

G-470

802.11g Wireless Ethernet Adapter

User's Guide

Version 1.00

Edition 1

6/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Z" and "y" are lowercase, while "XEL" are uppercase. The letters are closely spaced and have a slight shadow effect.

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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.

Caution

- 1 The 802.11g Wireless LAN Adapter has been tested to the FCC exposure requirements (Specific Absorption Rate).
- 2 The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
- 3 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.
- 4 This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Notice 1

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

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

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.

注意！

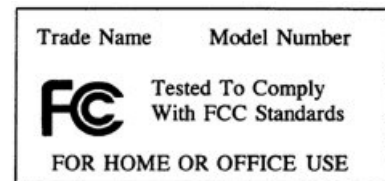
依據 低功率電波輻射性電機管理辦法

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。

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

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

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

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

Table of Contents

Copyright	3
Certifications	4
ZyXEL Limited Warranty	6
Safety Warnings	7
Customer Support	8
Table of Contents	11
List of Figures	15
List of Tables	17
Preface	19
Chapter 1	
Getting Started	21
1.1 About Your ZyXEL Device	21
1.1.1 ZyXEL Device Hardware Installation	22
1.1.2 Application Overview	23
1.1.2.1 Infrastructure	24
1.1.2.2 Roaming	24
Chapter 2	
Tutorial	27
2.1 Connecting to an Access Point	27
2.1.1 Before You Start	27
2.1.2 The Web Configurator	27
Chapter 3	
Wireless LAN Network	31
3.1 Wireless LAN Overview	31
3.2 Wireless LAN Security	32
3.2.1 User Authentication and Encryption	32
3.2.1.1 Certificates	32
3.2.1.2 WEP	33
3.2.1.3 IEEE 802.1x	34
3.2.1.4 WPA	34

3.2.1.5 WPA2	34
Chapter 4	
Introducing the Web Configurator.....	35
4.1 Web Configurator Overview	35
4.1.1 Setting Up Your Computer's IP Address	35
4.1.1.1 Windows 2000/NT/XP	36
4.2 Accessing the Web Configurator	39
4.2.1 The Status Screen	39
4.3 Navigating the Web Configurator	41
4.3.1 Change Your Password	41
4.3.2 Statistics	42
4.4 Configuring the ZyXEL Device Using the Wizard	43
4.4.1 Wizard: Basic Settings	43
4.4.2 Wizard: Wireless Settings	44
4.4.3 Wizard: Security Settings	45
4.4.3.1 Disable	45
4.4.3.2 WEP	46
4.4.3.3 WPA-PSK	47
4.4.4 Wizard: Confirm Your Settings	48
4.5 Using the AP Survey tool	49
4.6 Resetting the ZyXEL Device	49
4.6.1 Restoring Factory Defaults	49
4.6.1.1 Using the RESET Button	50
Chapter 5	
System Screen	51
5.1 TCP/IP Parameters	51
5.1.1 IP Address Assignment	51
5.1.2 IP Address and Subnet Mask	51
5.2 System Settings	52
Chapter 6	
Wireless Screens	55
6.1 Wireless LAN Overview	55
6.1.1 BSS (Infrastructure)	55
6.1.2 ESS	56
6.2 Wireless LAN Basics	56
6.2.1 Channel	56
6.2.2 SSID	57
6.2.3 RTS/CTS	57
6.2.4 Fragmentation Threshold	58
6.3 Configuring Wireless	58

6.3.1 The AP Survey Window	60
6.4 Wireless Security Overview	61
6.5 Configuring Wireless Security	61
6.5.1 Wireless Security: Disable	62
6.5.2 Wireless Security: WEP	62
6.5.3 Wireless Security: WPA(2)-PSK	64
6.5.4 Wireless Security: WPA(2)	64
6.5.5 Wireless Security: IEEE 802.1x	66
Chapter 7	
Management Screens	69
7.1 Management Overview	69
7.2 Password	69
7.3 Configuration File	70
7.3.1 Backup Configuration	71
7.3.2 Restore Configuration	71
7.3.3 Back to Factory Defaults	71
7.4 F/W Upload Screen	72
Chapter 8	
Troubleshooting	75
8.1 Problems Starting Up the ZyXEL Device	75
8.2 Problems with the Password	75
8.3 Problem with the Wireless Link Quality	76
8.4 Problems Communicating With Other Computers	76
8.5 Problems with the Ethernet Interface	77
8.5.1 Pop-up Windows, JavaScripts and Java Permissions	78
8.5.1.1 Internet Explorer Pop-up Blockers	78
8.5.1.2 JavaScripts	81
8.5.1.3 Java Permissions	83
8.6 Testing the Connection to the ZyXEL Device	85
Appendix A	
Product Specifications	87
Appendix B	
Wireless Security	89
Appendix C	
Setting up Your Computer's IP Address.....	95
Index.....	107

List of Figures

Figure 1 Device application: Basic	21
Figure 2 Device Application: Home Network	21
Figure 3 The ZyXEL Device: Front Panel	22
Figure 4 The ZyXEL Device: Rear Panel	23
Figure 5 Application: Infrastructure	24
Figure 6 Roaming Example	25
Figure 7 Example of a Wireless Network	31
Figure 8 Wired Connection	36
Figure 9 Control Panel	36
Figure 10 Network Connection	37
Figure 11 Local Area Connection Properties	37
Figure 12 Internet Protocol Properties	38
Figure 13 Advanced TCP/IP Settings	38
Figure 14 Web Configurator: Login Screen	39
Figure 15 Web Configurator: the Status icon	39
Figure 16 Web Configurator: the Status screen	40
Figure 17 Web Configurator: Change Administrator Login Password	42
Figure 18 View Statistics	42
Figure 19 Setup Wizard 1: Basic Settings	44
Figure 20 Setup Wizard 2: Wireless Settings.	45
Figure 21 Setup Wizard 3: Disable	46
Figure 22 Wizard 3: WEP	47
Figure 23 Wizard 3: WPA(2)-PSK	48
Figure 24 Wizard: Confirm Your Settings	49
Figure 25 System Settings	52
Figure 26 Basic Service set	55
Figure 27 Extended Service Set	56
Figure 28 RTS/CTS	57
Figure 29 Wireless: Wireless Settings	58
Figure 30 Wireless: the AP Survey Screen	60
Figure 31 Wireless Security: Disable	62
Figure 32 Wireless Security: WEP	63
Figure 33 Wireless Security: WPA(2)-PSK	64
Figure 34 Wireless Security: WPA(2)	65
Figure 35 Wireless Security: 802.1x	67
Figure 36 Management: Password	69
Figure 37 Management: Configuration File	70
Figure 38 Management: Configuration Upload Successful	71

Figure 39 Management: Reset Warning Message	71
Figure 40 Management: F/W Upload	72
Figure 41 Management: Firmware Upgrading Screen	73
Figure 42 Network Temporarily Disconnected	73
Figure 43 Management: Firmware Upload Error	73
Figure 44 Pop-up Blocker	78
Figure 45 Internet Options	79
Figure 46 Internet Options: Settings	80
Figure 47 Pop-up Blocker Settings	81
Figure 48 Internet Options: Custom Level	82
Figure 49 Security Settings - Java Scripting	83
Figure 50 Security Settings - Java	84
Figure 51 Java (Sun)	85
Figure 52 Pinging the G-470	85
Figure 53 WPA-PSK Authentication	93
Figure 54 WPA(2) with RADIUS Application Example	93
Figure 55 WIndows 95/98/Me: Network: Configuration	96
Figure 56 Windows 95/98/Me: TCP/IP Properties: IP Address	97
Figure 57 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	98
Figure 58 Windows XP: Start Menu	99
Figure 59 Windows XP: Control Panel	99
Figure 60 Windows XP: Control Panel: Network Connections: Properties	100
Figure 61 Windows XP: Local Area Connection Properties	100
Figure 62 Windows XP: Advanced TCP/IP Settings	101
Figure 63 Windows XP: Internet Protocol (TCP/IP) Properties	102
Figure 64 Macintosh OS 8/9: Apple Menu	103
Figure 65 Macintosh OS 8/9: TCP/IP	103
Figure 66 Macintosh OS X: Apple Menu	104
Figure 67 Macintosh OS X: Network	105

List of Tables

Table 1 The ZyXEL Device: Front Panel Lights.	23
Table 2 The ZyXEL Device: Rear Panel Connections	23
Table 3 Web Configurator: the Status screen	40
Table 4 Status: View Statistics	42
Table 5 Private IP Address Ranges	51
Table 6 System Settings	52
Table 7 Wireless: Wireless Settings	59
Table 8 Wireless: the AP Survey Screen	60
Table 9 Wireless Security Levels	61
Table 10 Wireless Security: Disable	62
Table 11 Wireless Security: WEP	63
Table 12 Wireless Security: WPA-PSK	64
Table 13 Wireless Security: WPA(2)	65
Table 14 Wireless Security: 802.1x	67
Table 15 Management: Password	69
Table 16 Management: Configuration File: Restore Configuration	71
Table 17 Management: F/W Upload	72
Table 18 Troubleshooting the Start-Up of Your ZyXEL Device	75
Table 19 Troubleshooting the Password	75
Table 20 Troubleshooting Link Quality	76
Table 21 Troubleshooting the Ethernet Interface	76
Table 22 Troubleshooting the Ethernet Interface	77
Table 23 Product Specifications	87
Table 24 Comparison of EAP Authentication Types	90
Table 25 Wireless Security Relational Matrix	94

Preface

Congratulations on your purchase of the G-470 802.11g Wireless Ethernet Adapter.

Note: 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.

Your ZyXEL Device is easy to install and configure. This User's Guide is designed to guide you through the configuration of your ZyXEL Device using the web configurator.

Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Quick Start Guide

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

- ZyXEL Glossary and Web Site

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





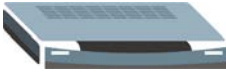



User's Guide Feedback

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

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The G-470 802.11g Wireless Ethernet Adapter may be referred to as the ZyXEL Device in this user's guide.

Graphics Icons Key

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

CHAPTER 1

Getting Started

This chapter introduces the ZyXEL Device and prepares you to use the Web Configurator.

1.1 About Your ZyXEL Device

The G-470 is an IEEE 802.11g compliant wireless LAN Ethernet adapter.

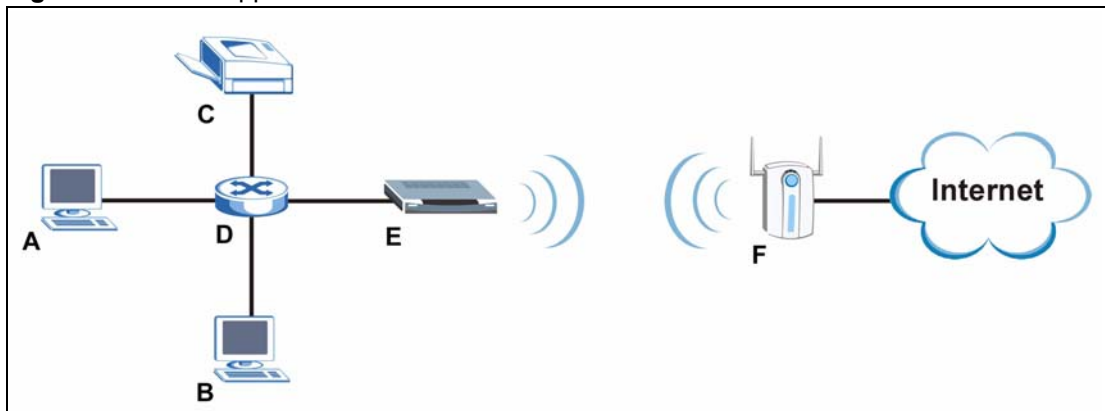
It acts as a bridge between your computer and a wireless network access point (AP) as in the following diagram, where **A** is your computer, **B** is the ZyXEL Device and **C** is the access point.

Figure 1 Device application: Basic



You can also use the ZyXEL Device to connect your home or small office network to a wireless network access point (AP) as in the following diagram, where **A** and **B** are your computers, **C** is your network printer, **D** is your Ethernet switch, **E** is the ZyXEL Device and **F** is the access point. When using a switch or router, up to sixteen network devices can access the Internet through the ZyXEL Device at any one time.

Figure 2 Device Application: Home Network



With the ZyXEL Device, you can enjoy wireless mobility within the coverage area.

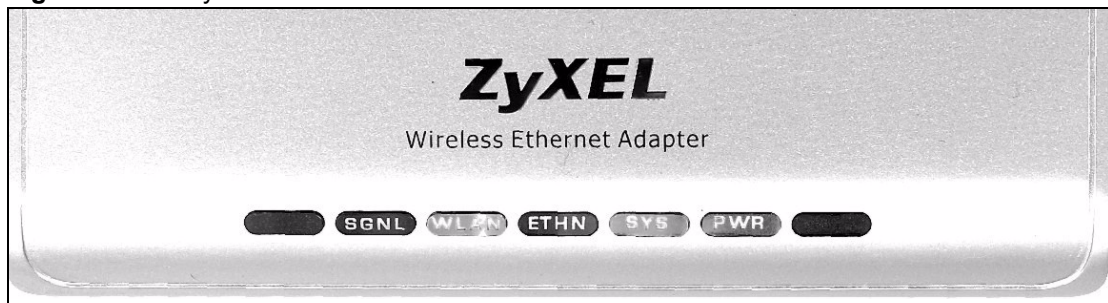
The following lists the main features of your ZyXEL Device. See the product specifications in the appendix for detailed features.

- **Hardware**
 - An external antenna.
 - Lights to indicate power, device status, LAN status, WLAN status and link quality.
 - Easy, driver-free installation.
- **Wireless LAN**
 - Your device can communicate with other IEEE 802.11b/g compliant wireless devices.
 - Automatic data rate selection.
 - Roaming capability.
- **Ethernet**
 - A built-in RJ-45 Ethernet port that connects to any Ethernet device.
 - DHCP client support.
 - Power over Ethernet (PoE) support.
- **Management**
 - The ZyXEL Device allows you to locate and configure the device from any computer on the network.
 - Embedded web-based configurator.
 - Firmware upgradeable.
- **Security**
 - Offers 64-bit and 128-bit WEP (Wired Equivalent Privacy) data encryption for network security.
 - Supports IEEE802.1x, Wi-Fi Protected Access (WPA) and WPA2.
 - Password-protected management interface.

1.1.1 ZyXEL Device Hardware Installation

- Follow the instructions in the Quick Start Guide to make hardware connections.

Figure 3 The ZyXEL Device: Front Panel



The following table describes the front panel of the ZyXEL Device.

Table 1 The ZyXEL Device: Front Panel Lights.

LIGHT	STATUS	DESCRIPTION
POWER	The light is on.	The power is on.
	The light is off.	The power is off.
STATUS	The light is off.	The device is ready.
	The light is blinking orange.	The device is not ready, or is rebooting.
LAN	The light is on.	Ethernet is connected.
	The light is blinking.	Ethernet is connected, and is sending or receiving data.
	The light is off.	Ethernet is not connected.
WLAN	The light is on.	The device is connected to the wireless network.
	The light is blinking.	The device is scanning for an access point (AP).
	The light is off.	The device is not connected to the wireless network.
SIGNAL	The blinking frequency of the SIGNAL light indicates the quality of the wireless signal.	
	The light is steady on.	Signal strength is 80% or more.
	The light is blinking once a second.	Signal strength is between 60 and 79%.
	The light is blinking twice a second.	Signal strength is between 30 and 59%.
	The light is blinking four times a second.	Signal strength is below 29%.
	The light is off.	The wireless network is not connected.

