

ZyAIR B-420

Wireless LAN Ethernet Adapter and Bridge

User's Guide

Version 3.50

September 2003



Copyright

Copyright © 2003 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.

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

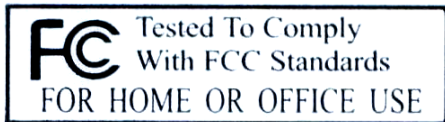
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

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



ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Customer Support

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

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

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science- Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0858	www.us.zyxel.com ftp.zyxel.com	
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

Copyright.....	ii
Federal Communications Commission (FCC) Interference Statement.....	iii
ZyXEL Limited Warranty	iv
Customer Support.....	v
List of Figures	ix
List of Tables	xii
Preface	xiii
OVERVIEW.....	I
Chapter 1 Getting to Know Your ZyAIR.....	1-1
1.1 Introducing the ZyAIR.....	1-1
1.2 ZyAIR Features.....	1-1
1.3 Applications for the ZyAIR	1-4
1.3.1 Infrastructure.....	1-4
1.3.2 Ad Hoc.....	1-5
1.3.3 Bridge	1-5
Chapter 2 Introducing the Web Configurator	2-1
2.1 Accessing the ZyAIR Web Configurator.....	2-1
2.2 Navigating the ZyAIR Web Configurator.....	2-2
2.3 Resetting the ZyAIR	2-3
2.3.1 Method of Restoring Factory-Defaults	2-3
SYSTEM, WIRELESS AND IP.....	II
Chapter 3 System Screens.....	3-1
3.1 System Overview	3-1
3.2 Configuring General Setup	3-1
3.3 Configuring Password.....	3-2
3.4 Configuring Time Setting	3-3
Chapter 4 Wireless LAN	4-1
4.1 Wireless LAN Basis.....	4-1
4.1.1 Channel	4-1
4.1.2 ESS ID	4-1
4.1.3 WEP Encryption	4-1
4.1.4 RTS/CTS.....	4-1
4.1.5 Fragmentation Threshold	4-3
4.2 Wireless Security Overview.....	4-3
4.3 WEP Overview	4-3
4.3.1 Data Encryption	4-4
4.3.2 Authentication.....	4-4
4.4 Configuring Wireless.....	4-5
4.4.1 Infrastructure.....	4-5

4.4.2	Ad-Hoc	4-8
4.4.3	Bridge	4-10
Chapter 5	IP Screen	5-1
5.1	Factory Ethernet Defaults	5-1
5.2	TCP/IP Parameters	5-1
5.2.1	IP Address and Subnet Mask	5-1
5.3	Configuring IP	5-2
LOGS		III
Chapter 6	Logs Screens	6-1
6.1	Configuring View Log	6-1
6.2	Configuring Log Settings	6-2
MAINTENANCE		IV
Chapter 7	Maintenance	7-1
7.1	Maintenance Overview	7-1
7.2	System Status Screen	7-1
7.2.1	System Statistics	7-2
7.3	Wireless Screen	7-3
7.4	F/W Upload Screen	7-5
7.5	Configuration Screen	7-7
7.5.1	Backup Configuration	7-7
7.5.2	Restore Configuration	7-8
7.5.3	Back to Factory Defaults	7-10
SMT CONFIGURATION.....		V
Chapter 8	Introducing the SMT	8-1
8.1	Connect to your ZyAIR Using Telnet	8-1
8.2	Changing the System Password	8-1
8.3	ZyAIR SMT Menu Overview Example	8-2
8.4	Navigating the SMT Interface.....	8-4
8.4.1	System Management Terminal Interface Summary	8-5
Chapter 9	General Setup	9-1
9.1	General Setup	9-1
9.1.1	Procedure To Configure Menu 1	9-1
Chapter 10	LAN Setup	10-1
10.1	LAN Setup	10-1
10.2	TCP/IP Ethernet Setup	10-1
10.3	Wireless LAN Setup	10-2
10.3.1	Configuring Bridge Link	10-5
Chapter 11	SNMP Configuration.....	11-1
11.1	About SNMP	11-1
11.2	Supported MIBs	11-2
11.3	SNMP Configuration	11-2

11.4	SNMP Traps	11-3
Chapter 12	System Information	12-1
12.1	System Status.....	12-1
12.2	System Information.....	12-3
12.2.1	System Information.....	12-3
12.2.2	Console Port Speed.....	12-4
12.3	Log and Trace	12-5
12.3.1	Viewing Error Log.....	12-5
Chapter 13	Firmware and Configuration File Maintenance	13-1
13.1	Filename Conventions	13-1
13.2	Backup Configuration.....	13-2
13.2.1	Backup Configuration Using FTP.....	13-2
13.2.2	Using the FTP command from the DOS Prompt	13-3
13.2.3	Backup Configuration Using TFTP	13-4
13.2.4	Example: TFTP Command	13-4
13.3	Restore Configuration.....	13-5
13.4	Uploading Firmware and Configuration Files	13-6
13.4.1	Firmware Upload	13-7
13.4.2	Configuration File Upload	13-7
13.4.3	Using the FTP command from the DOS Prompt Example	13-8
13.4.4	TFTP File Upload	13-9
13.4.5	Example: TFTP Command	13-10
Chapter 14	System Maintenance and Information	14-1
14.1	Command Interpreter Mode.....	14-1
14.2	Time and Date Setting	14-2
APPENDICES.....		VI
Appendix A	Troubleshooting.....	A-1
Appendix B	Brute-Force Password Guessing Protection	B-1
Appendix C	Setting up Your Computer's IP Address.....	C-1
Appendix D	Wireless LAN and IEEE 802.11	D-1
Appendix E	Antenna Selection and Positioning Recommendation	E-1
Appendix F	Power over Ethernet Specifications.....	F-1
Appendix G	IP Subnetting	G-1
Appendix H	Command Interpreter.....	H-1
Appendix I	Log Descriptions	I-1
Appendix J	Power Adaptor Specifications	J-1
Appendix K	Index.....	K-1

List of Figures

Figure 1-1 PoE Installation Example	1-2
Figure 1-2 Infrastructure Network Example	1-4
Figure 1-3 Ad-hoc Application Example	1-5
Figure 1-4 Bridge Application Example	1-5
Figure 2-1 Web Browser Address Field	2-1
Figure 2-2 Change Password Screen.....	2-1
Figure 2-3 The MAIN MENU Screen of the Web Configurator	2-2
Figure 3-1 System General Setup	3-1
Figure 3-2 Password.....	3-3
Figure 3-3 Time Setting	3-4
Figure 4-1 RTS/CTS	4-2
Figure 4-2 ZyAIR Wireless Security Levels	4-3
Figure 4-3 WEP Authentication Steps.....	4-4
Figure 4-4 Infrastructure Network Example	4-5
Figure 4-5 Roaming Example	4-6
Figure 4-6 Wireless : Infrastructure	4-7
Figure 4-7 Ad-hoc (IBSS) Wireless LAN	4-9
Figure 4-8 Wireless : Ad Hoc.....	4-9
Figure 4-9 Bridging Example.....	4-10
Figure 4-10 Bridge Loop: Two Bridges Connected to Hub	4-11
Figure 4-11 Bridge Loop: Bridge Connected to Wired LAN.....	4-11
Figure 4-12 Wireless : Bridge	4-12
Figure 5-1 IP	5-2
Figure 6-1 View Log	6-1
Figure 6-2 Log Settings.....	6-3
Figure 7-1 System Status	7-1
Figure 7-2 System Status: Show Statistics	7-2
Figure 7-3 Channel Usage.....	7-4
Figure 7-4 Firmware Upload.....	7-5
Figure 7-5 Firmware Upload In Process	7-6
Figure 7-6 Network Temporarily Disconnected.....	7-7
Figure 7-7 Firmware Upload Error	7-7
Figure 7-8 Backup Configuration	7-8
Figure 7-9 Restore Configuration	7-8
Figure 7-10 Configuration Upload Successful.....	7-9
Figure 7-11 Network Temporarily Disconnected.....	7-9
Figure 7-12 Configuration Upload Error	7-10
Figure 7-13 Back to Factory Default.....	7-10
Figure 7-14 Reset Warning Message.....	7-11

Figure 8-1 Login Screen	8-1
Figure 8-2 Menu 23.1 System Security : Change Password	8-2
Figure 8-3 ZyAIR B-420 SMT Menu Overview Example	8-3
Figure 8-4 ZyAIR B-420 SMT Main Menu.....	8-5
Figure 9-1 Menu 1 General Setup.....	9-1
Figure 10-1 Menu 3 LAN Setup	10-1
Figure 10-2 Menu 3.2 TCP/IP Setup.....	10-1
Figure 10-3 Menu 3.5 Wireless LAN Setup	10-3
Figure 10-4 Menu 3.5 Wireless LAN Setup	10-5
Figure 10-5 Menu 3.5.4 Bridge Link Configuration.....	10-5
Figure 11-1 SNMP Management Model.....	11-1
Figure 11-2 Menu 22 SNMP Configuration	11-3
Figure 12-1 Menu 24 System Maintenance	12-1
Figure 12-2 Menu 24.1 System Maintenance : Status	12-2
Figure 12-3 Menu 24.2 System Information and Console Port Speed.....	12-3
Figure 12-4 Menu 24.2.1 System Information : Information.....	12-3
Figure 12-5 Menu 24.2.2 System Maintenance : Change Console Port Speed.....	12-4
Figure 12-6 Menu 24.3 System Maintenance : Log and Trace	12-5
Figure 12-7 Sample Error and Information Messages	12-5
Figure 13-1 Menu 24.5 Backup Configuration.....	13-2
Figure 13-2 FTP Session Example.....	13-3
Figure 13-3 Menu 24.6 Restore Configuration.....	13-6
Figure 13-4 Menu 24.7 System Maintenance : Upload Firmware	13-6
Figure 13-5 Menu 24.7.1 System Maintenance : Upload System Firmware	13-7
Figure 13-6 Menu 24.7.2 System Maintenance : Upload System Configuration File	13-8
Figure 13-7 FTP Session Example.....	13-9
Figure 14-1 Menu 24 System Maintenance	14-1
Figure 14-2 Valid CI Commands	14-1
Figure 14-3 Menu 24.10 System Maintenance : Time and Date Setting	14-2

List of Tables

Table 3-1 System General Setup.....	3-2
Table 3-2 Password.....	3-3
Table 3-3 Time Setting.....	3-4
Table 4-1 Wireless : Infrastructure.....	4-7
Table 4-2 Wireless : Ad Hoc	4-10
Table 4-3 Wireless : Bridge.....	4-12
Table 5-1 Private IP Address Ranges	5-2
Table 5-2 IP.....	5-3
Table 6-1 View Log	6-2
Table 6-2 Log Settings.....	6-3
Table 7-1 System Status.....	7-1
Table 7-2 System Status: Show Statistics	7-2
Table 7-3 Channel Usage.....	7-4
Table 7-4 Firmware Upload.....	7-6
Table 7-5 Restore Configuration.....	7-9
Table 8-1 Main Menu Commands	8-4
Table 8-2 Main Menu Summary	8-5
Table 9-1 Menu 1 General Setup	9-2
Table 10-1 Menu 3.2 TCP/IP Setup	10-2
Table 10-2 Menu 3.5 Wireless LAN Setup	10-3
Table 10-3 Menu 3.5.4 Bridge Link Configuration	10-6
Table 11-1 Menu 22 SNMP Configuration	11-3
Table 11-2 SNMP Traps.....	11-4
Table 11-3 Ports and Interface Types.....	11-4
Table 12-1 Menu 24.1 System Maintenance : Status.....	12-2
Table 12-2 System Maintenance : Information.....	12-4
Table 13-1 Filename Conventions	13-2
Table 13-2 General Commands for Third Party FTP Clients.....	13-3
Table 13-3 General Commands for Third Party TFTP Clients	13-5
Table 14-1 Menu 24.10 System Maintenance : Time and Date Setting	14-2

Preface

Congratulations on your purchase of the ZyAIR B-420 Wireless LAN Ethernet Adapter and Bridge.

The ZyAIR B-420 is an IEEE 802.11b compliant 11Mbps wireless LAN Ethernet Adapter and Bridge, which supports Wireless Distribution System (WDS) for workgroup bridge applications.

This User's Guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT.

Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your ZyAIR. Not all features can be configured through all interfaces.

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information on features not configurable by the web configurator.

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Installation Guide
Our Quick Installation Guide is designed to help you get up and running right away. It contains information on the configuration of key features and hardware connections and installation.
- ZyXEL Web Site
The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- “Type” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one predefined choices.
- Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.

- The ZyAIR B-420 Wireless LAN Ethernet Adapter and Bridge will be referred to simply as the ZyAIR in the user's guide.

User Guide Feedback

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

Part I:

OVERVIEW

This part introduces the main features and applications of the ZyAIR and shows how to access the web configurator.

Chapter 1

Getting to Know Your ZyAIR

This chapter introduces the main features and applications of the ZyAIR.

1.1 Introducing the ZyAIR

The ZyAIR is an IEEE802.11b compliant 11Mbps wireless LAN Ethernet Adapter and Bridge. The ZyAIR provides easy network access to mobile users. The ZyAIR also supports Wireless Distribution System (WDS) for workgroup bridge applications.

You may configure and manage the ZyAIR using SMT via Telnet, embedded web configurator or SNMP. You can access the SMT or web configurator from the LAN only in Infrastructure and Ad-Hoc modes. But in WDS mode, the ZyAIR is configurable from either end of the bridge link.

1.2 ZyAIR Features

Your ZyAIR is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

10/100M Auto-negotiating Ethernet/Fast Ethernet Interface

This auto-negotiating feature allows the ZyAIR to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

10/100M Auto-crossover Ethernet/Fast Ethernet Interface

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

Reset Button

The ZyAIR reset button is built into the top panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.11, subnet mask to 255.255.255.0.

ZyAIR LED

The blue ZyAIR LED (also known as the Breathing LED) is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. You may use the web configurator to turn this LED off even when the ZyAIR is on and data is being transmitted/received.

Bridge

A Bridge link LED turns steady on green when your ZyAIR acts as a bridge, establishing a wireless link to another AP.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is the ability to provide power to your ZyAIR via an 8-pin CAT 5 Ethernet cable, eliminating the need for a nearby power source. An injector or PoE device (not included) is also needed to supply the Ethernet cable with power. This feature allows increased flexibility in the locating of your ZyAIR. You only need to connect the external power adaptor if you are not using PoE. If you simultaneously use both PoE and the external power adaptor, the ZyAIR will draw power from the PoE connection only. Refer to the appendix for more information about PoE.

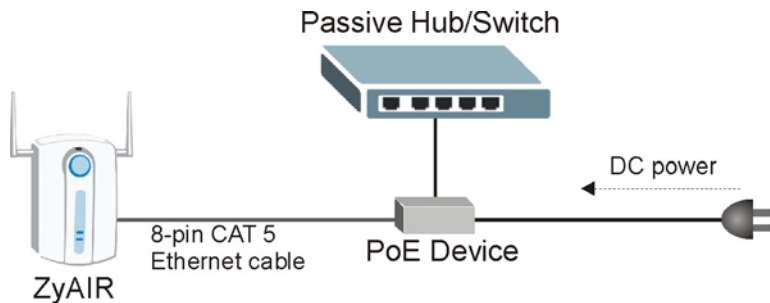


Figure 1-1 PoE Installation Example

802.11b Wireless LAN Standard

ZyAIR products containing the letter “B” in the model name, such as ZyAIR B-1000, ZyAIR B-1020, comply with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

802.11b	
Data Rate (Mbps)	Modulation
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

The ZyAIR may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

Output Power Management

Power Management is the ability to set the level of output power. This feature is only available in bridge mode.

