# ZyAIR G-5100

*Outdoor Dual-802.11g Wireless LAN Access Point & Bridge*

# User's Guide

Version 3.50
5/2005

ZyXEL

# Copyright

## Disclaimer

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

## Trademarks

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

# Certifications

## Federal Communications Commission (FCC) Interference Statement

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.

## FCC Warning

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

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

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

## Notice 1

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

## FCC Caution:

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

## IMPORTANT NOTE:

## FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**Note:** Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antennas or antenna connector cable. Only use the included antennas or antenna connector cable.

## Canadian Note

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Certifications

Go to www.zyxel.com

1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

2 Select the certification you wish to view from this page.

# Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to corrosive liquids.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

# 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.

# Customer Support

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

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

| **METHOD** | **SUPPORT E-MAIL** | **TELEPHONE**[A] | **WEB SITE** | **REGULAR MAIL** |
|---|---|---|---|---|
| **LOCATION** | **SALES E-MAIL** | **FAX** | **FTP SITE** | |
| **CORPORATE HEADQUARTERS (WORLDWIDE)** | support@zyxel.com.tw | +886-3-578-3942 | www.zyxel.com<br>www.europe.zyxel.com | ZyXEL Communications Corp.<br>6 Innovation Road II<br>Science Park<br>Hsinchu 300<br>Taiwan |
| | sales@zyxel.com.tw | +886-3-578-2439 | ftp.zyxel.com<br>ftp.europe.zyxel.com | |
| **CZECH REPUBLIC** | info@cz.zyxel.com | +420 241 091 350 | www.zyxel.cz | ZyXEL Communications Czech s.r.o.<br>Modranská 621<br>143 01 Praha 4 - Modrany<br>Ceská Republika |
| | info@cz.zyxel.com | +420 241 091 359 | | |
| **DENMARK** | support@zyxel.dk | +45 39 55 07 00 | www.zyxel.dk | ZyXEL Communications A/S<br>Columbusvej 5<br>2860 Soeborg<br>Denmark |
| | sales@zyxel.dk | +45 39 55 07 07 | | |
| **FINLAND** | support@zyxel.fi | +358-9-4780-8411 | www.zyxel.fi | ZyXEL Communications Oy<br>Malminkaari 10<br>00700 Helsinki<br>Finland |
| | sales@zyxel.fi | +358-9-4780 8448 | | |
| **FRANCE** | info@zyxel.fr | +33 (0)4 72 52 97 97 | www.zyxel.fr | ZyXEL France<br>1 rue des Vergers<br>Bat. 1 / C<br>69760 Limonest<br>France |
| | | +33 (0)4 72 52 19 20 | | |
| **GERMANY** | support@zyxel.de | +49-2405-6909-0 | www.zyxel.de | ZyXEL Deutschland GmbH.<br>Adenauerstr. 20/A2 D-52146<br>Wuerselen<br>Germany |
| | sales@zyxel.de | +49-2405-6909-99 | | |
| **NORTH AMERICA** | support@zyxel.com | +1-800-255-4101<br>+1-714-632-0882 | www.us.zyxel.com | ZyXEL Communications Inc.<br>1130 N. Miller St.<br>Anaheim<br>CA 92806-2001<br>U.S.A. |
| | sales@zyxel.com | +1-714-632-0858 | ftp.us.zyxel.com | |
| **NORWAY** | support@zyxel.no | +47 22 80 61 80 | www.zyxel.no | ZyXEL Communications A/S<br>Nils Hansens vei 13<br>0667 Oslo<br>Norway |
| | sales@zyxel.no | +47 22 80 61 81 | | |
| **SPAIN** | support@zyxel.es | +34 902 195 420 | www.zyxel.es | ZyXEL Communications<br>Arte, 21 5ª planta<br>28033 Madrid<br>Spain |
| | sales@zyxel.es | +34 913 005 345 | | |
| **SWEDEN** | support@zyxel.se | +46 31 744 7700 | www.zyxel.se | ZyXEL Communications A/S<br>Sjöporten 4, 41764 Göteborg<br>Sweden |
| | sales@zyxel.se | +46 31 744 7701 | | |

| METHOD<br>LOCATION | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| | SALES E-MAIL | FAX | FTP SITE | |
| UNITED KINGDOM | support@zyxel.co.uk | +44 (0) 1344 303044<br>08707 555779 (UK only) | www.zyxel.co.uk | ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK) |
| | sales@zyxel.co.uk | +44 (0) 1344 303034 | ftp.zyxel.co.uk | |

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

# Table of Contents

# List of Figures

# List of Tables

# Preface

Congratulations on your purchase of the ZyAIR G-5100 Outdoor 802.11g Business Access Point/Bridge/Repeater.

The ZyAIR is an Access Point (AP) through which wireless stations can communicate and/or access a wired network. The ZyAIR can also function as a wireless network bridge/repeater and establish wireless links with other APs.

The ZyAIR also supports both AP and bridge connections at the same time.

Your ZyAIR is easy to install and configure.

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

## About This User's Guide

This User's Guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the System Management Terminal (SMT).  The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator

**Note:** 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 Start Guide

  The Quick Start Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

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

## User Guide Feedback

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

## Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- 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-5100 may be referred to simply as the ZyAIR in the user's guide.

## Graphics Icons Key

| | | |
|---|---|---|
| ZyAIR<br> | Computer<br> | Notebook computer<br> |
| Server<br> | Modem<br> | Switch<br> |
| Router<br> | Wireless Signal<br> | |

# CHAPTER 1 Getting to Know Your ZyAIR

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

## 1.1 Introducing the ZyAIR

The ZyAIR G-5100 is an enterprise level, outdoor IEEE 802.11g compliant business access point, bridge and repeater with excellent wireless performance. Wireless Distribution System (WDS) support provides flexibility in building an extended wireless network with bridge and repeater applications. IEEE 802.1x, Wi-Fi Protected Access, WEP data encryption and MAC address filtering offer highly secured wireless connectivity.

Rugged die-cast, watertight construction, built-in lightening protection, and grounding make the ZyAIR perfect for outdoors applications.

It is easy to install and configure the ZyAIR. The web-based configurator allows remote configuration and management of your ZyAIR. The Power over Ethernet (PoE) feature means that power can be delivered to the ZyAIR over an Ethernet line. This allows you to mount the ZyAIR in areas where there are no nearby power sources.

## 1.2 ZyAIR Features

The following sections describe the features of the ZyAIR

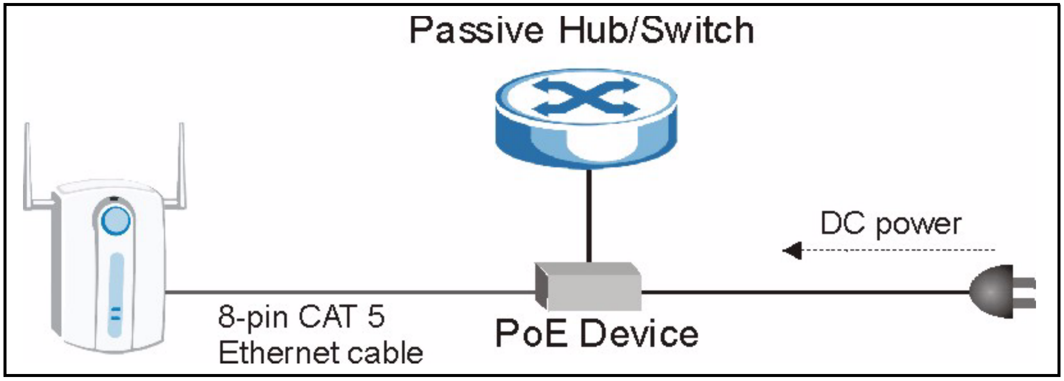
### 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface

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.

### Power over Ethernet (PoE)

Power over Ethernet (PoE) is the ability to provide power to your ZyAIR via an 8-pin CAT 5 Ethernet cable, eliminating the need for a nearby power source. The ZyAIR G-5100 includes a special high current power injector that allows the ZyAIR to be located farther away. This feature allows increased flexibility in the locating of your ZyAIR.

**Figure 1** PoE Installation Example



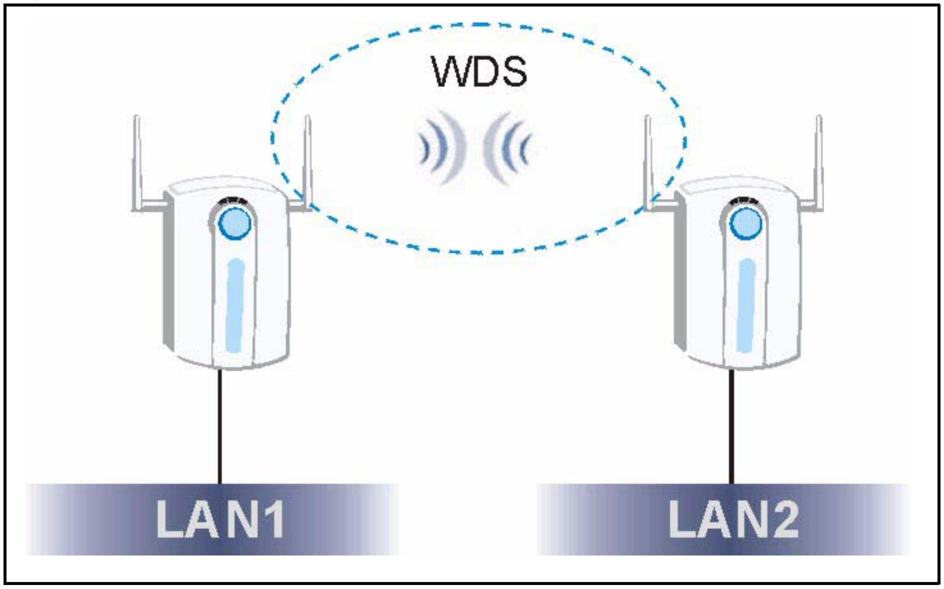
## Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

## WDS Functionality

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

**Figure 2** WDS Functionality Example



## IEEE 802.11g Wireless LAN Standard

The ZyAIR complies with the IEEE 802.11g wireless standard. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows. The modulation technique defines how bits are encoded onto radio waves.

**Table 1** IEEE 802.11g

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing) |

**Note:** 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.

## IEEE 802.11b Wireless LAN Standard

The ZyAIR also fully complies with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g device (and vice versa) at 11 Mbps or lower depending on range.

The IEEE 802.11b data rate and corresponding modulation techniques are shown in the table below.

**Table 2** IEEE 802.11b

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 1 | DBPSK (Differential Binary Phase Shift Keyed) |
| 2 | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11 | CCK (Complementary Code Keying) |

## STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network.

## SSL Passthrough

SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https” instead of “http”. The ZyAIR allows SSL connections to take place through the ZyAIR.

### VPN Passthrough

VPN (Virtual Private Network) connections use data encryption to provide secure communications over unsecure networks (like the Internet). The ZyAIR allows VPN connections to go through it.

### Wireless LAN MAC Address Filtering

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

### WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

### IEEE 802.1x Network Security

The ZyAIR supports the IEEE 802.1x standard to enhance user authentication. This allows you to use a RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate users.

### Embedded RADIUS Server

The ZyAIR's embedded RADIUS server eliminates the need to purchase and maintain a standalone external RADIUS server. Use the embedded  RADIUS server to authenticate up to 32 users. You can also use an external RADIUS server to authenticate a potentially unlimited number of users.

### Backup RADIUS Server

You can configure the ZyAIR to use backup external RADIUS servers and accounting servers in case the primary external RADIUS or accounting server does not respond.

### 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 web configurator is an HTML-based management interface that allows easy setup and management via Internet browser. 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.
- 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.

### Wireless LAN Channel Usage

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

## 1.3 Applications for the ZyAIR

The ZyAIR can be configured using the following WLAN operating modes

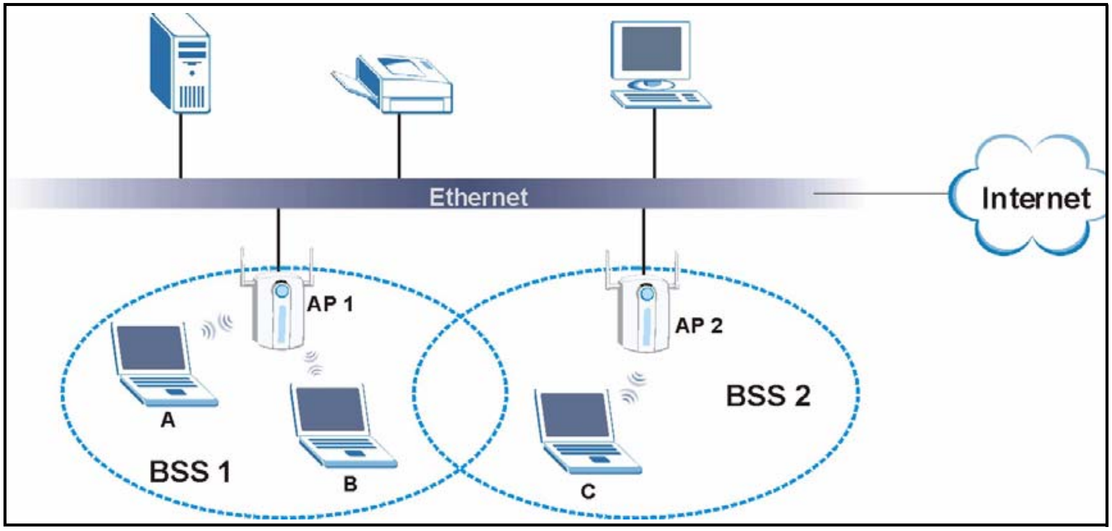
1. AP
2. AP+Bridge
3. Bridge/Repeater

Applications for each operating mode are shown below.

### 1.3.1 Access Point

The ZyAIR is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyAIR is shown as follows. Stations A, B and C can access the wired network through the ZyAIRs.

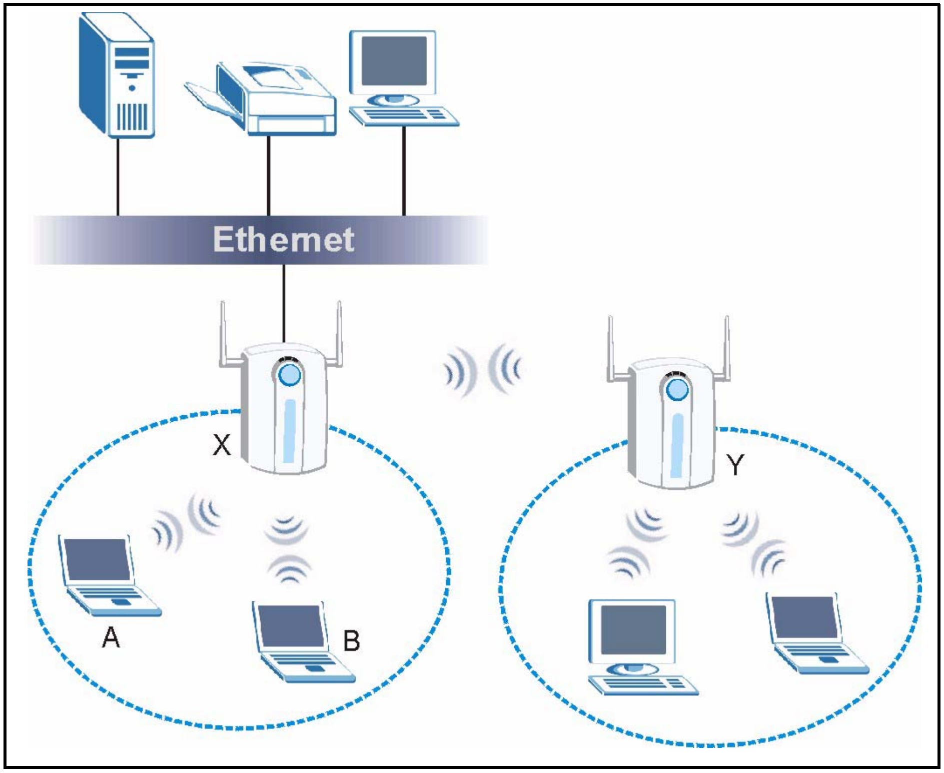
**Figure 3** Access Point Application



## 1.3.2 AP + Bridge

In **AP+Bridge** mode, the ZyAIR supports both AP connections (**A** and **B** can connect to the wired network through **X**) and bridge connections (**X** can communicate with **Y**) at the same time.

**Figure 4** AP+Bridge Application



### 1.3.3 Bridge / Repeater

The ZyAIR can act as a wireless network bridge and establish wireless links with other APs. In bridge mode, the ZyAIRs (see **A** and **B** in Figure 5 on page 35) are connected to independent wired networks and have a bridge (**A** can communicate with **B**) connection at the same time. A ZyAIR without a wired connection can act as a repeater (see **C** in Figure 6 on page 36).

**Figure 5** Bridge Application

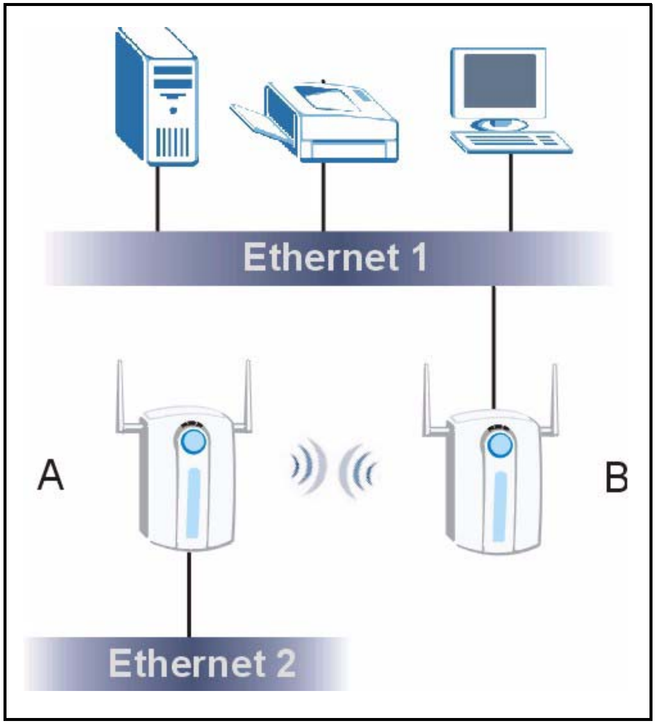
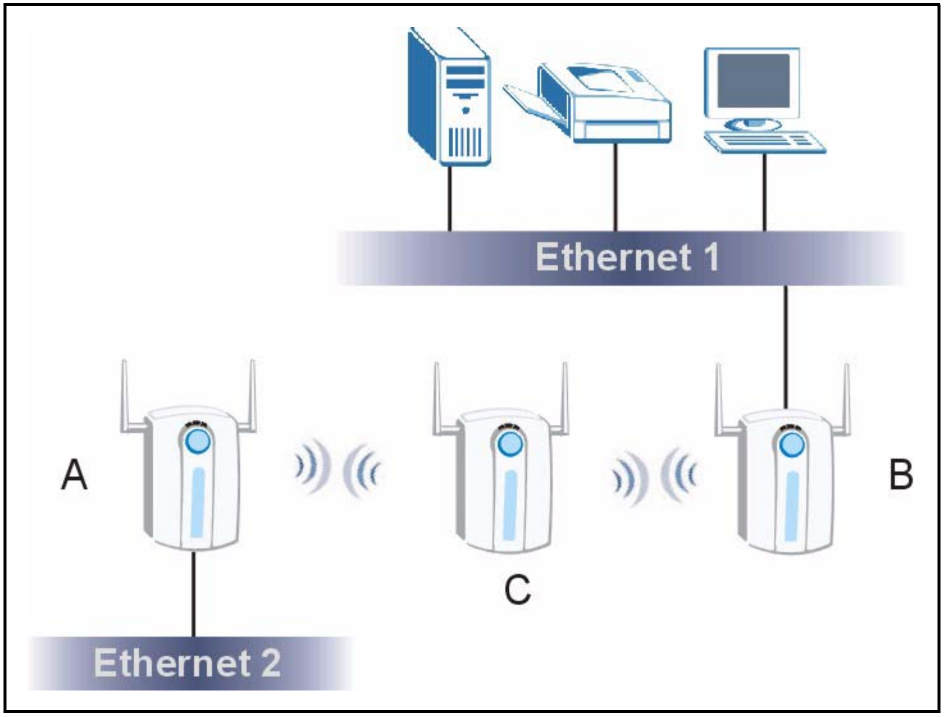


**Figure 6** Repeater Application



# CHAPTER 2 Introducing the Web Configurator

This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens.

## 2.1 Web Configurator Overview

The embedded web configurator allows you to manage the ZyAIR from anywhere through a browser such as Microsoft Internet Explorer. Use Internet Explorer 6.0 and later versions with JavaScript enabled.

It is recommended that you set your screen resolution to 1024 by 768 pixels.

## 2.2 Accessing the ZyAIR Web Configurator

1 Make sure your ZyAIR hardware is properly connected (refer to the Quick Start Guide).

2 Prepare your computer/computer network to connect to the ZyAIR (refer to Appendix D on page 201).

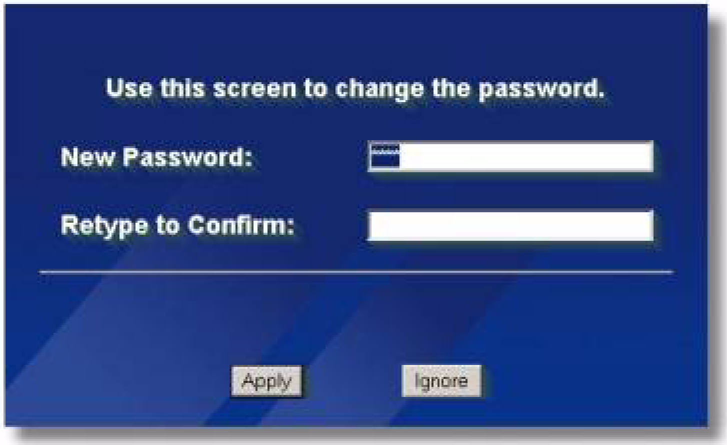
3 Launch your web browser.

4 Type "192.168.1.2" (the default IP address of the ZyAIR) as the URL.

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**.

6 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore** to allow access without password change.

**Figure 7** Change Password Screen



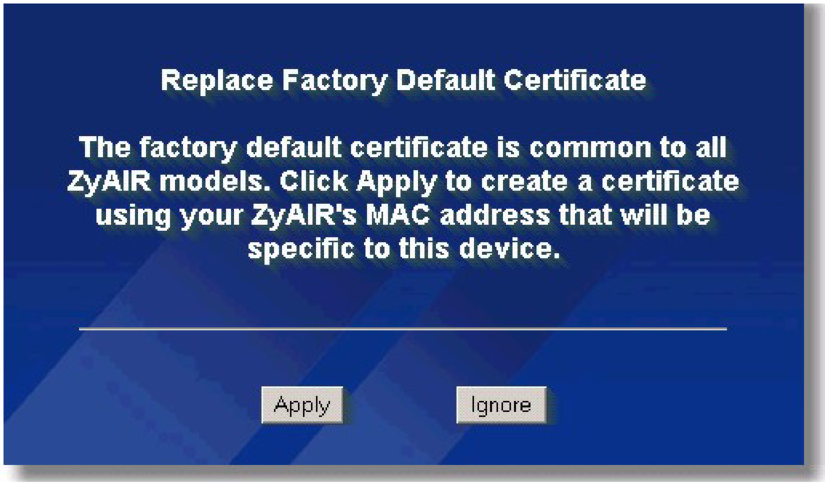
Use this screen to change the password.

New Password:

Retype to Confirm:

**7** Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyAIR's MAC address that will be specific to this device.

**Figure 8** Replace Certificate Screen.



Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

**8** You should now see the **MAIN MENU** screen (see Figure 10 on page 40).

**Note:** The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the ZyAIR if this happens to you.

## 2.3 Resetting the ZyAIR

If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to "1234" and the IP address will be reset to 192.168.1.2.

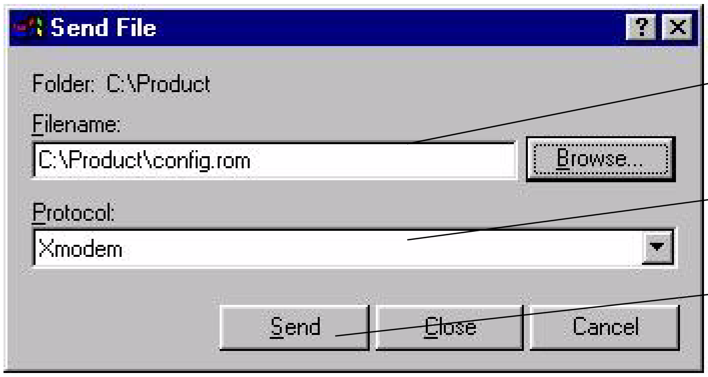
Do the following to erase the current configuration and restore factory defaults.

Obtain the default configuration file, unzip it and save it in a folder. Use a console cable to connect a computer with terminal emulation software to the ZyAIR's console port. Turn the ZyAIR off and then on to begin a session. When you turn on the ZyAIR again, you will see the initial screen. When you see the message "Press any key to enter Debug Mode within 3 seconds" press a key to enter debug mode.

To upload the configuration file, do the following:

1. Type "atlc" after the Enter Debug Mode message.
2. Wait for the Starting XMODEM upload message before activating XMODEM upload on your terminal.
3. This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer,** then **Send File** to display the following screen.

**Figure 9** Example Xmodem Upload



Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4. After a successful configuration file upload, type "atgo" to restart the ZyAIR.

The ZyAIR is now reinitialized with a default configuration file including the default password of "1234" and IP address of 192.168.1.2.

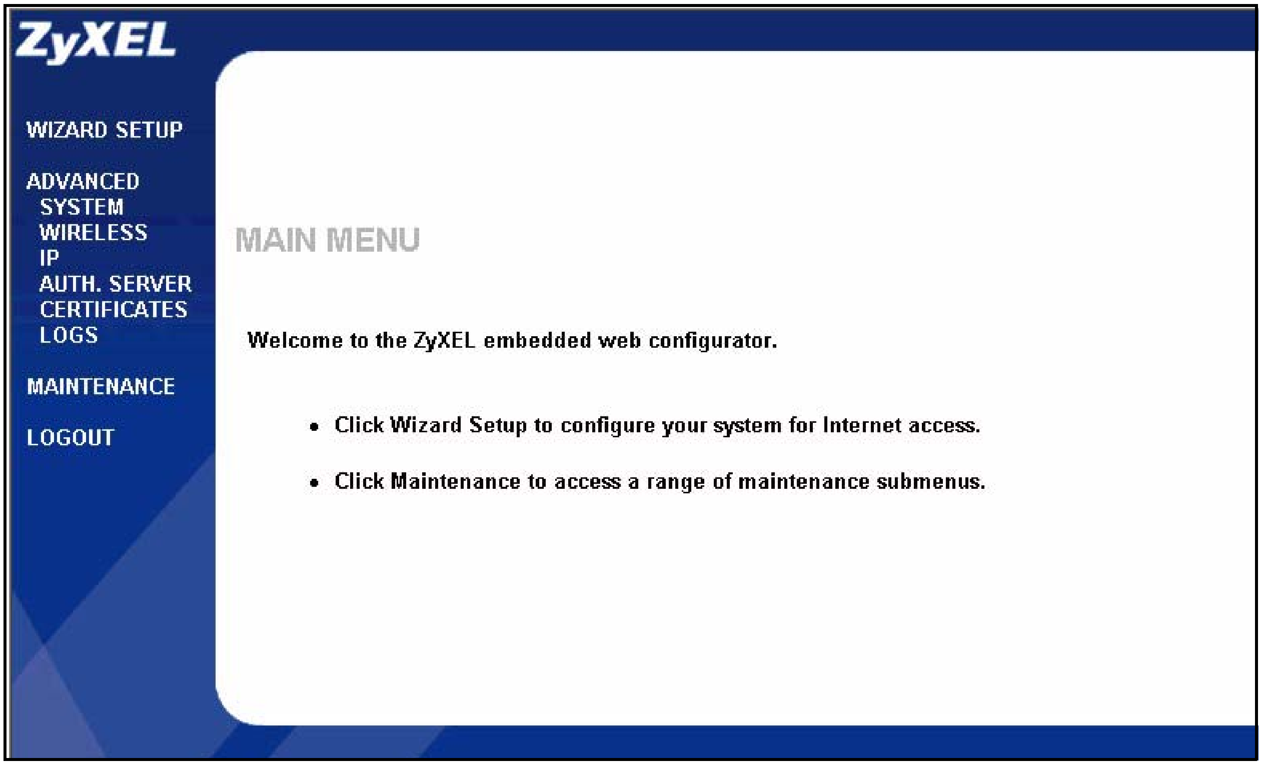
## 2.4 Navigating the ZyAIR Web Configurator

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

**Note:** 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.

**Figure 10** The MAIN MENU Screen of the Web Configurator



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access.
- Click Maintenance to access a range of maintenance submenus.

Use submenus to configure ZyAIR features.

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

The following table describes the sub-menus.

**Table 3** Screens Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| WIZARD SETUP | | Click **WIZARD SETUP** for initial configuration including general setup, wireless LAN setup and IP address assignment. |
| SYSTEM | General | This screen contains administrative and system-related information. |
| | Password | Use this screen to change your password. |
| | Time Setting | Use this screen to change your ZyAIR’s time and date settings. |
| WIRELESS | Wireless | Use this screen to configure the wireless LAN settings and WLAN authentication/security settings. |
| | MAC Filter | Use this screen to change MAC filter settings on the ZyAIR |
| | Roaming | Use this screen to configure the ZyAIR to allow wireless users to roam seamlessly between APs that are within the same subnet. |
| | 802.1x/WPA | Use this screen to configure wireless LAN security. |
| IP | IP | Use this screen to configure IP address settings. |

**Table 3** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| AUTH. SERVER | Setting | Configure this screen to use the internal server to authenticate wireless users. |
| | Trusted AP | Configure this screen to allow specified AP's to communicate with the ZyAIR. |
| | Trusted Users | Use this screen to configure the local user account(s) on the ZyAIR. |
| CERTIFICATES | My Certificates | Use this screen to view a summary list of certificates and manage certificates and certification requests. |
| | Trusted CAs | Use this screen to view and manage the list of the trusted CAs. |
| LOGS | View Log | Use this screen to view the logs for the categories that you selected. |
| | Log Settings | Use this screen to change your ZyAIR's log settings. |
| MAINTENANCE | Status | This screen contains administrative and system-related information. |
| | Association List | Use this screen to view a list of wireless clients that are connected to the ZyAIR. |
| | Channel Usage | Use this screen to see which APs are using which wireless channels within range of your ZyAIR. |
| | F/W Upload | Use this screen to upload firmware to your ZyAIR |
| | Configuration | Use this screen to backup and restore the configuration or reset the factory defaults to your ZyAIR. |
| | Restart | This screen allows you to reboot the ZyAIR without turning the power off. |
| LOGOUT | | Click **LOGOUT** to exit the web configurator. |

# CHAPTER 3 Wizard Setup

This chapter provides information on the **WIZARD SETUP** screens in the web configurator.

## 3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your ZyAIR for wireless stations to access your wired LAN.

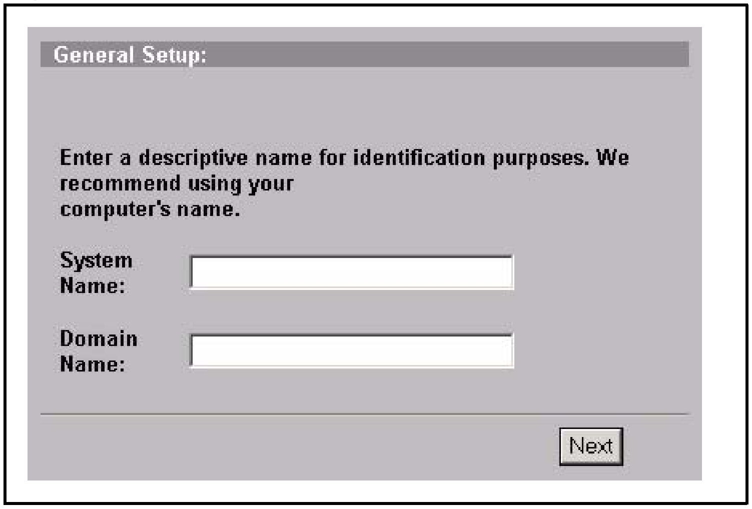
**Note:** Click **Next** in each screen to continue or click **Back** to return to the previous screen.

Your settings are not saved when you click **Back**.

## 3.2 Wizard Setup: General Setup

**General Setup** contains administrative and system-related information.

**Figure 11** Wizard: General Setup



Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

Domain Name:

The following table describes the labels in this screen.

**Table 4** Wizard: General Setup

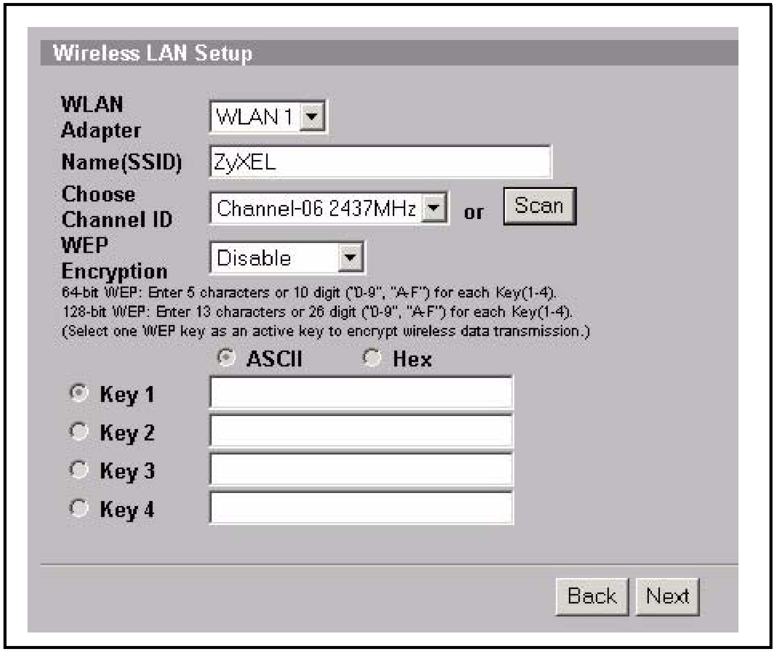
| LABEL | DESCRIPTION |
|---|---|
| System Name | It is recommended you type your computer's "Computer name".<br>In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.<br>In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.<br>In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyAIR **System Name**.<br>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. |
| Next | Click **Next** to proceed to the next screen. |

## 3.3 Wizard Setup: Wireless LAN

Use this wizard screen to configure one of the ZyAIR’s two wireless LAN (WLAN) adapters to function as an AP (**WLAN 1** is recommended). Use the **ADVANCED WIRELESS** screens to configure a WLAN adapter for bridge/repeater functions.

**Note:** The wireless clients and ZyAIR must use the same SSID, channel ID and WEP encryption key (if you enable WEP) for wireless communication.

**Figure 12** Wizard: Wireless LAN Setup



Wireless LAN Setup

WLAN Adapter: WLAN 1

Name(SSID): ZyXEL

Choose Channel ID: Channel-06 2437MHz or Scan

WEP Encryption: Disable

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("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

The following table describes the labels in this screen.