Figure 4 The ZyXEL Device: Rear Panel



The following table describes the rear panel of the ZyXEL Device.

Table 2 The ZyXEL Device: Rear Panel Connections

LABEL	DESCRIPTION
1	External antenna connector (R-SMA type)
2	Reset button
3	ETHERNET port
4	POWER socket

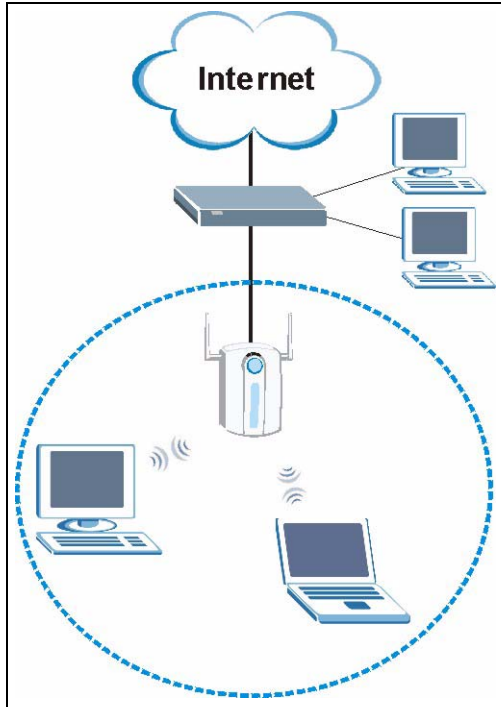
1.1.2 Application Overview

This section describes some network applications for the ZyXEL Device.

1.1.2.1 Infrastructure

Infrastructure mode allows your ZyXEL Device to connect to a network via an access point (AP). Through the AP, you can access the Internet or the wired network behind the AP.

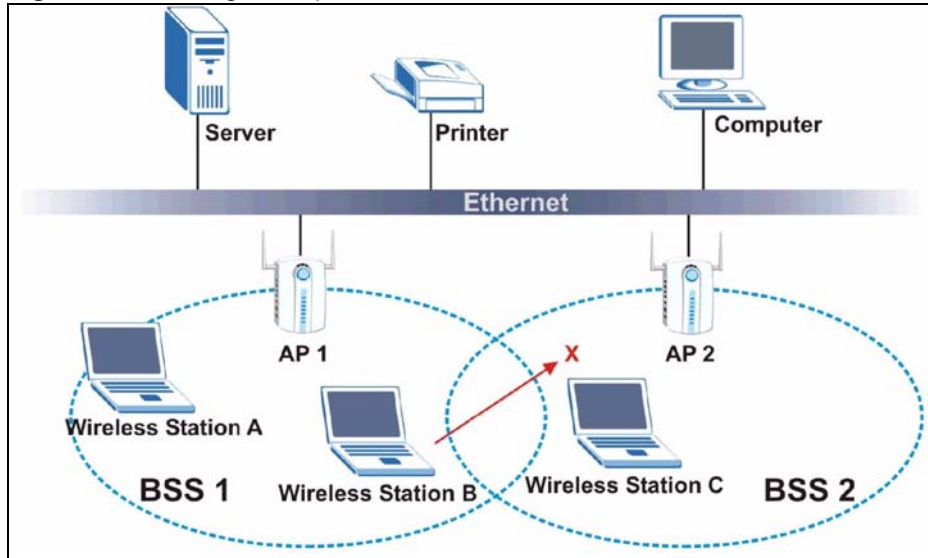
Figure 5 Application: Infrastructure



1.1.2.2 Roaming

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

The following figure depicts a roaming example. When Wireless Station **B** moves to position **X**, its wireless device automatically switches the channel to the one used by access point **AP 2** in order to stay connected to the network.

Figure 6 Roaming Example

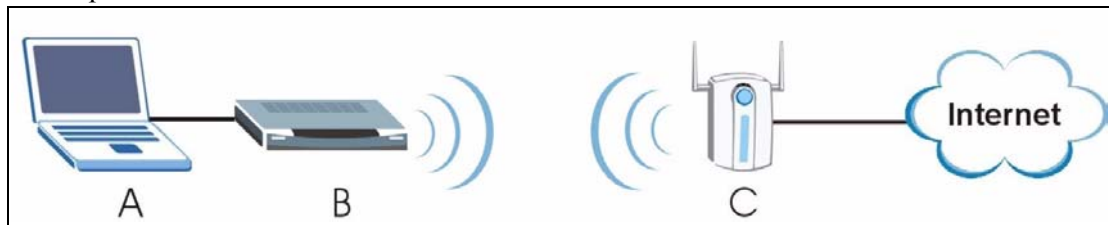
CHAPTER 2

Tutorial

2.1 Connecting to an Access Point

This example shows you how to connect your ZyXEL Device to an access point (AP) configured for WPA-PSK security, in order to access the Internet.

In the following diagram, your computer is labeled **A**, the ZyXEL Device is labeled **B** and the access point is labeled **C**.



2.1.1 Before You Start

Before you connect to the AP, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key.

In this example, the AP's SSID is "AP6" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

Connect your ZyXEL Device to your computer's Ethernet port and set your computer's IP address as shown in the Quick Start Guide.

2.1.2 The Web Configurator

Use the following steps to set up your Internet connection using the Web Configurator.

- 1 Open your Internet browser and enter 192.168.1.11 in the Address (URL) bar.

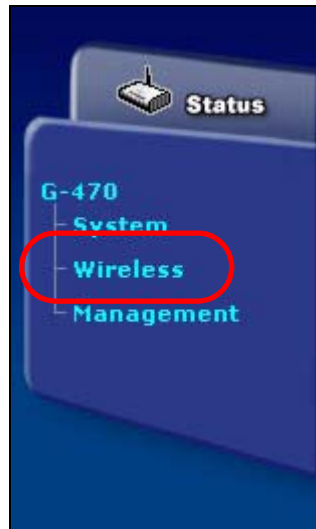
Address	192.168.1.11
---------	--------------

2 The **Login** screen appears. Enter **admin** as the username and **1234** as the password, then click **Login**.



The screenshot shows the login interface for the G-470 Embedded Web Configurator. At the top, it says "G-470" and "Welcome to the G-470 Embedded Web Configurator! Enter your username and password, and click to login." Below this are two input fields: "Username:" with the text "admin" and "Password:" with "****". A note below the password field states "(max. 19 alphanumeric, printable characters)". At the bottom, there is a "Note:" icon and text: "Please turn on the Javascript and ActiveX control setting on Internet Explorer." Two buttons, "Login" and "Reset", are located at the bottom center.

3 In the **Status** screen, click on **Wireless**.



- 4 The **Wireless Settings** screen appears. Click **AP Survey** to search for available wireless access points.

Wireless Settings Security

Basic Settings

SSID: ZyXEL (max. 32 printable characters) **AP Survey**

Wireless Mode: Mixed Mode

Clone Mac Address: Disable Auto-Single Auto-Multi Manual Clone MAC Address:

Advanced Settings

Radio Enable: Yes No

Output Power Management: Full

Data Rate Management: best

Preamble Type: Dynamic

RTS/CTS Threshold: 2345 (0~2345)

Fragmentation Threshold: 2340 (256~2340)

Apply **Reset**

The **Access Point List** screen displays. The **Security Mode** entry shows that AP6 is using WPA-PSK security with TKIP data encryption.

Access Point List

No.	SSID	Channel	Signal Strength	Security Mode
1	AP6	6	94%	[WPA-PSK-TKIP]

Rescan

- 5 Click on the **AP6** entry. The **AP Survey** window closes, and the entry **AP6** now appears in the **Wireless Settings** screen's **SSID** field.

Wireless Settings Security

Basic Settings

SSID: AP6 (max. 32 printable characters) **AP Survey**

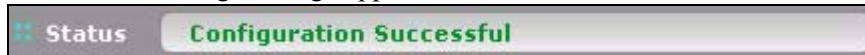
Wireless Mode: Mixed Mode

- 6 In the **Wireless Settings** screen's **Advanced Settings** section, ensure that **Radio Enable** is checked **Yes**.

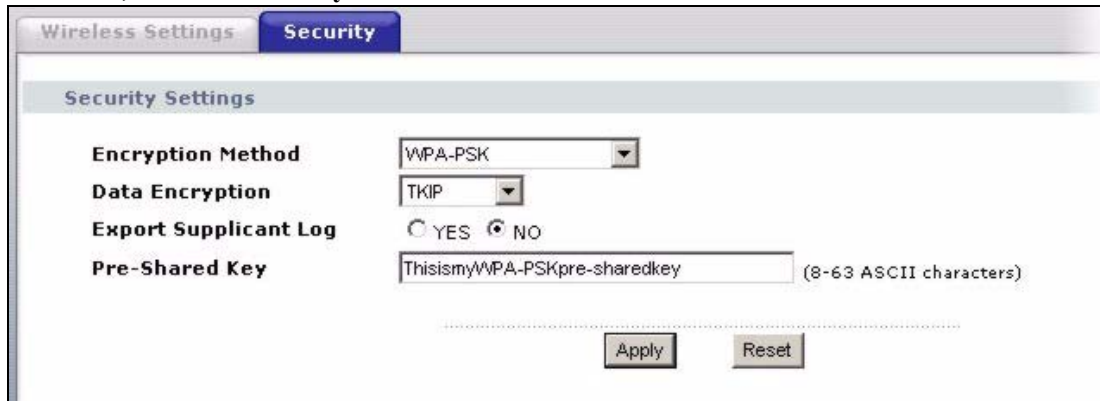
Radio Enable Yes No

- 7 Click **Apply** to save your wireless settings.

The following message appears in the **Status** bar.

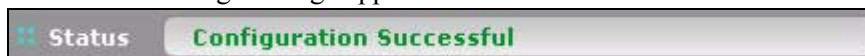


8 Next, click the **Security** tab.



In the **Security** screen, select **WPA-PSK** from the **Encryption Method** menu. Select **TKIP** from the **Data Encryption** menu. Enter your PSK "ThisismyWPA-pre-sharedkey" in the **Pre-Shared Key** box and click **Apply**.

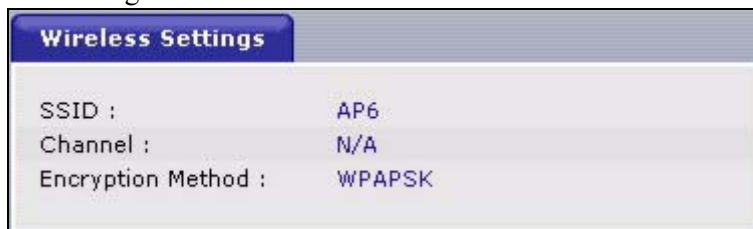
The following message appears in the **Status** bar.



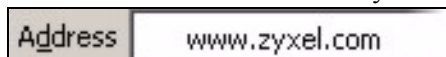
The ZyXEL Device automatically tries to connect to the AP using your settings. The following message then appears in the **Link Status** bar.




9 Go back to the **Status** screen, and check that your wireless settings are correctly configured.



Enter a web site's URL in your Internet browser's address bar.



If you are able to access the web site, your wireless connection is successfully configured. Go back to the Web Configurator and log out ().

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

CHAPTER 3

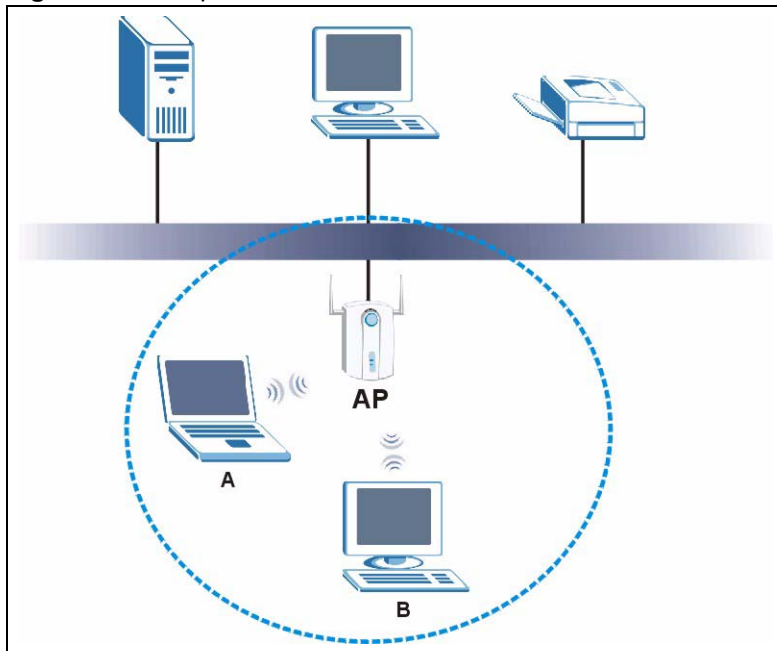
Wireless LAN Network

This chapter provides background information on wireless LAN networks.

3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP.

Figure 7 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.

If you do not enable any wireless security on your ZyXEL Device, the ZyXEL Device's wireless communications are accessible to any wireless networking device that is in the coverage area. See [Section 6.4 on page 61](#) for more information on configuring wireless security for your device.

3.2.1 User Authentication and Encryption

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

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

3.2.1.1 Certificates

Your ZyXEL Device can use certificates (also called digital IDs) for user authentication. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.

- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

3.2.1.2 WEP

3.2.1.2.1 Data Encryption

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

There are two ways to create WEP keys in your ZyXEL Device.

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

For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the Security Settings screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

Your ZyXEL Device allows you to configure up to four 64-bit or 128-bit WEP keys. Only one key is used as the default key at any one time.

3.2.1.2.2 Authentication Type

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

- Open System mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key (WEP key). Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- Shared Key mode involves a shared secret key (WEP key) to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- Auto authentication mode allows the ZyXEL Device to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

3.2.1.3 IEEE 802.1x

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

3.2.1.3.1 EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. The ZyXEL Device supports EAP-TLS, EAP-TTLS and EAP-PEAP. Refer to the Wireless Security appendix for descriptions.

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

3.2.1.4 WPA

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

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

Select WEP only when the AP does not support WPA. WEP is less secure than WPA.

3.2.1.5 WPA2

WPA 2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

CHAPTER 4

Introducing the Web Configurator

This chapter shows you how to configure the ZyXEL Device using the embedded web configurator.

4.1 Web Configurator Overview

The embedded web configurator allows you to manage the ZyXEL Device from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels.