There may be interference or difficulty with channel assignment when there is a high density of APs within a coverage area. In this case you can lower the output power of each access point, thus enabling you to place access points closer together.

WDS Functionality

A Distribution System (DS) is a wired connection between two or more APs, while a Wireless Distribution System (WDS) is a wireless connection. Your ZyAIR supports WDS, providing a cost-effective solution for wireless network expansion.

Brute-Force Password Guessing Protection

The ZyAIR has a special protection mechanism to discourage brute-force password guessing attacks on the ZyAIR's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendix for details about this feature.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyAIR's management settings. Most functions of the ZyAIR are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

Logging and Tracing

- ◆ Built-in message logging and packet tracing.
- ◆ Unix syslog facility support.

Embedded FTP and TFTP Servers

The ZyAIR's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

Wireless LAN Channel Usage

The **Wireless Channel Usage** screen displays whether the radio channels are used by other wireless devices within the transmission range of the ZyAIR. This allows you to select the channel with minimum interference for your ZyAIR.

1.3 Applications for the ZyAIR

Here are some application examples of what you can do with your ZyAIR.

1.3.1 Infrastructure

When wireless stations wish to access and share resources on the wired network, they should use infrastructure mode. Wireless stations may move from one coverage area to another seamlessly without network interruption. This is called roaming.

The figure below depicts an infrastructure network example.

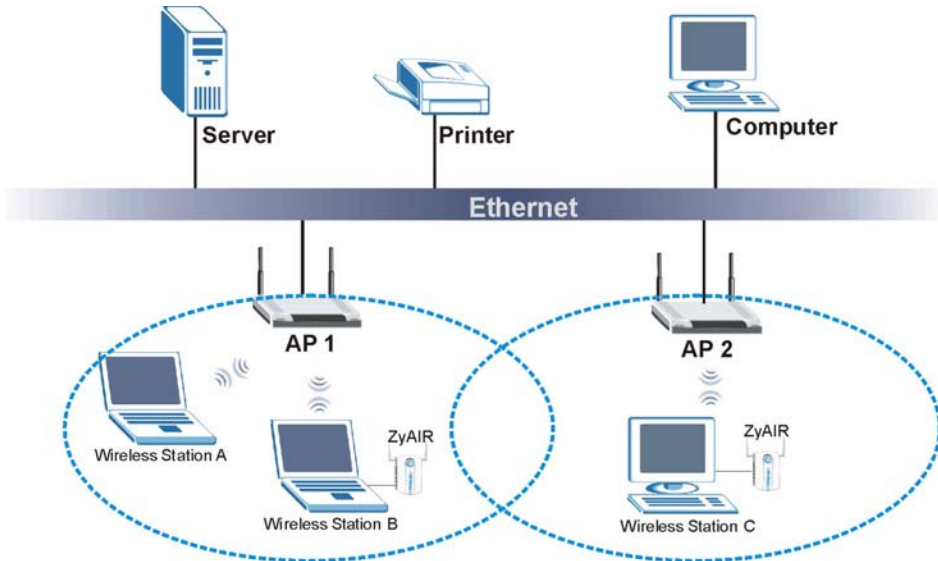


Figure 1-2 Infrastructure Network Example

1.3.2 Ad Hoc

An ad-hoc network consists of two or more computers communicating with one another through the wireless network. No access points (APs) or existing wired networks are needed. An access point acts as a bridge between the wireless and wired networks.



Figure 1-3 Ad-hoc Application Example

1.3.3 Bridge

The ZyAIR can function as wireless network bridge allowing you to connect two wired network segments. This wireless bridge connection is equivalent to a Wireless Distribution System (WDS).

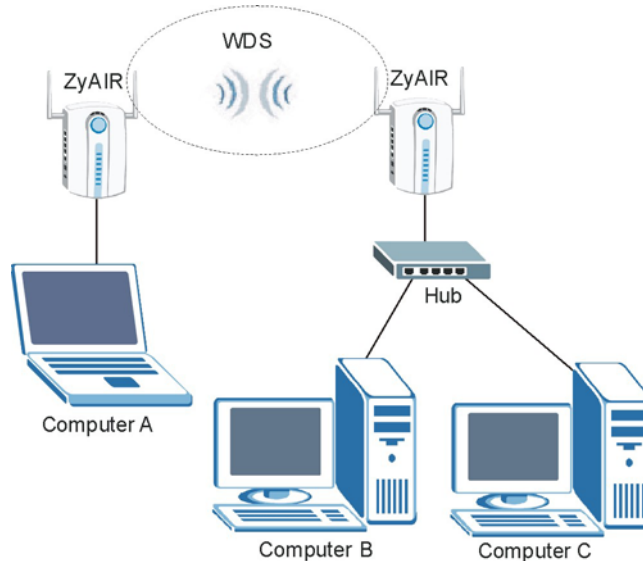


Figure 1-4 Bridge Application Example

Chapter 2

Introducing the Web Configurator

This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens. The default IP address of the ZyAIR is 192.168.1.11.

2.1 Accessing the ZyAIR Web Configurator

- Step 1.** Make sure your ZyAIR hardware is properly connected (refer to the Quick Installation Guide).
- Step 2.** Prepare your computer/computer network to connect to the ZyAIR (refer to the appendix).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.11" (default) as the URL.

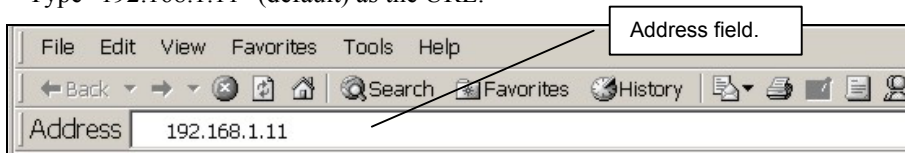


Figure 2-1 Web Browser Address Field

- Step 5.** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- Step 6.** You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore** to allow access without password change.

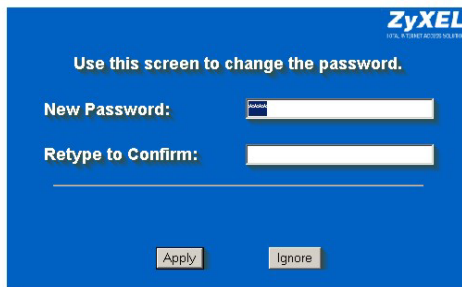


Figure 2-2 Change Password Screen

Step 7. You should now see the **MAIN MENU** screen.

The ZyAIR automatically times out after five minutes of inactivity. Simply log back into the ZyAIR if this happens to you.

2.2 Navigating the ZyAIR Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

Follow the instructions you see in the **MAIN MENU** screen or click the  icon (located in the top right corner of most screens) to view online help.

The  icon does not appear in the **MAIN MENU** screen.

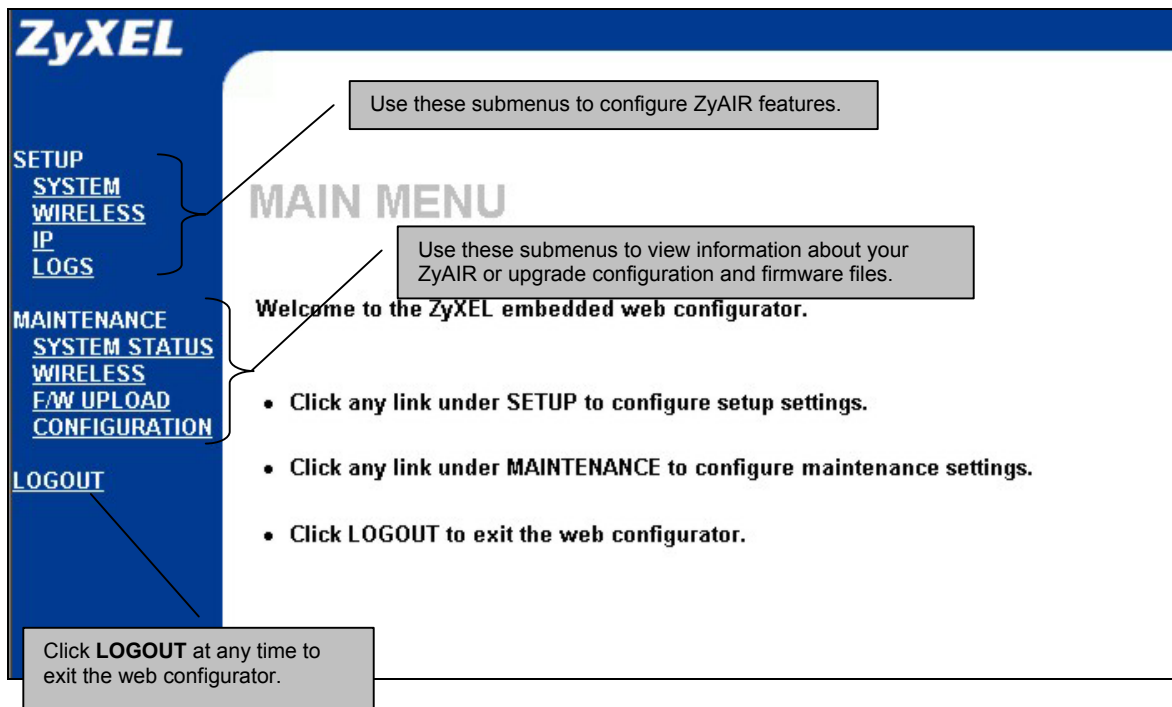


Figure 2-3 The MAIN MENU Screen of the Web Configurator

2.3 Resetting the ZyAIR

If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file or use the **RESET** button on the top panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to “1234”, also.

2.3.1 Method of Restoring Factory-Defaults

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

1. Use the **RESET** button on the top panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the Link LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known.
2. Use the web configurator to restore defaults (refer to the *Maintenance* chapter).
3. Transfer the configuration file to your ZyAIR using FTP. See the part on SMT configuration for more information.

Part II:

SYSTEM, WIRELESS AND IP

This part covers System, Wireless and IP web configurator screens.

Chapter 3

System Screens

This chapter provides information on the System screens.

3.1 System Overview

This section provides information on general system setup.

3.2 Configuring General Setup

Click **SYSTEM** under **SETUP** to open the **General** screen.

SYSTEM

General Password Time Setting

System Name B-420

Domain Name

Administrator Inactivity Timer 5 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server None 0.0.0.0

Second DNS Server User-Defined 0.0.0.0

Third DNS Server None 0.0.0.0

Apply Reset

Figure 3-1 System General Setup

The following table describes the labels in this screen.

Table 3-1 System General Setup

LABEL	DESCRIPTION
System Name	Type a descriptive name to identify the ZyAIR in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select From DHCP if your DHCP server dynamically assigns DNS server information (and the ZyAIR's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is None .
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

3.3 Configuring Password

To change your ZyAIR's password (recommended), click **SYSTEM** under **SETUP** and then the **Password** tab. The screen appears as shown. This screen allows you to change the ZyAIR's password.

If you forget your password (or the ZyAIR IP address), you will need to reset the ZyAIR. See the *Resetting the ZyAIR* section for details.

SYSTEM

General Password Time Setting

Old Password

New Password

Retype to Confirm

Apply Reset

Figure 3-2 Password

The following table describes the labels in this screen.

Table 3-2 Password

LABEL	DESCRIPTION
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type your new system password again for confirmation.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

3.4 Configuring Time Setting

To change your ZyAIR's time and date, click **SYSTEM** under **SETUP** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the ZyAIR's system time.

SYSTEM

General

Password

Time Setting

Current Time (hh:mm:ss)

0

:

8

:

19

New Time (hh:mm:ss)

0

:

8

:

14

Current Date (yyyy/mm/dd)

2000

/

1

/

1

New Date (yyyy/mm/dd)

2000

/

1

/

1

Apply

Reset

Figure 3-3 Time Setting

The following table describes the labels in this screen.

Table 3-3 Time Setting

LABEL	DESCRIPTION
Current Time (hh:mm:ss)	This field displays the time of your ZyAIR.
New Time (hh:mm:ss)	Enter the new time in this field.
Current Date (yyyy:mm:dd)	This field displays the date of your ZyAIR.
New Date (yyyy:mm:dd)	Enter the new date in this field.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

Chapter 4

Wireless LAN

This chapter discusses how to configure Wireless LAN screens on the ZyAIR.

4.1 Wireless LAN Basis

This section provides basic background information on the wireless LAN screens.

4.1.1 Channel

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

Adjacent channels partially overlap however. To avoid interference due to overlap, your ZyAIR 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.

The ZyAIR’s “Scan” function is especially designed to automatically scan for a channel with the least interference.

4.1.2 ESS ID

An Extended Service Set (ESS) is a group of access points connected to a wired LAN on the same subnet. An ESS ID uniquely identifies each set. All access points and their associated wireless stations in the same set must have the same ESSID.

4.1.3 WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

4.1.4 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 (STA) 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.

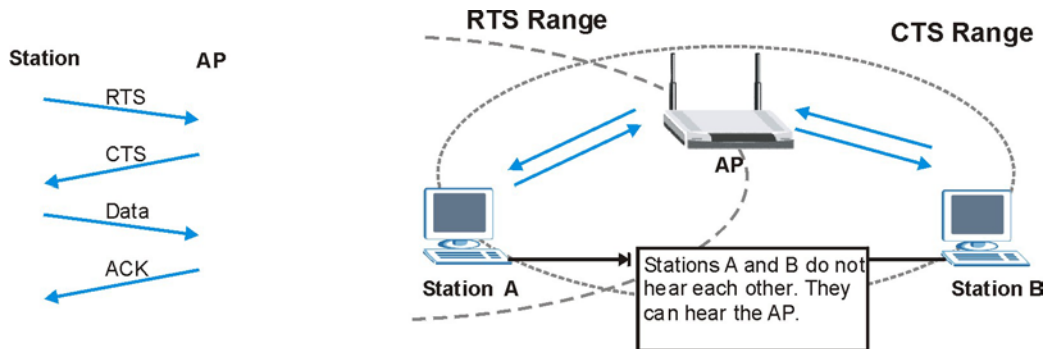


Figure 4-1 RTS/CTS

When station A sends data to the ZyAIR, it might not know that 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.

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

4.1.5 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 ZyAIR 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.

