ZyAIR G-1000

Wireless 54 Mbps Access Point

User's Guide

Version 3.50

July 2003

ZyXEL
Unleash Networking Power

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

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.

FC Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

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 lightening.

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	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
FINLAND	sales@zyxel.fi	+359-9-4780-8400 +359-9-4780-8448	http://www.zyxel.fi/	ZyXEL Communications Oy, Malminkaari 10 00700 Helsinki, Finland
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

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyAIR G-1000.

ZyAIR G-1000 is an IEEE802.11g-compliant 54 Mbps Ethernet wireless LAN Access Point (AP). It is suited for wireless connection to the wired network in the home and small office environment allowing users to enjoy the convenience of wireless LAN access. An AP acts as a bridge between the wireless and wired networks, extending your existing wired network without any additional wiring.

This user's guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT. Background information on features configurable by both is in web configuration parts and on features configurable by SMT only is in the part about SMT configuration.

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.

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 a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- 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.

User Guide Feedback

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

Syntax Conventions

- "Enter" means for you to type one or more characters (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 G-1000 Access Point may be referred to simply as the "ZyAIR", the "access point" or the "ZyAIR G-1000" in the user's guide.

Part I:

GETTING STARTED

This part introduces the main features and applications of ZyAIR, hardware installation and setup 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 G-1000 Access Point

The ZyAIR G-1000 Access Point extends the range of your existing wired network without any additional wiring efforts, providing easy network access to mobile users.

The ZyAIR incorporates the IEEE 802.11g standard for high-speed (up to 54 Mbps) wireless transmission. In line with the standard, your ZyAIR is backward compatible with IEEE 802.11b-enabled devices.

Additionally, the ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption and MAC address filtering.

The ZyAIR is easy to install and configure. The embedded web-based configurator and SNMP network management enables remote configuration and management.

1.2 ZyAIR Features

Your ZyAIR has a number of features that give it the flexibility to provide a complete wireless networking solution.

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 Etherent 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 192.168.1.2, subnet mask to 255.255.255.0.

ZyAIR LED

The blue ZyAIR LED (also known as the Breathing LED) is on (dimmed) when the ZyAIR is on and blinks brightly 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.

802.11g Wireless LAN Standard

ZyAIR products containing the letter "G" in the model name, such as ZyAIR G-1000, ZyAIR G-2000, support the 802.11g wireless standard.

802.11g will be fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates. The 802.11g data rate and modulation are as follows:

802.11g	
Data Rate (Mbps)	Data Rate (Mbps)
1 ~ 54	1 ~ 54

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.

Wireless LAN MAC Address Filtering

Your ZyAIR checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

IEEE 802.1x Network Security

The ZyAIR supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

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 manger 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 Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the ZyAIR to access your wired network.

1.3 Applications for the ZyAIR

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

1.3.1 Internet Access Application

The ZyAIR is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyAIR is shown as follows.

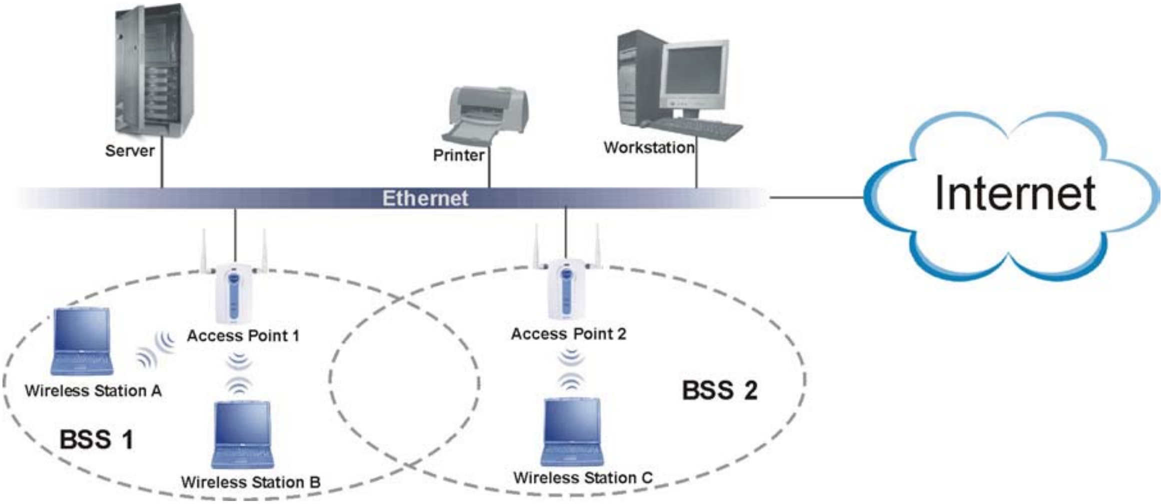


Figure 1-1 Internet Access Application

1.3.2 Corporation Network Application

In situations where users are always on the move in the coverage area but still need access to corporate network access, the ZyAIR is an ideal solution for wireless stations to connect to the corporate network without expensive network cabling.

The following figure depicts a typical application of the ZyAIR in an enterprise environment. The two computers with wireless adapters are allowed to access the network resource through the ZyAIR after account validation by the network authentication server.

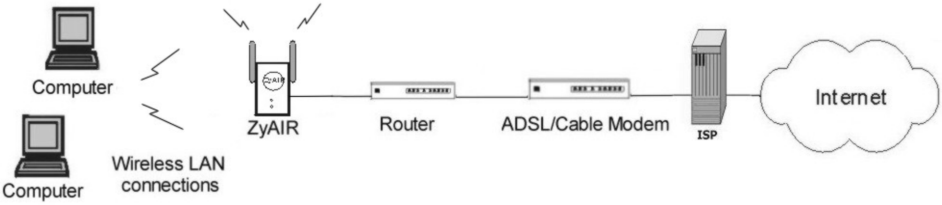


Figure 1-2 Corporation Network Application

Chapter 2 Hardware Installation and Initial Setup

This chapter describes the physical features of the ZyAIR and how to make cable connections.

2.1 Front Panel of the ZyAIR

The LEDs on the front panel indicate the operational status of your ZyAIR.

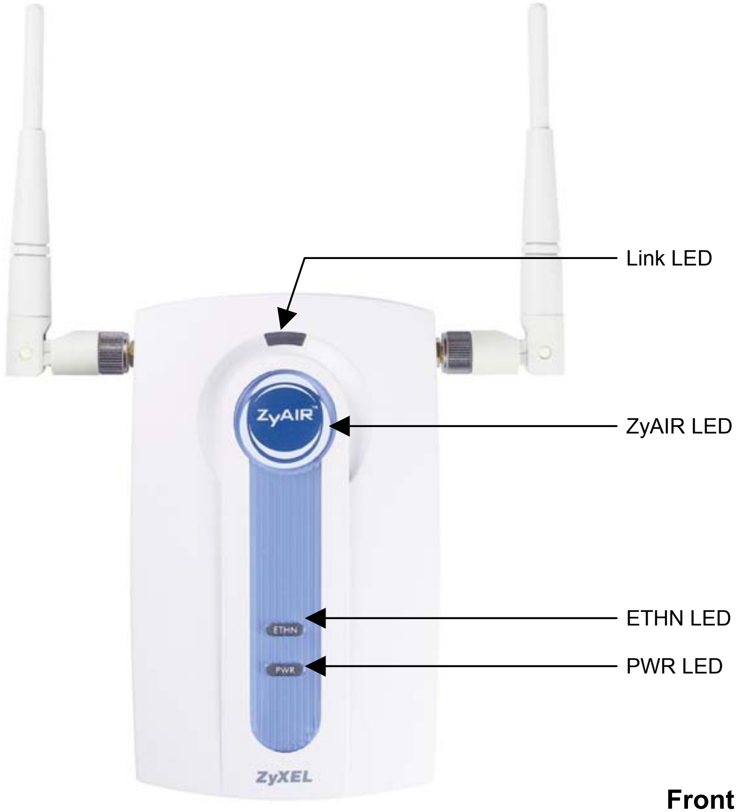


Figure 2-1 ZyAIR Front Panel

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
Link	Red	Blinking	The ZyAIR is not ready or rebooting.
		Off	The ZyAIR is working properly.
ZyAIR (WLAN ACK)	Blue	Breathing	The ZyAIR is sending/receiving data.
		On (dim)	The ZyAIR is ready, but is not sending/receiving data.
ETHN	Green	On	The ZyAIR has a successful 10Mb Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 10Mb Ethernet connection.
	Orange	On	The ZyAIR has a successful 100Mb Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 100Mb Ethernet connection.
PWR	Green	On	The ZyAIR is receiving power.
		Off	The ZyAIR is not receiving power.

2.2 Top Panel and Connections of the ZyAIR

The following figure shows the top panel of your ZyAIR.

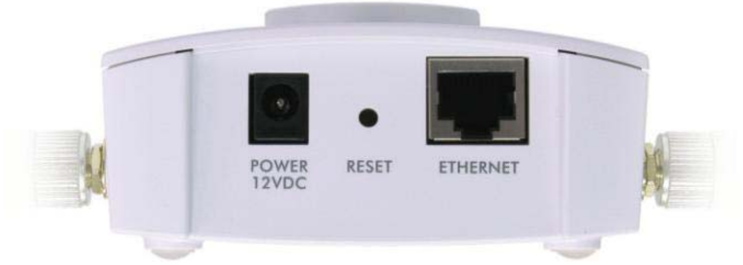


Figure 2-2 ZyAIR Top Panel

2.2.1 One 10/100M Ethernet Port

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. The **ETHERNET** port is auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your ZyAIR to a computer/external hub.

When the ZyAIR is turned on and properly connected to a computer or a hub, the ETHN **LED on the front panel turns on.**

2.2.2 Power Port

Connect the power adapter to the port labeled POWER 12VDC on the top panel of your ZyAIR which then automatically turns on.

The ZyAIR will reboot if the supplied power is too low. This is a normal operation.

To avoid damage to the ZyAIR , make sure you use the supplied power adapter. Refer to the *Power Adapter Specification* appendix for more information.

2.2.3 The RESET Button

Hold this button in for about 10 seconds (or until the Link LED turns red) to reboot and restore your ZyAIR to factory default values.

All custom settings will be lost once you reset to the default settings.

2.2.4 Antennas

The ZyAIR is equipped with two reverse SMA connectors and two detachable omni-directional 2dBi antennas to provide clear radio signal between the wireless stations and the access points. Refer to the *Antenna Selection and Positioning Recommendations* appendix for more information.

The following table shows the ZyAIR's coverage (in meters) using the included antennas. The distance may differ depending on the network environment.

Table 2-2 ZyAIR G-1000 Wireless LAN Coverage

	≤11 Mbps	≤ 5.5 Mbps or lower
Indoor	50 m	80 m
Outdoor	200 m	300 m

Refer to the *Quick Installation Guide* for instructions to attach the antennas to the ZyAIR.

2.3 Hardware Mounting Options

The ZyAIR may be placed on a flat surface or wall mounted.

In general, the best place for the access point is at the center of your intended wireless coverage area. For better performance, mount the ZyAIR in a high position free of obstructions.

Refer to the *Quick Installation Guide* for hardware mounting procedure.

2.4 Additional Installation Requirements

- A computer(s) with an installed network card or an IEEE 802.11g-compliant PCMCIA wireless LAN card.
- To enable remote RADIUS authentication for wireless clients, you need
  - A wireless client computer running IEEE 802.1x-compliant client software. Currently, this is bundled with Windows XP.
  - A network RADIUS server for remote user authentication and accounting.

2.5 Configuring Your ZyAIR

Configure your ZyAIR using:

- Web configurator
- SMT (System Management Terminal). Access the SMT using Telnet.

Chapter 3
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 192.168.1.2.

3.1 Accessing the ZyAIR Web Configurator

Step 1. Make sure your ZyAIR hardware is properly connected.

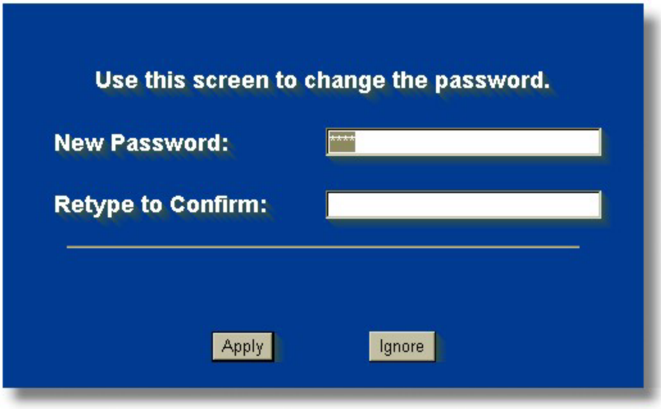
Step 2. Prepare your computer/computer network to connect to the ZyAIR (refer to the *Quick Installation Guide*.

Step 3. Launch your web browser.

Step 4. Type "192.168.1.2" (default) as the URL.

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**.



Use this screen to change the password.

New Password: ****

Retype to Confirm:

Figure 3-1 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.

3.2 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 and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to “1234”, also.

3.2.1 Method of Restoring Factory-Defaults

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

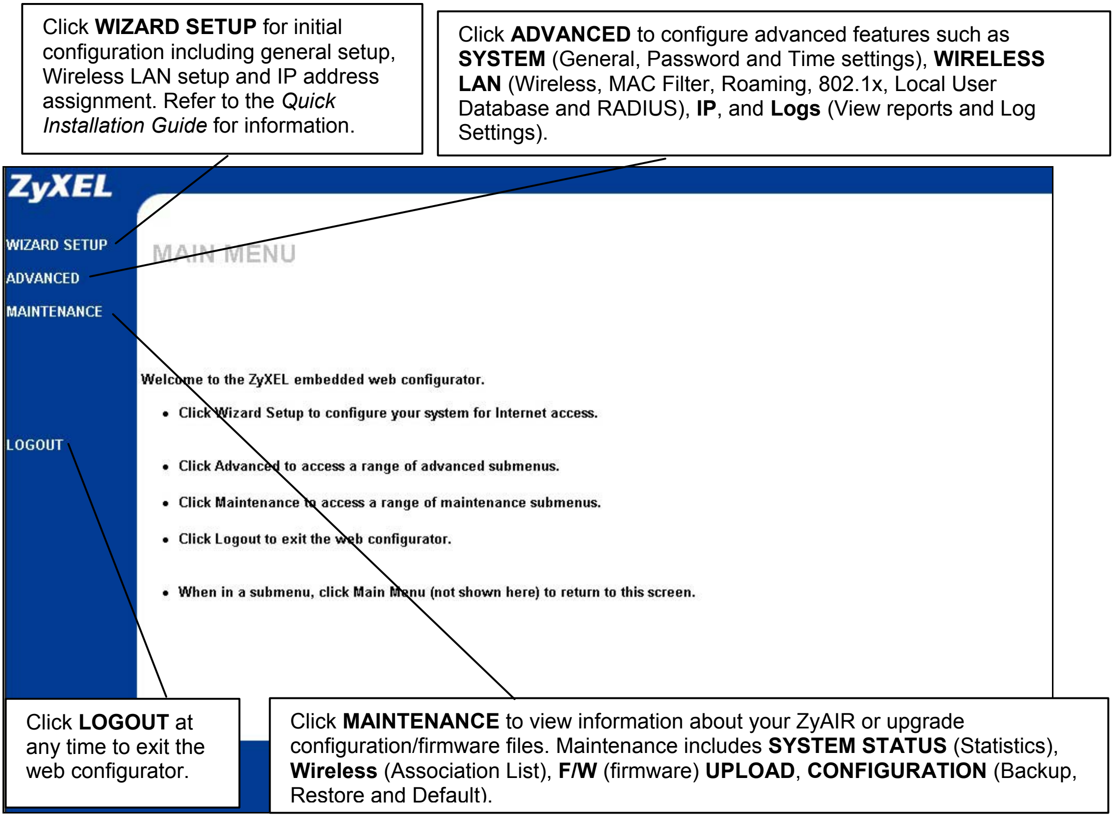
1. Use the **RESET** button on the top panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the Link LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known.
2. Use the web configurator to restore defaults.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

3.3 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 HELP ? icon (located in the top right corner of most screens) to view online help.

The HELP ? icon does not appear in the MAIN MENU screen.



Click **WIZARD SETUP** for initial configuration including general setup, Wireless LAN setup and IP address assignment. Refer to the *Quick Installation Guide* for information.

Click **ADVANCED** to configure advanced features such as **SYSTEM** (General, Password and Time settings), **WIRELESS LAN** (Wireless, MAC Filter, Roaming, 802.1x, Local User Database and RADIUS), **IP**, and **Logs** (View reports and Log Settings).

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access.
- Click Advanced to access a range of advanced submenus.
- Click Maintenance to access a range of maintenance submenus.
- Click Logout to exit the web configurator.
- When in a submenu, click Main Menu (not shown here) to return to this screen.

Click **LOGOUT** at any time to exit the web configurator.

Click **MAINTENANCE** to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes **SYSTEM STATUS** (Statistics), **Wireless** (Association List), **F/W** (firmware) **UPLOAD**, **CONFIGURATION** (Backup, Restore and Default).

Figure 3-2 Web Configurator: Main Menu

Refer to the *Quick Installation Guide* for information on configuring the Wizard screens.

Part II:

SYSTEM AND WIRELESS LAN

This part covers the System and Wireless LAN screens.

Chapter 4 System Screens

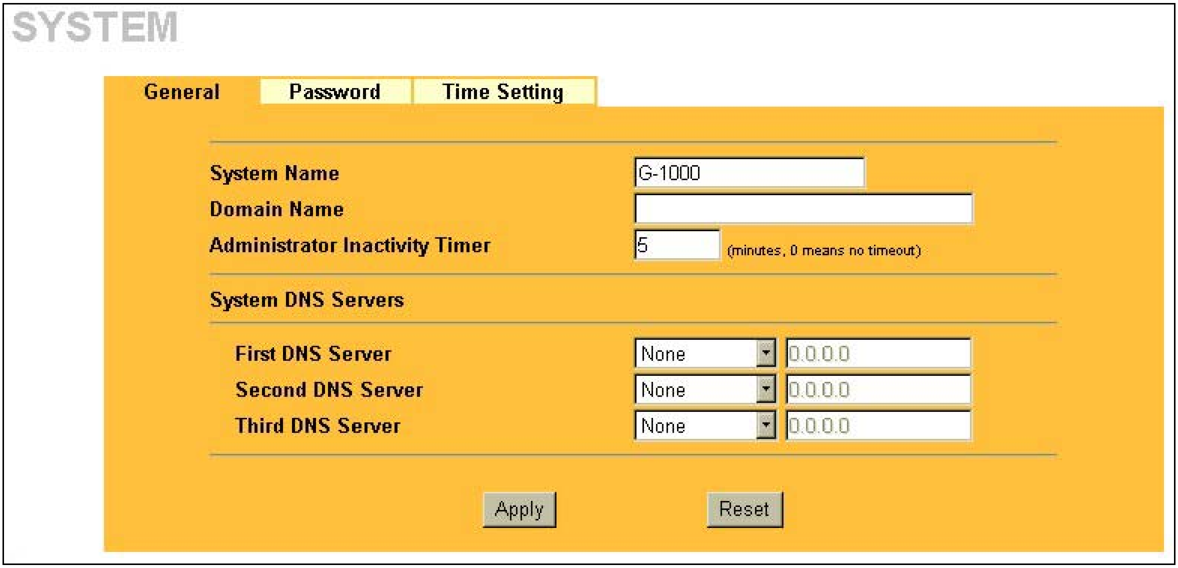
This chapter provides information on the System screens.

4.1 System Overview

This section provides information on general system setup.

4.2 Configuring General Setup

Click **ADVANCED** and then **SYSTEM** to open the **General** screen.



System Name: G-1000

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: None 0.0.0.0

Third DNS Server: None 0.0.0.0

Figure 4-1 System General Setup

The following table describes the labels in this screen.

Table 4-1 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 ISP assigns. If you chose **From DHCP**, but the ZyAIR has a fixed Ethernet IP address, **From DHCP** changes to **None** after you click **Apply**. If you chose **From DHCP** for the second or third DNS server, but the DHCP server does not provide a second or third IP address, **From DHCP** changes to **None** after you click **Apply**. 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.

4.3 Configuring Password

To change your ZyAIR's password (recommended), click **ADVANCED**, **SYSTEM** 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 in for details.

