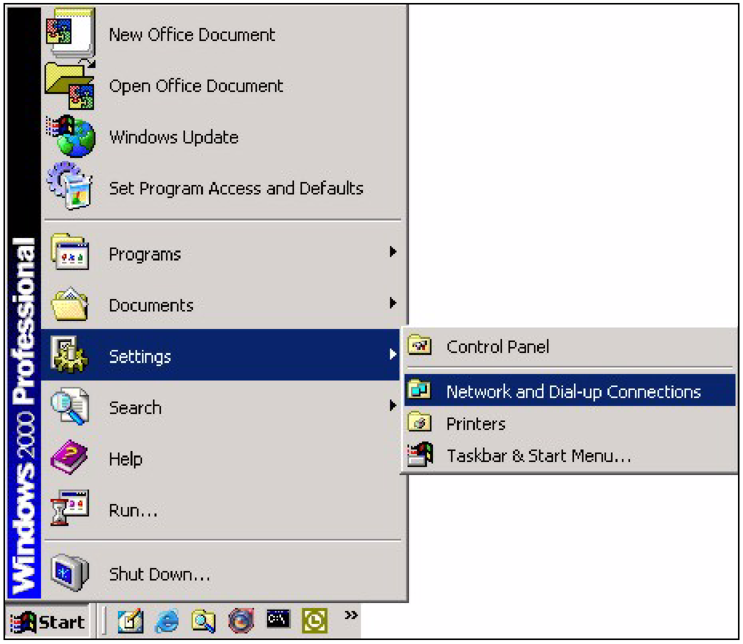
Steps may vary depending on your Windows version. You may need to install additional software in Windows 98 Second Edition and Windows ME.

Configuring the Computer on Which You Install the AG-320

1 Refer to Section 1.2.3 on page 26 to set the AG-320 to operate in AP mode.

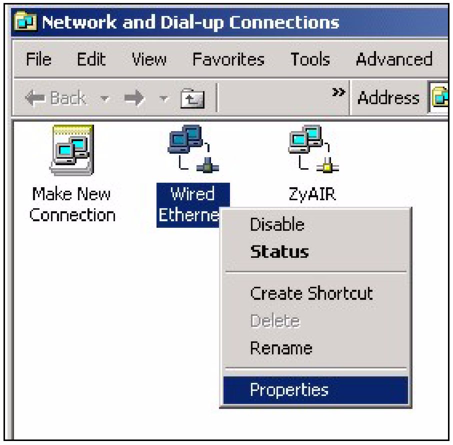
2 Click **Start**, **Settings**, **Network and Dial-up Connections** (or click **Start**, **Settings**, **Control Panel** and double-click **Network and Dial-up Connections**).

Figure 49 Windows 2000: Start



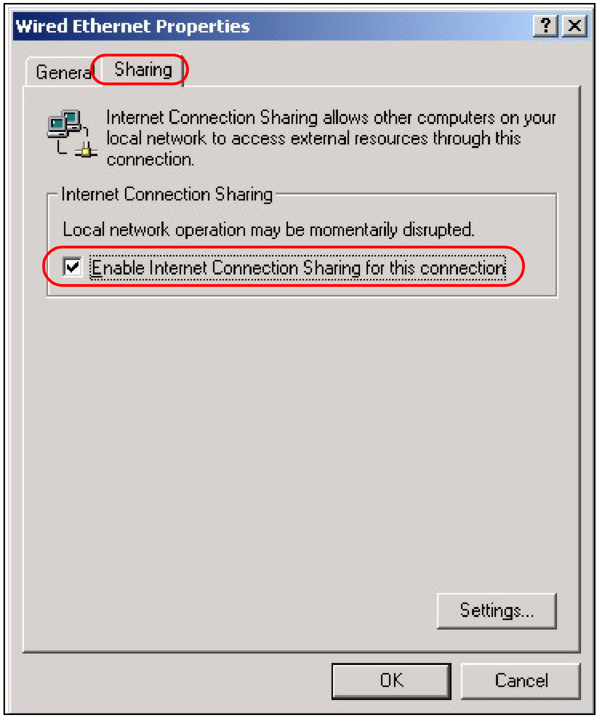
3 Right-click on the icon for your wired Ethernet adapter and click **Properties**.

Figure 50 Windows 2000: Network and Dial-up Connections



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

Figure 51 Windows 2000: Network Properties


Wired Ethernet Properties

General | Sharing

Internet Connection Sharing allows other computers on your local network to access external resources through this connection.

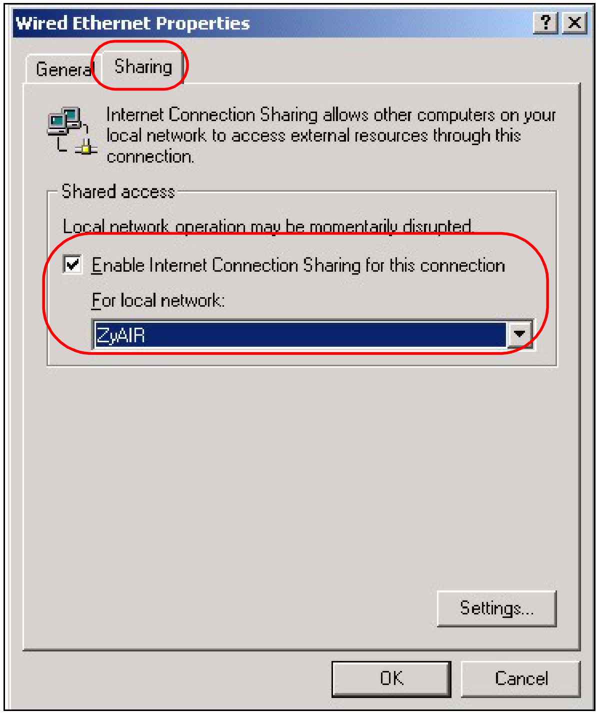
Internet Connection Sharing

Local network operation may be momentarily disrupted.

☑ Enable Internet Connection Sharing for this connection

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

Figure 52 WIndows 2000: Network Properties: Select Network Adapter



Internet Connection Sharing allows other computers on your local network to access external resources through this connection.

Shared access

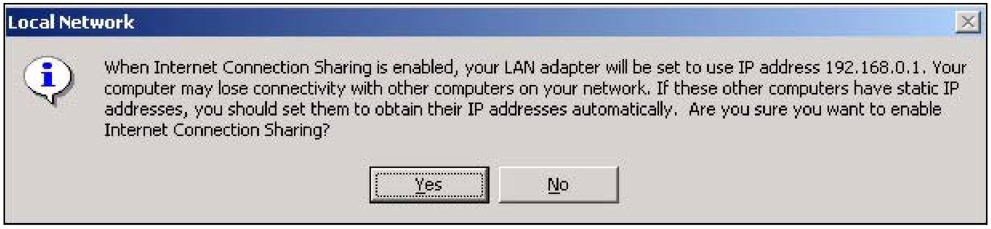
Local network operation may be momentarily disrupted

☑ Enable Internet Connection Sharing for this connection

For local network: ZyAIR

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

Figure 53 Windows 2000: Local Network



When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, you should set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

Configuring the Wireless Station Computer

Refer to Appendix E on page 99 for more information on how to set up the wireless station computer(s) IP address.