In order to use the web configurator you need to allow:

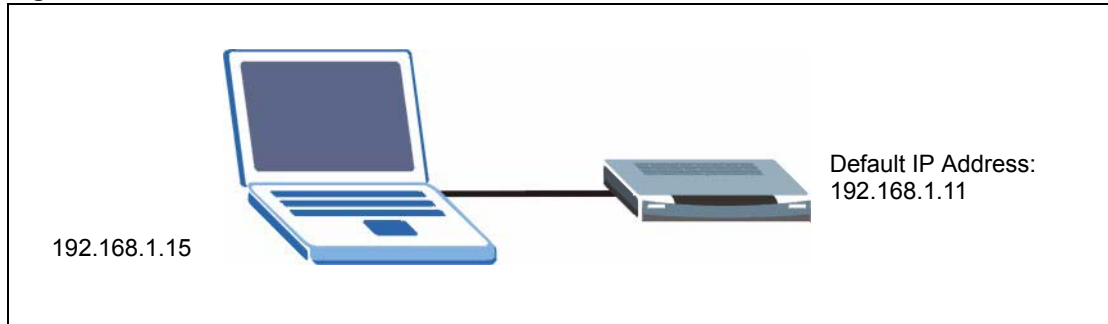
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

4.1.1 Setting Up Your Computer's IP Address

You must prepare your computer / computer network to connect to the ZyXEL Device. Your computer's IP address and subnet mask must be on the same subnet as the ZyXEL Device. This can be done by setting up your computer's IP address.

The following figure shows you an example of accessing your ZyXEL Device via a wired connection with an Ethernet cable.

Figure 8 Wired Connection

Note: Skip this section if your computer's IP address is already between 192.168.1.12 and 192.168.1.254 with subnet mask 255.255.255.0.

Your computer must have a network card and TCP/IP installed. TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems. Refer to the appendix about setting up your computer's IP address for other operating systems.

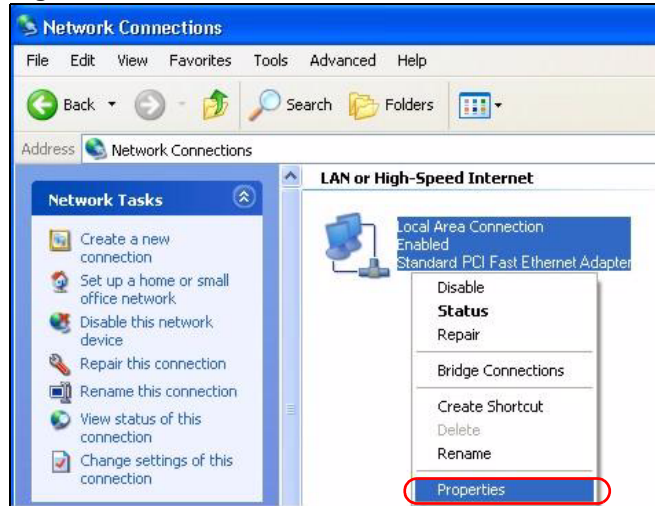
4.1.1.1 Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme. For details on setting up your computer's IP address using other operating systems, refer to the appendices.

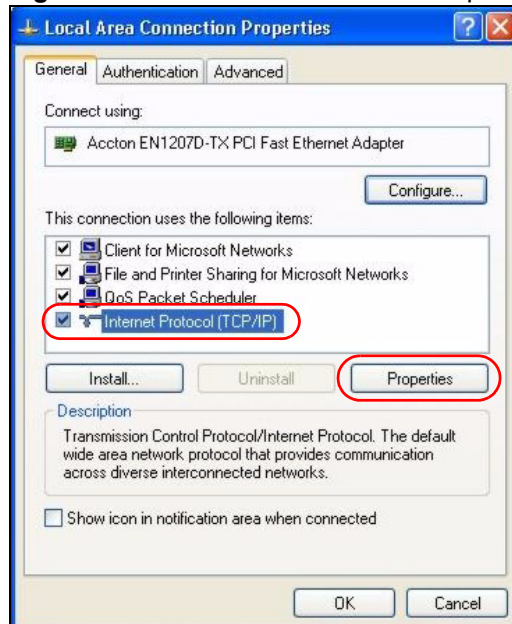
- 1 Click **start (Start in Windows 2000/NT) > Settings > Control Panel**.
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections in Windows 2000/NT)**.

Figure 9 Control Panel

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

Figure 10 Network Connection

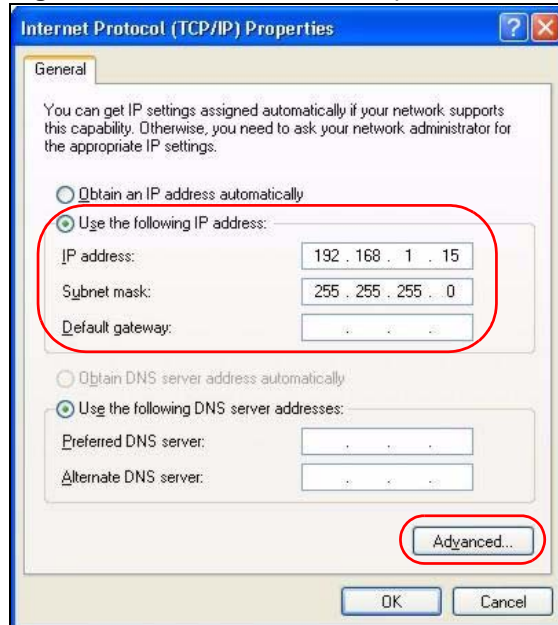
4 Select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 11 Local Area Connection Properties

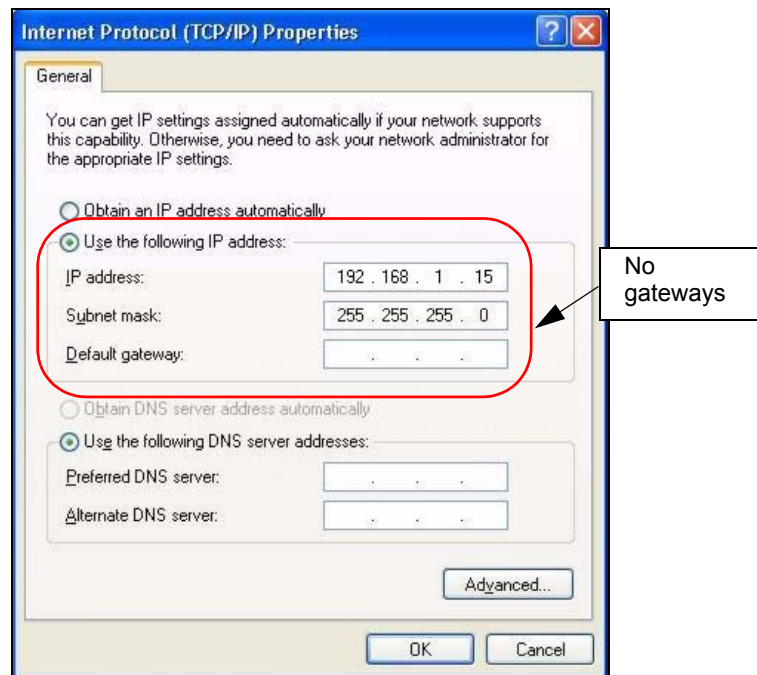
5 Select **Use the following IP Address** and fill in an **IP address** (between 192.168.1.12 and 192.168.1.254).

- Type 255.255.255.0 as the **Subnet mask**.
- Click **Advanced**¹.

1. See the appendices for information on configuring DNS server addresses.

Figure 12 Internet Protocol Properties

- 6** Remove any previously installed gateways in the **IP Settings** tab and click **OK** to go back to the **Internet Protocol TCP/IP Properties** screen.

Figure 13 Advanced TCP/IP Settings

- 7** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.

Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

4.2 Accessing the Web Configurator

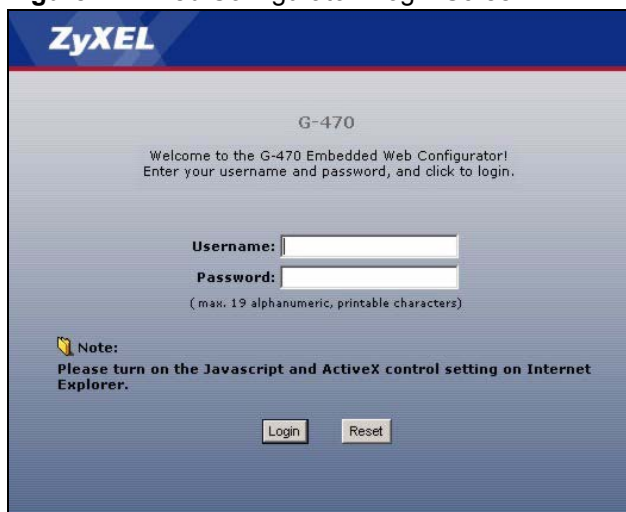
Follow the steps below to access the web configurator using a web browser.

- 1 Make sure your ZyXEL Device is properly connected and prepare your computer/network to connect to the G-470.
- 2 Launch your web browser.
- 3 Type <http://192.168.1.11> (default) as the URL and press [ENTER].

Address	<input type="text" value="http://192.168.1.11"/>
---------	--

- 4 A login screen displays as shown.

Figure 14 Web Configurator: Login Screen



- 5 Enter **admin** (default) as the username and **1234** (default) as the password and click **Login**.

The **Status** screen displays.

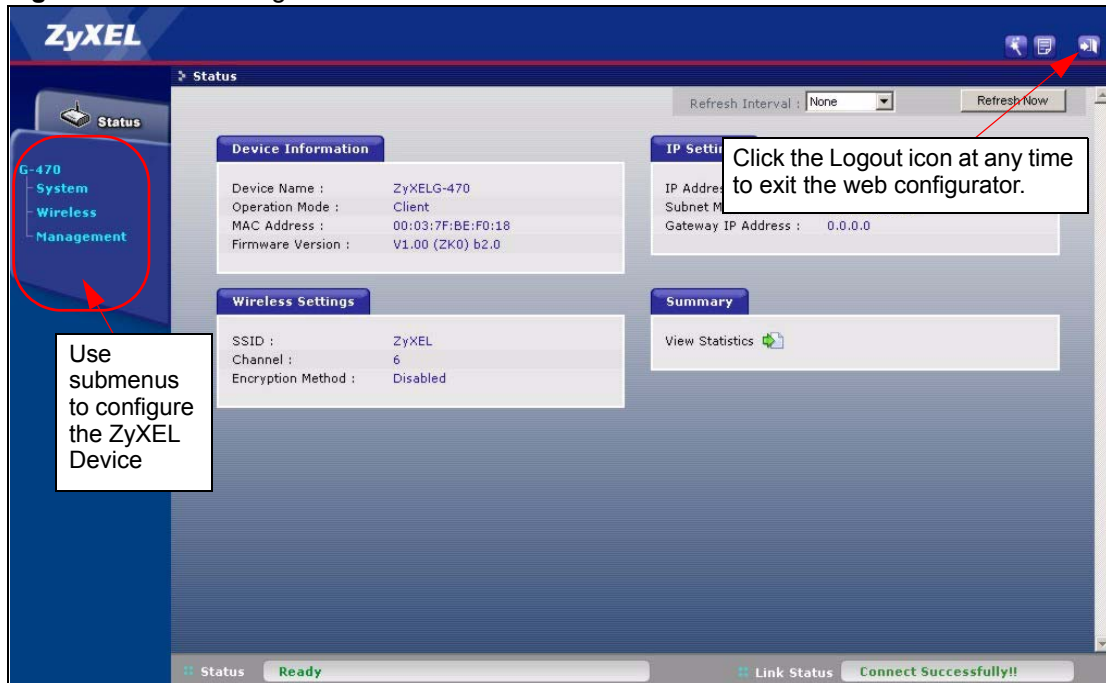
4.2.1 The Status Screen

The **Status** screen displays every time you access the web configurator and can also be accessed by clicking on the **Status** icon. The Status screen displays a snapshot of your device's settings. You can also view network statistics and a list of wireless stations currently associated with your device. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 15 Web Configurator: the Status icon






This screen shows the current configuration of your ZyXEL Device.

Figure 16 Web Configurator: the Status screen

The following table describes the labels in this screen.

Table 3 Web Configurator: the Status screen

LINK/ICON		FUNCTION
Wizard		Use these screens for initial configuration including general setup, wireless and security settings.
About		Click this icon to see details about your ZyXEL Device.
Logout		Click this icon to exit the web configurator.
Status		Use this screen to look at the ZyXEL Device's general device, system and interface status information.
System		Use this screen to change the name of the device and change IP address settings.
Wireless	Wireless Settings	Use this screen to check for available access points and configure basic and advanced wireless network setup.
	Security	Use this screen to configure encryption settings.
Management	Password	Use this screen to change your password.
	Configuration File	Use this screen to backup and restore configuration files and reset the ZyXEL Device to its factory default settings.
	F/W Upload	Use this screen to upload new firmware.
Device Information	Device Name	This is the same as the device name you entered in the first wizard screen if you entered one there. It is for identification purposes.

LINK/ICON		FUNCTION
	MAC Address	This field displays the MAC address of the device. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer. A network interface device such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
	Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Wireless Settings	SSID	This is the name used to identify the ZyXEL Device in the wireless LAN. The default SSID is "ZyXEL".
	Channel	This is the channel number used by the ZyXEL Device now.
	Encryption Method	This displays the type of wireless security used by the ZyXEL Device now.
IP Settings	IP Address	This field displays the IP address of the device.
	Subnet Mask	This field displays the subnet mask of the device.
	Gateway IP Address	This field displays the IP address of the gateway device.
Summary	View Statistics	Click View Statistics to see performance statistics such as number of packets sent and number of packets received.
Status		This field shows messages about the ZyXEL Device's current condition.
Link Status		This field shows messages about the quality of the ZyXEL Device's wireless connection.
Refresh Interval		Use the drop-down list box to select how often you want the device to renew the information on this screen.
Refresh Now		Click this button to have the device renew the information on this screen.

4.3 Navigating the Web Configurator

The following section summarizes how to navigate the web configurator from the **Status** screen.

4.3.1 Change Your Password

After you log in for the first time, it is strongly recommended that you change the default administrator password.

Click **Management** on the left of the **Status** screen to access the following screen.

Figure 17 Web Configurator: Change Administrator Login Password

Enter a new password between 1 and 19 characters, retype it to confirm and click **Apply**. Click on **Reset** to clear all fields.

4.3.2 Statistics

Click **View Statistics** in the **Status** screen. This screen displays read-only information including port status and packet specific statistics. Also provided are "system up time" and "poll interval". The **Poll Interval** field is configurable.

Figure 18 View Statistics

View Status		
Ethernet		
	Received	Transmitted
Packets	1980	2081
Bytes	225615	917508
Wireless		
	Received	Transmitted
Unicast Packets	0	2
Broadcast Packets	0	6
Multicast Packets	0	0
Total Packets	0	8
Total Bytes	0	1109
System Up Time : 0:57:40		
Poll Interval : 5 sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>		

The following table describes the labels in this screen.

Table 4 Status: View Statistics

LABEL	DESCRIPTION
Ethernet	
Packets	This row displays the numbers of packets received and transmitted by the Ethernet port.