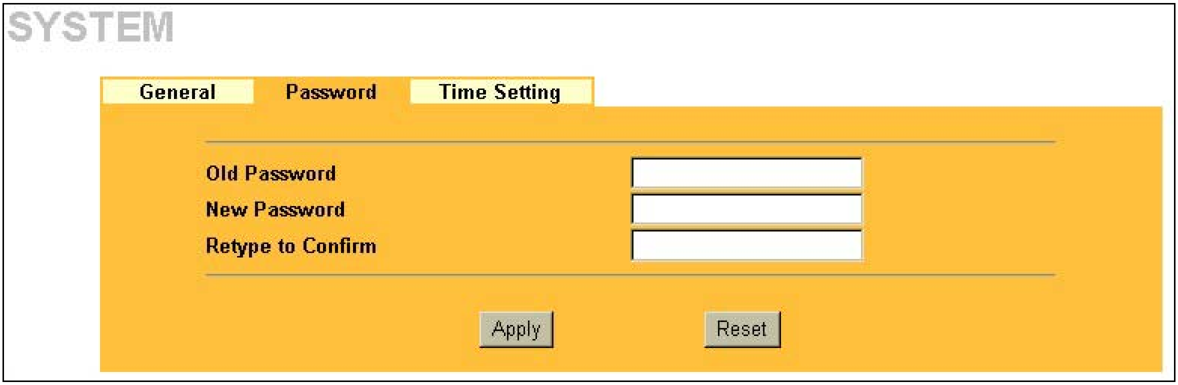


Figure 4-2 Password

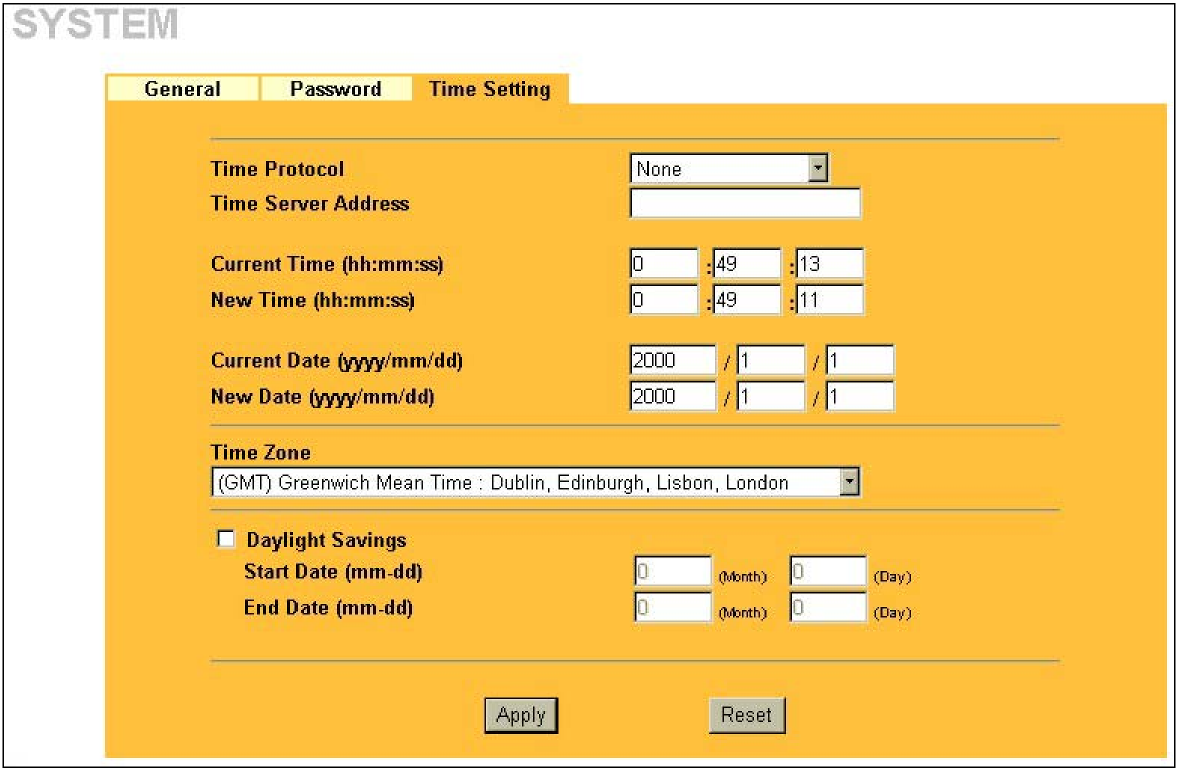
The following table describes the labels in this screen.

Table 4-2 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	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4 Setting the Time

To set the time and date on your ZyAIR, click **ADVANCED**, **SYSTEM** and then the **Time Setting** tab. The screen appears as shown.



Time Protocol: None

Time Server Address:

Current Time (hh:mm:ss): 0 : 49 : 13

New Time (hh:mm:ss): 0 : 49 : 11

Current Date (yyyy/mm/dd): 2000 / 1 / 1

New Date (yyyy/mm/dd): 2000 / 1 / 1

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

☐ Daylight Savings

Start Date (mm-dd): 0 (Month) 0 (Day)

End Date (mm-dd): 0 (Month) 0 (Day)

Figure 4-3 Time Setting

The following table describes the labels in this screen.

Table 4-3 Time/Date

LABEL	DESCRIPTION
Time Protocol	Select the time protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.

Table 4-3 Time/Date

LABEL	DESCRIPTION
Time Server Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw).
Current Time (hh:mm:ss)	This field displays the time of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in this field.
Current Date (yy/mm/dd)	This field displays the date of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
New Date (yy/mm/dd)	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 5
Wireless Configuration and Roaming

This chapter discusses how to configure Wireless and *Roaming screens on the ZyAIR..*

5.1 Wireless LAN Overview

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

5.1.1 IBSS

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

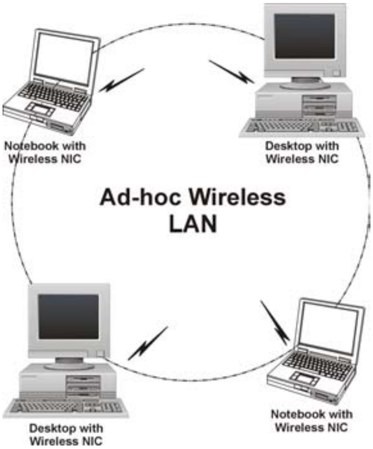

Notebook with Wireless NIC
Desktop with Wireless NIC
Ad-hoc Wireless LAN
Desktop with Wireless NIC
Notebook with Wireless NIC

Figure 5-1 IBSS (Ad-hoc) Wireless LAN

5.1.2 BSS

A Basic Service Set (BSS) is when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS.

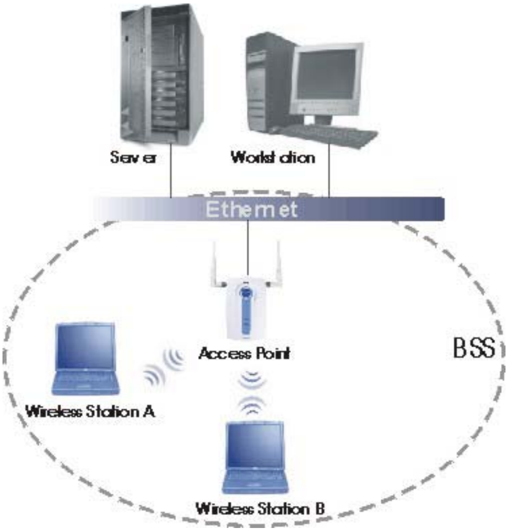


Figure 5-2 Basic Service set

5.1.3 ESS

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

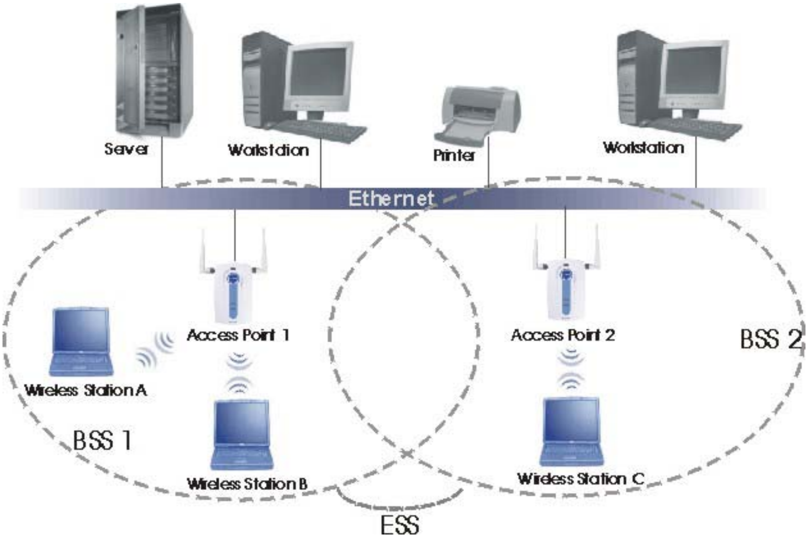


Figure 5-3 Extended Service Set

5.2 Wireless LAN Basics

Refer also to the *Wizard Setup* chapter for more background information on Wireless LAN features, such as channels.

5.2.1 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.

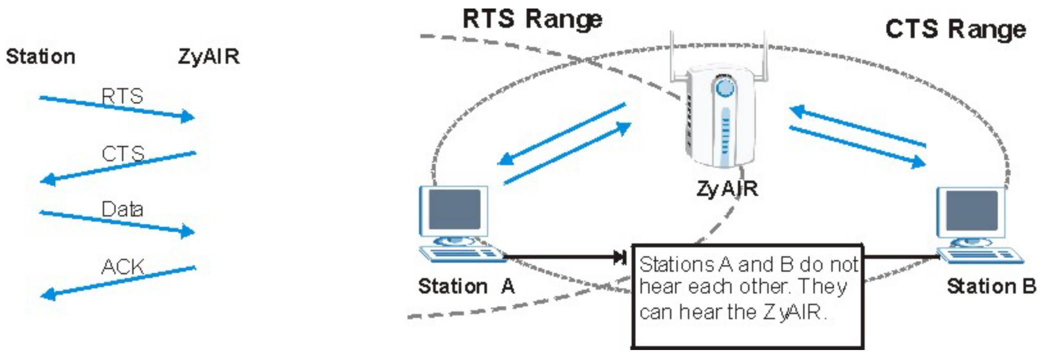


Figure 5-4 RTS/CTS

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

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

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

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

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

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

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

5.2.2 Fragmentation Threshold

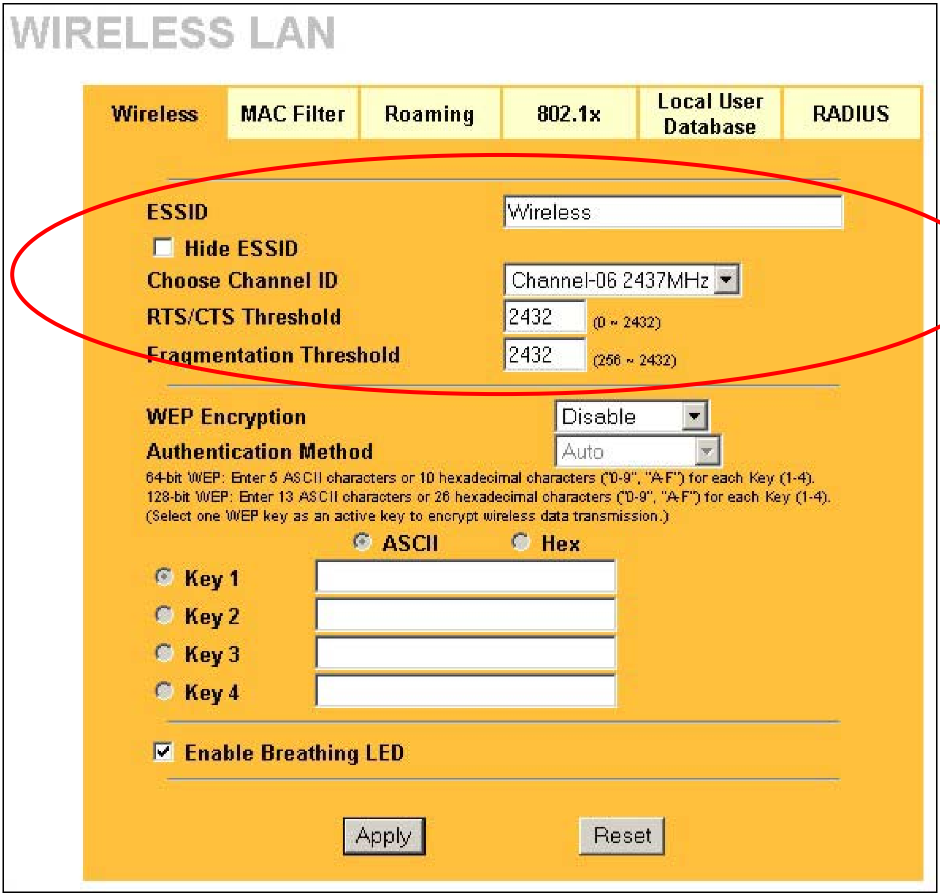
A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyAIR will fragment the packet into smaller data frames.

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.

5.3 Configuring Wireless

Click **ADVANCED** and then **WIRELESS** to display the **Wireless** screen.



ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

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

Figure 5-5 Wireless

The following table describes the general wireless LAN labels in this screen.

Table 5-1 Wireless

LABEL	DESCRIPTION
ESSID	(Extended Service Set IDentity) The **ESSID** identifies the Service Set with to which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.**
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
Choose Channel ID	Set the operating frequency/channel depending on your particular region.
RTS/CTS Threshold	RTS/CTS handshake avoids retransmitting due to hidden nodes. Enter a value between **0** and **2432**. The default is **2432**.
Fragmentation Threshold	Fragmentation threshold defines the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

See the *Wireless Security* chapter for information on the other fields in this screen.

5.4 Configuring Roaming

A wireless station is a device with an IEEE 802.11b or 802.11g-compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown *in Figure 5-6*.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

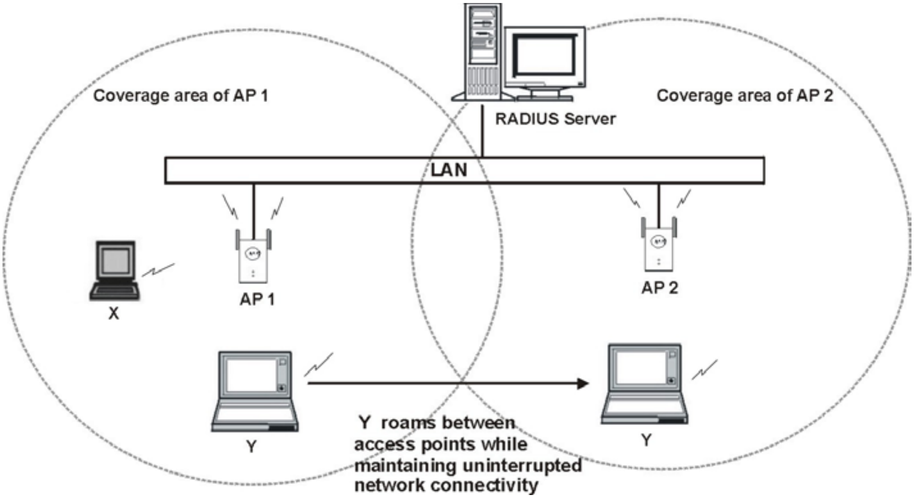

Coverage area of AP 1
RADIUS Server
Coverage area of AP 2
LAN
X
AP 1
AP 2
Y
Y roams between access points while maintaining uninterrupted network connectivity
Y

Figure 5-6 Roaming Example

The steps below describe the roaming process.

Step 1. As wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**, it scans and uses the signal of access point **AP 2**.

Step 2. Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

Step 3. Access point **AP 1** updates the new position of wireless station.

Step 4. Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

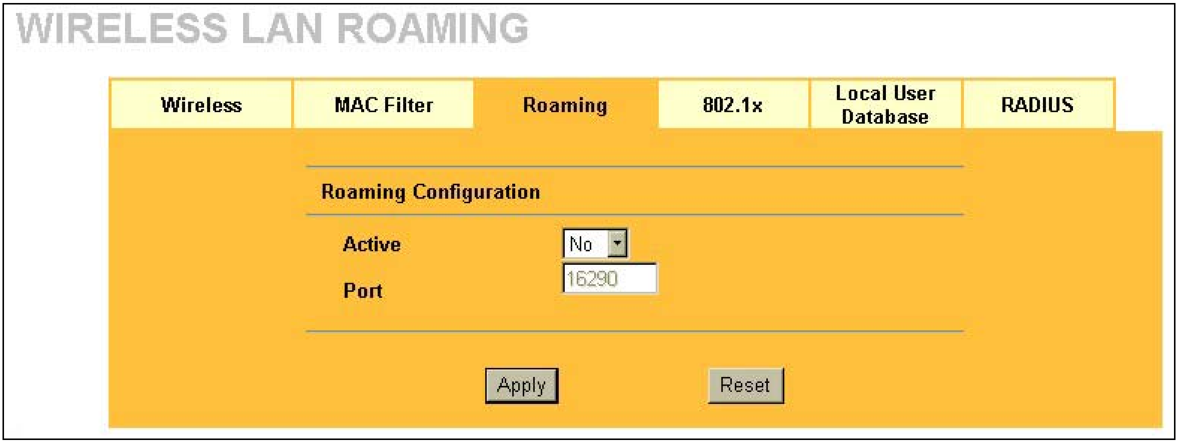
5.4.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your ZyAIR, click **ADVANCED**, **WIRELESS** and then the **Roaming** tab. The screen appears as shown.



Roaming Configuration

Active: No

Port: 16290

Figure 5-7 Roaming

The following table describes the labels in this screen.

Table 5-2 Roaming

LABEL	DESCRIPTION
Active	Select **Yes** from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. **All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.**
Port	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **16290**. Make sure this port is not used by other services.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 6
Wireless Security

This chapter describes how to configure WEP encryption, MAC filter, 802.1x, Local User Database and RADIUS to set up wireless security on your ZyAIR

6.1 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.

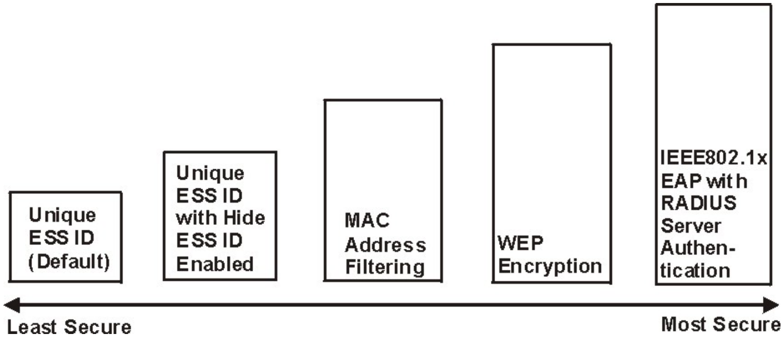

Unique ESS ID (Default)
Unique ESS ID with Hide ESS ID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tication
Least Secure
Most Secure

Figure 6-1 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.

6.2 WEP Overview

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

6.2.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. 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.

6.2.2 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.

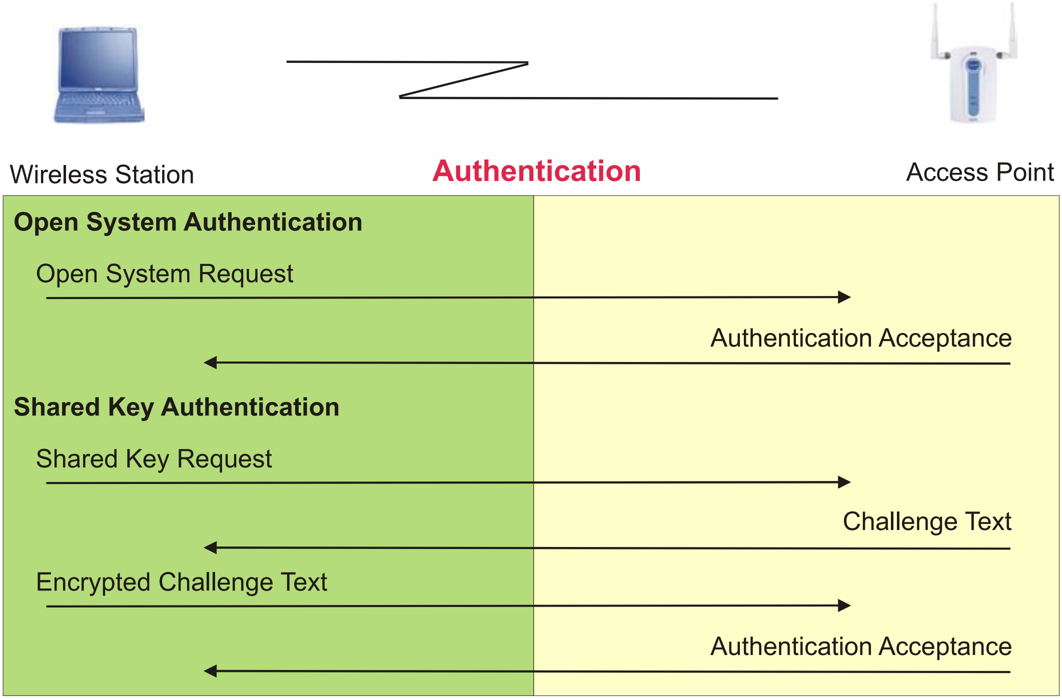


Figure 6-2 WEP Authentication Steps

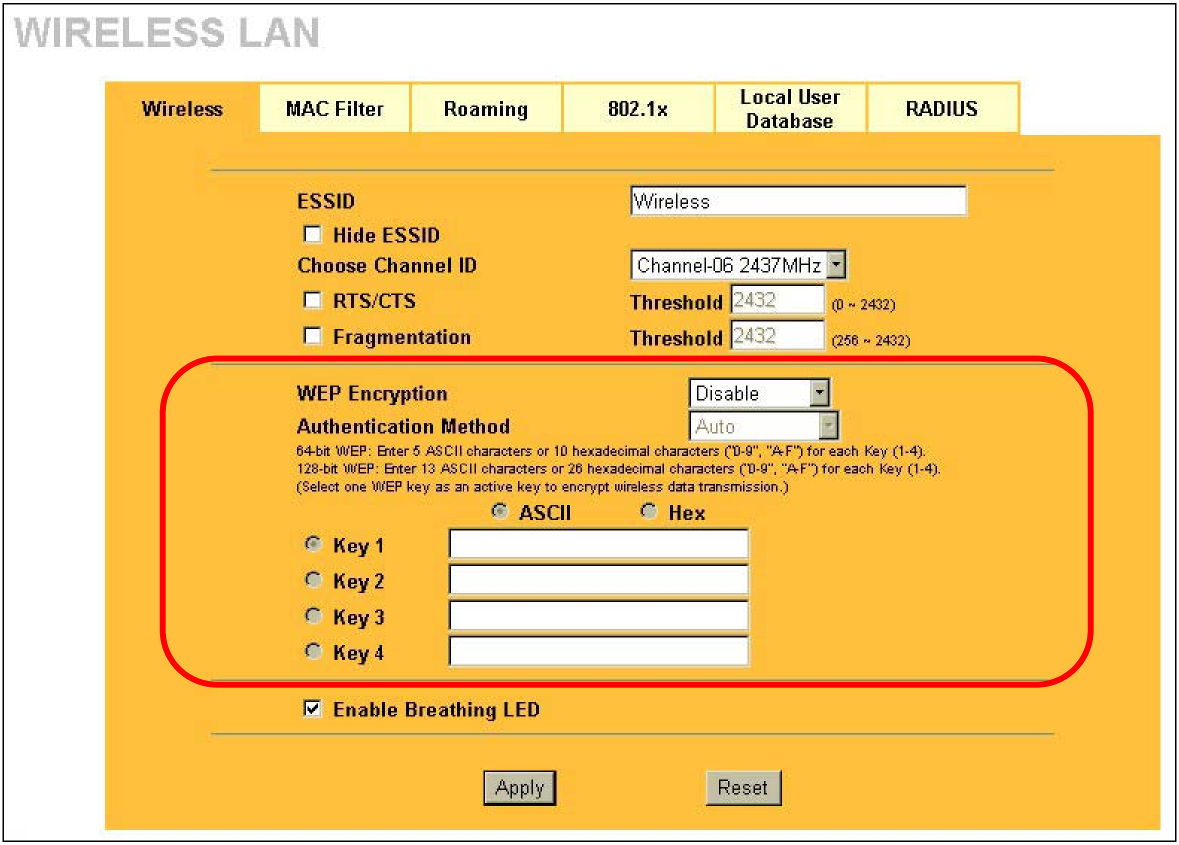
Open System authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station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

6.3 Configuring WEP Data Encryption

In order to configure and enable WEP encryption; click **ADVANCED** and then **WIRELESS** to display the **Wireless** screen.



ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

□ 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

Figure 6-3 Wireless

The following table describes the wireless LAN security fields in this screen.

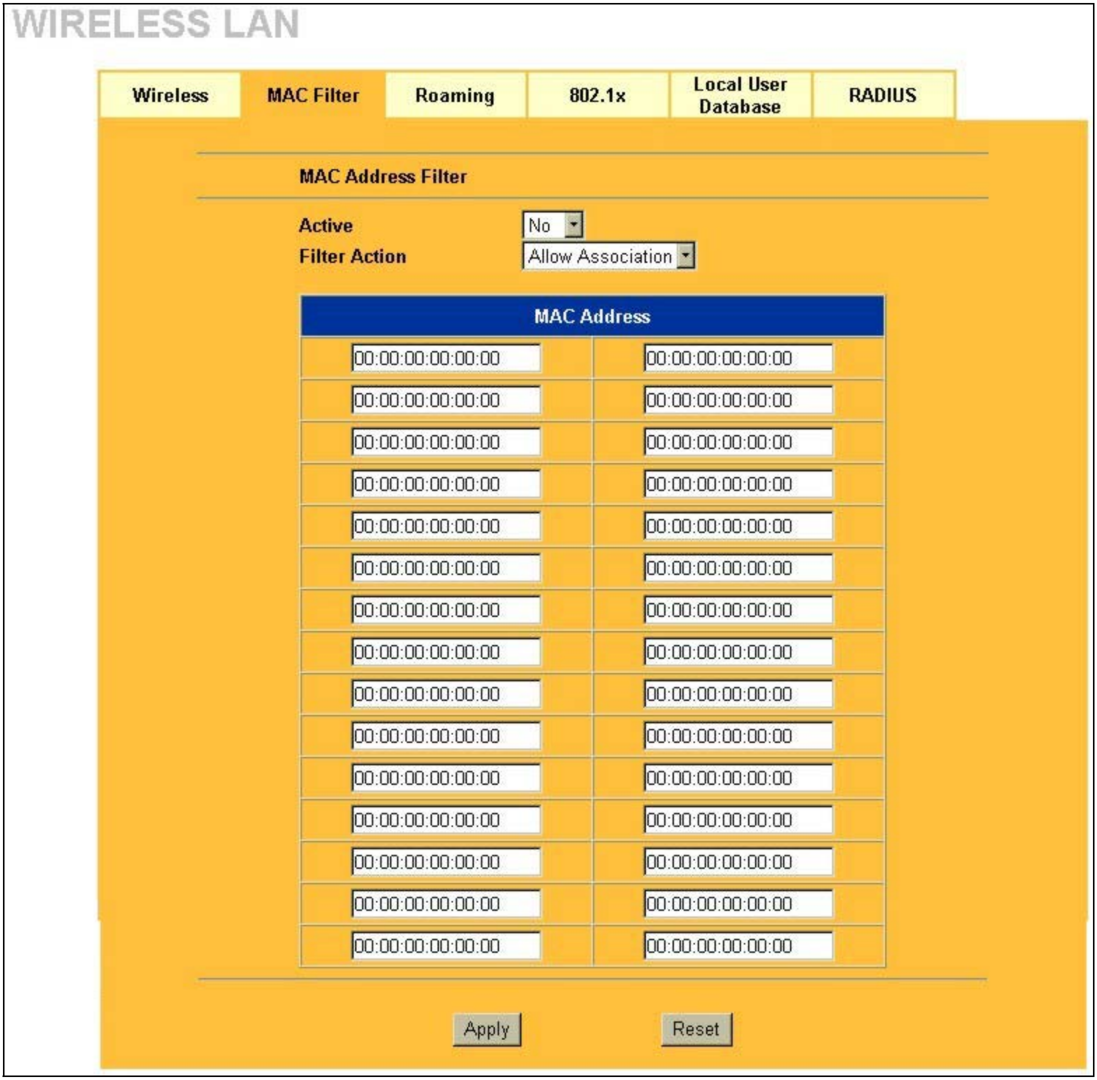
Table 6-1 Wireless

LABEL	DESCRIPTION
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.
Authentication Method	Select **Auto**, **Open System** or **Shared Key** 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 ZyAIR 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 (dimmed) when the ZyAIR is on and blinks brightly (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.

6.4 MAC Filter

The MAC filter screen allows you to configure the ZyAIR to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the ZyAIR (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your ZyAIR's MAC filter settings, click **ADVANCED**, **WIRELESS** and then the **MAC Filter** tab. The screen appears as shown.



MAC Address Filter

Active: No

Filter Action: Allow Association

MAC Address	
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00

Figure 6-4 MAC Address Filter

The following table describes the fields in this screen.

Table 6-2 MAC Address Filter

LABEL	DESCRIPTION
MAC Address Filter	
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the ZyAIR in these address fields.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the ZyAIR (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

6.6 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your ZyAIR acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

6.6.1 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyAIR supports EAP-TLS, EAP-TTLS and DEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the four common types.

Your ZyAIR supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database and RADIUS.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

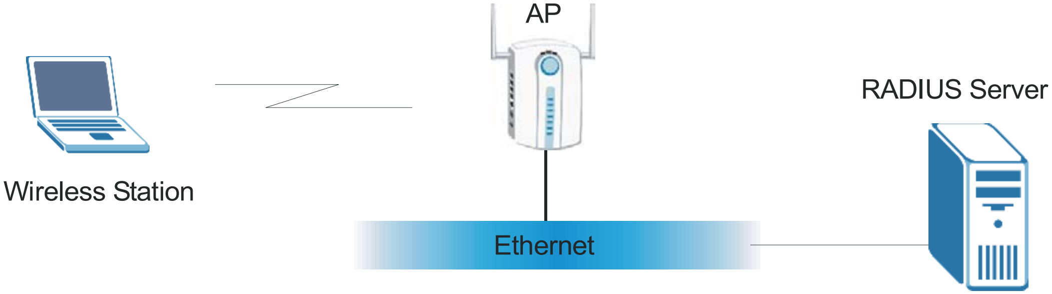


Figure 6-5 EAP Authentication

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

- The wireless station sends a "start" message to the ZyAIR.
- The ZyAIR sends a "request identity" message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

6.7 Dynamic WEP Key Exchange

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

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

To use Dynamic WEP, enable and configure the RADIUS server (see *section 6.11*) and enable Dynamic WEP Key Exchange in the 802.1x screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

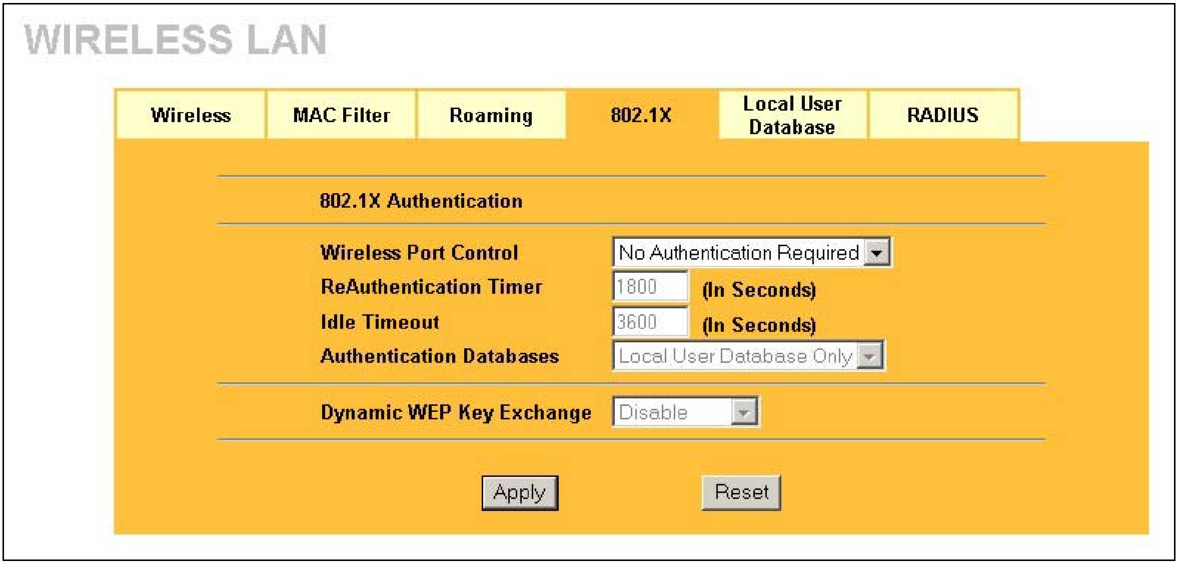
EAP-MD5 cannot be used with Dynamic WEP Key Exchange.

6.8 Introduction to Local User Database

By storing user profiles locally on the ZyAIR, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.9 Configuring 802.1x

To change your ZyAIR's authentication settings, click **ADVANCED**, **WIRELESS** and then the **802.1x** tab. The screen appears as shown.



802.1X Authentication

Wireless Port Control: No Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

Dynamic WEP Key Exchange: Disable

Figure 6-6 802.1x Authentication

The following table describes the fields in this screen.

Table 6-3 802.1x Authentication

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. **No Access Allowed** blocks all wireless stations access to the wired network.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). **If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**
Idle Timeout (in seconds)	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (1 hour).

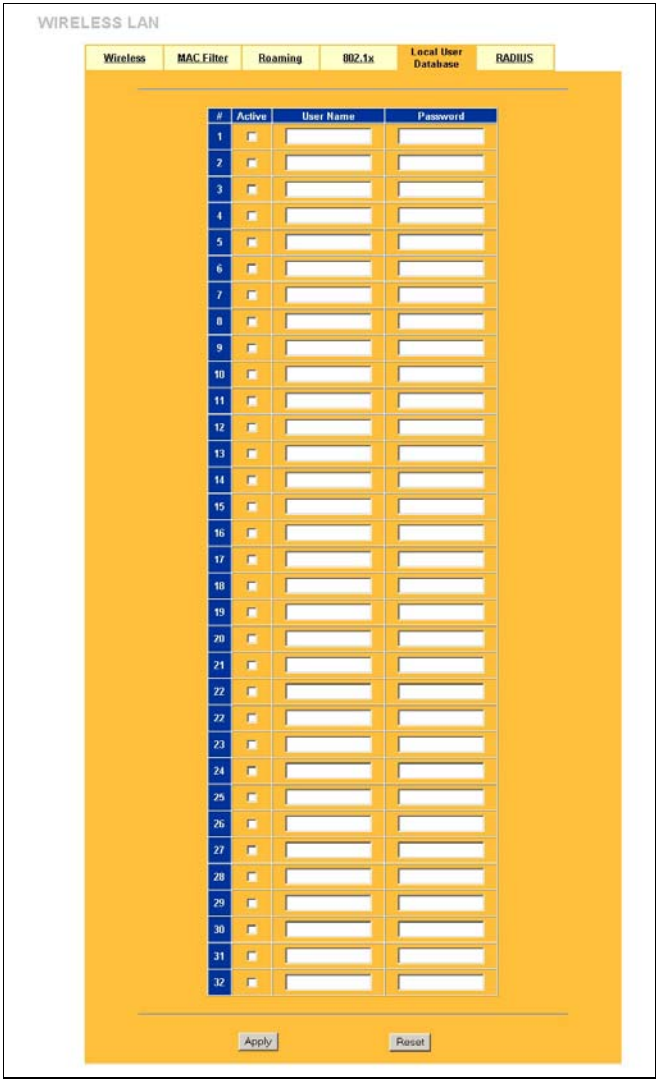
Table 6-3 802.1x Authentication

LABEL	DESCRIPTION
Authentication Databases	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password. Select **RADIUS Only** to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication.

6.10 Configuring Local User Database

To change your ZyAIR's local user database, click **ADVANCED**, **WIRELESS** and then the **Local User Database** tab. The screen appears as shown.



#	Active	User Name	Password
1	☐		
2	☐		
3	☐		
4	☐		
5	☐		
6	☐		
7	☐		
8	☐		
9	☐		
10	☐		
11	☐		
12	☐		
13	☐		
14	☐		
15	☐		
16	☐		
17	☐		
18	☐		
19	☐		
20	☐		
21	☐		
22	☐		
22	☐		
23	☐		
24	☐		
25	☐		
26	☐		
27	☐		
28	☐		
29	☐		
30	☐		
31	☐		
32	☐		

Figure 6-7 Local User Database

The following table describes the fields in this screen.

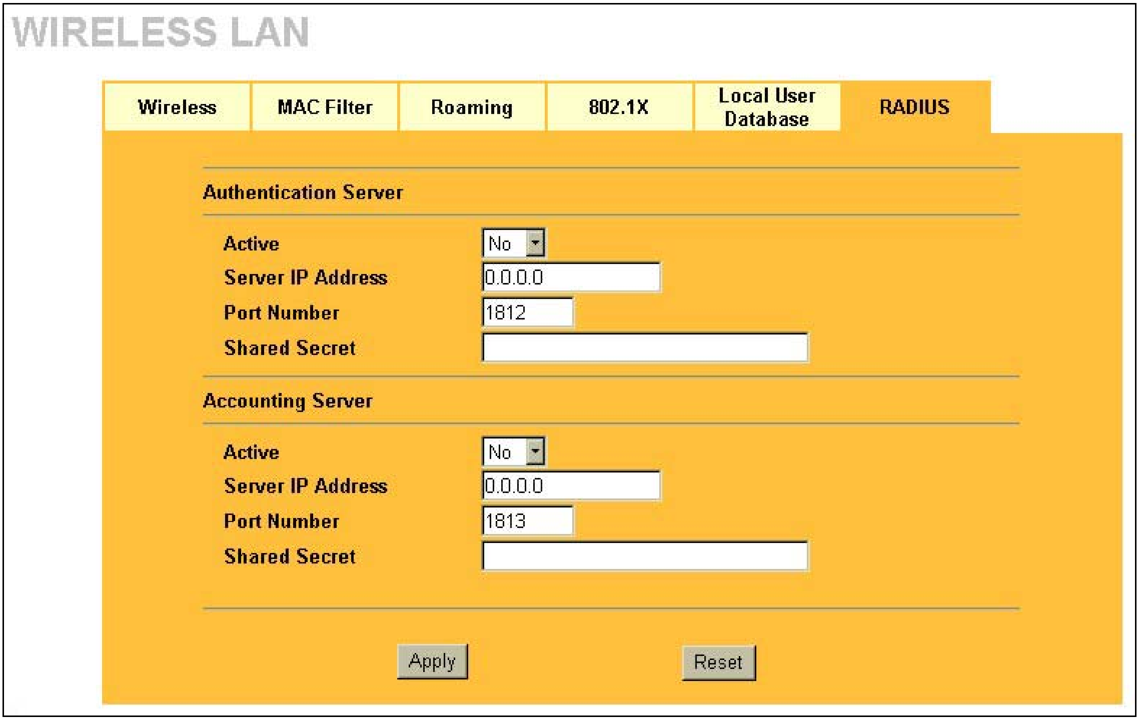
Table 6-4 Local User Database

LABEL	DESCRIPTION
Active	Select this check box to activate the user profile.
User Name	Enter the username (up to 31 characters) for this user profile.
Password	Type a password (up to 31 characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

6.11 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using an external server.

To set up your ZyAIR's RADIUS server settings, click **ADVANCED**, **WIRELESS** and then the **RADIUS** tab. The screen appears as shown.



Authentication Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Accounting Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

Figure 6-8 RADIUS

The following table describes the fields in this screen.

Table 6-5 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user profile on the ZyAIR.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.

Table 6-5 RADIUS

LABEL	DESCRIPTION
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Part III:

IP AND LOGS

This part provides information and configuration instructions for the IP screen and for the logs.

Chapter 7
IP Screen

This chapter discusses how to configure IP settings on the ZyAIR

7.1 Factory Ethernet Defaults

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

- IP address of 192.168.1.2
- Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

7.2 TCP/IP Parameters

7.2.1 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section for this information.

7.2.2 WAN IP Address Assignment

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

Table 7-1 Private IP Address Ranges

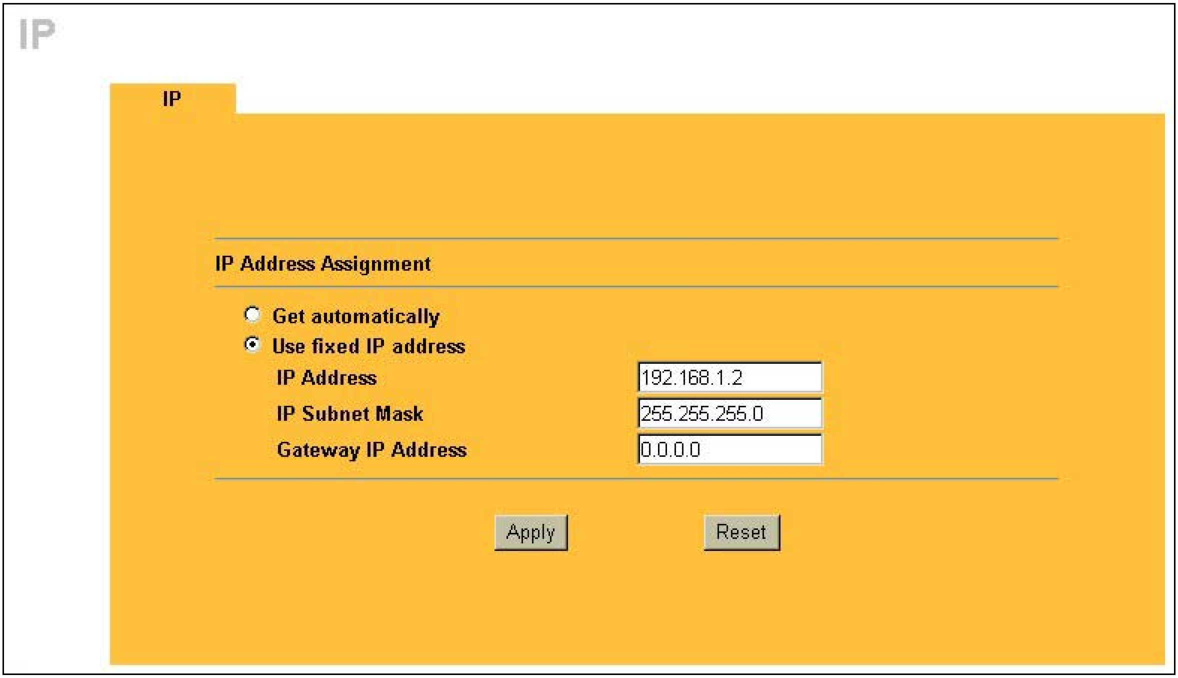
10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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.

7.3 Configuring IP Address

Click **ADVANCED** and then **IP** to display the screen shown next.



IP Address Assignment

○ Get automatically
● Use fixed IP address

IP Address	192.168.1.2
IP Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0

Figure 7-1 IP Setup

The following table describes the fields in this screen.

Table 7-2 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	

Table 7-2 IP Setup

LABEL	DESCRIPTION
Get automatically	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time. **You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.**
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	Enter the IP address of your ZyAIR in dotted decimal notation. **If you change the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.**
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; over the WAN, the gateway must be the IP address of one of the remote node.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 8
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.

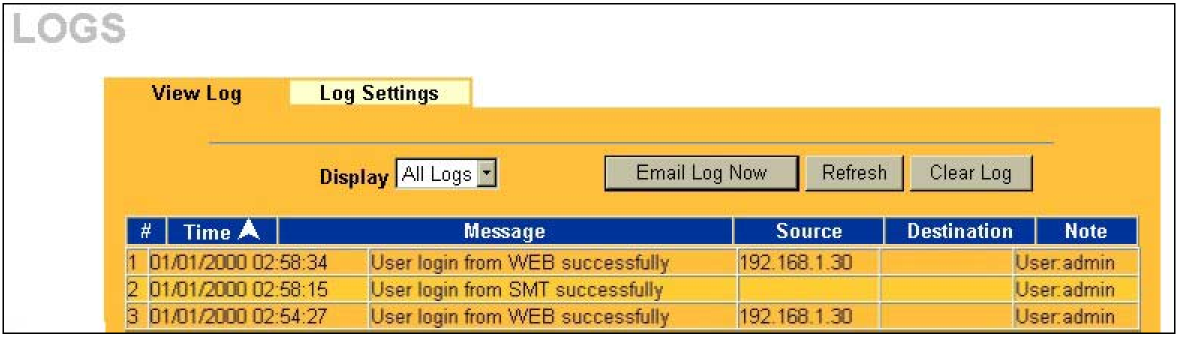
8.1 Displaying Logs

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

Click **ADVANCED** and then **LOGS** 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 8.2*). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the 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.



#	Time ▲	Message	Source	Destination	Note
1	01/01/2000 02:58:34	User login from WEB successfully	192.168.1.30		User:admin
2	01/01/2000 02:58:15	User login from SMT successfully			User:admin
3	01/01/2000 02:54:27	User login from WEB successfully	192.168.1.30		User:admin

Figure 8-1 View Log

The following table describes the fields in this screen.

Table 8-1 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.