APPENDIX C
Management with Wireless Zero Configuration

This appendix shows you how to manage your AG-320 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.

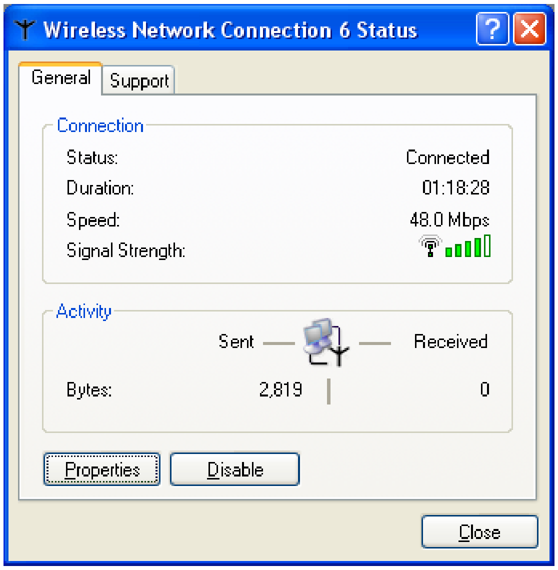
Activating Wireless Zero Configuration

1 Click **Start**, **Control Panel** and double-click **Network Connections**.

2 Double-click on the icon for wireless network connection.

3 The status window displays as shown below. Click **Properties**.

Figure 54 Windows XP SP1: Wireless Network Connection Status



Status: Connected

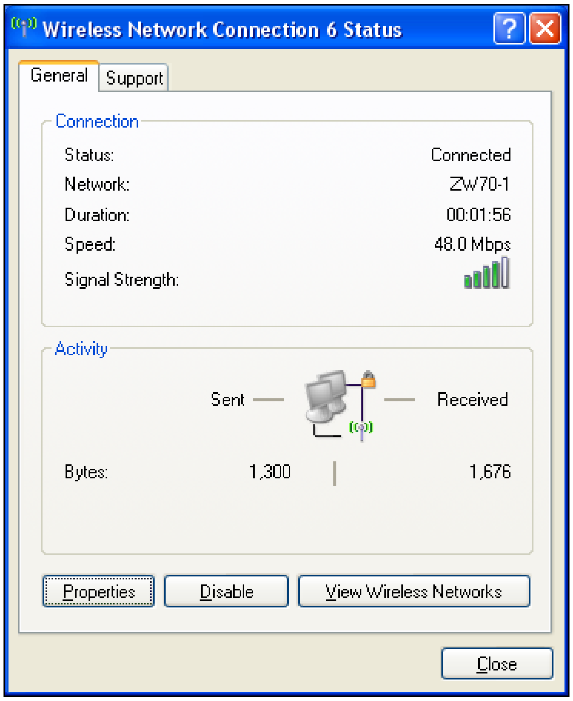
Duration: 01:18:28

Speed: 48.0 Mbps

Signal Strength:

	Sent	Received
Bytes:	2,819	0

Figure 55 Windows XP SP2: Wireless Network Connection Status



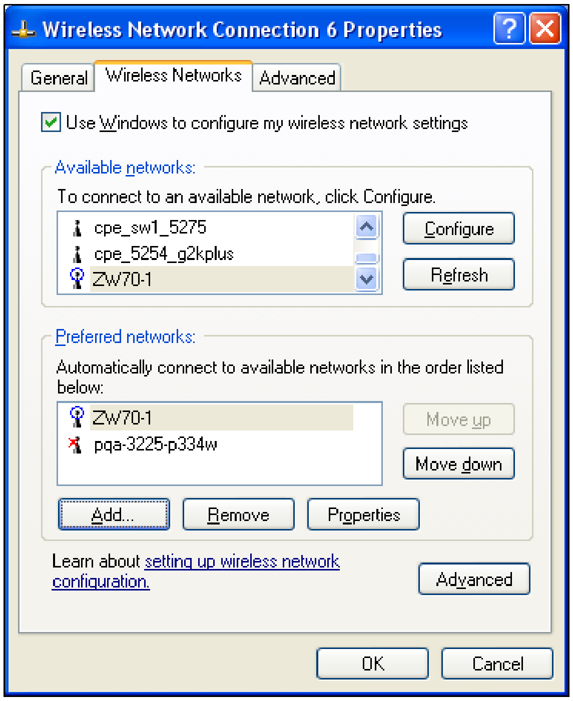
Status: Connected
Network: ZW70-1
Duration: 00:01:56
Speed: 48.0 Mbps
Signal Strength:

Bytes: 1,300 | 1,676

4 The **Wireless Network Connection Properties** screen displays. Click the **Wireless Networks** tab.

Make sure the **Use Windows to configure my wireless network settings** check box is selected.

Figure 56 Windows XP SP1: Wireless Network Connection Properties



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

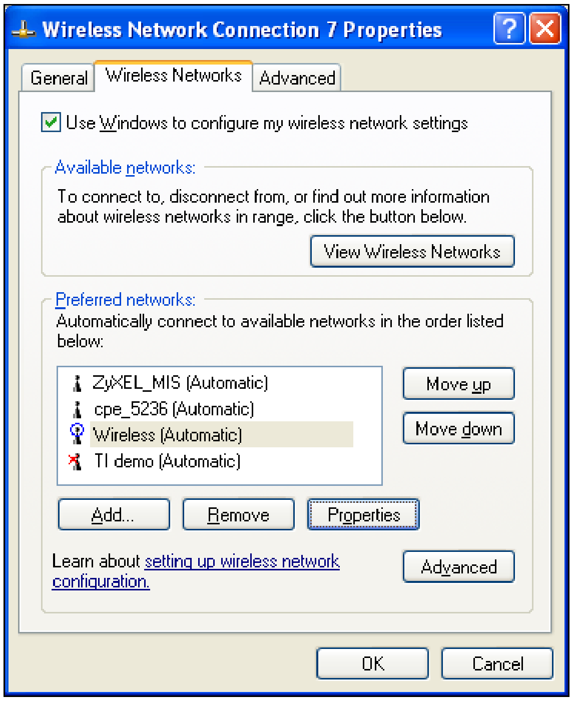
cpe_sw1_5275
cpe_5254_g2kplus
ZW70-1

Automatically connect to available networks in the order listed below:

ZW70-1
pqa-3225-p334w

Learn about setting up wireless network configuration.