4.2 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 ZyAIR. The highest security level relies on EAP (Extensible Authentication Protocol) for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

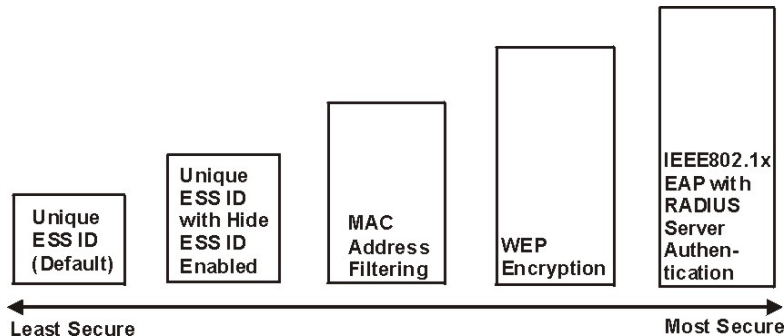


Figure 4-2 ZyAIR Wireless Security Levels

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

4.3 WEP Overview

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

4.3.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. The values for the keys must be set up exactly the same on the APs or other peer ad-hoc wireless computers as they are on the ZyAIR to encrypt and decrypt data. Your ZyAIR allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

4.3.2 Authentication

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

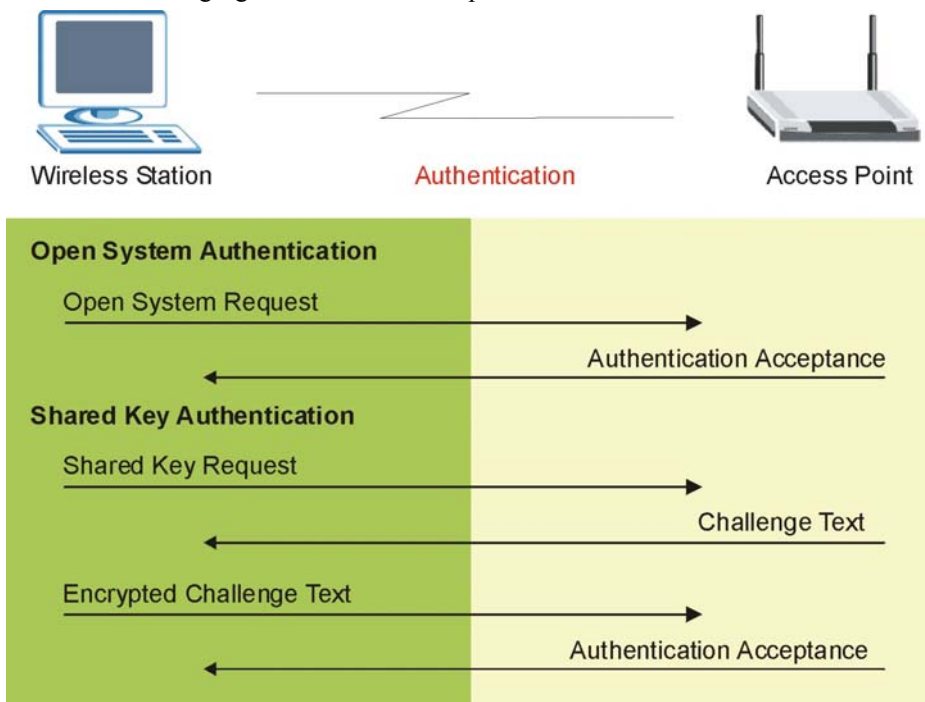


Figure 4-3 WEP Authentication Steps

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station

must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your ZyAIR's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the ZyAIR will accept either type of authentication request and the ZyAIR will fall back to use open authentication if the shared key does not match.

4.4 Configuring Wireless

Click **WIRELESS** under **SETUP** to display the **Wireless** screen.

To use your ZyAIR as a wireless LAN adapter, select the **Infrastructure** or **Ad Hoc** operating mode. To use your ZyAIR as a wireless LAN bridge connecting two wired network segments, select the **Bridge** operating mode. The screen varies according to the operating mode you select.

4.4.1 Infrastructure

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

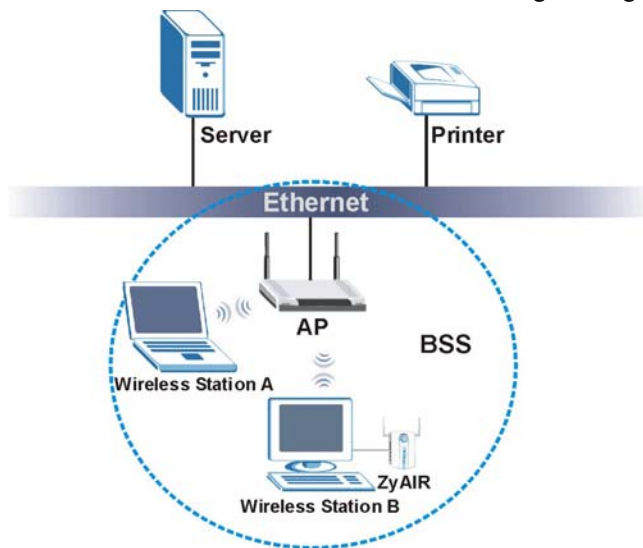


Figure 4-4 Infrastructure Network Example

Roaming

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

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

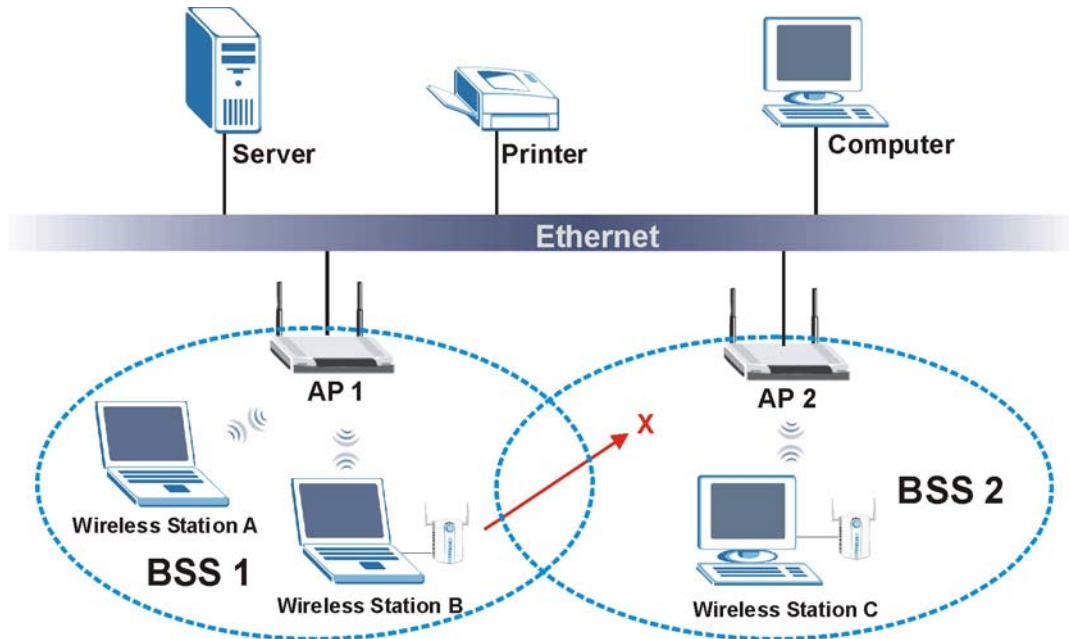


Figure 4-5 Roaming Example

Select **Infrastructure** from the **Operating Mode** drop-down list box to display the screen as shown.

WIRELESS LAN

Wireless

Operating Mode

Infrastructure

ESSID

Any

RTS/CTS Threshold

2432 (0 ~ 2432)

Fragmentation Threshold

2432 (256 ~ 2432)

WEP Encryption

Disable

Authentication Method

Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
 (Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII
 ☐ Hex

☒ Key 1
☐ Key 2
☐ Key 3
☐ Key 4

☒ Enable Breathing LED

Apply

Reset

Figure 4-6 Wireless : Infrastructure

The following table describes the labels in this screen.

Table 4-1 Wireless : Infrastructure

LABEL	DESCRIPTION
Operating Mode	Select Infrastructure from the drop-down list.
ESSID	In this field enter the ESSID of the AP to which you want to associate. To associate to an ad-hoc network, you must enter the same ESSID as the peer ad-hoc computer. Enter Any to associate to or roam between any infrastructure wireless networks.
RTS/CTS Threshold	Enter a value between 0 and 2432 . The default is 2432 .

Table 4-1 Wireless : Infrastructure

LABEL	DESCRIPTION
Fragmentation Threshold	Enter a value between 256 and 2432 . It is the maximum data fragment size that can be sent.
WEP Encryption	Select Disable to allow wireless stations to communicate with the AP without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	Select Auto , Open System Only or Shared Key Only from the drop-down list box. This field is N/A if WEP is not activated. If WEP encryption is activated, the default setting is Auto .
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the AP 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"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

4.4.2 Ad-Hoc

An Ad-hoc network, also called an Independent Basic Service Set (IBSS), is the simplest WLAN configuration. An Ad-hoc network is defined as two or more computers with wireless adapters within range of each other that form an independent (wireless) network without the need of an access point (AP).

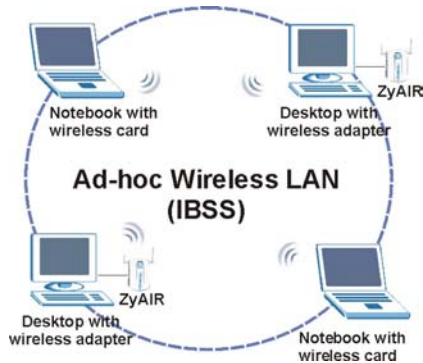


Figure 4-7 Ad-hoc (IBSS) Wireless LAN

Select **Ad Hoc** in the **Operating Mode** drop-down list box to display the screen as shown.

WIRELESS LAN

Wireless

Operating Mode

ESSID

Choose Channel ID or

RTS/CTS Threshold (0 ~ 2432)

Fragmentation Threshold (256 ~ 2432)

WEP Encryption

Authentication Method

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ('0-9', 'A-F') for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ('0-9', 'A-F') for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII ☐ Hex

☒ Key 1

☐ Key 2

☐ Key 3

☐ Key 4

☒ Enable Breathing LED

Figure 4-8 Wireless : Ad Hoc

The following table describes the additional fields that display when you select the **Ad Hoc** operating mode in the **Wireless** screen.

Table 4-2 Wireless : Ad Hoc

LABEL	DESCRIPTION
Operating Mode	Select Ad Hoc in this field to display the screen.
ESSID	In this field enter the ESSID of the peer ad-hoc computer to which you want to associate. To associate to an ad-hoc network, you must enter the same ESSID as the peer ad-hoc computer. Enter Any to associate to or roam between any infrastructure wireless networks.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click WIRELESS under MAINTENANCE to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click Scan instead.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.

4.4.3 Bridge

The ZyAIR can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. You need to know the MAC address of the peer device, which also must be in bridge mode. In the example below, Computers B and C will be able to communicate with Computer A through the ZyAIR bridges, forming a Wireless Distribution System (WDS).

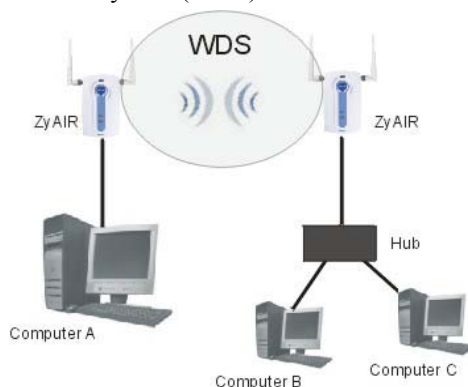


Figure 4-9 Bridging Example

Be careful to avoid bridge loops when you enable bridging in the ZyAIR. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

- If two or more ZyAIRs (in bridge mode) are connected to the same hub as shown next.

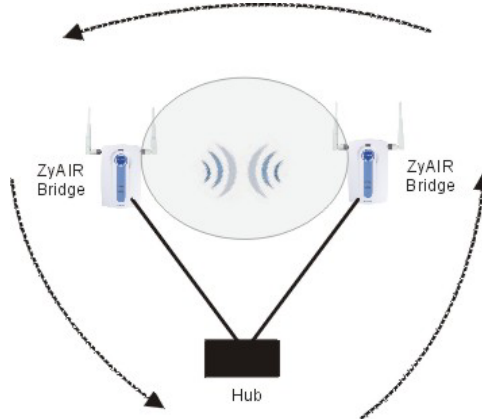


Figure 4-10 Bridge Loop: Two Bridges Connected to Hub

- If your ZyAIR (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN as shown next.

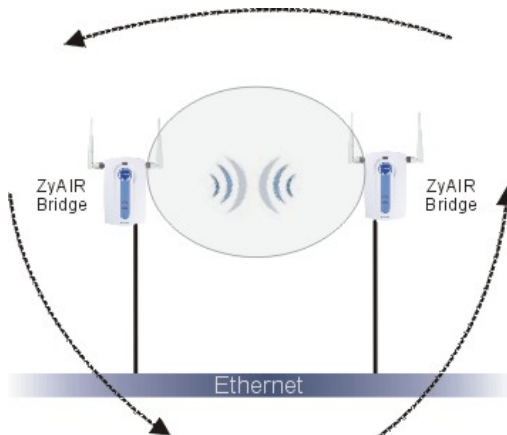


Figure 4-11 Bridge Loop: Bridge Connected to Wired LAN

To prevent bridge loops, ensure that your ZyAIR is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

Click **WIRELESS** under **SETUP**. Select **Bridge** in the **Operating Mode** drop-down list box to display the screen as shown.

WIRELESS LAN

Wireless

Operating Mode

Bridge

Choose Channel ID

Channel-06 2437MHz

or

Scan

RTS/CTS Threshold

2432

(0 ~ 2432)

Fragmentation Threshold

2432

(256 ~ 2400)

Peer Bridge MAC Address

00:00:00:00:00:00

WEP Encryption

Disable

Authentication Method

Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

ASCII

Hex

Key 1

Key 2

Key 3

Key 4

Enable Breathing LED

☒

Output Power

17dBm (50mW)

Apply

Reset

Figure 4-12 Wireless : Bridge

The following table describes the additional fields that display when you select the **Bridge** operating mode in the **Wireless** screen.

Table 4-3 Wireless : Bridge

LABEL	DESCRIPTION
Operating Mode	Select Bridge in this field to display the screen as shown in <i>Figure 4-12</i> .

Table 4-3 Wireless : Bridge

LABEL	DESCRIPTION
Peer Bridge MAC Address	Type the MAC address of peer device in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
WEP Encryption	Select Disable to allow wireless stations to communicate with the AP without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	Select Auto , Open System Only or Shared Key Only from the drop-down list box. This field is N/A if WEP is not activated. If WEP encryption is activated, the default setting is Auto .
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the AP 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"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Output Power	Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. The options are 11dBm (12.6mW) , 13dBm (20mW) , 15dBm (32mW) or 17dBm (50mW) .

Chapter 5

IP Screen

This chapter discusses how to configure IP on the ZyAIR.

5.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyAIR are preset in the factory with the following values:

- IP address of 192.168.1.11
- Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

5.2 TCP/IP Parameters

5.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do 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.

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 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, 192.168.1.11, for your ZyAIR, 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 ZyAIR 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 ZyAIR unless you are instructed to do otherwise.

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 5-1 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.

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.

5.3 Configuring IP

Click **IP** to display the screen shown next.

WAN

IP

IP Address Assignment

☐ Get automatically

☒ Use fixed IP address

IP Address

192.168.1.11

IP Subnet Mask

255.255.255.0

Gateway IP Address

0.0.0.0

Apply

Reset

Figure 5-1 IP

The following table describes the labels in this screen.