Table 4 Status: View Statistics

LABEL		DESCRIPTION
Bytes		This row displays the numbers of bytes received and transmitted by the Ethernet port.
Wireless		
	Unicast Packets	This row displays the numbers of unicast packets received and transmitted by the wireless adapter.
	Broadcast Packets	This row displays the numbers of broadcast packets received and transmitted by the wireless adapter.
	Multicast Packets	This row displays the numbers of multicast packets received and transmitted by the wireless adapter.
	Total Packets	This row displays the numbers of all types of packets received and transmitted by the wireless adapter.
	Total Bytes	This row displays the numbers of bytes received and transmitted by the wireless adapter.
System Up Time		This is the total time the device has been on.
Poll Interval(s)		Enter the time interval for refreshing statistics.
Set Interval		Click this button to apply the new poll interval you entered above.
Stop		Click this button to stop refreshing statistics.

4.4 Configuring the ZyXEL Device Using the Wizard


The wizard consists of a series of screens to help you configure your ZyXEL Device to access the wireless network.

Use the following buttons to navigate the Wizard:

Back	Click Back to return to the previous screen.
Next	Click Next to continue to the next screen.

No configuration changes will be saved to the ZyXEL Device until you click **Finish**.

4.4.1 Wizard: Basic Settings

Click on the **Wizard** icon in the **Status** screen to start the setup wizard (). The **Basic Settings** screen appears.

- 1 Enter a descriptive name to identify the device in the Ethernet network.
- 2 Select **Obtain IP Address Automatically** only if you want to put the device behind a router that assigns an IP address.

Warning: If you select **Obtain IP Address Automatically** you will not be able to access the ZyXEL Device through the Web Configurator unless you have a router that assigns an IP address. If you select this by mistake, use the **RESET** button to restore the factory default IP address.

- 3 Select **Use fixed IP Address** to give the device a static IP address. The IP address you configure here is used for management of the device (accessing the web configurator).
- 4 Enter a **Subnet Mask** appropriate to your network and the **Gateway IP Address** of the neighboring device, if you know it. If you do not, leave the **Gateway IP Address** field as **0.0.0.0**.

Figure 19 Setup Wizard 1: Basic Settings

SETUP WIZARD **ZyXEL**

STEP 1 | STEP 2 | STEP 3 | STEP 4

Basic Settings

Device Name

Device Name:

IP Address Assignment

Obtain IP Address Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway IP Address:

Click **Next** to continue.

4.4.2 Wizard: Wireless Settings

Use this wizard screen to set up the wireless LAN. See the chapter on the wireless screens for background information.

- 1 The SSID is a unique name to identify the device in a wireless network. Enter up to 32 printable characters. Spaces are allowed. If you change the SSID on the device, make sure all wireless stations use the same SSID in order to access the network.

Note: The wireless AP and your ZyXEL Device must use the same SSID, channel and wireless security settings for wireless communication.

Figure 20 Setup Wizard 2: Wireless Settings.

SETUP WIZARD ZyXEL

STEP 1 **STEP 2** STEP 3 STEP 4

Wireless Settings

Wireless Settings

Enter the name (SSID) of your wireless network. To connect to an access point, both devices must use the same SSID. You can change the SSID you set at any time.

SSID:

< Back Next >

Click **Next** to continue, or **Back** to return to the **Basic Settings** screen.

4.4.3 Wizard: Security Settings

Use this screen to configure security for your wireless LAN connection. The screen varies depending on what you select in the **Encryption Method** field. Select **Disable** to have no wireless security configured, select **WEP**, or select **WPA-PSK** if your wireless AP supports WPA-PSK.

In the **Status** page, go to **Wireless > Security** if you want to use WPA2, WPA or 802.1x. See [Chapter 6 on page 55](#) for background information.

4.4.3.1 Disable

Select **Disable** to have no wireless LAN security configured. If you do not enable any wireless security on your device, your network is accessible to any wireless networking device that is within range.

Note: With no wireless security a neighbor can access and see traffic in your network.

Figure 21 Setup Wizard 3: Disable

4.4.3.2 WEP

- 1 WEP (Wired Equivalent Privacy) encrypts data frames before transmitting them over the wireless network. Select **64-bit** or **128-bit** from the **WEP Encryption** drop-down list box and then follow the on-screen instructions to set up the WEP keys.
- 2 Choose an encryption level from the drop-down list. The higher the WEP encryption, the higher the security but the slower the throughput.
- 3 You can generate or manually enter a WEP key.
 - If you selected 64-bit or 128-bit WEP, you can enter a **Passphrase** (up to 16 printable characters) and click **Generate**. The device automatically generates WEP keys. One key displays in the **Key 1** field. Go to **Wireless > Security** if you want to see the other WEP keys.
 - or
 - Enter a manual key in the **Key 1** field.

Figure 22 Wizard 3: WEP

SETUP WIZARD **ZyXEL**

STEP 1 STEP 2 **STEP 3** STEP 4

Security Settings

Security Settings

WEP key is the basic encryption method. Choose one below.

Encryption Method:

WEP Encryption:

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase: (max. 16 alphanumeric, printable characters)

Key 1:

Note:
Manual WEP Key :
 64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

4.4.3.3 WPA-PSK

Select **WPA-PSK** only if your wireless AP supports it.

Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.

Figure 23 Wizard 3: WPA(2)-PSK

SETUP WIZARD **ZyXEL**

STEP 1 STEP 2 **STEP 3** STEP 4

Security Settings

Security Settings

WPA-PSK is an advanced encryption method. By sharing the Pre-Shared Key you entered below, all the devices in the wireless network can securely associate.

Encryption Method:

Pre-Shared Key: (8-63 ASCII characters)

4.4.4 Wizard: Confirm Your Settings

This read-only screen shows the status of the current settings. Use the summary table to check whether what you have configured is correct. Click **Finish** to complete the wizard configuration and save your settings.

Figure 24 Wizard: Confirm Your Settings

4.5 Using the AP Survey tool

To scan for available wireless access points in your network, click **AP Survey** in the **Wireless** screen. Wait for the scan process to complete. A screen displays showing the scan results. Click on an entry in the **SSID** column to select that device for the **Basic Settings SSID** field in your **Wireless** page. See [Section 6.3.1 on page 60](#) for more information on using the AP Survey screen.

4.6 Resetting the ZyXEL Device

If you forget your password or cannot access the ZyXEL Device you will need to reset the ZyXEL Device to the factory defaults. This means that you will lose all configurations that you had previously saved. The username will be reset to **admin** and the password to **1234**.

4.6.1 Restoring Factory Defaults

You can erase the current configuration and restore factory defaults in two ways:

- Use the RESET button on the ZyXEL Device to reset to the factory defaults. Use this method for cases when the password or IP address of the ZyXEL Device is not known.
- Use the web configurator to restore defaults.

4.6.1.1 Using the RESET Button

Make sure the POWER light is steady on.

- 1** Press the RESET button for about 10 seconds, then release it and press the button in once.
- 2** If the POWER light begins to blink, the defaults have been restored and the ZyXEL Device restarts.

Wait for the ZyXEL Device to finish restarting before accessing it again.

CHAPTER 5

System Screen

This chapter provides information on the **System** screen.

5.1 TCP/IP Parameters

5.1.1 IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet (for instance, only between your two branch offices) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 5 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

5.1.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number, which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers (in this case, 192, 168 and 1) specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the device unless you are instructed to do otherwise.

5.2 System Settings

Click **System** to open the **System Settings** screen.

Figure 25 System Settings

The following table describes the labels in this screen.

Table 6 System Settings

LABEL	DESCRIPTION
Device Name	This name can be up to 15 printable characters long. Spaces are allowed.
IP Address Assignment	

Table 6 System Settings

LABEL	DESCRIPTION
Obtain IP Address Automatically	<p>Select this option to have your device use a dynamically assigned IP address from a router each time.</p> <p>Warning: If you select Obtain IP Address Automatically you will not be able to access the ZyXEL Device through the Web Configurator unless you have a router that assigns an IP address. If you select this by mistake, use the RESET button to restore the factory default IP address.</p>
Use fixed IP address	<p>Select this option to have your device use a static IP address. When you select this option, fill in the fields below.</p>
IP Address	<p>Enter the IP address of your device in dotted decimal notation.</p>
Subnet Mask	<p>Enter the subnet mask.</p>
Gateway IP Address	<p>Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device. The gateway helps forward packets to their destinations. Leave this field as 0.0.0.0 if you do not know it.</p>
Apply	<p>Click Apply to save your changes to the device. The ZyXEL Device will restart using the new settings and you will need to log in again.</p> <p>Note: If you have changed the IP address, you will need to use the new address to log in to the ZyXEL Device.</p>
Reset	<p>Click Reset to clear any unsaved changes to this screen.</p>

CHAPTER 6

Wireless Screens

This chapter discusses how to configure wireless settings and wireless security on your ZyXEL Device.

6.1 Wireless LAN Overview

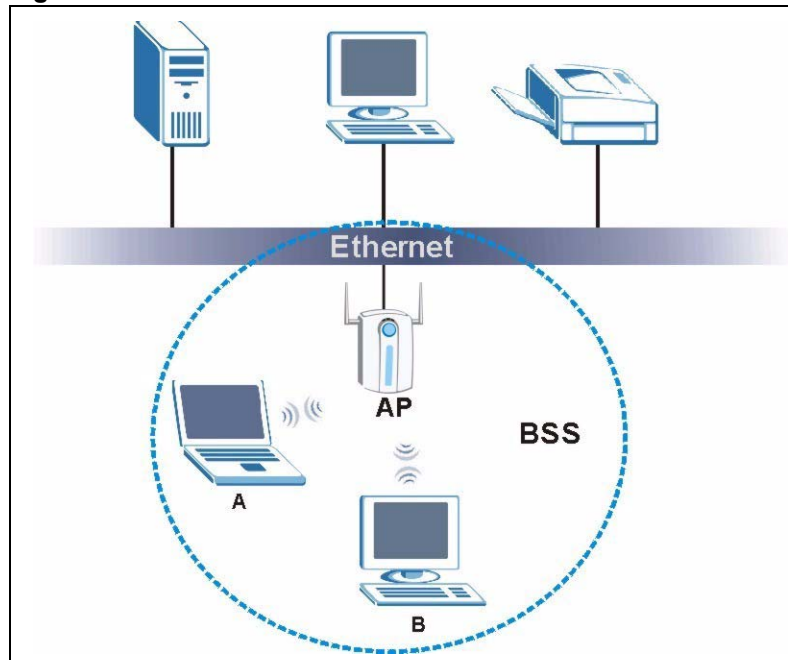
This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 BSS (Infrastructure)

A Basic Service Set (BSS), also called an Infrastructure network, exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station **A** and **B** can still access the wired network but cannot communicate with each other.

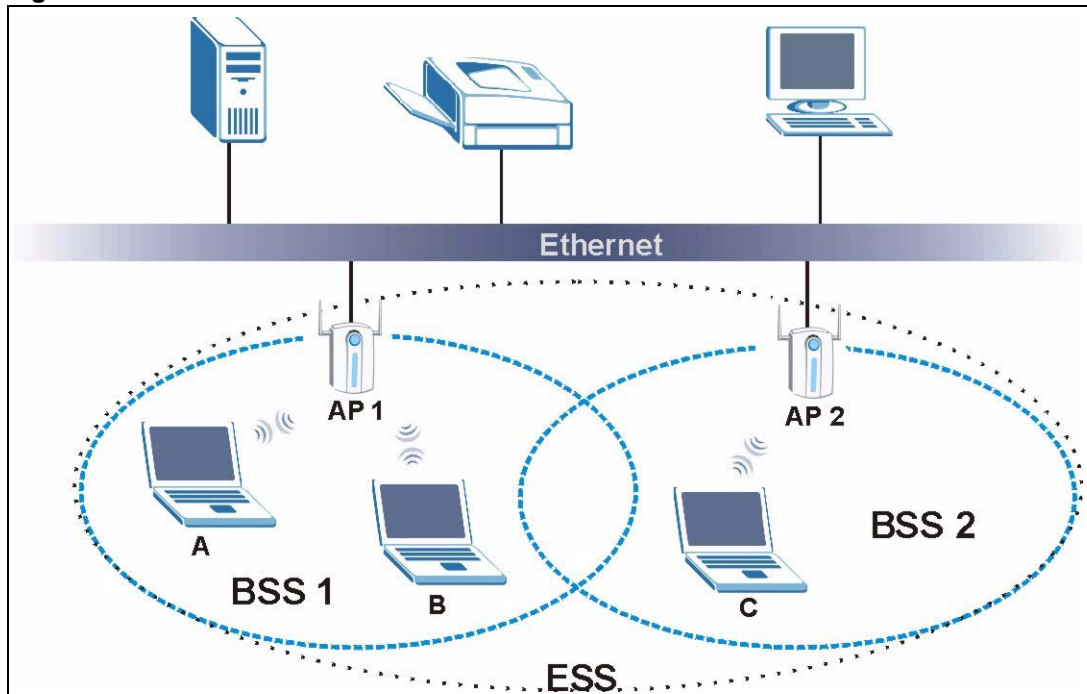
Figure 26 Basic Service set



6.1.2 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 27 Extended Service Set



6.2 Wireless LAN Basics

This section describes the wireless LAN network terms.

6.2.1 Channel

A channel is the radio frequency or frequencies used by IEEE 802.11b wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap, causing signal disruption and degrading performance.

Adjacent channels partially overlap, however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

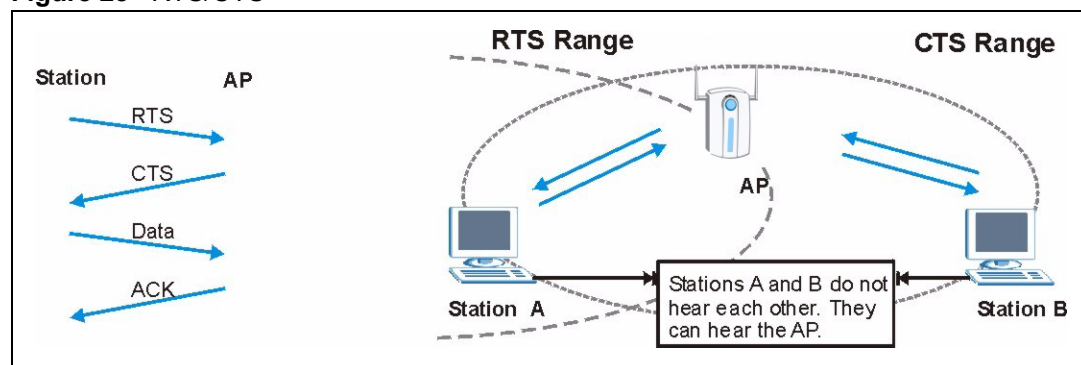
6.2.2 SSID

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

6.2.3 RTS/CTS

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

Figure 28 RTS/CTS



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

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

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

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

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

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

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

6.2.4 Fragmentation Threshold

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

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

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

6.3 Configuring Wireless

Click **Wireless** to display the **Wireless Settings** screen.

Figure 29 Wireless: Wireless Settings

The screenshot shows the 'Wireless Settings' configuration page. It includes the following fields and options:

- Basic Settings:**
 - SSID: ZyXEL (max. 32 printable characters)
 - Wireless Mode: Mixed Mode
 - Clone Mac Address: Disable, Auto-Single, Auto-Multi, Manual
- Advanced Settings:**
 - Radio Enable: Yes, No
 - Output Power Management: Full
 - Data Rate Management: best
 - Preamble Type: Dynamic
 - RTS/CTS Threshold: 2345 (0~2345)
 - Fragmentation Threshold: 2340 (256~2340)

Buttons: Apply, Reset

The following table describes the labels in this screen.