Figure 57 Windows XP SP2: Wireless Network Connection Properties



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:

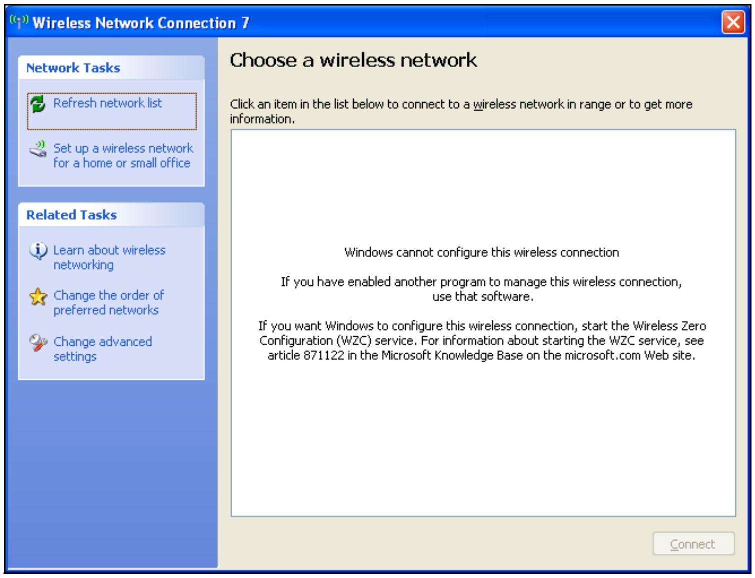
Automatically connect to available networks in the order listed below:

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

Learn about setting up wireless network configuration.

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

Figure 58 Windows XP SP2: WZC Not Available



Wireless Network Connection 7

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.

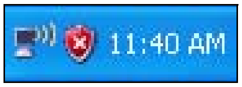
If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.

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

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 59 Windows XP SP2: System Tray Icon



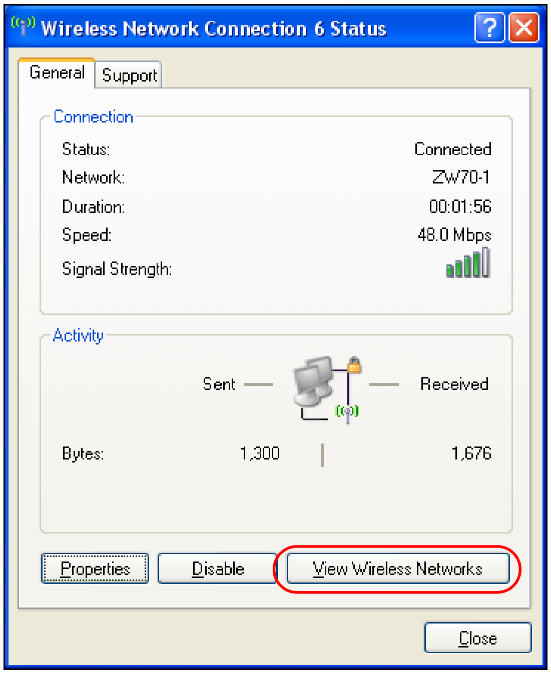
The type of the wireless network icon in Windows XP SP2 indicates the status of the AG-320. Refer to the following table for details.

Table 27 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
🖥	The AG-320 is connected to a wireless network.
🖥	The AG-320 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 AG-320 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 60 Windows XP SP2: Wireless Network Connection Status



Wireless Network Connection 6 Status

General | Support

Connection

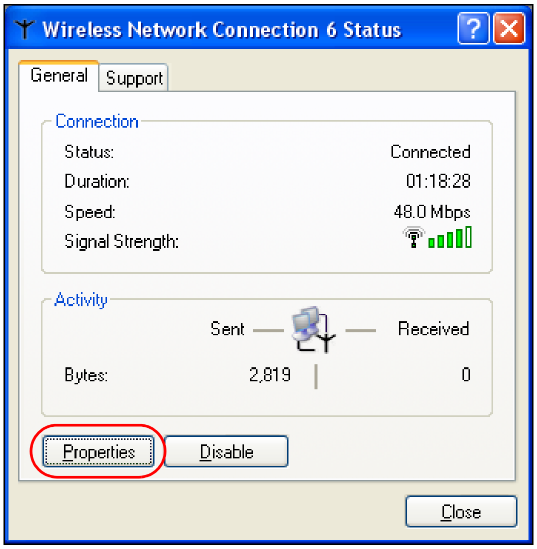
Status:	Connected
Network:	ZW70-1
Duration:	00:01:56
Speed:	48.0 Mbps
Signal Strength:	

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 61 Windows XP SP1: Wireless Network Connection Status



Connection

Status: Connected

Duration: 01:18:28

Speed: 48.0 Mbps

Signal Strength:

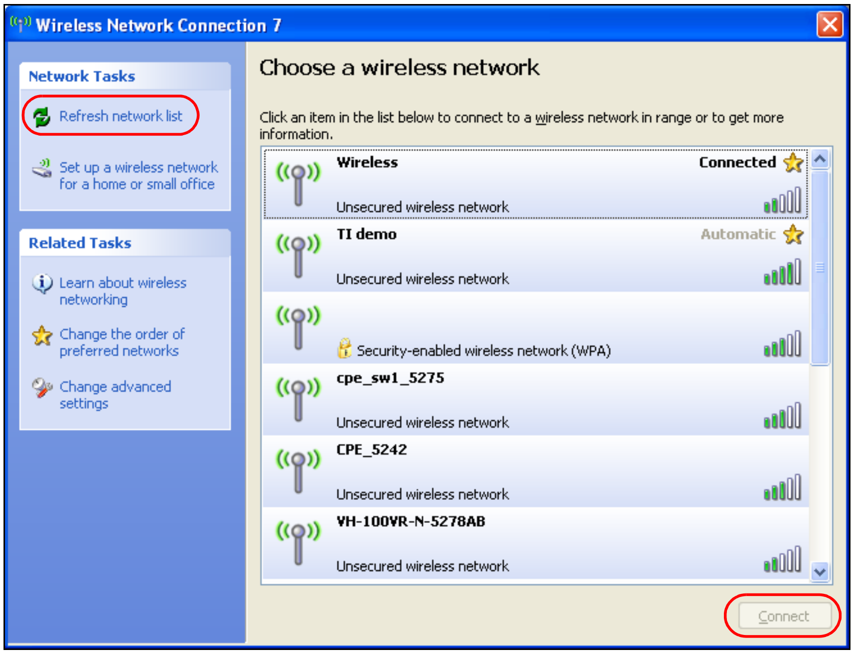
Activity

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 62 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
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.

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

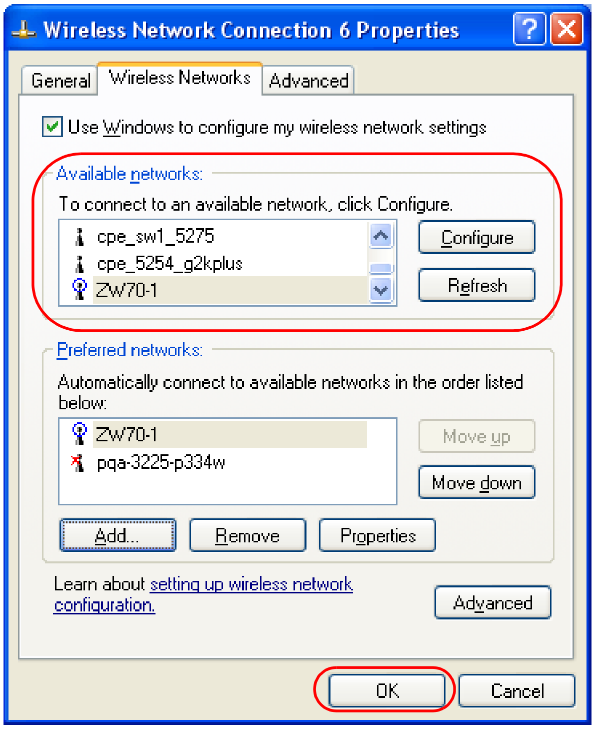
The following table describes the icons in the wireless network list.