Table 5-2 IP

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically	<p>Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time.</p> <p>You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.</p>
Use fixed IP address	Select this option if your ZyAIR is using a static IP address. When you select this option, fill in the fields below.
IP Address	<p>Enter the IP address of your ZyAIR in dotted decimal notation.</p> <p>If you change the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.</p>
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

Part III:

LOGS

This part provides information and configuration instructions for the logs.

Chapter 6

Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyAIR's logs. Refer to the appendix for example log message explanations.

6.1 Configuring View Log

The web configurator allows you to look at all of the ZyAIR's logs in one location.

Click **LOGS** under **SETUP** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 6.2*). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Alerts are displayed in red and logs are displayed in black. Once the number of log entries are all used, the log will wrap around and the old logs will be deleted. Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

LOGS

View Log **Log Settings**

Display: All Logs [v] [Email Log Now] [Refresh] [Clear Log]

#	Time ▲	Message	Source	Destination	Note
1	01/01/2000 00:03:32	User login from WEB successfully	192.168.1.30		User:admin
2	01/01/2000 00:01:22	User login from TELNET successfully	192.168.1.30		User:admin

Figure 6-1 View Log

The following table describes the labels in this screen.

Table 6-1 View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select All Logs . The number of categories shown in the drop down list box depends on the selection in the Log Settings page.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page.
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to clear all the logs.

6.2 Configuring Log Settings

To change your ZyAIR’s log settings, click **LOGS** under **SETUP** and then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyAIR is to send the logs; the schedule for when the ZyAIR is to send the logs and which logs and/or immediate alerts the ZyAIR is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

LOGS

View Log

Log Settings

Address Info

Mail Server

(Outgoing SMTP Server Name or IP Address)

Mail Subject

Send Log to

(E-Mail Address)

Send Alerts to

(E-Mail Address)

Syslog Logging

☐ Active

Syslog Server IP Address

0.0.0.0

(Server Name or IP Address)

Log Facility

Local 1

Send Log

Log Schedule

When Log is Full

Day for Sending Log

Sunday

Time for Sending Log

0 (hour) 0 (minute)

Log

☒ System Maintenance
☒ System Errors
☒ TCP Reset
☒ Packet Filter

Send Immediate Alert

☒ System Errors

Apply

Reset

Figure 6-2 Log Settings

The following table describes the labels in this screen.

Table 6-2 Log Settings

LABEL	DESCRIPTION
Address Info	

Table 6-2 Log Settings

LABEL	DESCRIPTION
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyAIR sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	
Active	Click Active to enable UNIX syslog.
Syslog IP Address	Enter the server name or the IP address of the syslog server that will log the CDR (Call Detail Record) and system messages.
Log Facility	Select the Local from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to your UNIX manual for more information.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When the Log is Full • None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	This field is only available when you select Weekly in the Log Schedule field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record.

Table 6-2 Log Settings

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to reconfigure all the fields in this screen.

Part IV:

MAINTENANCE

This part describes the Maintenance web configurator screens.

Chapter 7

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

7.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyAIR.

7.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your ZyAIR. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

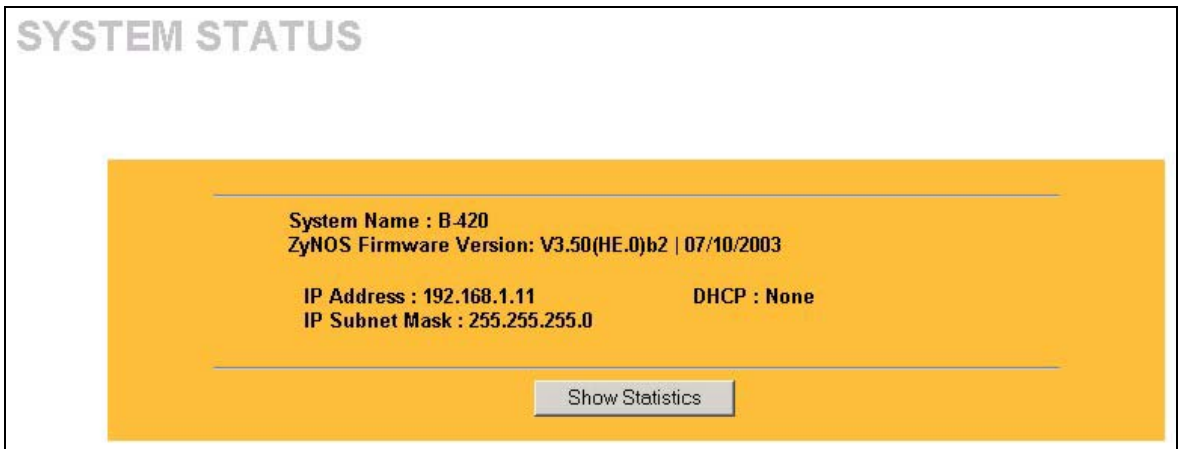


Figure 7-1 System Status

The following table describes the labels in this screen.

Table 7-1 System Status

LABEL	DESCRIPTION
System Name	This is the System Name you enter in the first Internet Access Wizard screen. It is for identification purposes

Table 7-1 System Status

LABEL	DESCRIPTION
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.
DHCP	This is the Ethernet port DHCP role - Client or None .
Show Statistics	Click Show Statistics to see router performance statistics such as number of packets sent and number of packets received for each port.

7.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval". The **Poll Interval** field is configurable.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
Ethernet	100M/Full	264	663	0	0	124	0:15:34
Wireless	11M	293	0	0	64	0	0:15:35

System Up Time : 0:15:40

Poll Interval : sec

Figure 7-2 System Status: Show Statistics

The following table describes the labels in this screen.

Table 7-2 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port.

Table 7-2 System Status: Show Statistics

LABEL	DESCRIPTION
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission speed only for wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
System Up Time	This is the total time the ZyAIR has been on.
Poll Interval	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.

7.3 Wireless Screen

The **Channel Usage** screen shows whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **WIRELESS** under **MAINTENANCE** to display the screen as shown next.

Wait a moment while the ZyAIR compiles the information.

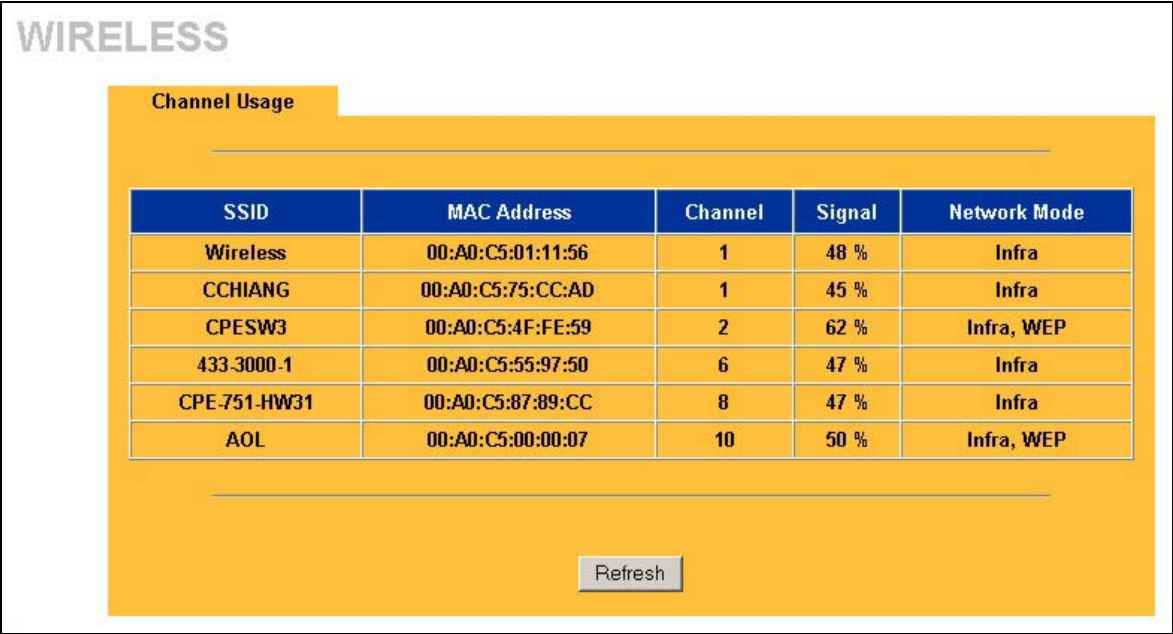


Figure 7-3 Channel Usage

The following table describes the labels in this screen.

Table 7-3 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the <i>Wireless LAN</i> chapter for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.

Table 7-3 Channel Usage

LABEL	DESCRIPTION
Network Mode	<p>“Network mode” in this screen refers to your wireless LAN infrastructure (refer to the <i>Wireless LAN</i> chapter) and WEP setup.</p> <p>Network modes are: Infra (same as an extended service set ESS), Infra, WEP (WEP encryption is enabled), Ad-Hoc (same as an independent basic service set IBSS), or Ad-Hoc, WEP.</p>
Refresh	Click Refresh to reload the screen.

7.4 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "zyair.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the *Firmware and Configuration File Maintenance* chapter for upgrading firmware using FTP/TFTP commands.

Click **F/W UPLOAD** under **MAINTENANCE**. Follow the instructions in this screen to upload firmware to your ZyAIR.

FIRMWARE UPLOAD

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.

File Path:

Figure 7-4 Firmware Upload

The following table describes the labels in this screen.

Table 7-4 Firmware 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 .bin 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 interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyAIR. When the firmware upload process is complete, the ZyAIR will automatically restart.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

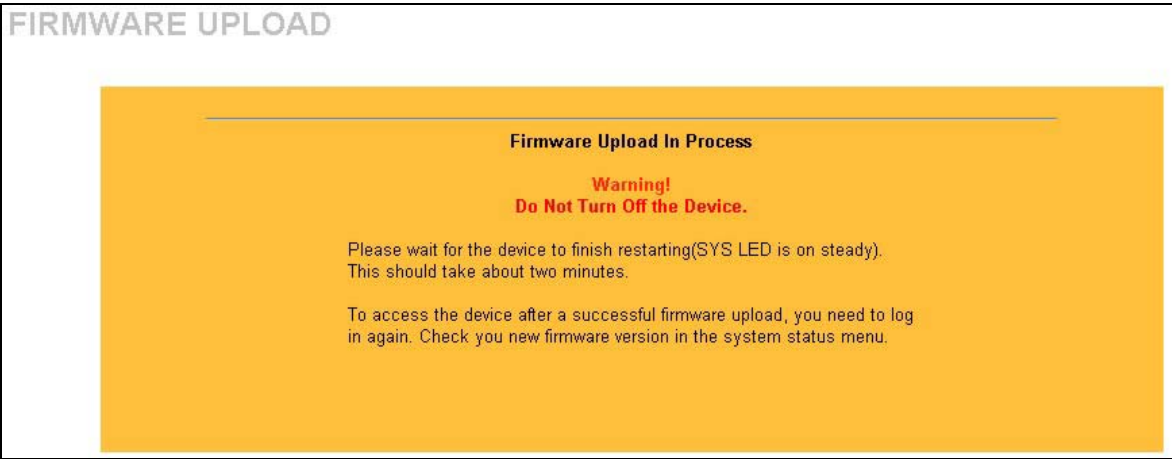


Figure 7-5 Firmware Upload In Process

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

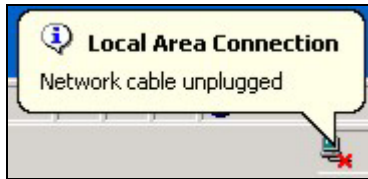


Figure 7-6 Network Temporarily Disconnected

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 screen will appear. Click **Return** to go back to the **F/W Upload** screen.

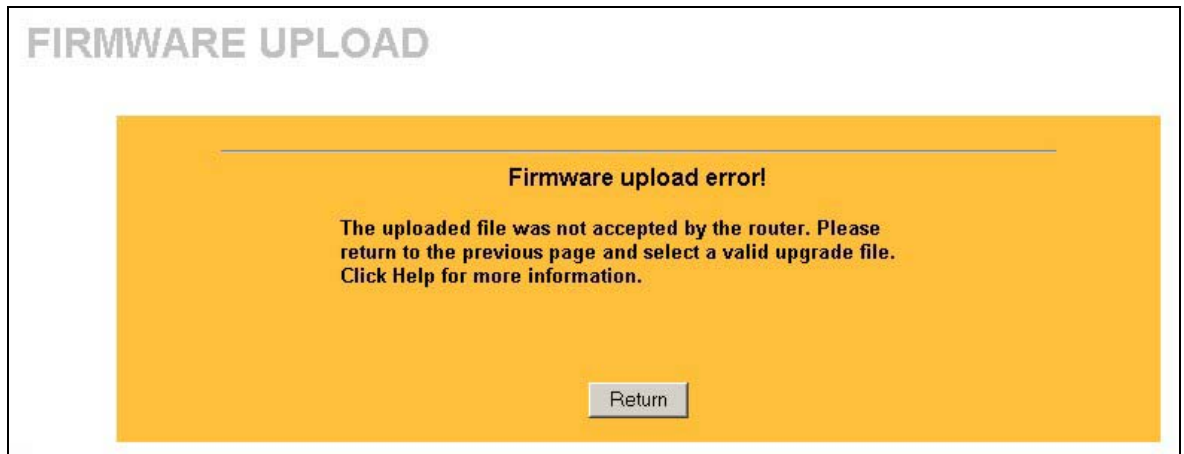


Figure 7-7 Firmware Upload Error

7.5 Configuration Screen

The web configurator uses TFTP to transfer files. See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE** and then **CONFIGURATION**. Information related to backup configuration, restoring configuration and factory defaults appears as shown next.

7.5.1 Backup Configuration

Backup Configuration allows you to backup (save) the current system (ZyAIR) configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly.

Click **Backup** to save your current ZyAIR configuration to your computer.



Figure 7-8 Backup Configuration

7.5.2 Restore Configuration

Restore configuration replaces your ZyAIR's current configuration with a previously saved configuration. Restore files (usually) have a .ROM extension, e.g., "zyair.rom". The system reboots automatically after the file transfer is complete and uses the configured values in the file.

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyAIR. When the Restore Configuration process is complete, the ZyAIR will automatically restart.

