ZyAIR 100

Wireless PC Card

User's Guide

Version 1.0

September, 2000

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

ZyAIR 100

Wireless PC Card

COPYRIGHT

DISCLAIMER

TRADEMARKS

Federal Communications Commission (FCC) Interference Statement (No. M4Y-XI-300)

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

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

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

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

NOTICE 1

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

NOTICE 2

Shielded RS-232C cables are required to be used to ensure compliance with FCC Part 15, and it is the responsibility of the user to provide and use shielded RS-232C cables.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

NOTE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

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; refer to the separate Warranty Card 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 (USA and territories only). If the customer desires some other return destination beyond the U.S. borders, the customer shall bear the cost of the return shipment. This warranty gives you specific legal rights and you may also have other rights that vary from state to state.

Online Registration

Do not forget to register your Prestige (fast, easy online registration at www.zyxel.com for free future product updates and information.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Method / Region	EMAIL – Support / EMAIL – Sales	Telephone / Fax	Web Site / FTP Site	Regular Mail
Worldwide	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	support@europe.zyxel.com		www.europe.zyxel.com	
	sales@zyxel.com.tw	+886-3-578-2439	ftp.europe.zyxel.com	
North America	support@zyxel.com	+1-714-632-0882 800-255-4101	www.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.zyxel.com	
Scandinavia	support@zyxel.dk	+45-3955-0700	www.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	sales@zyxel.dk	+45-3955-0707	ftp.zyxel.dk	
Austria	support@zyxel.at	+43-1-4948677-0 0810-1-ZyXEL 0810-1-99935	www.zyxel.at	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria.
	sales@zyxel.at	+43-1-4948678	ftp.zyxel.at NOTE: for Austrian users with *.at domain only!	
Germany	support@zyxel.de	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	www.zyxel.de	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuerselen, Germany.
	sales@zyxel.de	+49-2405-6909-99	ftp.europe.zyxel.com	

Table of Contents

List of Figures

List of Tables

Preface

About Your ZyAIR 100

Congratulations on your purchase of the ZyAIR 100 Wireless PC Card.

✎ Online Registration

Do not forget to register your ZyAIR 100 (fast, easy online registration at www.zyxel.com for free future product updates and information.

With the built-in Access Point and the powerful routing feature of the Prestige series models, you can place a wireless Prestige anywhere on a local network to create a wireless infrastructure for real time database accessing, file sharing, email sending/retrieving, printer sharing, and fast Internet accessing. A mobile investment saves you office construction cost, maintenance effort, and it's easy to extend the connection nodes by just adding a ZyAIR 100 on a laptop. A mobile office can highly increase the office efficiency. It is designed for:

❑ Home offices and small businesses with Cable, DSL and wireless modem as Internet access media.
❑ Wireless LAN connectivity allows you to work anywhere in the coverage area.
❑ Multiple office/department connections via access devices.
❑ E-commerce/EDI applications.

Your ZyAIR 100 is easy to install and to configure.

About This User's Manual

This manual is designed to guide you through the hardware and software installation of your ZyAIR 100 for its various applications.

Structure of this Manual

This manual is structured as follows:

Part I.   *Getting Started* (Chapters 1 to 3) is structured as a step-by-step guide to help you connect, install and setup your ZyAIR 100 to operate on your notebook computer.

Part II.   *Advanced Management and Troubleshooting* (Chapters 4 and 5) provides information on Configuring Parameters, System Diagnosis and solving common problems as well as some Appendices, a Glossary and an Index.

Regardless of your particular application, it is important that you follow the steps outlined in *Chapters 2* and *3* to install your ZyAIR 100. You can then refer to the appropriate chapters of the manual, depending on your applications.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.
- A single keystroke is in Arial font and enclosed in square brackets, for instance, [Enter] means the Enter, or carriage return key; [Esc] means the Escape key.
- 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.

Part I:

GETTING STARTED

Chapters 1 to 3 are structured as a step-by-step guide to help you connect, install and setup your ZyAIR 100 to operate on your notebook computer.

Chapter 1
Getting to Know Your ZyAIR 100

This chapter introduces the main features and applications of the ZyAIR 100.

1.1   The ZyAIR 100 Wireless PC Card

The ZyAIR 100 is an 11 Mbps IEEE 802.11(b) Wireless PC Card and standard PCMCIA adapter that fits into any standard PCMCIA Type II slot on a notebook computer. Its 11 Mbps data rate gives equivalent Ethernet speed to access corporate networks or the Internet in a wireless environment. When installed, the ZyAIR 100 is able to communicate with any 802.11 and 802.11b-compliant product, allowing you to work anywhere in the coverage area, enjoying its convenience and mobility.

1.2   Features of the ZyAIR 100

The following are the essential features of the ZyAIR 100.

- Supports 1, 2, 5.5 and 11 Mbps Data Rate

- Working Range up to 800 ft. in an Open Environment

- Supports Point-to-Point and Point-to-Multi-point Access

- Seamless Connectivity to Wired Ethernet and PC Network LAN's Helps to Augment Existing Networks Quickly and Easily

- Direct Sequence Spread Spectrum (DSSS) Technology Provides Robust, Interference-Resistant and Secure Wireless Connection

- Wireless Connectivity Minus the Cost of Cabling

- Supports a Wide Range of LAN NOS (Network Operating System), e.g., Windows® 95/98/NT, DOS and Windows® 2000

- Supports Plug and Play

- Ease of Installation

- Greater Flexibility and Mobility to Locate or Move Networked PCs

1.3 **Applications for ZyAIR 100**

ZyAIR 100 offers a fast, reliable and cost-effective solution for wireless client access to the network with applications such as these:

- Remote Access to Corporate Network Information

  For accessing emails, file transfer and terminal emulation.

- Difficult to Wire Environments

  For use in historical or old buildings, asbestos installations and open areas where wiring is difficult to deploy.

- Frequently Changing Environments

  For retailers, manufacturers and those who frequently rearrange the workplace and change location.

- Temporary LANs for Special Projects or During Peak Time

  For trade shows, exhibitions and construction sites where a temporary network is required. For retailers, airline and shipping companies who need additional workstations during peak periods. For auditors requiring workgroups at customer sites.

- Access to Database for Mobile Users

  Doctors, nurses, retailers who needs to access their database while being mobile in the hospital, retail store or office campus.

- SOHO (Small Office and Home Office) Users

  SOHO users who need easy and quick installation of a small computer network.

- High Security Connection

  The secure wireless network can be installed quickly and provide flexibility.

Chapter 2
Hardware Installation

This chapter shows you how to properly install the hardware.

2.1   System Requirements

In order to use the ZyAIR 100, your computer must be equipped with the following:

- Available PCMCIA Type II slot and a PCMCIA card and socket services that is Revision 2.1-compliant to the PCMCIA specification (or higher)

- Windows® 95 (OSR2) / 98 Operating System (with the Windows® installation CD-ROM disc readily available during actual installation)

- 500 Kbytes free hard disk space (minimum) for driver and utility program installation.

2.2   Installing the ZyAIR 100

This section outlines how to install the ZyAIR 100. Please also see the *Appendices* for important safety instructions on handling the ZyAIR 100.

Step 1.   Find an available Type II or Type III PCMCIA slot in your notebook computer.

Step 2.   With the ZyAIR 100 adapter's 68-pin connector facing the PCMCIA slot and its label side facing up, slide the ZyAIR 100 completely into the PCMCIA slot.

> **NOTE: Upon inserting the ZyAIR 100, Windows® would automatically detect the new hardware and prompt you to install the driver needed. Go to the next chapter for more instructions on installing the driver.**

Figure 2-1 Inserting the ZyAIR 100 into the Notebook Computer

NOTE: The PCMCIA slot allows "hot swapping" of PCMCIA adapter, allowing you to insert or remove the ZyAIR 100 from the slot whenever you like, even when the power to your computer is on. However, you are advised to always disable the ZyAIR 100 prior to removing the card from the PC Card slot. This allows the Windows® operating system to log off from the network server. Disable the driver properly and disconnect power to the PC Card slot.

Chapter 3
Software Installation

This chapter shows you how to install the driver for using the ZyAIR 100 on the Windows® 95 (OSR2) / 98 / NT 4.0 / 2000 Operating Systems.

3.1 Setting Up the ZyAIR 100 for Windows® 95 (OSR2) / 98

NOTE: Before starting driver installation, make sure that the ZyAIR 100 has been inserted into a standard type II PCMCIA slot on your notebook computer.

Step 1. Upon inserting the ZyAIR 100 into your notebook computer, Windows® would automatically detect the new hardware and prompt you to install the driver needed. When the *Add New Hardware Wizard* dialog box appears, click on the *Next* button.

Step 2. Select *Search for the best driver for your device* and click on the *Next* button.

Step 3. Insert the *ZyAIR Support* CD-ROM disc into the CD-ROM drive and select the location where the corresponding driver is located, then click on the *Next* button.

Step 4. Windows® 95 (OSR2) / 98 will locate *ZyAIR 100 PCMCIA*, then click on the *Next* button.

Step 5. Click on the *Next* button to install the necessary driver to support your new ZyAIR 100.