Table 28 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 AG-320 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 63 Windows XP SP1: Wireless Network Connection Properties



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:

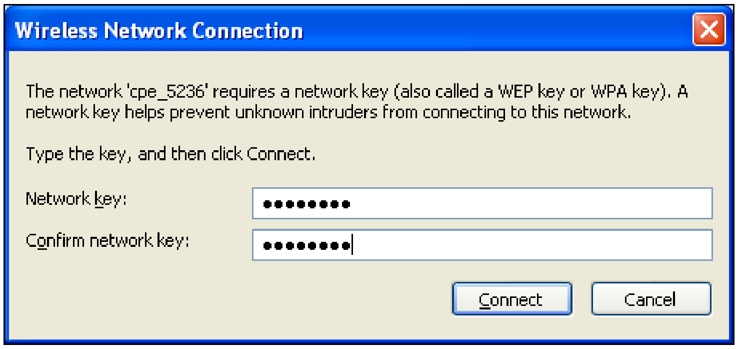
- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

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



Wireless Network Connection

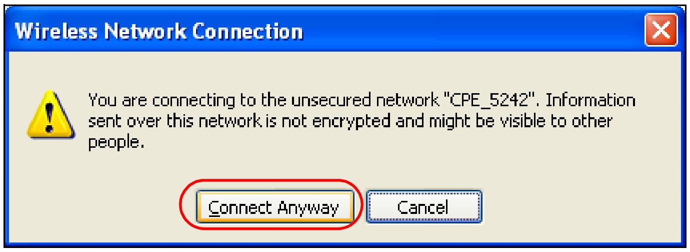
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Figure 65 Windows XP SP2: Wireless Network Connection: No Security



Wireless Network Connection

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 29 Windows XP: Wireless Networks

ICON	DESCRIPTION
📡	This denotes the wireless network is an available wireless network.
(📡)	This denotes the AG-320 is associated to the wireless network.
📡✗	This denotes the wireless network is not available.

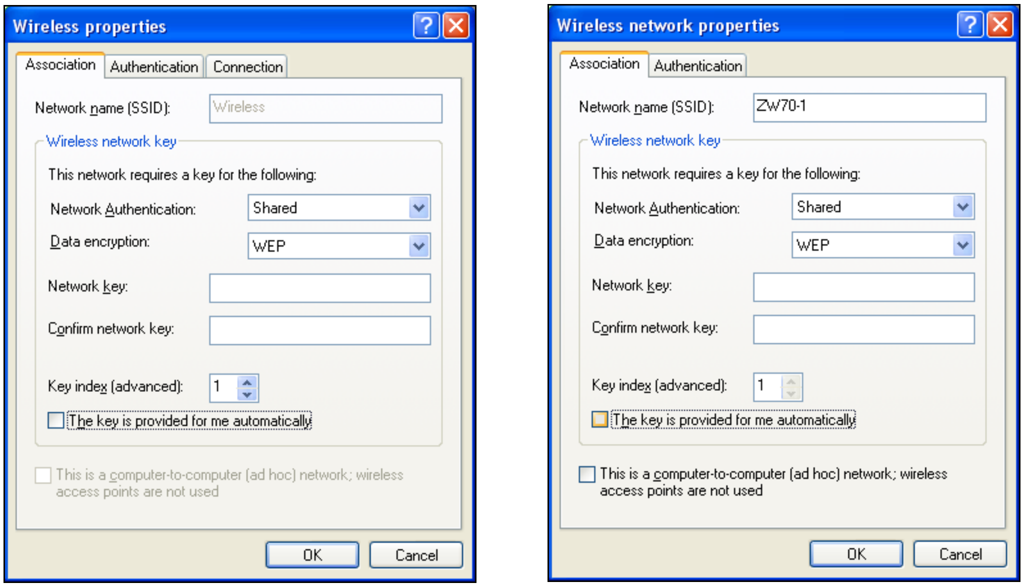
Security Settings

When you configure the AG-320 to connect to a secure network but the security settings are not yet enabled on the AG-320, 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 66 Windows XP: Wireless (network) properties: Association



Wireless properties

Association | Authentication | Connection

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

OK | Cancel

Wireless network properties

Association | Authentication

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

OK | Cancel

The following table describes the labels in this screen.

Table 30 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 AG-320 a key.

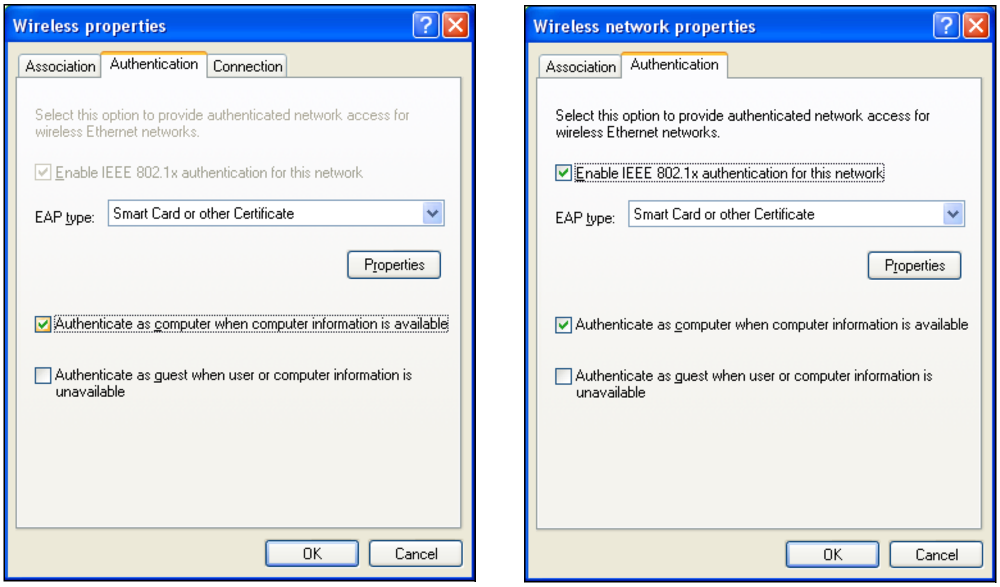
Table 30 Windows XP: Wireless (network) properties: Association (continued)

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

Authentication

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

Figure 67 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 31 Windows XP: Wireless (network) properties: Authentication

LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication. Options are **Protected EAP (PEAP)** and **Smart Card or other Certificate**.
Properties	Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the **EAP type** field.