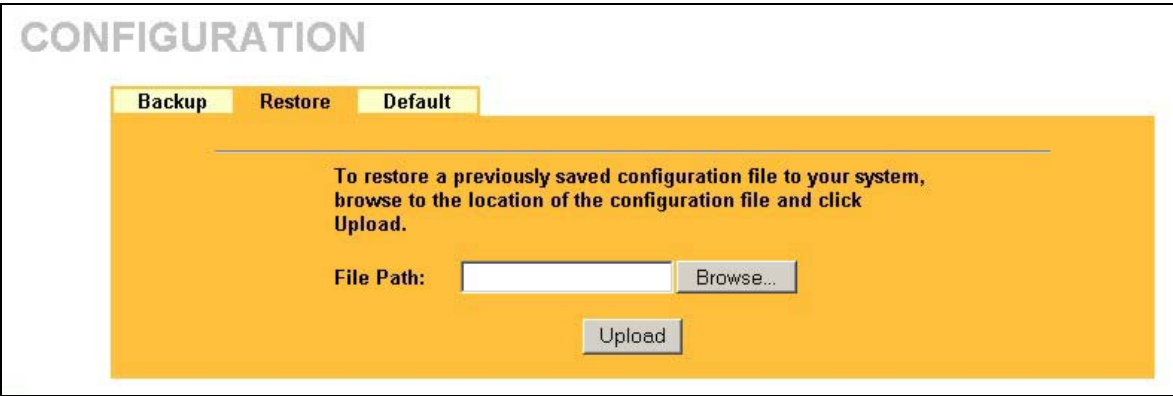


Figure 7-9 Restore Configuration

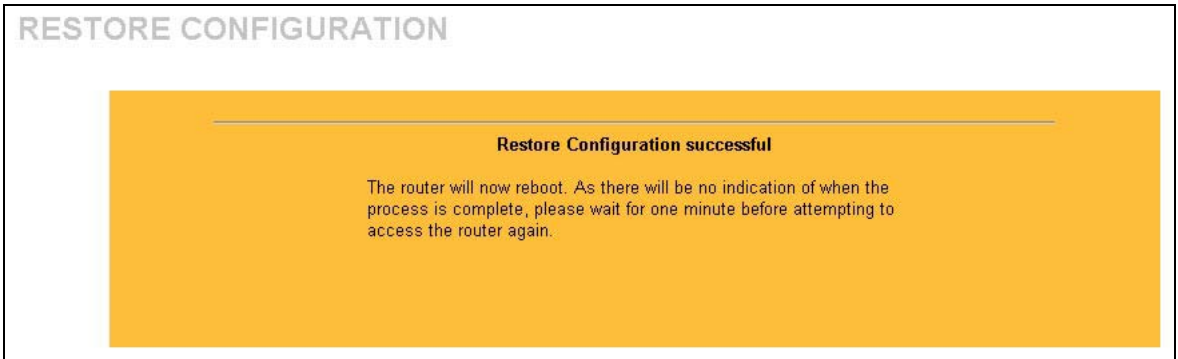
The following table describes the labels in this screen.

Table 7-5 Restore Configuration

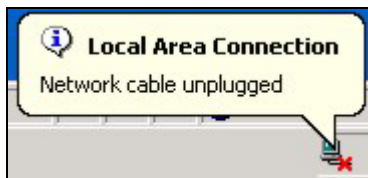
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin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

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

After you see a “configuration upload successful” screen, you must then wait one minute before logging into the ZyAIR again.

**Figure 7-10 Configuration Upload Successful**

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

**Figure 7-11 Network Temporarily Disconnected**

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 ZyAIR IP address (192.168.1.11). See the appendix for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

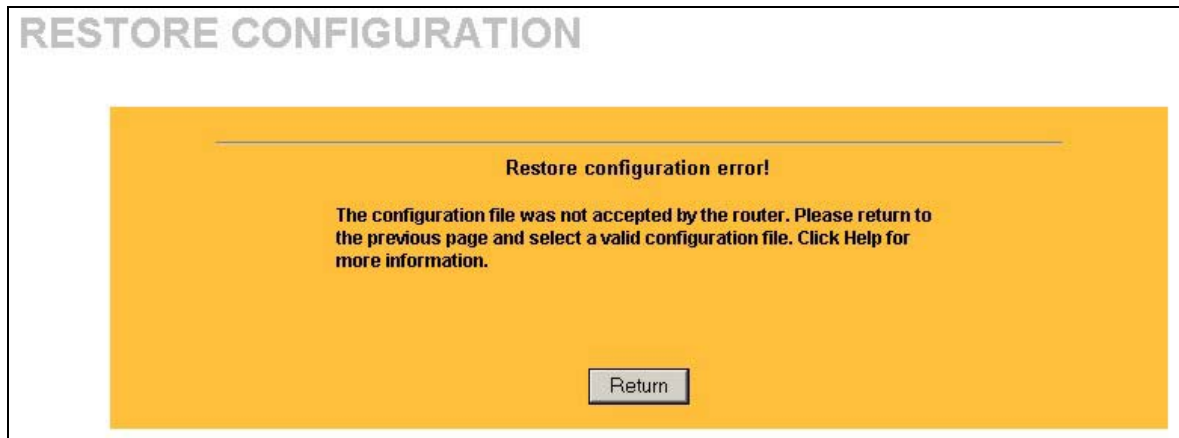


Figure 7-12 Configuration Upload Error

7.5.3 Back to Factory Defaults

Clicking the **Reset** button in this section clears all user-entered configuration information and returns the ZyAIR to its factory defaults as shown on the screen. This will erase all configurations that you have applied.

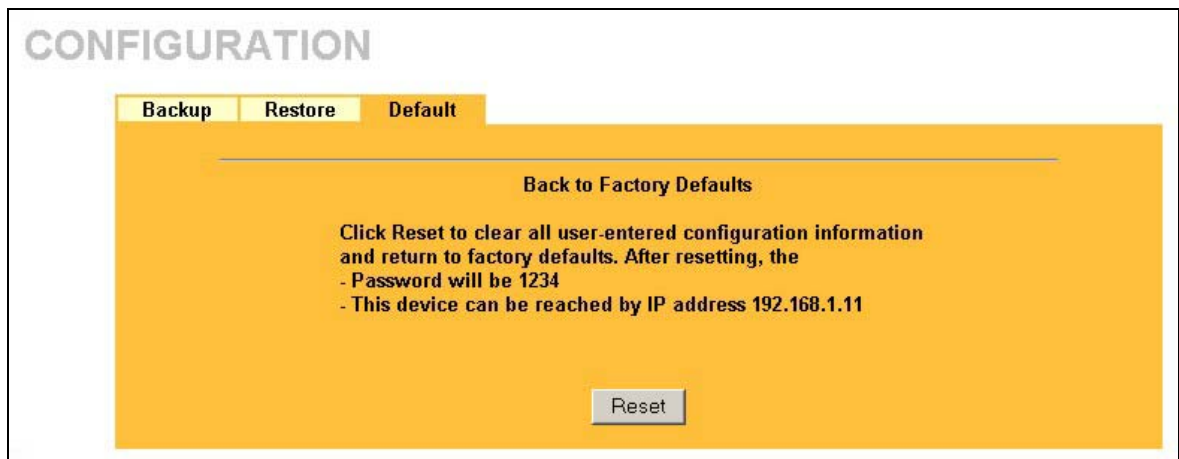


Figure 7-13 Back to Factory Default

The following warning screen will appear.

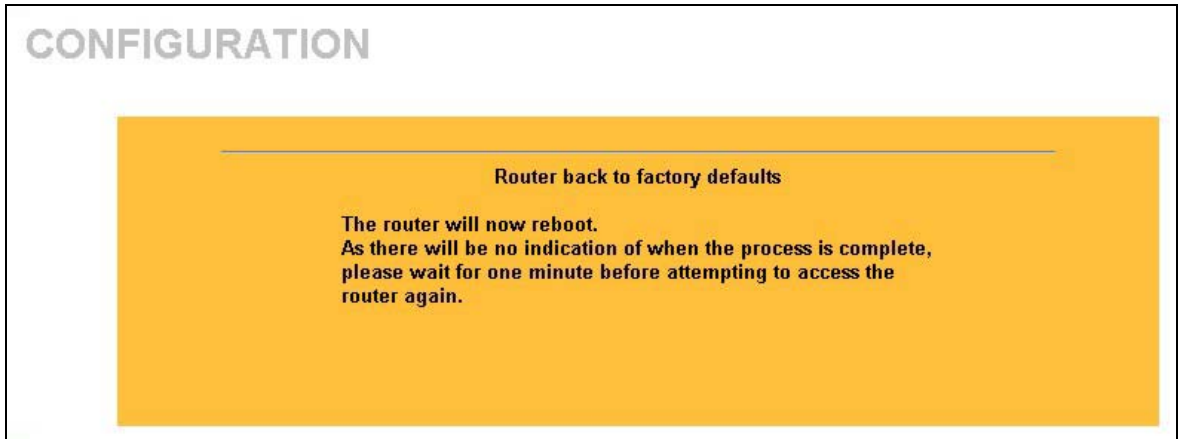


Figure 7-14 Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyAIR. Refer to the *Resetting the ZyAIR* section for more information on the **RESET** button.

Part V:

SMT CONFIGURATION

This part contains SMT (System Management Terminal) configuration and background information for features only configurable by SMT.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 8

Introducing the SMT

This chapter describes how to access the SMT and provides an overview of its menus.

8.1 Connect to your ZyAIR Using Telnet

The following procedure details how to telnet into your ZyAIR.

- Step 1.** In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.11” (the default IP address) and click **OK**.
- Step 2.** For your first login, enter the default password “1234”. As you type the password, the screen displays an asterisk “*” for each character you type.

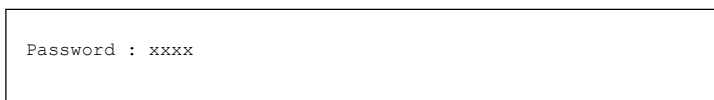


Figure 8-1 Login Screen

- Step 3.** After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyAIR will automatically log you out. You will then have to telnet into the ZyAIR again. You can use the web configurator or the CI commands to change the inactivity time out period.

8.2 Changing the System Password

Change the ZyAIR default password by following the steps shown next.

- Step 1.** From the main menu, enter 23 to display **Menu 23 – System Security**.
- Step 2.** Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.
- Step 3.** Type your existing system password in the **Old Password** field, and press [ENTER].

```
Menu 23.1 - System Security - Change Password

Old Password= ****
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 8-2 Menu 23.1 System Security : Change Password

- Step 4.** Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- Step 5.** Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk “*” for each character you type.

8.3 ZyAIR SMT Menu Overview Example

The following figure gives you an example overview of the various SMT menu screens for your ZyAIR.

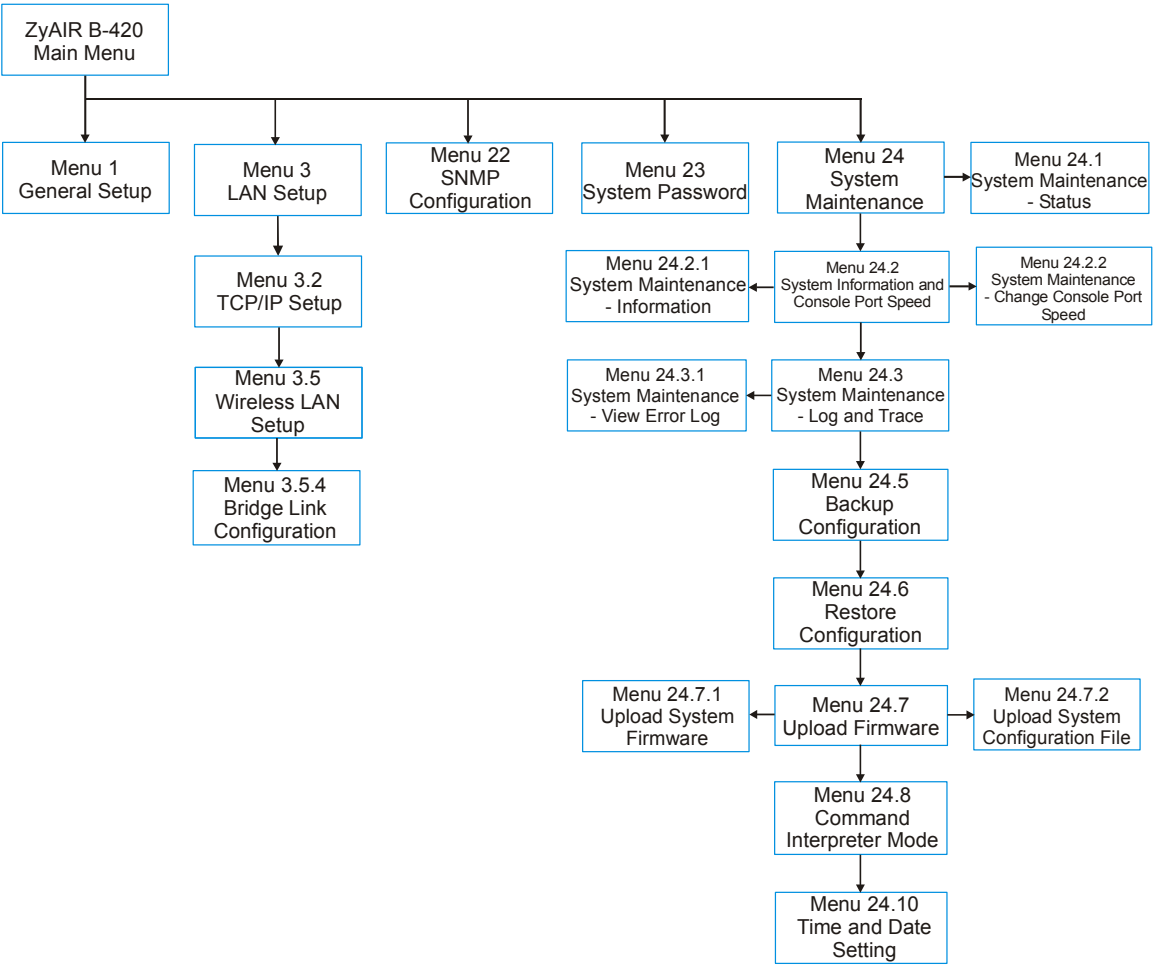


Figure 8-3 ZyAIR B-420 SMT Menu Overview Example

8.4 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyAIR.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 8-1 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of No . Press [SPACE BAR] once to change No to Yes , then press [ENTER] to go to the “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?> or ChangeMe	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with ChangeMe must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

ZyAIR B-420 Main Menu

Getting Started
1. General Setup
3. LAN Setup

Advanced Management
22. SNMP Configuration
23. System Password
24. System Maintenance

Advanced Applications

99. Exit

Enter Menu Selection Number:
```

Figure 8-4 ZyAIR B-420 SMT Main Menu

8.4.1 System Management Terminal Interface Summary

Table 8-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
99	Exit	Use this to exit from SMT and return to a blank screen.

Chapter 9

General Setup

The chapter shows you the information on general setup.

9.1 General Setup

Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. It is recommended you type your computer's "Computer name".

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyAIR via DHCP.

9.1.1 Procedure To Configure Menu 1

Step 1. Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown next.

Menu 1 - General Setup

System Name= B-420
Domain Name=
First System DNS Server= None
 IP Address= N/A
Second System DNS Server= None
 IP Address= N/A
Third System DNS Server= None
 IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

Figure 9-1 Menu 1 General Setup

Step 2. Fill in the required fields. Refer to the following table for more information about these fields.

Table 9-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	B-420
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.	
First/Second/Third System DNS Server	Press [SPACE BAR] to select From DHCP , User Defined or None and press [ENTER].	None
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select User-Defined in the field above.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Chapter 10

LAN Setup

This chapter shows you how to configure the LAN on your ZyAIR..

10.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter 3 to display menu 3.

```
Menu 3 - LAN Setup

2. TCP/IP Setup

5. Wireless LAN Setup

Enter Menu Selection Number:
```

Figure 10-1 Menu 3 LAN Setup

Detailed explanation about the LAN Setup menu is given in the next chapter.