**Table 5** Wizard: Wireless LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| Wireless LAN Setup | |
| WLAN Adapter | Select which WLAN adapter you want to configure (**WLAN 1** recommended). |
| Name (SSID) | Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>If you change this field on the ZyAIR, make sure all wireless stations use the same Name (SSID) in order to access the network. |
| Choose Channel ID | To manually set the ZyAIR to use a channel, select the channel from the drop-down list box.<br>To have the ZyAIR automatically select a channel, click **Scan** instead. |
| Scan | Click this button to have the ZyAIR automatically scan for and select a channel with the least interference. |
| WEP Encryption | Select **Disable** allows all wireless computers to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to use data encryption.<br>Note: Use the **ADVANCED WIRELESS** screens to configure stronger types of security (such as WPA). |
| ASCII | Select this option in order to enter ASCII characters as the WEP keys. |
| Hex | Select this option to enter hexadecimal characters as the WEP keys.<br>The preceding 0x is entered automatically. |

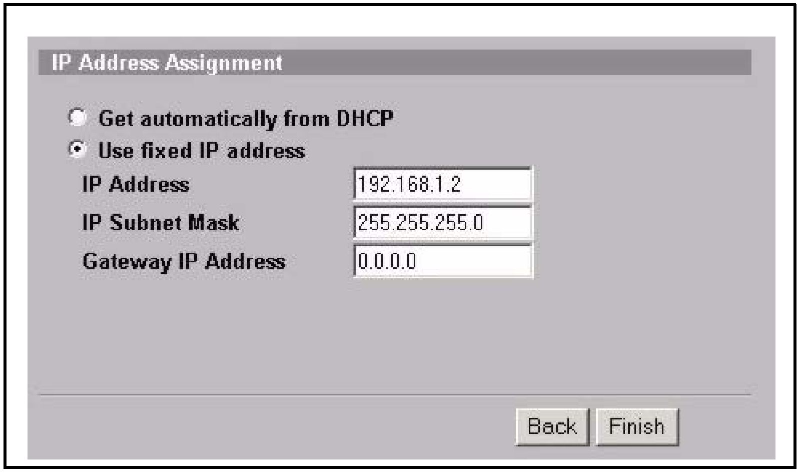
Table 5 Wizard: Wireless LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 3.4 Wizard Setup: IP Address Assignment

Use this wizard screen to configure IP address assignment for the ZyAIR.

Figure 13 Wizard: IP Address Assignment



IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address: 192.168.1.2

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 6 Wizard: IP Address Assignment

| LABEL | DESCRIPTION |
|---|---|
| IP Address Assignment | |
| Get automatically from DHCP | Select this option to have the ZyAIR use a dynamically assigned IP address from a DHCP server.<br>**Note:** 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. |

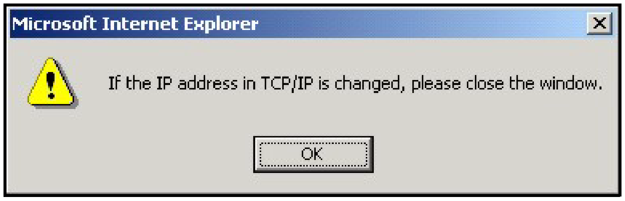
**Table 6** Wizard: IP Address Assignment

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the IP address of your ZyAIR in dotted decimal notation.<br>**Note:** If you changed 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. The gateway must be a router on the same segment as your ZyAIR's LAN or WAN port. |
| Back | Click **Back** to return to the previous screen. |
| Finish | Click **Finish** to proceed to complete the Wizard setup. |

## 3.5 Basic Setup Complete

When you click **Finish** in the **Wizard IP Address Assignment** screen, a warning window displays as shown. Click **OK** to close the window. Log into the web configurator again using the new IP address if you change the default IP address (192.168.1.2).

**Figure 14** TCP/IP Warning Screen

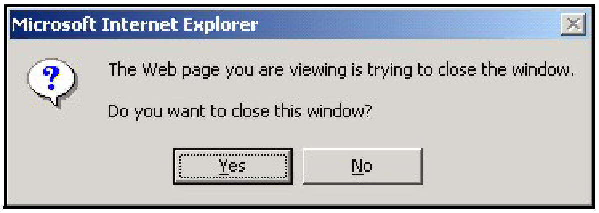


Microsoft Internet Explorer

If the IP address in TCP/IP is changed, please close the window.

The following screen displays prompting you to close the web browser.

**Figure 15** Close Browser Screen



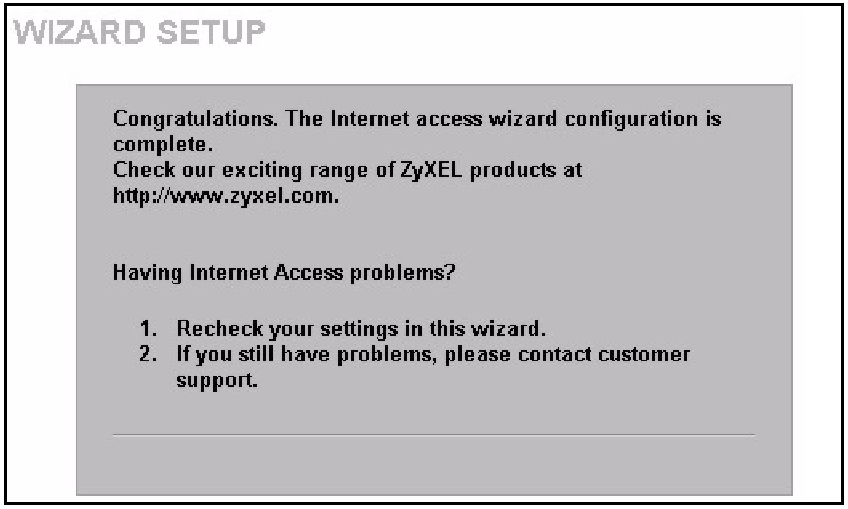
Microsoft Internet Explorer

The Web page you are viewing is trying to close the window.

Do you want to close this window?

Click **Yes** to close the web configurator. Otherwise, click **No** to use the **ADVANCED** screens to configure other features (the congratulations screen shows next).

**Figure 16** Wizard: Setup Complete



WIZARD SETUP

Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.

Having Internet Access problems?

1. Recheck your settings in this wizard.
2. If you still have problems, please contact customer support.

Well done! You have set up your ZyAIR to operate on your network and access the Internet.

# CHAPTER 4
# System Screens

This section provides information on general system setup.

## 4.1 System Overview

This chapter describes how to configure the ZyAIR’s general, DNS, password and time settings.

## 4.2 General Screen

The **General** screen contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyAIR **System Name**.

### 4.2.1 Domain Name

You can manually enter a domain name or the ZyAIR can get it automatically by DHCP.

### 4.2.2 DNS Server Address Assignment

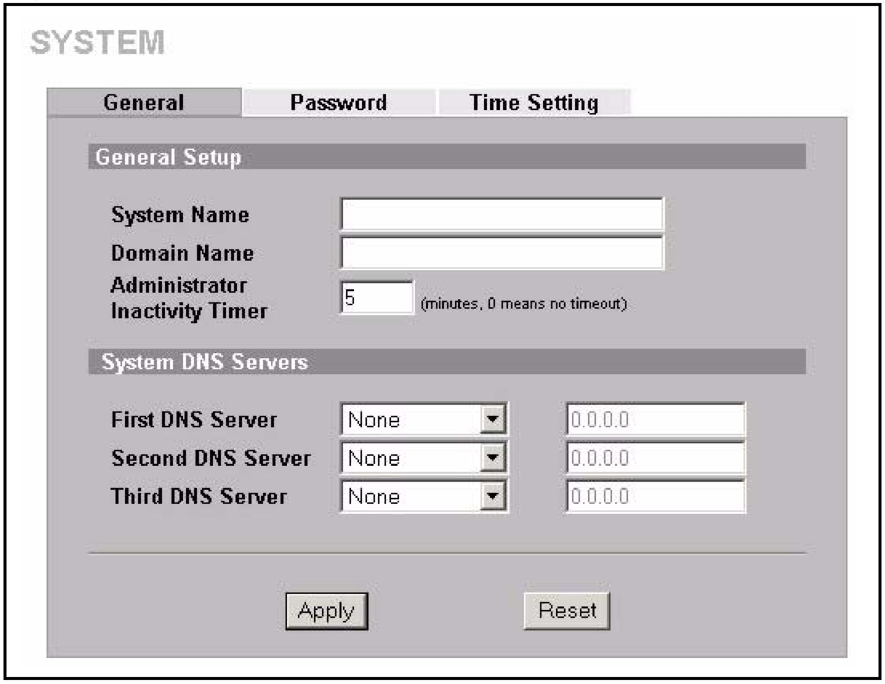
Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

You can manually configure DNS server addresses if you know them or the ZyAIR can receive them automatically through DHCP.

## 4.3 Configuring General Setup

Click the **SYSTEM** link under **ADVANCED** to open the **General** screen.

**Figure 17** System General



General Setup

System Name

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

The following table describes the labels in this screen.

**Table 7** System General Setup

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| System Name | Type a descriptive name to identify the ZyAIR in the Ethernet network.<br>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.<br>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.<br>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 | |

**Table 7** System General Setup (continued)

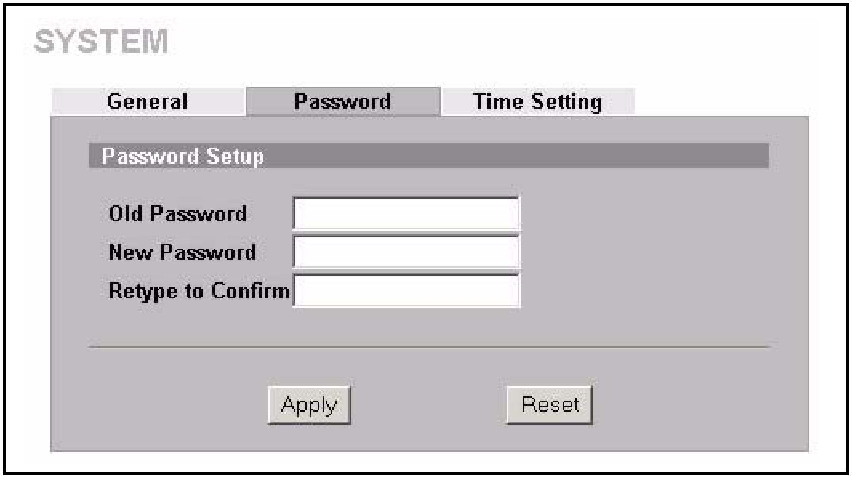
| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Select **From DHCP** if your ISP dynamically assigns DNS server information. The field to the right displays the (read-only) DNS server IP address that the DHCP assigns.<br>Select **User-Defined** if you have 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**.<br>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.<br>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. |

## 4.4 Configuring Password

To change your ZyAIR's password (recommended), click the **SYSTEM** link under **ADVANCED** 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 Section 2.3 on page 38 for details.

**Figure 18** Password.



The following table describes the labels in this screen.

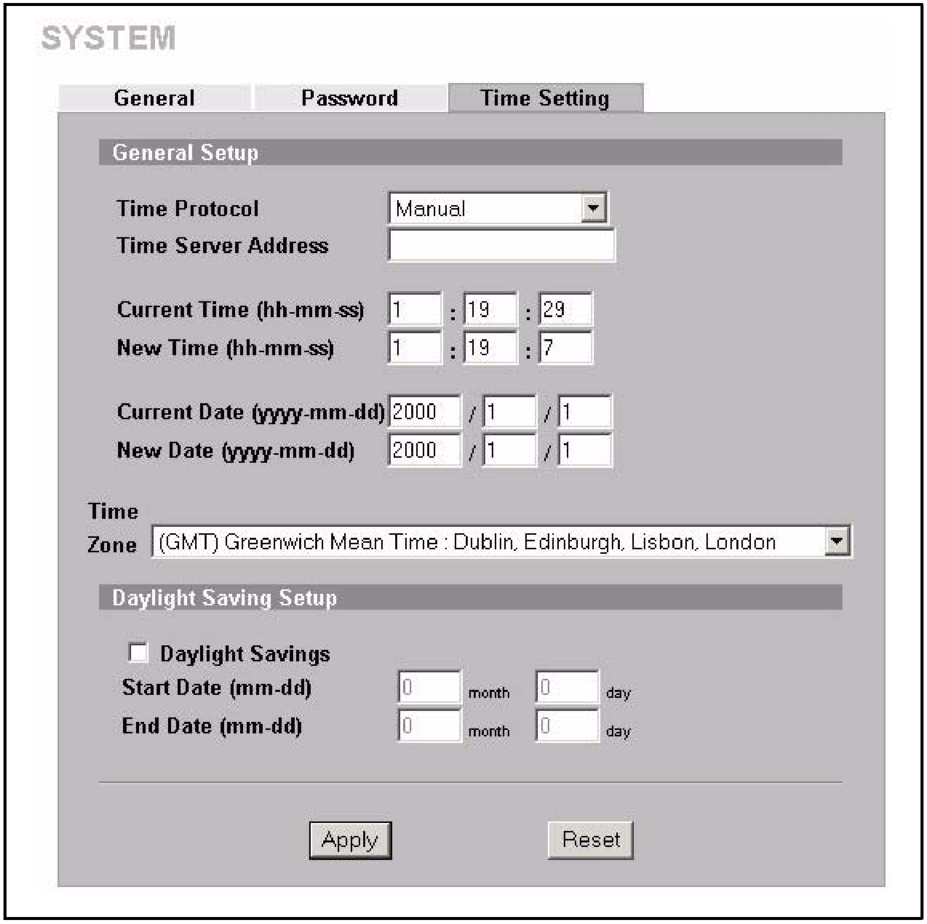
Table 8 Password

| LABEL | DESCRIPTIONS |
|---|---|
| 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. |

## 4.5 Configuring Time Setting

To change your ZyAIR's time and date, click the **SYSTEM** link under **ADVANCED** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the ZyAIR's time based on your local time zone.

Figure 19 Time Setting



SYSTEM

General | Password | Time Setting

General Setup

Time Protocol: Manual
Time Server Address:

Current Time (hh-mm-ss): 1 : 19 : 29
New Time (hh-mm-ss): 1 : 19 : 7

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 Saving Setup

□ Daylight Savings
Start Date (mm-dd): 0 month 0 day
End Date (mm-dd): 0 month 0 day

The following table describes the labels in this screen.

**Table 9** Time Setting

| LABEL | DESCRIPTION |
|---|---|
| Time Protocol | Select the time service protocol that your time server uses. 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.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**NTP (RFC 1305),** is similar to Time (RFC 868).<br>Select **Manual** to enter the time and date manually. |
| Time Server Address | Enter the IP address or the URL of your time server. Check with your ISP/ network administrator if you are unsure of this information. |
| Current Time (hh:mm:ss) | This field displays the time of your ZyAIR.<br>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.<br>When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**. |
| Current Date (yyyy/ mm/dd) | This field displays the date of your ZyAIR.<br>Each time you reload this page, the ZyAIR synchronizes the date with the time server. |
| New Date (yyyy/mm/ dd) | This field displays the last updated date from the time server.<br>When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**. |
| 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 saving 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-saving time starts on if you selected **Daylight Savings**. |
| End Date (mm-dd) | Enter the month and day that your daylight-saving time ends on if you selected **Daylight Savings**. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to reload the previous configuration for this screen. |

# CHAPTER 5 Wireless LAN

This chapter discusses how to configure wireless LAN.

## 5.1 Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

**Note:** See the WLAN appendix for more detailed information on WLANs.

## 5.2 Wireless Security Overview

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

Wireless security methods available on the ZyAIR are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyAIR identity.

### 5.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off.

### 5.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the ZyAIR.

- Use the Local User Database if you have less than 32 wireless clients in your network. The ZyAIR uses MD5 encryption when a client authenticates with the Local User Database

### 5.2.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

### 5.2.4 Hide ZyAIR Identity

If you hide the SSID, then the ZyAIR cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the ZyAIR may be inconvenience for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

### 5.2.5 Configuring Wireless LAN on the ZyAIR

1 Configure the **ESSID** and **WEP** in the **Wireless** screen.

2 Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.

3 Configure **WPA** or **WPA-PSK** in the **802.1x/WPA** screen. You can also configure 802.1x wireless client authentication in the **802.1x/WPA** screen.

4 Configure the RADIUS settings in the **AUTH. SERVER** screens.

The following table shows the relative effectiveness of these wireless security methods available on your ZyAIR.

**Table 10** ZyAIR Wireless Security Levels

| Security Level | Security Type |
|---|---|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| Most Secure | Wi-Fi Protected Access (WPA) |

**Note:** You must enable the same wireless security settings on the ZyAIR and on all wireless clients that you want to associate with it.

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

## 5.3 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

### 5.3.1 Rapid STP

The ZyAIR uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

### 5.3.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

**Table 11** STP Path Costs

| | LINK SPEED | RECOMMENDED VALUE | RECOMMENDED RANGE | ALLOWED RANGE |
|---|---|---|---|---|
| Path Cost | 4Mbps | 250 | 100 to 1000 | 1 to 65535 |
| Path Cost | 10Mbps | 100 | 50 to 600 | 1 to 65535 |
| Path Cost | 16Mbps | 62 | 40 to 400 | 1 to 65535 |
| Path Cost | 100Mbps | 19 | 10 to 60 | 1 to 65535 |
| Path Cost | 1Gbps | 4 | 3 to 10 | 1 to 65535 |
| Path Cost | 10Gbps | 2 | 1 to 5 | 1 to 65535 |

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

### 5.3.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

### 5.3.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

**Table 12** STP Port States

| PORT STATES | DESCRIPTIONS |
|---|---|
| Disabled | STP is disabled (default). |
| Blocking | Only configuration and management BPDUs are received and processed. |
| Listening | All BPDUs are received and processed. |
| Learning | All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded. |
| Forwarding | All BPDUs are received and processed. All information frames are received and forwarded. |

## 5.4 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

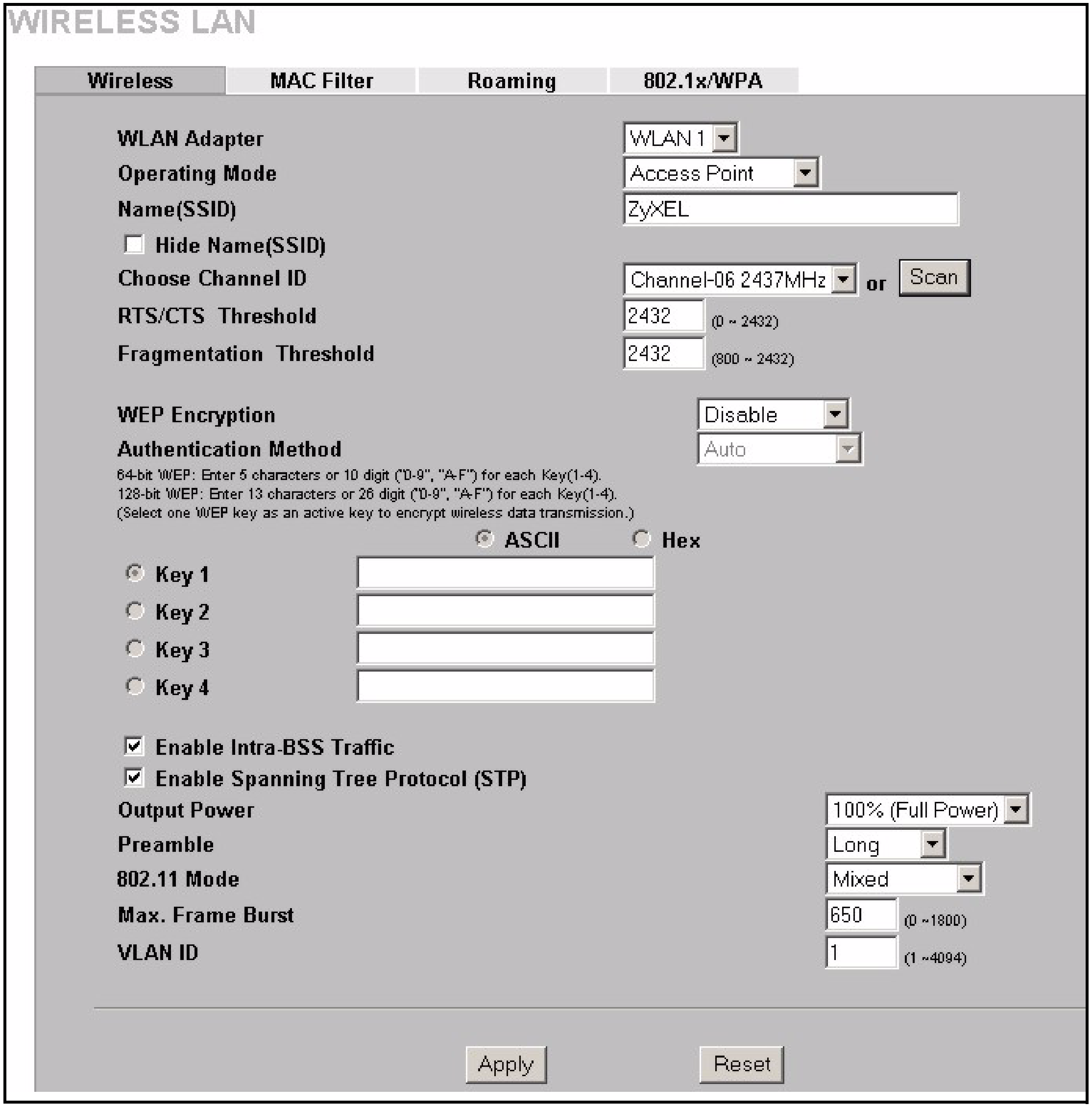
## 5.5 Configuring the Wireless Screen

Click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. The screen varies depending upon the operating mode you select.

## 5.5.1 Access Point Mode

Select **Access Point** in the **Operating Mode** drop-down list box to display the screen as shown next.

**Figure 20** Wireless: Access Point



| | |
|---|---|
| WLAN Adapter | WLAN 1 |
| Operating Mode | Access Point |
| Name(SSID) | ZyXEL |
| □ Hide Name(SSID) | |
| Choose Channel ID | Channel-06 2437MHz or Scan |
| RTS/CTS Threshold | 2432 (0 ~ 2432) |
| Fragmentation Threshold | 2432 (800 ~ 2432) |
| WEP Encryption | Disable |
| Authentication Method | Auto |

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("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 Intra-BSS Traffic
☑ Enable Spanning Tree Protocol (STP)

| | |
|---|---|
| Output Power | 100% (Full Power) |
| Preamble | Long |
| 802.11 Mode | Mixed |
| Max. Frame Burst | 650 (0 ~1800) |
| VLAN ID | 1 (1 ~4094) |

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

**Table 13** Wireless: Access Point

| LABEL | DESCRIPTION |
|---|---|
| WLAN Adapter | Select which WLAN adapter you want to configure.<br>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions. |
| Operating Mode | Select the operating mode from the drop-down list. The options are **Access Point**, **Bridge/Repeater** and **AP+Bridge**. |
| Name (SSID) | (Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>**Note:** If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's SSID or WEP settings, you will lose your wireless connection when you click **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings. |
| Hide Name (SSID) | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool. |
| Choose Channel ID | Set the operating frequency/channel depending on your particular region.<br>To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.<br>To have the ZyAIR automatically select a channel, click **Scan** instead. |
| Scan | Click this button to have the ZyAIR automatically scan for and select a channel with the least interference. |
| RTS/CTS Threshold | (Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**. |
| Fragmentation Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **800** and **2432**. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.<br>Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Authentication Method | If you use WEP encryption, select **Auto**, **Open System** or **Shared Key** from the drop-down list box. |

**Table 13** Wireless: Access Point (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.<br>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. |
| Enable Intra-BSS Traffic | Intra-BSS traffic is traffic between wireless stations in the same BSS.<br>Enable Intra-BSS traffic to allow wireless stations connected to the ZyAIR to communicate with each other.<br>Disable Intra-BSS traffic to only allow wireless stations to communicate with the wired network, not with each other. |
| Enable Spanning Tree Protocol (STP) | (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyAIR. |
| Output Power | Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. The options are **100% (Full Power)**, **50%**, **25%** or **12.5%**. The power output at full power is 18 ± 2 dBm. |
| Preamble | Preamble is used to signal that data is coming to the receiver.<br>Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble.<br>Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.<br>Select **Dynamic** to have the ZyAIR automatically use short preamble when all wireless clients support it, otherwise the ZyAIR uses long preamble.<br>**Note:** The ZyAIR and the wireless stations MUST use the same preamble mode in order to communicate. |
| 802.11 Mode | Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.<br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.<br>Select **Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced. |
| Max. Frame Burst | Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only.<br>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. |

**Table 13** Wireless: Access Point (continued)

| LABEL | DESCRIPTION |
|---|---|
| VLAN ID | The ZyAIR supports IEEE 802.1 tagged VLAN for partioning a physical network into multiple logical networks. Enter a number from 1 to 4094 to set the VLAN ID tag that the ZyAIR adds to the Ethernet frames that this WLAN adapter receives from wireless clients or other APs.<br>Use the **VLAN** screen to enable or disable the ZyAIR's VLAN feature. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

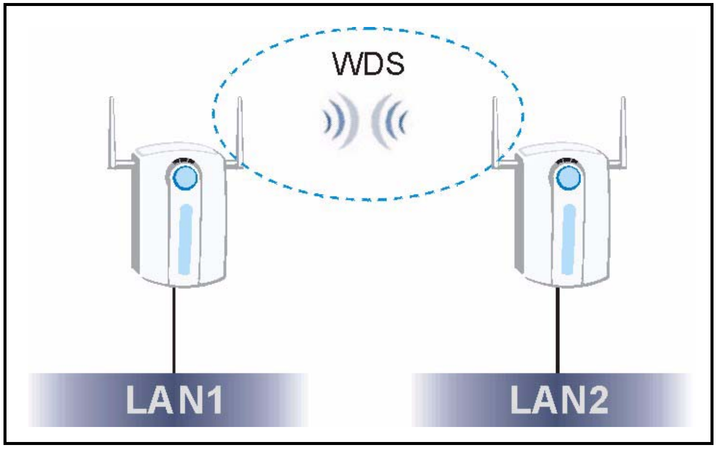
## 5.5.2 Bridge/Repeater Mode

The ZyAIR can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

The ZyAIR can establish wireless links with other APs.

In the example below, when both ZyAIRs are in Bridge/Repeater mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

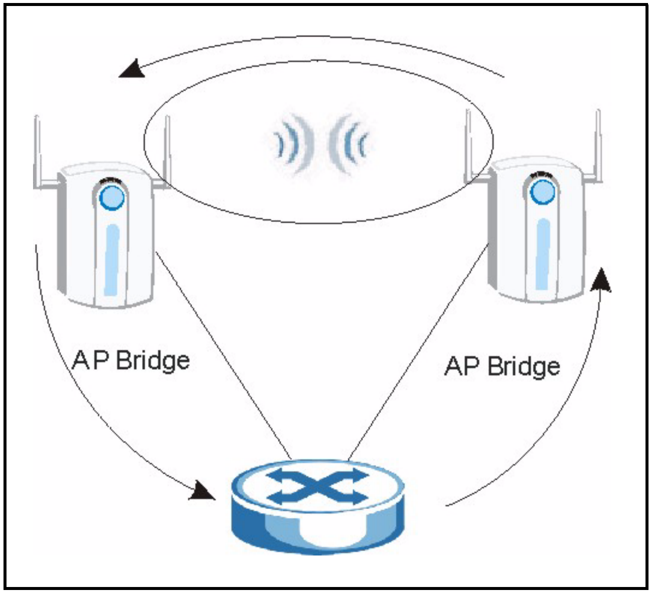
**Figure 21** Bridging Example



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

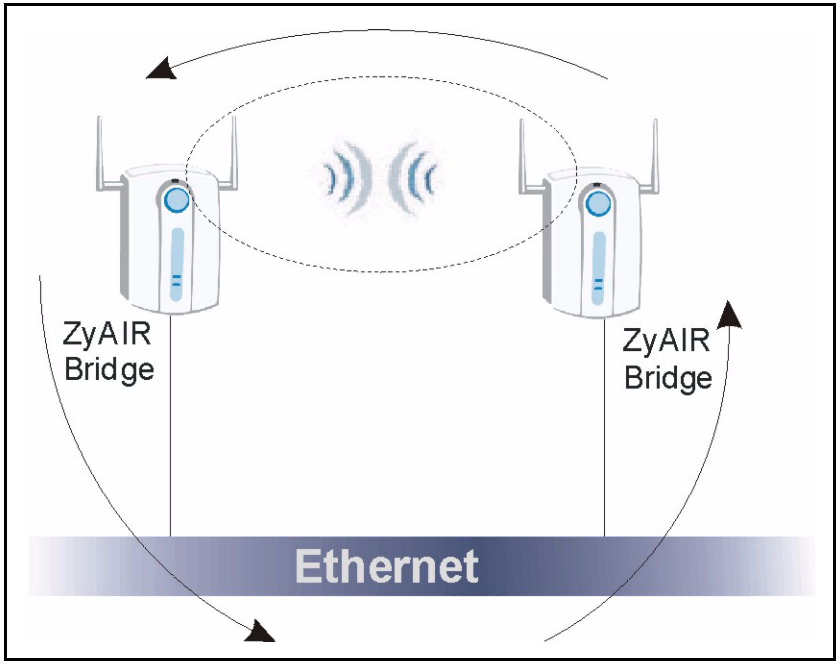
If two or more ZyAIRs (in bridge mode) are connected to the same hub as shown next.

**Figure 22** Bridge Loop: Two Bridges Connected to Hub



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

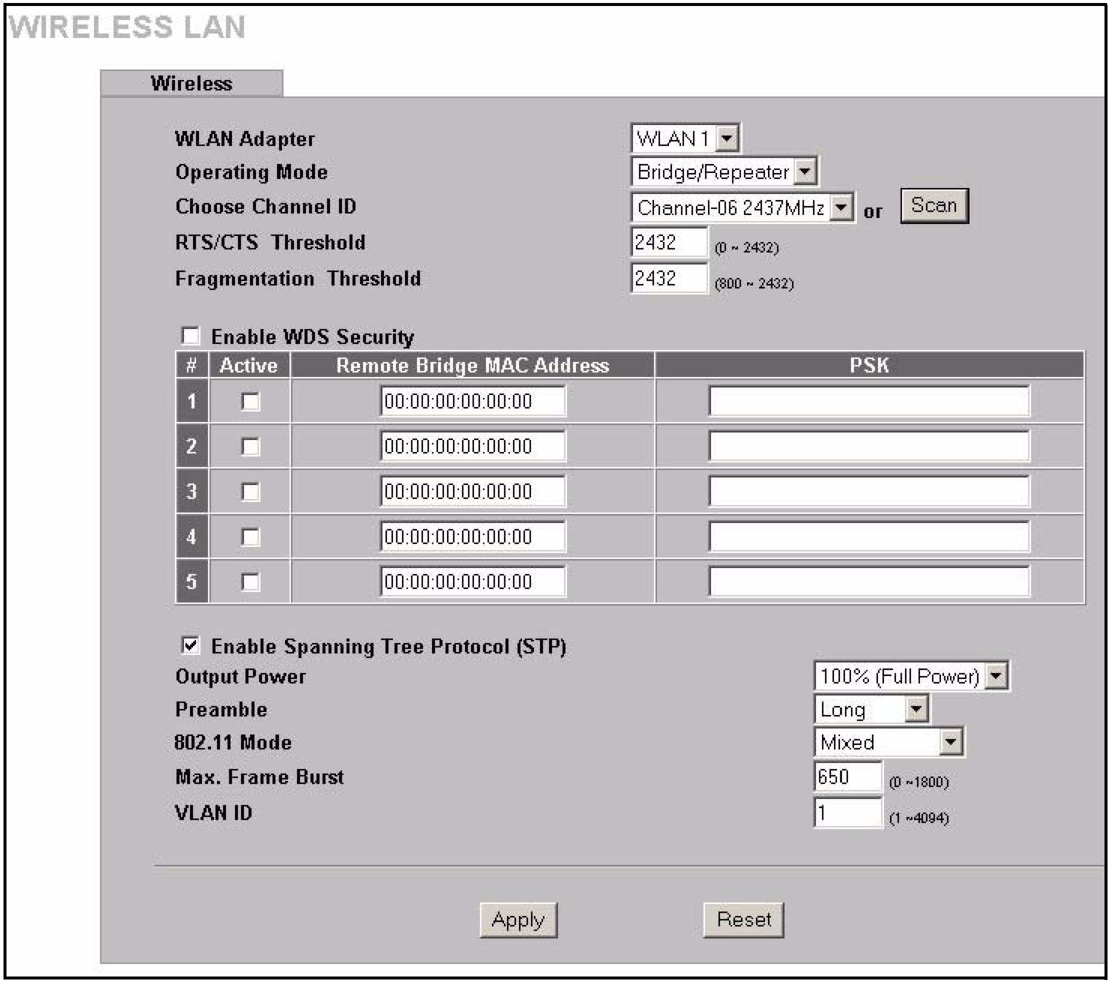
**Figure 23** Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyAIR is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

Click the **WIRELESS** link under **ADVANCED**. Select **Bridge/Repeater** in the **Operating Mode** drop-down list box to have the ZyAIR act as a wireless bridge only.

**Figure 24** Wireless: Bridge/Repeater



WIRELESS LAN

Wireless

WLAN Adapter: WLAN 1

Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

□ Enable WDS Security

| # | Active | Remote Bridge MAC Address | PSK |
|---|---|---|---|
| 1 | □ | 00:00:00:00:00:00 | |
| 2 | □ | 00:00:00:00:00:00 | |
| 3 | □ | 00:00:00:00:00:00 | |
| 4 | □ | 00:00:00:00:00:00 | |
| 5 | □ | 00:00:00:00:00:00 | |

☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 1 (1 ~4094)

The following table describes the labels in this screen that are specific to bridge/repeater mode.

**Table 14** Wireless: Bridge/Repeater

| LABEL | DESCRIPTIONS |
|---|---|
| WLAN Adapter | Select which WLAN adapter you want to configure.<br>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions. |
| Operating Mode | Select **Bridge/Repeater** in this field to display the screen shown above. |
| Enable WDS Security | A Wireless Distribution System (WDS) is a wireless connection between two or more APs.<br>Select the check box to use TKIP to encrypt traffic on the WDS between APs.<br>When you enable WDS security, type a Pre-Shared Key (PSK) for each link.<br>**Note:** Other APs must use the same encryption method in order to communicate with the ZyAIR when you enable WDS security. |
| # | This is the index number of the bridge connection. |
| Active | Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it. |

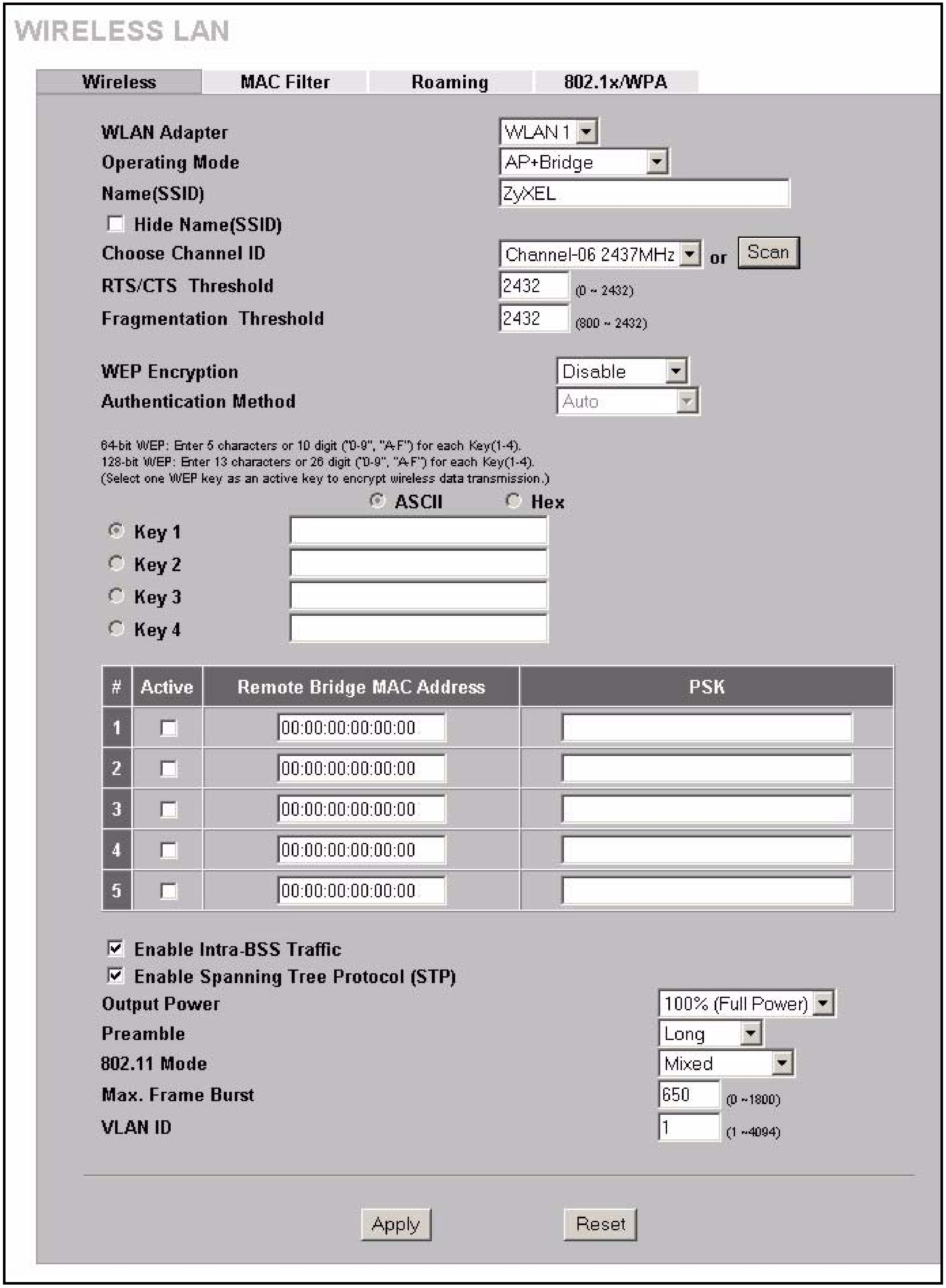
**Table 14** Wireless: Bridge/Repeater (continued)

| LABEL | DESCRIPTIONS |
|---|---|
| Remote Bridge MAC Address | Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| PSK | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).<br>When the ZyAIR is in **Bridge/Repeater** mode, you don't have to enter a pre-shared key, but the traffic between devices won't be encrypted if you don't. The peer bridge must use the same pre-shared key and encryption method. |
| Enable Spanning Tree Protocol (STP) | Select the check box to activate STP on the ZyAIR. |

### 5.5.3 AP+Bridge Mode

Click the **WIRELESS** link under **ADVANCED**. Select **AP+Bridge** in the **Operating Mode** drop-down list box to display the screen as shown next. In this screen, you can configure the ZyAIR to function as an AP and bridge simultaneously. See the section on ZyAIR applications for more information.