Step 6. Set the parameters for the ZyAIR 100, then click on the *OK* button (refer to the next chapter for the definition of each parameter).
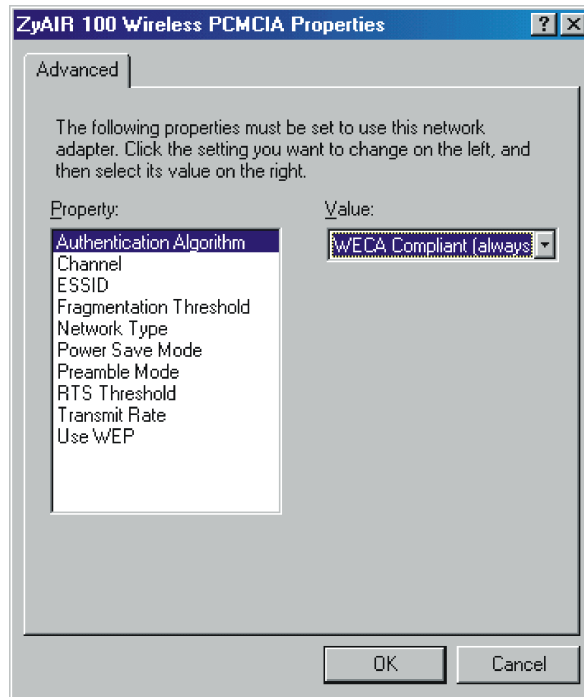
Step 7. Click on the *Finish* button to complete the driver installation.
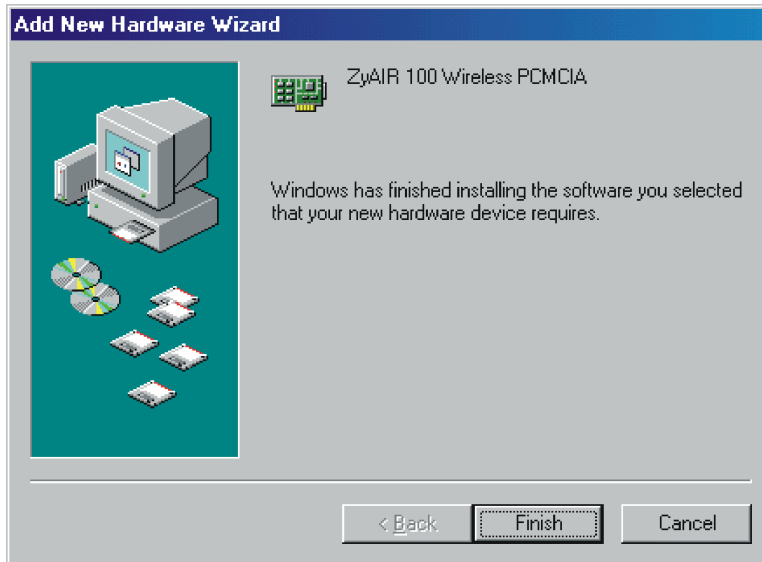
Step 8.   Click on the *Yes* button when you are prompted to restart your computer.

Step 9.   Click on the *Start* button (Windows® taskbar), then *Control Panel/System/Device Manager.* Check the item *Network Adapters* to see if any error icon appears. If no, that means your ZyAIR 100 is working well with your Windows® 95 (OSR2) / 98 operating system.
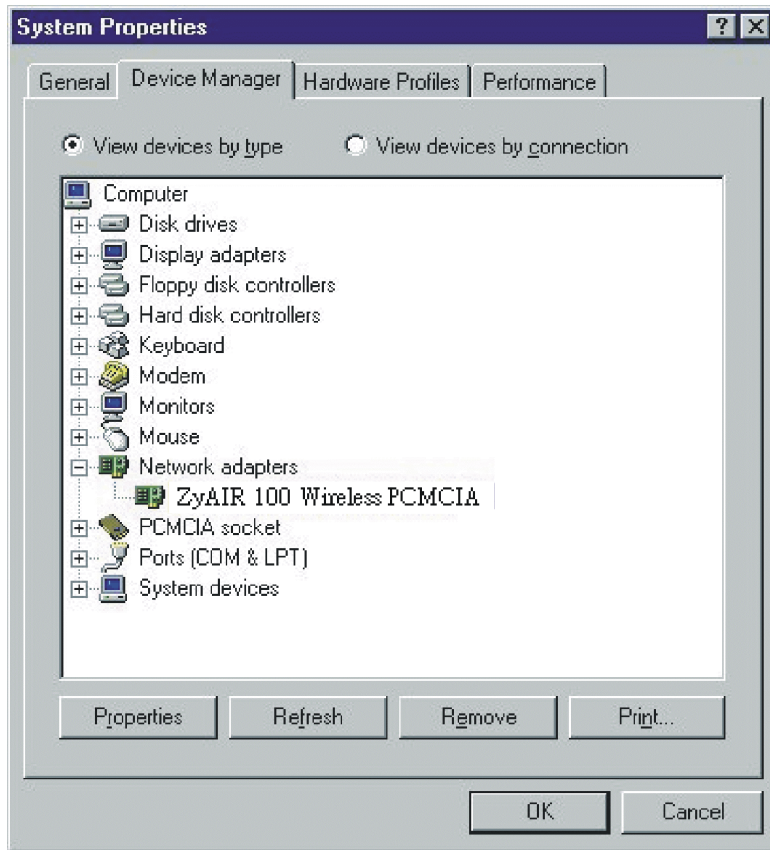
Step 10. Click on the *OK* button. This completes your driver installation for Windows® 95 (OSR2) / 98 operating system.

3.2 Setting Up the ZyAIR 100 for Windows® NT 4.0

NOTE: Before starting driver installation, make sure that the ZyAIR 100 has been inserted into a standard type II PCMCIA slot on your notebook computer.

Step 1. Login as *Administrator*.

Step 2. Click on the *Start* button (Windows® taskbar), then *Control Panel*. Double-click on *Network,* click on the *Adapters* tab, then click on the *Add* button.
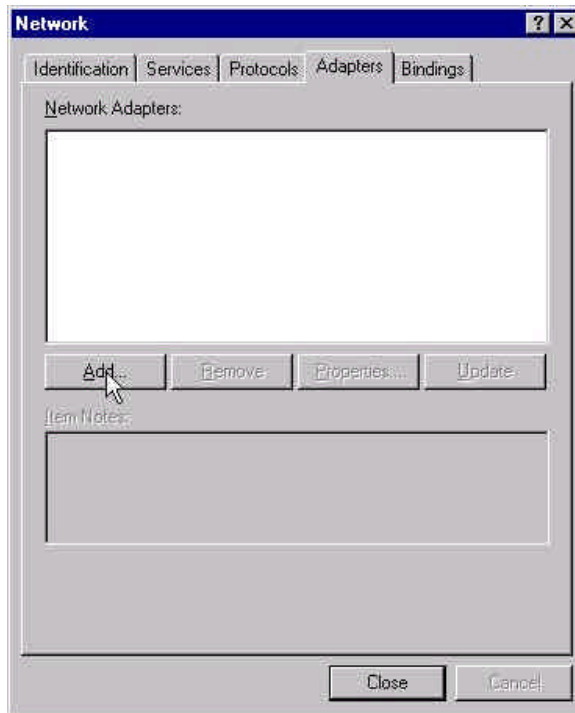
Step 3. Windows® NT will present a list of all the supported adapters. Select *OTHERS*, or click on the *Have Disk* button.
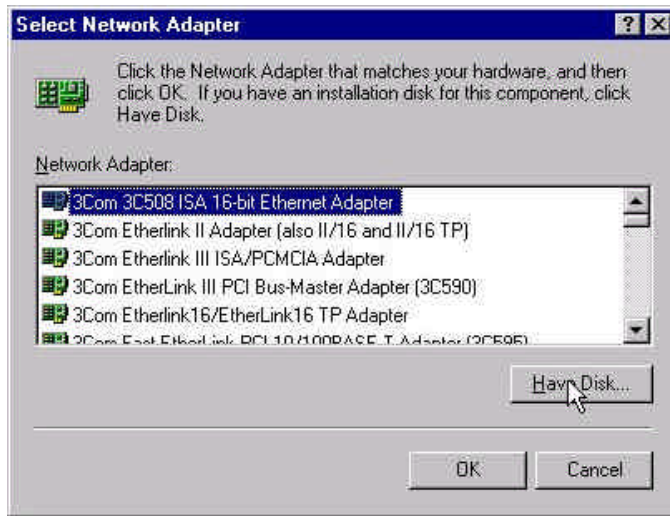
Step 4. Windows® NT will ask for the drive/path containing the ZyAIR 100 drivers. Insert the *ZyAIR Support* CD-ROM disc into the CD-ROM drive and type the location where it is located.
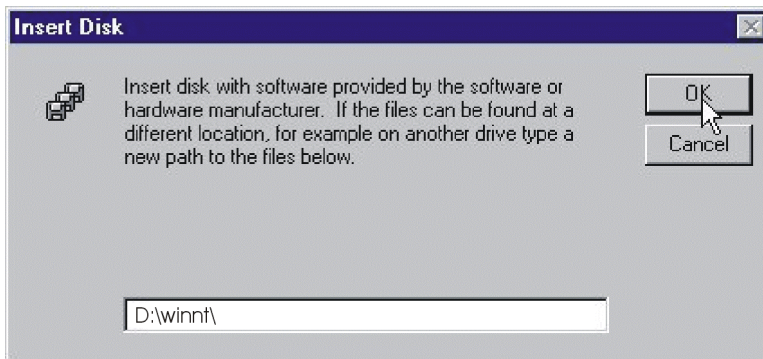
Step 5. Windows® NT will attempt to locate the *INF* file in the specified path. If you have entered the path name correctly, Windows® NT should copy the appropriate drivers to your system.
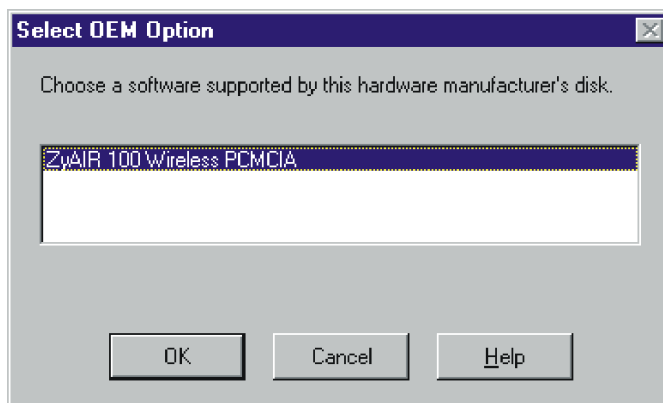
Step 6. The ZyAIR 100 setup dialog box will appear. Select the *Default Channel*, *Network Type* and *ESSID* manually according to the setting in the next figure. Your ZyAIR 100 will thereafter work on this configuration under Windows® NT. Click on the *OK* button to continue.
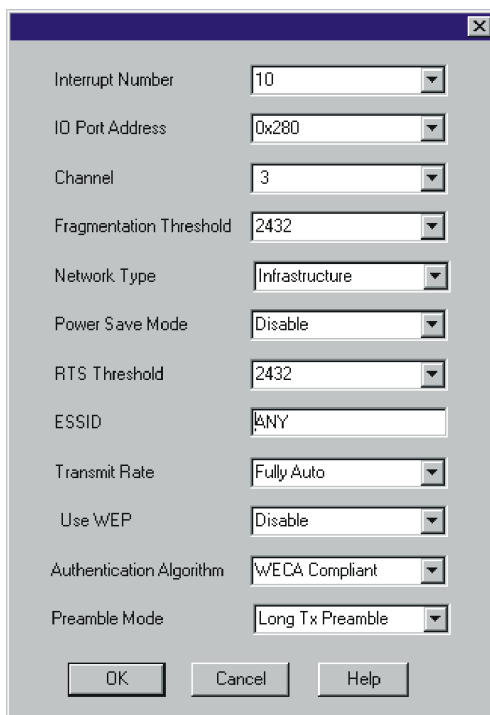
Step 7. The driver should now be copied. Click on the *Start* button (Windows® taskbar), then *Control Panel*. Double-click on *Network,* click on the *Adapters* tab, then click on the *Properties* button. Please specify each parameters required for the network to operate on such as *IP Address*, *Subnet Mask* and *Default Gateway*.
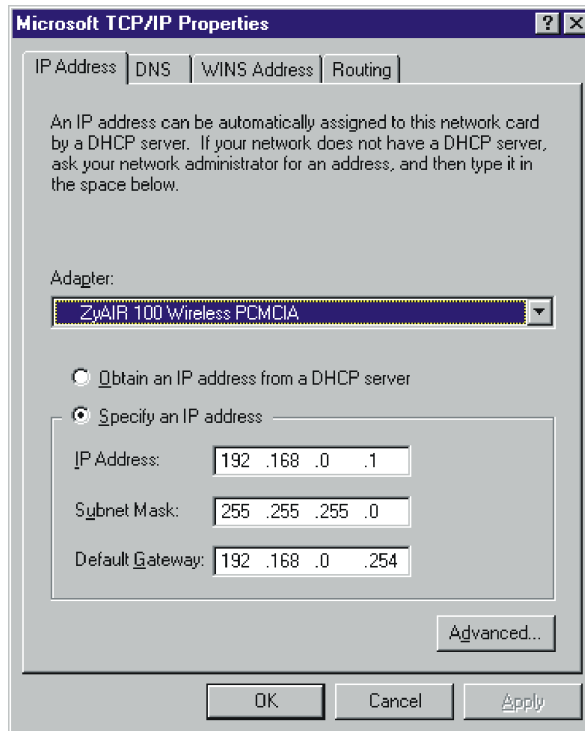
Step 8. Click on the *Yes* button when you are prompted to restart your computer.