Table 8-1 View Log

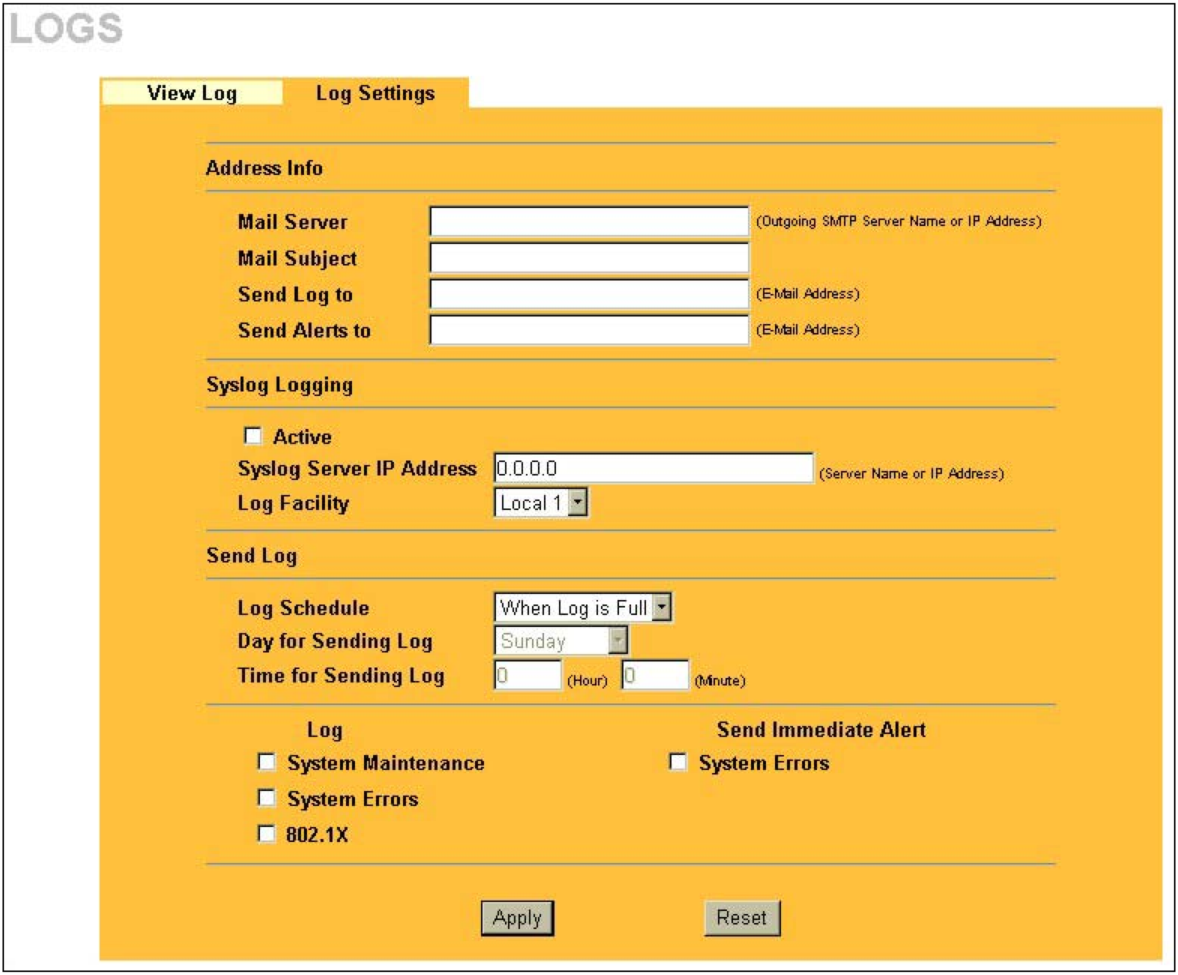
LABEL	DESCRIPTION
#	This is the index number of the log entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination 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.

8.2 Configuring Log Settings

To change your ZyAIR's log settings, click **ADVANCED**, **LOGS** 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

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
□ 802.1X

Send Immediate Alert
□ System Errors

Figure 8-2 Log Settings

The following table describes the fields in this screen.

Table 8-2 Log Settings

LABEL	DESCRIPTION
Address Info	

Table 8-2 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	Syslog logging sends a log to an external UNIX server used to store logs.
Active	Click **Active** to enable Syslog Logging.
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	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When the Log is Full** • **None.** 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.
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 8-2 Log Settings

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyAIR to send immediately 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 screens.

Chapter 9 Maintenance

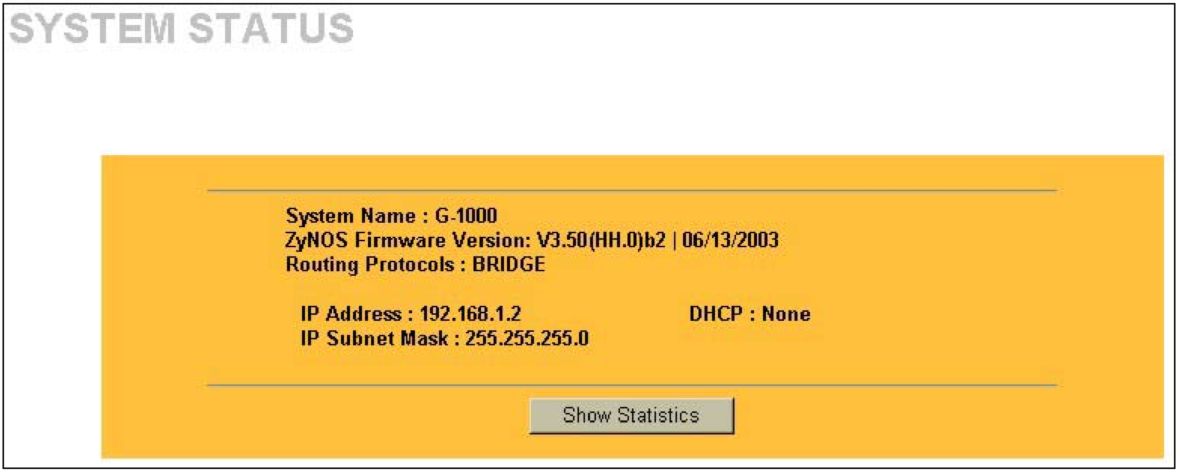
This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

9.1 Maintenance Overview

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

9.2 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.



SYSTEM STATUS

System Name : G-1000
ZyNOS Firmware Version: V3.50(HH.0)b2 | 06/13/2003
Routing Protocols : BRIDGE

IP Address : 192.168.1.2
DHCP : None
IP Subnet Mask : 255.255.255.0

Figure 9-1 System Status

The following table describes the fields in this screen.

Table 9-1 System Status

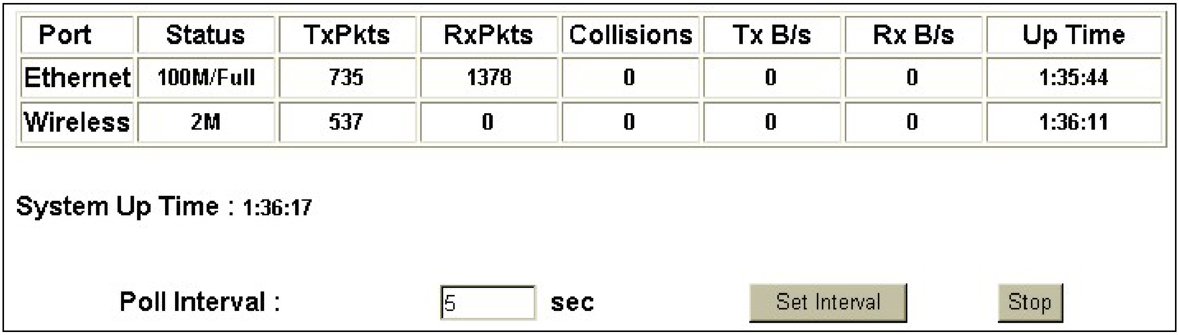
LABEL	DESCRIPTION
System Name	This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes

Table 9-1 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.
Routing Protocols	This shows the routing protocol – **BRIDGE** for which the ZyAIR is configured.
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.

9.2.1 System Statistics

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



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
Ethernet	100M/Full	735	1378	0	0	0	1:35:44
Wireless	2M	537	0	0	0	0	1:36:11

System Up Time : 1:36:17

Poll Interval : 5 sec

Figure 9-2 System Status: Show Statistics

The following table describes the fields in this screen.

Table 9-2 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port.

Table 9-2 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(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

9.3 Wireless Screen

9.3.1 Association List

View the wireless stations that are currently associated to the ZyAIR in the **Association List** screen. Click **MAINTENANCE** and then **WIRELESS** to display the screen as shown next.

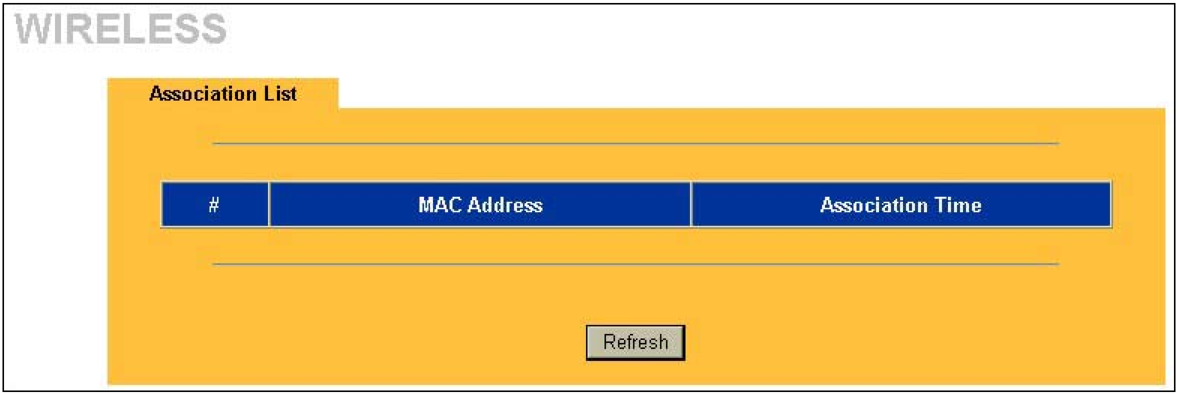


Figure 9-3 Association List

The following table describes the fields in this screen.

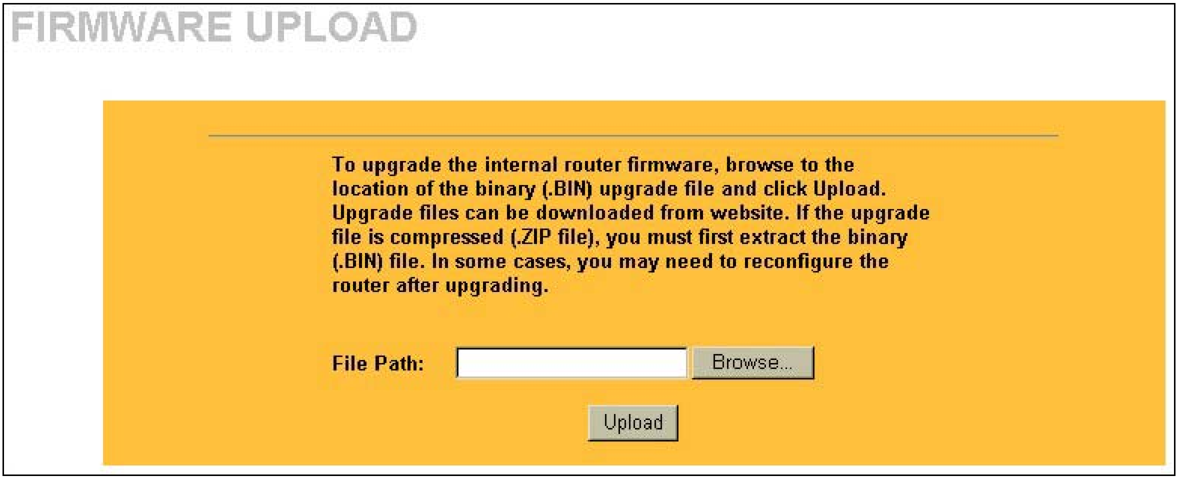
Table 9-3 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyAIR.
Refresh	Click **Refresh** to reload the screen.

9.4 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 TFTP (Trivial File 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 **MAINTENANCE** and then **F/W UPLOAD**. 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 9-4 Firmware Upload

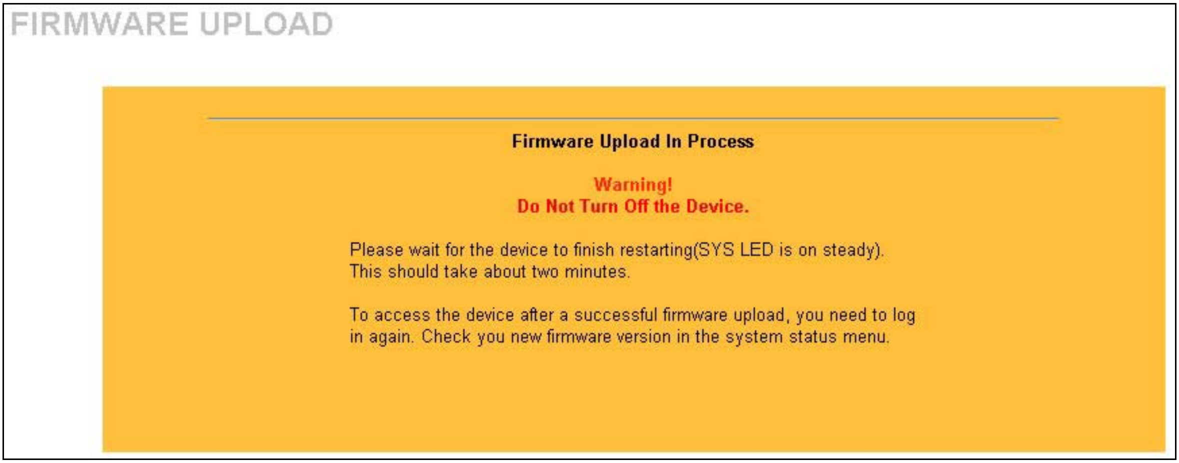
The following table describes the fields in this screen.

Table 9-4 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.

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

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



FIRMWARE UPLOAD

Firmware Upload In Process

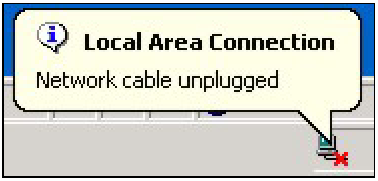
Warning!
Do Not Turn Off the Device.

Please wait for the device to finish restarting(SYS LED is on steady).
This should take about two minutes.

To access the device after a successful firmware upload, you need to log in again. Check you new firmware version in the system status menu.

Figure 9-5 Firmware Upload In Process

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

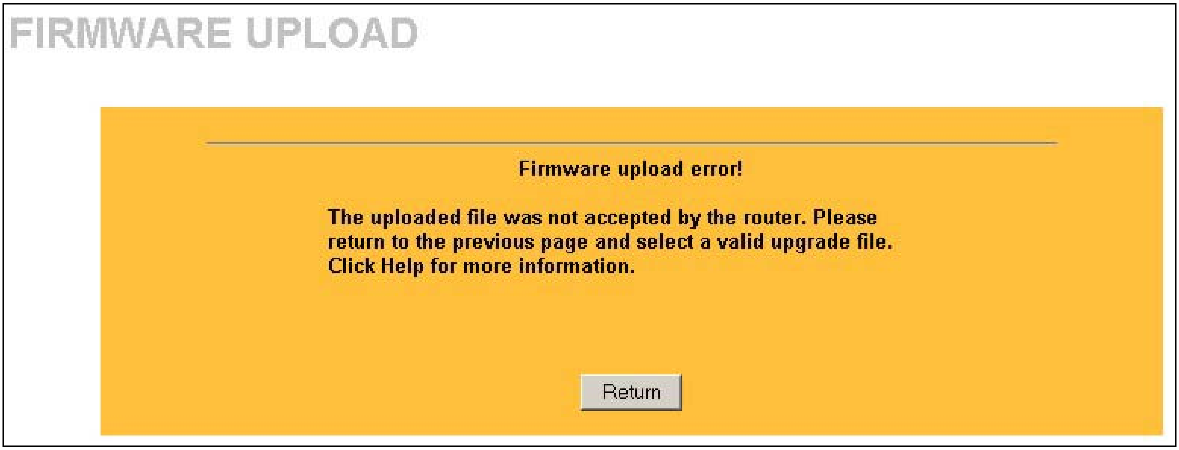


Local Area Connection
Network cable unplugged

Figure 9-6 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.



FIRMWARE UPLOAD

Firmware upload error!

The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

Figure 9-7 Firmware Upload Error

9.5 Configuration Screen

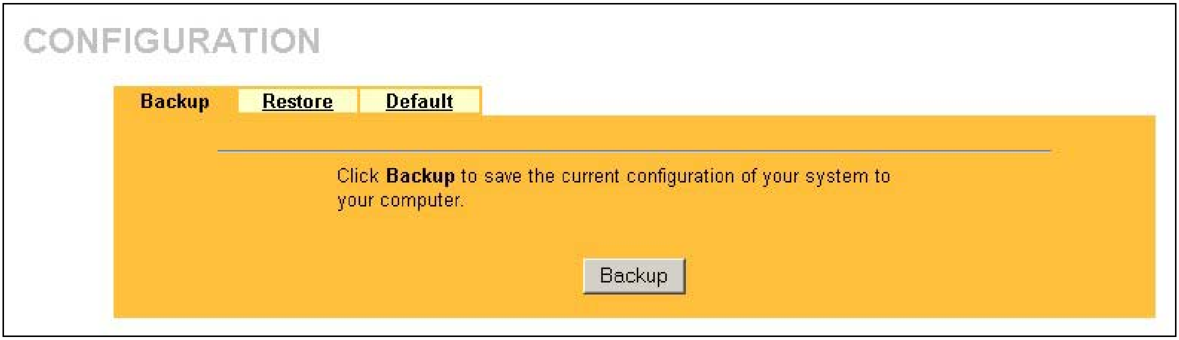
The web configurator uses TFTP to transfer files. See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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

9.5.1 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.



CONFIGURATION

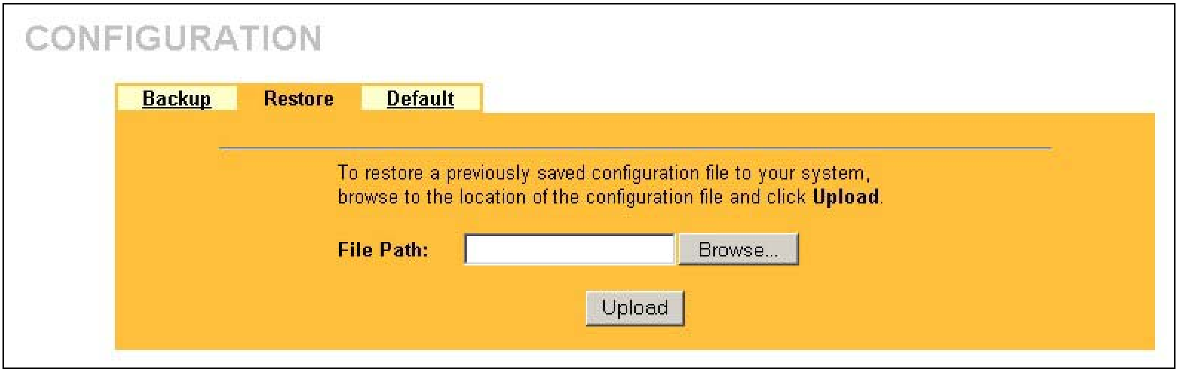
Click **Backup** to save the current configuration of your system to your computer.

Figure 9-8 Backup Configuration

9.5.2 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.



To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.

File Path:

Figure 9-9 Restore Configuration

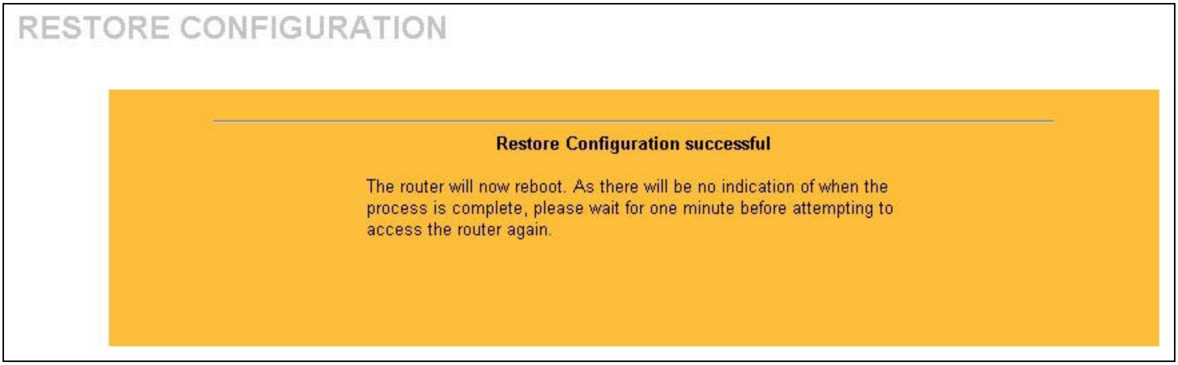
The following table describes the fields in this screen.

Table 9-5 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 device again.