**Figure 25** Wireless: AP+Bridge



WLAN Adapter: WLAN 1

Operating Mode: AP+Bridge

Name(SSID): ZyXEL

□ Hide Name(SSID)

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("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

| # | Active | Remote Bridge MAC Address | PSK |
|---|---|---|---|
| 1 | □ | 00:00:00:00:00:00 | |
| 2 | □ | 00:00:00:00:00:00 | |
| 3 | □ | 00:00:00:00:00:00 | |
| 4 | □ | 00:00:00:00:00:00 | |
| 5 | □ | 00:00:00:00:00:00 | |

☑ Enable Intra-BSS Traffic

☑ Enable Spanning Tree Protocol (STP)

Output Power: 100% (Full Power)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 1 (1 ~4094)

See Table 13 on page 60 and Table 14 on page 64 descriptions of the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

When you enable WEP encryption, you can also specify MAC addresses and pre-shared keys of peer bridges in order to use TKIP (see Appendix F on page 221 for more on TKIP) to encrypt traffic between the bridges.

**Note:** The following screens are configurable only in Access Point and AP+Bridge operating modes.

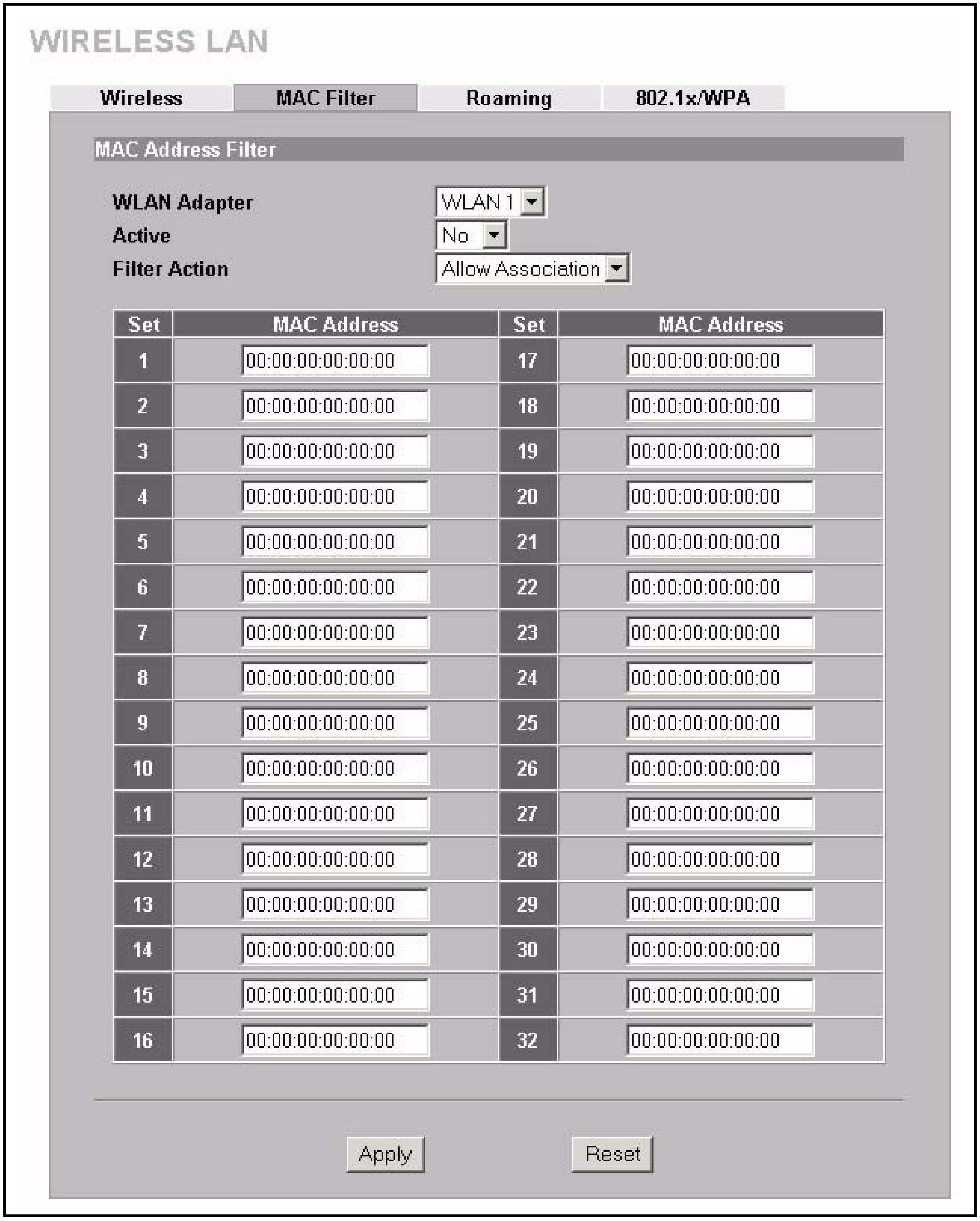
## 5.6 Configuring MAC Filters

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 the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

**Note:** Be careful not to list your computer's MAC address and set the **Action** field to **Deny Association** when managing the ZyAIR via a wireless connection. This would lock you out.

**Figure 26** MAC Address Filter



MAC Address Filter

WLAN Adapter: WLAN 1

Active: No

Filter Action: Allow Association

| Set | MAC Address | Set | MAC Address |
|---|---|---|---|
| 1 | 00:00:00:00:00:00 | 17 | 00:00:00:00:00:00 |
| 2 | 00:00:00:00:00:00 | 18 | 00:00:00:00:00:00 |
| 3 | 00:00:00:00:00:00 | 19 | 00:00:00:00:00:00 |
| 4 | 00:00:00:00:00:00 | 20 | 00:00:00:00:00:00 |
| 5 | 00:00:00:00:00:00 | 21 | 00:00:00:00:00:00 |
| 6 | 00:00:00:00:00:00 | 22 | 00:00:00:00:00:00 |
| 7 | 00:00:00:00:00:00 | 23 | 00:00:00:00:00:00 |
| 8 | 00:00:00:00:00:00 | 24 | 00:00:00:00:00:00 |
| 9 | 00:00:00:00:00:00 | 25 | 00:00:00:00:00:00 |
| 10 | 00:00:00:00:00:00 | 26 | 00:00:00:00:00:00 |
| 11 | 00:00:00:00:00:00 | 27 | 00:00:00:00:00:00 |
| 12 | 00:00:00:00:00:00 | 28 | 00:00:00:00:00:00 |
| 13 | 00:00:00:00:00:00 | 29 | 00:00:00:00:00:00 |
| 14 | 00:00:00:00:00:00 | 30 | 00:00:00:00:00:00 |
| 15 | 00:00:00:00:00:00 | 31 | 00:00:00:00:00:00 |
| 16 | 00:00:00:00:00:00 | 32 | 00:00:00:00:00:00 |

The following table describes the labels in this screen.

**Table 15** MAC Address Filter

| LABEL | DESCRIPTION |
|---|---|
| WLAN Adapter | Select the WLAN adapter for which you want to configure MAC address filtering. |
| Active | Select **Yes** from the drop down list box to enable MAC address filtering. |

**Table 15** MAC Address Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router.<br>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. |

## 5.7 Configuring Roaming

A wireless station is a device with an IEEE 802.11b or an IEEE 802.11g compliant wireless interface. 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.

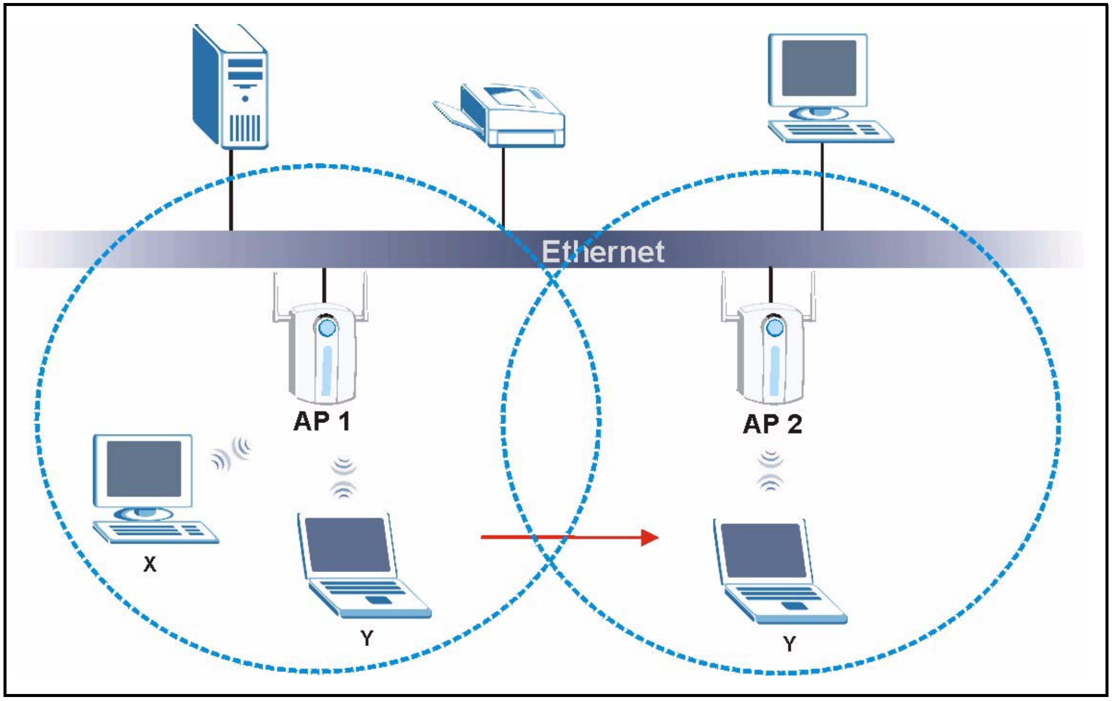
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending 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 27 on page 70.

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.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). IEEE 802.1x authentication information is not exchanged (at the time of writing).

**Figure 27** Roaming Example



The steps below describe the roaming process.

1. As wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point
2. **AP 2**, it scans and uses the signal of access point **AP 2**.
3. Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
4. Access point **AP 1** updates the new position of wireless station.
5. Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

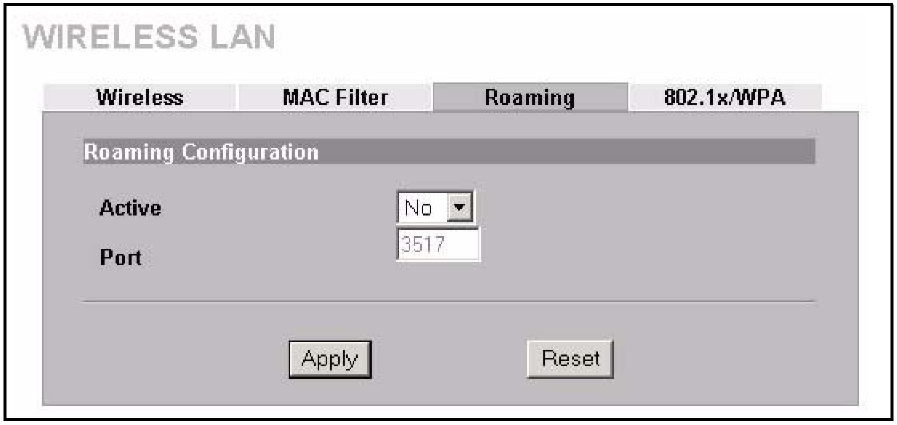
## 5.7.1 Requirements for Roaming

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 SSID.
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 the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

**Figure 28** Roaming



WIRELESS LAN

Wireless | MAC Filter | Roaming | 802.1x/WPA

Roaming Configuration

Active: No

Port: 3517

The following table describes the labels in this screen.

**Table 16** Roaming

| LABEL | DESCRIPTION |
|---|---|
| Active | Select **Yes** from the drop-down list box to enable roaming on the ZyAIR if you have two or more APs on the same subnet.<br>**Note:** All APs on the same subnet and the wireless stations must have the same SSID 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 3517. 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. |

## 5.8 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

## 5.9 WPA-PSK Application Example

A WPA-PSK application looks as follows.

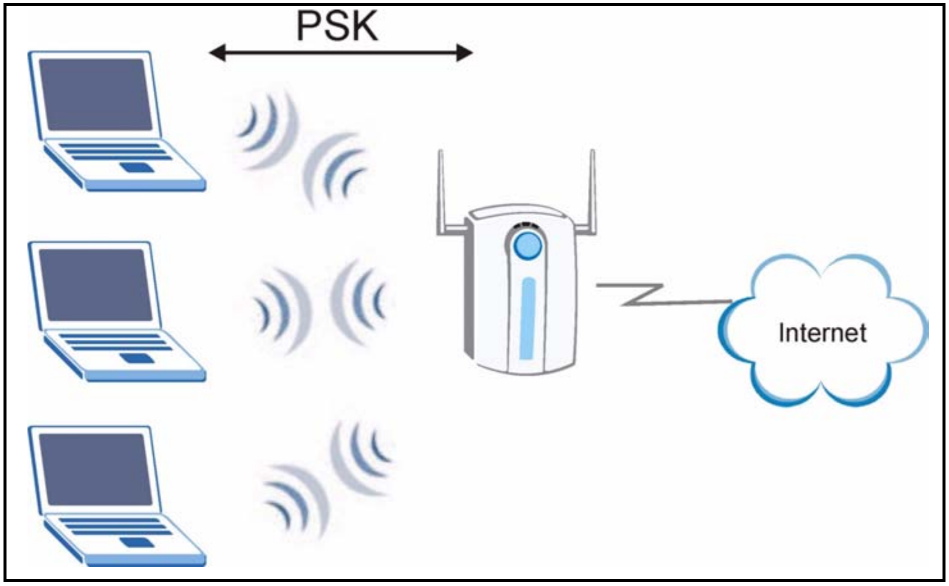
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

2 The AP checks each client's password and (only) allows it to join the network if it matches its password.

3 The AP derives and distributes keys to the wireless clients.

4 The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

**Figure 29 WPA - PSK Authentication**



## 5.10 WPA with RADIUS Application Example

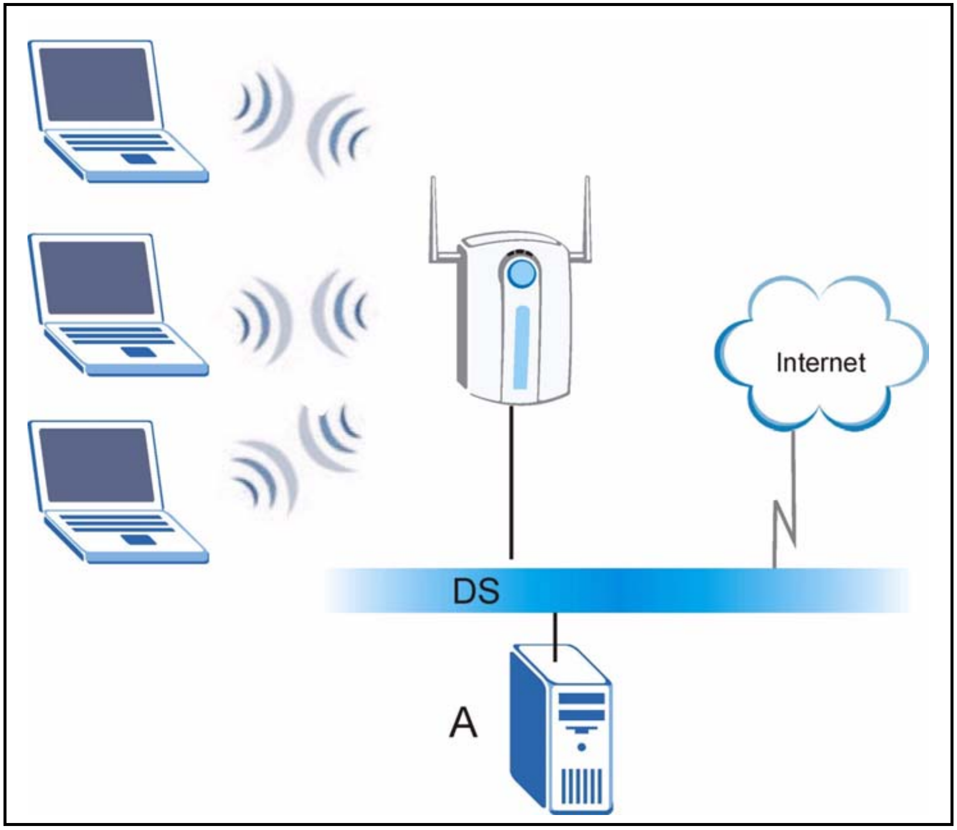
This example is for using WPA with an external RADIUS server. You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 30** WPA with RADIUS Application Example



## 5.11 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

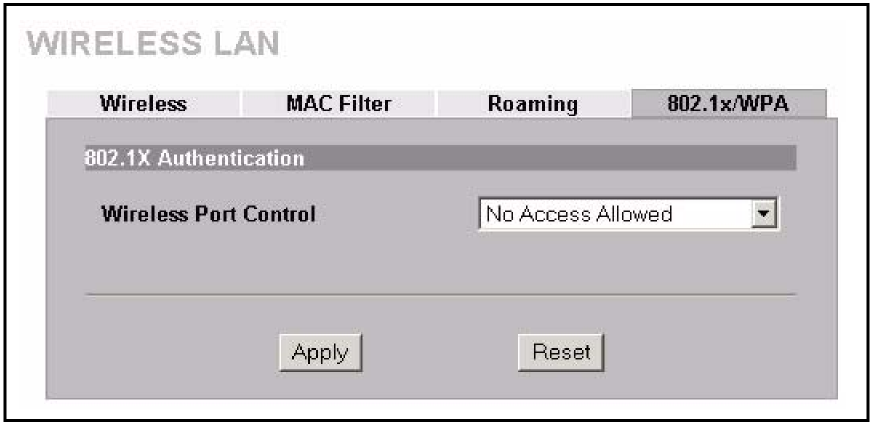
The Funk Software's Odyssey client is bundled free (at the time of writing) with some of ZyXEL's client wireless adapter(s).

## 5.12 Configuring 802.1x and WPA

To change your ZyAIR's authentication settings, click the **WIRELESS** link under **ADVANCED** and then the **802.1x/WPA** tab. The screen varies by the key management protocol you select. The WPA function is not available on all ZyAIR models.

You see the next screen when you select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control** field.

**Figure 31** Wireless LAN: 802.1x/WPA



Wireless Port Control: No Access Allowed

The following table describes the labels in this screen.

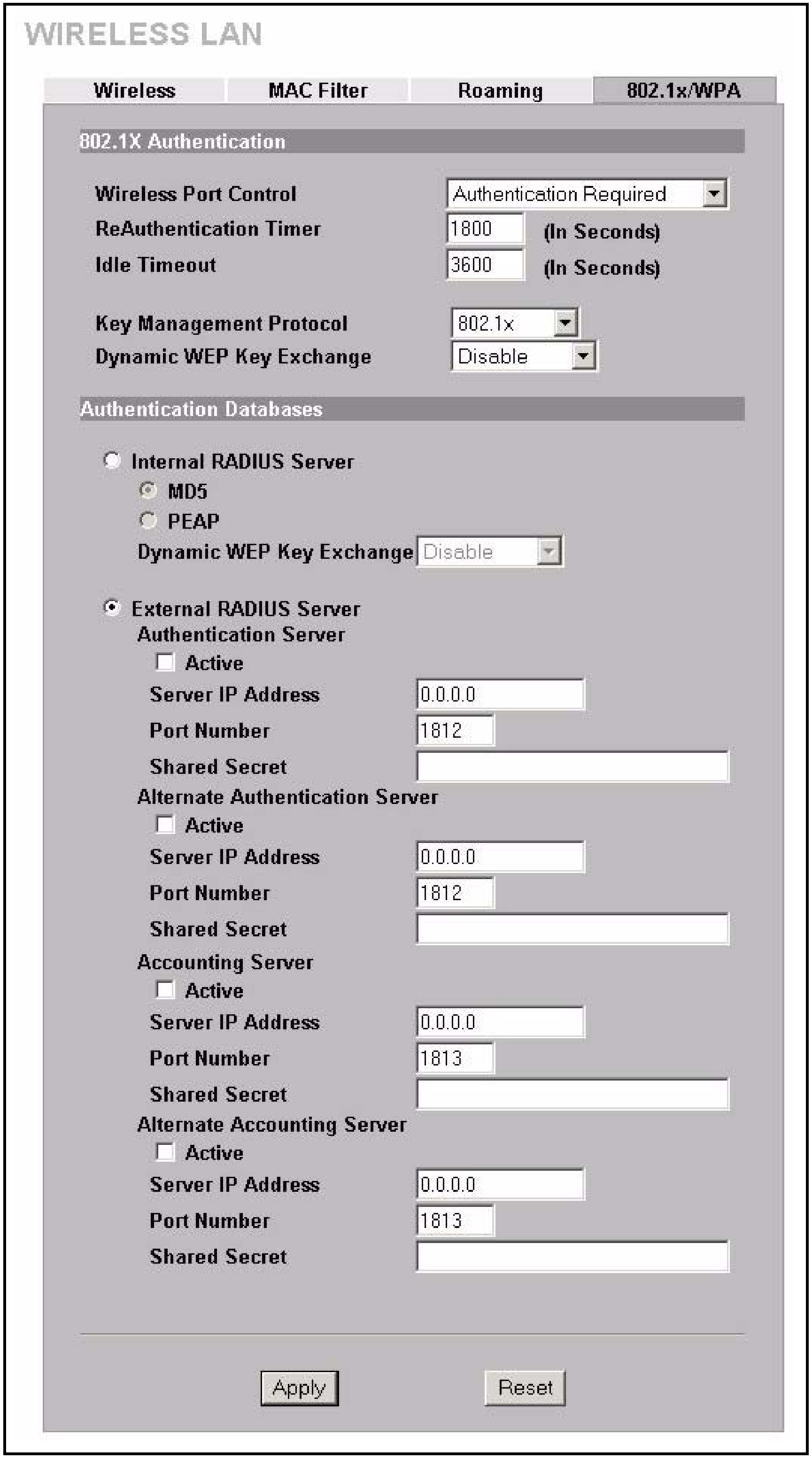
**Table 17** Wireless LAN: 802.1x/WPA

| 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 Access Allowed**, **No Authentication Required** and **Authentication Required**.<br>**No Access Allowed** blocks all wireless stations access to the wired network.<br>**No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.<br>**Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>Select **Authentication Required** to configure **Key Management Protocol** and other related fields. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.13 Authentication Required: 802.1x

Select **Authentication Required** in the **Wireless Port Control** field and **802.1x** in the **Key Management Protocol** field to display the next screen.

**Figure 32** Wireless LAN: 802.1x/WPA for 802.1x Protocol



WIRELESS LAN

802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

Authentication Databases

○ Internal RADIUS Server

● MD5

○ PEAP

Dynamic WEP Key Exchange: Disable

● External RADIUS Server

Authentication Server

□ Active

Server IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Alternate Authentication Server

□ Active

Server IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server

□ Active

Server IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

Alternate Accounting Server

□ Active

Server IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

The following table describes the labels in this screen.

**Table 18** Wireless LAN: 802.1x/WPA for 802.1x Protocol

| 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**.<br>**No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.<br>**Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>**No Access Allowed** blocks all wireless stations access to the wired network.<br>The following fields are only available when you select **Authentication Required**. |
| 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.<br>Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes).<br>**Note:** 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.<br>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). |
| Key Management Protocol | Choose **802.1x** from the drop-down list. |
| Dynamic WEP Key Exchange | This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field.<br>Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption.<br>This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**. |
| Authentication Databases | The authentication database contains wireless station login information. |
| Internal RADIUS Server | Select this radio button to use the ZyAIR's **Internal RADIUS Server**.<br>Select the **MD5** radio button to use this EAP authentication type to authenticate other APs or wireless clients in other wireless networks.<br>Select the **PEAP** radio button to use this EAP authentication type to authenticate other APs or wireless clients in other wireless networks. Use the drop-down list box to select **Disable**, **64-bit WEP** or **128-bit WEP** for Dynamic WEP Exchange.<br>**Note:** MD5 cannot be used with Dynamic WEP Key Exchange. |
| External RADIUS Server | Select the radio button to use an external radius server to authenticate the ZyAIR's wireless clients.<br>Configure the server(s) details in the following fields. |

**Table 18** Wireless LAN: 802.1x/WPA for 802.1x Protocol (continued)

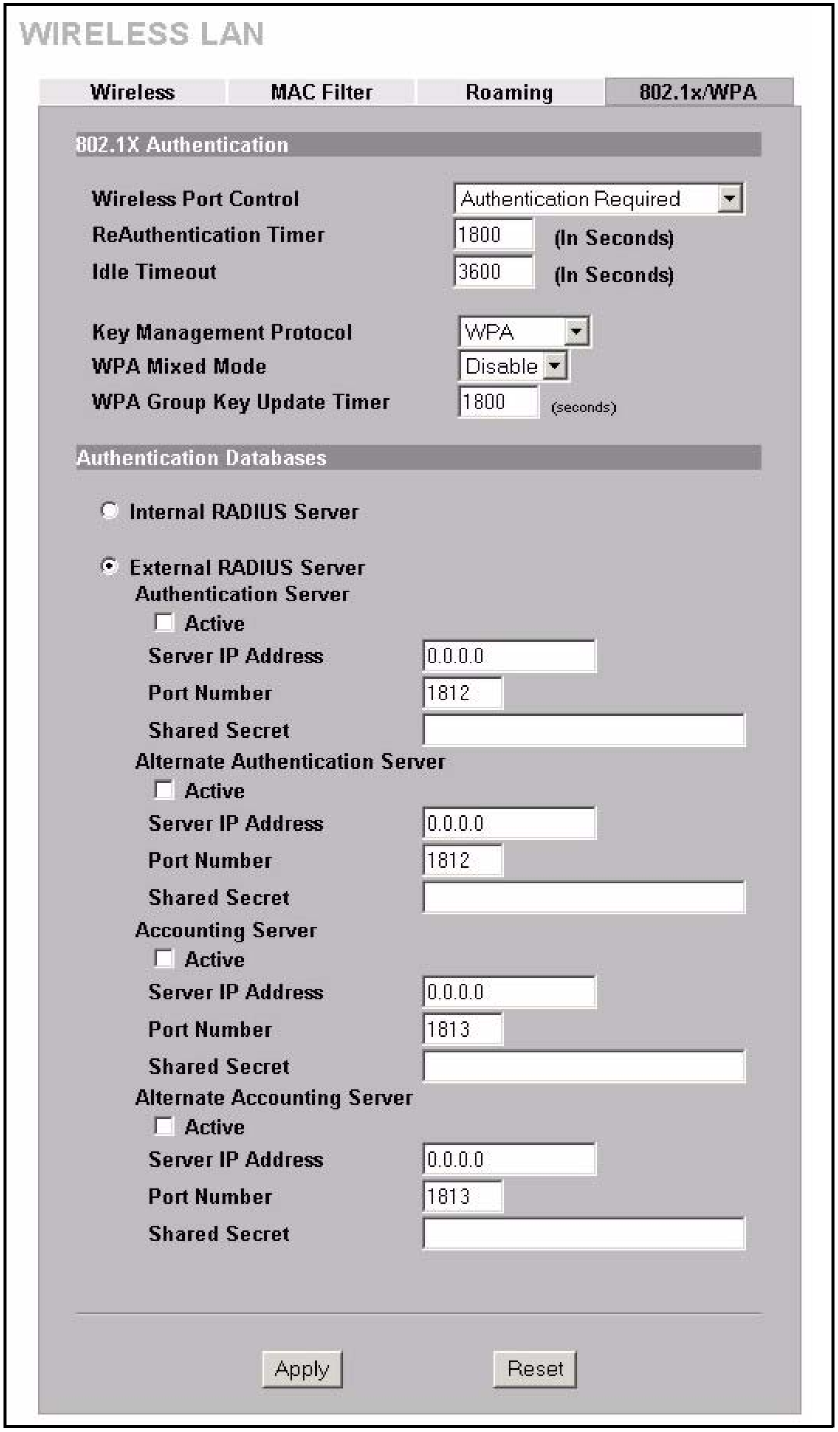
| LABEL | DESCRIPTION |
|---|---|
| Authentication Server /Alternate | The ZyAIR will make three attempts to authenticate wireless users using the authentication server before attempting to use the alternate authentication server.<br>Requests can be issued from the client interface to use the alternate authentication server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field.<br>**Note:** You can use the command line interface to configure the ZyAIR to use up to four alternate authentication servers. |
| Active | Select **Active** to enable user authentication through this external authentication server.<br>Clear the **Active** check box to not use this to not perform user authentication through this external authentication server. |
| 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.<br>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.<br>The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network. |
| Accounting Server /Alternate | The ZyAIR will make three attempts to communicate with the accounting server before attempting to use the alternate accounting server.<br>**Note:** You can use the command line interface to configure the ZyAIR to use up to four alternate accounting servers. |
| Active | Select **Active** to enable user accounting through this external accounting server.<br>Clear the **Active** check box to not use this to not perform user accounting through this external accounting 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.<br>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 accounting server and the ZyAIR.<br>The key must be the same on the external accounting 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. |

**Note:** If you enable the ZyAIR’s internal RADIUS server, configure trusted user accounts in the **AUTH SERVER Trusted Users** screen.

## 5.14 Authentication Required: WPA

Select **Authentication Required** in the **Wireless Port Control** field and **WPA** in the **Key Management Protocol** field to display the next screen.

**Figure 33** Wireless LAN: 802.1x/WPA for WPA Protocol



802.1X Authentication

| | | |
|---|---|---|
| Wireless Port Control | Authentication Required | |
| ReAuthentication Timer | 1800 | (In Seconds) |
| Idle Timeout | 3600 | (In Seconds) |
| Key Management Protocol | WPA | |
| WPA Mixed Mode | Disable | |
| WPA Group Key Update Timer | 1800 | (seconds) |

Authentication Databases

○ Internal RADIUS Server

● External RADIUS Server

Authentication Server

| | |
|---|---|
| □ Active | |
| Server IP Address | 0.0.0.0 |
| Port Number | 1812 |
| Shared Secret | |

Alternate Authentication Server

| | |
|---|---|
| □ Active | |
| Server IP Address | 0.0.0.0 |
| Port Number | 1812 |
| Shared Secret | |

Accounting Server

| | |
|---|---|
| □ Active | |
| Server IP Address | 0.0.0.0 |
| Port Number | 1813 |
| Shared Secret | |

Alternate Accounting Server

| | |
|---|---|
| □ Active | |
| Server IP Address | 0.0.0.0 |
| Port Number | 1813 |
| Shared Secret | |

The following table describes the labels not previously discussed.

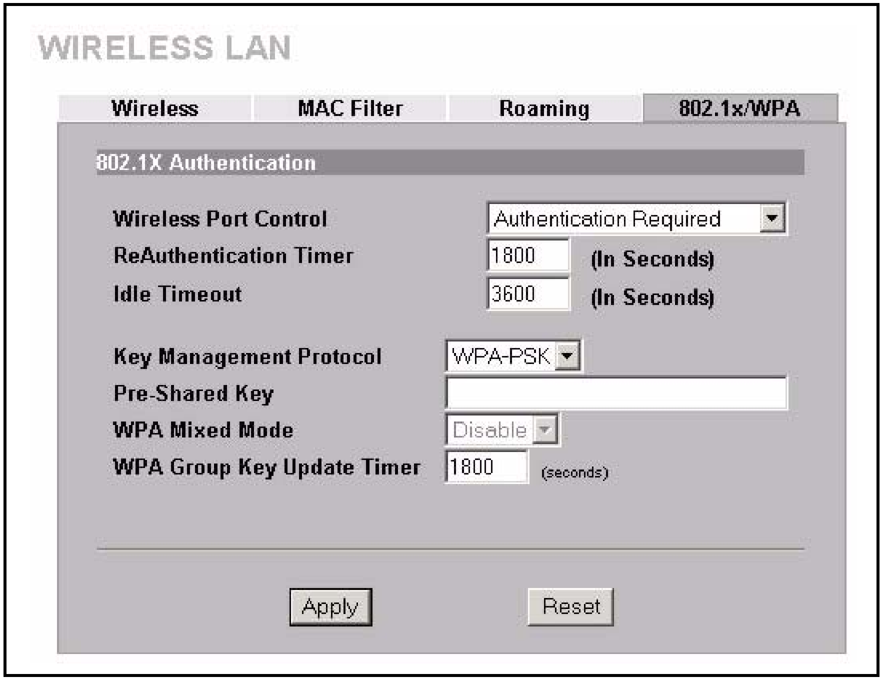
**Table 19** Wireless LAN: 802.1x/WPA for WPA Protocol

| LABEL | DESCRIPTIONS |
|---|---|
| Key Management Protocol | Choose **WPA** in this field. |
| WPA Mixed Mode | The ZyAIR can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with IEEE 802.1x in the same Wi-Fi network.<br>Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable**. |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes). |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.15 Authentication Required: WPA-PSK

Select **Authentication Required** in the **Wireless Port Control** field and **WPA-PSK** in the **Key Management Protocol** field to display the next screen.

**Figure 34** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol



Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)
Key Management Protocol: WPA-PSK
Pre-Shared Key:
WPA Mixed Mode: Disable
WPA Group Key Update Timer: 1800 (seconds)

The following table describes the labels not previously discussed.

**Table 20** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

| LABEL | DESCRIPTION |
|---|---|
| Key Management Protocol | Choose **WPA-PSK** in this field. |
| Pre-Shared Key | The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 6
# Internal RADIUS Server

The ZyAIR can use its internal RADIUS server to authenticate wireless clients. It can also serve as a RADIUS server to authenticate other APs and their wireless clients. For more background information on RADIUS, see the *Introduction to RADIUS* section.

## 6.1 Internal RADIUS Overview

The ZyAIR has a built-in RADIUS server that can authenticate wireless clients or other APs (that are configured as trusted APs).

The ZyAIR can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the appendices for more information on the types of EAP authentication and the internal RADIUS authentication method used in your ZyAIR.