Table 7 Wireless: Wireless Settings

LABEL	DESCRIPTION
SSID	<p>Your ZyXEL Device must have the same SSID as the AP you want to connect to. Enter a descriptive name (up to 32 printable characters) for the wireless LAN. Spaces are allowed.</p> <p>Note: If you are configuring the device from a computer connected to the wireless LAN and you change the device's SSID, channel or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the device's new settings.</p>
AP Survey	Click this button to open the AP Survey window and select an access point.
Wireless Mode	<p>Select Mixed Mode to set the ZyXEL Device to operate in a wireless network with both 802.11b and 802.11g wireless devices.</p> <p>Select Pure B Mode to set the ZyXEL Device to operate in a wireless network with only 802.11b wireless devices. If you select this, the ZyXEL Device may not communicate with IEEE802.11g wireless devices</p> <p>Select Pure G Mode to set the ZyXEL Device to operate in a wireless network with only 802.11g wireless devices. If you select this, the ZyXEL Device may not communicate with IEEE802.11b wireless devices</p>
Clone MAC Address	<p>Every Ethernet-capable device is issued with a unique Media Access Control (MAC) address at the factory. This address is used to identify the device across a network.</p> <p>Your ZyXEL Device is capable of “cloning”, or emulating, the MAC addresses of one or more other devices.</p> <p>Select Auto-Single to have the ZyXEL Device automatically use the MAC address of a single Ethernet device connected to the ETHERNET port.</p> <p>Select Auto-Multi to have the ZyXEL Device automatically use the MAC addresses of multiple Ethernet devices connected to the ETHERNET port via a hub.</p> <p>Alternatively, enter a MAC address into the Clone MAC address field and select Manual to have the ZyXEL Device use that address.</p>
Advanced Settings	
Radio Enable	Select Yes to allow wireless communications between the device and other IEEE 802.11b and IEEE 802.11g compliant wireless devices. Select No to stop wireless communications between the device and other IEEE 802.11b and IEEE 802.11g compliant wireless devices.
Output Power Management	Set the output power of the device in this field. If there is a high density of APs within an area, decrease the output power of the device to reduce interference with other wireless LAN devices.
Data Rate Management	Use this field to select a maximum data rate for the wireless connection.

Table 7 Wireless: Wireless Settings (continued)

LABEL	DESCRIPTION
Preamble Type	<p>Preamble is used to signal that data is coming to the receiver. Select the preamble type that the AP uses. Short and Long refer to the length of the synchronization field in a packet.</p> <p>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.</p> <p>Select Auto to have the ZyXEL Device automatically use short preamble when all access point or wireless stations support it; otherwise the ZyXEL Device uses long preamble.</p> <p>Note: The ZyXEL Device and the access point MUST use the same preamble mode in order to communicate.</p>
RTS/CTS Threshold	Enter a value between 0 and 2345. The default is 2345 .
Fragmentation Threshold	Enter a value between 256 and 2340. The default is 2340 . It is the maximum data fragment size that can be sent.
Apply	Click Apply to save your changes back to the device.
Reset	Click Reset to begin configuring this screen afresh.

6.3.1 The AP Survey Window

Click on **Wireless > Wireless Settings > AP Survey** to display the **AP Survey** screen. The ZyXEL Device searches for available access points (APs).

Figure 30 Wireless: the AP Survey Screen

Access Point List				
No.	SSID	Channel	Signal Strength	Security Mode
1	CPE 5548	6	80%	[WEP]
2	121	6	71%	[WPA-PSK-TKIP]
3	ZYS	11	71%	[WPA-EAP-TKIP]
4	330W	11	66%	[WPA-PSK-TKIP]

.....

The following table describes the labels in this screen.

Table 8 Wireless: the AP Survey Screen

LABEL	DESCRIPTION
Access Point List	
No.	This field displays the number of the access point. The access points are ranked by signal strength.

Table 8 Wireless: the AP Survey Screen

LABEL	DESCRIPTION
SSID	This field displays the SSID (Service Set Identifier) of each access point. Click on an SSID to select that wireless device.
Channel	This field displays the channel number used by each access point.
Signal Strength	This field displays the signal strength of each access point.
Security Mode	This field displays details of the access point's security and data encryption settings.
Rescan	Click Rescan to have the ZyXEL Device search again for available access points.

6.4 Wireless Security Overview

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

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

Table 9 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	Wi-Fi Protected Access (WPA)
	WPA2

If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

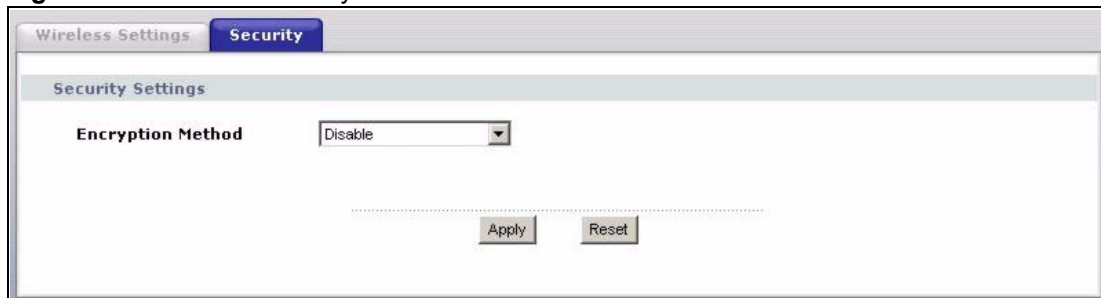
6.5 Configuring Wireless Security

In order to configure and enable wireless security; click **Wireless > Security** to display the **Security** screen. This screen varies according to the encryption method you select.

6.5.1 Wireless Security: Disable

If you do not enable any wireless security on your device, your network is accessible to any wireless networking device that is within range.

Figure 31 Wireless Security: Disable



The following table describes the labels in this screen.

Table 10 Wireless Security: Disable

LABEL	DESCRIPTION
Encryption Method	Select Disable to have no wireless LAN security configured.
Apply	Click Apply to save your changes back to the device.
Reset	Click Reset to begin configuring this screen afresh.

6.5.2 Wireless Security: WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. You can configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

Figure 32 Wireless Security: WEP

Wireless Settings Security

Security Settings

Encryption Method

Authentication Type

Data Encryption

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase (max. 16 alphanumeric, printable characters)

ASCII HEX

Key 1

Key 2

Key 3

Key 4

Note:
 64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

The following table describes the labels in this screen.

Table 11 Wireless Security: WEP

LABEL	DESCRIPTION
Encryption Method	Select WEP if you want to configure WEP encryption parameters.
Authentication Type	Select Open or Shared from the drop-down list box.
Data Encryption	Select 64 bit WEP or 128 bit WEP to enable data encryption.
Passphrase	With 64-bit or 128-bit WEP, you can enter a "passphrase" (password phrase) of up to 32 case-sensitive printable characters and click Generate to have the device create four different WEP keys.
Generate	After you enter the passphrase, click Generate to have the device generate four different WEP keys automatically.
Key 1 to Key 4	If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the device and the wireless stations must use the same WEP key for data transmission. If you chose 64 bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128 bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Apply	Click Apply to save your changes back to the device.
Reset	Click Reset to begin configuring this screen afresh.

6.5.3 Wireless Security: WPA(2)-PSK

Select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK & WPA2-PSK** in the **Encryption Method** drop down list-box to display the next screen.

Figure 33 Wireless Security: WPA(2)-PSK

The screenshot shows a web interface for configuring wireless security. At the top, there are tabs for 'Wireless Settings' and 'Security'. Below this is a 'Security Settings' section. It contains three main configuration areas: 'Encryption Method' with a dropdown menu currently showing 'WPA-PSK', 'Data Encryption' with a dropdown menu showing 'TKIP', and 'Pre-Shared Key' with a text input field and a note '(8-63 ASCII characters)'. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 12 Wireless Security: WPA-PSK

LABEL	DESCRIPTION
Encryption Method	Select WPA-PSK , WPA2-PSK or WPA-PSK & WPA2-PSK if you want to configure a pre-shared key. Choose this option only if your AP supports it.
Data Encryption	Select TKIP , AES or TKIP + AES to enable data encryption. For more information, see the Wireless Security appendix.
Pre-Shared Key	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.
Apply	Click Apply to save your changes to the device.
Reset	Click Reset to begin configuring this screen afresh.

6.5.4 Wireless Security: WPA(2)

WPA (Wi-Fi Protected Access) 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 user authentication and improved data encryption.

Figure 34 Wireless Security: WPA(2)

The following table describes the labels in this screen.

Table 13 Wireless Security: WPA(2)

LABEL	DESCRIPTION
Encryption Method	Select WPA , WPA2 or WPA & WPA2 to configure user authentication and improved data encryption.
EAP Type	Select EAP-TLS, EAP-TTLS, EAP-LEAP or EAP-PEAP from the drop-down box. See the Wireless Security appendix for more information.
Data Encryption	Select TKIP , AES or TKIP + AES to enable data encryption. For more information, see the Wireless Security appendix.
Trusted Root CA File (EAP-TLS, EAP-TTLS and EAP-PEAP only)	This is the name of the certificate issued by the certificate authority (CA).
Select File	Click here to choose a certificate. Select a certificate from the list box and click Select to activate it. Click Delete if you want to remove a certificate from the list. Alternatively, click Browse to locate a certificate. Click Upload to add it to the list. The certificate file must have a .pem or .cer ending. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA).
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password (EAP-TTLS, EAL-LEAP and EAP-PEAP only)	Enter the password associated with the login name above.
User Certificate File	This is your encrypted private key file.

Table 13 Wireless Security: WPA(2) (continued)

LABEL	DESCRIPTION
Select File	Click here to choose a private key. Select a private key from the list box and click Select to activate it. Click Delete if you want to remove a private key from the list. Alternatively, click Browse to locate a private key. Click Upload to add it to the list. The private key file must have a .pfx ending.
Private Key Password (EAP-TLS only)	Enter the password associated with the private key above.
Validate Server Certificate (EAP-TLS, EAP-TTLS and EAP-PEAP only)	Select the check box to verify the certificate of the authentication server.
Apply	Click Apply to save your changes to the device.
Reset	Click Reset to begin configuring this screen afresh.

6.5.5 Wireless Security: IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management.

Note: Once you enable user authentication, you need to specify an external RADIUS server on the device for authentication.

Figure 35 Wireless Security: 802.1x

The following table describes the labels in this screen.

Table 14 Wireless Security: 802.1x

LABEL	DESCRIPTION
Encryption Method	Select 802.1X to configure encryption key management.
EAP Type	Select EAP-TLS, EAP-TTLS, EAP-LEAP or EAP-PEAP from the drop-down box. See the Wireless Security appendix for more information.
Data Encryption (EAP-MD5 only)	Select 64 bit WEP or 128 bit WEP to enable data encryption.
Trusted Root CA File (EAP-TLS, EAP-TTLS and EAP-PEAP only)	This is the name of the certificate issued by the certificate authority (CA).
Select File (EAP-TLS, EAP-TTLS and EAP-PEAP only)	Click here to choose a certificate. Select a certificate from the list box and click Select to activate it. Click Delete if you want to remove a certificate from the list. Alternatively, click Browse to locate a certificate. Click Upload to add it to the list. The certificate file must have a .pem or .cer ending. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA).

Table 14 Wireless Security: 802.1x

LABEL	DESCRIPTION
Login Name	Enter a user name. This is the user name that you or an administrator set up on a RADIUS server.
Password (EAP-TTLS, EAP-LEAP and EAP-PEAP only)	Enter the password associated with the login name above.
User Certificate File (EAP-TLS only)	This is your encrypted private key file.
Select File (EAP-TLS only)	Click here to choose a private key. Select a private key from the list box and click Select to activate it. Click Delete if you want to remove a private key from the list. Alternatively, click Browse to locate a private key. Click Upload to add it to the list. The private key file must have a .pfx ending.
Private Key Password (EAP-TLS only)	Enter the password associated with the private key above.
Validate Server Certificate (EAP-TLS, EAP-TTLS and EAP-PEAP only)	Select the check box to verify the certificate of the authentication server.
Passphrase (EAP-MD5 only)	With 64-bit or 128-bit WEP, you can enter a "passphrase" (password phrase) of up to 32 case-sensitive printable characters and click Generate to have the device create four different WEP keys.
Generate (EAP-MD5 only)	After you enter the passphrase, click Generate to have the device generate four different WEP keys automatically.
Key 1 to Key 4 (EAP-MD5 only)	If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the device and the wireless stations must use the same WEP key for data transmission. If you chose 64 bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128 bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Apply	Click Apply to save your changes to the device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 7

Management Screens

This chapter describes the Management screens.

7.1 Management Overview

Use these management screens to change the password, back up or restore the configuration files and upgrade your ZyXEL Device's firmware.

7.2 Password

To change your device's password (recommended), click **Management**. The screen appears as shown. This screen allows you to change the device's password.

If you forget your password (or the device IP address), you will need to reset the device. See [Section 4.3 on page 41](#) for details.

Figure 36 Management: Password

The following table describes the labels in this screen.

Table 15 Management: Password

LABEL	DESCRIPTION
Password Setup (admin)	Use this section to change the password details for the admin username.
Current Password	Type in your existing system password (1234 is the default password).

Table 15 Management: Password (continued)

LABEL	DESCRIPTION
New Password	Type your new system password (up to 19 printable characters). Spaces are not allowed. As you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Save your changes back to the device.
Reset	Reload the previous configuration for this screen.

7.3 Configuration File

The configuration file (often called the romfile or rom-0) contains the factory default settings such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a .rom filename extension. Once you have customized the device's settings, they can be saved back to your computer under a filename of your choosing.

Click **Management > Configuration File**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 37 Management: Configuration File

The screenshot shows a web interface with three tabs: "Password", "Configuration File" (selected), and "F/W Upload". The main content area is divided into three sections:

- Backup Configuration:** A text block stating "This page allows you to backup your current configuration to your computer. Click the **Backup** button to start the backup process." followed by a "Backup" button.
- Restore Configuration:** A text block stating "To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the **Upload** button". Below this is a "File Path:" label, a text input field, a "Browse..." button, and an "Upload" button.
- Back to Factory Defaults:** A text block stating "The **Reset** button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following values needed to access the device..". Below this is a list of default values:
 - username: admin
 - Password: 1234
 - LAN IP Address: 192.168.1.11
 followed by a "Reset" button.

7.3.1 Backup Configuration

Backup configuration allows you to back up (save) the device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is strongly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

7.3.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your device.

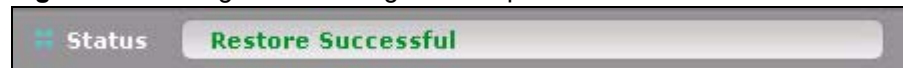
Table 16 Management: Configuration File: Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process.

Warning: Do not turn off the device while configuration file upload is in progress.