Step 9. To find out if the ZyAIR 100 can function properly or not, click on the *Start* button (Windows® taskbar), then *Control Panel*. Double-click on *Devices,* then verify whether the ZyAIR 100 has *Started* by looking on the *Status* column. Click on the *Close* button to exit.

Device	Status	Startup	
v7vram		Disabled	Close
VgaSave	Started	System	
VgaStart		System	Start
Wd33c93		Disabled	
wd90c24a		Disabled	Stop
wdvga		Disabled	
weitekp9		Disabled	Startup...
WINS Client(TCP/IP)	Started	Automatic	
Xga		Disabled	HW Profiles...
ZyAIR100 Adapter Driver		Automatic	Help
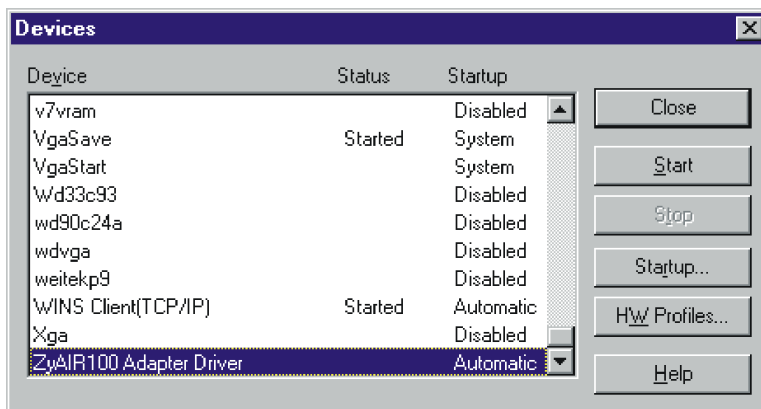
3.3   Setting Up the ZyAIR 100 for Windows® 2000

Step 1. Upon inserting the ZyAIR 100 into your notebook computer, Windows® would automatically detect the new hardware and the *Found New Hardware* dialog box appears.

Found New Hardware

ZyXEL ZyAIR/100

Installing ...
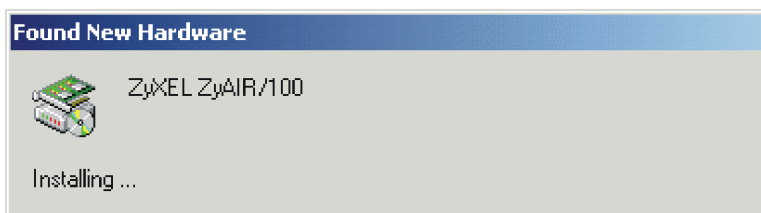
Step 2. The *Upgrade Device Driver Wizard* dialog box appears. Insert the *ZyAIR Support* CD-ROM disc into the CD-ROM drive and click on the *Have Disk* button to specify the location of the driver.
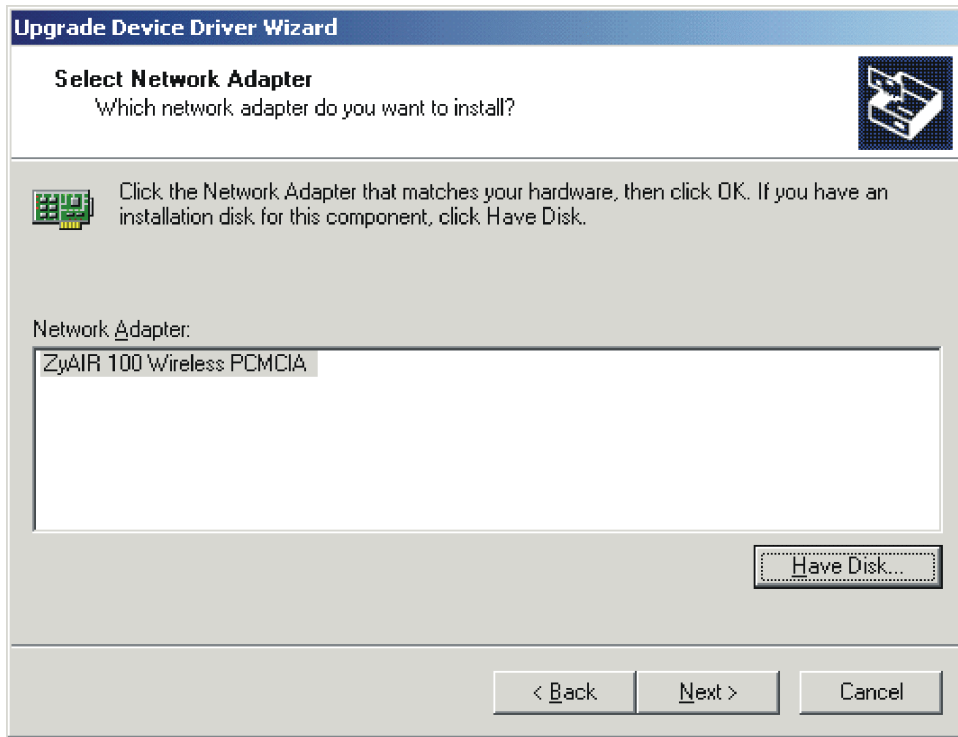
Step 3.   Follow the on screen instructions to complete driver installation.

NOTE: Restart your computer when you are prompted to do so.

3.4   Basic Setup Complete

Well Done! You have successfully installed and set up your ZyAIR 100 to operate on your notebook computer.

Part II:

ADVANCED MANAGEMENT, TROUBLESHOOTING, APPENDICES, GLOSSARY AND INDEX

Chapter 4 provides information on configuring parameters, solving common problems, followed by some Appendices, a Glossary of Terms and an Index.

Chapter 4
Parameter Configuration

This chapter shows you how to install the utility for using the ZyAIR 100.

4.1 Setting Up the ZyAIR 100 Utility

Step 1. Insert the *ZyAIR 100 Support* CD-ROM disc into your CD-ROM drive and run the *setup.exe* file found in the *Utility* folder. Follow the on-screen instructions that guides you through the entire installation process.
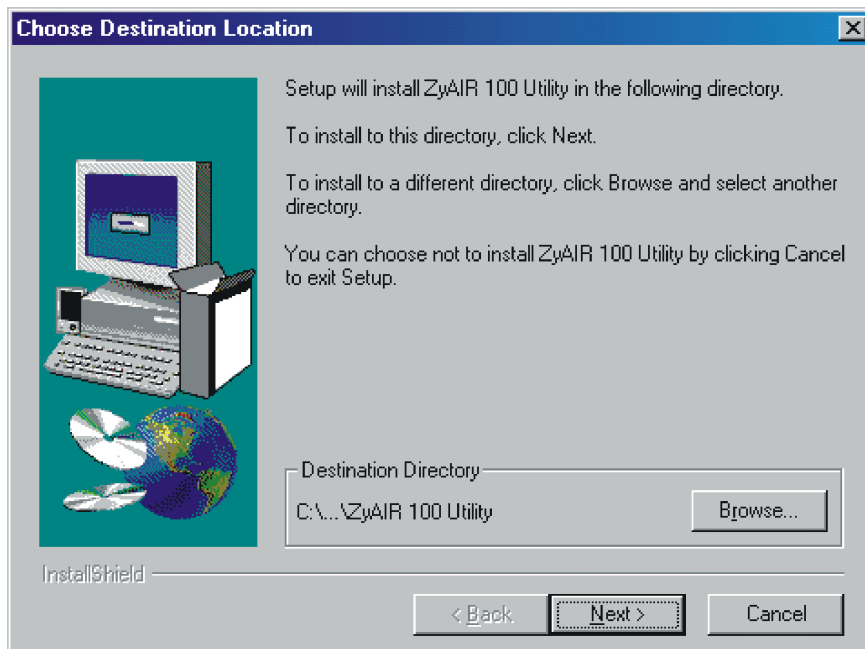
Step 2. Click on the *Finish* button to complete the ZyAIR 100 utility installation.
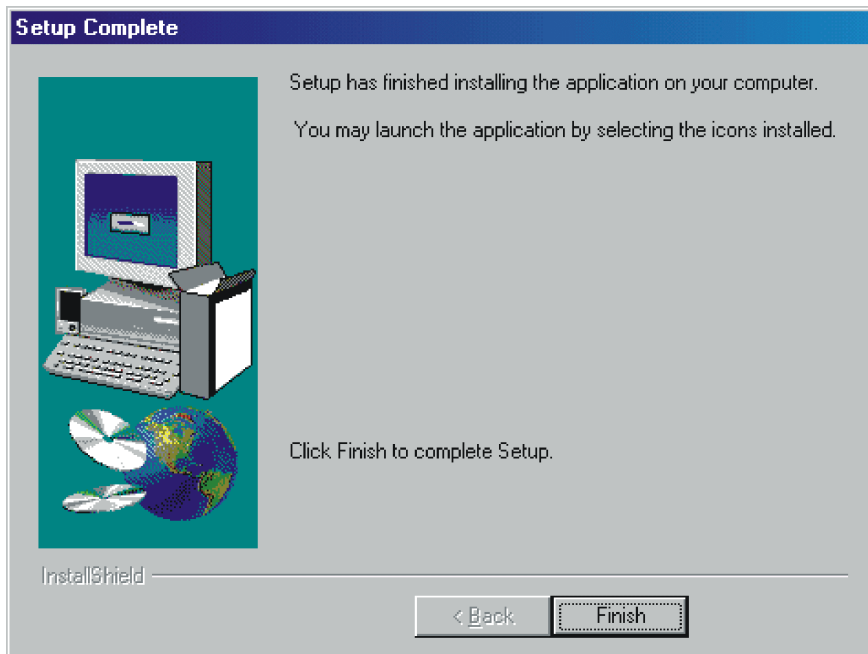
Step 3. Proceed to the next section to configure your ZyAIR 100.