**Figure 35** ZyAIR Authenticates Wireless Stations

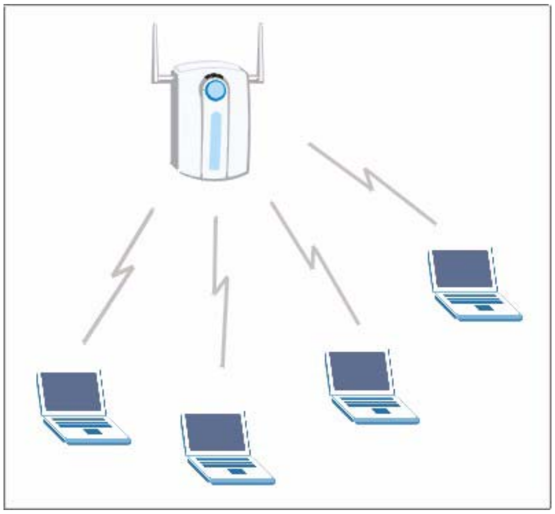


**Figure 36** ZyAIR Authenticates Trusted APs

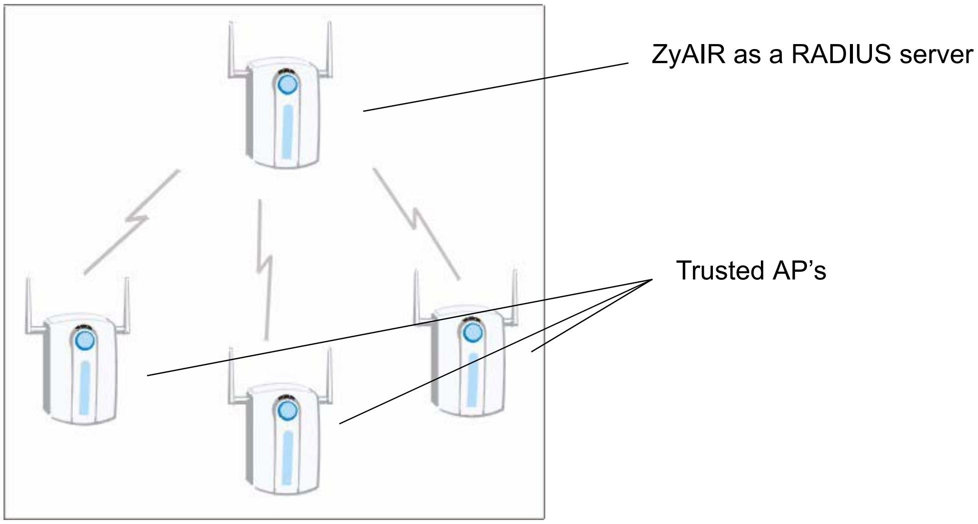


**Table 21** Internal RADIUS Server Screens Overview

| LABEL | DESCRIPTION |
|---|---|
| Setting | Use the **Setting** screen to turn the ZyAIR's internal RADIUS server off or on and to view information about the ZyAIR's certificates. |
| Trusted AP | Use the **Trusted AP** screen to specify APs as trusted APs so they can use the ZyAIR's internal RADIUS server to authenticate wireless clients. You can set up to 31 trusted AP's. |
| Trusted Users | Use the **Trusted Users** screen to configure a list of wireless client user names and passwords for the ZyAIR to authenticate. The ZyAIR internal RADIUS server can authenticate up to 32 wireless clients. |

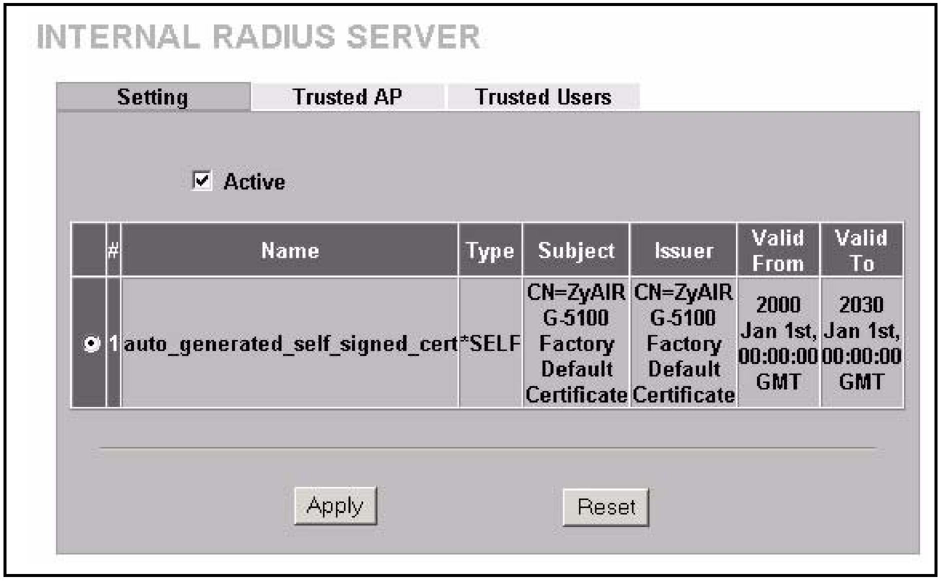
## 6.2 Internal RADIUS Server Setting

The **INTERNAL RADIUS SERVER Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless clients utility, for example, Funk Software's Odyssey client. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.

**Note:** The internal RADIUS server does not support domain accounts (DOMAIN/ user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/ MS-CHAPv2 settings, deselect the **Use Windows logon name and password** check box. When authentication begins, a pop-up dialog box requests you to type a **Name**, **Password** and **Domain** of the RADIUS server. Specify a name and password only, do not specify a domain.

Click the **AUTH SERVER** link under **ADVANCED** and then the **Setting** tab. The screen appears as shown.

**Figure 37** Internal RADIUS Server Setting Screen



☑ Active

| | # | Name | Type | Subject | Issuer | Valid From | Valid To |
|---|---|---|---|---|---|---|---|
| ● | 1 | auto_generated_self_signed_cert | *SELF | CN=ZyAIR G-5100 Factory Default Certificate | CN=ZyAIR G-5100 Factory Default Certificate | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT |

The following table describes the labels in this screen.

**Table 22** My Certificates

| LABEL | DESCRIPTION |
|---|---|
| Active | Select the **Active** check box to have the ZyAIR use its internal RADIUS server to authenticate wireless clients or other APs. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. Use the **CERTIFICATES** screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used, depends on the certificate information configured on the wireless client. |
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.<br>**auto_generated_self_signed_cert** is the factory default certificate common to all ZyAIR’s that use certificates.<br>**Note:** ZyXEL recommends that you replace the factory default certificate with one that uses your ZyAIR's MAC address. Do this when you first log in to the ZyAIR or in the **CERTIFICATES My Certificates** screen. |
| Type | This field displays what kind of certificate this is.<br>**REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request.<br>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate, which the ZyAIR uses to sign imported trusted remote host certificates.<br>**CERT** represents a certificate issued by a certification authority. |
| Subject | This field displays identifying information about the certificate’s owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information. |

**Table 22** My Certificates (continued)

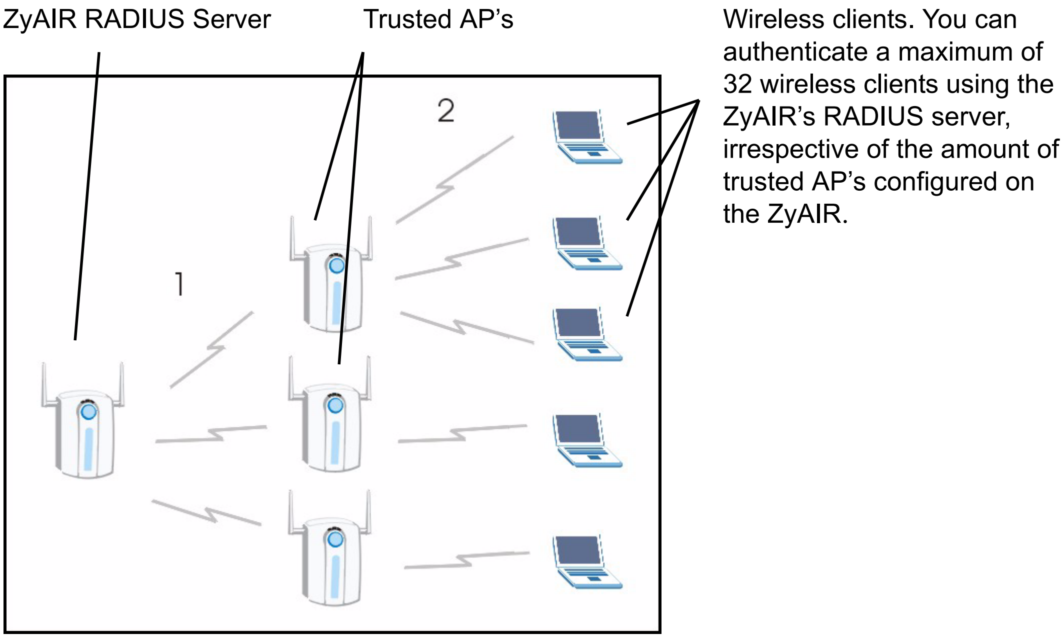
| LABEL | DESCRIPTION |
|---|---|
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired. |
| Apply | Click **Apply** to have the ZyAIR use certificates to authenticate wireless clients. |
| Reset | Click **Reset** to start configuring this screen afresh. |

## 6.3 Trusted AP Overview

A trusted AP is an AP that uses the ZyAIR's internal RADIUS server to authenticate its wireless clients. Each wireless client must have a user name and password configured in the **Trusted Users** screen.

The following figure shows how this is done in two phases.

**Figure 38** Trusted AP Overview



ZyAIR RADIUS Server
Trusted AP's
Wireless clients. You can authenticate a maximum of 32 wireless clients using the ZyAIR's RADIUS server, irrespective of the amount of trusted AP's configured on the ZyAIR.
2
1

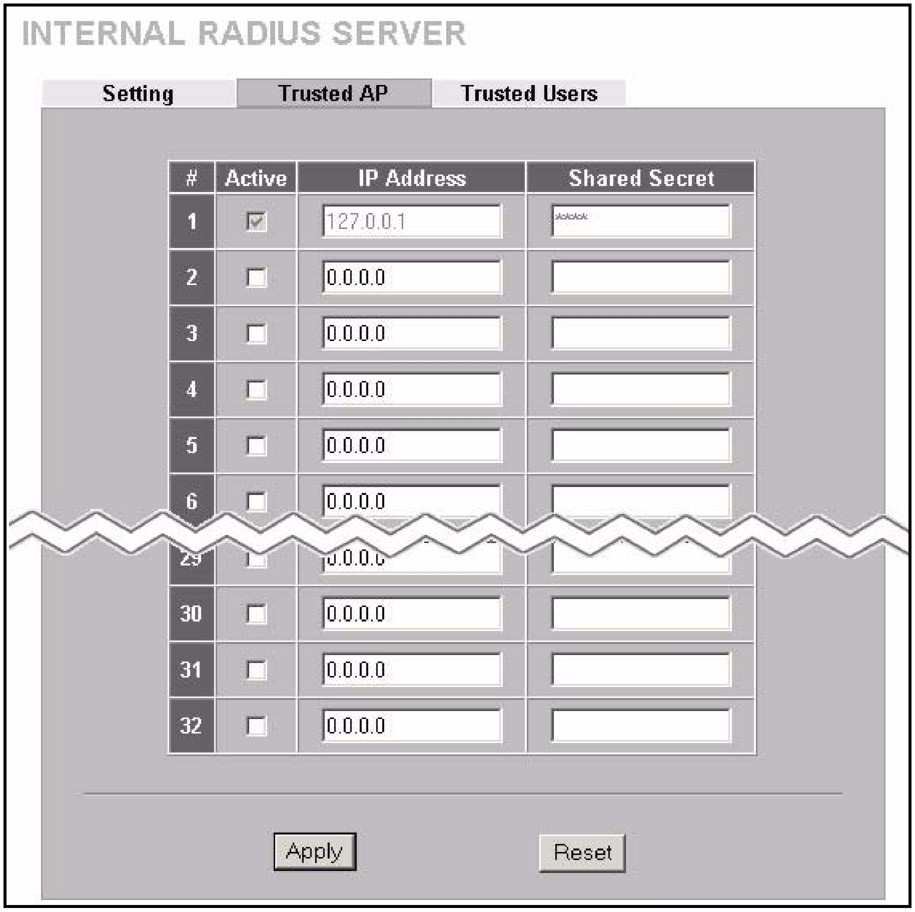
**1** Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.

**2** Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the ZyAIR's internal RADIUS server and the wireless clients. The wireless clients can then be authenticated by the ZyAIR's internal RADIUS server.

## 6.4 Configuring Trusted AP

To specify APs as trusted APs so they can use the ZyAIR's internal RADIUS server to authenticate wireless clients, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

**Figure 39** Trusted AP Screen



INTERNAL RADIUS SERVER

| # | Active | IP Address | Shared Secret |
|---|---|---|---|
| 1 | ☑ | 127.0.0.1 | **** |
| 2 | □ | 0.0.0.0 | |
| 3 | □ | 0.0.0.0 | |
| 4 | □ | 0.0.0.0 | |
| 5 | □ | 0.0.0.0 | |
| 6 | □ | 0.0.0.0 | |
| 29 | □ | 0.0.0.0 | |
| 30 | □ | 0.0.0.0 | |
| 31 | □ | 0.0.0.0 | |
| 32 | □ | 0.0.0.0 | |

The following table describes the labels in this screen.

**Table 23** Trusted AP

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the trusted AP index number. |
| Active | Select this check box to have the ZyAIR use the **IP Address** and **Shared Secret** to authenticate a trusted AP. |

**Table 23** Trusted AP

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Type the IP address of the trusted AP in dotted decimal notation. |
| Shared Secret | Enter a password (up to 31 alphanumeric characters, no spaces) as the key for encrypting communications between the AP and the ZyAIR. The key is not sent over the network. This key must be the same on the AP and the ZyAIR.<br>Both the ZyAIR's IP address and this shared secret must also be configured in the "external RADIUS" server fields of the trusted AP.<br>**Note:** The first trusted AP fields are for the ZyAIR itself. Use SMT menu 23.2 to configure them. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

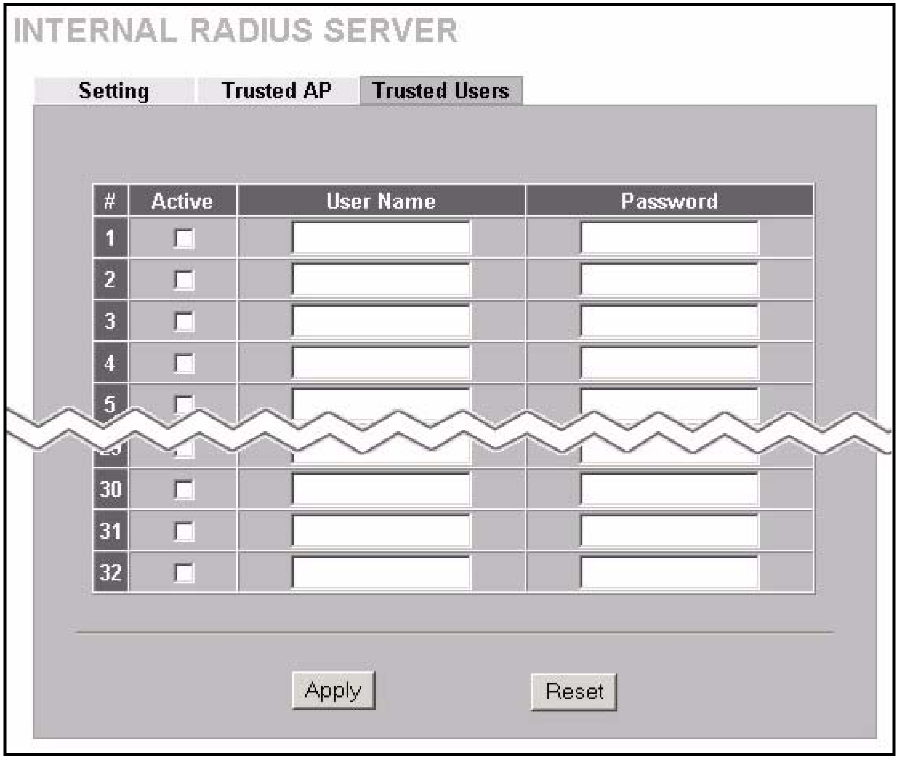
## 6.5 Trusted Users Overview

A trusted user entry consists of a wireless client user name and password

## 6.6 Configuring Trusted Users

To configure trusted user entries, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted Users** tab. The screen appears as shown.

**Figure 40** Trusted Users Screen



The following table describes the labels in this screen.

**Table 24** Trusted Users

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the trusted user index number. |
| Active | Select this check box to have the ZyAIR authenticate wireless clients with the same user name and password activated on their wireless utilities. |
| User Name | Enter the user name for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The wireless client's utility must use this name as its login name. |
| Password | Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.<br>The password on the wireless client's utility must be the same as this password.<br>**Note:** If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 7 VLAN

This chapter discusses how to configure VLAN on the ZyAIR

## 7.1 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to one or more groups. Only stations within the same group can talk to each other.

The ZyAIR supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyAIR can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

### 7.1.1 Management VLAN ID

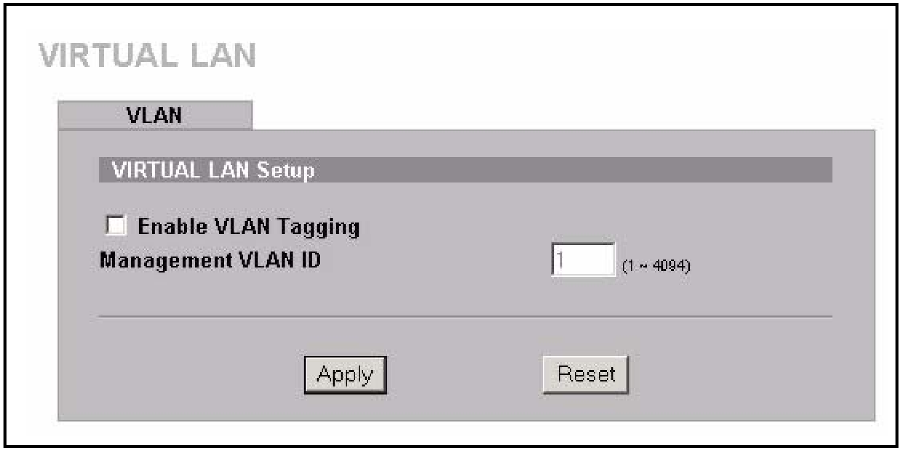
The management VLAN ID identifies the "management VLAN". A computer must be a member of this "management VLAN" in order to access and manage the ZyAIR. A computer that is not a member of this VLAN, then that device cannot manage the ZyAIR.

If no devices are in the management VLAN, then you will only be able to access the ZyAIR through the console port (not through the network).

## 7.2 Configuring VLAN

Click **ADVANCED** and then **VLAN**. The screen appears as shown next.

Figure 41 VLAN



VIRTUAL LAN

VIRTUAL LAN Setup

□ Enable VLAN Tagging

Management VLAN ID 1 (1 ~ 4094)

The following table describes the labels in this screen.

**Table 25** VLAN

| LABEL | DESCRIPTION |
|---|---|
| Enable VLAN Tagging | Select this check box to turn on VLAN tagging.<br>Use the **Wireless** screen to set the VLAN ID tag that the ZyAIR adds to the Ethernet frames that a WLAN adapter receives from wireless clients or APs. |
| Management VLAN ID | Enter a number from 1 to 4094 to define this VLAN group. Your management computer must belong to this VLAN group in order to manage the ZyAIR. This can be done in the following ways:<br>• The management computer could be a wireless client of the ZyAIR if the ZyAIR’s WLAN adapter is set to add the add the management VLAN ID tag to Ethernet frames received from wireless clients.<br>• The management computer could be on the wired network, behind a VLAN-aware switch that is configured to add the management VLAN ID tag to Ethernet frames from the computer before sending them to ZyAIR.<br>**Note:** Mail and FTP servers must have the same management VLAN ID to communicate with the ZyAIR. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 8 IP Screen

This chapter discusses how to configure IP on the ZyAIR

## 8.1 Factory Ethernet Defaults

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

1. IP address of 192.168.1.2
2. Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

## 8.2 IP Address and Subnet Mask

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

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

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

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

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

### 8.2.1 IP Address Assignment

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

**Table 26** Private IP Address Ranges

| | | |
|---|---|---|
| 10.0.0.0 | - | 10.255.255.255 |
| 172.16.0.0 | - | 172.31.255.255 |
| 192.168.0.0 | - | 192.168.255.255 |

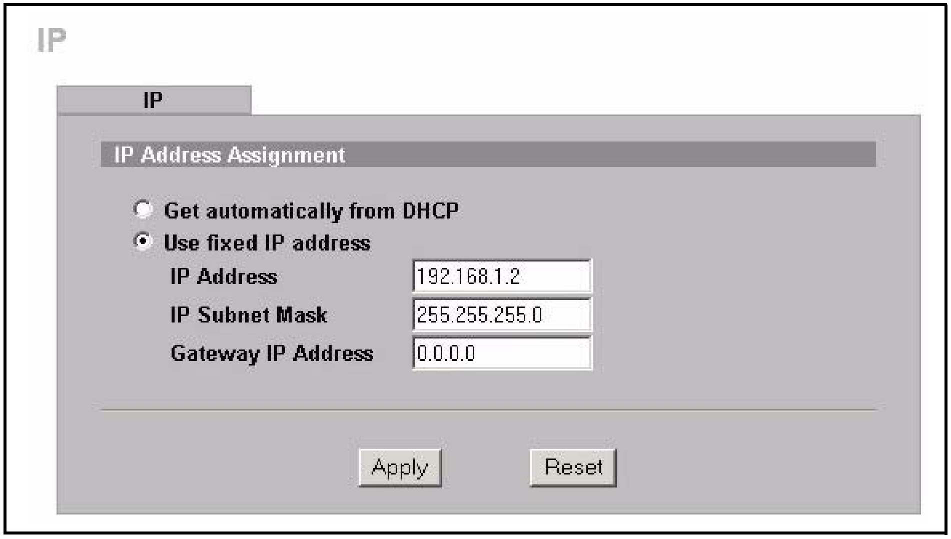
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much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

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

## 8.3 Configuring IP

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

**Figure 42** IP Setup



IP

IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address: 192.168.1.2

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

**Table 27** IP Setup

| LABEL | DESCRIPTION |
|---|---|
| IP Address Assignment | |
| Get automatically from DHCP | Select this option to have the ZyAIR use a dynamically assigned IP address from a DHCP server.<br>**Note:** 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.<br>**Note:** 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 a router or switch on the same network segment as the ZyAIR. The gateway helps forward packets to their destinations. Leave this field as 0.0.0.0 if you do not know it. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 9 Certificates

This chapter gives background information about public-key certificates and explains how to use them.

## 9.1 Certificates Overview

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

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyAIR to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

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

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

The ZyAIR uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

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

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyAIR does not trust a certificate if any certificate on its path has expired or been revoked.

### 9.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyAIR only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

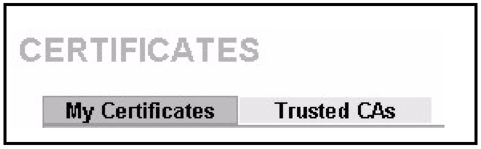
## 9.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyAIR act as a certification authority and sign its own certificates.

## 9.3 Configuration Summary

This section summarizes how to manage certificates on the ZyAIR.

**Figure 43** Certificate Configuration Overview



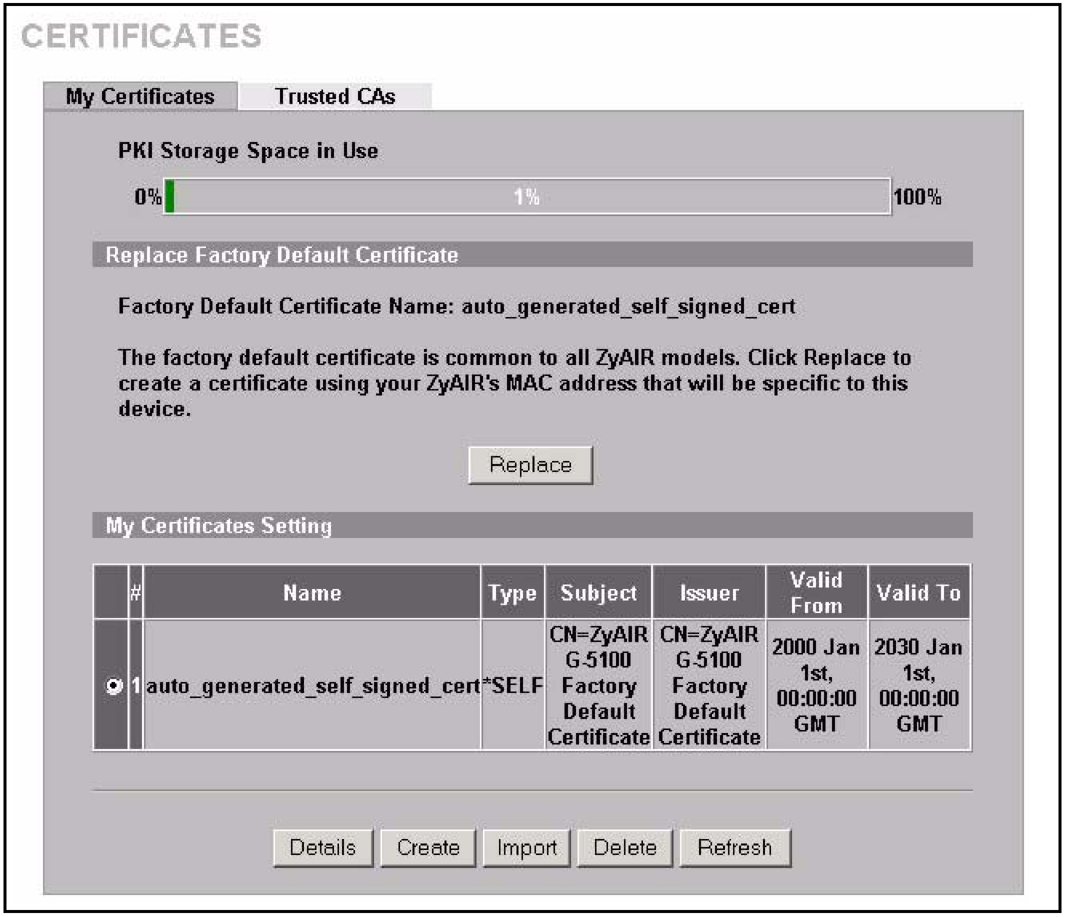
Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyAIRs' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyAIR.

## 9.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the ZyAIR's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

**Figure 44** My Certificates



PKI Storage Space in Use

0% 1% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

My Certificates Setting

| | # | Name | Type | Subject | Issuer | Valid From | Valid To |
|---|---|---|---|---|---|---|---|
| ● | 1 | auto_generated_self_signed_cert | *SELF | CN=ZyAIR G-5100 Factory Default Certificate | CN=ZyAIR G-5100 Factory Default Certificate | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT |

The following table describes the labels in this screen.

**Table 28** My Certificates

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| Replace | This button displays when the ZyAIR has the factory default certificate. The factory default certificate is common to all ZyAIRs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyAIR's MAC address. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |

**Table 28** My Certificates (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | This field displays what kind of certificate this is.<br>**REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request.<br>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate, which the ZyAIR uses to sign imported trusted remote host certificates.<br>**CERT** represents a certificate issued by a certification authority. |
| Subject | This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Details | Select a certificate’s radio button and click **Details** to open a screen with an in-depth list of information about the certificate. |
| Create | Click **Create** to go to the screen where you can have the ZyAIR generate a certificate or a certification request. |
| Import | Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyAIR. |
| Delete | Select a certificate’s radio button and click **Delete** to remove the certificate.<br>A window displays asking you to confirm that you want to delete the certificate.<br>You cannot delete a certificate that one or more features is configured to use.<br>Do the following to delete a certificate that shows ***SELF** in the **Type** field.<br>1. Make sure that no features are configured to use the ***SELF** certificate.<br>2. Select the radio button of another self-signed certificate and click **Details** (see the description on the **Create** button if you need to create a self-signed certificate).<br>3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box.<br>4. Click **Apply** to save the changes and return to the **My Certificates** screen.<br>5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now.<br>Subsequent certificates move up by one when you take this action. |
| Refresh | Click **Refresh** to display the current validity status of the certificates. |

## 9.5 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

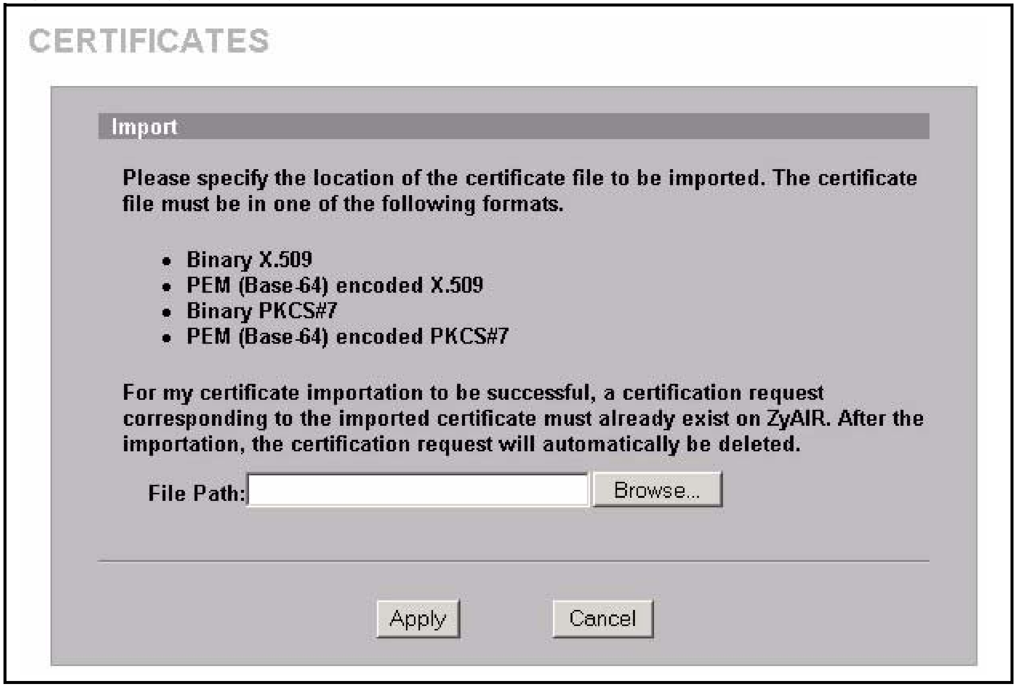
- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyAIR currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

## 9.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyAIR, see the following figure.

**Note:** 1. You can only import a certificate that matches a corresponding certification request that was generated by the ZyAIR.
**Note:** 2. The certificate you import replaces the corresponding request in the **My Certificates** screen.
**Note:** 3. You must remove any spaces from the certificate's filename before you can import it.

**Figure 45** My Certificate Import


CERTIFICATES

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyAIR. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

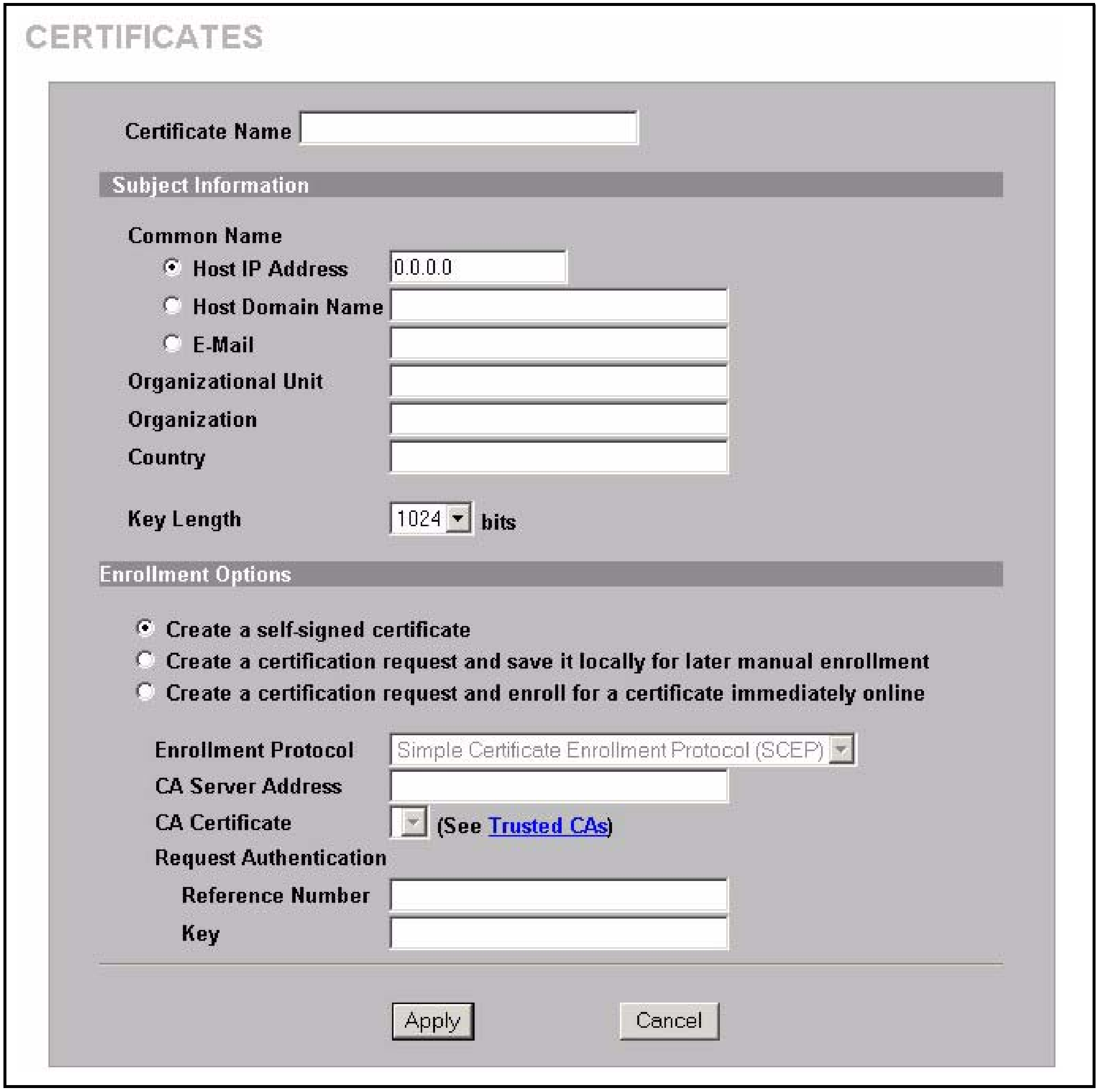
**Table 29** My Certificate Import

| 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 certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyAIR. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 9.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyAIR create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

**Figure 46** My Certificate Create



CERTIFICATES

Certificate Name

Subject Information

Common Name

● Host IP Address 0.0.0.0

○ Host Domain Name

○ E-Mail

Organizational Unit

Organization

Country

Key Length 1024 bits

Enrollment Options

● Create a self-signed certificate

○ Create a certification request and save it locally for later manual enrollment

○ Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Simple Certificate Enrollment Protocol (SCEP)

CA Server Address

CA Certificate (See Trusted CAs)

Request Authentication

Reference Number

Key

The following table describes the labels in this screen.

**Table 30** My Certificate Create

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type up to 31 ASCII characters (not including spaces) to identify this certificate. |
| Subject Information | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. |
| Common Name | Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |

**Table 30** My Certificate Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| Organizational Unit | Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces. |
| Organization | Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces. |
| Country | Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyAIR drops trailing spaces. |
| Key Length | Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. |
| Enrollment Options | These radio buttons deal with how and when the certificate is to be generated. |
| Create a self-signed certificate | Select **Create a self-signed certificate** to have the ZyAIR generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates. |
| Create a certification request and save it locally for later manual enrollment | Select **Create a certification request and save it locally for later manual enrollment** to have the ZyAIR generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority.<br>Copy the certification request from the **My Certificate Details** screen (see Section 9.8 on page 103) and then send it to the certification authority. |
| Create a certification request and enroll for a certificate immediately online | Select **Create a certification request and enroll for a certificate immediately online** to have the ZyAIR generate a request for a certificate and apply to a certification authority for a certificate.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen.<br>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them. |
| Enrollment Protocol | Select the certification authority's enrollment protocol from the drop-down list box.<br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br>**Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510. |
| CA Server Address | Enter the IP address (or URL) of the certification authority server. |
| CA Certificate | Select the certification authority's certificate from the **CA Certificate** drop-down list box.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyAIR's list of certificates of trusted certification authorities. |
| Request Authentication | When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol. |

**Table 30** My Certificate Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key | Type the key that the certification authority gave you. |
| Apply | Click **Apply** to begin certificate or certification request generation. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyAIR is generating the self-signed certificate or certification request.