Table 31 Windows XP: Wireless (network) properties: Authentication (continued)

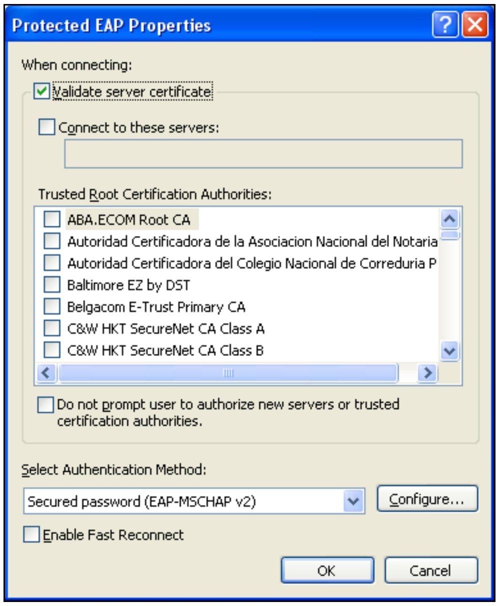
LABEL	DESCRIPTION
Authenticate as computer when computer information is available	Select this check box to have the computer send its information to the network for authentication when a user is not logged on.
Authenticate as guest when user or computer information is unavailable	Select this check box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

Authentication Properties

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

Protected EAP Properties

Figure 68 Windows XP: 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

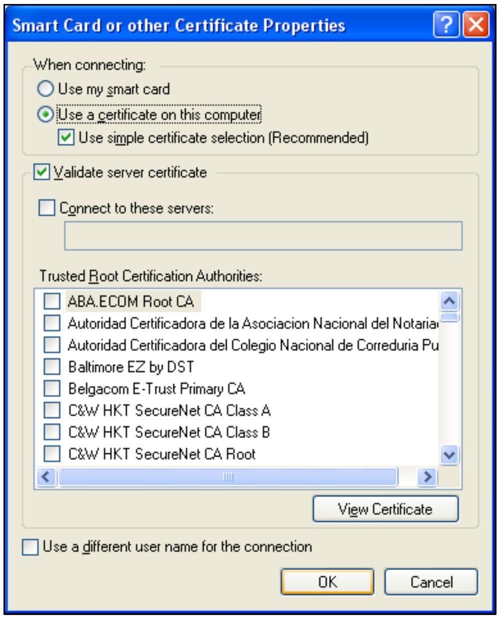
The following table describes the labels in this screen.

Table 32 Windows XP: Protected EAP Properties

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

Smart Card or other Certificate Properties

Figure 69 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 33 Windows XP: Smart Card or other Certificate Properties

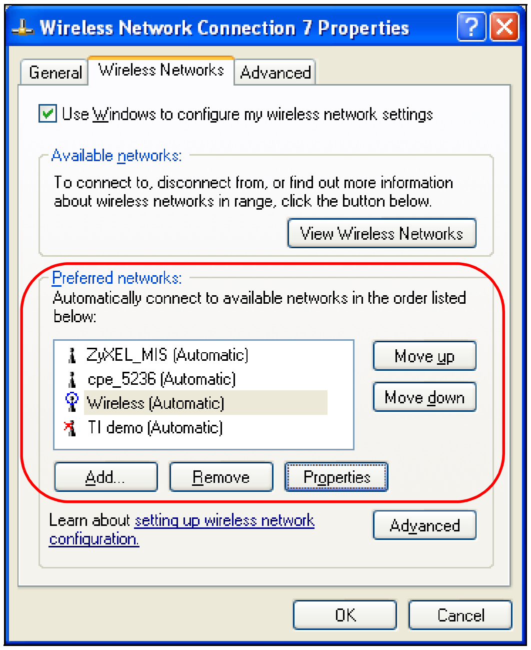
LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication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

Ordering the Preferred Networks

Follow the steps below to manage your preferred networks.

1 Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see Figure 62 on page 83). The screen displays as shown.

Figure 70 Windows XP SP2: Wireless Networks: Preferred Networks



☑ 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.

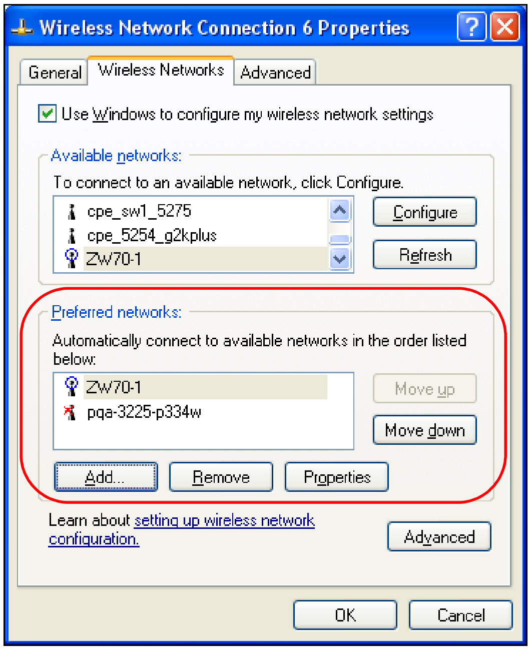
Automatically connect to available networks in the order listed below:

- 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 71 Windows XP SP1: Wireless Networks: Preferred Networks



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

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 AG-320 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 its 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 D
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 digital IDs) 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 34 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 and WPA2

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

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

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

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

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

Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

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

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

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

User Authentication

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

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

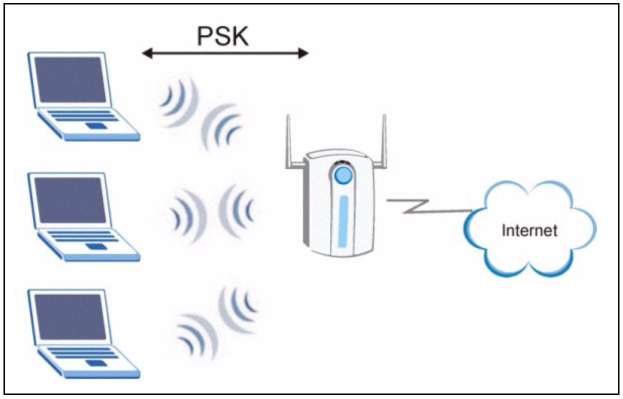
Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WPA(2)-PSK Application Example

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

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP and wireless clients use the pre-shared key to generate a common PMK.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 72 WPA-PSK Authentication