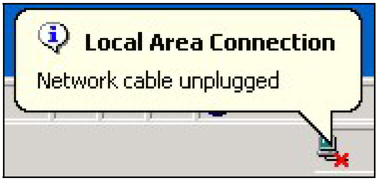

RESTORE CONFIGURATION

Restore Configuration successful

The router will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

Figure 9-10 Configuration Upload Successful

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

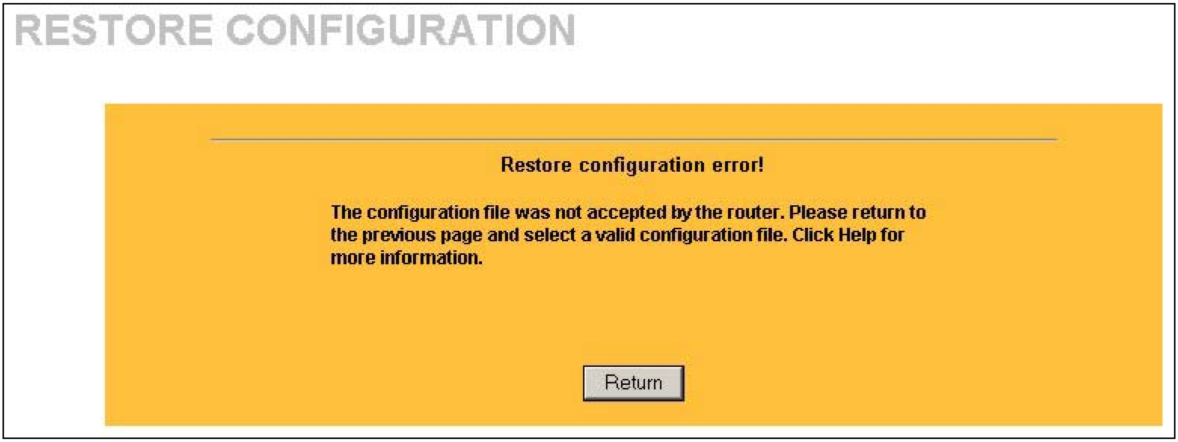

Local Area Connection

Network cable unplugged

Figure 9-11 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 device IP address (192.168.1.2). 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.



RESTORE CONFIGURATION

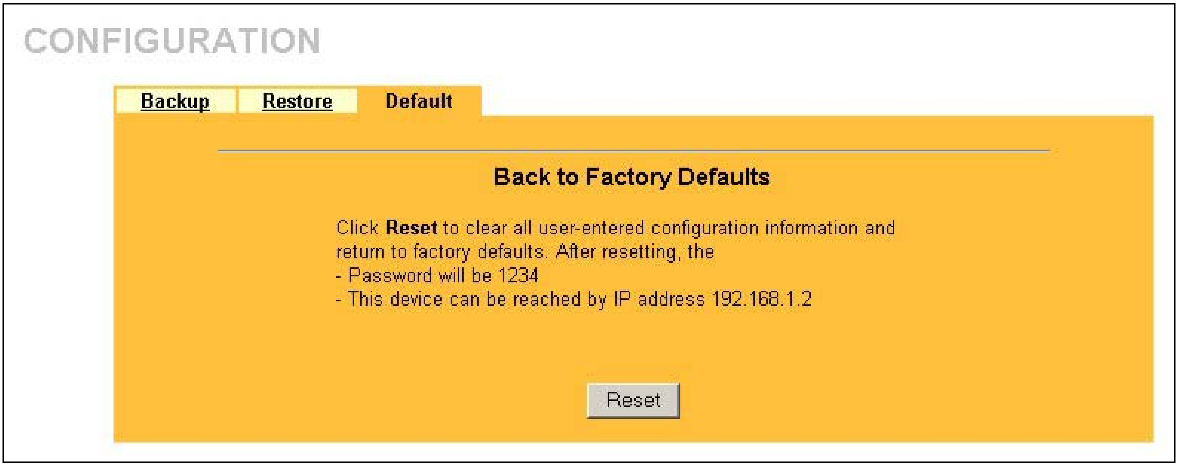
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

Figure 9-12 Configuration Upload Error

9.5.3 Back to Factory Defaults

Pressing 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.



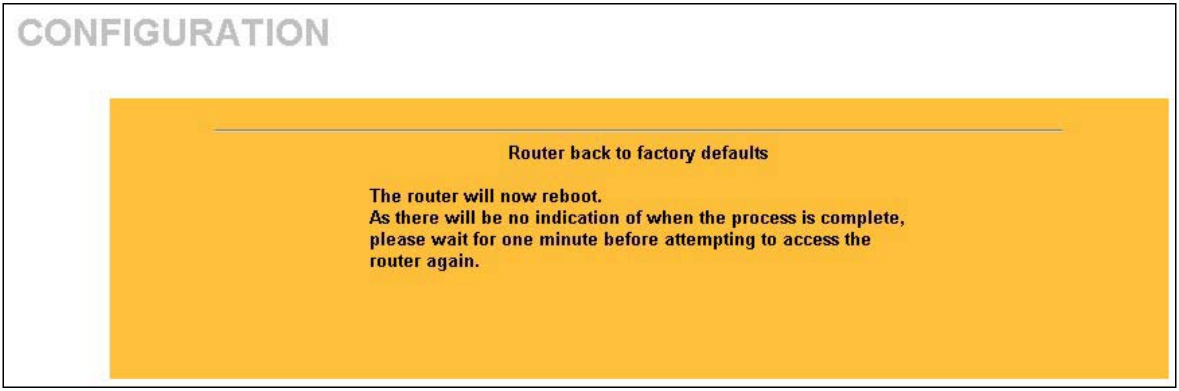
CONFIGURATION

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- This device can be reached by IP address 192.168.1.2

Figure 9-13 Back to Factory Default

The following warning screen will appear.



Router back to factory defaults

The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

Figure 9-14 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 chapter on top panel connections 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 10
Introducing the SMT

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

10.1 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 192.168.1.2" (the default IP address) and click **OK**.

Step 2. Enter "1234" in the **Password** field.

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.

10.2 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "*" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyAIR will automatically log you out. You may change inactivity timer using the web configurator or the CI commands.

```
Password : xxxx
```

Figure 10-1 Login Screen

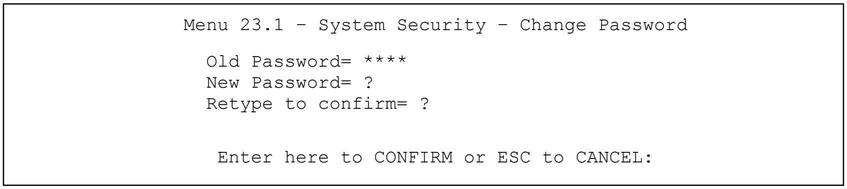
10.3 Changing the System Password

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 10-2 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.

10.4 ZyAIR SMT Menu Overview Example

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

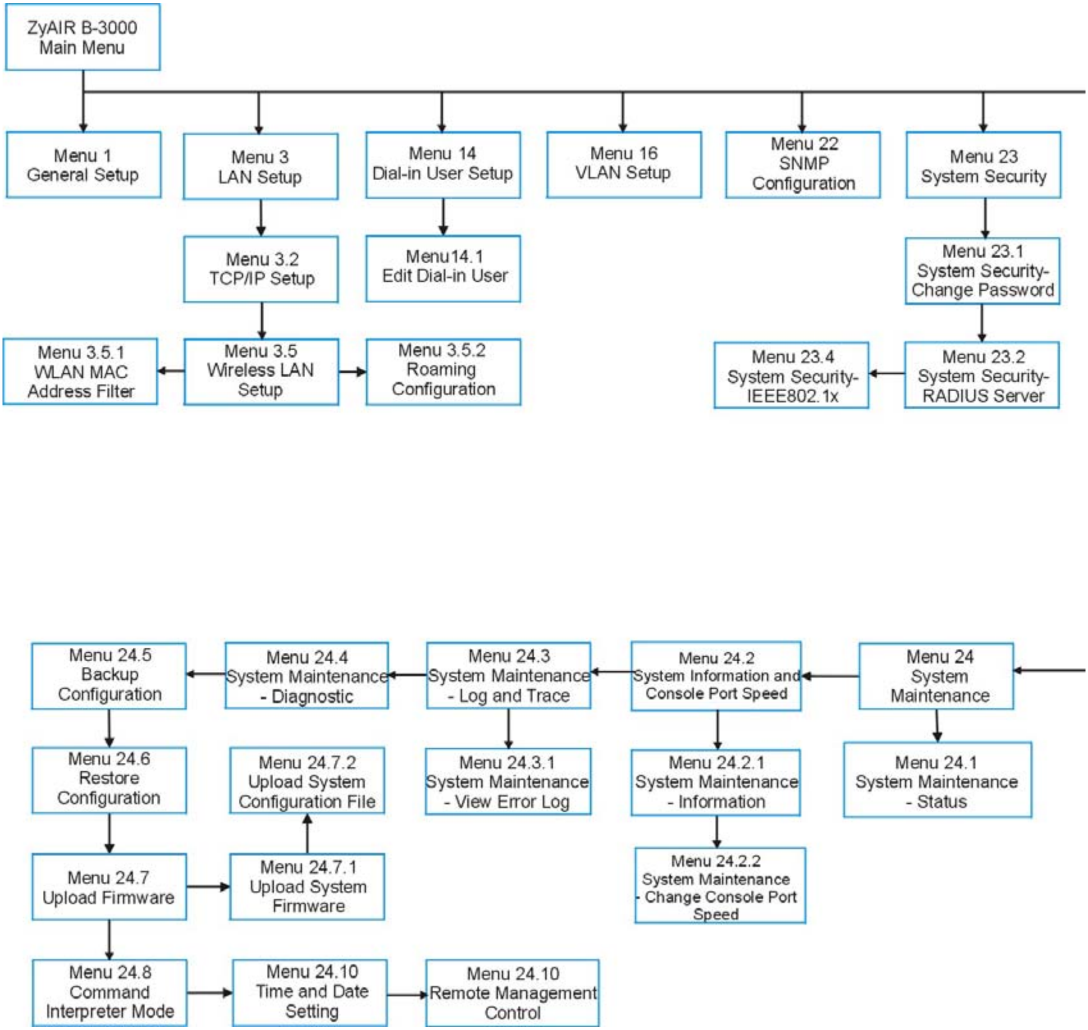


Figure 10-3 SMT Menu Overview

10.5 Navigating the SMT Interface

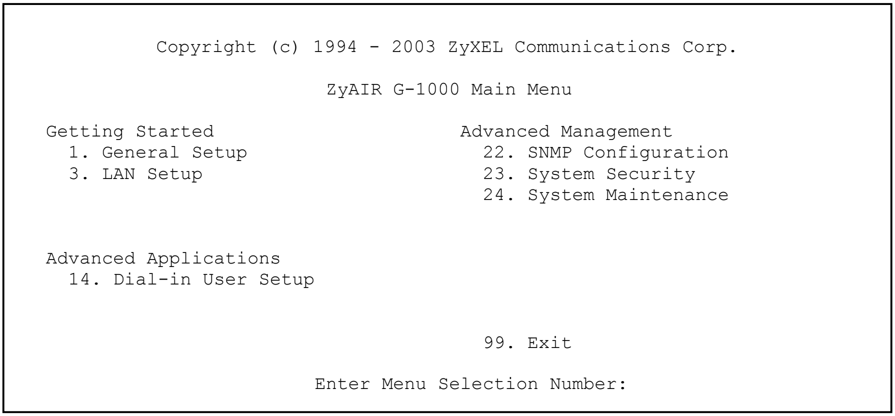
The SMT (System Management Terminal) is the interface that you use to configure your ZyAIR.

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

Table 10-1 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 G-1000 Main Menu

     Getting Started                      Advanced Management
       1. General Setup                     22. SNMP Configuration
       3. LAN Setup                         23. System Security
                                            24. System Maintenance


     Advanced Applications
       14. Dial-in User Setup


                                            99. Exit

                              Enter Menu Selection Number:
```

Figure 10-4 SMT Main Menu

10.5.1 System Management Terminal Interface Summary

Table 10-2 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.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyAIR.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password and enable network user authentication.
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 11 General Setup

The chapter shows you the information on general setup.

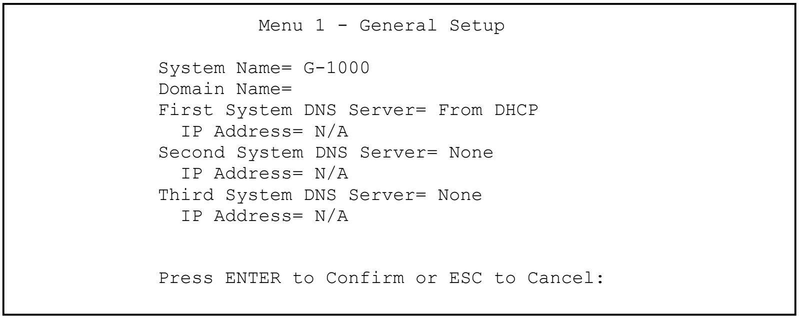
11.1 General Setup

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** field is not a required field. Leave this field blank or enter the domain name here if you know it.

11.1.1 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= G-1000
        Domain Name=
        First System DNS Server= From DHCP
          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 11-1 Menu 1 General Setup

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

Table 11-1 Menu 1 General Setup

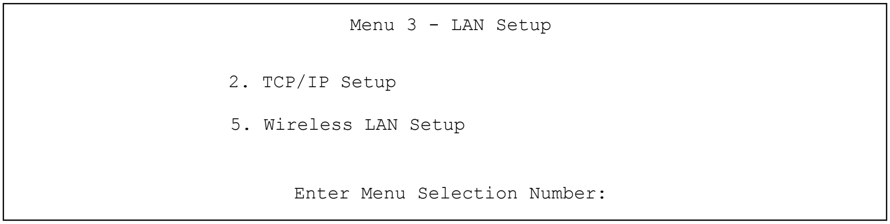
FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted.	**G-1000**
Domain Name	This is not a required field. Leave this field blank or 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].	**From DHCP**
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 12
LAN Setup

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

12.1 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:
```

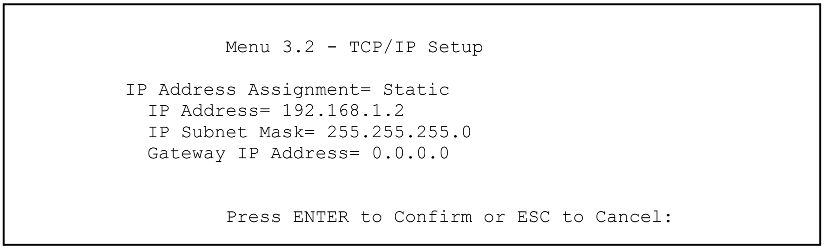
Figure 12-1 Menu 3 LAN Setup

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

12.2 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= 192.168.1.2
            IP Subnet Mask= 255.255.255.0
            Gateway IP Address= 0.0.0.0


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

Figure 12-2 Menu 3.2 TCP/IP Setup

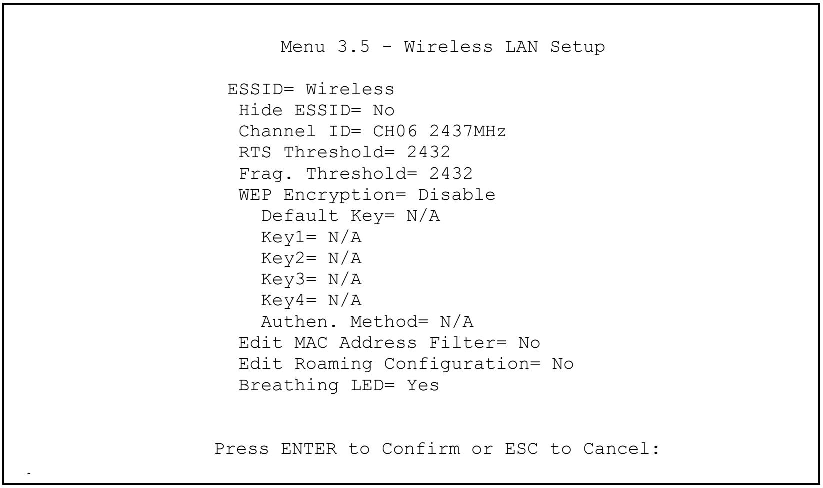
Follow the instructions in the following table on how to configure the DHCP fields.

Table 12-1 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.	
IP Address	Enter the (LAN) IP address of your ZyAIR in dotted decimal notation	192.168.1.2
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 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.		

12.3 Wireless LAN Setup

Use menu 3.5 to set up your ZyAIR as the wireless access point. 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

               ESSID= Wireless
                Hide ESSID= No
                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
                Edit MAC Address Filter= No
                Edit Roaming Configuration= No
                Breathing LED= Yes


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

Figure 12-3 Menu 3.5 Wireless LAN Setup

The following table describes the fields in this menu.

Table 12-2 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP the wireless station is to associate to. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name up to 32 printable 7-bit ASCII characters. This field is only available when you select **Access Point** in the **Operating Mode** field.	Wireless
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing data frame so a intruder cannot obtain the ESSID through passive scanning.	**No**
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	**CH06 2437MHz**
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 12-2 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"). **Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.**	0x12345abcde
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**
Edit MAC Address Filter	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER] to configure a list of MAC addresses that may be allowed or denied access to your ZyAIR.	**No**
Edit Roaming Configuration	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER] to configure your ZyAIR for roaming.	**No**
Breathing LED	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER]. The blue ZyAIR LED is on (dimmed) when the ZyAIR is on and blinks brightly (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.	
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.		

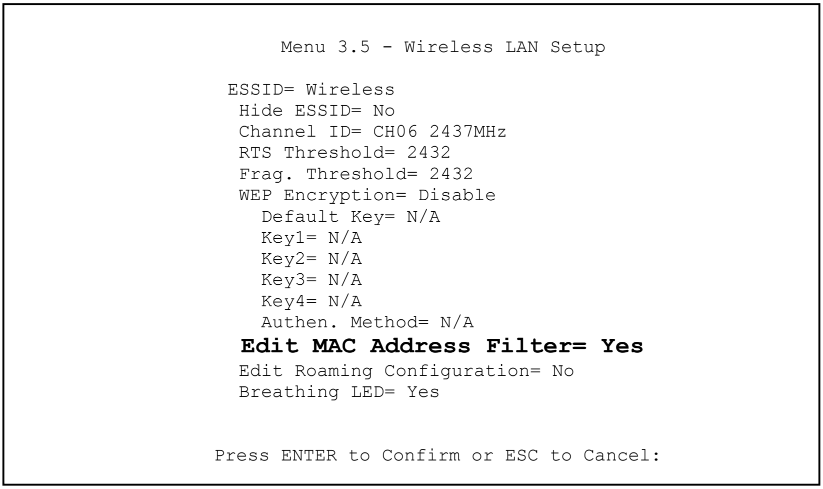
12.3.1 Configuring MAC Address Filtering

Your ZyAIR checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyAIR.

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

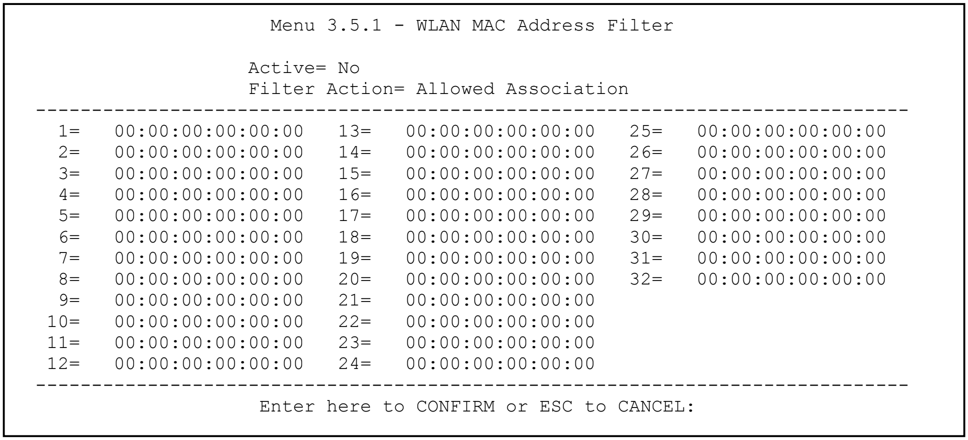
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
      Menu 3.5 - Wireless LAN Setup

 ESSID= Wireless
  Hide ESSID= No
  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
  Edit MAC Address Filter= Yes
  Edit Roaming Configuration= No
  Breathing LED= Yes


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

Figure 12-4 Menu 3.5 Wireless LAN Setup

Step 3. In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.



```
                        Menu 3.5.1 - WLAN MAC Address Filter

                      Active= No
                      Filter Action= Allowed Association
------------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------------
                    Enter here to CONFIRM or ESC to CANCEL:
```

Figure 12-5 Menu 3.5.1 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 12-3 Menu 3.5.1 WLAN MAC Address Filter

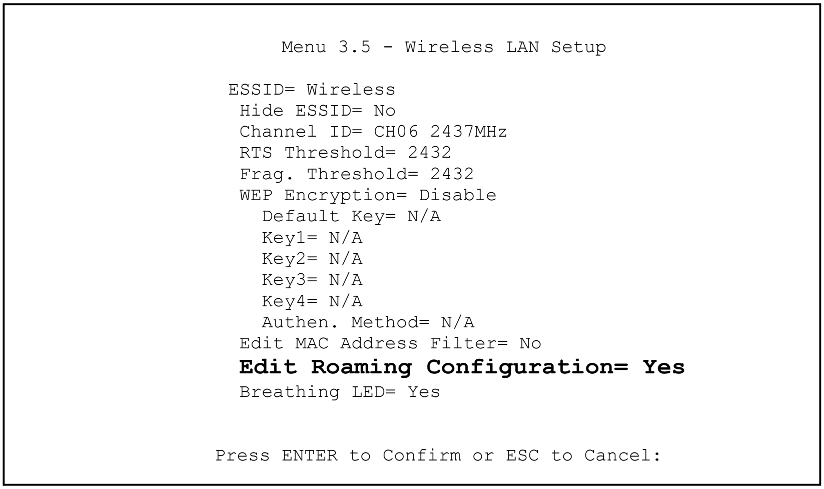
FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyAIR, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the ZyAIR. MAC addresses not listed will be denied access to the router.
1…32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyAIR in these address fields.
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.	