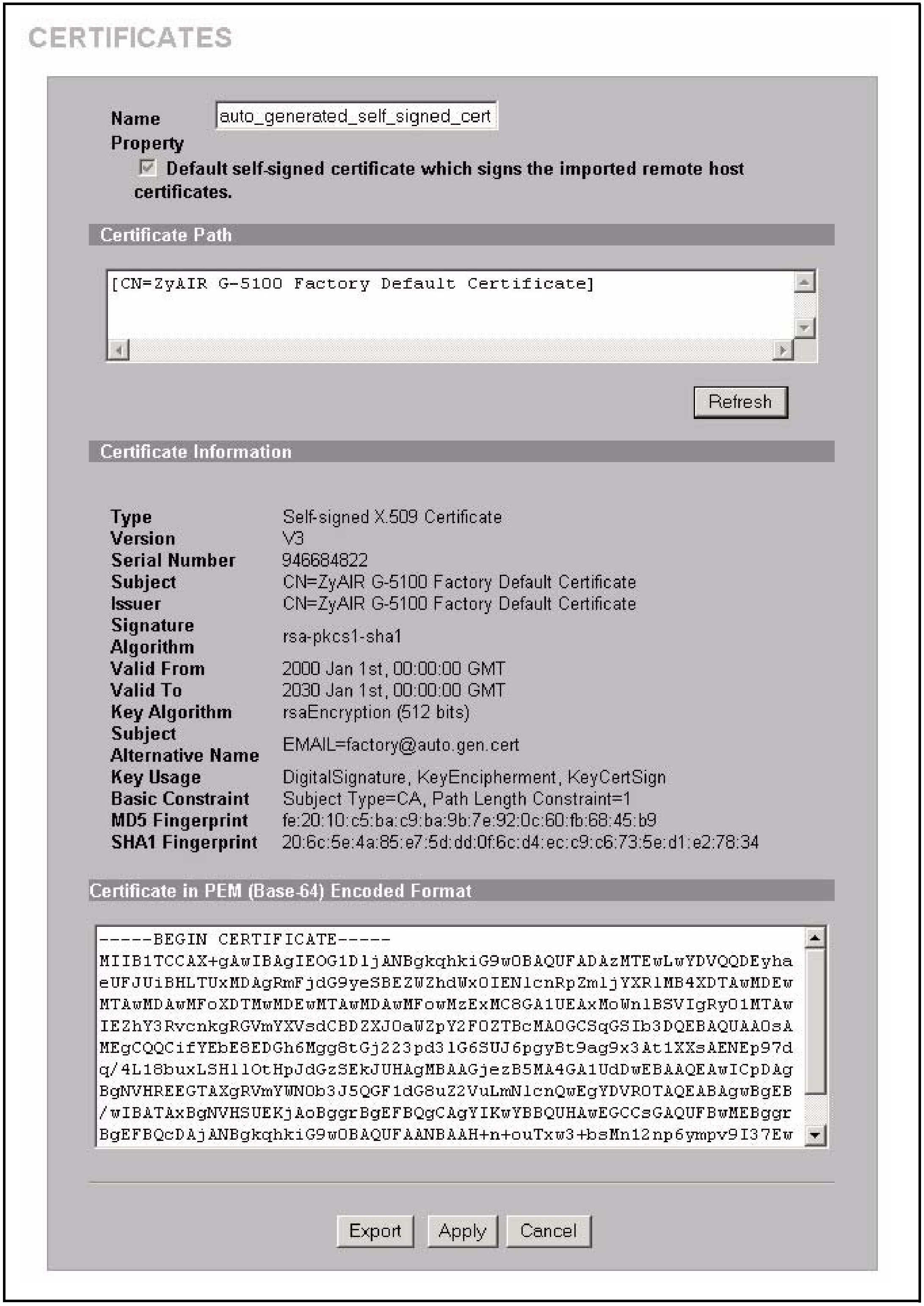
After the ZyAIR successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyAIR enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyAIR to enroll a certificate online.

## 9.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 44 on page 97). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyAIR uses to sign the trusted remote host certificates that you import to the ZyAIR.

**Figure 47** My Certificate Details



| | |
|---|---|
| **Name** | auto_generated_self_signed_cert |

**Property**

☑ **Default self-signed certificate which signs the imported remote host certificates.**

```
[CN=ZyAIR G-5100 Factory Default Certificate]
```

| | |
|---|---|
| **Type** | Self-signed X.509 Certificate |
| **Version** | V3 |
| **Serial Number** | 946684822 |
| **Subject** | CN=ZyAIR G-5100 Factory Default Certificate |
| **Issuer** | CN=ZyAIR G-5100 Factory Default Certificate |
| **Signature Algorithm** | rsa-pkcs1-sha1 |
| **Valid From** | 2000 Jan 1st, 00:00:00 GMT |
| **Valid To** | 2030 Jan 1st, 00:00:00 GMT |
| **Key Algorithm** | rsaEncryption (512 bits) |
| **Subject Alternative Name** | EMAIL=factory@auto.gen.cert |
| **Key Usage** | DigitalSignature, KeyEncipherment, KeyCertSign |
| **Basic Constraint** | Subject Type=CA, Path Length Constraint=1 |
| **MD5 Fingerprint** | fe:20:10:c5:ba:c9:ba:9b:7e:92:0c:60:fb:68:45:b9 |
| **SHA1 Fingerprint** | 20:6c:5e:4a:85:e7:5d:dd:0f:6c:d4:ec:c9:c6:73:5e:d1:e2:78:34 |

```
-----BEGIN CERTIFICATE-----
MIIB1TCCAX+gAwIBAgIEOG1D1jANBgkqhkiG9w0BAQUFADAzMTEwLwYDVQQDEyha
eUFJUiBHLTUxMDAgRmFjdG9yeSBEZWZhdWx0IENlcnRpZmljYXRlMB4XDTAwMDEw
MTAwMDAwMFoXDTMwMDEwMTAwMDAwMFowMzExMC8GA1UEAxMoWnlBSVIgRy01MTAw
IEZhY3RvcnkgRGVmYXVsdCBDZXJ0aWZpY2F0ZTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQCifYEbE8EDGh6Mgg8tGj223pd31G6SUJ6pgyBt9ag9x3At1XXsAENEp97d
q/4L18buxLSH11OtHpJdGzSEkJUHAgMBAAGjezB5MA4GA1UdDwEBAAQEAwICpDAg
BgNVHREEGTAXgRVmYWN0b3J5QGF1dG8uZ2VuLmNlcnQwEgYDVR0TAQEABAgwBgEB
/wIBATAxBgNVHSUEKjAoBggrBgEFBQcCAgYIKwYBBQUHAwEGCCsGAQUFBwMEBggr
BgEFBQcDAjANBgkqhkiG9w0BAQUFAANBAAH+n+ouTxw3+bsMn12np6ympv9I37Ew
```

The following table describes the labels in this screen.

**Table 31** My Certificate Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces). |
| Property<br>Default self-signed certificate which signs the imported remote host certificates. | Select this check box to have the ZyAIR use this certificate to sign the trusted remote host certificates that you import to the ZyAIR. This check box is only available with self-signed certificates.<br>If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates. |
| Certification Path | Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).<br>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyAIR does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click **Refresh** to display the certification path. |
| Certificate Information | These read-only fields display detailed information about the certificate. |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the certification authority or generated by the ZyAIR. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (**CN**), Organizational Unit (**OU**), Organization (**O**) and Country (**C**). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the **Subject Name** field. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. The ZyAIR uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example). |

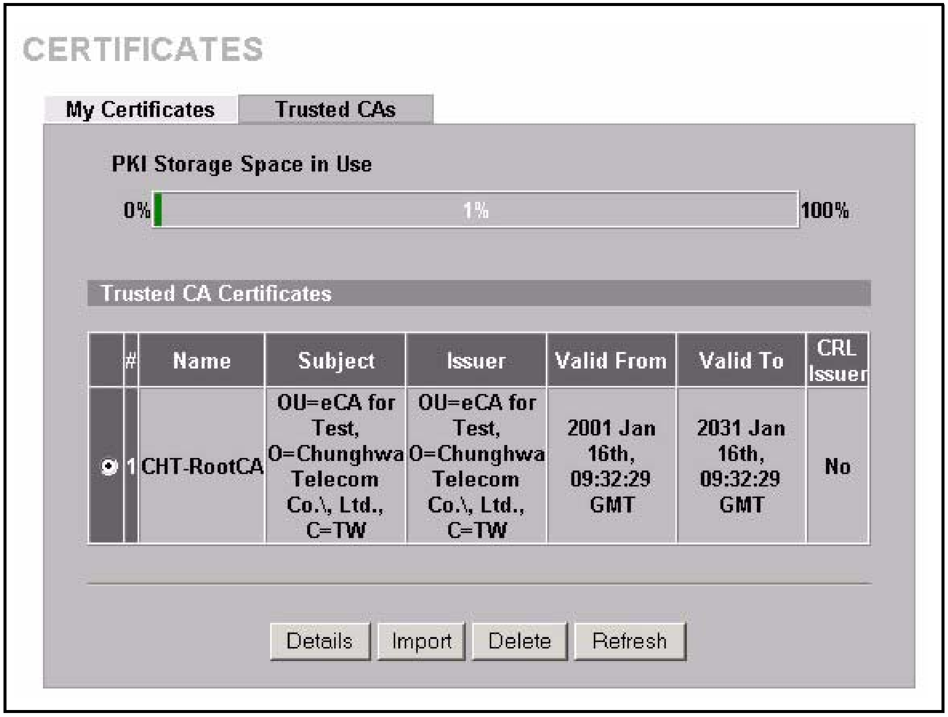
**Table 31** My Certificate Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subject Alternative Name | This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. |
| MD5 Fingerprint | This is the certificate's message digest that the ZyAIR calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the ZyAIR calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.<br>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Export | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.<br>**Note:** When you are saving your certificate, use "cer" or "cert" as the file name extension. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 9.9 Trusted CAs

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyAIR to accept as trusted. The ZyAIR accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

**Figure 48** Trusted CAs



CERTIFICATES

PKI Storage Space in Use

Trusted CA Certificates

|  | # | Name | Subject | Issuer | Valid From | Valid To | CRL Issuer |
|---|---|---|---|---|---|---|---|
| ● | 1 | CHT-RootCA | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | 2001 Jan 16th, 09:32:29 GMT | 2031 Jan 16th, 09:32:29 GMT | No |

The following table describes the labels in this screen.

**Table 32** Trusted CAs

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |

**Table 32** Trusted CAs (continued)

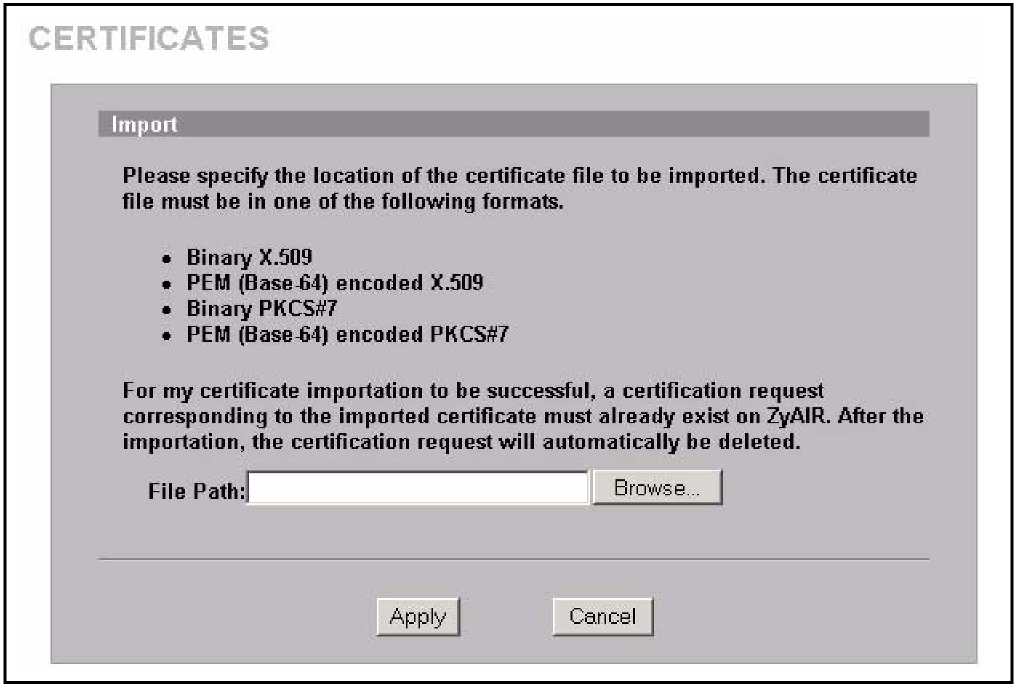
| LABEL | DESCRIPTION |
|---|---|
| CRL Issuer | This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the ZyAIR check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No". |
| Details | Select a certificate's radio button and click **Details** to open a screen with an in-depth list of information about the certificate where you can change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority. |
| Import | Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyAIR. |
| Delete | Select a certificate's radio button and click **Delete** to remove the certificate.<br>A window displays asking you to confirm that you want to delete the certificate.<br>Subsequent certificates move up by one when you take this action. |
| Refresh | Click this button to display the current validity status of the certificates. |

## 9.10 Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyAIR, see the following figure.

**Note:** You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 49** Trusted CA Import



CERTIFICATES

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyAIR. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

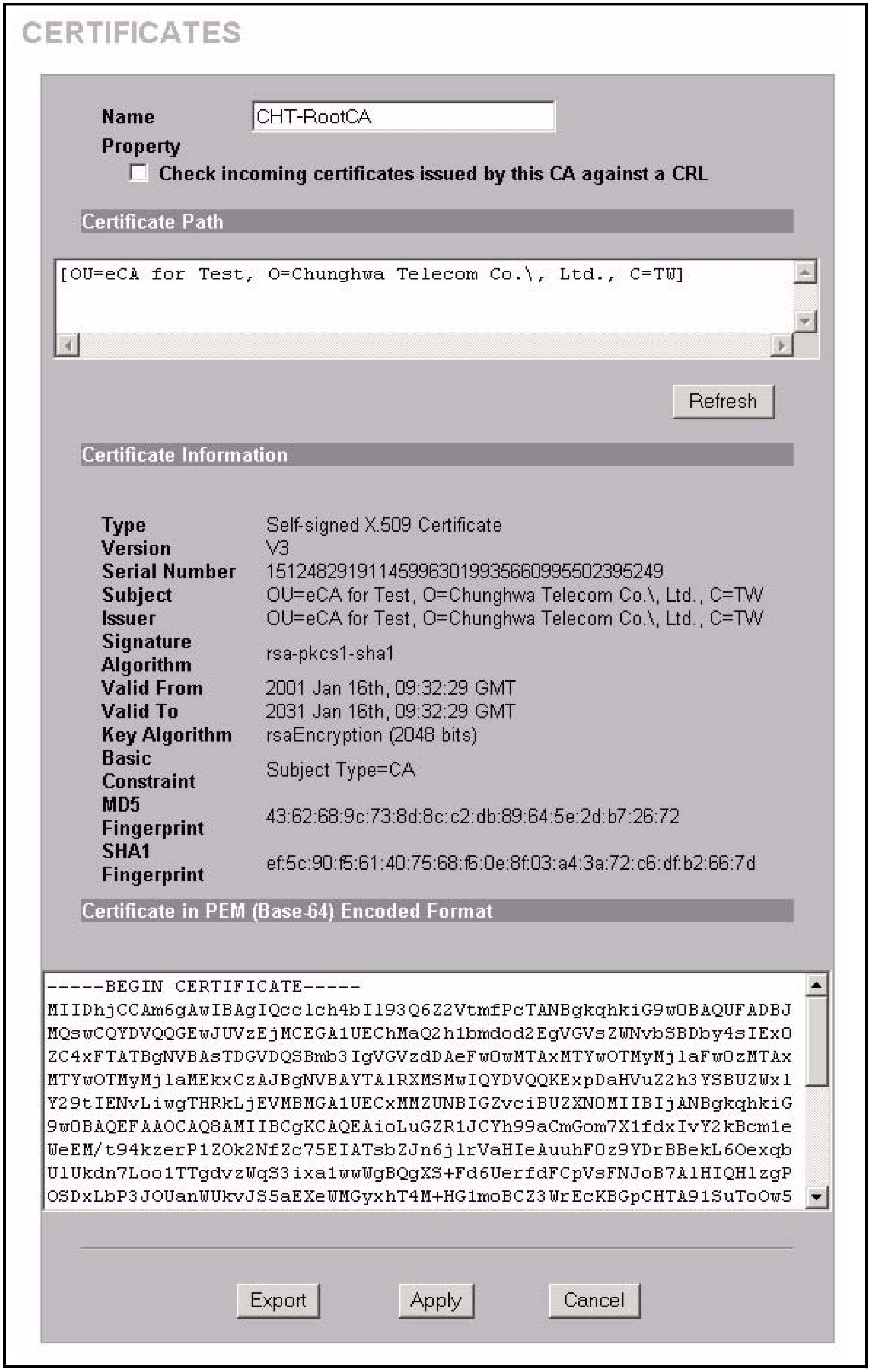
**Table 33** Trusted CA Import

| 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 certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyAIR. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

## 9.11 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

**Figure 50** Trusted CA Details



CERTIFICATES

Name: CHT-RootCA

Property

□ Check incoming certificates issued by this CA against a CRL

Certificate Path

```
[OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW]
```

Certificate Information

| | |
|---|---|
| Type | Self-signed X.509 Certificate |
| Version | V3 |
| Serial Number | 151248291911459963019935660995502395249 |
| Subject | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW |
| Issuer | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW |
| Signature Algorithm | rsa-pkcs1-sha1 |
| Valid From | 2001 Jan 16th, 09:32:29 GMT |
| Valid To | 2031 Jan 16th, 09:32:29 GMT |
| Key Algorithm | rsaEncryption (2048 bits) |
| Basic Constraint | Subject Type=CA |
| MD5 Fingerprint | 43:62:68:9c:73:8d:8c:c2:db:89:64:5e:2d:b7:26:72 |
| SHA1 Fingerprint | ef:5c:90:f5:61:40:75:68:f6:0e:8f:03:a4:3a:72:c6:df:b2:66:7d |