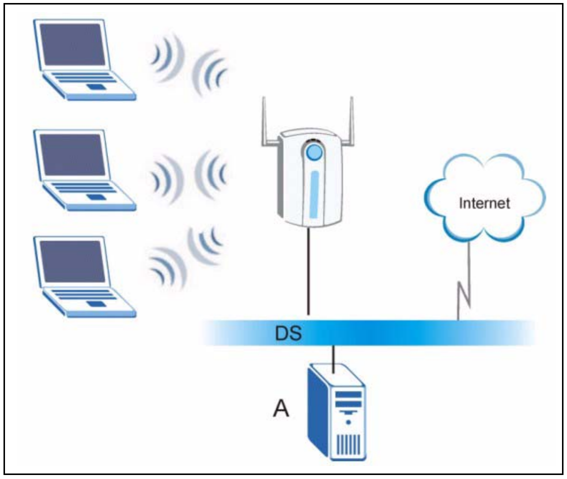


WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 73 WPA(2) with RADIUS Application Example



Security Parameters Summary

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

Table 35 Wireless Security Relational Matrix

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

APPENDIX E
Setting up Your Computer's IP Address

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

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

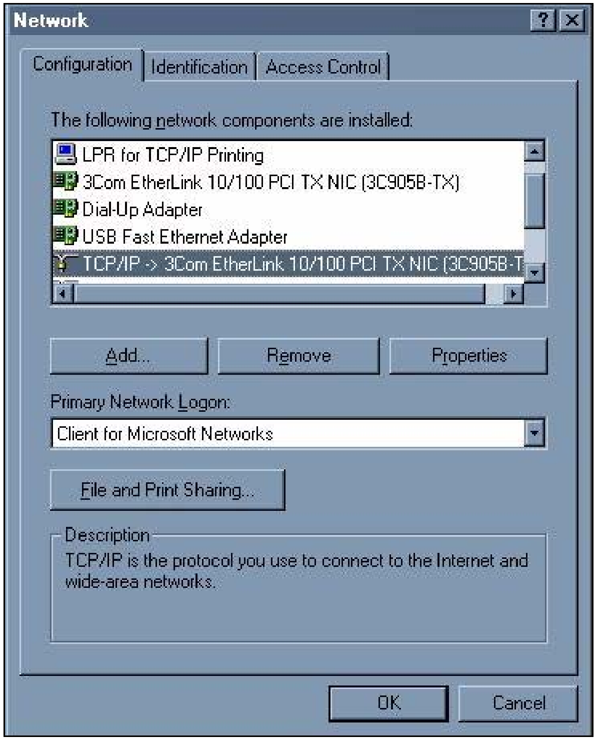
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

Windows 95/98/Me

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

Figure 74 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

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

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

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

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

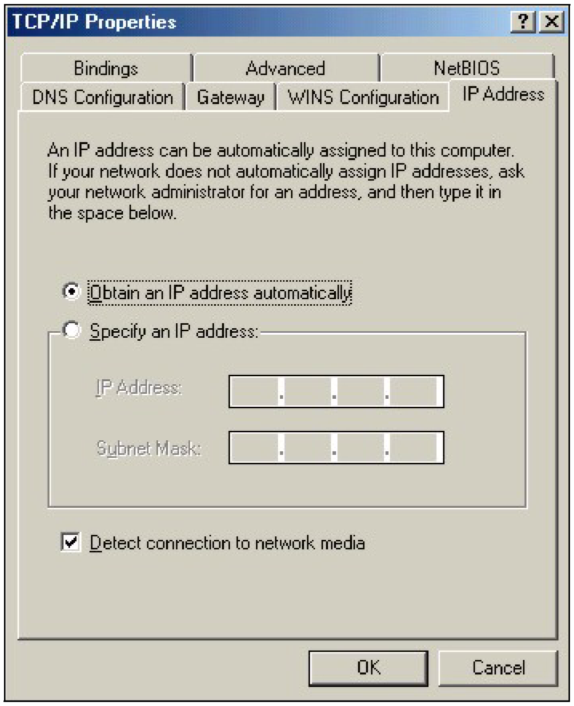
Configuring

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

2 Click the **IP Address** tab.

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

Figure 75 Windows 95/98/Me: TCP/IP Properties: IP Address



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

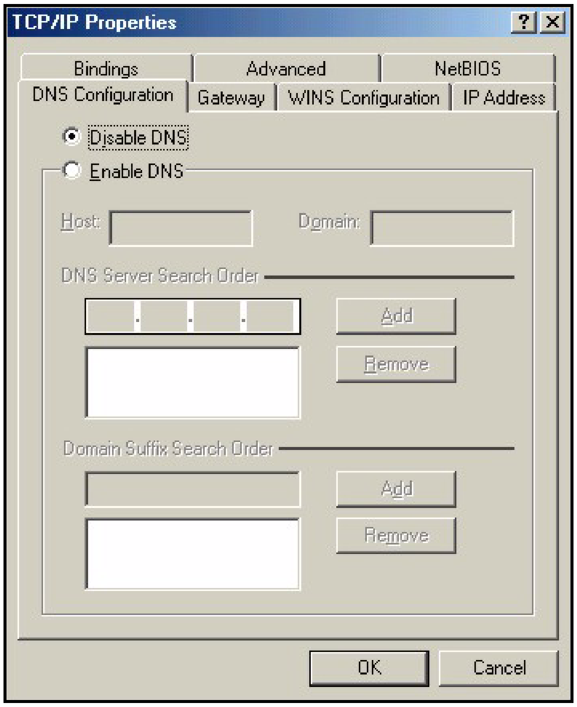
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

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

Figure 76 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

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

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

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

7 Restart your computer when prompted.

Verifying Settings

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

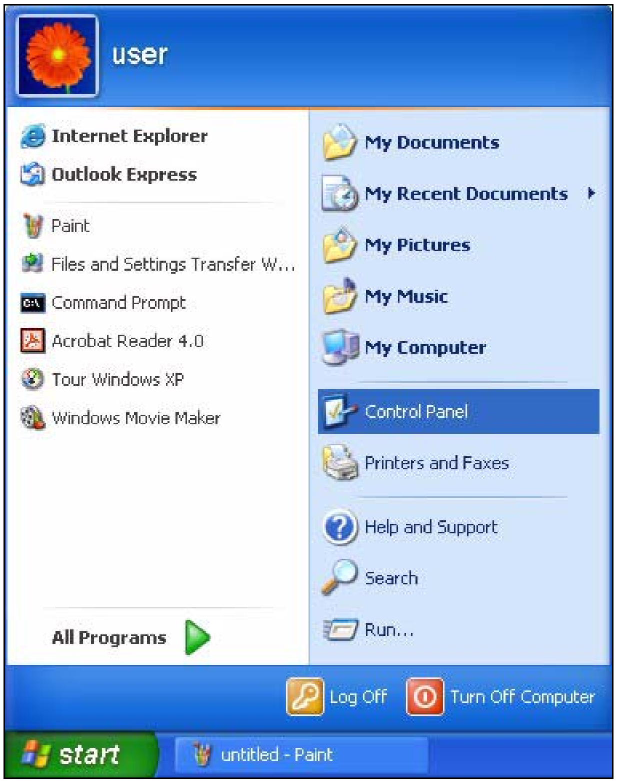
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