4.2 Using the ZyAIR 100 Utility

Your ZyAIR 100 is a plug-and-play device and its default settings can be set for a typical *Infrastructure Wireless LAN*. Simply install the ZyAIR 100 into your computer and it is ready for use. In special circumstances however, you may need to change configuration settings depending on how you would like to manage your wireless network. The *ZyAIR 100 Utility* enables you to make configuration changes and perform user-level diagnostics on your ZyAIR 100 in the Windows® 95 (OSR2) /98/NT/2000 operating system environments.

Step 1. Click on the *Start* button (Windows® taskbar), then *Programs*. Run the *ZyAIR 100 Utility*. The Main Menu appears.
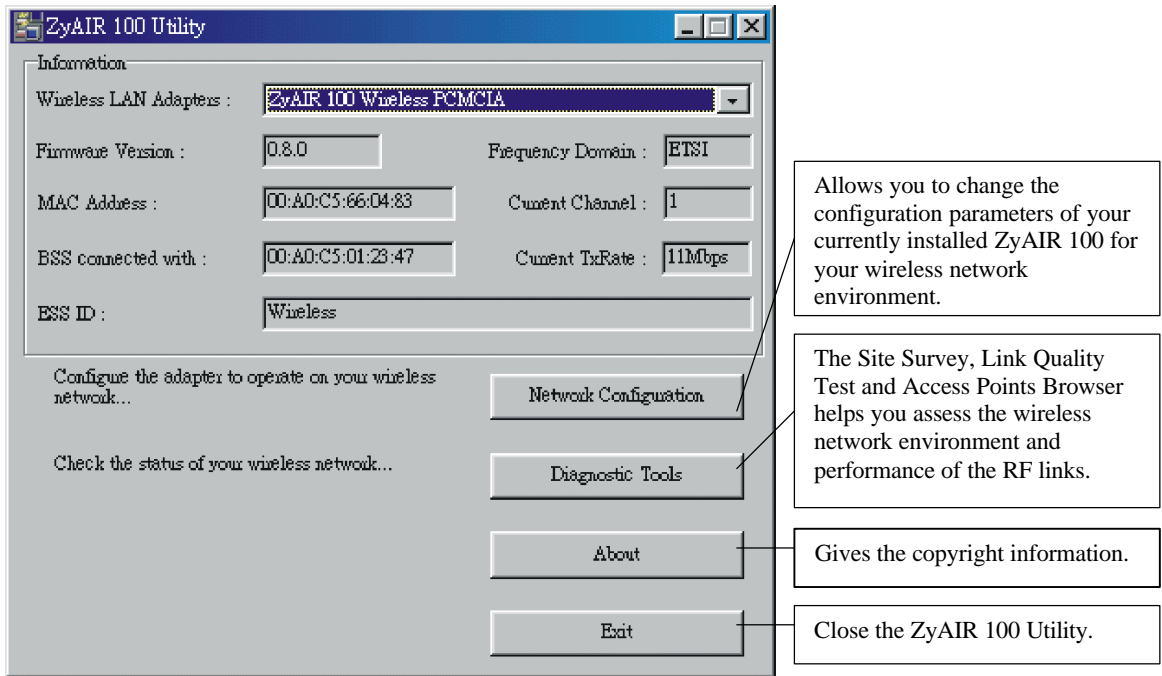
Figure 4-1 ZyAIR 100 Utility – Main Menu

4.2.1 Main Menu

When the Main Menu appears, the ZyAIR 100 hardware information is displayed in real time. Shown is the current adapter configuration information in terms of *MAC Address*, *Firmware Version*, *Frequency Domain*, *BSS connected with*, *Current Channel, Current Transfer Rate* and *ESS ID* of the wireless LAN adapter that you installed in your desktop or notebook computer.

4.2.2 Network Configuration

The Network Configuration menu allows you to view and modify the current configurations of your ZyAIR 100 easily and quickly. The configuration settings include: *ESS ID*, *Network Type, RTS Threshold*, *Frag. Threshold*, *Power Save*, *Use WEP* and *Transmission Rate*.
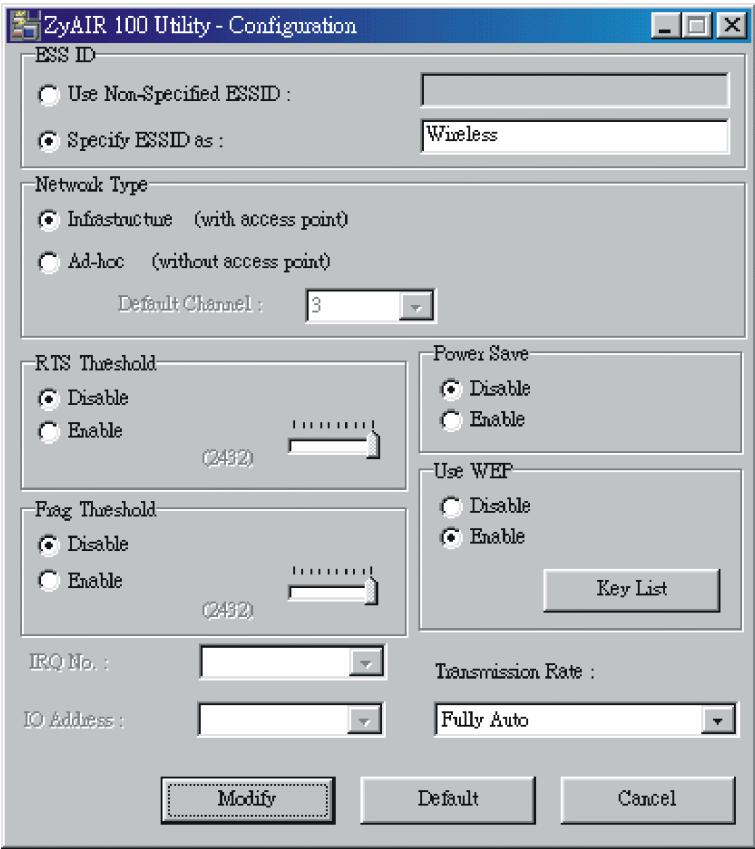
Figure 4-2 ZyAIR 100 Utility – Network Configuration Screen

ESS ID

The ESSID is a unique ID given to the Access Point. Wireless clients associating to any Access Point must have the same ESSID. Select *Specified ESSID as* and enter a specific ESSID (Access Point) you desire to connect with. Alternatively, you may select *Use Non-Specified ESSID* (default setting). This allows your wireless adapter to automatically associate to any Access Point in the vicinity of your wireless adapters. You can leave *Use Non-Specified ESSID* field blank, or enter the name *ANY* (all characters in uppercase). It is recommended that you select the *Specified ESSID as* option. This will prevent your computer from accidentally connecting to a different wireless network.

When moving your computer to another location within the network environment and it becomes out-of-range of the current Access Point, the roaming function will automatically connect your computer to another Access Point.

NOTE: Once the ESSID is set on the initial ZyAIR 100 and the rest of the clients are set to the default value of ANY, then the initial ZyAIR 100 with the ESSID must be started first.

Network Type

To connect your wireless station to a local network infrastructure, set the station operation mode to *Infrastructure* (*with Access Point* as default setting). In case you do not wish to connect to a network infrastructure, but prefer to set up a small wireless workgroup, you can enable the *Ad-hoc (without Access Point)* tick box. Be aware that when the Ad-hoc mode is selected, be sure to set your wireless stations with the same channel.

NOTE: ZyAIR 100 works with any IEEE 802.11 and 802.11(b)-compliant Access Points.