The following screen displays in the Status bar at the bottom of the configurator screen.

Figure 38 Management: Configuration Upload Successful

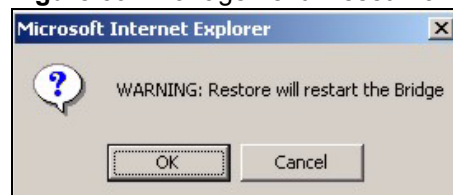


If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.12 to 1.192.168.1.254).

7.3.3 Back to Factory Defaults

Clicking the **RESET** button in this section clears all user-entered configuration information and returns the device to its factory defaults. The following warning screen will appear.

Figure 39 Management: Reset Warning Message



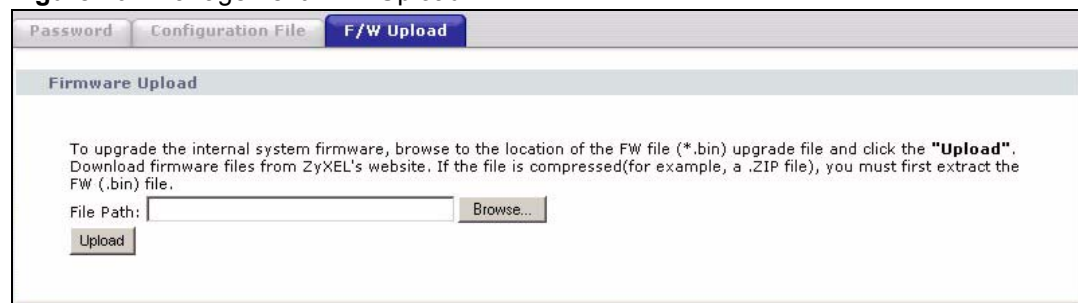
You can also press the **RESET** button on the rear panel to reset the factory defaults of your device. Refer to [Section 4.6.1 on page 49](#) for more information on the **RESET** button.

7.4 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .rmt extension, for example, "zyxel.rmt". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Management > F/W Upload** to display the screen as shown. Follow the instructions in this screen to upload firmware to your device.

Figure 40 Management: F/W Upload



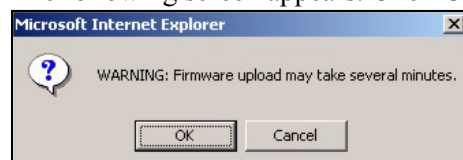
The following table describes the labels in this screen.

Table 17 Management: F/W Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .rmt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

Warning: Do not turn off the device while firmware upload is in progress!

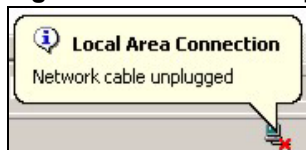
The following screen appears. Click **OK** to continue.



Wait until the countdown reaches zero before logging into the device again.

Figure 41 Management: Firmware Upgrading Screen

The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 42 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following status message displays at the bottom of the screen.

Figure 43 Management: Firmware Upload Error

CHAPTER 8

Troubleshooting

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

8.1 Problems Starting Up the ZyXEL Device

Table 18 Troubleshooting the Start-Up of Your ZyXEL Device

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The device reboots automatically sometimes.	The supplied power to the ZyXEL Device is too low. Check that the ZyXEL Device is receiving enough power. Make sure the power source is working properly.

8.2 Problems with the Password

Table 19 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The Password field is case-sensitive. Make sure that you enter the correct password using the proper casing. Use the RESET button on the rear panel of the ZyXEL Device to restore the factory default configuration file (hold this button in for about 10 seconds or release the button when the PWR LED starts blinking). This will restore all of the factory defaults including the password.

8.3 Problem with the Wireless Link Quality

Table 20 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	<p>Search and connect to another AP with a better link quality using the Site Survey screen.</p> <p>Move your computer closer to the AP or the peer computer(s) within the transmission range.</p> <p>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.</p> <p>Make sure there are not too many wireless stations connected to a wireless network.</p>

8.4 Problems Communicating With Other Computers

Table 21 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
The computer with the ZyXEL Device installed cannot communicate with the other computer(s).	<p>In Infrastructure Mode</p> <ul style="list-style-type: none">• Make sure that the AP and the associated computers are turned on and working properly.• Make sure the ZyXEL Device and the associated AP use the same SSID.• Change the AP and the associated wireless clients to use another radio channel if interference is high.• Make sure that the computer and the AP share the same security option and key. Verify the settings in the Profile Security Settings screen.• If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.

8.5 Problems with the Ethernet Interface

Table 22 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device from the LAN.	<p>If the ETHN LED on the front panel is off, check the Ethernet cable connection between your ZyXEL Device and the Ethernet device connected to the ETHERNET port.</p> <p>Check for faulty Ethernet cables.</p> <p>Make sure your computer's Ethernet adapter is installed and working properly.</p> <p>Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the ZyXEL Device, the Ethernet device and your computer are on the same subnet.</p>
I cannot ping any computer on the LAN.	<p>If the ETHN LED on the front panel is off, check the Ethernet cable connections between your ZyXEL Device and the Ethernet device.</p> <p>Check the Ethernet cable connections between the Ethernet device and the LAN computers.</p> <p>Check for faulty Ethernet cables.</p> <p>Make sure the LAN computer's Ethernet adapter is installed and working properly.</p> <p>Verify that the IP address and the subnet mask of the ZyXEL Device, the Ethernet device and the LAN computers are on the same subnet.</p>
I cannot access the web configurator.	<p>Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyXEL Device's IP address, then enter the new one as the URL.</p> <p>If you don't know the ZyXEL Device's IP address, type the device name of your ZyXEL Device as the URL. ZyXELXXXX is the default where "XXXX" is the last four digits of the MAC address. The MAC address is on the bottom of the device).</p> <p>If you just changed the ZyXEL Device's IP address, your computer's cache of machine names may contain an entry that maps the name of the ZyXEL Device to its previous IP address.</p> <p>In Windows, use nbststat -R at the command prompt to delete all entries in your computer's cache of machine names.</p> <p>Open a new browser window.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p> <hr/> <p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click Tools and then Internet Options to open the Internet Options screen.</p> <p>In the General tab, click Delete Files. In the pop-up window, select the Delete all offline content check box and click OK. Click OK in the Internet Options screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use arp -d at the command prompt to delete all entries in your computer's ARP table.</p> <p>Open a new browser window.</p>

8.5.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

8.5.1.1 Internet Explorer Pop-up Blockers

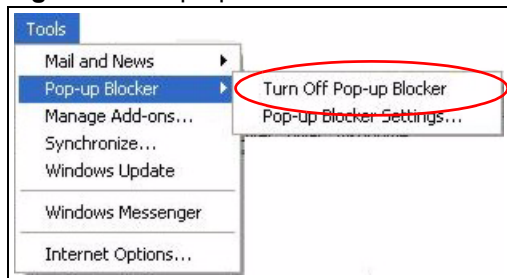
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

8.5.1.1.1 Disable pop-up Blockers

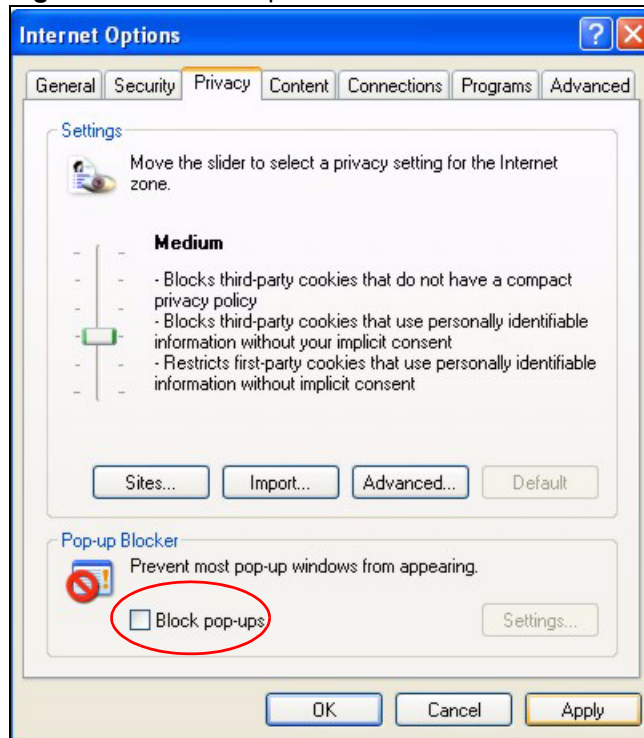
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 44 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

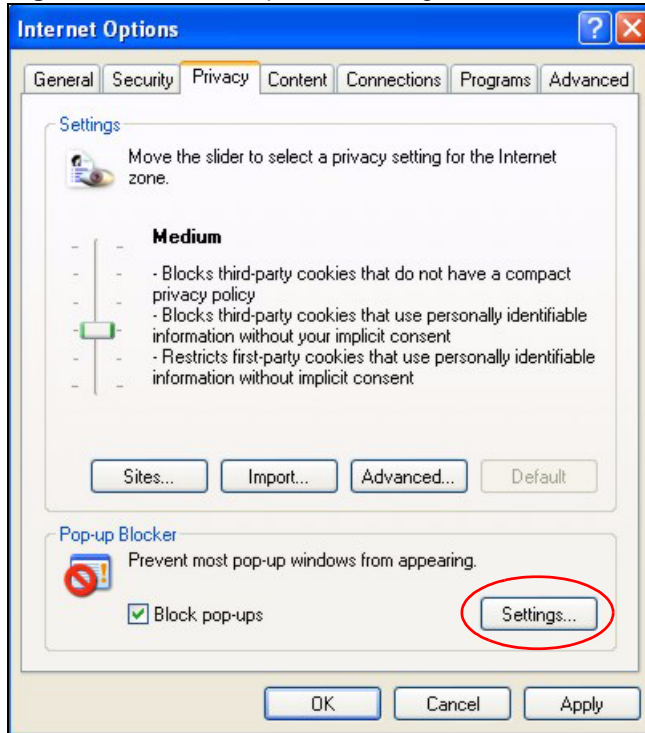
Figure 45 Internet Options

3 Click **Apply** to save this setting.

8.5.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1** In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2** Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 46 Internet Options: Settings

- 3** Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, <http://192.168.1.11>.
- 4** Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 47 Pop-up Blocker Settings

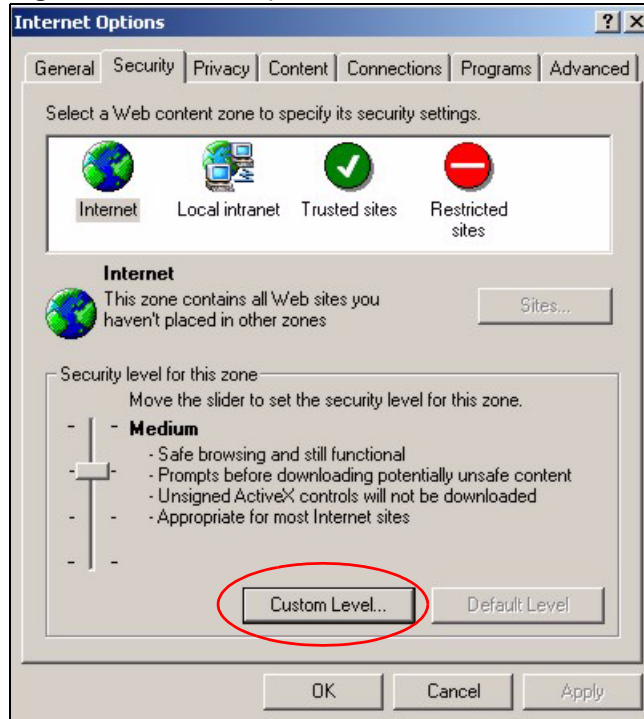
5 Click **Close** to return to the **Privacy** screen.

6 Click **Apply** to save this setting.

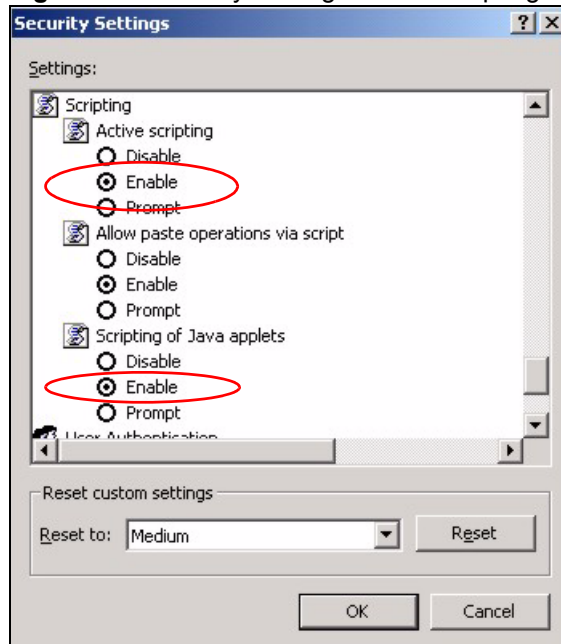
8.5.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

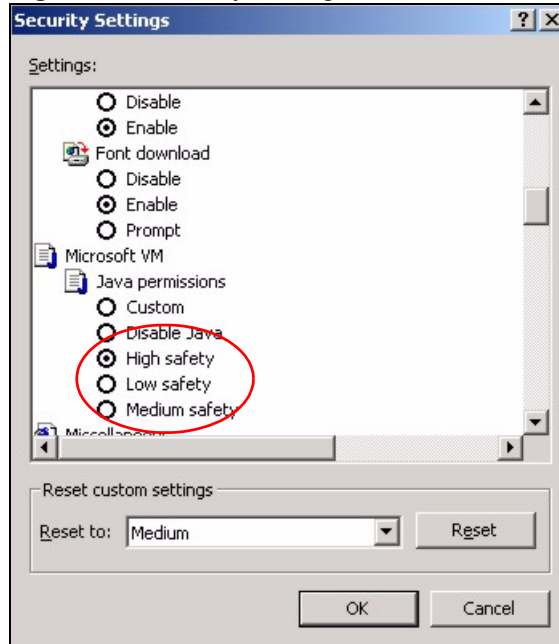
Figure 48 Internet Options: Custom Level

- 2** Click the **Custom Level...** button.
- 3** Scroll down to **Scripting**.
- 4** Under **Active scripting** make sure that **Enable** is selected (the default).
- 5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6** Click **OK** to close the window.