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIQcc1ch4bI193Q6Z2VtmfPcTANBgkqhkiG9w0BAQUFADBJ
MQswCQYDVQQGEwJUVzEjMCEGA1UEChMaQ2h1bmdod2EgVGVsZWNvbSBDby4sIEx0
ZC4xFTATBgNVBAsTDGVDQSBmb3IgVGVzdDAeFw0wMTAxMTYwOTMyMjlaFw0zMTAx
MTYwOTMyMjlaMEkxCzAJBgNVBAYTAlRXMSMwIQYDVQQKExpDaHVuZ2h3YSBUZWx1
Y29tIENvLiwgTHRkLjEVMBMGA1UECxMMZUNBIGZvciBUZXN0MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAioLuGZR1JCYh99aCmGom7X1fdxIvY2kBcm1e
WeEM/t94kzerP1ZOk2NfZc75EIATsbZJn6j1rVaHIeAuuhF0z9YDrBBekL60exqb
U1Ukdn7Loo1TTgdvzWqS3ixa1wwWgBQgXS+Fd6UerfdFCpVsFNJoB7A1HIQH1zgP
OSDxLbP3JOUanWUkvJS5aEXeWMGyxhT4M+HG1moBCZ3WrEcKBGpCHTA91SuToOw5
```

The following table describes the labels in this screen.

**Table 34** Trusted CA Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces). |
| Property<br>Check incoming certificates issued by this CA against a CRL | Select this check box to have the ZyAIR check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).<br>Clear this check box to have the ZyAIR not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). |
| Certificate Path | Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyAIR does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click **Refresh** to display the certification path. |
| Certificate Information | These read-only fields display detailed information about the certificate. |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the certification authority. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same information as in the **Subject Name** field. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example). |

**Table 34** Trusted CA Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subject Alternative Name | This field displays the certificate’s owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path. |
| CRL Distribution Points | This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers. |
| MD5 Fingerprint | This is the certificate’s message digest that the ZyAIR calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |
| SHA1 Fingerprint | This is the certificate’s message digest that the ZyAIR calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Export | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Apply | Click **Apply** to save your changes back to the ZyAIR. You can only change the name and/or set whether or not you want the ZyAIR to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

# CHAPTER 10
# Log Screens

This chapter contains information about configuring general log settings and viewing the ZyAIR's logs. Refer to Appendix K on page 249 for example log message explanations.

## 10.1 Configuring View Log

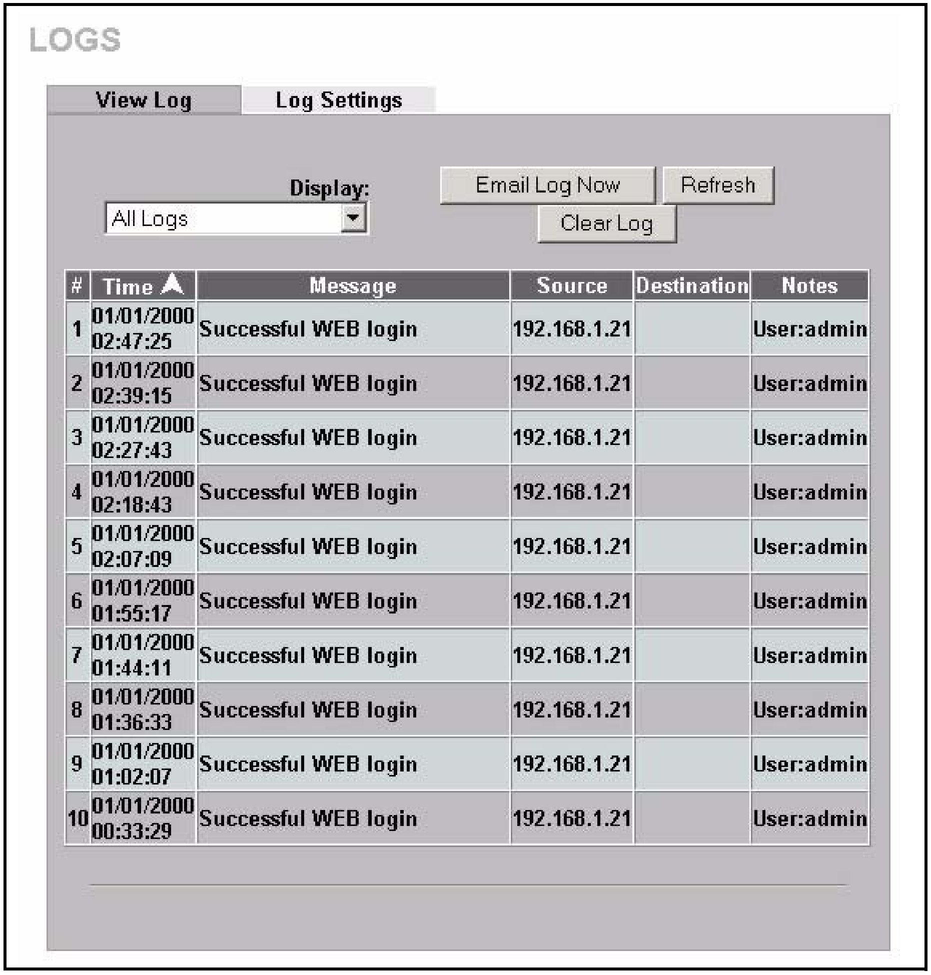
The web configurator allows you to look at all of the ZyAIR's logs in one location.

Click **LOGS** to open the **View Log** screen. The **View Log** screen displays logs for the categories that you selected in the **Log Settings** screen (see Figure 52 on page 116).

You can view logs and alert messages in this screen. Log entries in red indicate alerts. Once the log table is full, old logs are deleted as new logs are created.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

**Figure 51** View Log



Display: All Logs

| # | Time | Message | Source | Destination | Notes |
|---|---|---|---|---|---|
| 1 | 01/01/2000 02:47:25 | Successful WEB login | 192.168.1.21 | | User:admin |
| 2 | 01/01/2000 02:39:15 | Successful WEB login | 192.168.1.21 | | User:admin |
| 3 | 01/01/2000 02:27:43 | Successful WEB login | 192.168.1.21 | | User:admin |
| 4 | 01/01/2000 02:18:43 | Successful WEB login | 192.168.1.21 | | User:admin |
| 5 | 01/01/2000 02:07:09 | Successful WEB login | 192.168.1.21 | | User:admin |
| 6 | 01/01/2000 01:55:17 | Successful WEB login | 192.168.1.21 | | User:admin |
| 7 | 01/01/2000 01:44:11 | Successful WEB login | 192.168.1.21 | | User:admin |
| 8 | 01/01/2000 01:36:33 | Successful WEB login | 192.168.1.21 | | User:admin |
| 9 | 01/01/2000 01:02:07 | Successful WEB login | 192.168.1.21 | | User:admin |
| 10 | 01/01/2000 00:33:29 | Successful WEB login | 192.168.1.21 | | User:admin |

The following table describes the labels in this screen.

**Table 35** 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**.<br>The number of categories shown in the drop down list box depends on the selection in the **Log Settings** page. |
| 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. |
| 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. |

**Table 35** View Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Destination | This field lists the destination IP address and the port number of the incoming packet. |
| Notes | This field displays additional information about the log entry. |

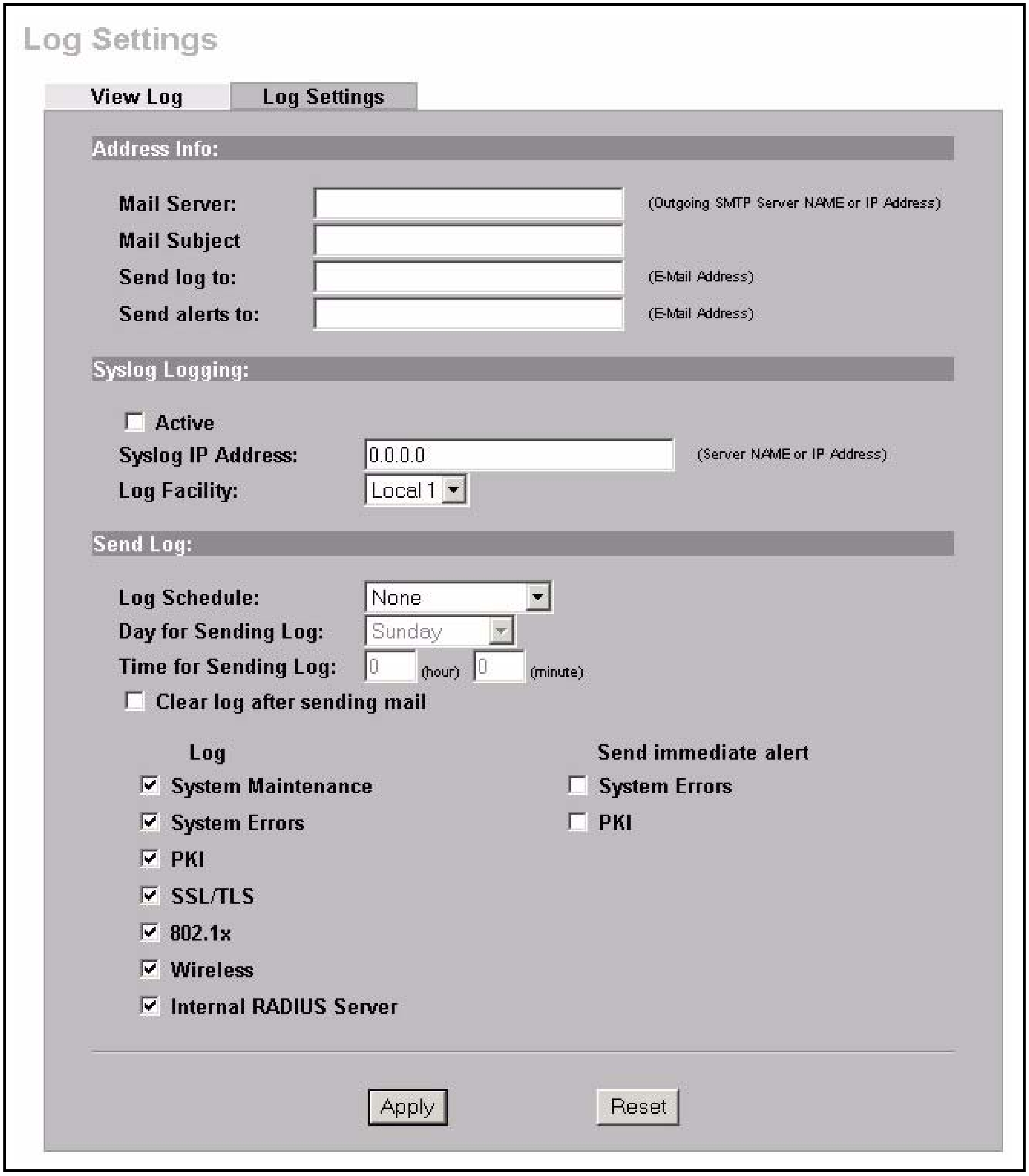
## 10.2 Configuring Log Settings

To change your ZyAIR's log settings, click **LOGS** and then **Log Settings**. The **Log Settings** screen opens.

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.

**Figure 52** Log Settings



Address Info:

Mail Server: (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

Syslog Logging:

□ Active

Syslog IP Address: 0.0.0.0 (Server NAME or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

| Log | Send immediate alert |
|---|---|
| ☑ System Maintenance | □ System Errors |
| ☑ System Errors | □ PKI |
| ☑ PKI | |
| ☑ SSL/TLS | |
| ☑ 802.1x | |
| ☑ Wireless | |
| ☑ Internal RADIUS Server | |

The following table describes the labels in this screen.

**Table 36** Log Settings

| LABEL | DESCRIPTION |
|---|---|
| Address Info | |
| 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. |

**Table 36** Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 syslog server used to store logs. |
| Active | Click **Active** to enable syslog logging. |
| Syslog IP Address | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Send Log | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>• Daily<br>• Weekly<br>• Hourly<br>• When Log is Full<br>• None.<br>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.<br>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. |
| Clear log after sending mail | Select the check box to clear all logs after logs and alert messages are sent via e-mail. |
| Log | Select the categories of logs that you want to record. |
| Send immediate alert | Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to reconfigure all the fields in this screen. |

# CHAPTER 11 Maintenance

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

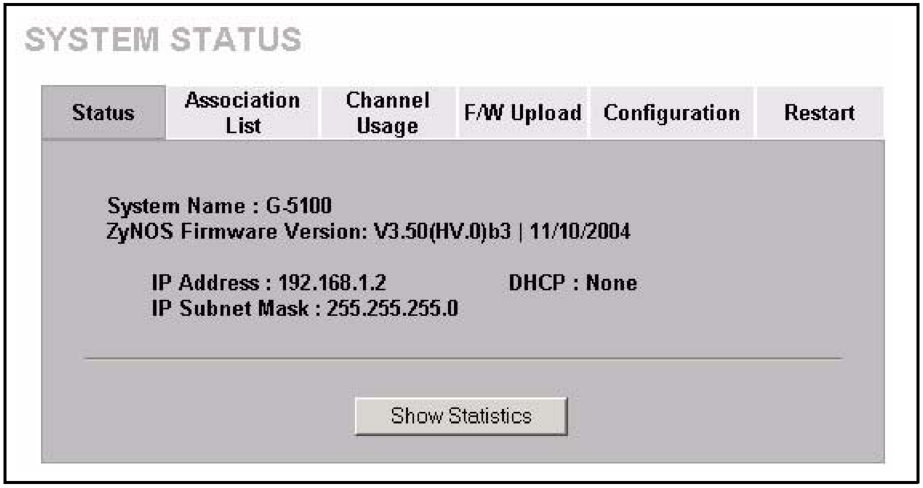
## 11.1 Maintenance Overview

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

## 11.2 System Status Screen

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

**Figure 53** System Status



System Name : G-5100
ZyNOS Firmware Version: V3.50(HV.0)b3 | 11/10/2004

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

The following table describes the labels in this screen.

**Table 37** System Status

| LABEL | DESCRIPTION |
|---|---|
| System Name | This is the **System Name** you enter in the first Internet Access Wizard screen. It is for identification purposes |
| ZyNOS Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. |

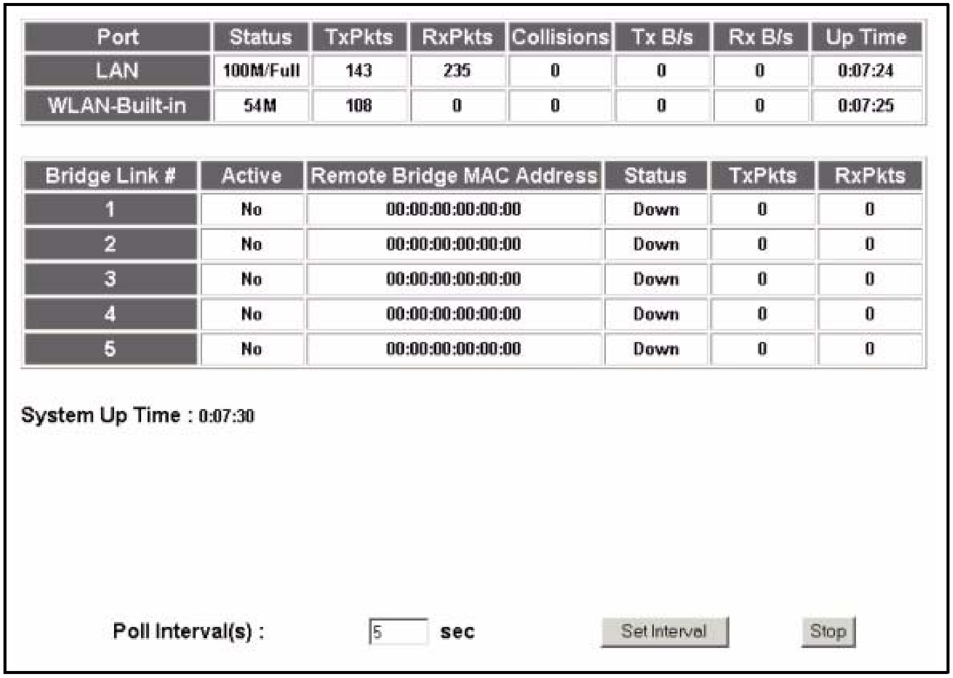
**Table 37** System Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 11.2.1 System Statistics

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

**Figure 54** System Status: Show Statistics



| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|---|---|---|---|---|---|---|---|
| LAN | 100M/Full | 143 | 235 | 0 | 0 | 0 | 0:07:24 |
| WLAN-Built-in | 54M | 108 | 0 | 0 | 0 | 0 | 0:07:25 |

| Bridge Link # | Active | Remote Bridge MAC Address | Status | TxPkts | RxPkts |
|---|---|---|---|---|---|
| 1 | No | 00:00:00:00:00:00 | Down | 0 | 0 |
| 2 | No | 00:00:00:00:00:00 | Down | 0 | 0 |
| 3 | No | 00:00:00:00:00:00 | Down | 0 | 0 |
| 4 | No | 00:00:00:00:00:00 | Down | 0 | 0 |
| 5 | No | 00:00:00:00:00:00 | Down | 0 | 0 |

System Up Time : 0:07:30

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

**Table 38** System Status: Show Statistics

| LABEL | DESCRIPTION |
|---|---|
| Port | This is the Ethernet port or the built-in wireless card. |
| Status | This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port.<br>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. |

**Table 38** System Status: Show Statistics (continued)

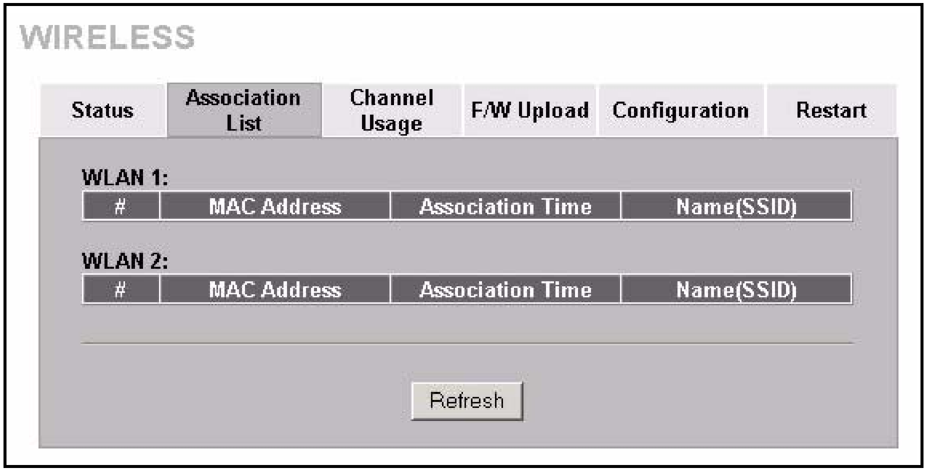
| LABEL | DESCRIPTION |
|---|---|
| Collisions | This is the number of collisions on this port. |
| Tx B/s | This shows the transmission speed in bytes per second on this port. |
| Rx B/s | This shows the reception speed in bytes per second on this port. |
| Up Time | This is total amount of time the line has been up. |
| Bridge Link # | This is the index number of the bridge connection. |
| Active | This shows whether the bridge connection is activated or not. |
| Remote Bridge MAC Address | This is the MAC address of the peer device in bridge mode. |
| Status | This shows the current status of the bridge connection, which can be **Up** or **Down**. |
| TxPkts | This is the number of transmitted packets on the wireless bridge. |
| RxPkts | This is the number of received packets on the wireless bridge. |
| 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. |

## 11.3 Association List

View the wireless stations that are currently associated to the ZyAIR's WLAN cards in the **Association List** screen.

Click **MAINTENANCE** and then the **Association List** tab to display the screen as shown next.

**Figure 55** Association List



WLAN 1:

| # | MAC Address | Association Time | Name(SSID) |
|---|---|---|---|

WLAN 2:

| # | MAC Address | Association Time | Name(SSID) |
|---|---|---|---|

The following table describes the labels in this screen.

**Table 39** Association List

| LABEL | DESCRIPTION |
|---|---|
| WLAN 1, 2 | This identifies the WLAN adapter to which the list of wireless clients is associated. |
| # | 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. |
| Name (SSID) | This field displays the SS identification name to which the wireless station is associated. |
| Refresh | Click **Refresh** to reload the screen. |

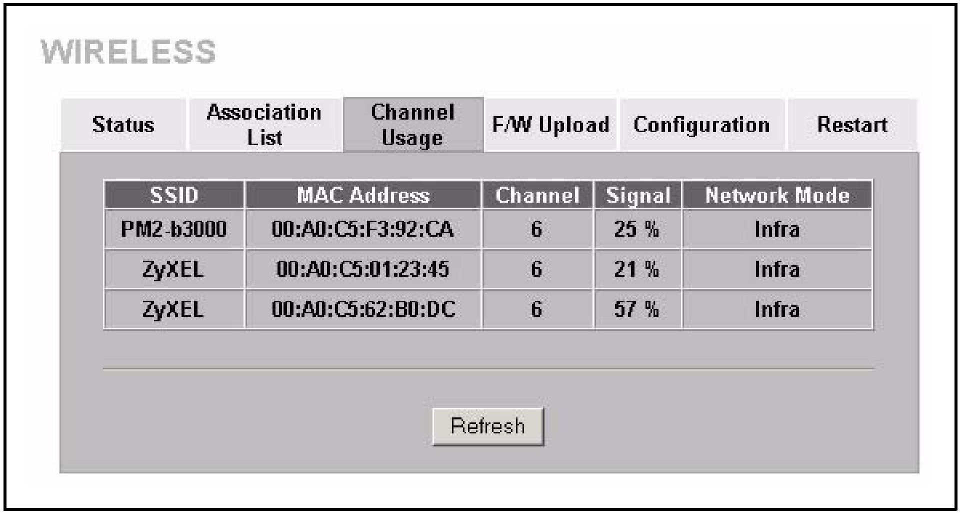
## 11.4 Channel Usage

The **Channel Usage** screen shows which channels are being used by other wireless networks within the ZyAIR's transmission range. If a channel is being used, select a channel removed from it by five channels to avoid overlap.

Click **MAINTENANCE** and then the **Channel Usage** tab to display the screen shown next.

Wait a moment while the ZyAIR compiles the information.

**Figure 56** Channel Usage



| SSID | MAC Address | Channel | Signal | Network Mode |
|---|---|---|---|---|
| PM2-b3000 | 00:A0:C5:F3:92:CA | 6 | 25 % | Infra |
| ZyXEL | 00:A0:C5:01:23:45 | 6 | 21 % | Infra |
| ZyXEL | 00:A0:C5:62:B0:DC | 6 | 57 % | Infra |

The following table describes the labels in this screen.

**Table 40** Channel Usage

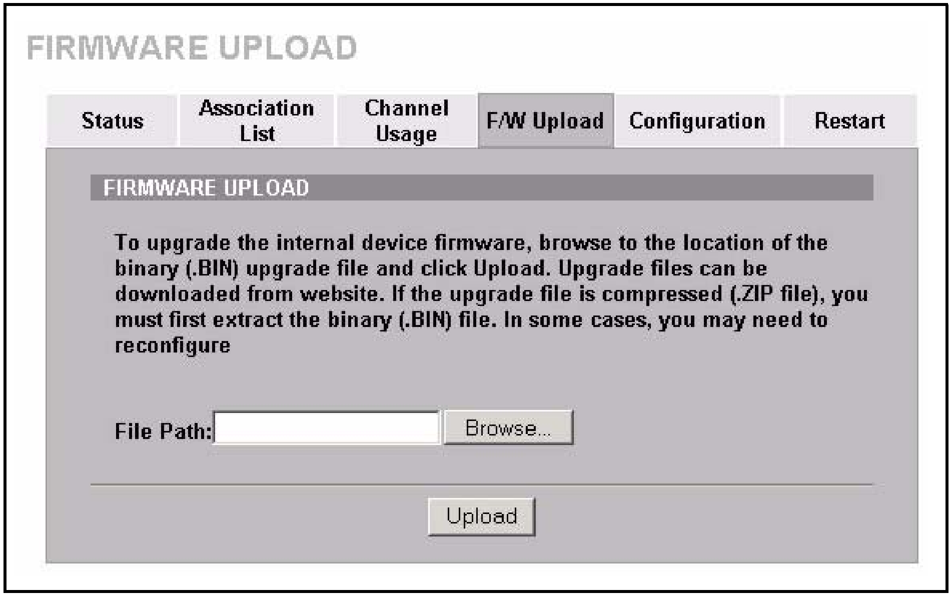
| LABEL | DESCRIPTION |
|---|---|
| SSID | This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See Chapter 5 on page 55 for more information on basic service sets (BSS) and extended service sets (ESS). |
| MAC Address | This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network. |
| Channel | This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. |
| Signal | This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference. |
| Network Mode | "Network Mode" in this screen refers to your wireless LAN infrastructure and WEP setup (refer to Chapter 5 on page 55).<br>Network modes are: **Infra** (Infrastructure which is the same as an extended service set ESS), **Infra, WEP** (Infrastructure with WEP encryption enabled), **Ad-Hoc** (same as an independent basic service set IBSS), or **Ad-Hoc with WEP**. |
| Refresh | Click **Refresh** to reload the screen. |

## 11.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zyair.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Chapter 20 on page 169 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.

**Figure 57** Firmware Upload



FIRMWARE UPLOAD

FIRMWARE UPLOAD

To upgrade the internal device 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

File Path:

The following table describes the labels in this screen.

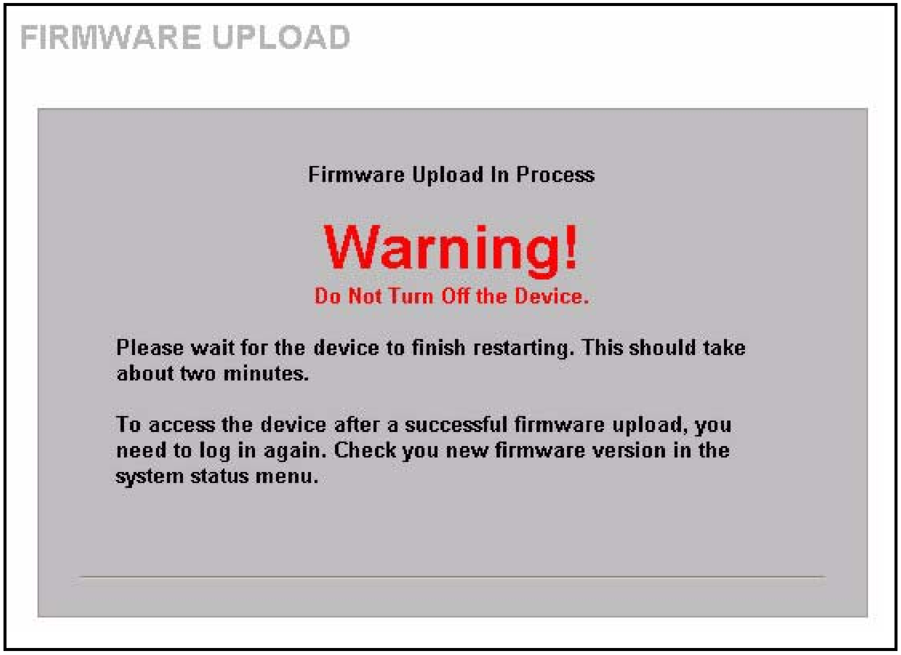
**Table 41** Firmware Upload

| 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. |

**Note:** Do not turn off the ZyAIR while firmware upload is in progress!

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

**Figure 58** Firmware Upload In Process



FIRMWARE UPLOAD

Firmware Upload In Process

Warning!

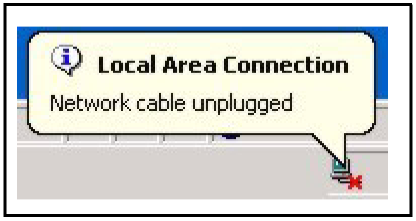
Do Not Turn Off the Device.

Please wait for the device to finish restarting. 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.

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

**Figure 59** Network Temporarily Disconnected



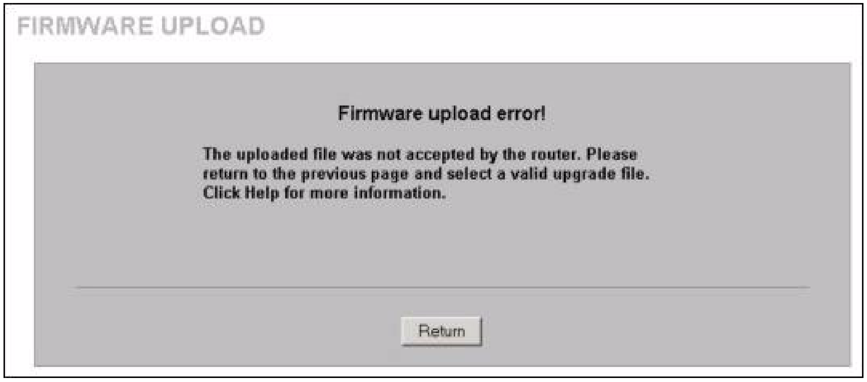
Local Area Connection

Network cable unplugged

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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 60** Firmware Upload Error



Firmware upload error!

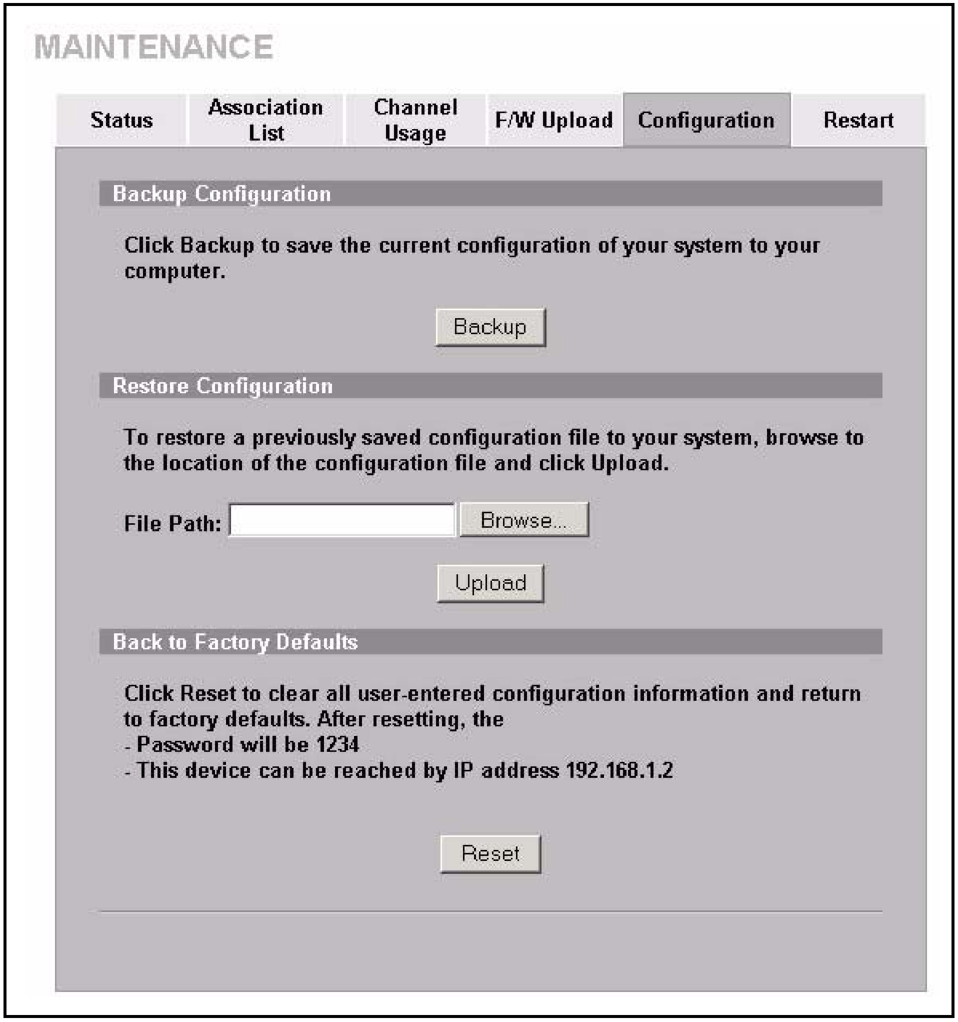
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

## 11.6 Configuration Screen

See Chapter 20 on page 169 for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to backing up configuration, restoring configuration and restoring factory defaults appears as shown next.

**Figure 61** Configuration



Backup Configuration

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

Restore Configuration

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

File Path:

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

## 11.6.1 Backup Configuration

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

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

## 11.6.2 Restore Configuration

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

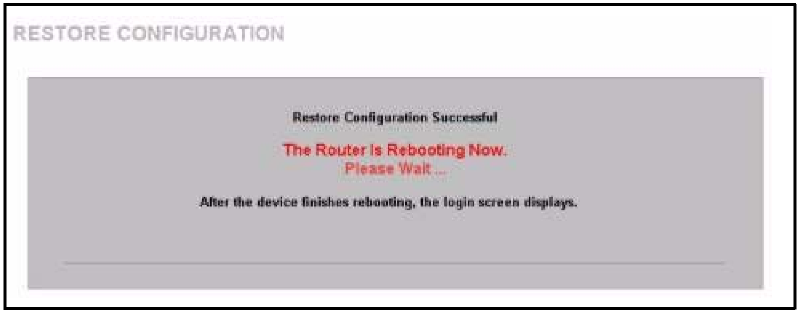
**Table 42** Restore Configuration

| 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. |

**Note:** Do not turn off the ZyAIR while configuration file upload is in progress.

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

**Figure 62** Configuration Upload Successful



RESTORE CONFIGURATION

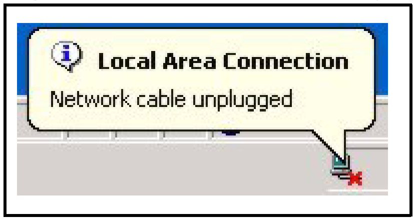
Restore Configuration Successful

The Router Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

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

**Figure 63** Network Temporarily Disconnected



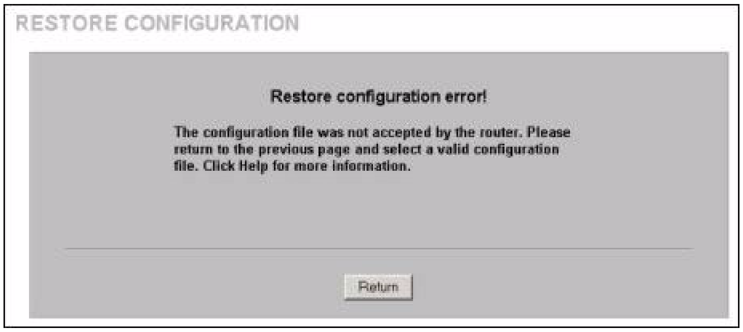
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyAIR IP address (192.168.1.2). See Appendix D on page 201 for details on how to set up your computer’s IP address.

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

**Figure 64** Configuration Upload Error



RESTORE CONFIGURATION

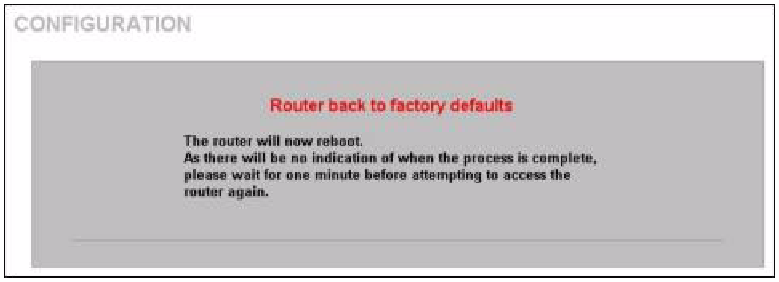
Restore configuration error!

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.

## 11.6.3 Back to Factory Defaults

Click the **Reset** button in this section to clear all user-entered configuration information and returns the ZyAIR to its factory defaults as shown on the screen. The following warning screen will appear.

**Figure 65** Reset Warning Message



CONFIGURATION

Router back to factory defaults

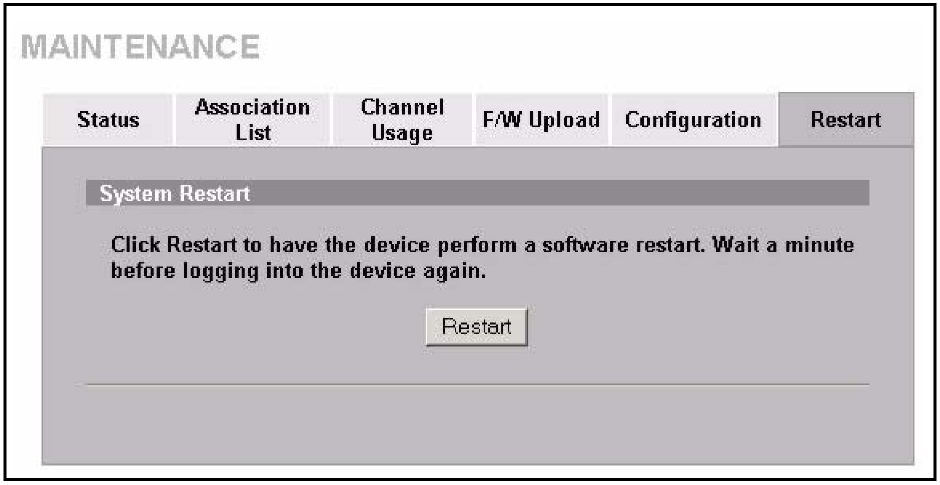
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

# 11.7 Restart Screen

System restart allows you to reboot the ZyAIR without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the ZyAIR reboot. This does not affect the ZyAIR's configuration.

**Figure 66** Restart Screen



Click Restart to have the device perform a software restart. Wait a minute before logging into the device again.

# CHAPTER 12 Introducing the SMT

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

## 12.1 Introduction to the SMT

The ZyAIR's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

## 12.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

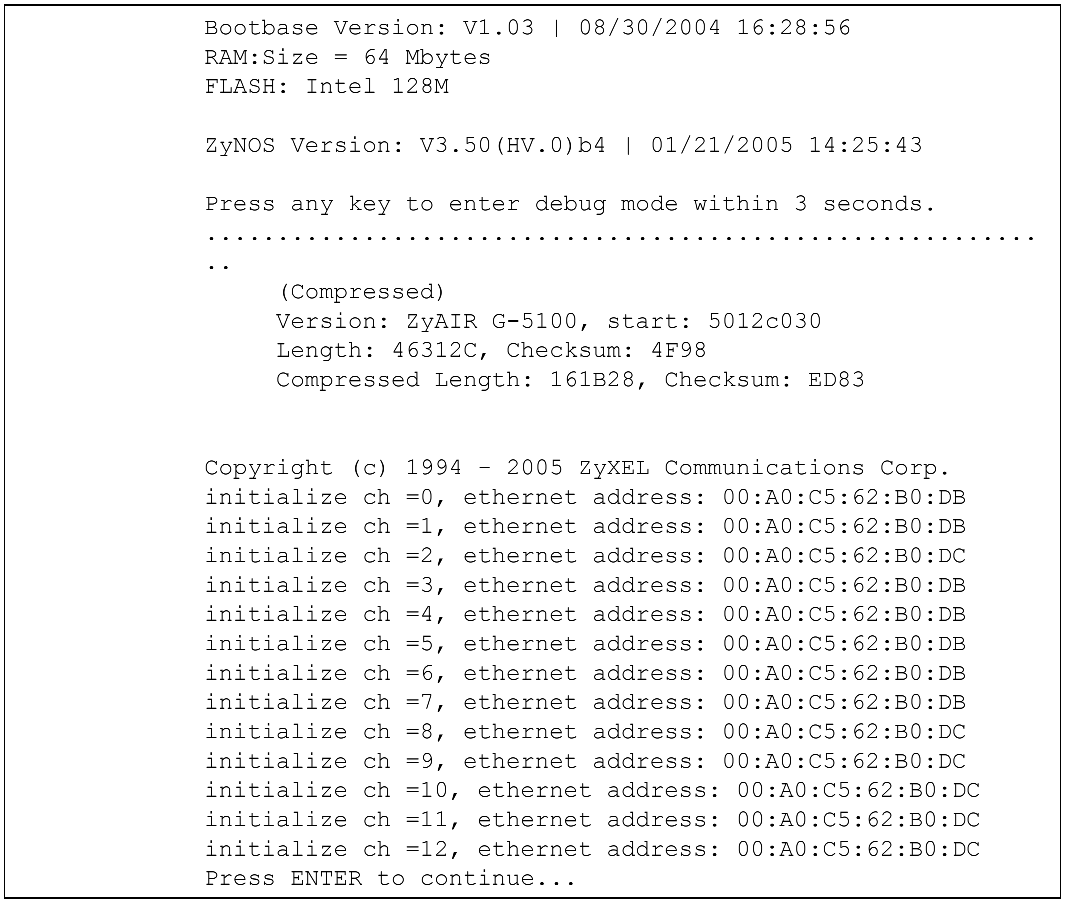
- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

### 12.2.1 Initial Screen

When you turn on your ZyAIR, it performs several internal tests.

After the tests, the ZyAIR asks you to press [ENTER] to continue, as shown next.

**Figure 67** Initial Screen



```
Bootbase Version: V1.03 | 08/30/2004 16:28:56
RAM:Size = 64 Mbytes
FLASH: Intel 128M

ZyNOS Version: V3.50(HV.0)b4 | 01/21/2005 14:25:43

Press any key to enter debug mode within 3 seconds.
..........................................................
..
     (Compressed)
     Version: ZyAIR G-5100, start: 5012c030
     Length: 46312C, Checksum: 4F98
     Compressed Length: 161B28, Checksum: ED83


Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =1, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =2, ethernet address: 00:A0:C5:62:B0:DC
initialize ch =3, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =4, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =5, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =6, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =7, ethernet address: 00:A0:C5:62:B0:DB
initialize ch =8, ethernet address: 00:A0:C5:62:B0:DC
initialize ch =9, ethernet address: 00:A0:C5:62:B0:DC
initialize ch =10, ethernet address: 00:A0:C5:62:B0:DC
initialize ch =11, ethernet address: 00:A0:C5:62:B0:DC
initialize ch =12, ethernet address: 00:A0:C5:62:B0:DC
Press ENTER to continue...
```

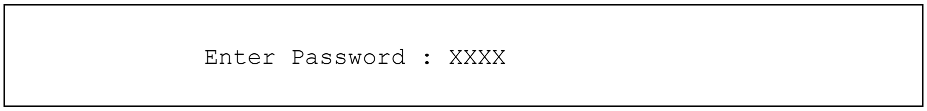
## 12.2.2 Entering the Password

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

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” 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 and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 68** Password Screen



```
Enter Password : XXXX
```

## 12.3 Accessing the SMT via Telnet

The following procedure details how to telnet into your ZyAIR.

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**.

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

**Figure 69** Login Screen

```
                Password : xxxx
```

3 After entering the password you will see the main menu.

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

## 12.4 Navigating the SMT Interface

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

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

**Table 43** Main Menu Commands

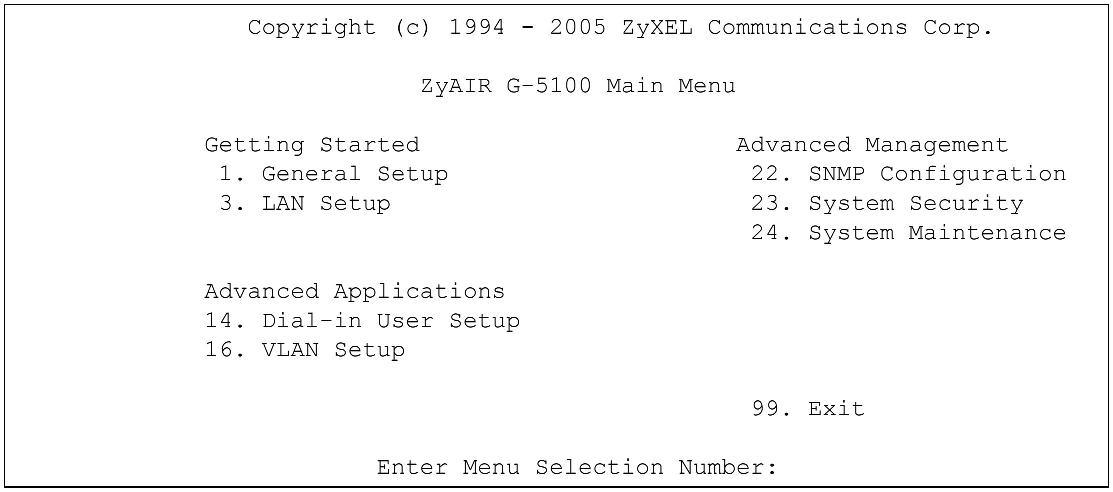
| OPERATION | KEYSTROKE | DESCRIPTION |
|---|---|---|
| Move down to another menu | [ENTER] | To move forward to a submenu, type in the number of the desired submenu and press [ENTER]. |
| Move up to a previous menu | [ESC] | Press [ESC] to move back to the previous menu. |
| Move to a "hidden" menu | 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.<br>When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu. |
| 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]. |

**Table 43** Main Menu Commands (continued)

| OPERATION | KEYSTROKE | DESCRIPTION |
|---|---|---|
| Required fields | <?> or **ChangeMe** | All fields with the symbol <?> must be filled in order to be able to save the new configuration.<br>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.<br>Make sure you save your settings in each screen that you configure. |
| 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.

**Figure 70 SMT Main Menu**



```
                Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

                            ZyAIR G-5100 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
             16. VLAN Setup


                                                   99. Exit

                        Enter Menu Selection Number:
```

## 12.4.1 System Management Terminal Interface Summary

**Table 44** 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. |
| 16 | VLAN Setup | Use this menu to set up your VLAN ID. |
| 22 | SNMP Configuration | Use this menu to set up SNMP related parameters. |

**Table 44** Main Menu Summary (continued)

| # | MENU TITLE | DESCRIPTION |
|---|---|---|
| 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. |

## 12.4.2 SMT Menus Overview

The following table gives you an overview of your ZyAIR's various SMT menus.

**Table 45** SMT Menus Overview

| MENUS | SUB MENUS | |
|---|---|---|
| 1 General Setup | | |
| 3 LAN Setup | 3.1 LAN Port Filter Setup | |
| | 3.2 TCP/IP Setup | |
| | 3.5 Wireless LAN Setup | 3.5.1 WLAN MAC Address Filter |
| | | 3.5.4 Bridge Link Configuration |
| 14 Dial-in User Setup | 14.1 Edit Dial-in User Setup | |
| 16 VLAN Setup | | |
| 22 SNMP Configuration | | |
| 23 System Security | 23.1 Change Password | |
| | 23.2 RADIUS Server | |
| | 23.4 IEEE802.1x | |
| 24 System Maintenance | 24.1 System Status | |
| | 24.2 System Information and Console Port Speed | 24.2.1 System Information |
| | | 24.2.2 Console Port Speed |
| | 24.3 Log and Trace | 24.3.1 View Error Log |
| | | 24.3.2 Syslog Logging |
| | | 24.3.4 Call-Triggering Packet |
| | 24.4 Diagnostic | |
| | 24.5 Backup Configuration | |
| | 24.6 Restore Configuration | |
| | 24.7 Upload Firmware | 24.7.1 Upload System Firmware |
| | | 24.7.2 Upload System Configuration File |
| | 24.8 Command Interpreter Mode | |
| | 24.10 Time and Date Setting | |

## 12.5 Changing the System Password

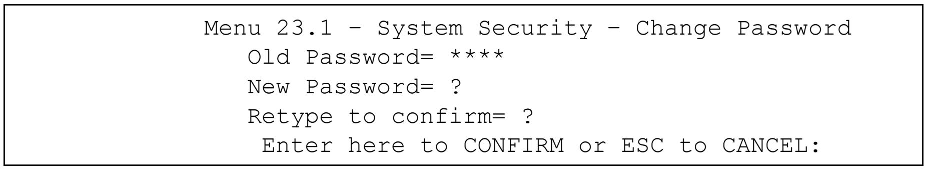
Change the ZyAIR default password by following the steps shown next.

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

2 Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.

3 Type your existing system password in the **Old Password** field, and press [ENTER].

**Figure 71 Menu 23.1 System Security: Change Password**



```
             Menu 23.1 - System Security - Change Password
                Old Password= ****
                New Password= ?
                Retype to confirm= ?
                 Enter here to CONFIRM or ESC to CANCEL:
```

4 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

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.

# CHAPTER 13
# General Setup

The chapter shows you the information on general setup.

## 13.1 General Setup

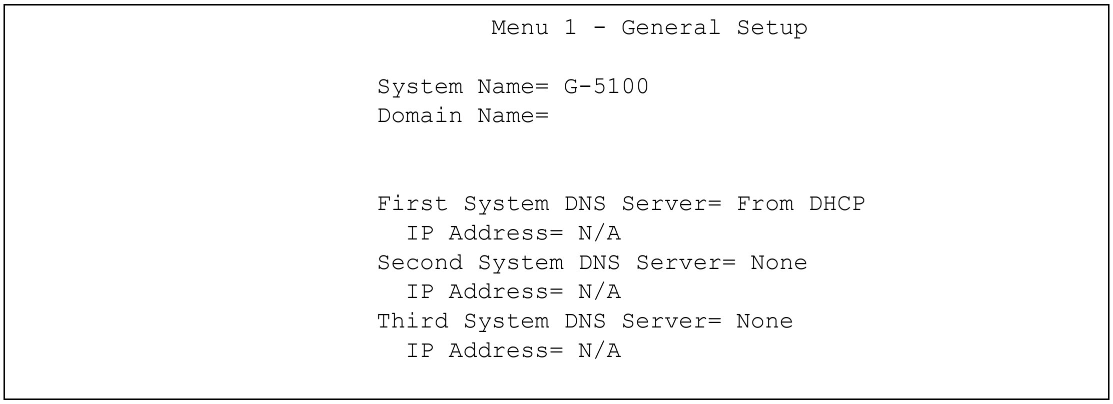
**Menu 1 – General Setup** contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. It is recommended you type your computer's "Computer name".

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

### 13.1.1 Procedure To Configure Menu 1

Enter 1 in the main menu to open **Menu 1 – General Setup** as shown next.

**Figure 72** Menu 1 General Setup



```
                    Menu 1 - General Setup

            System Name= G-5100
            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
```

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

**Table 46** Menu 1 General Setup

| FIELD | DESCRIPTION |
|---|---|
| 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. |
| 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].<br>These fields are not available on all models. |
| IP Address | Enter the IP addresses of the DNS servers. This field is available when you select **User-Defined** in the field above. |
| 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. | |

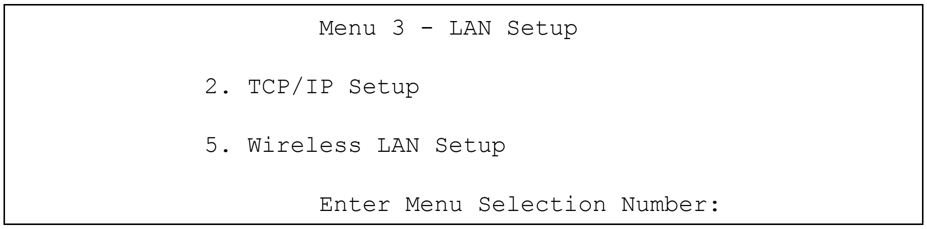
# CHAPTER 14
# LAN Setup

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

## 14.1 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.

**Figure 73** Menu 3 LAN Setup



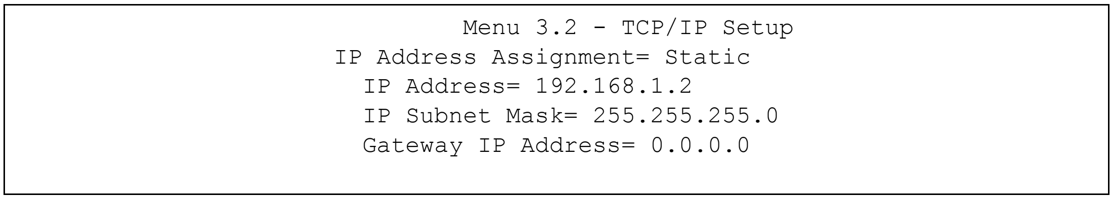
```
                      Menu 3 - LAN Setup

              2. TCP/IP Setup

              5. Wireless LAN Setup

                      Enter Menu Selection Number:
```

## 14.2 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:

**Figure 74** Menu 3.2 TCP/IP Setup



```
                               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
```

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

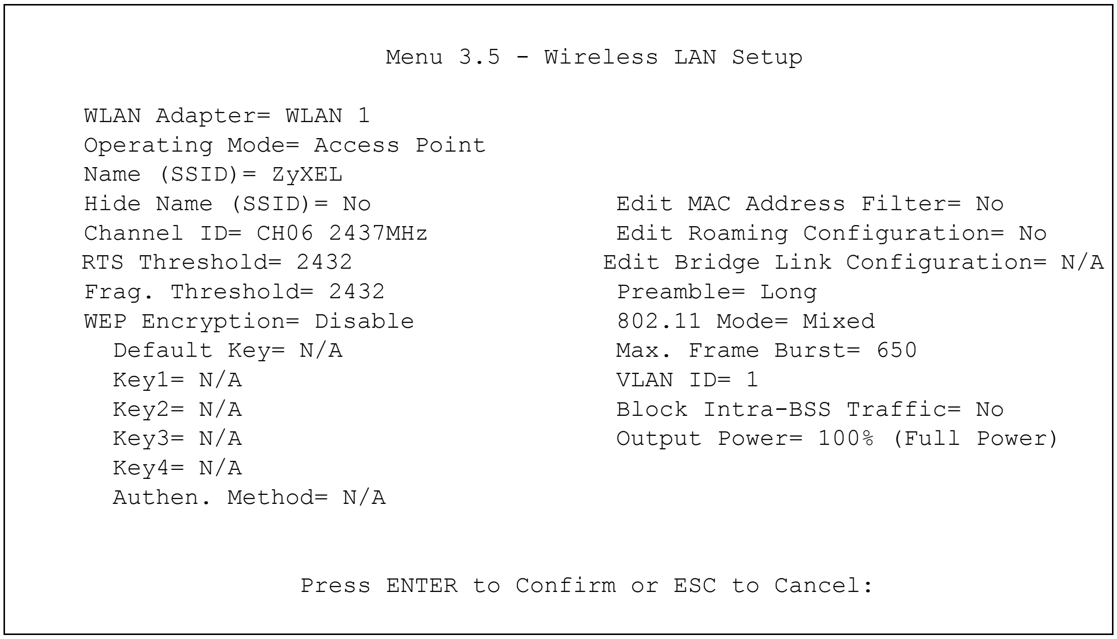
**Table 47** Menu 3.2 TCP/IP Setup

| FIELD | DESCRIPTION |
|---|---|
| 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.<br>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 |
| 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. |
| Gateway IP Address | Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your ZyAIR. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 14.3 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.

**Figure 75** Menu 3.5 Wireless LAN Setup



```
                         Menu 3.5 - Wireless LAN Setup

    WLAN Adapter= WLAN 1
    Operating Mode= Access Point
    Name (SSID)= ZyXEL
    Hide Name (SSID)= No                 Edit MAC Address Filter= No
    Channel ID= CH06 2437MHz             Edit Roaming Configuration= No
    RTS Threshold= 2432                 Edit Bridge Link Configuration= N/A
    Frag. Threshold= 2432                Preamble= Long
    WEP Encryption= Disable              802.11 Mode= Mixed
      Default Key= N/A                   Max. Frame Burst= 650
      Key1= N/A                          VLAN ID= 1
      Key2= N/A                          Block Intra-BSS Traffic= No
      Key3= N/A                          Output Power= 100% (Full Power)
      Key4= N/A
      Authen. Method= N/A


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

The following table describes the fields in this menu.