10.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your ZyAIR for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3-LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP Setup**, as shown next:

```
Menu 3.2 - TCP/IP Setup

IP Address Assignment= Static
IP Address= 192.168.1.11
IP Subnet Mask= 255.255.255.0
Gateway IP Address= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
```

Figure 10-2 Menu 3.2 TCP/IP Setup

Follow the instructions in the following table to configure the fields in this menu.

Table 10-1 Menu 3.2 TCP/IP Setup

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic to have the ZyAIR obtain an IP address from a DHCP server. You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again. Select Static to give the ZyAIR a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable.	Static
IP Address	Enter the (LAN) IP address of your ZyAIR in dotted decimal notation	192.168.1.11
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.	255.255.255.0
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your ZyAIR.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

10.3 Wireless LAN Setup

Use menu 3.5 to configure your ZyAIR’s wireless settings. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

```
Menu 3.5 - Wireless LAN Setup

Operating Mode= Infrastructure
ESSID= Any
Channel ID= N/A
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= Disable
    Default Key= N/A
    Key1= N/A
    Key2= N/A
    Key3= N/A
    Key4= N/A
    Authen. Method= N/A
Breathing LED= Yes
Output Power= N/A
Edit Bridge Link Configuration= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 10-3 Menu 3.5 Wireless LAN Setup

The following table describes the fields in this menu.

Table 10-2 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
Operating Mode	Press [SPACE BAR] and select Infrastructure , Ad Hoc or Bridge .	Infrastruct ure
ESSID	Enter the ESSID of the AP or the peer ad-hoc computer to which you want to associate in this field. To associate to an ad-hoc network, you must enter the same ESSID as the peer ad-hoc computer. Enter any to associate to or roam between any infrastructure wireless networks.	Any
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region. This filed is not available if you select Infrastructure in the Operating Mode field.	N/A
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	2432
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	2432

Table 10-2 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
WEP Encryption	Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.	Disable
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyAIR and the wireless stations to communicate.	1
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP in the WEP Encryption field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP in the WEP Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). <div style="border: 1px solid black; padding: 5px; text-align: center;">Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.</div>	0x12345ab cde
Authen. Method	Press [SPACE BAR] to select Auto , Open System Only or Shared Key Only and press [ENTER]. This field is N/A if WEP is not activated. If WEP encryption is activated, the default setting is Auto .	Auto
Breathing LED	Press [SPACE BAR] to select Yes or No and press [ENTER].	
Output Power	Press [SPACE BAR] to select 11dBm , 13dBm , 15dBm or 17dBm and press [ENTER].	17dBm
Edit Bridge Link Configuration	This field is only available when you select Bridge in the Operating Mode field. Press [SPACE BAR] to select Yes or No and press [ENTER].	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

10.3.1 Configuring Bridge Link

Follow the steps below to configure bridge link on your ZyAIR.

Step 1. From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```

Menu 3.5 - Wireless LAN Setup

Operating Mode= Bridge
ESSID= N/A
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= Disable
Default Key= N/A
Key1= N/A
Key2= N/A
Key3= N/A
Key4= N/A
Authen. Method= N/A
Breathing LED= Yes
Output Power= N/A
Edit Bridge Link Configuration= Yes

Press ENTER to Confirm or ESC to Cancel:

```

Figure 10-4 Menu 3.5 Wireless LAN Setup

Step 3. In the **Operating Mode** field, press [SPACE BAR] to select **Bridge** and press [ENTER].

Step 4. Move the cursor to the **Edit Bridge Link Configuration** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.4 – Bridge Link Configuration** displays as shown next.

```

Menu 3.5.4 - Bridge Link Configuration

Active = Yes
-----
Peer Address = 00:a0:c5:55:97:50
-----

Press ENTER to Confirm or ESC to Cancel:

```

Figure 10-5 Menu 3.5.4 Bridge Link Configuration

The following table describes the fields in this menu.

Table 10-3 Menu 3.5.4 Bridge Link Configuration

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select Yes or No and press [ENTER].	Yes
Peer Address	Type the MAC address of peer device in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Chapter 11

SNMP Configuration

This chapter explains SNMP configuration menu 22.

11.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

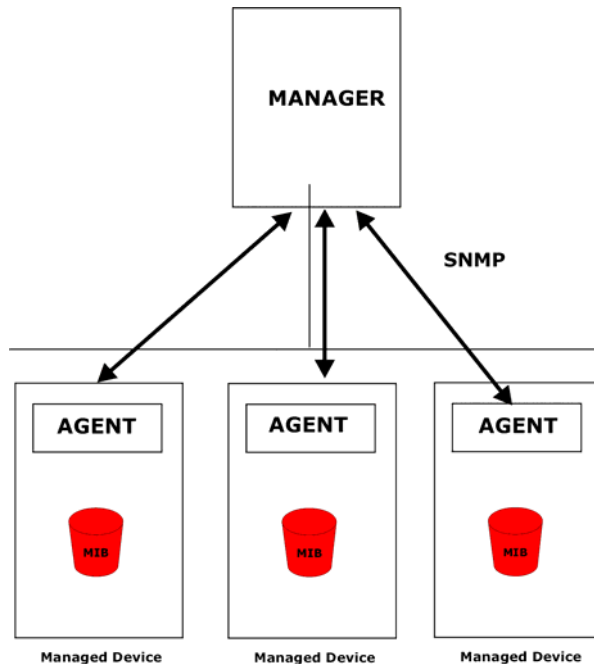


Figure 11-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyAIR). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.2 Supported MIBs

The ZyAIR supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

11.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

```
Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
```

Figure 11-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 11-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the Set Community , which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

11.4 SNMP Traps

The ZyAIR will send traps to the SNMP manager when any one of the following events occurs:

Table 11-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent when the port is up.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent when the port is down.

The following table maps the physical port and encapsulation to the interface type.

Table 11-3 Ports and Interface Types

PHYSICAL PORT/ENCAP	INTERFACE TYPE
LAN port(s)	enet0
Wireless port	enet1
PPPoE encap	pppoe
1483 encap	mpoa
Ethernet encap	enet-encap
PPPoA	ppp

Chapter 12

System Information

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.3.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace

5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode

10. Time and Date Setting

Enter Menu Selection Number:
```

Figure 12-1 Menu 24 System Maintenance

12.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your ZyAIR. Specifically, it gives you information on your Ethernet and Wireless LAN status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 – System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering 9 resets the counters; pressing [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are read-only and meant for diagnostic purposes.

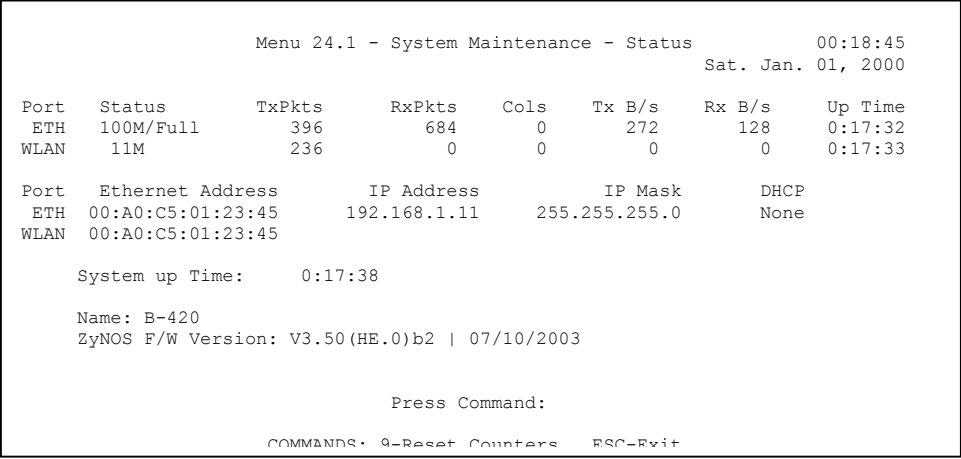


Figure 12-2 Menu 24.1 System Maintenance : Status

The following table describes the fields present in this menu.

Table 12-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Port	This is the port type. Port types are: Ethernet and Wireless
Status	This shows the status of the remote node.
TxPkts	This is the number of transmitted packets to this remote node.
RxPkts	This is the number of received packets from this remote node.
Cols	This is the number of collisions on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
Ethernet Address	This shows the MAC address of the port.
IP Address	This shows the IP address of the network device connected to the port.
IP Mask	This shows the subnet mask of the network device connected to the port.
DHCP	This shows the DHCP setting (None or Client) for the port.

Table 12-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
System Up Time	This is the time the ZyAIR is up and running from the last reboot.

12.2 System Information

To get to the System Information:

- Step 1.** Enter 24 to display **Menu 24 – System Maintenance**.
- Step 2.** Enter 2 to display **Menu 24.2 – System Information and Console Port Speed**.
- Step 3.** From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information and Console Port Speed
      1. System Information
      2. Console Port Speed

Please enter selection:
```

Figure 12-3 Menu 24.2 System Information and Console Port Speed

The ZyAIR has an internal console port for support personnel only. Do not open the ZyAIR as it will void your warranty.

12.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
Menu 24.2.1 - System Maintenance - Information

Name: B-420
Routing: BRIDGE
ZyNOS F/W Version: V3.50(HE.0)b2 | 07/10/2003
Country Code: 255

LAN
  Ethernet Address: 00:A0:C5:55:66:22
  IP Address: 192.168.1.11
  IP Mask: 255.255.255.0
  DHCP: None

Press ESC or RETURN to Exit:
```

Figure 12-4 Menu 24.2.1 System Information : Information

The following table describes the fields in this menu.

Table 12-2 System Maintenance : Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyAIR.
IP Address	This is the IP address of the ZyAIR in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyAIR.
DHCP	This field shows the DHCP setting of the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

12.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyAIR supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

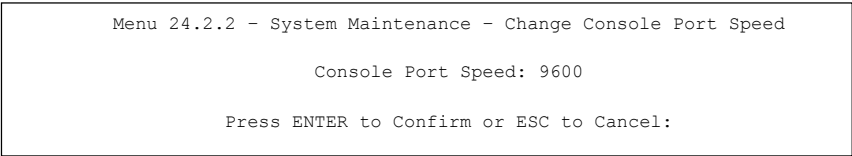


Figure 12-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

After you changed the console port speed on your ZyAIR, you must also make the same change to the console port speed parameter of your communication software.

12.3 Log and Trace

Your ZyAIR provides the error logs and trace records that are stored locally.

12.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

```

Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log

Please enter selection:

```

Figure 12-6 Menu 24.3 System Maintenance : Log and Trace

Step 3. Enter 1 from **Menu 24.3 – System Maintenance – Log and Trace** and press [ENTER] twice to display the error log in the system.

After the ZyAIR finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```

57 Sat Jan 01 14:10:24 2000 PINI INFO Last errorlog repeat 1 Times
58 Sat Jan 01 14:10:24 2000 PINI INFO main: init completed
59 Sat Jan 01 14:10:26 2000 PP05 -WARN SNMP TRAP 3: link up
60 Sat Jan 01 14:10:54 2000 PSSV -WARN Last errorlog repeat 1 Times
61 Sat Jan 01 14:10:54 2000 PSSV -WARN SNMP TRAP 0: cold start
62 Sat Jan 01 14:11:50 2000 PP0a INFO SMT Password pass
63 Sat Jan 01 14:11:50 2000 PINI INFO SMT Session Begin

Clear Error Log (y/n):

```

Figure 12-7 Sample Error and Information Messages

Chapter 13

Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

13.1 Filename Conventions

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

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyAIR.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyAIR only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyAIR and the external filename refers to the filename not on the ZyAIR, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

Table 13-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the ZyAIR. Uploading the rom-0 file replaces the entire ROM file system, including your ZyAIR configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyAIR.

13.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyAIR to the computer, while upload means from your computer to the ZyAIR.

13.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 – System Maintenance** to get the following screen.

```
Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the
procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your
   workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:
```

Figure 13-1 Menu 24.5 Backup Configuration

13.2.2 Using the FTP command from the DOS Prompt

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open” and the IP address of your ZyAIR.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter “root” and your SMT password as requested. The default is 1234.
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 6.** Use “get” to transfer files from the ZyAIR to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter “quit” to exit the FTP prompt.

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK

ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

Figure 13-2 FTP Session Example

The following table describes some of the commands that you may see in third party FTP clients.

Table 13-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	<p>Anonymous.</p> <p>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p>
Transfer Type	<p>Transfer files in either ASCII (plain text format) or in binary mode.</p> <p>The ZyAIR requires binary mode.</p>

Table 13-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

13.2.3 Backup Configuration Using TFTP

The ZyAIR supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

- Step 1.** Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer and “binary” to set binary transfer mode.

13.2.4 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR IP address, “get” transfers the file source on the ZyAIR (rom-0 name of the configuration file on the ZyAIR) to the file destination on the computer and renames it config.rom.

The following table describes some of the fields that you may see in third party TFTP clients.

Table 13-3 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.11 is the ZyAIR's default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyAIR and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyAIR. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

13.3 Restore Configuration

Menu 24.6 – System Maintenance – Restore Configuration allows you to restore the configuration via FTP or TFTP to your ZyAIR. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyAIR restarts automatically after the file transfer is complete.

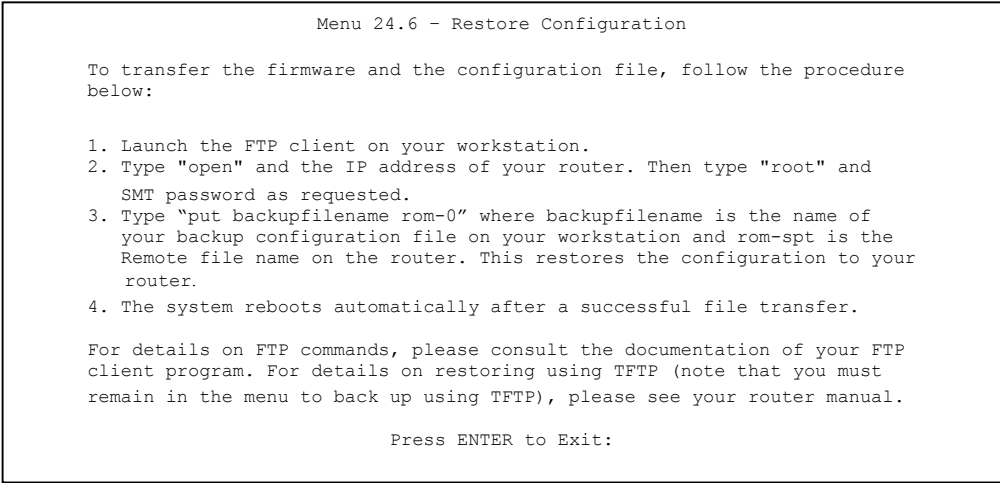


Figure 13-3 Menu 24.6 Restore Configuration

13.4 Uploading Firmware and Configuration Files

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file.