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

Windows 2000/NT/XP

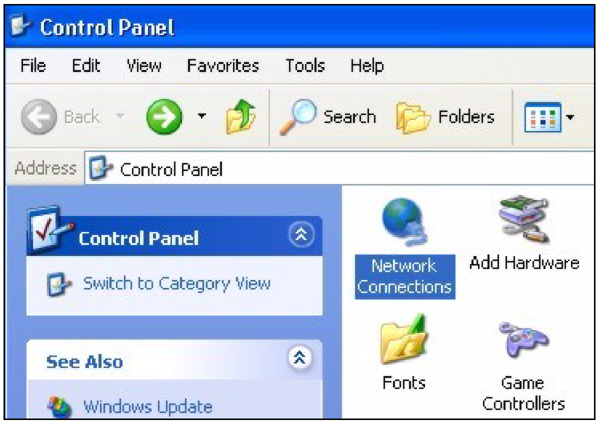
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 77 Windows XP: Start Menu



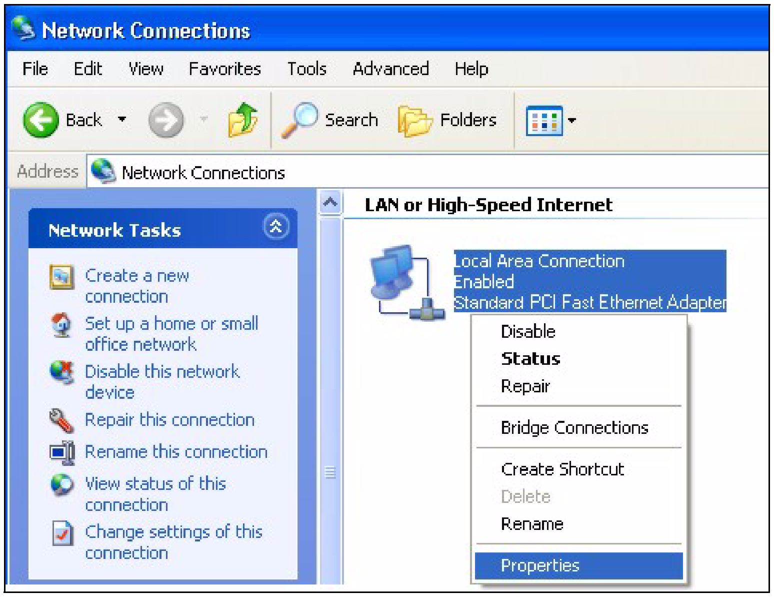
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 78 Windows XP: Control Panel



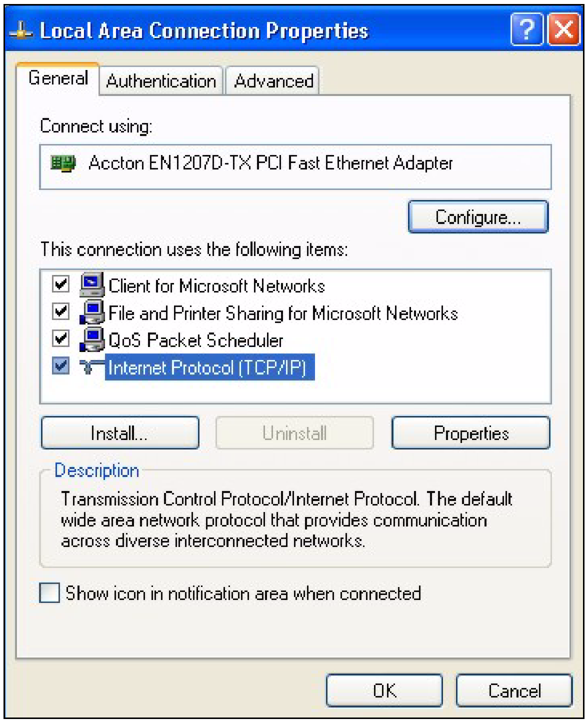
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 79 Windows XP: Control Panel: Network Connections: Properties



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

Figure 80 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

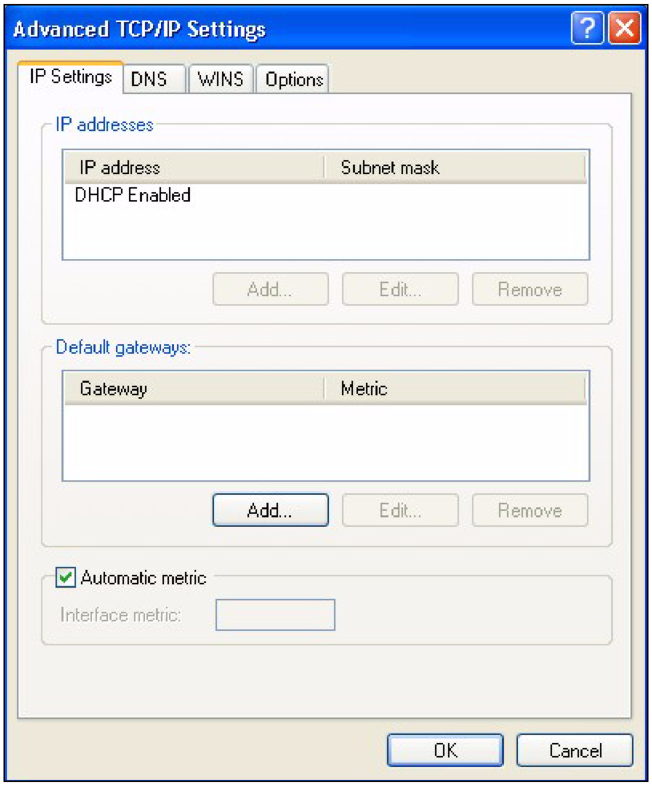
☐ Show icon in notification area when connected

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

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

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

Figure 81 Windows XP: Advanced TCP/IP Settings



DHCP Enabled

☑ Automatic metric

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

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

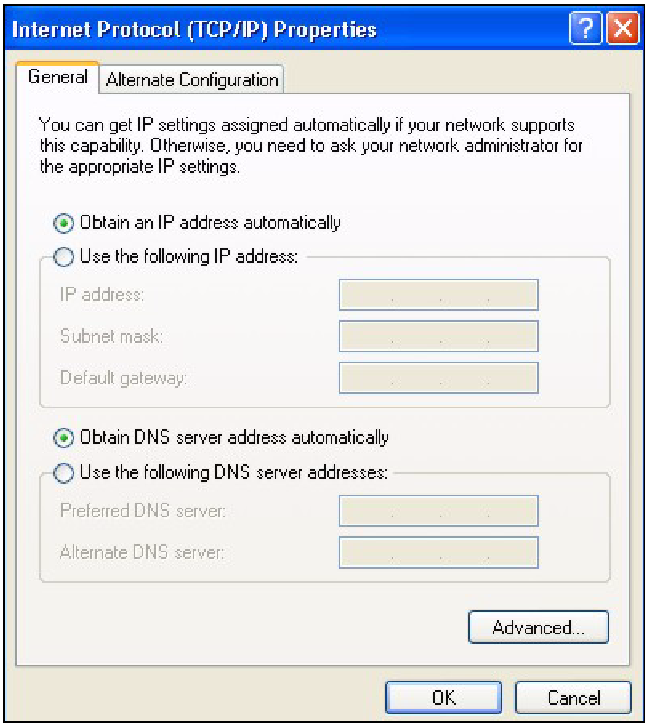
- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the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

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

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

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

Figure 82 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

10Restart your computer (if prompted).