**Table 48** Menu 3.5 Wireless LAN Setup

| FIELD | DESCRIPTION |
|---|---|
| WLAN Adapter Index | Press [SPACE BAR] and select a wireless LAN adapter to configure. |
| Operating Mode | Press [SPACE BAR] and select **Access Point**, **Multiple ESS**, **Bridge / Repeater** or **AP + Bridge**. |
| Name (SSID) | The SSID (Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.<br>This field is only available when you select **Access Point** or **AP + Bridge** in the **Operating Mode** field. |
| Hide Name (SSID) | Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning. |
| Channel ID | Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region. |
| RTS Threshold | Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432. |
| Frag. Threshold | This is the maximum data fragment size that can be sent. Enter a value between 800 and 2432. |
| WEP Encryption | Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| 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. |

**Table 48** Menu 3.5 Wireless LAN Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| 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.<br>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").<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>**Note:** Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key. |
| Authen. Method | Press [SPACE BAR] to select **Auto**, **Open System Only** or **Shared Key Only** and press [ENTER].<br>This field is **N/A** if WEP is not activated.<br>If WEP encryption is activated, the default setting is **Auto**. |
| Edit MAC Address Filter | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.1 - WLAN MAC Address Filter**. |
| Edit Roaming Configuration | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.2 - Roaming Configuration**. |
| Edit Bridge Link Configuration | Use [SPACE BAR] to choose **Yes** and press [ENTER] to go to **Menu 3.5.4 - Bridge Link Configuration**. |
| Preamble | Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. The default setting is **Long**.<br>See the section on preamble for more information. |
| 802.11 Mode | Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.<br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.<br>Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced. |
| Max. Frame Burst | Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only.<br>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. |
| VLAN ID | The ZyAIR supports IEEE 802.1 tagged VLAN for partioning a physical network into multiple logical networks. Enter a number from 1 to 4094 to set the VLAN ID tag that the ZyAIR adds to the Ethernet frames that this WLAN adapter receives from wireless clients or other APs. |
| Block Intra-BSS Traffic | Press [SPACE BAR] to select **Yes** to only allow wireless stations to communicate with the wired network, not with each other.<br>Press [SPACE BAR] to select **No** to allow wireless stations connected to the ZyAIR to communicate with each other. |
| Output Power Level | Press [SPACE BAR] to select the amount of power you want the ZyAIR to use for the wireless signal. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. The options are **100% (Full Power)**, **50%**, **25%** or **12.5%**. The power output at full power is 18 ± 2 dBm. |
| 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. | |

### 14.3.1 Configuring MAC Address Filter

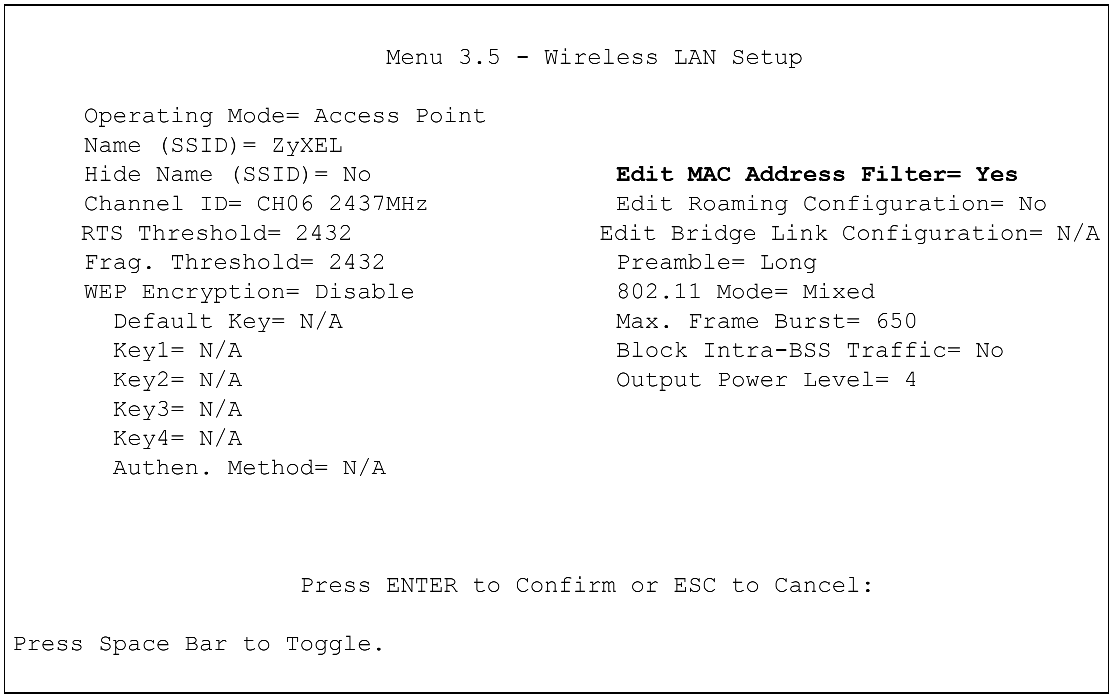
Your ZyAIR checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

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

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

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

**Figure 76** Menu 3.5 Wireless LAN Setup

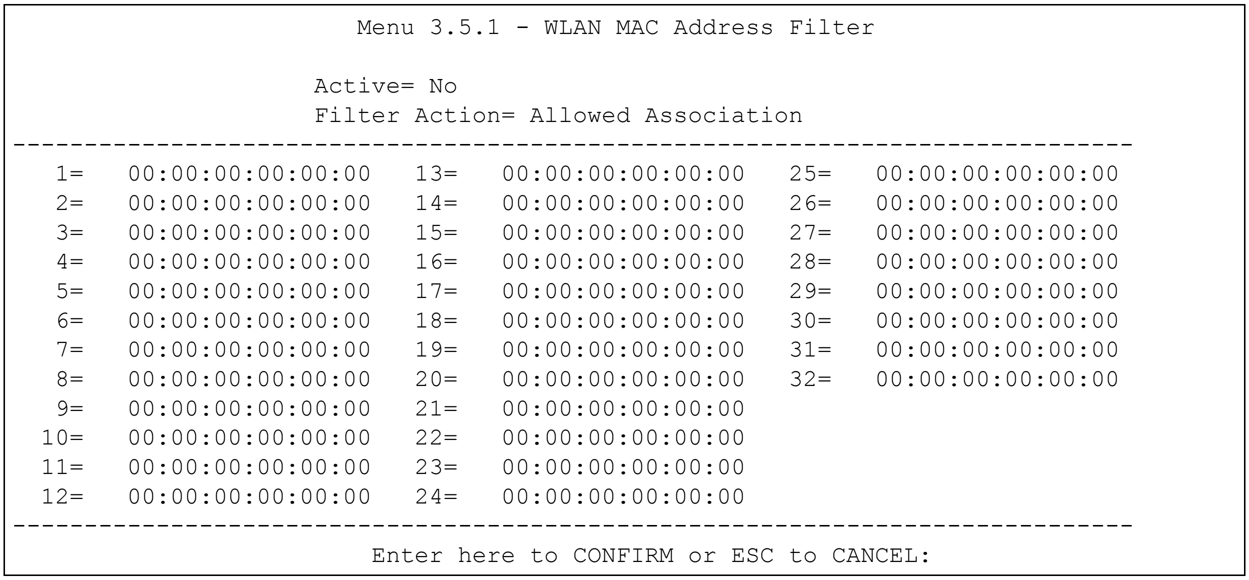


```
                          Menu 3.5 - Wireless LAN Setup

     Operating Mode= Access Point
     Name (SSID)= ZyXEL
     Hide Name (SSID)= No                  Edit MAC Address Filter= Yes
     Channel ID= CH06 2437MHz              Edit Roaming Configuration= No
     RTS Threshold= 2432                  Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                 Preamble= Long
     WEP Encryption= Disable               802.11 Mode= Mixed
       Default Key= N/A                    Max. Frame Burst= 650
       Key1= N/A                           Block Intra-BSS Traffic= No
       Key2= N/A                           Output Power Level= 4
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A



                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**3** Press [SPACE BAR] to select **Access Point** or **AP + Bridge** in the **Operating Mode** field and press [ENTER].

**4** 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.

**Figure 77** Menu 3.5.1 WLAN MAC Address Filter



```
                        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:
```

The following table describes the fields in this menu.

**Table 49** 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.<br>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.<br>The default action, **Allowed Association**, permits association with the ZyAIR. MAC addresses not listed will be denied access to the router. |
| MAC Address Filter | |
| 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. | |

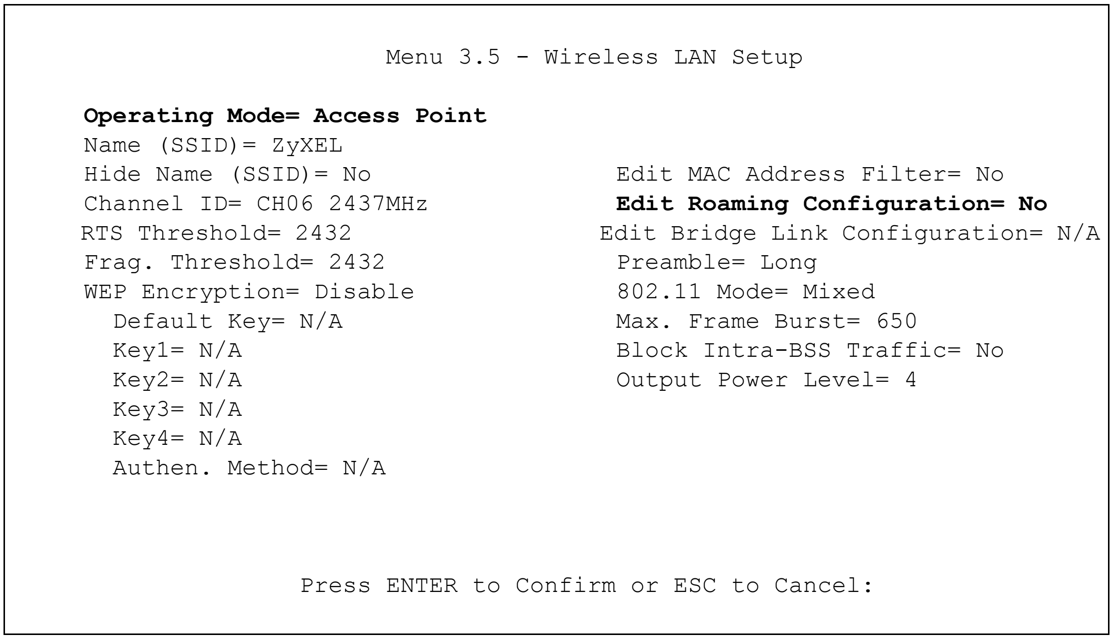
## 14.3.2 Configuring Roaming

Follow the steps below to configure roaming on your ZyAIR.

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

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

**Figure 78** Menu 3.5 Wireless LAN Setup

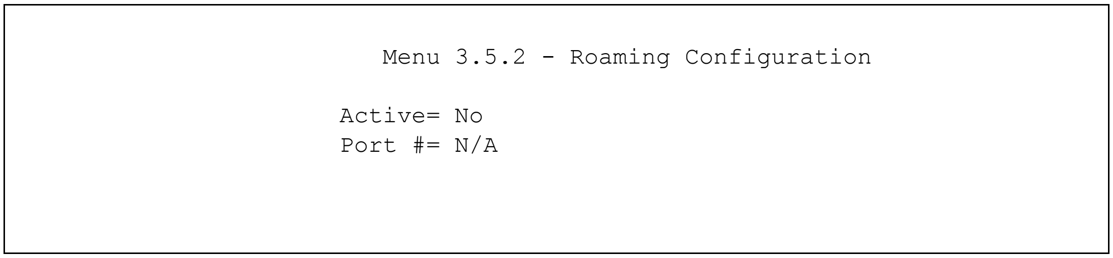


```
                        Menu 3.5 - Wireless LAN Setup

     Operating Mode= Access Point
     Name (SSID)= ZyXEL
     Hide Name (SSID)= No                 Edit MAC Address Filter= No
     Channel ID= CH06 2437MHz             Edit Roaming Configuration= No
     RTS Threshold= 2432                 Edit Bridge Link Configuration= N/A
     Frag. Threshold= 2432                Preamble= Long
     WEP Encryption= Disable              802.11 Mode= Mixed
       Default Key= N/A                   Max. Frame Burst= 650
       Key1= N/A                          Block Intra-BSS Traffic= No
       Key2= N/A                          Output Power Level= 4
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A



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

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

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

**Figure 79** Menu 3.5.2 - Roaming Configuration



```
                         Menu 3.5.2 - Roaming Configuration

                      Active= No
                      Port #= N/A
```

The following table describes the fields in this menu.

**Table 50** Menu 3.5.2 - Roaming Configuration

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] to 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.<br>**Note:** All APs on the same subnet and the wireless stations must have the same SSID to allow roaming. |
| 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 3517. 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. | |

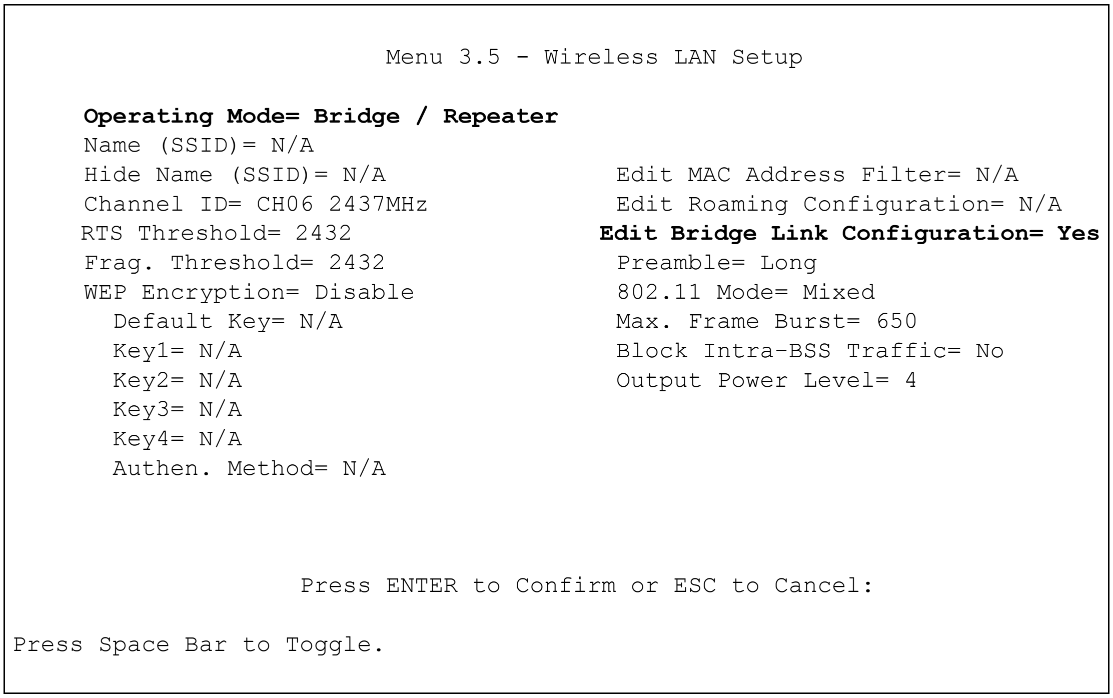
## 14.3.3 Configuring Bridge Link

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

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

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

**Figure 80** Menu 3.5 Wireless LAN Setup

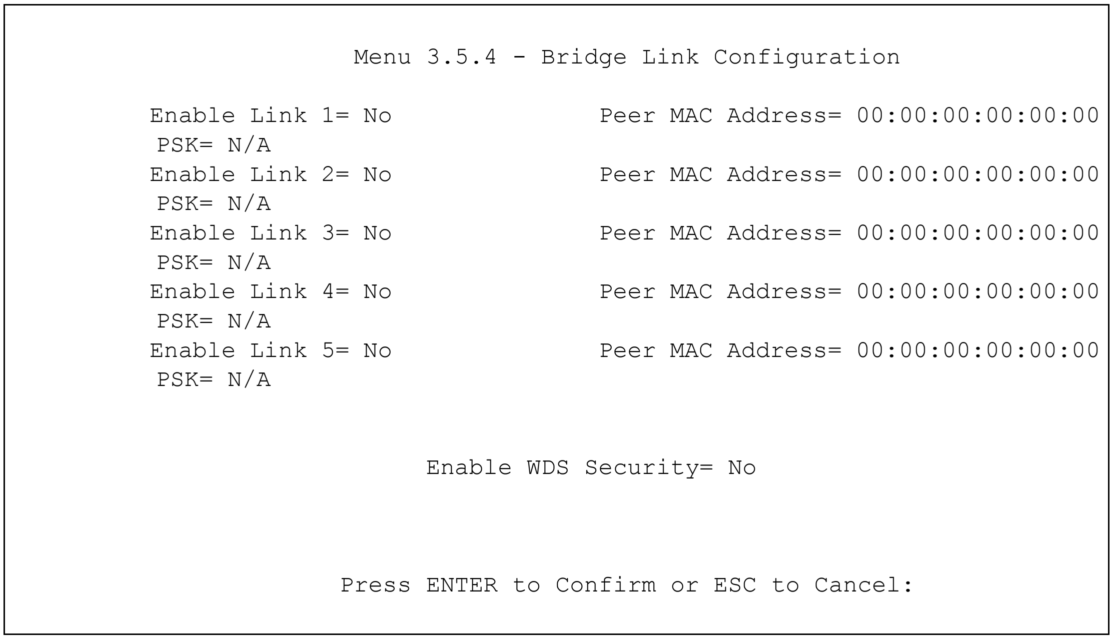


```
                         Menu 3.5 - Wireless LAN Setup

     Operating Mode= Bridge / Repeater
     Name (SSID)= N/A
     Hide Name (SSID)= N/A                  Edit MAC Address Filter= N/A
     Channel ID= CH06 2437MHz               Edit Roaming Configuration= N/A
     RTS Threshold= 2432                   Edit Bridge Link Configuration= Yes
     Frag. Threshold= 2432                  Preamble= Long
     WEP Encryption= Disable                802.11 Mode= Mixed
       Default Key= N/A                     Max. Frame Burst= 650
       Key1= N/A                            Block Intra-BSS Traffic= No
       Key2= N/A                            Output Power Level= 4
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A



                   Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**3** In the **Operating Mode** field, press [SPACE BAR] to select **Bridge / Repeater** or **AP + Bridge** and press [ENTER].

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

**Figure 81** Menu 3.5.4 - Bridge Link Configuration



```
                    Menu 3.5.4 - Bridge Link Configuration

    Enable Link 1= No             Peer MAC Address= 00:00:00:00:00:00
     PSK= N/A
    Enable Link 2= No             Peer MAC Address= 00:00:00:00:00:00
     PSK= N/A
    Enable Link 3= No             Peer MAC Address= 00:00:00:00:00:00
     PSK= N/A
    Enable Link 4= No             Peer MAC Address= 00:00:00:00:00:00
     PSK= N/A
    Enable Link 5= No             Peer MAC Address= 00:00:00:00:00:00
     PSK= N/A


                        Enable WDS Security= No



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

The following table describes the fields in this menu.

**Table 51** Menu 3.5.4 Bridge Link Configuration

| FIELD | DESCRIPTION |
|---|---|
| Enable Link 1-6 | Press [SPACE BAR] to select **Yes** or **No** and press [ENTER]. |
| Peer MAC Address | Type the MAC address of a wireless bridge in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Enable WDS Security | A Wireless Distribution System (WDS) is a wireless connection between two or more APs.<br>Press [SPACE BAR] to select **Yes** to use TKIP to encrypt traffic on the WDS between APs.<br>When you enable WDS security, type a Pre-Shared Key (PSK) for each link.<br>**Note:** Other wireless bridges must use the same encryption method to enable WDS security. |
| PSK | When you enable WDS, type a Pre-Shared Key (PSK) for each link. The pre-shared key can be from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| 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 15
# Dial-in User Setup

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

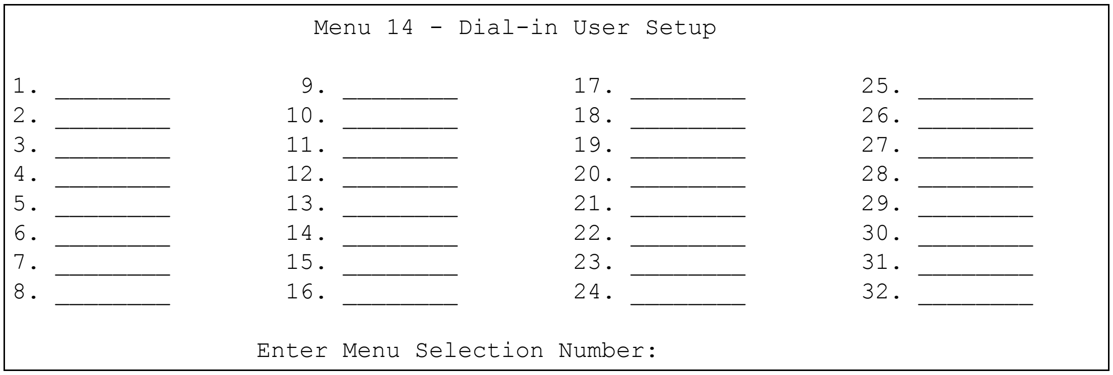
## 15.1 Dial-in User Setup

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.

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

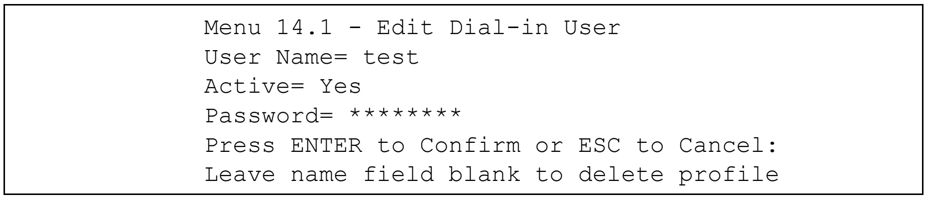
**Figure 82 Menu 14- Dial-in User Setup**



```
                       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:
```

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

**Figure 83** Menu 14.1- Edit Dial-in User



```
              Menu 14.1 - Edit Dial-in User
              User Name= test
              Active= Yes
              Password= ********
              Press ENTER to Confirm or ESC to Cancel:
              Leave name field blank to delete profile
```

The following table describes the fields in this screen.

**Table 52** Menu 14.1- Edit Dial-in User

| FIELD | DESCRIPTION |
|---|---|
| User Name | Enter a username up to 31 alphanumeric characters long for this user profile.<br>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. | |

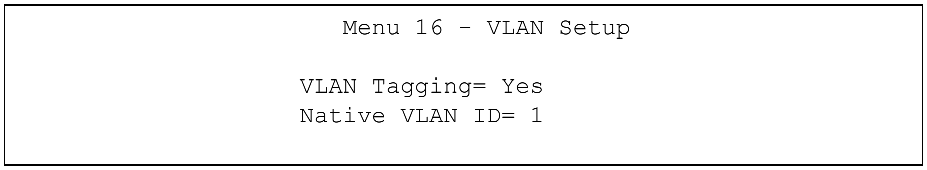
# CHAPTER 16 VLAN Setup

This chapter explains VLAN setup menu 16. Refer to the web configurator VLAN chapter for background information on VLAN.

## 16.1 VLAN Setup

To setup VLAN, select option 16 from the main menu to open Menu 16 – VLAN Setup as shown next.

**Figure 84** Menu 16 VLAN Setup



```
                    Menu 16 - VLAN Setup

                VLAN Tagging= Yes
                Native VLAN ID= 1
```

The following table describes the fields in this menu.

**Table 53** Menu 16 VLAN Setup

| FIELD | DESCRIPTION |
|---|---|
| VLAN Tagging | To enable VLAN tagging, press [SPACE BAR] to select Yes and press [ENTER]. |
| Native VLAN ID | This field is activated only when you select Yes in the VLAN Tagging field.<br>Enter a number from 1 to 4094 to specify the ID of the management VLAN. Your management computer must belong to this VLAN group in order to manage the ZyAIR. This can be done in the following ways:<br>• The management computer could be a wireless client of the ZyAIR if the ZyAIR's WLAN adapter is set to add the add the management VLAN ID tag to Ethernet frames received from wireless clients.<br>• The management computer could be on the wired network, behind a VLAN-aware switch that is configured to add the management VLAN ID tag to Ethernet frames from the computer before sending them to ZyAIR.<br>**Note:** Mail and FTP servers must have the same management VLAN ID to communicate with 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. | |

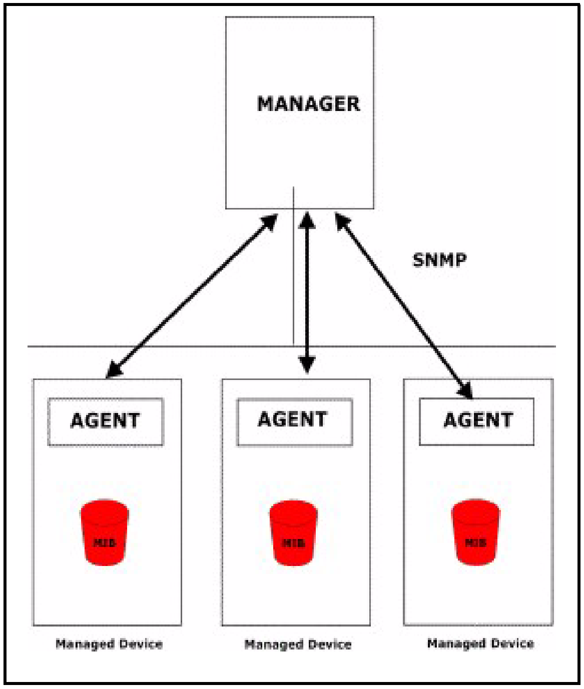
# CHAPTER 17
# SNMP Configuration

This chapter explains SNMP Configuration menu 22.

## 17.1 About SNMP

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

**Figure 85** 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.

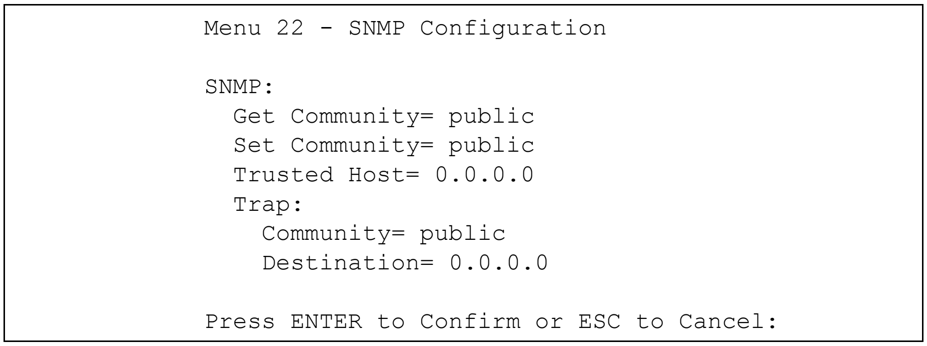
## 17.2 Supported MIBs

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.

## 17.3 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.

**Figure 86 Menu 22 SNMP Configuration**



```
              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:
```

The following table describes the SNMP configuration parameters.

**Table 54** Menu 22 SNMP Configuration

| FIELD | DESCRIPTION |
|---|---|
| SNMP: | |
| Get Community | Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station. |
| Set Community | Type the **Set Community**, which is the password for incoming Set requests from the management station. |
| 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. |
| Trap: | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| 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. | |

## 17.4 SNMP Traps

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

**Table 55** 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 when the port is up. |
| 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 when the port is down. |

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

**Table 56** Ports and Interface Types

| PHYSICAL PORT/ENCAP | INTERFACE TYPE |
|---|---|
| WLAN 1 | enet0 |
| Ethernet port | enet1 |
| WLAN 2 | enet2 |

# CHAPTER 18 System Security

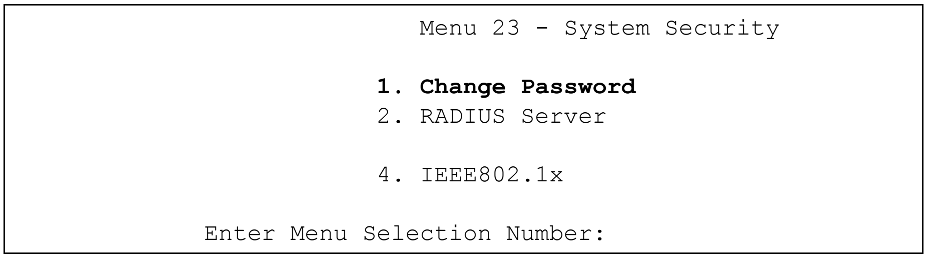
This chapter describes how to configure the system security on the ZyAIR.

## 18.1 System Security

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

### 18.1.1 System Password

**Figure 87** Menu 23 System Security



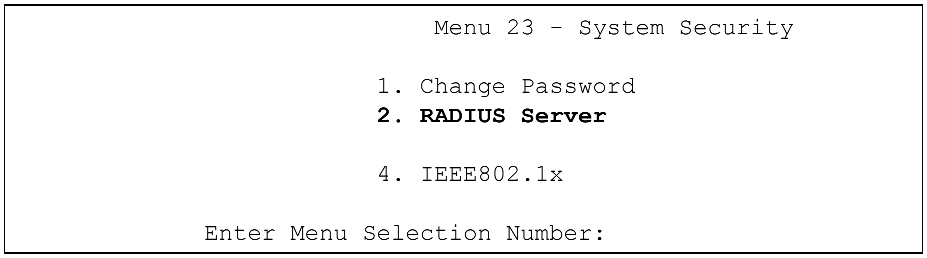
```
                              Menu 23 - System Security

                           1. Change Password
                           2. RADIUS Server

                           4. IEEE802.1x

              Enter Menu Selection Number:
```

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

### 18.1.2 Configuring External RADIUS Server

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

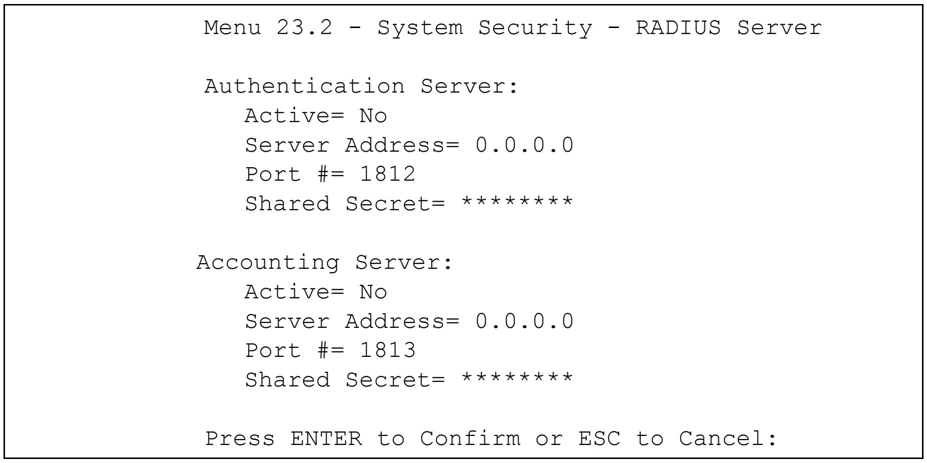
**Figure 88** Menu 23 System Security



```
                               Menu 23 - System Security

                           1. Change Password
                           2. RADIUS Server

                           4. IEEE802.1x

              Enter Menu Selection Number:
```

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

**Figure 89** Menu 23.2 System Security: RADIUS Server



```
             Menu 23.2 - System Security - RADIUS Server

             Authentication Server:
                Active= No
                Server Address= 0.0.0.0
                Port #= 1812
                Shared Secret= ********

            Accounting Server:
                Active= No
                Server Address= 0.0.0.0
                Port #= 1813
                Shared Secret= ********

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

The following table describes the fields in this menu.

**Table 57** Menu 23.2 System Security: RADIUS Server

| FIELD | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server. |
| Server Address | To use an external authentication server, enter its IP address in dotted decimal notation.<br>Enter **127.0.0.1** to use the internal authentication server. |
| Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | To use an external authentication server, specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points.<br>The key is not sent over the network. This key must be the same on the external authentication server and ZyAIR.<br>Enter **1234** to use the internal authentication server. |
| Accounting Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server. |
| Server Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |

**Table 57** Menu 23.2 System Security: RADIUS Server (continued)

| FIELD | DESCRIPTION |
|---|---|
| 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.<br>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. | |

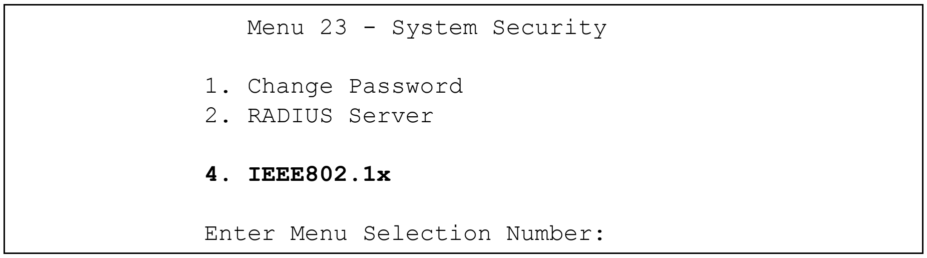
## 18.1.3 802.1x

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.

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

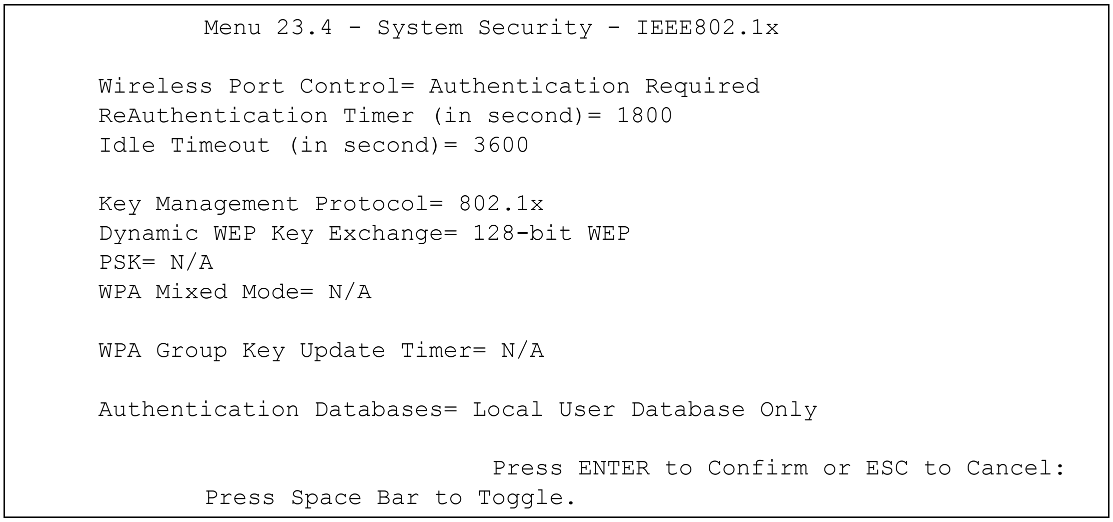
**Figure 90** Menu 23 System Security