WARNING!
**PLEASE WAIT A FEW MINUTES FOR THE ZYAIR TO RESTART AFTER FIRMWARE
OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS
MAY PERMANENTLY DAMAGE YOUR ZYAIR.**

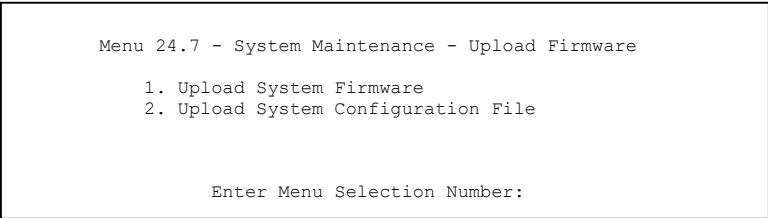


Figure 13-4 Menu 24.7 System Maintenance : Upload Firmware

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

13.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyAIR, you will see the following screens for uploading firmware and the configuration file using FTP.

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 13-5 Menu 24.7.1 System Maintenance : Upload System Firmware

13.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

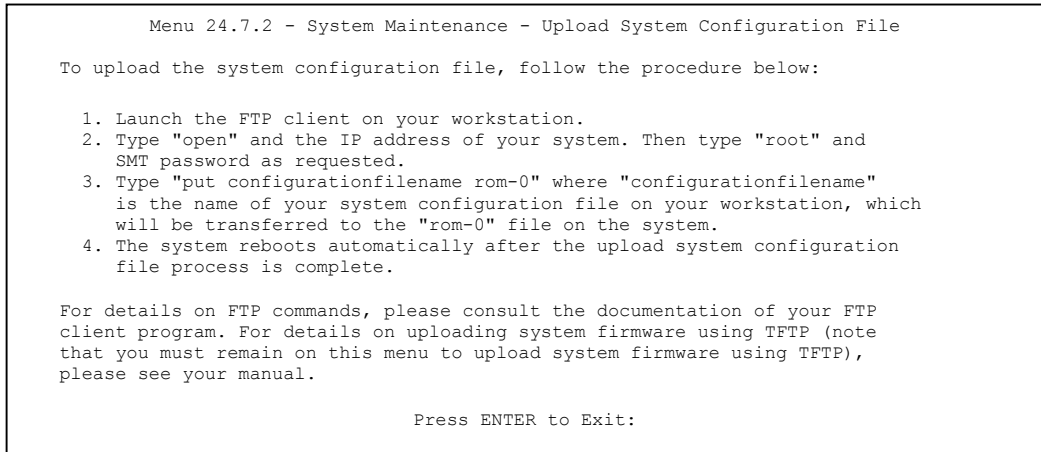


Figure 13-6 Menu 24.7.2 System Maintenance : Upload System Configuration File

To transfer the firmware and the configuration file, follow these examples:

13.4.3 Using the FTP command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open" and the IP address of your ZyAIR.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter "root" and your SMT password as requested. The default is 1234.
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Use "put" to transfer files from the computer to the ZyAIR, e.g., put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the ZyAIR and renames it "ras". Similarly "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the ZyAIR and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the ZyAIR to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter "quit" to exit the FTP prompt.

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 13-7 FTP Session Example

More commands that you may find in third party FTP clients, are listed earlier in this chapter.

13.4.4 TFTP File Upload

The ZyAIR also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

- Step 1.** Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer, “put” the other way around, and “binary” to set binary transfer mode.

13.4.5 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyAIR).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

Chapter 14

System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

14.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

```

Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace

5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode

10. Time and Date Setting

Enter Menu Selection Number:

```

Figure 14-1 Menu 24 System Maintenance

```

Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
B-420> ?
Valid commands are:
sys                exit                device                ether
config            wlan                ip                    ppp
bridge            hdap
B-420>

```

Figure 14-2 Valid CI Commands

14.2 Time and Date Setting

The ZyAIR keeps track of the time and date. There is also a software mechanism to set the time manually. Menu 24.10 allows you to update the time and date settings of your ZyAIR. The real time is then displayed in the ZyAIR error logs and firewall logs.

- Step 1.** Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.
- Step 2.** Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyAIR as shown in the following screen.

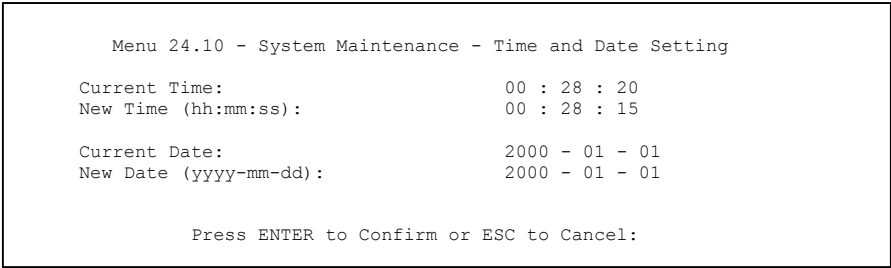


Figure 14-3 Menu 24.10 System Maintenance : Time and Date Setting

The following table describes the fields in this menu.

Table 14-1 Menu 24.10 System Maintenance : Time and Date Setting

FIELD	DESCRIPTION
Current Time	This field displays an updated time only when you re-enter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel” to save your configuration, or press [ESC] to cancel.	

Part VI:

APPENDICES

This part provides troubleshooting and background information about setting up your computer's IP address, wireless LAN, antenna selection and IP subnetting. It also provides information on the antenna, PoE, command interpreter interface, logs and power adaptor specifications.

Appendix A

Troubleshooting

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

Problems Starting Up the ZyAIR

Chart A-1 Troubleshooting the Start-Up of Your ZyAIR

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 ZyAIR reboots automatically sometimes.	The supplied power to the ZyAIR is too low. Check that the ZyAIR is receiving enough power. Make sure the power source is working properly.

Problems with the Password

Chart A-2 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the RESET button on the top panel of the ZyAIR to restore the factory default configuration file (hold this button in for about 10 seconds or until the link LED turns red). This will restore all of the factory defaults including the password.

Problems Communicating with Other Computers

Chart A-3 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The ZyAIR computer cannot communicate with the other computer.	Make sure you are connected to the network.
A. Infrastructure	<p>Make sure that the AP and the associated computers are turned on and working properly.</p> <p>Verify you select the right operating mode in the Wireless screen or menu 3.5.</p> <p>Make sure the ZyAIR and the associated AP use the same SSID.</p> <p>Configure the AP to use another radio channel if interference is high.</p> <p>Make sure that the computer and the AP share the same WEP key and authentication mode. Verify the settings in the Wireless screen.</p>
B. Ad-Hoc	<p>Verify that the peer computer(s) is turned on.</p> <p>Make sure you select the right operating mode in the Wireless screen or menu 3.5.</p> <p>Make sure the ZyAIR and the peer computer(s) are using the same SSID and channel.</p> <p>Configure the wireless stations to use another radio channel if interference is high.</p> <p>Make sure that the ZyAIR and the AP share the same WEP key and authentication mode. Verify the settings in the Wireless screen.</p>
C. Bridge	<p>Verify that the peer computer(s) is turned on and support wireless bridging.</p> <p>Verify you select the right operating mode in the Wireless screen or menu 3.5 and enter the right MAC address of peer device.</p> <p>Configure the wireless stations to use another radio channel if interference is high.</p> <p>Make sure that the ZyAIR and the AP share the same WEP key and authentication mode. Verify the settings in the Wireless screen.</p>

Appendix B

Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See the Command Interpreter appendix for information on the command structure.

Chart B-1 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
<code>sys pwderrrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrrtm 0</code>	This command turns off the password's protection from brute-force guessing.
<code>sys pwderrrtm N</code>	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

`sys pwderrrtm 5` This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

By default, the brute-force password guessing protection is turned ON with a 3-minute wait time.

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.

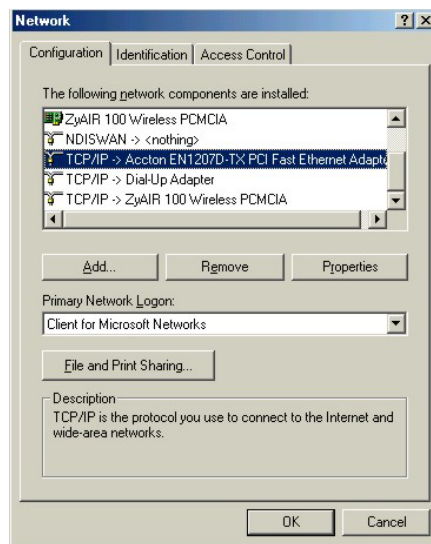
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

Windows 95/98/Me

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



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:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

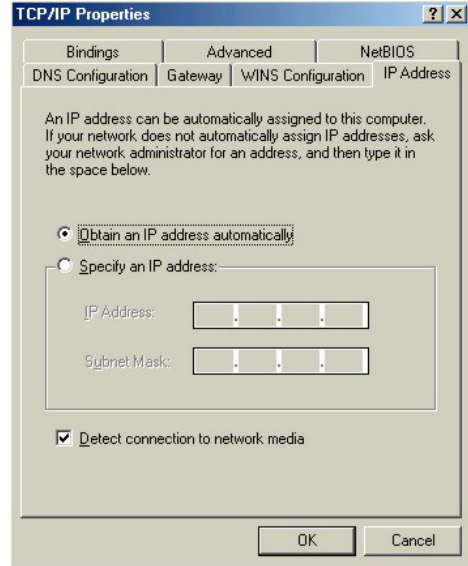
- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

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

1. Click the **IP Address** tab.

-If your IP address is dynamic, select **Obtain an IP address automatically**.

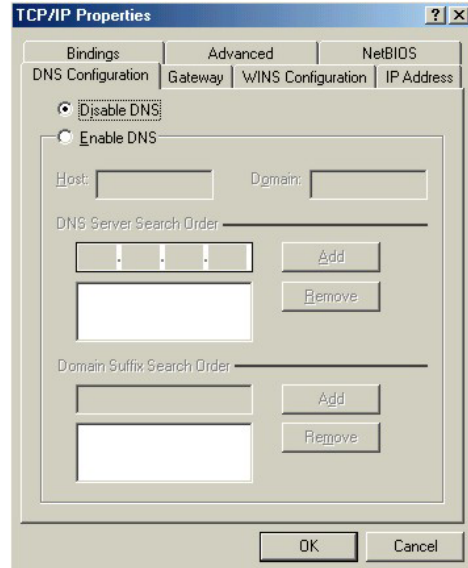
-If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



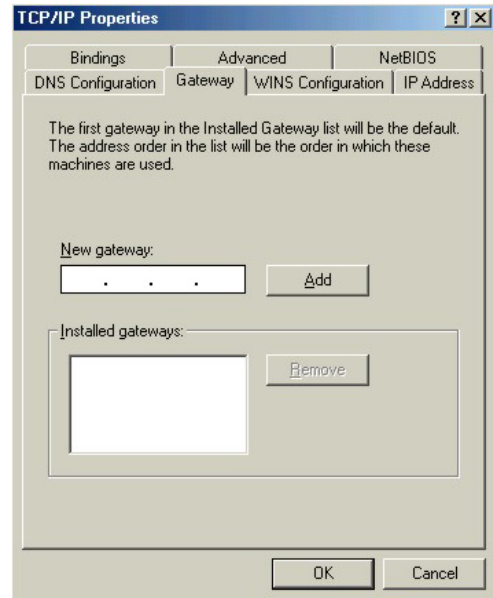
2. Click the **DNS Configuration** tab.

-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).



3. 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**.



4. Click **OK** to save and close the **TCP/IP Properties** window.
5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
6. Turn on your ZyAIR and restart your computer when prompted.

Verifying Your Computer's IP Address

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

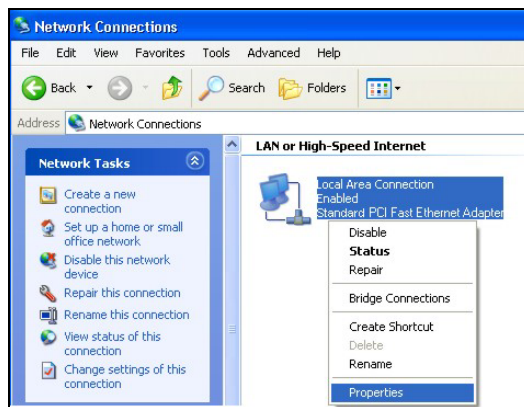
1. For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



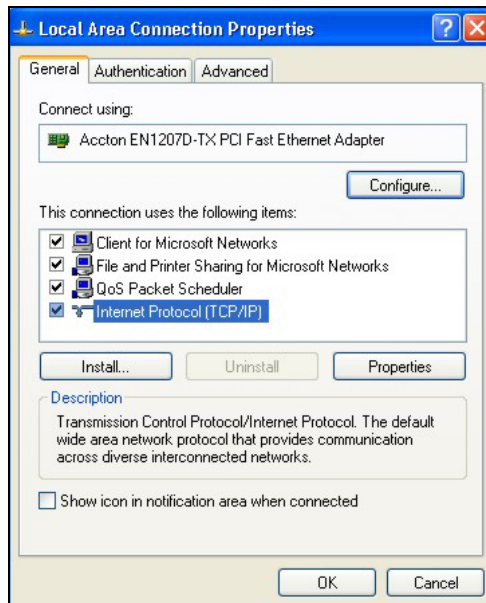
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial Connections**.



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



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

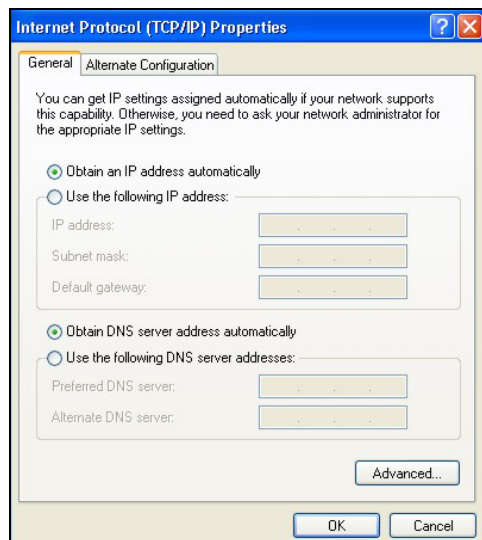


5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

-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**.



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.

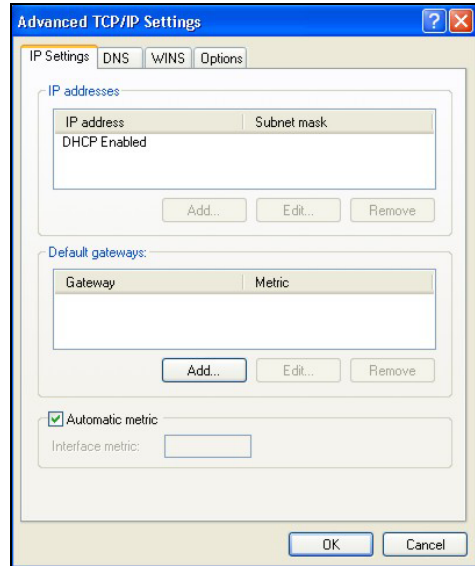
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-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.

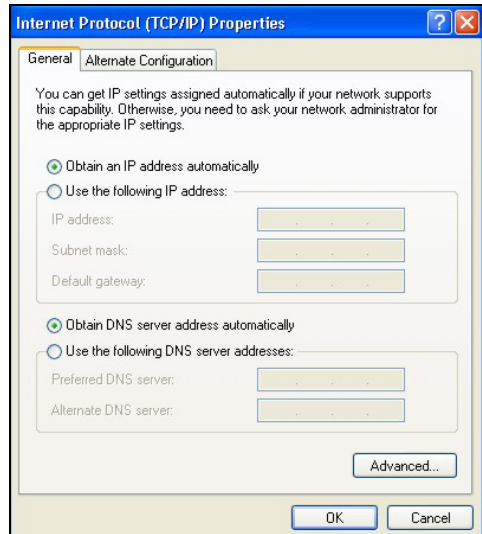


7. In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

-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.