RTS Threshold

The *RTS Threshold* prevents the *Hidden Node* problem. *Hidden Node* is a situation in which two stations are within range of the same Access Point, but are not within range of each other. The following figure illustrates an example of the *Hidden Node* problem. Both stations (STA) are within range of the Access Point, however, they cannot hear each other. Therefore, they are considered hidden nodes from each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations.
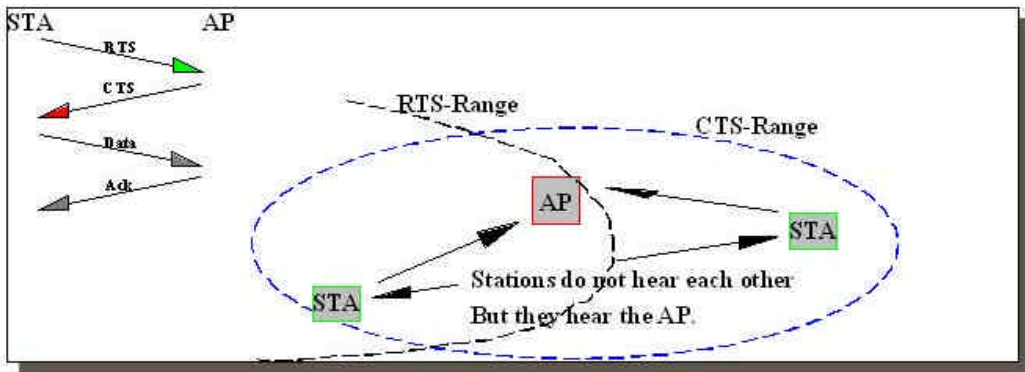
Figure 4-3 RTS Threshold

Thus, the *RTS Threshold* mechanism provides a solution to prevent data collisions. When you enable *RTS Threshold* on a possible *hidden station*, this station and its Access Point will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all stations within its range to notify all other stations to defer transmission. It will also confirm with the requesting station that the Access Point has reserved it for the time frame of the requested transmission.

Normally, the *Disable* option (default) is selected when you are not concerned with the *Hidden Node* problem. When the *Hidden Node* problem becomes an issue, please select *Enable* and specify the packet size. The RTS function will be activated if the packet size exceeds the value you set. It is highly recommended that you set the value ranging from *0* to *2432*.

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

Use WEP (Wired Equivalent Privacy)

To prevent unauthorized wireless stations from accessing data transmitted over the network, ZyAIR 100 offers highly secure data encryption known as WEP. If you require high security in transmission, please select *Enable* and click the *Key List* button.
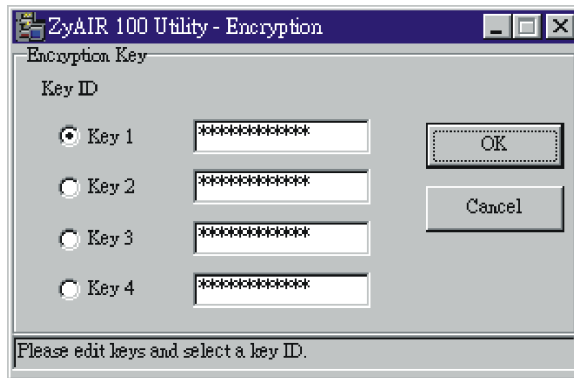
Figure 4-4 ZyAIR 100 Utility – WEP Encryption Screen

The *Encryption* dialog box enables you to identify 4 different encryption key and select one of them to encrypt your transmission data. The key value of your choice may either be:

- Five ASCII character string, or;

- 10-digit hexadecimal values in the range of *a* to *f*, *A* to *F* and *0* to *9*, proceeded by the characters *0x* (e.g., 0x11AA22BB33).

Select one key as the active key to encrypt wireless data. Then click on the *OK* button

> **NOTE: To allow encrypted data communications, you must set the same encryption key values on all wireless stations and/or Access Points. For example, if you use Key 1 on your ZyAIR 100 and the value is (e.g., MyCar), the same value must be assigned to Key 1 for all other client stations. The values you enter on the Encryption dialog box will only be visible the first time you enter the keys. After closing this dialog box, all Key values will be displayed as "xxxxxxxxxxxx" every time the tab is displayed again.**

Frag Threshold

The Fragmentation function is used for improving the efficiency when high traffic flows along in the wireless network. If your ZyAIR 100 often transmit large files in the wireless network, you can enable the *Fragmentation Threshold* by clicking the *Enable* button and the function will split the packet. The value can be set from *256* to *2432*. Default value is *Disable*.

Power Save

The *Power Save* function is used to conserve the battery life of your computer. When Power Save is enabled, your ZyAIR 100 will go into sleep mode to minimize power consumption.

> **NOTE: The Power Save function is only supported in the Ad-hoc Network Type. The Infrastructure Network Type is supported in upcoming firmware upgrades. Please contact your reseller for the most recent firmware.**

Transmission Rate

ZyAIR 100 provides various transmission (data) rate options for you to select. *Transmission Rate* options include *Fully Auto*, *Fixed 1 Mb/s*, *Fixed 2 Mb/s*, *Auto Select 1M or 2M*, *Fixed 5.5Mb/s* and *Fixed 11Mb/s*. In most networking scenarios, you will see that the factory default *Fully Auto* will prove the most efficient. This setting allows your ZyAIR 100 to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, ZyAIR 100 will automatically switch to a lower transmission (data) rate. Transmission at lower data speeds are usually more reliable. However, when the communication quality improves again, ZyAIR 100 will gradually increase the transmission (data) rate again until it reaches the highest available transmission rate.

If you wish to balance speed versus reliability, you can select any of the above options. *Fixed 11Mb/s* or *Fixed 5.5Mb/s* is used in a networking environment where you are certain that all wireless devices can communicate at the highest transmission (data) rate. *Fixed 1Mb/s*, *Fixed 2Mb/s*, *Auto Select 1M or 2M* are used often in networking environments where the range of the wireless connection is more important than speed.

4.2.3 Diagnostic Tools Screen

The *Diagnostic Tools* helps you troubleshoot the wireless LAN environment. The following explains each tool and gives instructions on how to perform diagnostic tests.
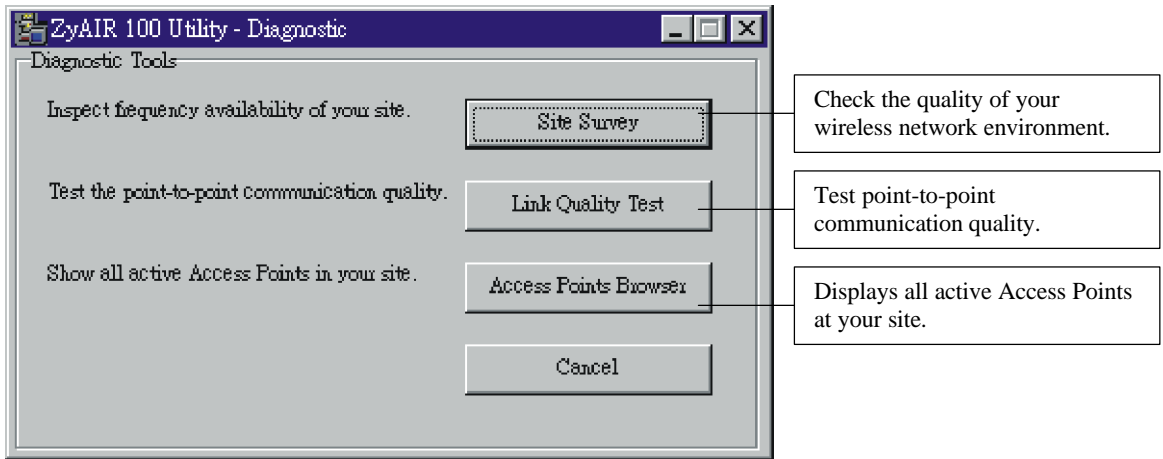
Figure 4-5 Diagnostic Tools Screen

The instructions for performing each diagnostic tool are as follows:

Site Survey

When the *Site Survey* screen is displayed, the channel quality of all 14 radio channels will be displayed. These channel quality measurements are shown on each gauge for the 14 radio channels. The higher the blue bar, the better the quality (i.e., less interference).
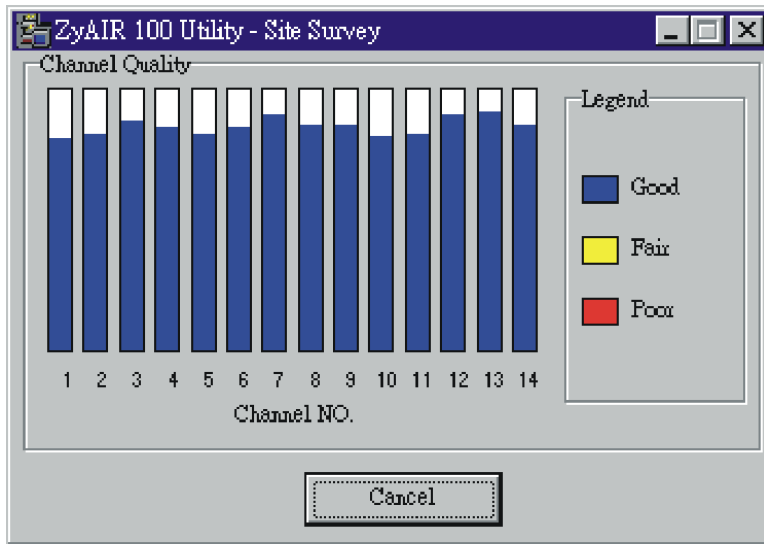
Figure 4-6 Diagnostic Tools – Site Survey Screen

Link Quality Test

The *Link Quality Test* is a useful diagnostic tool for you to test point-to-point data transmission quality between two wireless LAN stations. Or, if you use the *Infrastructure* wireless LAN configuration (*Network Type*), you can test the transmission quality between your wireless LAN station and Access Point.

When the *Link Quality Test* screen is displayed, you may choose one of the roles that this wireless LAN station should perform.

● Act as a *Master Test Station* (*Ad-hoc* Network Type)

Enter the MAC address of the destination *Slave Test Station* before clicking on the *Start* button. The slave MAC address can be found on the *Slave Test Station*'s screen. The *Master Test Station* screen is displayed after clicking on the *Start* button.

Figure 4-7 Diagnostic Tools – Link Quality Test (Master Test Station)

The following table explains the status/statistical information found in the *Master Test Station* screen.

Table 4-1 Diagnostic Tools – Link Quality Test Menu Fields (Master Test Station)

ITEM	DESCRIPTION
Slave/Test Address	The physical address of the *Destination Slave Test Station*. (The physical address of your wireless station will be displayed when performing Access Point loopback test.)
Packet Sent	Total test packets that have been sent.
Packet Received	Total responding packets that have been received.
Time Elapsed	Total test time.
Signal Level	The signal level when receiving the last responding packet. Signal level is calculated as the percentage of its signal level measurement relative to the full signal level.

● Act as a *Slave Test Station* (*Ad-hoc* Network Type)

Click on the *Start* button to start the *Slave Test Station* and display the following screen.

Figure 4-8 Diagnostic Tools – Link Quality Test (Slave Test Station)

The following table explains the status/statistical information found in the *Slave Test Station* screen.