12.3.2 Configuring Roaming

Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

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

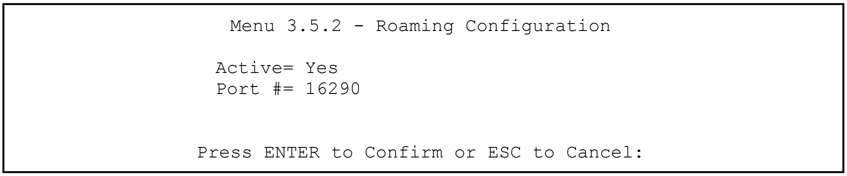
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
                    Menu 3.5 - Wireless LAN Setup

               ESSID= Wireless
                Hide ESSID= No
                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
                Edit MAC Address Filter= No
                Edit Roaming Configuration= Yes
                Breathing LED= Yes


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

Figure 12-6 Menu 3.5 Wireless LAN Setup

Step 3. Move the cursor to the **Edit Roaming Configuration** field. Press [SPACE BAR] to select **Yes** and then press [ENTER]. **Menu 3.5.2 – Roaming Configuration** displays as shown next.



```
                  Menu 3.5.2 - Roaming Configuration

                 Active= Yes
                 Port #= 16290


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

Figure 12-7 Menu 3.5.2 Roaming Configuration

The following table describes the fields in this menu.

Table 12-4 Menu 3.5.2 Roaming Configuration

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.

Table 12-4 Menu 3.5.2 Roaming Configuration

FIELD	DESCRIPTION
Port #	Type the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **16290**. Make sure this port is not used by other services.
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 13
Dial-in User Setup

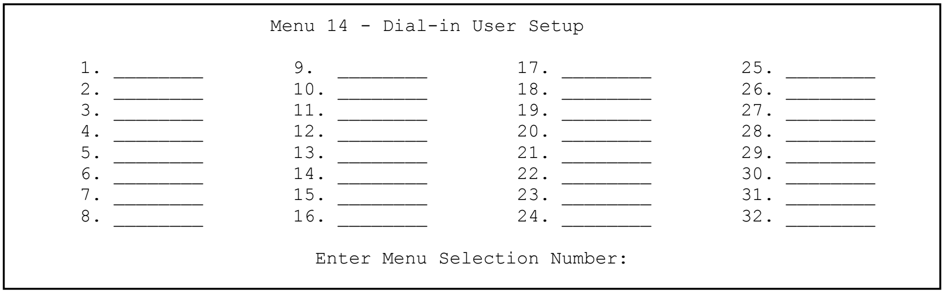
This chapter shows you how to create user accounts on the ZyAIR.

13.1 Dial-in User Setup

By storing user profiles locally, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your ZyAIR.

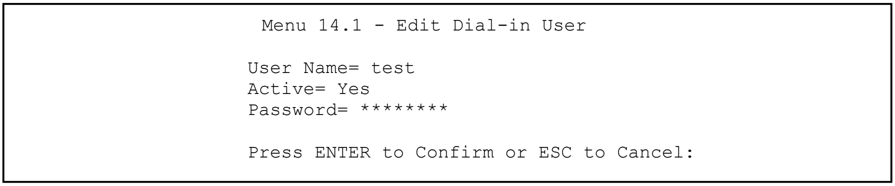
Step 1. From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.



```
                        Menu 14 - Dial-in User Setup

       1. ________        9.  ________       17. ________       25. ________
       2. ________        10. ________       18. ________       26. ________
       3. ________        11. ________       19. ________       27. ________
       4. ________        12. ________       20. ________       28. ________
       5. ________        13. ________       21. ________       29. ________
       6. ________        14. ________       22. ________       30. ________
       7. ________        15. ________       23. ________       31. ________
       8. ________        16. ________       24. ________       32. ________

                          Enter Menu Selection Number:
```

Figure 13-1 Menu 14- Dial-in User Setup

Step 2. Type a number and press [ENTER] to edit the user profile.



```
                       Menu 14.1 - Edit Dial-in User

                      User Name= test
                      Active= Yes
                      Password= ********

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

Figure 13-2 Menu 14.1- Edit Dial-in User

The following table describes the fields in this screen.

Table 13-1 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
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 14
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

14.1 SNMP Overview

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.

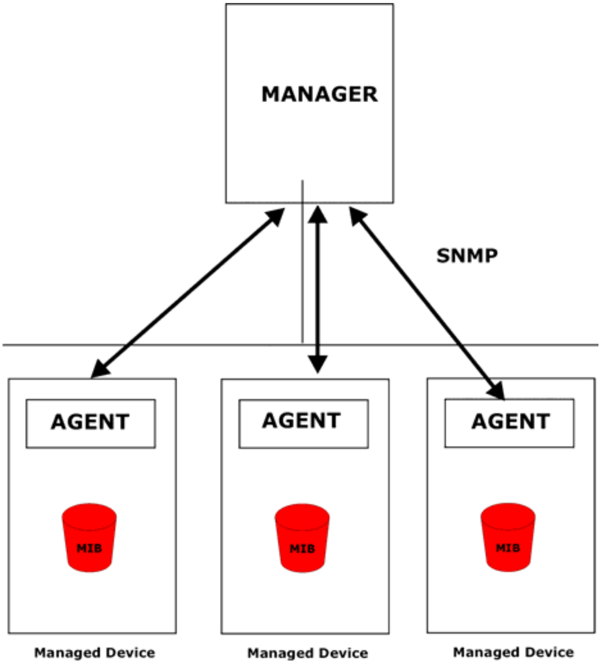


Figure 14-1 SNMP Management Model

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:

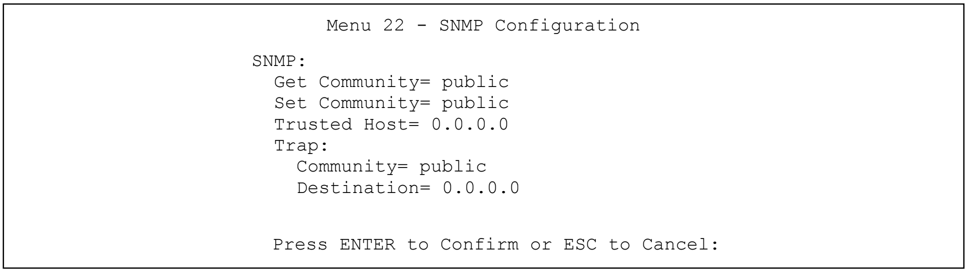
- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed 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.

14.2 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.

14.3 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 14-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 14-1 SNMP Configuration Menu Fields

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.		

14.4 SNMP Traps

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

Table 14-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 14-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	DSL

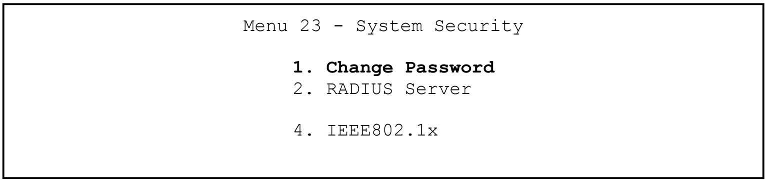
Chapter 15 System Security

This chapter describes how to configure the system security on the ZyAIR.

15.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

15.1.1 System Password



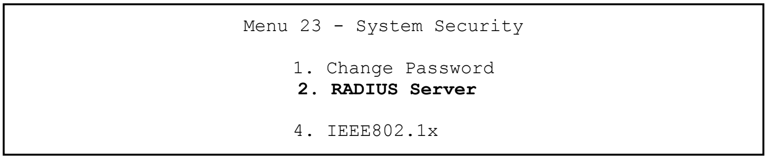
```
                Menu 23 - System Security

                     1. Change Password
                     2. RADIUS Server

                     4. IEEE802.1x
```

Figure 15-1 Menu 23 System Security

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the ZyAIR in the *Introducing the Web Configurator* chapter.

15.1.2 Configuring External RADIUS Server

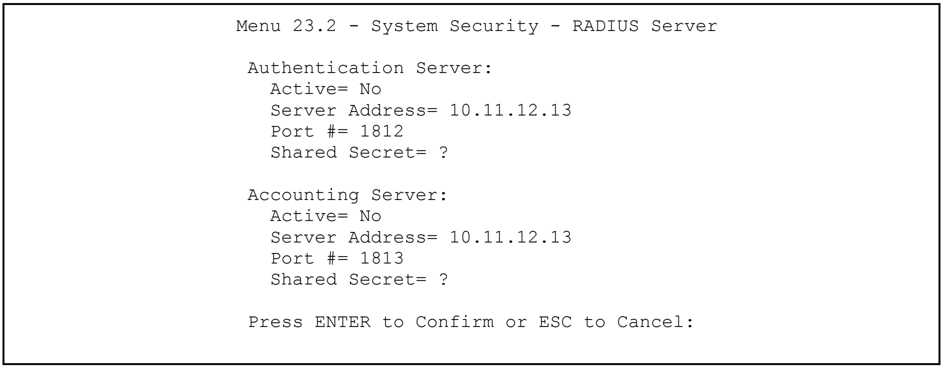
Enter 23 in the main menu to display **Menu 23 – System Security**.



```
                Menu 23 - System Security

                     1. Change Password
                     2. RADIUS Server

                     4. IEEE802.1x
```

Figure 15-2 Menu 23 System Security

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 – System Security – RADIUS Server** as shown next.



```
                    Menu 23.2 - System Security - RADIUS Server

                     Authentication Server:
                       Active= No
                       Server Address= 10.11.12.13
                       Port #= 1812
                       Shared Secret= ?

                     Accounting Server:
                       Active= No
                       Server Address= 10.11.12.13
                       Port #= 1813
                       Shared Secret= ?

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

Figure 15-3 Menu 23.2 System Security: RADIUS Server

The following table describes the fields in this menu.

Table 15-1 Menu 23.2 System Security: RADIUS Server

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.	**No**
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1812**
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyAIR.	
Accounting Server		
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.	**No**
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13

Table 15-1 Menu 23.2 System Security: RADIUS Server

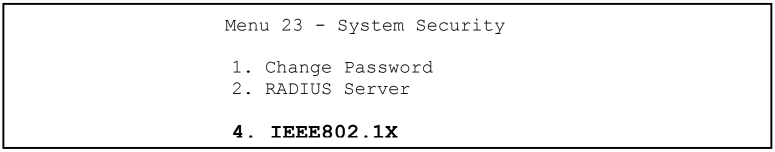
FIELD	DESCRIPTION	EXAMPLE
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1813**
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and 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.		

15.1.3 IEEE 802.1x

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

Follow the steps below to enable EAP authentication on your ZyAIR.

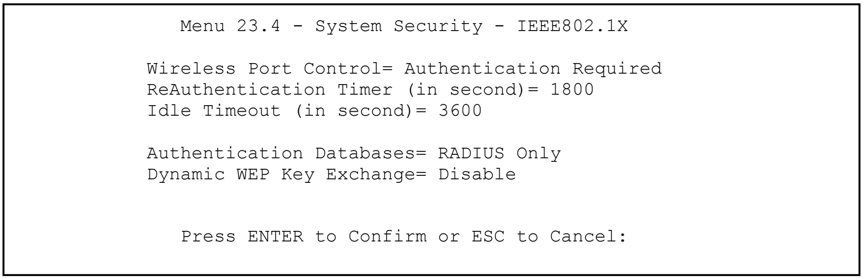
Step 1. From the main menu, enter 23 to display **Menu23 – System Security**.



```
                    Menu 23 - System Security

                     1. Change Password
                     2. RADIUS Server

                     4. IEEE802.1X
```

Figure 15-4 Menu 23 System Security

Step 2. Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.



```
                Menu 23.4 - System Security - IEEE802.1X

             Wireless Port Control= Authentication Required
             ReAuthentication Timer (in second)= 1800
             Idle Timeout (in second)= 3600

             Authentication Databases= RADIUS Only
             Dynamic WEP Key Exchange= Disable


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

Figure 15-5 Menu 23.4 System Security : IEEE802.1x

The following table describes the fields in this menu.

Table 15-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **No Access Allowed** to block all wireless stations access to the wired network.
ReAuthentication Timer (in seconds)	Specify how often a wireless station has to re-enter username and password to stay connected to the wired network. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).

Table 15-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Authentication Databases	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this field to decide which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password. Select **RADIUS Only** to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange.
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.	

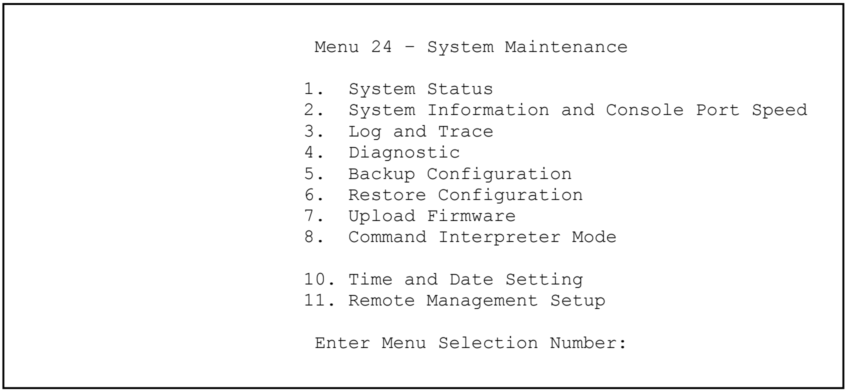
Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication

Chapter 16
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

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

                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

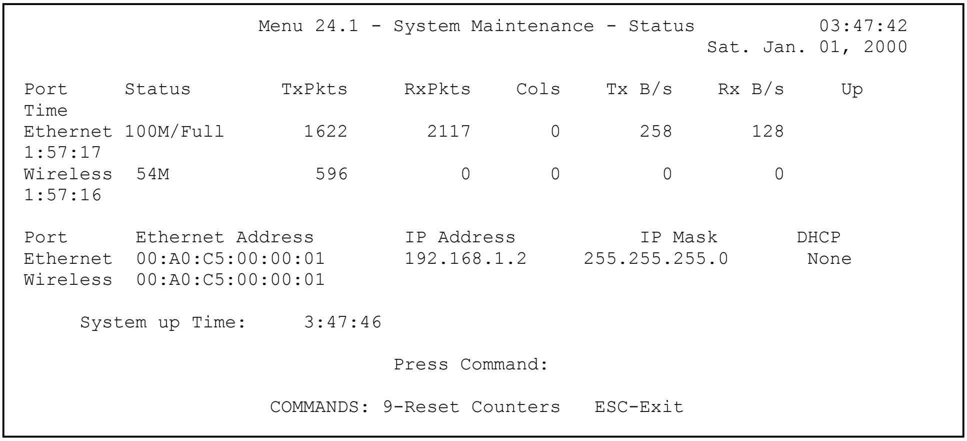
Figure 16-1 Menu 24 System Maintenance

16.1 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 1 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.



```
                      Menu 24.1 - System Maintenance - Status           03:47:42
                                                                Sat. Jan. 01, 2000

 Port      Status        TxPkts     RxPkts    Cols    Tx B/s    Rx B/s     Up
 Time
 Ethernet 100M/Full       1622       2117       0       258       128
 1:57:17
 Wireless  54M             596          0       0         0         0
 1:57:16

 Port      Ethernet Address         IP Address          IP Mask       DHCP
 Ethernet  00:A0:C5:00:00:01       192.168.1.2     255.255.255.0       None
 Wireless  00:A0:C5:00:00:01

      System up Time:     3:47:46

                                Press Command:

                       COMMANDS: 9-Reset Counters   ESC-Exit
```

Figure 16-2 Menu 24.1 System Maintenance: Status

The following table describes the fields present in this menu.

Table 16-1 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.
System Up Time	This is the time the ZyAIR is up and running from the last reboot.

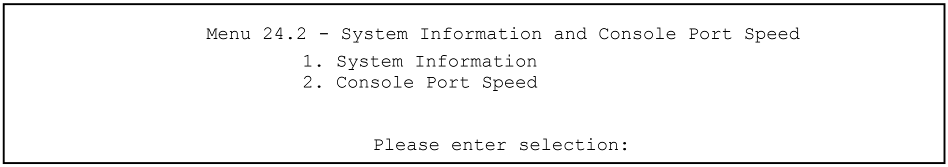
16.2 System Information and Console Port Speed

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:



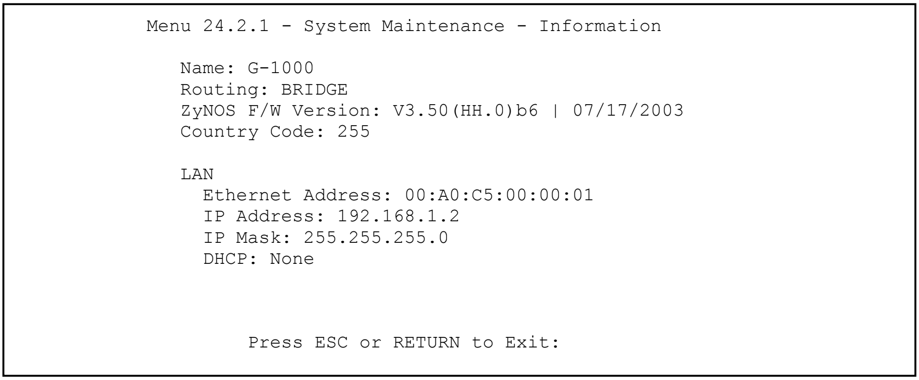
```
                  Menu 24.2 - System Information and Console Port Speed
                           1. System Information
                           2. Console Port Speed


                                 Please enter selection:
```

Figure 16-3 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.

16.2.1 System Maintenance- Information

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



```
             Menu 24.2.1 - System Maintenance - Information

                Name: G-1000
                Routing: BRIDGE
                ZyNOS F/W Version: V3.50(HH.0)b6 | 07/17/2003
                Country Code: 255

                LAN
                  Ethernet Address: 00:A0:C5:00:00:01
                  IP Address: 192.168.1.2
                  IP Mask: 255.255.255.0
                  DHCP: None



                      Press ESC or RETURN to Exit:
```

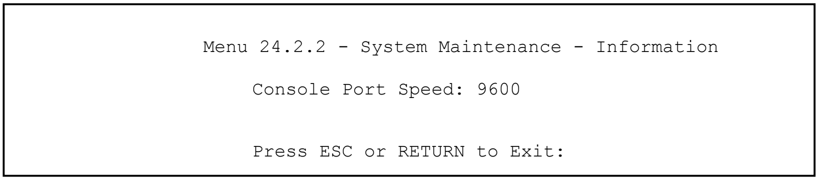
Figure 16-4 Menu 24.2.1 System Information: Information

Table 16-2 Menu 24.2.1 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) address 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. DHCP is not available for 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.	

16.2.2 System Maintenance- Information

Enter 2 in menu 24.2 to display the screen shown next. 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 115200bps. Use [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.



```
              Menu 24.2.2 - System Maintenance - Information

                  Console Port Speed: 9600


                  Press ESC or RETURN to Exit:
```

Figure 16-5 Menu 24.2.2 System Information: Change Console Port Speed

16.3 Log and Trace

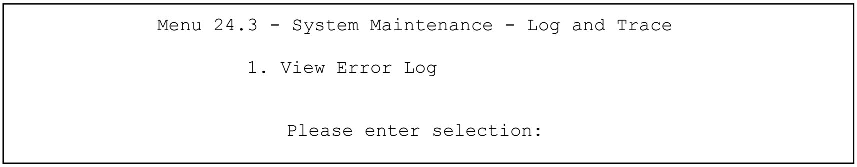
Your ZyAIR provides the error logs and trace records that are stored locally.

16.3.1 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**.

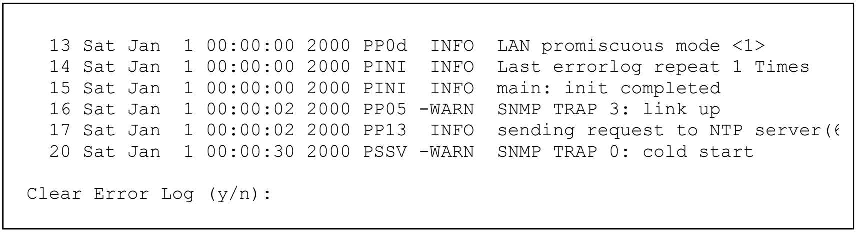


```
                    Menu 24.3 - System Maintenance - Log and Trace

                                1. View Error Log


                                    Please enter selection:
```

Figure 16-6 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.

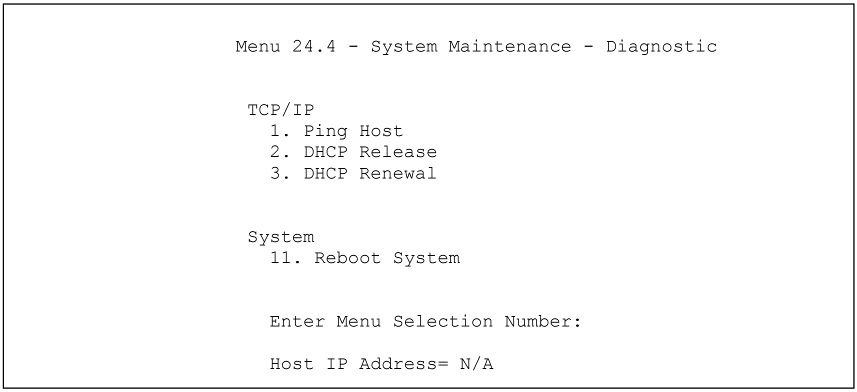


```
  13 Sat Jan  1 00:00:00 2000 PP0d  INFO  LAN promiscuous mode <1>
  14 Sat Jan  1 00:00:00 2000 PINI  INFO  Last errorlog repeat 1 Times
  15 Sat Jan  1 00:00:00 2000 PINI  INFO  main: init completed
  16 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
  17 Sat Jan  1 00:00:02 2000 PP13  INFO  sending request to NTP server(
  20 Sat Jan  1 00:00:30 2000 PSSV -WARN  SNMP TRAP 0: cold start

Clear Error Log (y/n):
```

Figure 16-7 Sample Error and Information Messages

16.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyAIR to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.



```
                    Menu 24.4 - System Maintenance - Diagnostic


                     TCP/IP
                       1. Ping Host
                       2. DHCP Release
                       3. DHCP Renewal


                     System
                       11. Reboot System


                       Enter Menu Selection Number:

                       Host IP Address= N/A
```

Figure 16-8 Menu 24.4 System Maintenance : Diagnostic

Follow the procedure next to get to display this menu:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4. Diagnostic to open **Menu 24.4** – **System Maintenance** – **Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for your ZyAIR and the connections.

Table 16-3 System Maintenance Menu : Diagnostic

FIELD	DESCRIPTION
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
DHCP Release	Release the IP address assigned by the DHCP server.
DHCP Renewal	Get a new IP address from the DHCP server.
Reboot System	Reboot the ZyAIR.
Host IP Address	If you typed 1 to Ping Host, now type the address of the computer you want to ping.

Chapter 17
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.

17.1 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 17-1 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.