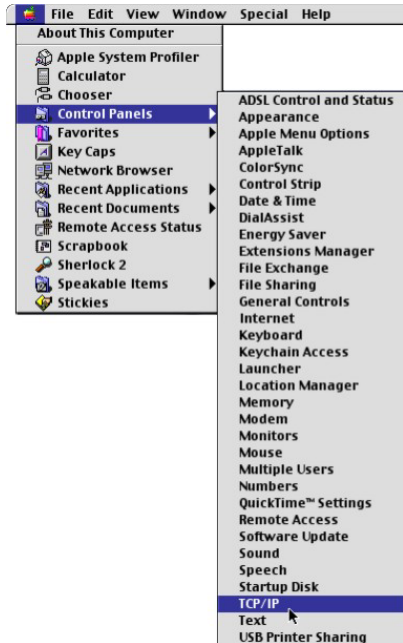
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

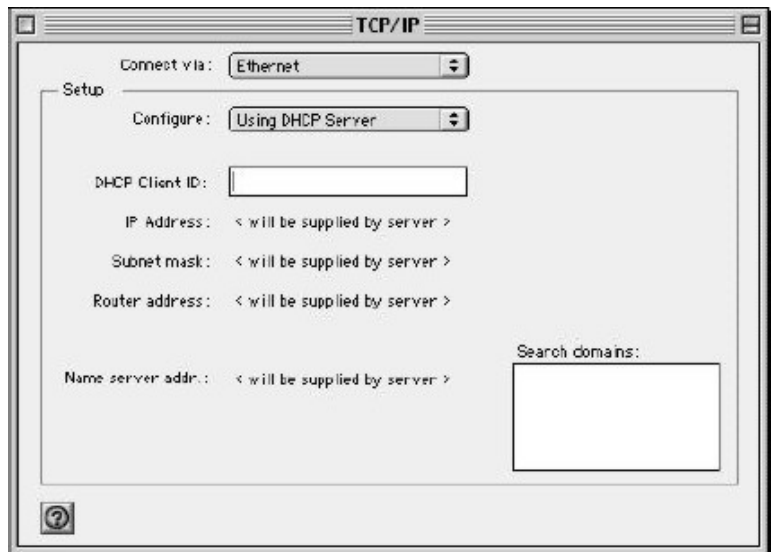
1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



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

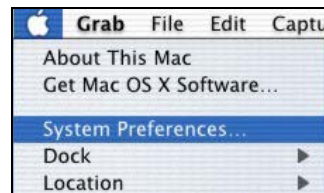
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your ZyAIR in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

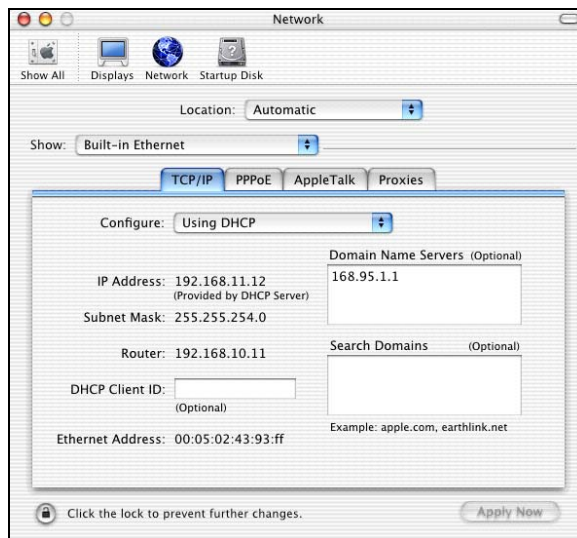
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

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



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.
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 ZyAIR in the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

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

Appendix D

Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence

Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

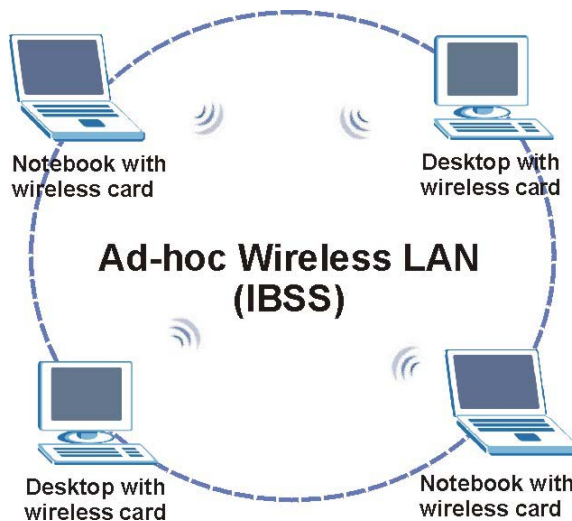


Diagram D-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access

points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

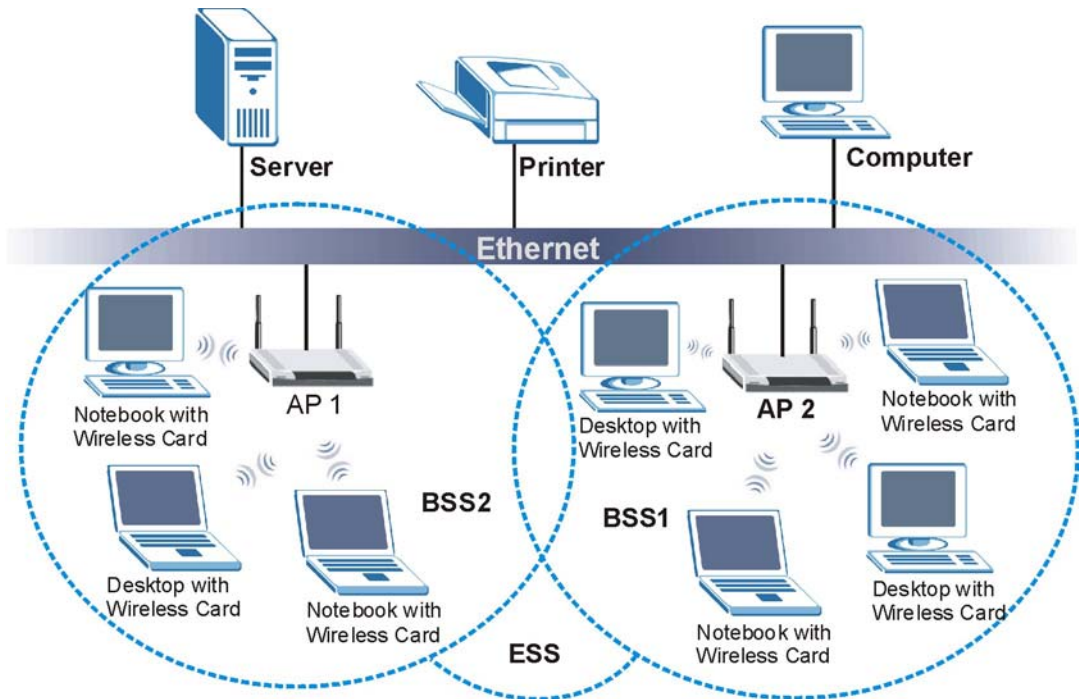


Diagram D-2 ESS Provides Campus-Wide Coverage

Appendix E

Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

➤ Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

➤ Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

➤ Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room

environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Connector Type

The ZyAIR is equipped with a reverse polarity SMA jack, so it will work with any 2.4GHz wireless antenna with a reverse polarity SMA plug.

Appendix F

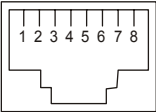
Power over Ethernet Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.

Chart F-1 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Chart F-2 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

Appendix G

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Chart G-1 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.
- A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24}-2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Chart G-2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Chart G-3 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous

sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Chart G-4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Chart G-5 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	0 0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	1 0000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart G-6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	1 0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	1 0000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.255		Highest Host ID: 192.168.1.254

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned

to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Chart G-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.63		Highest Host ID: 192.168.1.62

Chart G-8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64		Lowest Host ID: 192.168.1.65
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart G-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000

Chart G-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Chart G-10 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart G-11 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class “C” subnet planning.

Chart G-12 Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see *Chart J-1*) available for subnetting.

The following table is a summary for class “B” subnet planning.

Chart G-13 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254

Chart G-13 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix H

Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets `<>`.

The optional fields in a command are enclosed in square brackets `[]`.

The `|` symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix I

Log Descriptions

Chart I-1 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
SMT Login Successfully	Someone has logged on to the ZyAIR's SMT interface.
SMT Login Fail	Someone has failed to log on to the ZyAIR 's SMT interface.
WEB Login Successfully	Someone has logged on to the ZyAIR 's web configurator interface.
WEB Login Fail	Someone has failed to log on to the ZyAIR s web configurator interface.
TELNET Login Successfully	Someone has logged on to the ZyAIR via telnet.
TELNET Login Fail	Someone has failed to log on to the ZyAIR via telnet.
FTP Login Successfully	Someone has logged on to the ZyAIR via FTP.
FTP Login Fail	Someone has failed to log on to the ZyAIR via FTP.

Chart I-2 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable

Chart I-2 ICMP Notes

TYPE	CODE	DESCRIPTION
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message

Chart I-2 ICMP Notes

TYPE	CODE	DESCRIPTION
16		Information Reply
	0	Information reply message

Chart I-3 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

Log Commands

Go to the command interpreter interface (the *Command Interpreter Appendix* explains how to access and use the commands).

Configuring What You Want the ZyAIR to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyAIR is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Chart I-4 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyAIR (you must do this in order to record logs).

Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyAIR's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyAIR log category.

Use the `sys logs clear` command to erase all of the ZyAIR's logs.

Log Command Example

This example shows how to set the ZyAIR to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access
```

#	.time	source	destination
notes			
	message		
0	11/11/2002 15:10:12	172.22.3.80:137	172.22.255.255:137
	ACCESS BLOCK		

Appendix J

Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	AD48-1201200DUY
Input Power	AC120Volts/60Hz/0.25A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1950, CSA C22.2 No.234-M90)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	DV-121A2-5720
Input Power	AC120Volts/60Hz/27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223-M91)
EUROPEAN PLUG STANDARDS	
AC Power Adaptor Model	AD-1201200DV
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adaptor Model	AD-1201200DK
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950, BS7002)

JAPAN PLUG STANDARDS	
AC Power Adaptor Model	JOD-48-1124
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)
AUSTRALIA AND NEW ZEALAND PLUG STANDARDS	
AC Power Adaptor Model	AD-1201200DS or AD-121200DS
Input Power	AC240Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	NATA (AS 3260)

Appendix K

Index

A

Ad-hoc Configuration.....	D-2
Alternative Subnet Mask Notation	F-3
Antenna	
Directional	E-2
Omni-directional	E-1
Types.....	E-1
Antenna gain	E-1
Applications	1-4
auto-negotiation.....	1-1

B

backup	13-2
Backup.....	7-7
Basic Service Set.....	D-2
BSS.....	<i>See</i> Basic Service Set

C

Channel ID	4-10, 10-3
Classes of IP Addresses.....	F-1
Collision	12-2
Command Interpreter	14-1
Communication Problem	
Ad-hoc(IBSS)	A-2
Infrastructure.....	A-2
Community.....	11-2
Computer's IP Address	C-1
Copyright.....	ii
CPU Load.....	12-3
Customer Support.....	v

D

Data encryption	4-1
Default.....	7-10
DHCP	12-4

Diagnostic Tools.....	12-1
Direct Sequence Spread Spectrum	D-2
Distribution System	D-3
DS	<i>See</i> Distribution System
DSSS	<i>See</i> Direct Sequence Spread Spectrum

E

Error Log	12-5
Error/Information Messages	
Sample.....	12-5
ESS	<i>See</i> Extended Service Set
ESS ID	4-1
Extended Service Set	D-3

F

FCC	iii
FHSS	<i>See</i> Frequency-Hopping Spread Spectrum
Filename Conventions	13-1
Firmware File	
<i>Maintenance</i>	7-5, 7-7
Fragment Threshold.....	10-3
Fragmentation Threshold.....	4-3
Frequency-Hopping Spread Spectrum	D-2
FTP File Transfer.....	13-7

G

General Setup	3-1, 9-1
---------------------	----------

H

Hidden Menus.....	8-4
Host	3-3
Host IDs.....	F-1

I

IBSS.....	<i>See</i> Independent Basic Service Set
-----------	--

IEEE 802.11D-1
Independent Basic Service Set..... D-2, 4-8, 7-4
Infrastructure ConfigurationD-3
Internet access.....10-1
Internet Security Gateway1-1
IP Address5-1, 5-2, 10-2, 12-4
IP Addressing F-1
IP Classes..... F-1

L

Link type.....12-2
Log and Trace.....12-5
Log Descriptions.....H-1
Logs.....6-1

M

Main Menu8-4
Management Information Base (MIB).....11-2

N

Network Management1-3

P

Packets.....12-2
Password.....3-2, 8-1, 11-2
Private IP Address5-2

Q

Quick Start Guide xiii, 2-1

R

RAS12-4
Rate
 Receiving12-2
 Transmission12-2
Related Documentation xiii
Remote Node12-2
Required fields.....8-4
Restore.....7-8

Restore Configuration 13-5
RF signals D-2
Roaming.....4-6
 Example.....4-6
RTS Threshold4-1, 10-3

S

Service iv
SMT Menu Overview 8-2
SNMP
 Community 11-3
 Configuration.....11-2
 Get 11-2
 GetNext 11-2
 Manager.....11-2
 MIBs 11-2
 Set.....11-2
 Trap 11-2
 Traps.....11-3, 11-4
 Trusted Host 11-3
SSID.....4-7, 4-10, 10-3
Subnet Mask.....5-1, 10-2, 12-4
Subnet MasksF-2
SubnettingF-3
Supporting Disk xiii
System
 Console Port Speed 12-4
 Log and Trace 12-5
 System Information 12-3
 System Status.....12-1
 Time and Date 14-2
System Information.....12-3
System Information & Diagnosis 12-1
System Maintenance 12-1,
 12-3, 13-2, 13-4, 13-5, 13-6, 13-9, 14-1, 14-2
System Management Terminal.....8-4
System Name 3-2
System Status 12-2

T

TFTP File Transfer..... 13-9
Time and Date Setting.....14-2
Trace Records12-5
Troubleshooting

Accessing ZyAIR	A-2
Password	A-1
Start-Up.....	A-1
 U	
Upload Firmware.....	13-6
 V	
Valid CI Commands	14-1
 W	
Web Configurator.....	2-1, 2-2
 Z	
WEP.....	4-1
WEP Encryption	4-8, 4-13, 10-4
Wireless LAN	D-1, 10-2
Benefits	D-1
Wireless LAN Setup	10-2
WLAN	<i>See Wireless LAN</i>
 ZyNOS..... 13-1, 13-2	
ZyNOS F/W Version	13-1
ZyXEL Limited Warranty Note	iv