Table 4-2 Diagnostic Tools – Link Quality Test Menu Fields (Slave Test Station)

ITEM	DESCRIPTION
My Address	The physical address of the *Slave Test Station*.
Packet Received	Total test packets that have been received.
Time Elapsed	Total test time.

Signal Level	The signal level when receiving the last test packet. The signal level is calculated as the percentage of its signal level measurement relative to the full signal level.

● Loopback Through the Access Point (*Infrastructure* Network Type)

If you use the *Infrastructure* wireless LAN configuration (network type), you may select the Access Point loopback test to verify the communication quality between your wireless station and Access Point. To run the loopback test, select the *Loopback through the access point* option and click on the *Start* button. Note that it only works in the *Infrastructure* mode.
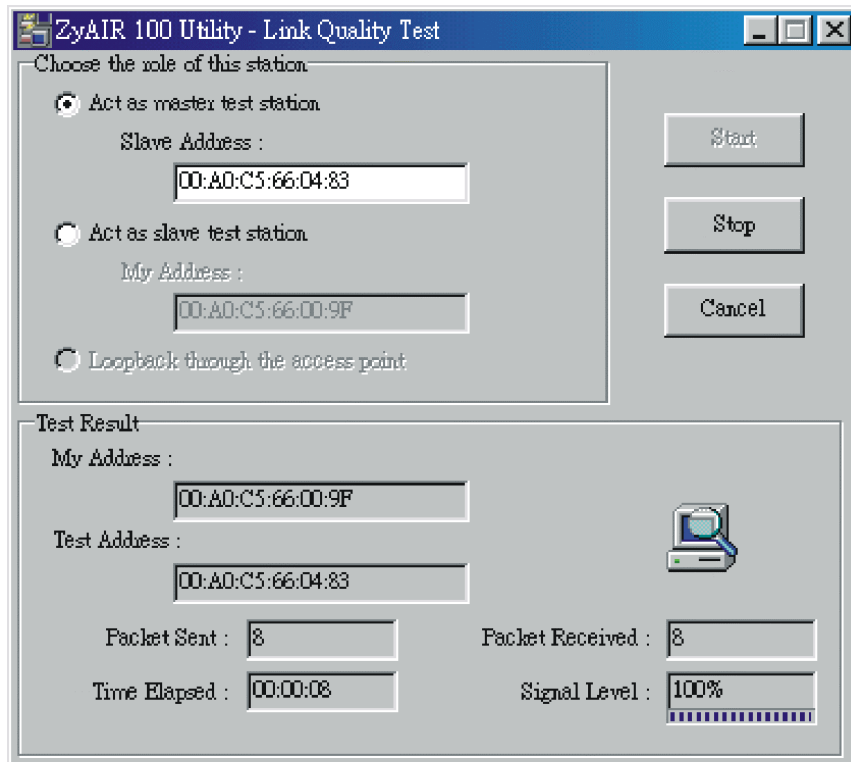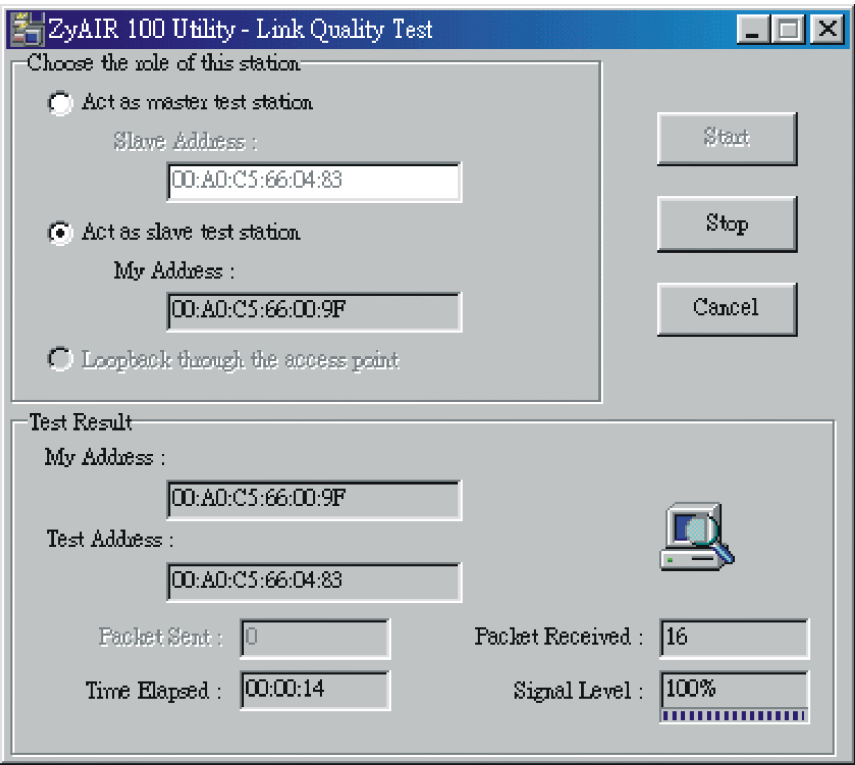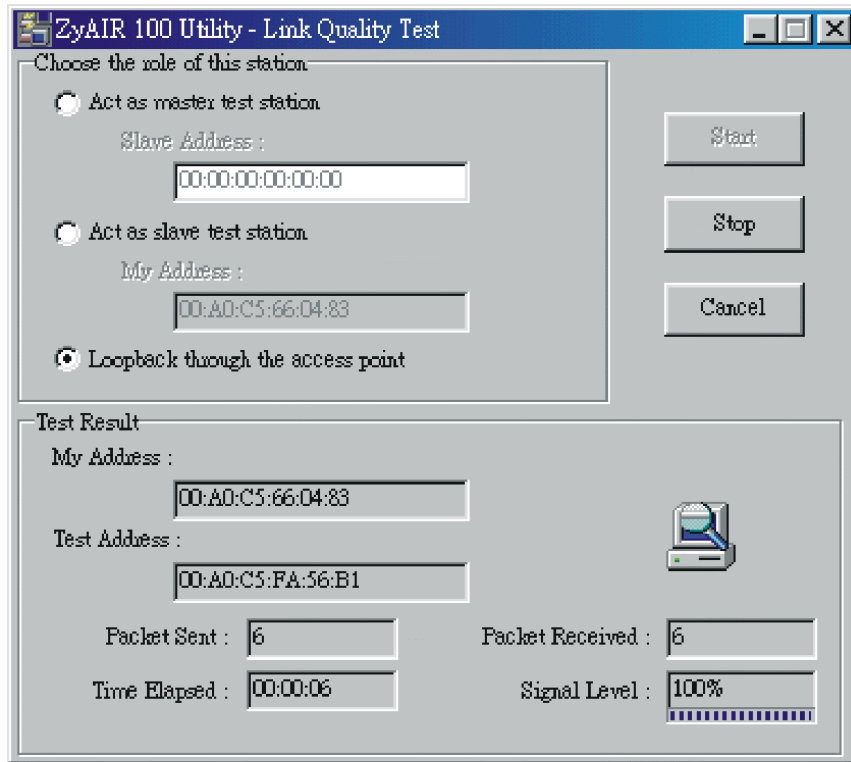

Figure 4-9 Diagnostic Tools – Link Quality Test (Loopback Through Access Point)

The following table explains the status/statistical information found in the *Loopback Through Access Point* screen.

Table 4-3 Diagnostic Tools – Link Quality Test Menu (Loopback Through Access Point)

ITEM	DESCRIPTION
Packet Sent	Total test packets that have been sent.
Packet Received	Total responding packets that have been received.
Time Elapsed	Total test time.
Signal Level	The signal level when receiving the last responding packet. The signal level is calculated as the percentage of its signal level measurement relative to the full signal level.

Access Points Browser

Clicking on the *Access Points Browser* button on the *Diagnostic Tools* screen will give you the following screen. Click on the *Go* button and all the active Access Points will be displayed.
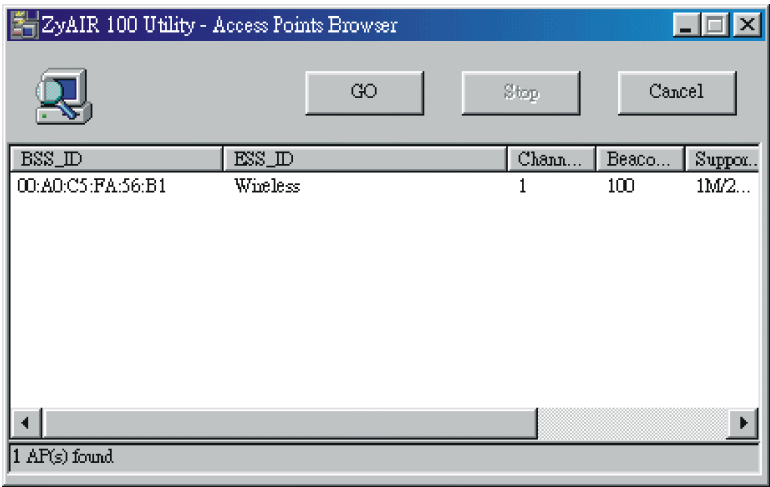
Figure 4-10 Diagnostic Tools – Access Point Browser Screen

The following table explains the status/statistical information found in the *Access Point Browser* screen.

Table 4-4 Diagnostic Tools – Access Point Browser Screen Menu Fields

ITEM	DESCRIPTION
BSS_ID	The BSS ID (MAC address) of the Access Point.
ESS_ID	The ESS ID of the Access Point.
Channel	The operating channel of the respective Access Point.
Beacon	Each Access Point broadcasts *beacon* periodically. The wireless station will process these *beacon*s to keep in touch with the network. It counts the *beacon*s cumulatively from the beginning of the *Access Point Browser* session. This item only shows in the Single-Channel browser screen.
Supported Rates	The data rates that ZyAIR 100 supports. For the 11 Mbps product the supported rates are *11M*, *5.5M*, *2M* and *1M*.
Capacity	This is information from the *beacon* of the Access Point. When communicating with any Access Point, it will display *ESS*. This means that the Access Point is capable of the *Infrastructure* mode. When the device is in *Ad-hoc* mode, no information appears in this column.
Signal Level	This signal level is in the range of *27* to *154*. A high number means that you have a strong signal. This information is for technician's use only. Please use the diagnostic tool to determine your signal strength.
Noise Level	This measurement is the actual amount of noise within your area. This information is for technician's use only. Please use the diagnostic tool and make sure you are above 70 percent. There may be situations where you are close to your Access Point but your signal is below 70 percent. This may indicate a high noise level.