Figure 49 Security Settings - Java Scripting

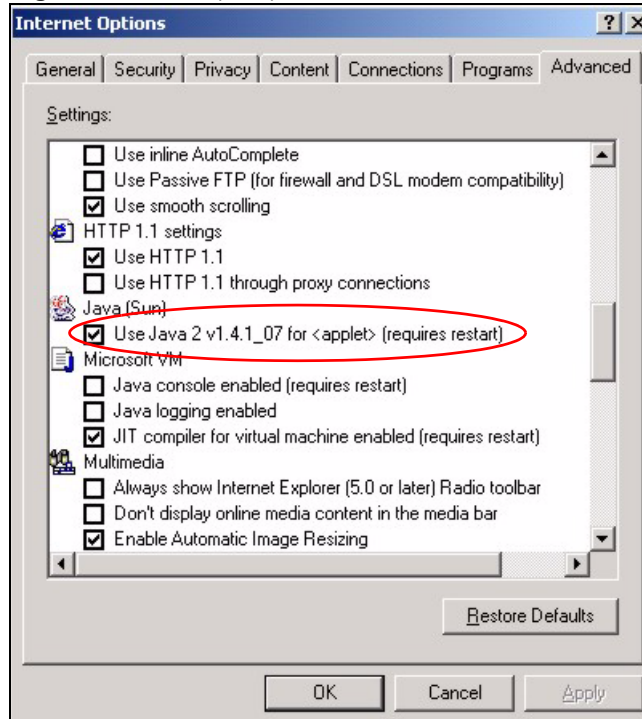
8.5.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 50 Security Settings - Java

8.5.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 51 Java (Sun)

8.6 Testing the Connection to the ZyXEL Device

- 1 Click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type “ping” followed by a space and the IP address of the ZyXEL Device (192.168.1.11 is the default).
- 3 Press **ENTER**. The following screen displays.

Figure 52 Pinging the G-470

```

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=10ms TTL=254
Reply from 192.168.1.11: bytes=32 time<10ms TTL=254
Reply from 192.168.1.11: bytes=32 time<10ms TTL=254
Reply from 192.168.1.11: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2m
  
```

Your computer can now communicate with the ZyXEL Device via the **ETHERNET** port.

APPENDIX A

Product Specifications

Table 23 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	G-470 802.11g Wireless Ethernet Adapter
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure
Security	64/128-bit WEP Encryption WPA/WPA-PSK IEEE 802.1x
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-25 ~ 70 degrees Centigrade
Operating Humidity	0 ~ 70% (non-condensing)
Storage Humidity	10 ~ 90% (non-condensing)
Power Consumption	TX: 620mA RX: 600mA
Voltage	5V
Dimensions	104mm × 127mm × 26mm excluding external antenna and foot stand.
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Frequency	USA (FCC) & Canada 11 Channels Europe (ETSI) 13 Channels Japan (TELEC) 13 Channels
Data Rate	IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11b: 11, 5.5, 2, 1 Mbps
Modulation	IEEE 802.11g: OFDM (64QAM, 16QAM, QPSK, BPSK) IEEE 802.11b: Direct Sequence Spread Spectrum (DSSS), (CCK, DQPSK, DBPSK)
Peak Output Power	27.88dBm
Rx Sensitivity	IEEE 802.11g At 54Mbps -72dBm (typical) IEEE 802.11g At 24Mbps -82dBm (typical)
SOFTWARE SPECIFICATIONS	
Device Drivers	Windows 2000, Windows XP, Windows ME, Windows 98SE, Windows NT 4.0
Roaming	IEEE 802.11b/g compliant
WEP	64/128-bit WEP encryption

APPENDIX B

Wireless Security

Types of EAP Authentication

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

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

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

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

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

Table 24 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

Table 24 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA(2)

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

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

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

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

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

Encryption

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

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

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

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

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

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

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

User Authentication

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

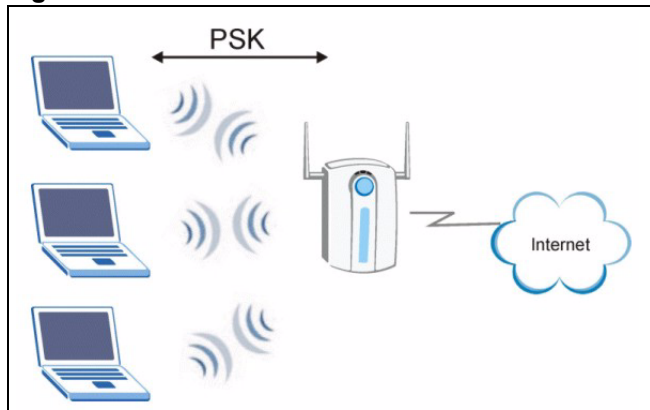
Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

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.

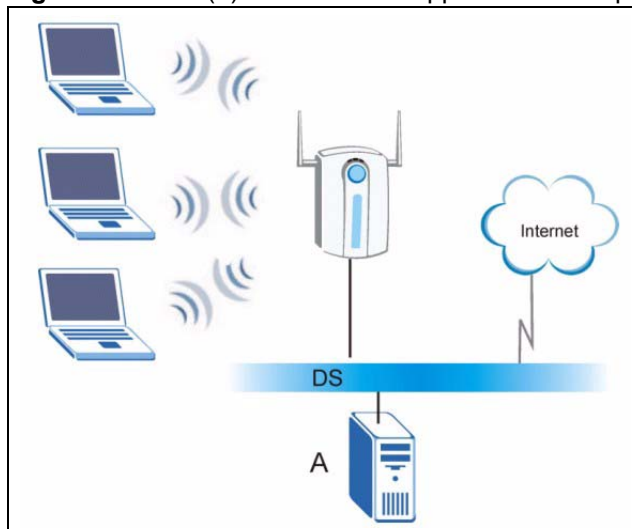
- 1** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2** The AP checks each client's password and (only) allows it to join the network if it 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 53 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 54 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 25 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 C

Setting up Your Computer's IP Address

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

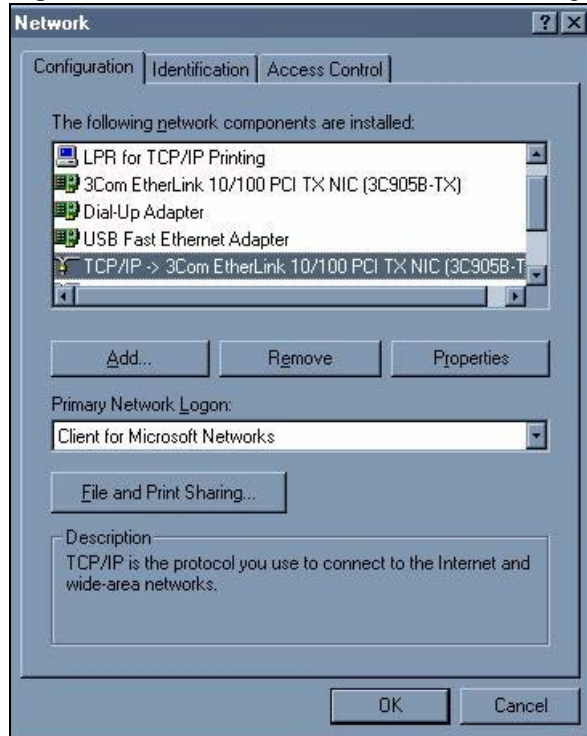
Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

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 55 WIndows 95/98/Me: Network: Configuration

Installing Components

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

If you need the adapter:

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

If you need TCP/IP:

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

If you need Client for Microsoft Networks:

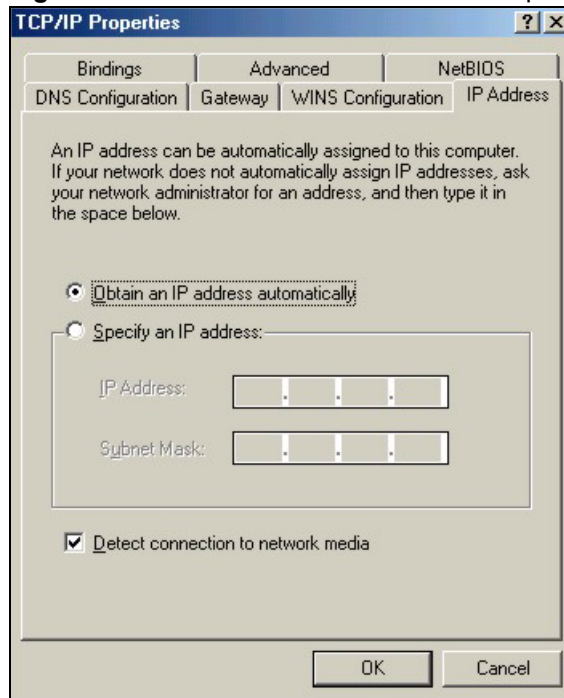
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

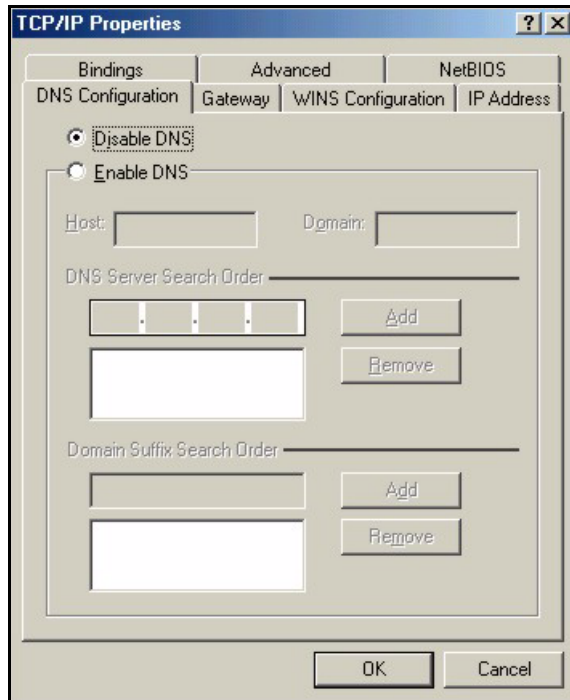
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 56 Windows 95/98/Me: TCP/IP Properties: IP Address



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

Figure 57 Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

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

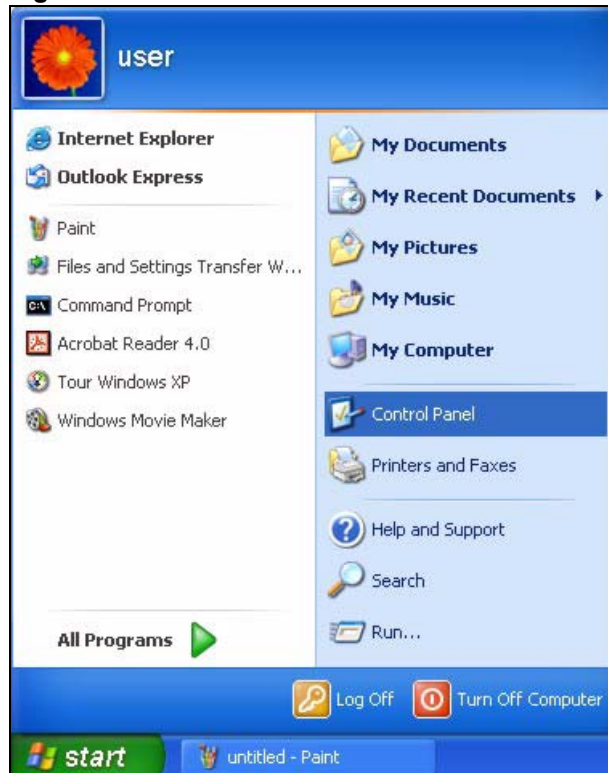
5 Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Restart your computer when prompted.

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

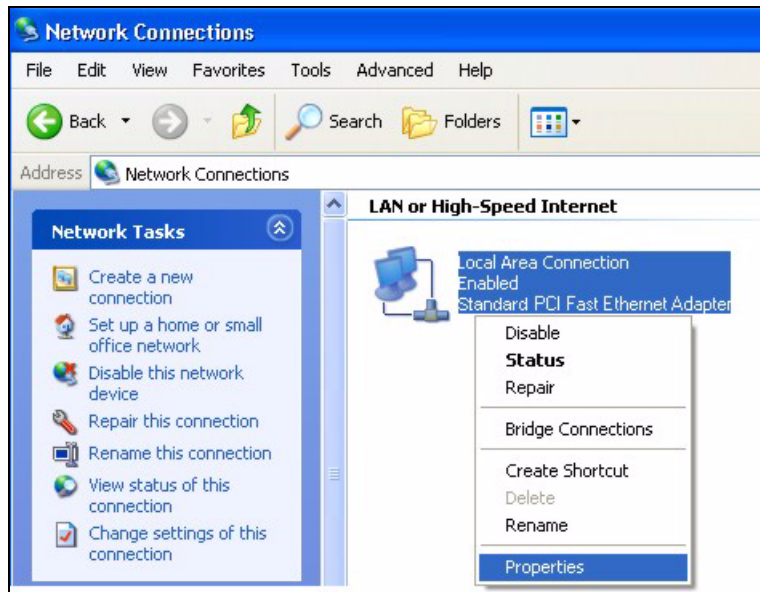
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 58 Windows XP: Start Menu

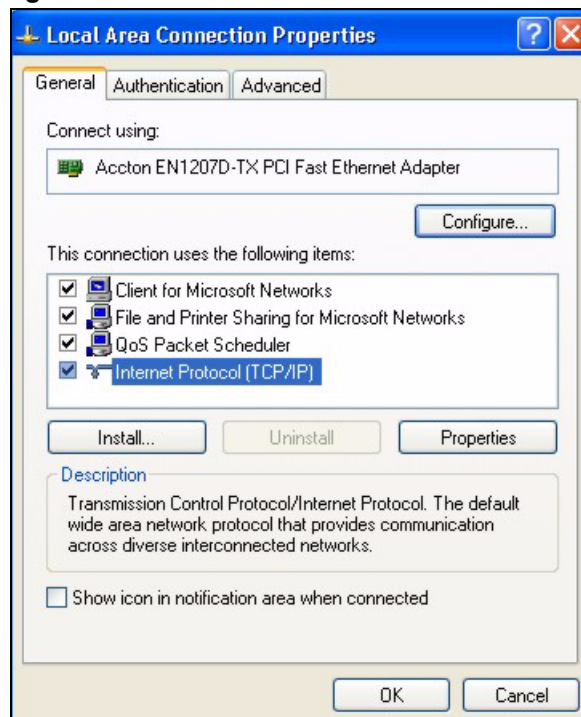
- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 59 Windows XP: Control Panel

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

Figure 60 Windows XP: Control Panel: Network Connections: Properties

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

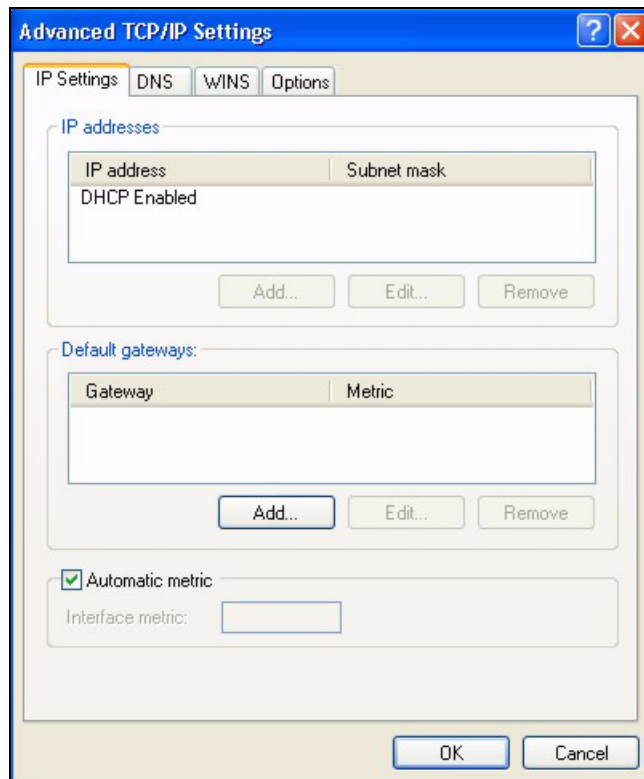
Figure 61 Windows XP: Local Area Connection Properties