Verifying Settings

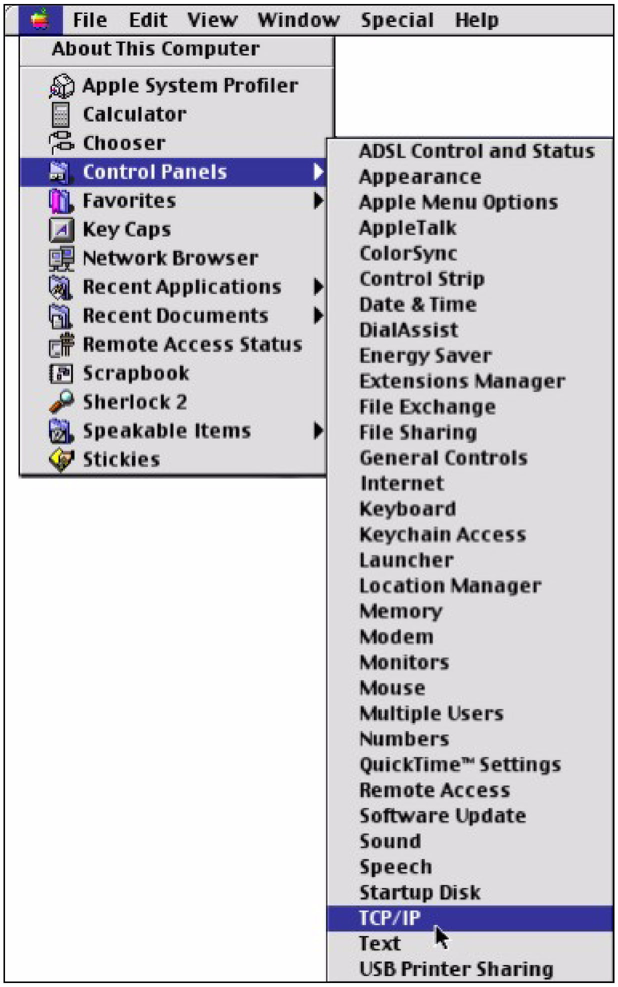
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

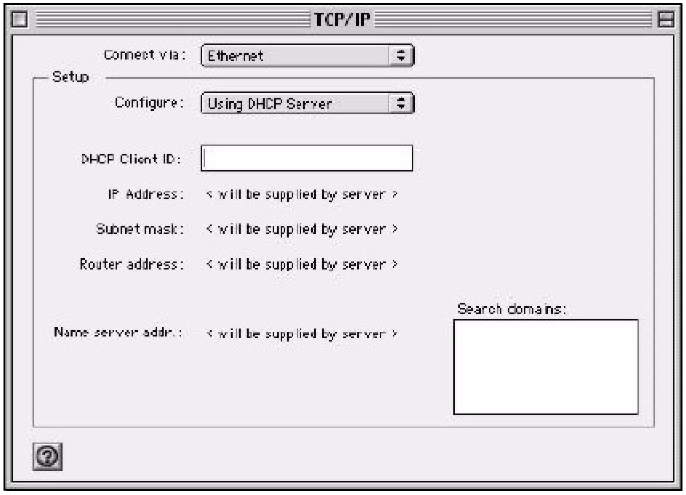
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 83 Macintosh OS 8/9: Apple Menu



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

Figure 84 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box if you have one.

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

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

7 Restart your computer (if prompted).

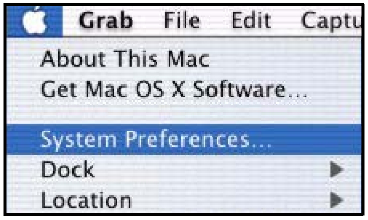
Verifying Settings

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

Macintosh OS X

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

Figure 85 Macintosh OS X: Apple Menu

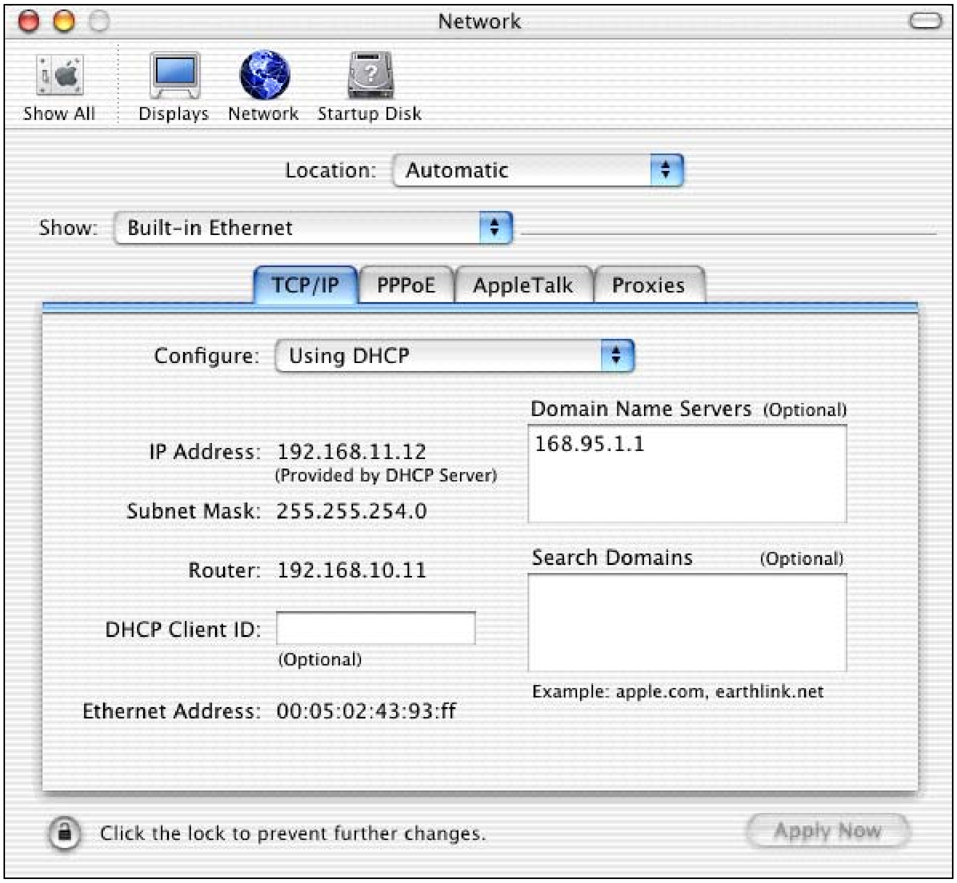


2 Click **Network** in the icon bar.

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

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

Figure 86 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box if you have one.

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

6 Restart your computer (if prompted).

Verifying Settings

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

Index