Chapter 5
Troubleshooting

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

5.1   Problems During Installation

Table 5-1 Troubleshooting the Installation of Your ZyAIR 100

PROBLEM	CORRECTIVE ACTION
Problems encountered during installation.	Insert the PCMCIA adapter into your notebook computer's slot again. The Power and Link LED should be on if the adapter is properly inserted.
	Check if the I/O and IRQ for the ZyAIR 100 has conflict problems with other devices connected to your computer.
	For Windows® 95 (OSR2) / 98 / NT / 2000 operating system, make sure that the PCMCIA card service driver is installed on your computer.

5.2   Problems With the Configuration

Table 5-2 Troubleshooting the Configuration

PROBLEM	CORRECTIVE ACTION
Problems encountered with the configuration.	Use the utility *Loopback Test* to check the link status with the Access Point it is associated with (*Infrastructure* mode).
	Use the utility *Master – Slave Test* to check the link status between the ZyAIR 100s (*Ad-hoc* mode).
	Use the utility *Site Survey* to check whether there is high interference around the environment.
	Ensure that you have set the correct IP address for the ZyAIR 100. Use the Ping command to ping the unit itself.
	If *Netbeui* is installed and relevant parameters are set properly, you can go to the *Network Neighborhood* found on your Windows® desktop to check if you can see your PC.

5.3   Problems With the Settings for the Access Point

Table 5-3 Troubleshooting the Settings for the Access Point

PROBLEM	CORRECTIVE ACTION
Problems with settings for the Access Point.	Make sure that the Access Point is powered on and all the LEDs are working properly.
	Use the Ping command to ping any other host. If the host does not respond, your Access Point might not be connected to the network.
	Re-configure and reset the Access Point.
	Use the Web Manager/Telnet of the Access Point to check whether all the Access Points are connected to the network.

5.4   Problems Communicating With the Computer

Table 5-4 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The ZyAIR 100 station cannot communicate with the computer in the Ethernet when the Infrastructure mode is configured.	Make sure that the Access Point with which the station is associated with is powered on.
	Use the *Site Survey* utility to verify if the operating radio channel is in good quality. Or, change the Access Point and all the stations within the BSS to another radio channel.
	Make sure that the station is configured with the same security option with the Access Point, either turn off or turn on with the same security key.
	Make sure that the BSS ID is the same as the Access Point for a roaming-disabled station, or the ESS ID is the same as the Access Point for a roaming-enabled station.

Appendix A
Network Configuration

The ZyAIR 100 supports the same network configuration options of the Legacy Ethernet LANs as defined by the IEEE 802 standard committee. The ZyAIR 100 can be configured as:

- Ad-hoc for departmental or SOHO LANs.

- Infrastructure for enterprise LANs.

- LAN-interconnection for point-to-point link as a campus backbone.

Ad-hoc Wireless LAN Topology
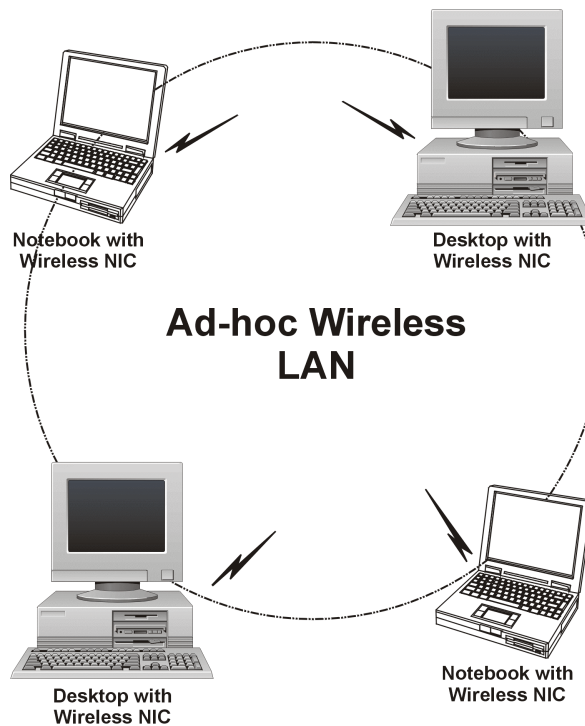
Diagram 1 Example of an Ad-hoc Wireless LAN

An Ad-hoc wireless LAN is a group of computers, each equipped with one wireless adapter, connected as an independent wireless LAN. Computers in a specific Ad-hoc wireless LAN must be configured at the same radio channel. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Infrastructure Wireless LAN Topology
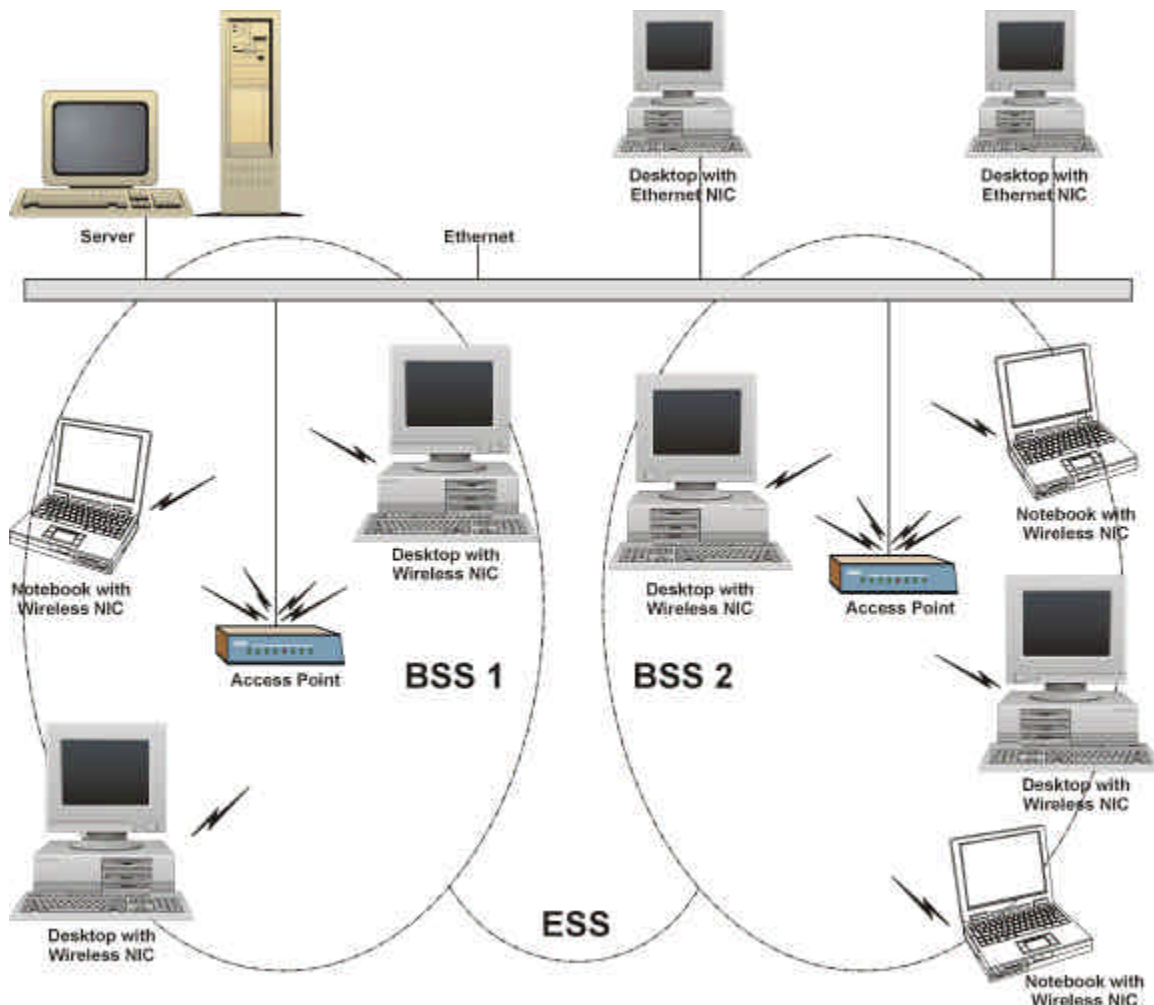
Diagram 2 Example of an Infrastructure Wireless LAN

The ZyAIR 100 provides access to a wired LAN for wireless workstations. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of wireless LAN PC users and an Access Point constitute a Basic Service Set (BSS). Each wireless-equipped PC in this BSS can talk to any computer in the wired LAN infrastructure via the Access Point.