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

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

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

Figure 62 Windows XP: Advanced TCP/IP Settings



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

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

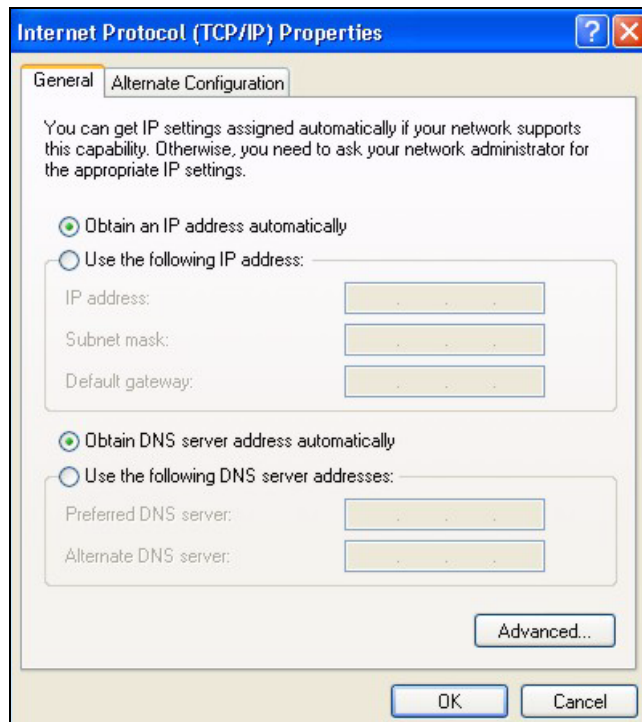
- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **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 63 Windows XP: Internet Protocol (TCP/IP) Properties



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

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

10 Restart your computer (if prompted).

Verifying Settings

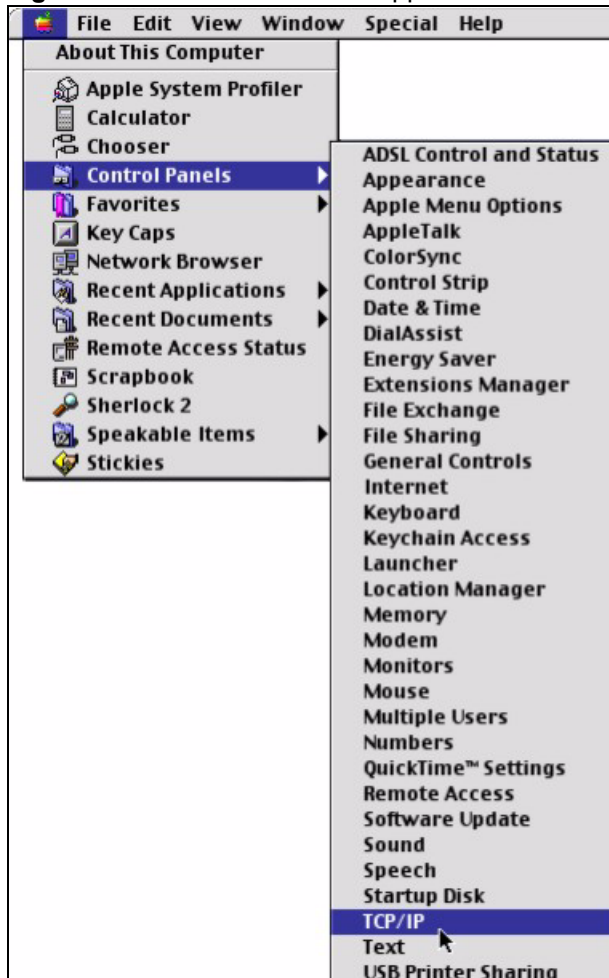
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

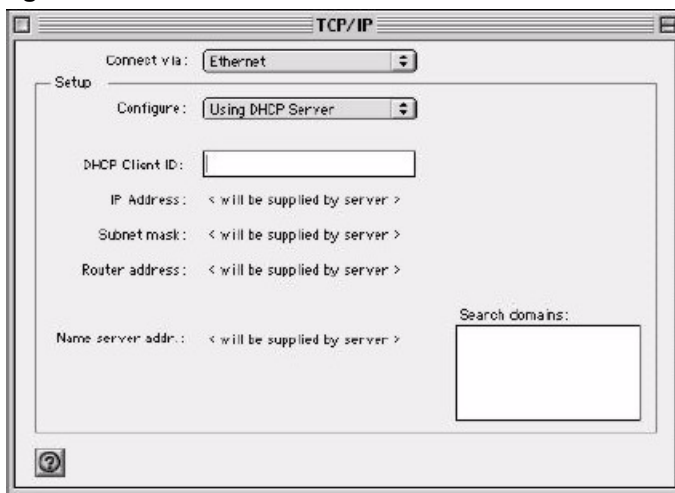
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 64 Macintosh OS 8/9: Apple Menu



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

Figure 65 Macintosh OS 8/9: TCP/IP



- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your 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).

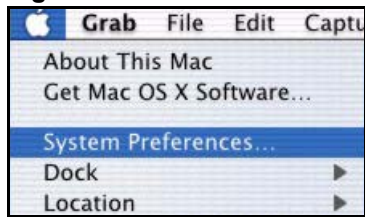
Verifying Settings

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.

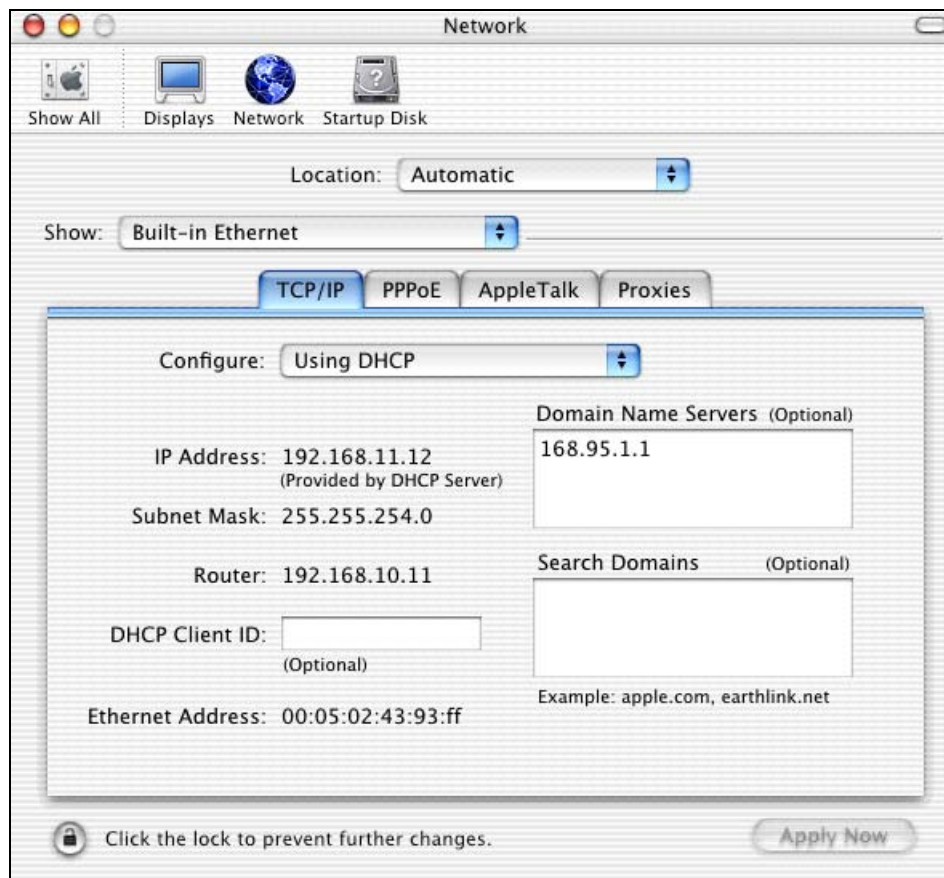
Figure 66 Macintosh OS X: Apple Menu



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 67 Macintosh OS X: Network

4 For statically assigned settings, do the following:

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

A

Access point [21](#), [24](#), [31](#)
Access point. See also AP.
Address assignment [51](#)
Advanced Encryption Standard (AES) [34](#), [91](#)
AES [34](#)
Antenna [22](#)
 connector [23](#)
 power output [87](#)
AP [31](#)
AP survey [49](#)
AP. See also access point.
Applications [23](#)
Authentication [32](#)
Authentication method
 auto [33](#)
 open system [33](#)
 shared key [33](#)
Auto authentication [33](#)

B

Backup [71](#)
Basic Service Set [55](#)
Bridge [21](#)
Browser [35](#)
BSS [55](#)

C

CA [89](#)
Cache [77](#)
CCMP [34](#)
Certificates [32](#)
Certification Authority (CA) [32](#), [89](#)
Certifications
 Viewing [5](#)
Channel [31](#), [56](#), [61](#)
 overlap [56](#)
Clone MAC address [59](#)

Configuration [35](#)
 backup [71](#)
Copyright [3](#)
Customer Support [8](#)

D

Data encryption [61](#)
Data rate [22](#), [87](#)
 management [59](#)
DCHP [22](#)
Default settings [49](#)
Defaults [71](#)
Digital ID [32](#)
Dimensions [87](#)
Direct Sequence Spread Spectrum (DSSS) [87](#)
Disclaimer [3](#)
Distribution System [56](#)
Dynamic WEP Key Exchange [90](#)

E

EAP Authentication [34](#)
Encryption [32](#), [91](#)
Encryption Type [33](#)
Environmental Specifications [87](#)
ESS [56](#)
ESS IDentification [56](#)
Ethernet [21](#), [22](#)
Ethernet port [23](#)
Examples [27](#)
Extended Service Set [56](#)

F

Factory defaults [71](#)
FCC [4](#)
Features [22](#)
Feedback [19](#)

Firmware [22, 72](#)
 upgrade [19](#)
Fragmentation Threshold [58, 60](#)
Frequency [31, 56, 87](#)
Front panel [23](#)

G

Getting started [21](#)
Graphics icons key [20](#)

H

Hardware [22](#)
 installation [19, 22](#)
Hardware connection [19](#)
Home network [21](#)
Humidity [87](#)

I

IEEE 802.11b [22](#)
IEEE 802.11b/g [33](#)
IEEE 802.11g [22](#)
IEEE 802.11i [34](#)
IEEE 802.1x [32, 34](#)
Infrastructure [24, 55](#)
Initialization vector (IV) [91](#)
Installation [22](#)
Interference [56, 58, 76](#)
Interference Statement [4](#)
Internet access [21](#)
 example [27](#)
Internet browser [35](#)
Internet connection setup [27](#)
introduction [35](#)
IP Address [35, 51](#)

J

Java permissions [83](#)
JavaScript [35, 81](#)

L

LAN light [23](#)
Lights [22, 23](#)
Log in [39](#)

M

MAC address cloning [59](#)
Management [69](#)
Media Access Control address [59](#)
Message Integrity Check (MIC) [34, 91](#)
MIC [34](#)
Microsoft Internet Explorer [35](#)
Mixed mode [59](#)
Modulation [87](#)

N

Netscape Navigator [35](#)
Network [21](#)
Network applications [23](#)
Network card [36](#)
Network number [51](#)
Network overlap [31](#)

O

Office network [21](#)
Open system authentication [33](#)
Output power
 management [59](#)
Output power [87](#)

P

Pairwise Master Key (PMK) [91](#)
Passphrase [33](#)
Password [39, 49](#)
Password phrase [33](#)
Physical specifications [87](#)
Ping [85](#)

Pop-up windows [35, 78](#)
Power [22](#)
Power light [23](#)
Power over Ethernet (PoE) [22](#)
Power socket [23](#)
Preamble [60](#)
Preface [19](#)
Pre-shared key [27](#)
Private IP Address [51](#)
Private key [32](#)
Public key [32](#)
Public-private key pairs [32](#)
Pure B mode [59](#)
Pure G mode [59](#)

Q

Quick Start Guide [19, 22](#)

R

Radio [56](#)
Radio enable [59](#)
Radio interference [76](#)
Radio specifications [87](#)
RADIUS [34](#)
Rear panel [23](#)
Registration [19](#)
Related Documentation [19](#)
Reset [23, 49](#)
Restore [49, 71](#)
Roaming [22, 24](#)
RTS Threshold [57](#)
RTS/CTS [57](#)
RTS/CTS Threshold [60](#)
Rx sensitivity [87](#)

S

safety warnings [7](#)
Scan [49](#)
Screen resolution [35](#)
Security [22, 33, 87](#)
 data encryption [33](#)

Security Parameters [94](#)
Service Set Identity [31, 57](#)
Shared key authentication [33](#)
Signal light [23](#)
Signal strength [24, 61](#)
Small office network [21](#)
Software specifications [87](#)
Specifications [87](#)
SSID [27, 31, 57, 61](#)
Statistics [42](#)
Status [39](#)
Status light [23](#)
Subnet Mask [51](#)
Subnet mask [35](#)
Support [8](#)
Support CD [19](#)
Syntax conventions [19](#)
System screen [51](#)

T

TCP/IP [36, 51](#)
Temperature [87](#)
Temporal Key Integrity Protocol (TKIP) [34, 91](#)
Testing connections [85](#)
TKIP [34](#)
Trademarks [3](#)
Troubleshooting [75](#)
Tutorial [27](#)

U

URL [27, 39](#)
User authentication [32, 92](#)
User name [39, 49](#)

V

Voltage [87](#)

W

- Warranty [6](#)
- Web Configurator [21](#), [35](#)
 - accessing [39](#)
- Web configurator [35](#)
- WEP [33](#)
 - default key [33](#)
 - manual setup [33](#)
 - passphrase [33](#)
- WEP (Wired Equivalent Privacy) [33](#)
- WEP key
 - automatic [33](#)
 - manual [33](#)
- Wi-Fi Protected Access [34](#), [91](#)
- Wired Equivalent Privacy [33](#)
- Wired network [24](#)
- Wireless client [31](#)
- Wireless LAN [22](#)
 - basics [56](#)
 - introduction [31](#)
 - security [32](#)
- Wireless LAN (WLAN) [31](#)
- Wireless mode [59](#)
- Wireless network [31](#)
 - guidelines [31](#)
- Wireless security [32](#)
 - compatibility [32](#)
- Wireless standard [87](#)
- WLAN
 - Security parameters [94](#)
- WLAN light [23](#)
- WPA [34](#), [91](#)
- WPA 2 [34](#)
- WPA2 [91](#)
- WPA2-Pre-Shared Key [91](#)
- WPA2-PSK [91](#)
- WPA-PSK [91](#)

Z

- ZyXEL glossary [19](#)
- ZyXEL Limited Warranty
 - Note [6](#)
- ZyXEL Web Site [19](#)