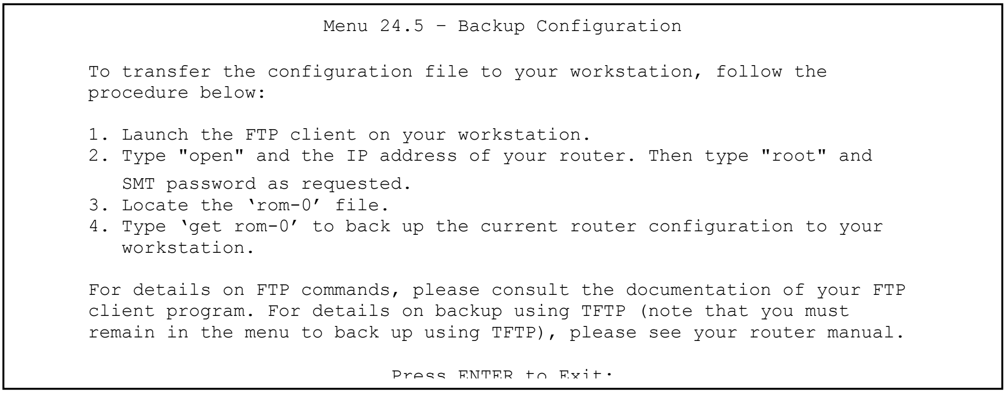
17.2 Backup Configuration

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.

17.2.1 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 17-1 Menu 24.5 Backup Configuration

17.2.2 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 17-2 FTP Session Example

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

Table 17-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. 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. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.

Table 17-2 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).

FTP over WAN will not work if you have disabled the FTP service in menu 24.11.

17.2.3 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.

17.2.4 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.

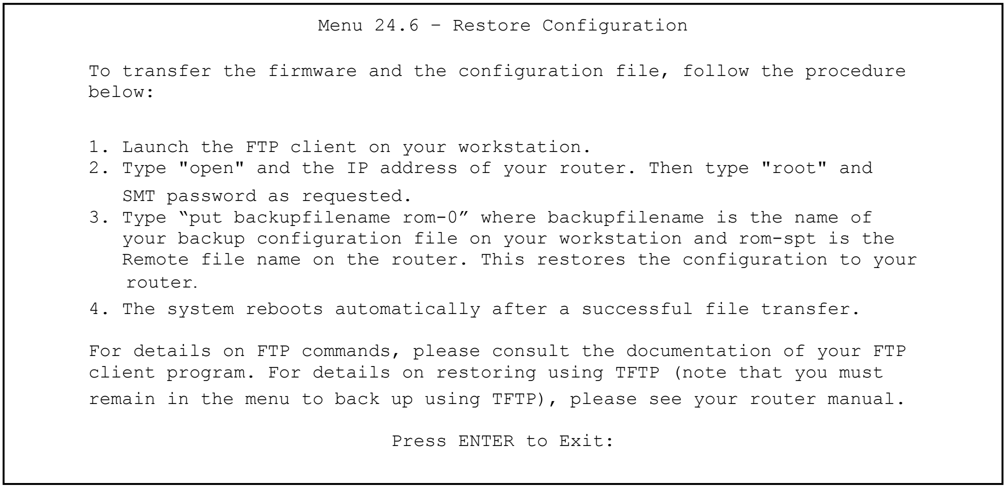
Table 17-3 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.2 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.

TFTP over WAN will not work if you have disabled the FTP service in menu 24.11.

17.3 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.



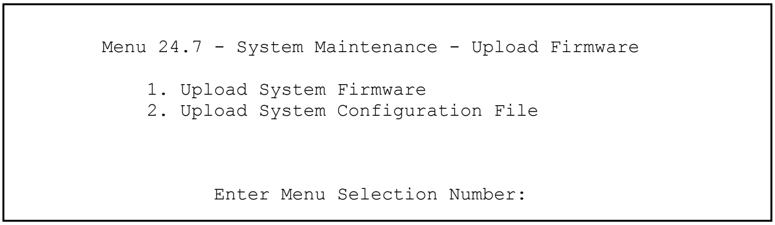
```
                    Menu 24.6 – Restore Configuration

To transfer the firmware and the configuration file, 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. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
   Remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring 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 17-3 Menu 24.6 Restore Configuration

17.4 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.



```
        Menu 24.7 - System Maintenance - Upload Firmware

            1. Upload System Firmware
            2. Upload System Configuration File



                  Enter Menu Selection Number:
```

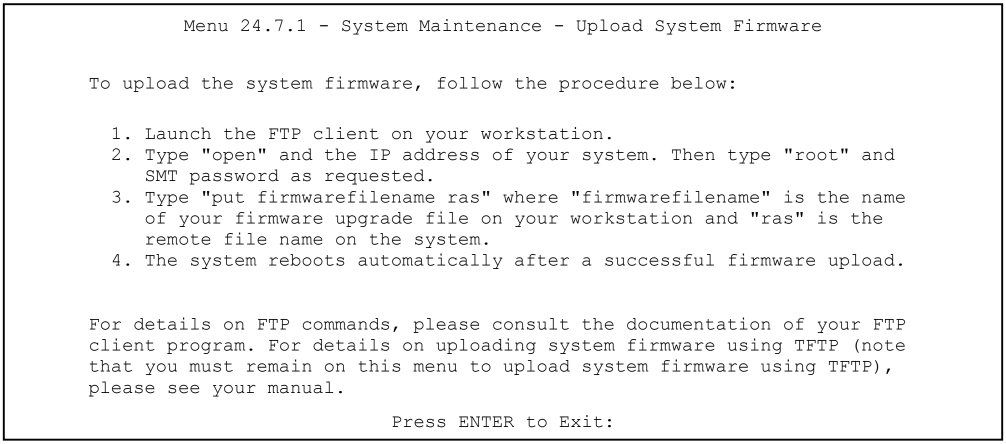
Figure 17-4 Menu 24.7 System Maintenance : Upload Firmware

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.

17.4.1 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.

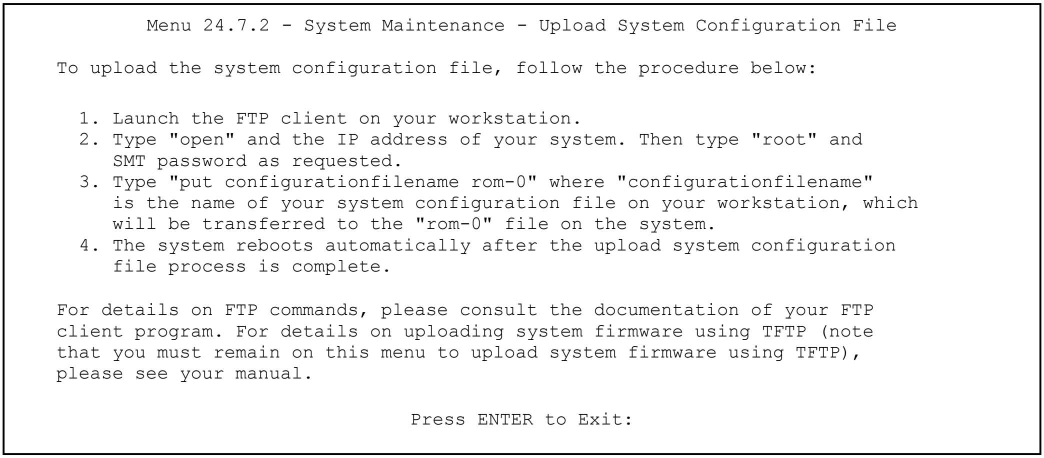


```
                Menu 24.7.1 - System Maintenance - Upload System Firmware


        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 17-5 Menu 24.7.1 System Maintenance : Upload System Firmware

17.4.2 Configuration File Upload

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



```
         Menu 24.7.2 - System Maintenance - Upload System Configuration File

 To upload the system configuration file, 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 configurationfilename rom-0" where "configurationfilename"
      is the name of your system configuration file on your workstation, which
      will be transferred to the "rom-0" file on the system.
   4. The system reboots automatically after the upload system configuration
      file process is complete.

 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 17-6 Menu 24.7.2 System Maintenance : Upload System Configuration File

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

17.4.3 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.

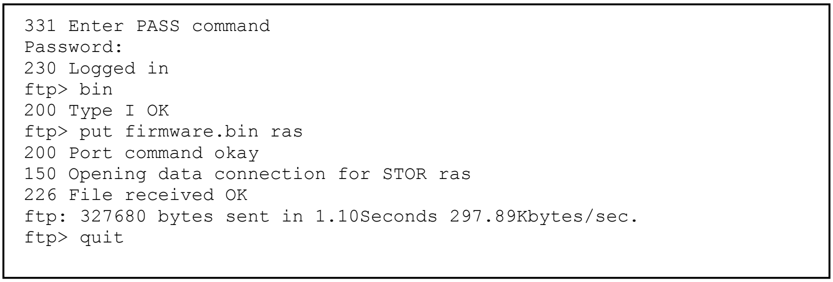
Step 3. Press [ENTER] when prompted for a username.

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 17-7 FTP Session Example

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

FTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

17.4.4 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.

17.4.5 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.

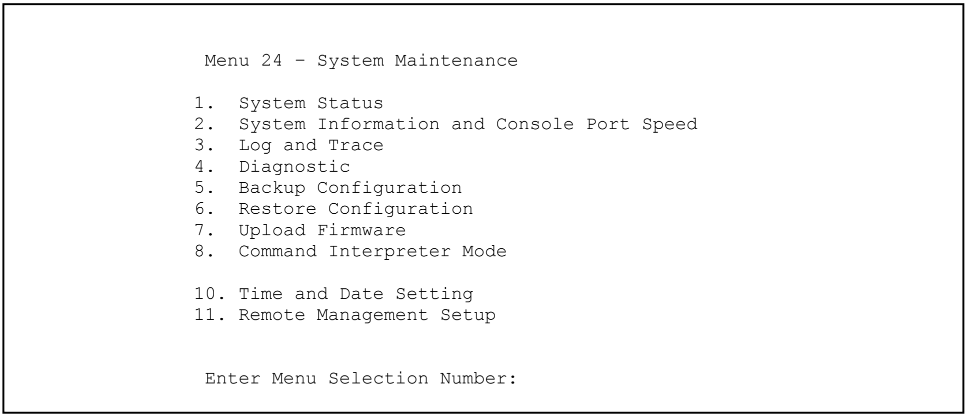
TFTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

Chapter 18
System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.11.

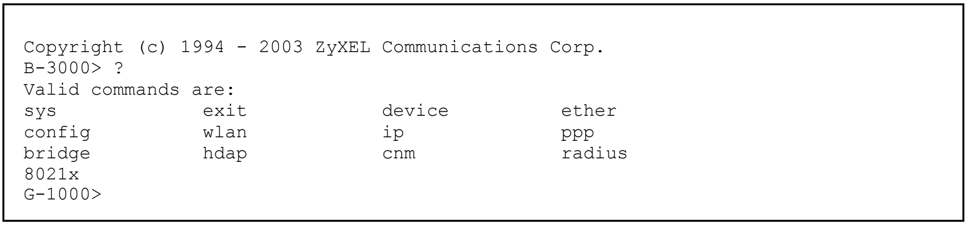
18.1 Command Interpreter Mode

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

                 10. Time and Date Setting
                 11. Remote Management Setup


                  Enter Menu Selection Number:
```

Figure 18-1 Menu 24 System Maintenance



```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
B-3000> ?
Valid commands are:
sys             exit            device          ether
config          wlan            ip              ppp
bridge          hdap            cnm             radius
8021x
G-1000>
```

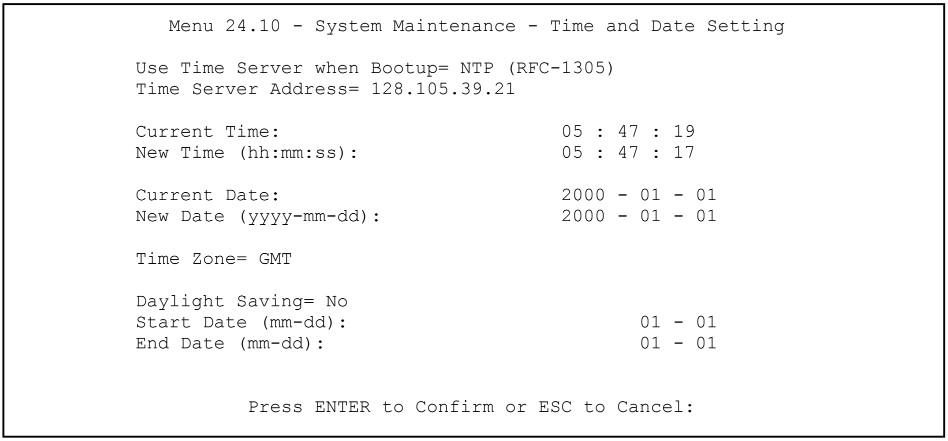
Figure 18-2 Valid CI Commands

18.2 Time and Date Setting

The ZyAIR keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyAIR. 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.



```
               Menu 24.10 - System Maintenance - Time and Date Setting

            Use Time Server when Bootup= NTP (RFC-1305)
            Time Server Address= 128.105.39.21

            Current Time:                         05 : 47 : 19
            New Time (hh:mm:ss):                  05 : 47 : 17

            Current Date:                         2000 - 01 - 01
            New Date (yyyy-mm-dd):                2000 - 01 - 01

            Time Zone= GMT

            Daylight Saving= No
            Start Date (mm-dd):                          01 - 01
            End Date (mm-dd):                            01 - 01


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

Figure 18-3 Menu 24.10 System Maintenance: Time and Date Setting

Table 18-1 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.

Table 18-1 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter 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.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
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.	

18.2.1 Resetting the Time

The ZyAIR resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the ZyAIR starts up, if there is a time server configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 19
Remote Management

This chapter covers remote management (SMT menu 24.11).

19.1 Telnet

You can configure your ZyAIR for remote Telnet access as shown next.

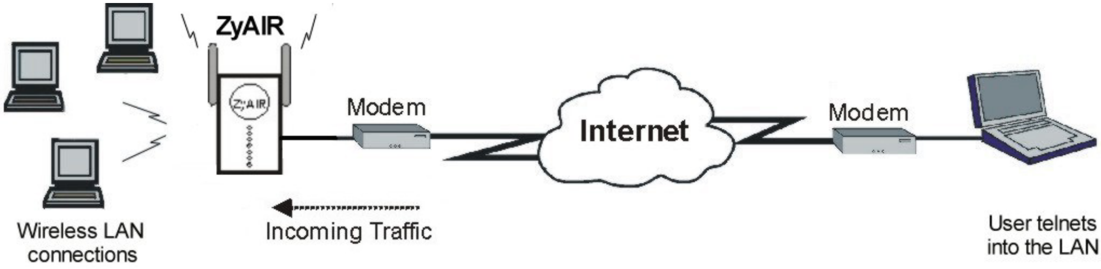


Figure 19-1 Telnet Configuration on a TCP/IP Network

19.2 FTP

You can upload and download ZyAIR firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

19.3 Web

You can use the ZyAIR's embedded web configurator for configuration and file management. See the online help for details.

19.4 Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to display **Menu 24.11 – Remote Management Control**.

19.4.1 Remote Management Setup

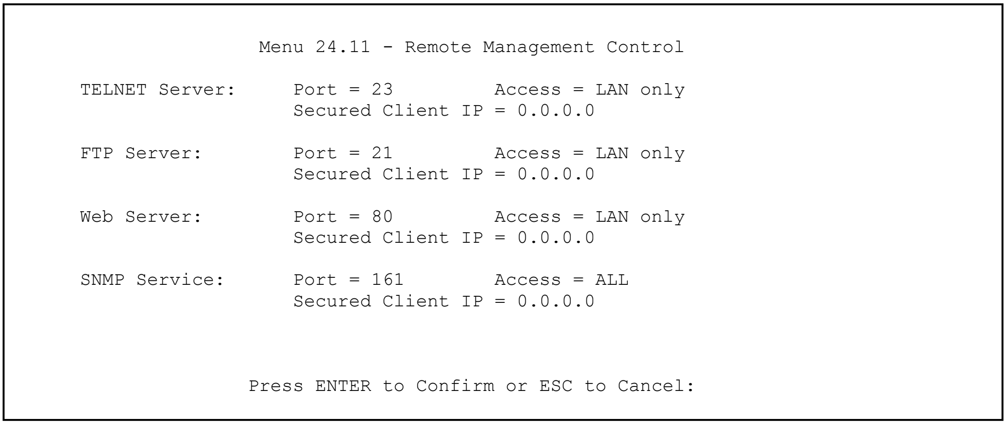
Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyAIR from a remote location via:

the wireless LAN(**WLAN only**), the **LAN only**, **All** (LAN and WLAN) or **Disable** (neither).

- WLAN only (wireless LAN)
- LAN only
- ALL (LAN and WLAN)
- Disable (Neither)

Enter 11, from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next).



```
                    Menu 24.11 - Remote Management Control

      TELNET Server:      Port = 23          Access = LAN only
                          Secured Client IP = 0.0.0.0

      FTP Server:         Port = 21          Access = LAN only
                          Secured Client IP = 0.0.0.0

      Web Server:         Port = 80          Access = LAN only
                          Secured Client IP = 0.0.0.0

      SNMP Service:       Port = 161         Access = ALL
                          Secured Client IP = 0.0.0.0



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

Figure 19-2 Menu 24.11 Remote Management Control

The following table describes the fields in this menu.

Table 19-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service	Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyAIR.	
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	

Table 19-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WLAN only**, **All** or **Disable**.	LAN only
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

19.4.2 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

1. You have disabled that service in menu 24.11.
2. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
3. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
4. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

19.5 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyAIR will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part VI:

APPENDICES

This part provides background information about setting up your computer's IP address, wireless LAN, 802.1x, PPPoE, PPTP and IP subnetting. It also provides information on the command interpreter interface, NetBIOS commands and logs.

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. Please see our included disk for further information

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 Ethernet Interface

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connection between your ZyAIR and the Ethernet device connected to the **ETHERNET** port. Check for faulty Ethernet cables. Make sure your computer's Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the ZyAIR, the Ethernet device and your computer are on the same subnet.

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot ping any computer on the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connections between your ZyAIR and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make the Ethernet cable does not exceed 100 meters. Make sure the LAN computer's Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of the ZyAIR, the Ethernet device and the LAN computers are on the same subnet.

Problems with the Password

Chart A-3 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. If you have entered three incorrect passwords, you must wait for the time specified before access to the ZyAIR is allowed.

Problems with Telnet

Chart A-4 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR through Telnet.	Refer to the *Problems with the Ethernet Interface* section for instructions on checking your Ethernet connection.

Problems with the WLAN Interface

Chart A-5 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the WLAN.	Make sure the ZyAIR is turned on and the Link LED is off. Make sure the wireless adapter on the wireless station is working properly. Check that both the ZyAIR and your wireless station are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
I cannot ping any computer on the WLAN.	Make sure the ZyAIR turned on and the Link LED is off. Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the ZyAIR and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Appendix B
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.

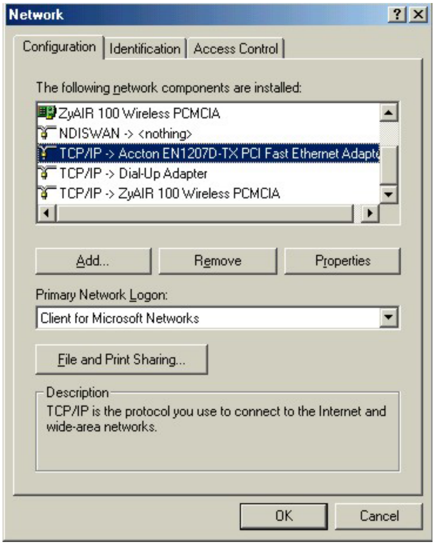
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 Ethernet port.

Windows 95/98/Me

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



The following network components are installed:

- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

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

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**.

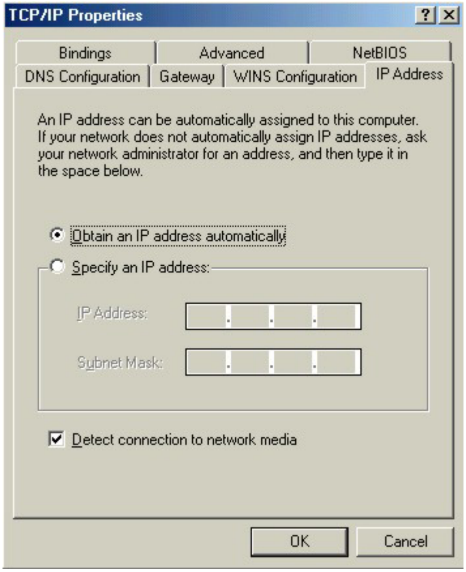
e. Restart your computer so the changes you made take effect.

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.



TCP/IP Properties

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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

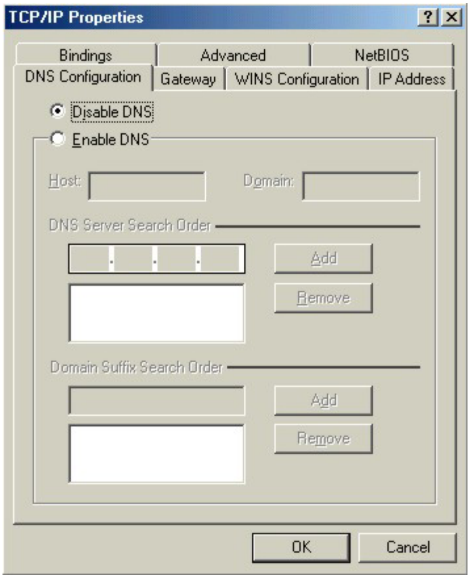
Subnet Mask: . . .

☑ Detect connection to network media

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).