Infrastructure configuration will extend the accessibility of a wireless station to the wired LAN. Multiple Access Points will allow roaming and it will increase the transmission range. The Access Point is also able to forward data within its BSS. The effective transmission range in an Infrastructure LAN is doubled.
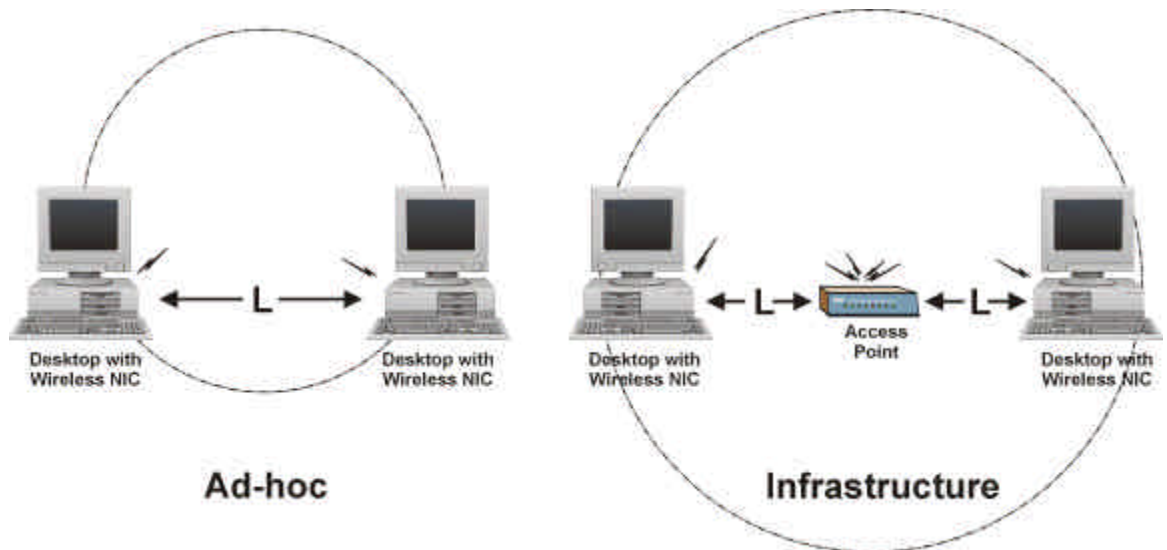
Diagram 3 Example of an Effective Transmission Range

Appendix B
Hardware Specifications

Table 1 ZyAIR 100 Specifications

PRODUCT	FEATURES
Operating Channels	11 for North America, 14 for Japan, 13 for Europe (ETSI), 2 for Spain, 4 for France
Operating Frequency	2.412 ~ 2.462 GHz (North America) 2.412 ~ 2.484 GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI) 2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)
Range	11 Mbps: 460 feet = 140m (in an open environment) 5.5 Mbps: 656 feet = 200m 2 Mbps: 885 feet = 270m 1 Mbps: 1311 feet = 400m
RF Technology	Direct Sequence Spread Spectrum
Modulation	CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
Voltage	3.3V and 5V DC
Power Consumption	Tx power consumption: < 350mA Rx power consumption: < 250mA Sleep Mode: 17mA
Output Power	13 dBm
Sensitivity	@PER < 0.08 11 Mbps < −83 dBm 5.5 Mbps < −86 dBm 2 Mbps < −89 dBm 1 Mbps < −91 dBm
Data Rate	1, 2, 5.5, 11 Mbps
Media Access Protocol	CSMA/CA, 802.11-compliant
Supported O/S	Windows® 95 (OSR2) / 98 / 2000 / NT4.0 / Linux, FreeBSD

Appendix C
Important Safety Instructions

The following safety instructions apply to the ZyAIR 100:

1. Be sure to read and follow all warning notices and instructions.
2. Do not service the product by yourself. Refer all servicing to qualified service personnel.
3. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
4. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and if necessary, implement corrective action before interconnecting the products. If the equipment is to be used with telecommunications circuit, take the following precautions:
   - Never install telephone wiring during a lightning storm.
   - Never install telephone jacks in wet location unless the jack is specially designed for wet location.
   - Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
   - Use caution when installing or modifying telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning
5. In order to limit Radio Frequency (RF) exposure, the following rules should be applied:
   - Install the antenna in a location where a distance of 20 cm from the antenna may be maintained.
   - While installing the antenna in the location, please do not turn on the power of wireless card.
   - While the device is working (transmitting or receiving), please do not touch or move the antenna.
   - Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use.
6. For Laptop (notebook) computer users, in order to comply with the FCC RF exposure limits, it is recommended when using a laptop with a wireless LAN adapter card that the card's integrated antenna should not be positioned closer than 5 cm (2 inches) from your body or nearby persons for extended periods of time while it is transmitting (or operating). If the antenna is positioned less than 5 cm (2 inches) from the user, it is recommended that the user limit exposure time.

Glossary of Terms

802.11	The IEEE standard that specifies Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
802.11b	The IEEE standard that specifies Higher-Speed Physical Layer Extension in the 2.4 GHz Band for 5.5 and 11 megabit per second wireless LANs.
802.3	The IEEE standard that specifies carrier sense media access control and physical layer specifications for Ethernet LANs.
Access Control	The prevention of unauthorized usage of resources.
Access Point (AP)	Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.
Ad-hoc	An Ad-hoc wireless LAN is a group of computers each with wireless adapters connected as an independent wireless LAN.
Advanced Mobile Phone Service (AMPS)	Advanced analog mobile service. Uses a 50 MHz segment of the 800 MHz band to provide 832 analog channels. Two service providers are each assigned one half of the channels in each service area. Analog cellular systems that are similar to AMPs but not compatible include Total Access Communications System (TACS) in the United Kingdom, China and other countries, and Nordic Mobile Telephone (NMT) in the Scandinavian countries.
Authentication	The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Back Door	A deliberately planned security breach in a program. Back doors allow special access to a computer or program. Sometimes back doors can be exploited and allow a cracker unauthorized access to data.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
Base Station	In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communication with the mobile radio telephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station; each base station in turn is interconnected with other cells' base stations.
Bit	(Binary Digit) – A single digit number in base-2, in other words, either a one or a zero. The smallest unit of computerized data.
Broadband	Refers to telecommunication that provides multiple channels of data over a single communications medium.
BSS	Basic Service Set. An Access Point associated with several wireless stations.
Byte	A set of bits that represent a single character. There are 8 bits in a byte.

Cryptoanalysis	The act of analyzing (or breaking into) secure documents or systems that are protected with encryption.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
Decryption	The act of restoring an encrypted file to its original state.
Directional Antennae	An antenna that concentrates transmission power into a direction thereby increasing coverage distance at the expense of coverage angle. Directional antenna types include yagi, patch and parabolic dish.
Direct Sequence Spread Spectrum (DSSS)	A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DTE	Originally, the DTE (data terminal equipment) meant a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Encryption	The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula that determines how the file is decrypted.
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
Events	These are network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system.
FAQ	(Frequently Asked Questions) – FAQs are documents that list and answer the most common questions on a particular subject.
FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Flash Memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted and rewritten as necessary.
Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages and/or architecture.

General Packet Radio Service (GPRS)	A packet-based data transmission technology that will initially provide data transfer rates of up to 115 Kbps. GPRS will work with CDMA and TDMA and it supports both the IP and X.25 communication protocols.
Gigahertz (GHz)	One billion cycles per second. A unit of measure for frequency.
Global System for Mobile Communication	GSM operates in the 900, 1,800 and 1,900 MHz frequency bands. GSM 1,800 is widely used in Europe and throughout many parts of the world. In the U.S., GSM 1,900 is the same as PCS 1,900; thus, these two technologies are compatible.
Hertz (Hz)	Cycles per second. A unit of measure for frequency.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
HTTP	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
IMTS	(Improved Mobile Telephone Service) First analog wireless telephone service in the U.S. Limited to six calls at one time in each service area.
Institute of Electrical and Electronic Engineers (IEEE)	A professional society serving electrical engineers through its publications, conferences and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
internet	(Lower case I) Any time you connect 2 or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
IRC	Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not dangerous can cause your system to crash.
ISP	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
Linux	A version of the UNIX operating system designed to run on IBM-compatible computers.

MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it is the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
Megahertz (MHz)	One million cycles per second. A unit of measure for frequency.
Modulation	Any of several techniques for combining user information with a transmitter's carrier signal.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network.
Packet	A basic message unit for communication across a network. A packet usually includes routing information, data and (sometimes) error detection information.
PCMCIA	Personal Computer Memory Card International Association which develops standards for PC cards, formerly known as PCMCIA cards. They are available in three types that are about the same length and width as credit cards but range in thickness from 3.3 mm (Type I) to 5.0 mm (Type II) to 10.5 mm (Type III). These cards provide many functions, including memory storage and acting as landline modems and as wireless LAN.
Personal Communication Systems	PCS networks in the U.S. provide narrowband digital communications in the 900 MHz band for paging and broadband digital communications in the 1,900 MHz band for cellular telephone service. In the U.S., PCS 1,900 is the same as Global System for Mobile Communications (GSM) 1,900.
Personal Digital Communication	PDC is used only in Japan and is rapidly being replaced with CDMA to alleviate overcrowding of PDC bandwidth.
Phreaking	Breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.
Pirate	Someone who steals or distributes software without paying the legitimate owner for it. This category of computer criminal includes several different types of illegal activities. Making copies of software for others to use. Distributing pirated software over the Internet or a Bulletin Board System. Receiving or downloading illegal copies of software in any form.
Pirated Software	Software that has been illegally copied, or that is being used in violation of the software's licensing agreement. Pirated software is often distributed through pirate bulletin boards or on the Internet. In the internet underground it is known as Warez.
Plain Text	The opposite of Cipher Text, Plain Text is readable by anyone.
POP	Post Office Protocol. This is a common protocol used for sending, receiving and delivering mail messages.
Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.

Port	An Internet port refers to a number that is part of a URL, appearing after a colon (☺) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g., web servers normally listen on port 80.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
Privacy	The service used to prevent the content of messages from being read by other than the intended recipients.
Protocol	A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
PSTN	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and called.
Public Key Encryption	System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption and a corresponding private key used during decryption.
Radio Frequency (RF)	A generic term for radio-based technology.
Range	A linear measure of the distance that a transmitter can send a signal.
RFC	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
Roaming	A function that enables one to travel with his mobile end system (e.g., wireless LAN mobile station) throughout a domain (e.g., an ESS) while being continuously connected to the infrastructure.
Router	A device that connects two networks together. Routers monitor, direct and filter information that passes between these networks. Because of their location, routers are a good place to

	install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
RTS Threshold	Transmitter contending for the medium may not hear each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will not be enabled.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
Service Set Identifier (SSID)	The SSID indicates the identity of an ESS or IBSS.
Snooping	Passively watching a network for information that could be used to a hacker's advantage, such as passwords. Usually done while Camping Out.
SPAM	Unwanted email, usually in the form of advertisements.
SSL (Secured Socket Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
Station (STA)	Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Emulation Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
UNIX	A widely-used operating system in large networks.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video and audio. A URL is the address of an object that is normally typed in the Address field of a web browser. The URL is basically a pointer to the location of an object.
VPN	Virtual Private Network. These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes.
Vulnerability	Point where a system can be attacked.
WAN	Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.
Wired Equivalent Privacy (WEP)	The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.

Wireless Local Area Network (WLAN)	A flexible data communications system implemented as an extension to, or as an alternative for a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections.
Wireless Medium (WM)	The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a wireless local area network (LAN).
Wire Tapping	Connecting to a network and monitoring all traffic. Most wire tapping features can only monitor the traffic on their subnet.
WWW	(World Wide Web) – Frequently used when referring to "The Internet", WWW has two major meanings – First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).

Index