TCP/IP Properties

● Disable DNS

○ Enable DNS

Host:

Domain:

DNS Server Search Order

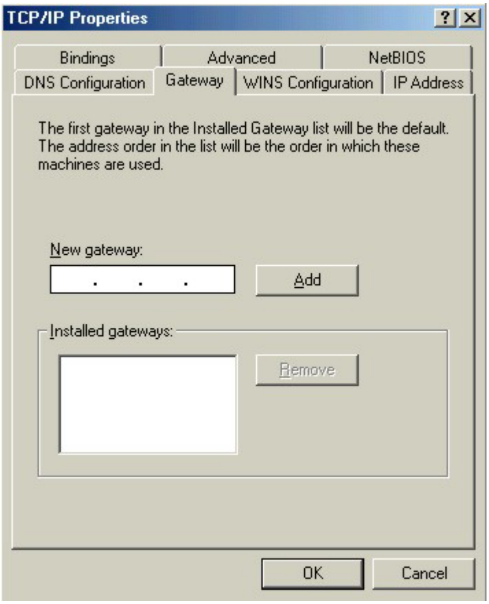
. . .

Domain Suffix Search Order

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**.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

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.

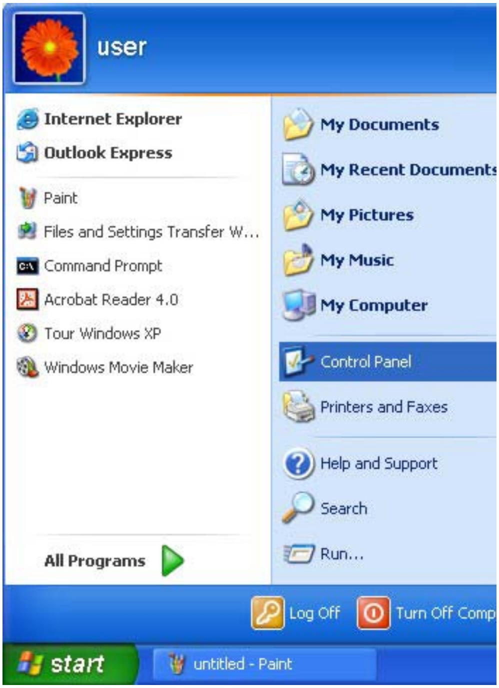
6. Turn on your ZyAIR and restart your computer when prompted.

Verifying Your Computer’s IP Address

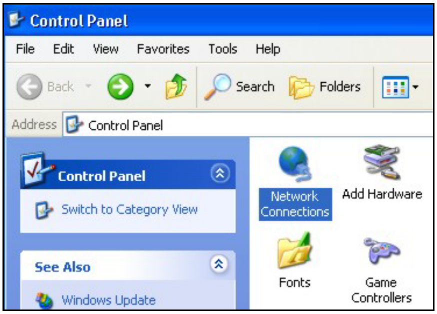
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

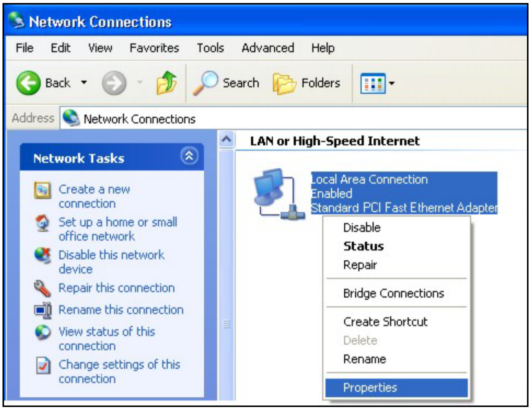
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



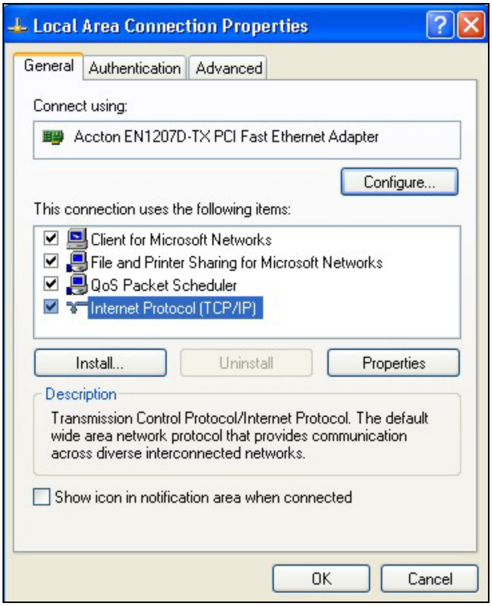
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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**.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

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

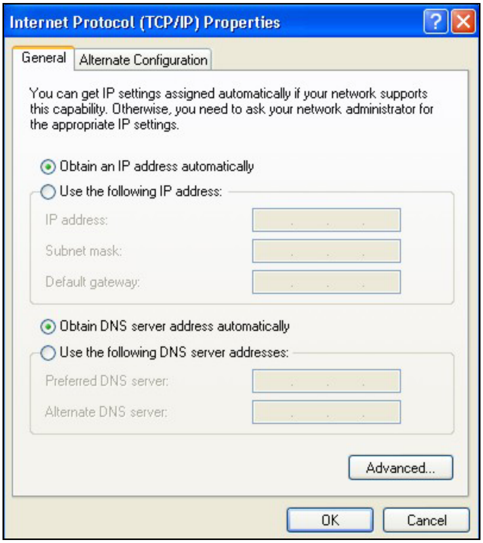
□ Show icon in notification area when connected

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

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

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

   Click **Advanced**.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

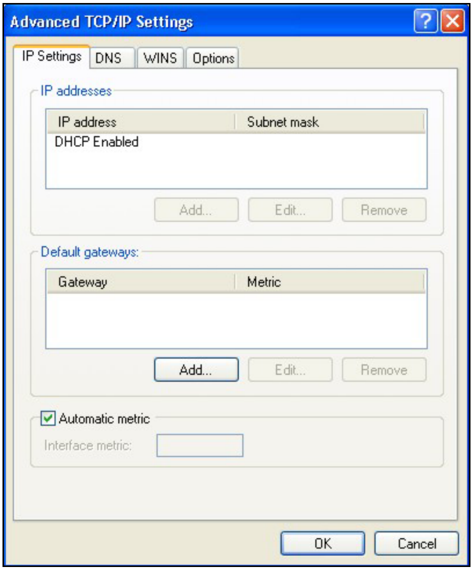
● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

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



DHCP Enabled

☑ Automatic metric

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.

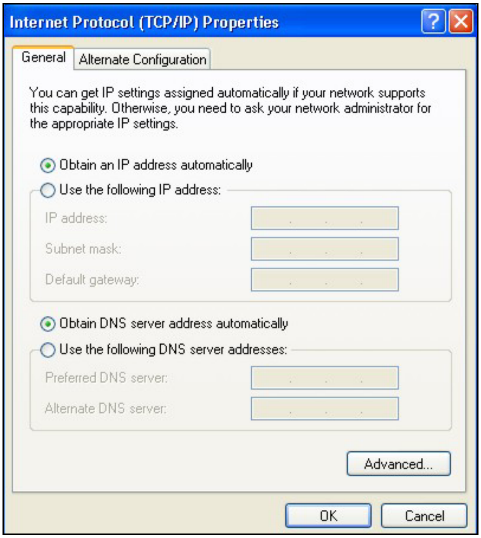
-Click **OK** when finished.

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.



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

10. Turn on your ZyAIR and restart your computer (if prompted).

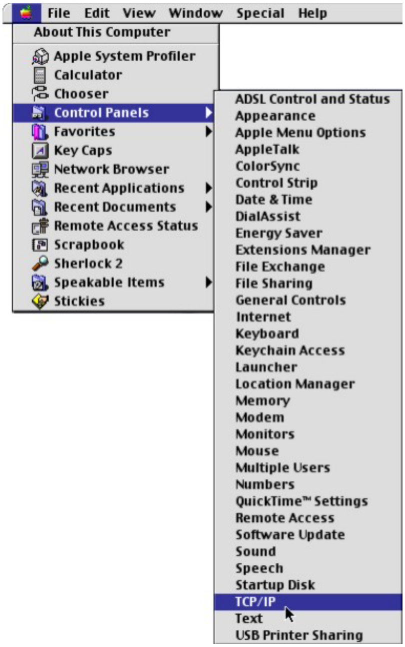
Verifying Your Computer's IP Address

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

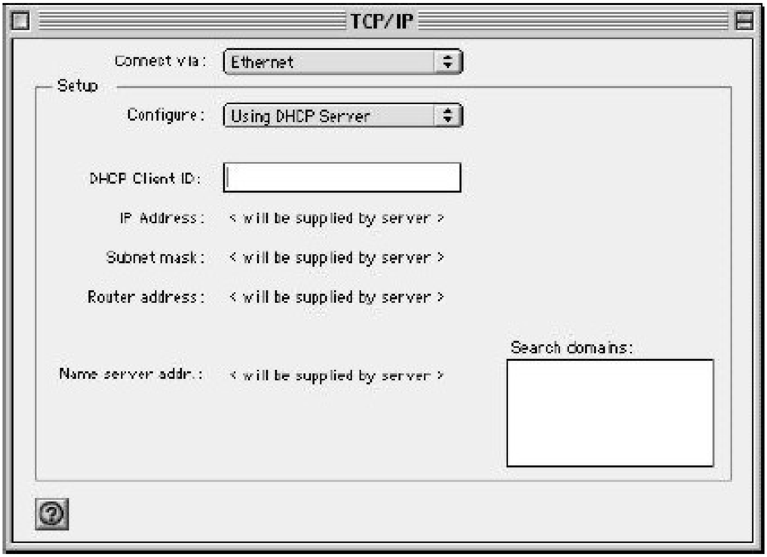
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

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.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

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

Search domains:

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.

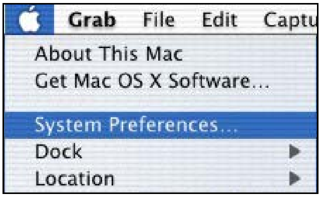
7. Turn on your ZyAIR and restart your computer (if prompted).

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.

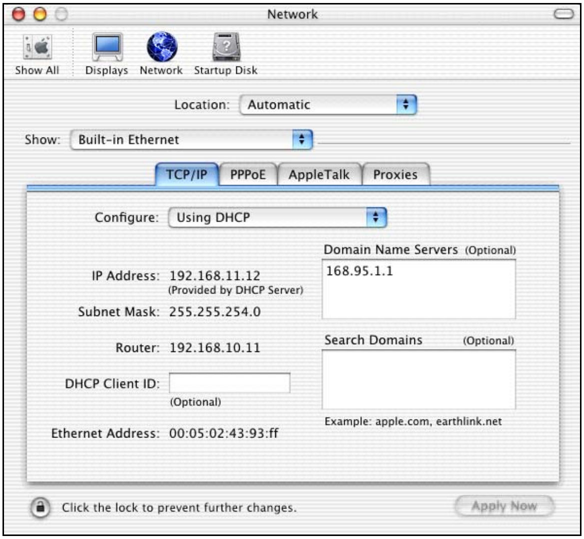


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

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 C
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.

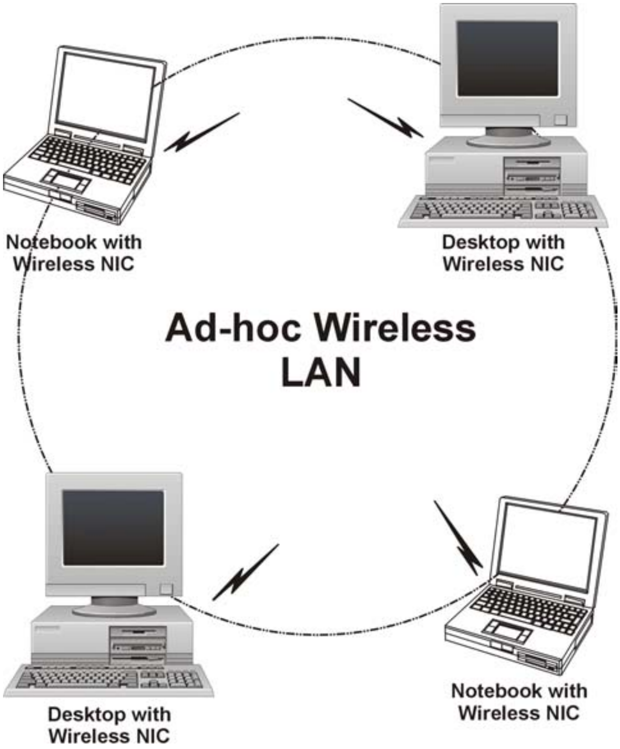

Notebook with Wireless NIC
Desktop with Wireless NIC
Ad-hoc Wireless LAN
Desktop with Wireless NIC
Notebook with Wireless NIC

Diagram 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.

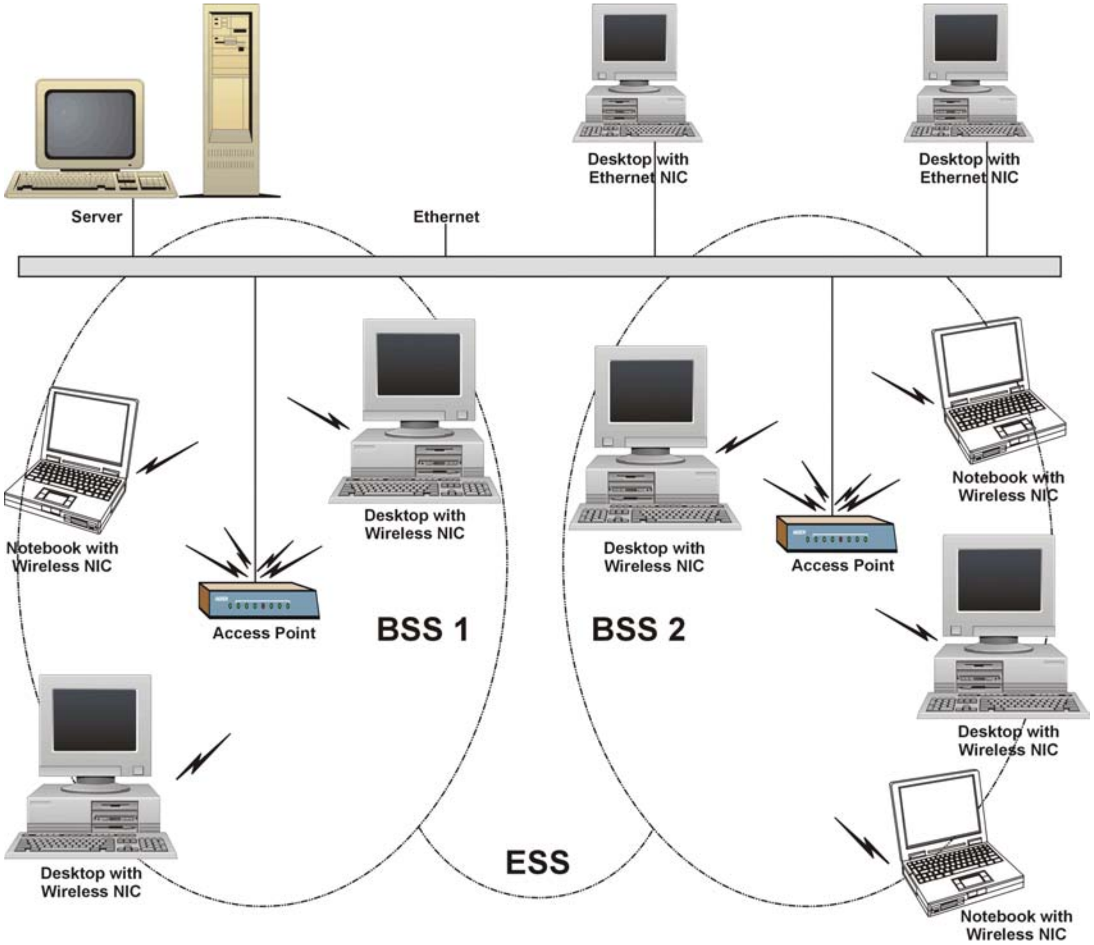

Server
Ethernet
Desktop with Ethernet NIC
Desktop with Ethernet NIC
Notebook with Wireless NIC
Desktop with Wireless NIC
Access Point
BSS 1
Desktop with Wireless NIC
Desktop with Wireless NIC
Access Point
BSS 2
Notebook with Wireless NIC
Desktop with Wireless NIC
ESS
Notebook with Wireless NIC

Diagram 2 ESS Provides Campus-Wide Coverage

Appendix D
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

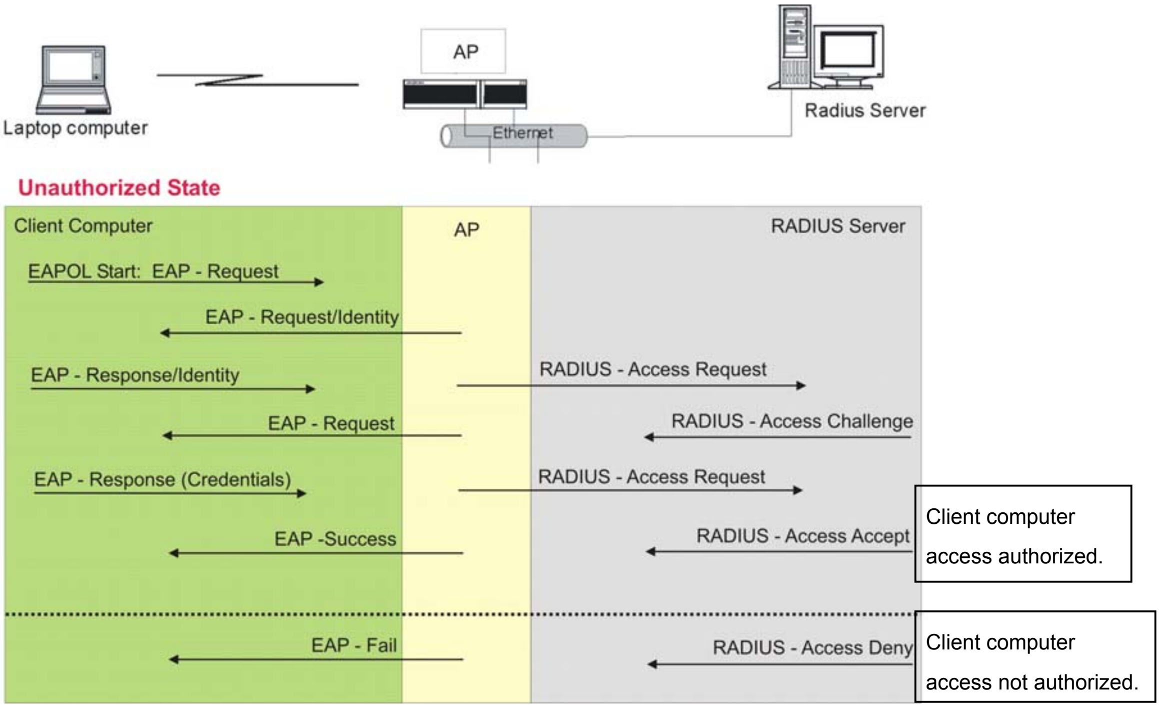


Diagram 3 Sequences for EAP MD5–Challenge Authentication

Appendix E
Types of EAP Authentication

This appendix discusses the four popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS** and **PEAP**. The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

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

Comparison of EAP Authentication Types

	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**PEAP**
Mutual Authentication	No	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional
Certificate – Server	No	Yes	Yes	Yes
Dynamic Key Exchange	No	Yes	Yes	Yes
Credential Security	None	Strong	Strong	Strong
Deployment Difficulty	Easy	Hard	Moderate	Moderate
Wireless Security	Poor	Best	Good	Good
Client Identity Protection	No	No	Yes	Yes

Appendix F
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 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 6 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 7 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	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 8 "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 9 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 10 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 11 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.**11**000000) 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 12 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 13 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 14 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000

Chart 14 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 15 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 16 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 17 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 6*) available for subnetting.

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

Chart 18 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 18 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
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See the *Command Interpreter* appendix for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

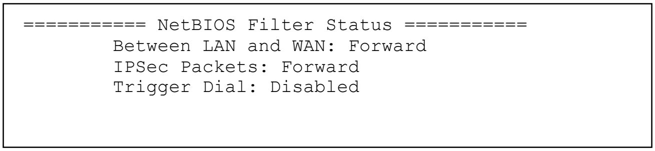
You can configure NetBIOS filters to do the following :

- Allow or disallow the sending of NetBIOS packets between the LAN and WAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the LAN.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for a ZyAIR



```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Forward
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

Diagram 4 NetBIOS Display Filter Settings Command Without DMZ Example

The filter types and their default settings are as follows.

Chart 19 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Forward

Chart 19 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type>`

`Usage =` config:

0 = between LAN and WAN

3 = IPSec packet pass through

4 = Trigger Dial

Example commands

Command: `sys filter netbios config 0 on`

This command blocks NetBIOS packets between LAN and WAN

Command: `sys filter netbios config 3 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 4 off`

This command stops NetBIOS commands from initiating calls.

Appendix J
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 14-1 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
`sys pwderrtm`	This command displays the brute-force guessing password protection settings.
`sys pwderrtm 0`	This command turns off the password's protection from brute-force guessing.
`sys pwderrtm N`	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 pwderrtm 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 K
Log Descriptions

This appendix describes some general log messages. Not all log messages are available on all models.

Chart 20 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Chart 21 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's web configurator interface.
`WEB Login Fail`	Someone has failed to log on to the router's web configurator interface.
`TELNET Login Successfully`	Someone has logged on to the router via telnet.

Chart 21 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via FTP.
`FTP Login Fail`	Someone has failed to log on to the router via FTP.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.

Chart 22 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Chart 23 ICMP Notes

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

Chart 23 ICMP Notes

TYPE	CODE	DESCRIPTION
	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
16		Information Reply
	0	Information reply message

Chart 24 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 25 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
`error`	`0, 1, 2, 3`
`mten`	`0, 1`
`upnp`	`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

    Firewall default policy: UDP(set:8)

  1|11/11/2002 15:10:12 |172.21.4.17:138       |172.21.255.255:138
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  2|11/11/2002 15:10:11 |172.17.2.1            |224.0.1.60
|ACCESS BLOCK

    Firewall default policy: IGMP(set:8)

  3|11/11/2002 15:10:11 |172.22.3.80:137       |172.22.255.255:137
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  4|11/11/2002 15:10:10 |192.168.10.1:520      |192.168.10.255:520
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

  5|11/11/2002 15:10:10 |172.21.4.67:137       |172.21.255.255:137
|ACCESS BLOCK
```

Appendix L
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 M
Index