```
                 Menu 23 - System Security

              1. Change Password
              2. RADIUS Server

              4. IEEE802.1x

              Enter Menu Selection Number:
```

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

**Figure 91** 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

      Key Management Protocol= 802.1x
      Dynamic WEP Key Exchange= 128-bit WEP
      PSK= N/A
      WPA Mixed Mode= N/A

      WPA Group Key Update Timer= N/A

      Authentication Databases= Local User Database Only

                                 Press ENTER to Confirm or ESC to Cancel:
              Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

**Table 58** 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.<br>Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.<br>Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>Select **No Access Allowed** to block all wireless stations access to the wired network.<br>The following fields are not available when you select **No Authentication Required** or **No Access Allowed**. |
| ReAuthentication Timer (in second) | Specify how often a client has to re-enter username and password to stay connected to the wired network.<br>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 (in second) | The ZyAIR automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.<br>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). |
| Key Management Protocol | Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER]. |

**Table 58** Menu 23.4 System Security: IEEE802.1x (continued)

| FIELD | DESCRIPTION |
|---|---|
| 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.<br>Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption.<br>Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange. |
| PSK | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field. |
| WPA Mixed Mode | Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Data Privacy for Broadcast/Multicast packets** field. |
| WPA Group Key Update Timer | The **WPA Broadcast/Multicast Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Broadcast/ Multicast Key Update Timer** is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes). |
| Authentication Databases | 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.<br>Before you specify the priority, make sure you have set up the corresponding database correctly first.<br>When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**.<br>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.<br>Select **RADIUS Only** to have the ZyAIR just check the user database on the external RADIUS server for a wireless station's username and password.<br>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 external RADIUS server.<br>Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the external 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. |
| 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

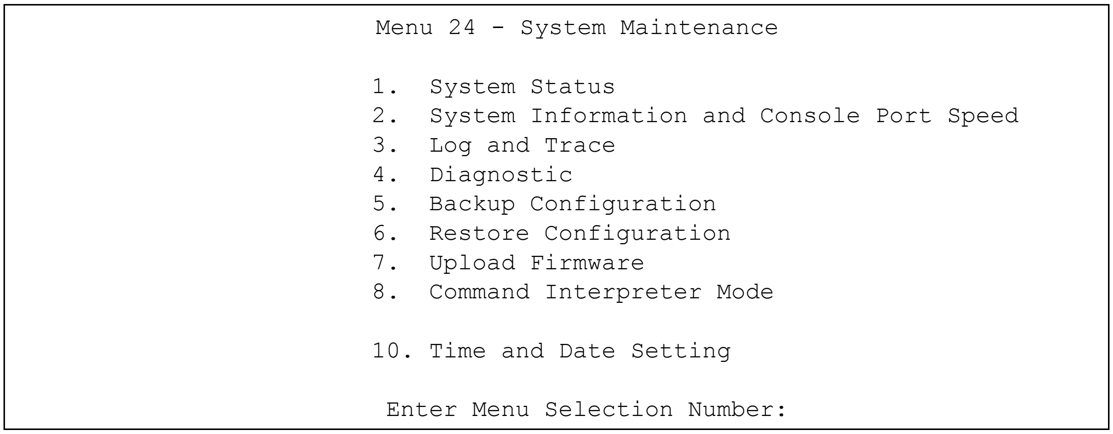
# CHAPTER 19 System Information and Diagnosis

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.

**Figure 92** Menu 24 System Maintenance



```
                         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

                          Enter Menu Selection Number:
```

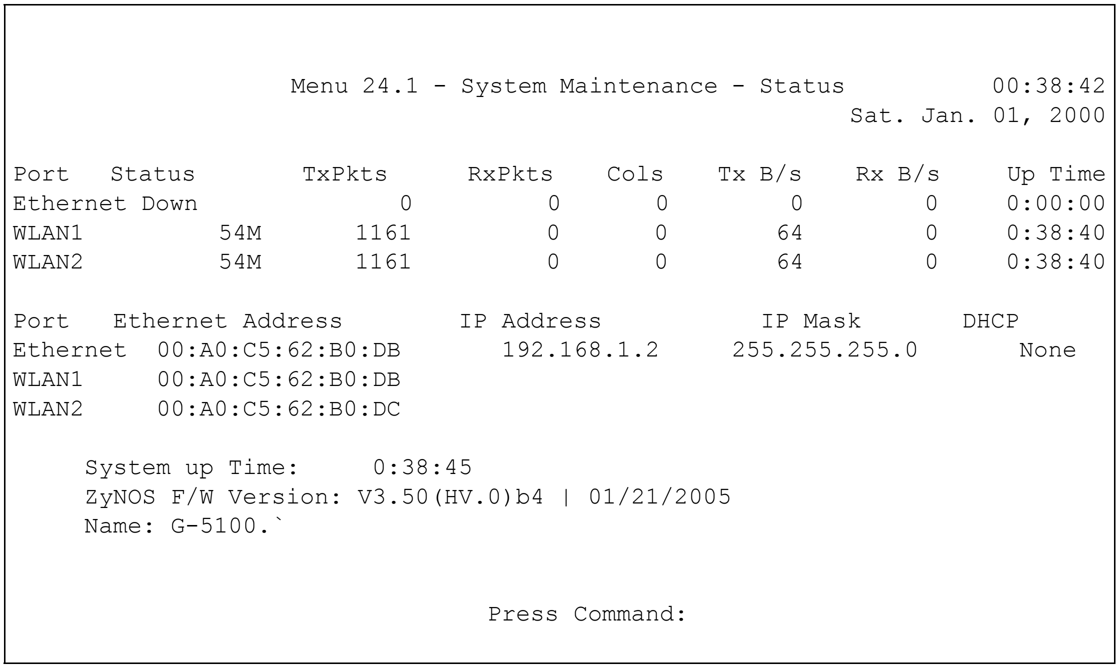
## 19.1 System Status

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

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

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

**Figure 93** Menu 24.1 System Maintenance: Status



```
                   Menu 24.1 - System Maintenance - Status           00:38:42
                                                           Sat. Jan. 01, 2000

Port   Status        TxPkts      RxPkts    Cols   Tx B/s    Rx B/s     Up Time
Ethernet Down              0         0       0         0        0     0:00:00
WLAN1         54M       1161         0       0        64        0     0:38:40
WLAN2         54M       1161         0       0        64        0     0:38:40

Port   Ethernet Address        IP Address           IP Mask       DHCP
Ethernet  00:A0:C5:62:B0:DB       192.168.1.2     255.255.255.0       None
WLAN1     00:A0:C5:62:B0:DB
WLAN2     00:A0:C5:62:B0:DC

     System up Time:     0:38:45
     ZyNOS F/W Version: V3.50(HV.0)b4 | 01/21/2005
     Name: G-5100.`


                                 Press Command:
```

The following table describes the fields present in this menu.

**Table 59** Menu 24.1 System Maintenance: Status

| FIELD | DESCRIPTION |
|---|---|
| Port | This identifies the port or WLAN adapter. |
| 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 or WLAN adapter. |
| 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. |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |
| Name | This displays the device name. |

## 19.2 System Information

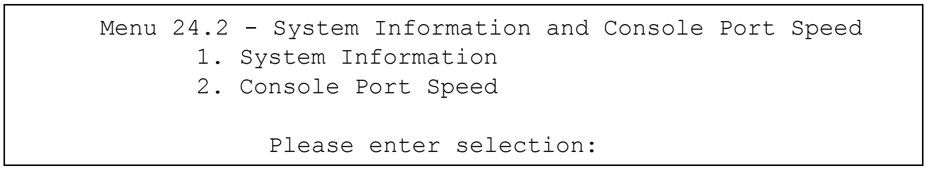
To get to the System Information:

1 Enter 24 to display **Menu 24 – System Maintenance**.

2 Enter 2 to display **Menu 24.2 – System Information and Console Port Speed**.

3 From this menu you have two choices as shown in the next figure:

**Figure 94** Menu 24.2 System Information and Console Port Speed



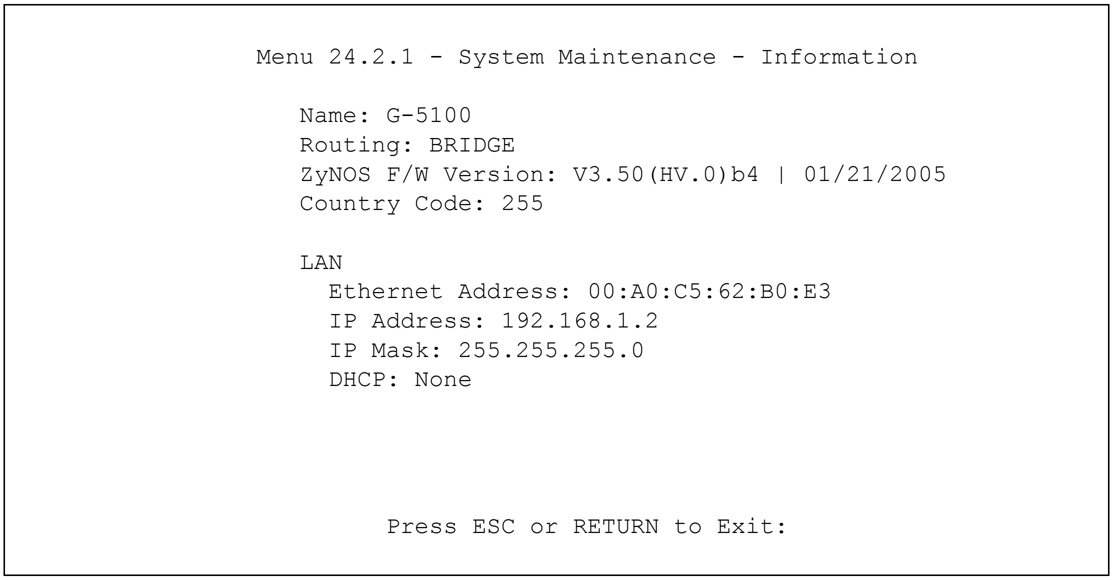
```
     Menu 24.2 - System Information and Console Port Speed
            1. System Information
            2. Console Port Speed

                 Please enter selection:
```

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

### 19.2.1 System Information

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

**Figure 95** Menu 24.2.1 System Information: Information



```
                Menu 24.2.1 - System Maintenance - Information

                   Name: G-5100
                   Routing: BRIDGE
                   ZyNOS F/W Version: V3.50(HV.0)b4 | 01/21/2005
                   Country Code: 255

                   LAN
                     Ethernet Address: 00:A0:C5:62:B0:E3
                     IP Address: 192.168.1.2
                     IP Mask: 255.255.255.0
                     DHCP: None




                         Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

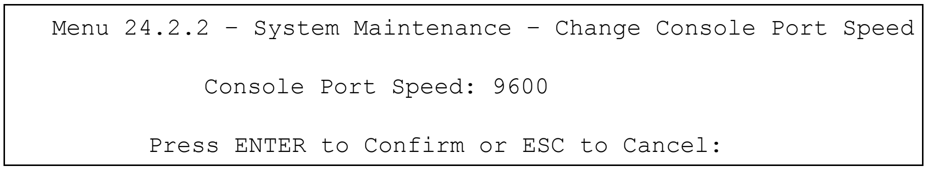
**Table 60** Menu 24.2.1 System Maintenance: Information

| 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) of your ZyAIR. |
| IP Address | This is the IP address of the ZyAIR in dotted decimal notation. |
| IP Mask | This shows the subnet mask of the ZyAIR. |
| DHCP | This field shows the DHCP setting of the ZyAIR. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

### 19.2.2 Console Port Speed

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

**Figure 96** Menu 24.2.2 System Maintenance: Change Console Port Speed



```
  Menu 24.2.2 - System Maintenance - Change Console Port Speed

              Console Port Speed: 9600

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

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

## 19.3 Log and Trace

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

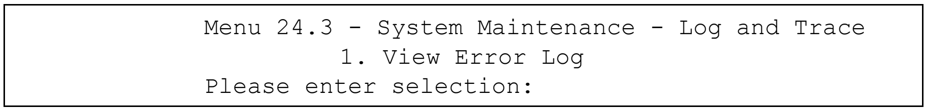
### 19.3.1 Viewing Error Log

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:

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

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

**Figure 97** Menu 24.3 System Maintenance: Log and Trace

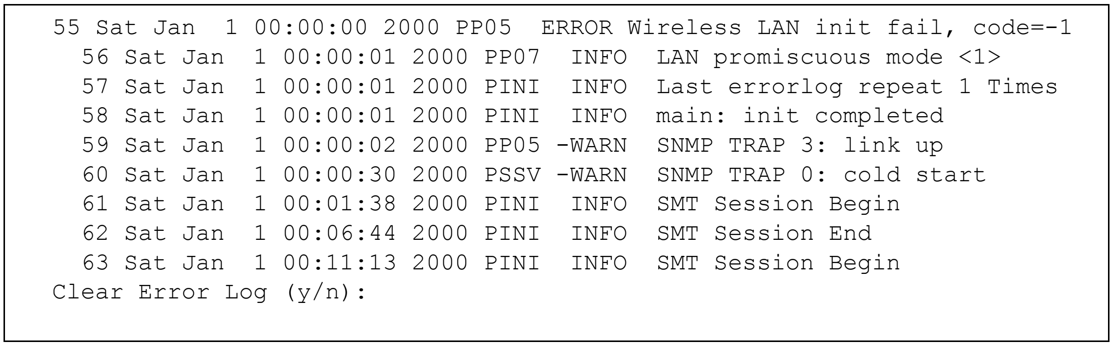


```
Menu 24.3 - System Maintenance - Log and Trace
         1. View Error Log
Please enter selection:
```

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.

**Figure 98** Sample Error and Information Messages

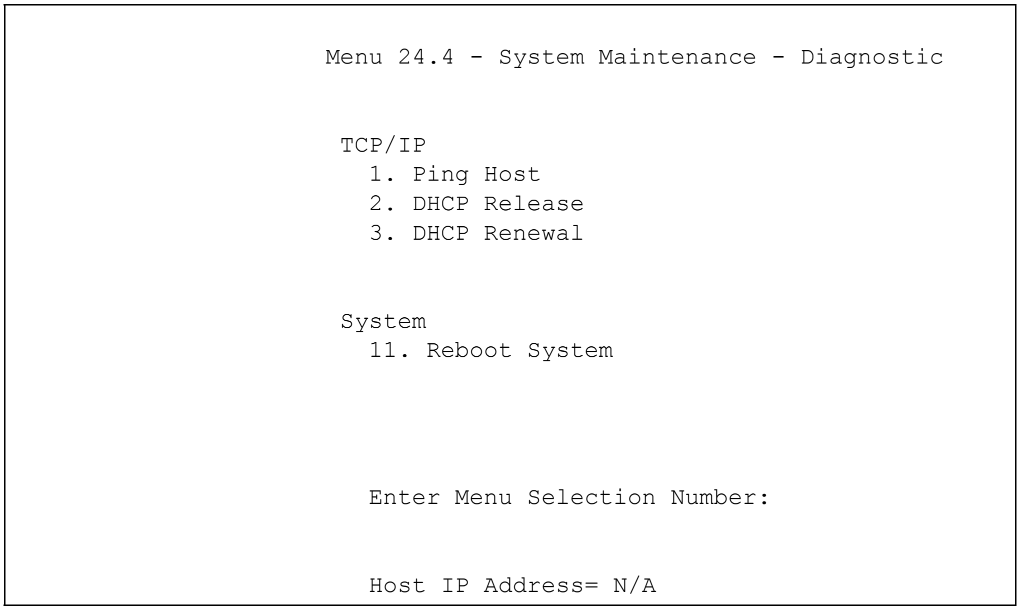


```
55 Sat Jan  1 00:00:00 2000 PP05  ERROR Wireless LAN init fail, code=-1
  56 Sat Jan  1 00:00:01 2000 PP07  INFO  LAN promiscuous mode <1>
  57 Sat Jan  1 00:00:01 2000 PINI  INFO  Last errorlog repeat 1 Times
  58 Sat Jan  1 00:00:01 2000 PINI  INFO  main: init completed
  59 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
  60 Sat Jan  1 00:00:30 2000 PSSV -WARN  SNMP TRAP 0: cold start
  61 Sat Jan  1 00:01:38 2000 PINI  INFO  SMT Session Begin
  62 Sat Jan  1 00:06:44 2000 PINI  INFO  SMT Session End
  63 Sat Jan  1 00:11:13 2000 PINI  INFO  SMT Session Begin
Clear Error Log (y/n):
```

## 19.4 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.

**Figure 99** Menu 24.4 System Maintenance: Diagnostic



```
                      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
```

Follow the procedure next to get to display this menu:

1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.
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 61** Menu 24.4 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 20 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.

## 20.1 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 62** 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. |

## 20.2 Backup Configuration

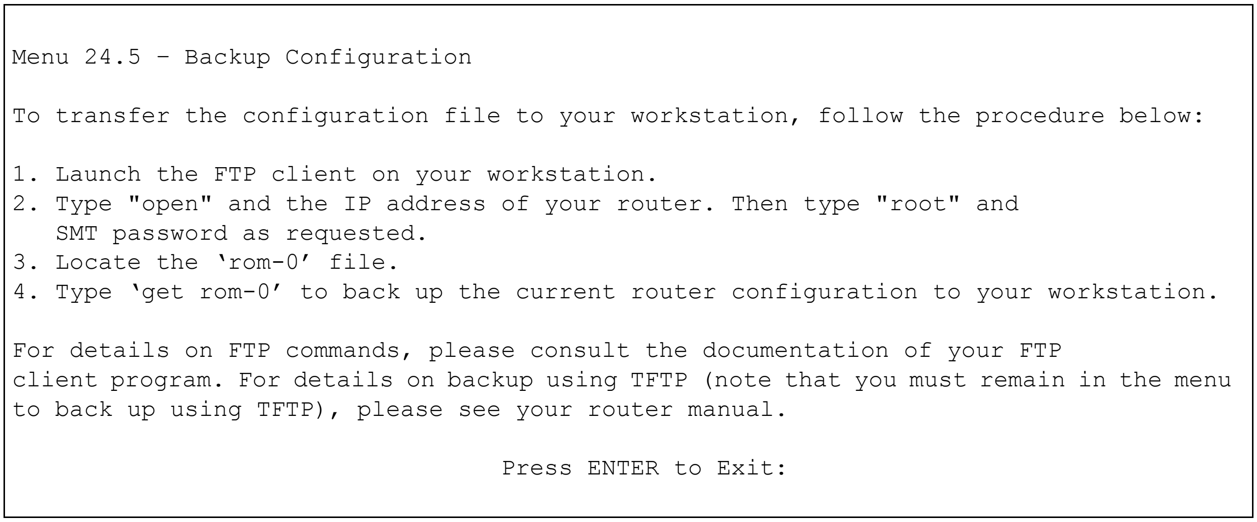
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred method, although TFTP can also be used.

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.

### 20.2.1 Backup Configuration Using FTP

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

**Figure 100** Menu 24.5 Backup Configuration



```
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:
```

## 20.2.2 Using the FTP command from the DOS Prompt

1 Launch the FTP client on your computer.

2 Enter "open" and the IP address of your ZyAIR.

3 Press [ENTER] when prompted for a username.

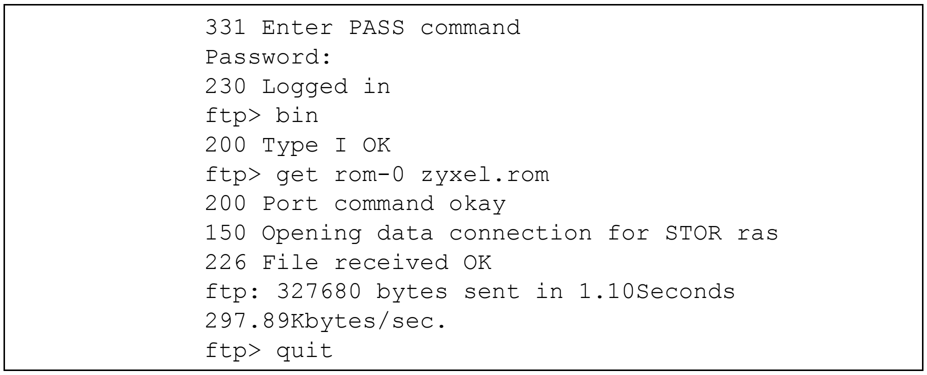
4 Enter your password as requested. The default is 1234.

5 Enter "bin" to set transfer mode to binary.

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.

7 Enter "quit" to exit the FTP prompt.

**Figure 101** FTP Session Example



```
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
```

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

**Table 63** General Commands for Third Party FTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>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.<br>Normal.<br>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. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### 20.2.3 Backup Configuration Using TFTP

The ZyAIR supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over Ethernet.

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

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.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

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.

4 Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.

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.

### 20.2.4 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 64** 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. |

**Table 64** General Commands for Third Party TFTP Clients (continued)

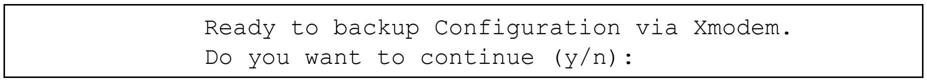
| COMMAND | DESCRIPTION |
|---|---|
| Local File | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer. |
| Remote File | This is the filename on the ZyAIR. The filename for the firmware is "ras" and for the configuration file, is "rom-0". |
| Binary | Transfer the file in binary mode. |
| Abort | Stop transfer of the file. |

### 20.2.5 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

**1** Display menu 24.5 and enter "y" at the following screen.

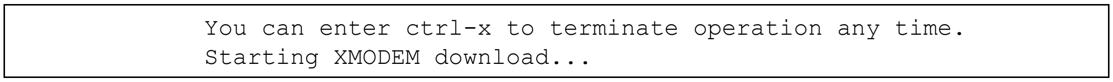
**Figure 102** System Maintenance: Backup Configuration



```
              Ready to backup Configuration via Xmodem.
              Do you want to continue (y/n):
```

**2** The following screen indicates that the Xmodem download has started.

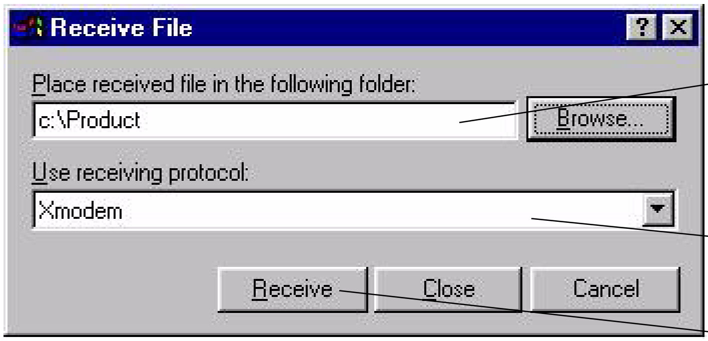
**Figure 103** System Maintenance: Starting Xmodem Download Screen



```
              You can enter ctrl-x to terminate operation any time.
              Starting XMODEM download...
```

**3** Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

**Figure 104** Backup Configuration Example



Place received file in the following folder: c:\Product

Use receiving protocol: Xmodem

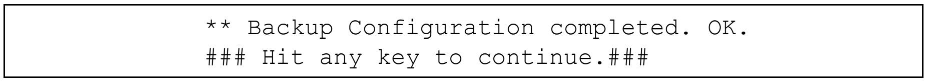
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

**4** After a successful backup you will see the following screen. Press any key to return to the SMT menu.

**Figure 105** Successful Backup Confirmation Screen



```
              ** Backup Configuration completed. OK.
              ### Hit any key to continue.###
```

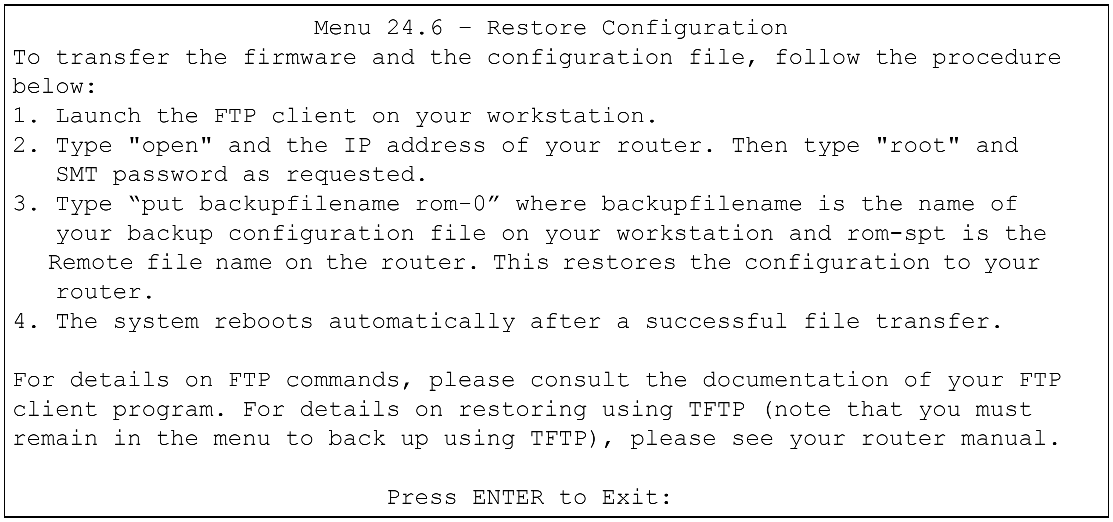
# 20.3 Restore Configuration

**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.

## 20.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

**Figure 106** Menu 24.6 Restore Configuration



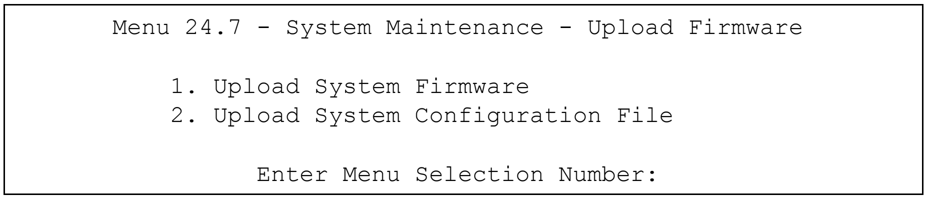
```
                     Menu 24.6 - Restore Configuration
To transfer the firmware and the configuration file, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type “put backupfilename 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:
```

# 20.4 Uploading Firmware and Configuration Files

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

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

**Figure 107** Menu 24.7 System Maintenance: Upload Firmware



```
       Menu 24.7 - System Maintenance - Upload Firmware

           1. Upload System Firmware
           2. Upload System Configuration File

                 Enter Menu Selection Number:
```

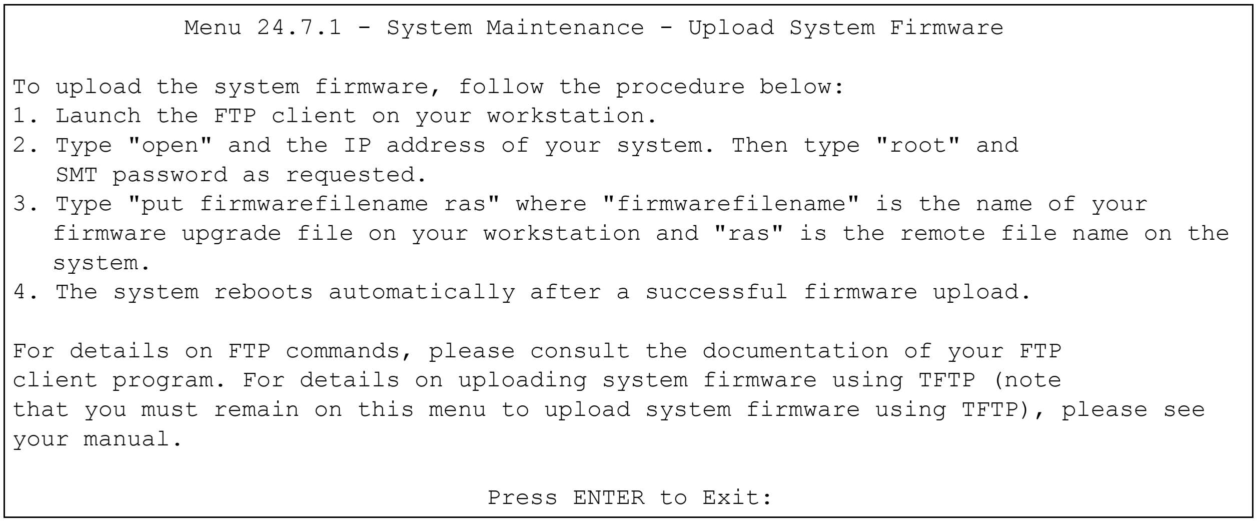
The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

## 20.4.1 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.

**Figure 108** Menu 24.7.1 System Maintenance: Upload System Firmware

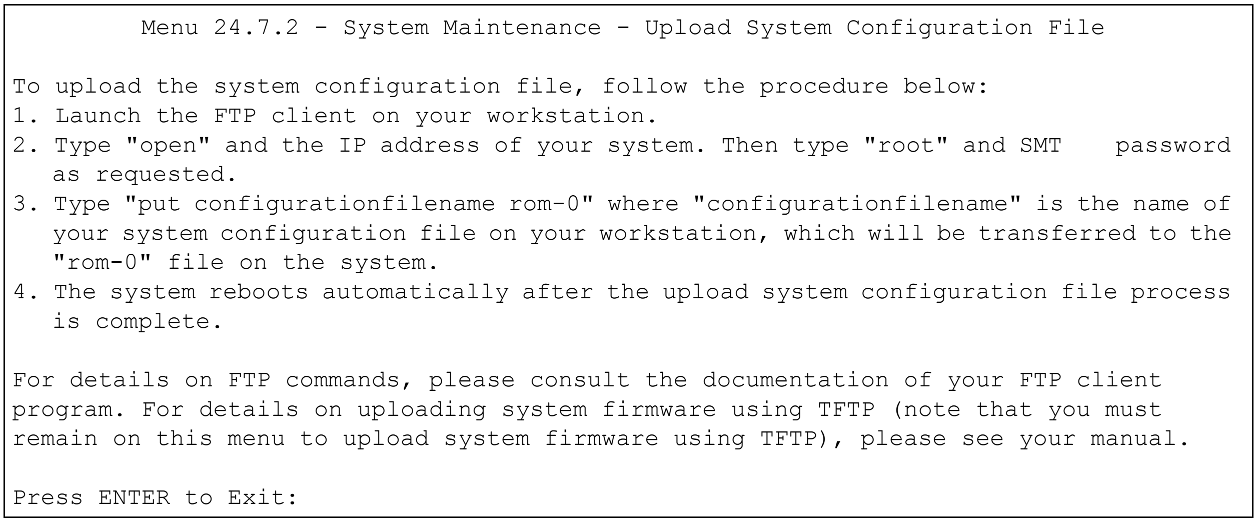


```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

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:
```

## 20.4.2 Configuration File Upload

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

**Figure 109** Menu 24.7.2 System Maintenance: Upload System Configuration File



```
         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:
```

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

## 20.4.3 Using the FTP command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open” and the IP address of your ZyAIR.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested. The default is 1234.
5. Enter “bin” to set transfer mode to binary.
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.
7. Enter “quit” to exit the FTP prompt.

**Figure 110** FTP Session Example

```
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
```

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

### 20.4.4 TFTP File Upload

The ZyAIR also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over Ethernet.

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:

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.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
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.
4. Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
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.

### 20.4.5 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.

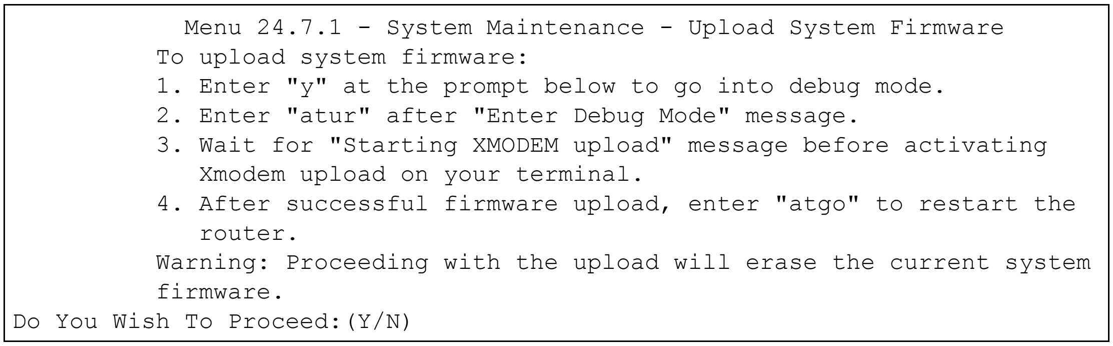
### 20.4.6 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyAIR. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyAIR via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

### 20.4.7 Uploading Firmware File Via Console Port

Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

**Figure 111** Menu 24.7.1 as Seen Using the Console Port



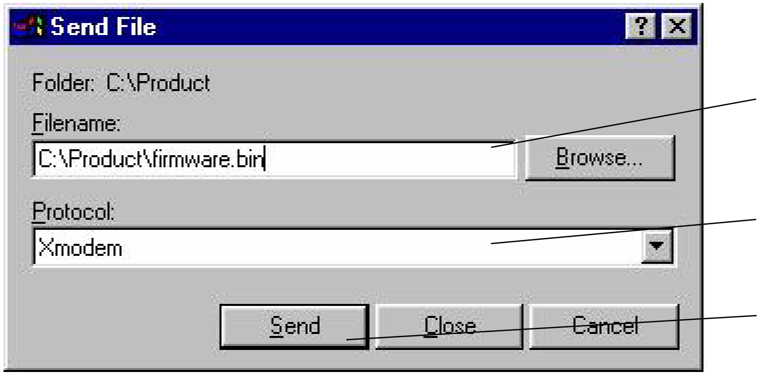
```
            Menu 24.7.1 - System Maintenance - Upload System Firmware
          To upload system firmware:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atur" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             router.
          Warning: Proceeding with the upload will erase the current system
          firmware.
Do You Wish To Proceed:(Y/N)
```

After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

### 20.4.8 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 112** Example Xmodem Upload



Type the firmware file’s location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

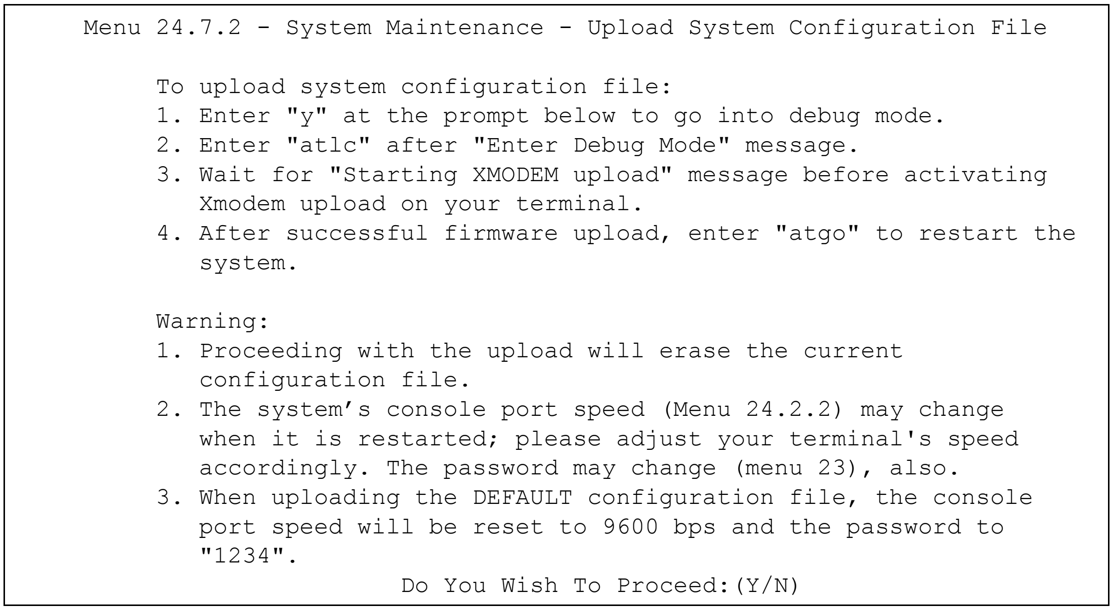
Then click **Send**.

After the firmware upload process has completed, the ZyAIR will automatically restart.

## 20.4.9 Uploading Configuration File Via Console Port

**1** Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

**Figure 113** Menu 24.7.2 as Seen Using the Console Port



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

          To upload system configuration file:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atlc" after "Enter Debug Mode" message.
          3. Wait for "Starting XMODEM upload" message before activating
             Xmodem upload on your terminal.
          4. After successful firmware upload, enter "atgo" to restart the
             system.

          Warning:
          1. Proceeding with the upload will erase the current
             configuration file.
          2. The system’s console port speed (Menu 24.2.2) may change
             when it is restarted; please adjust your terminal's speed
             accordingly. The password may change (menu 23), also.
          3. When uploading the DEFAULT configuration file, the console
             port speed will be reset to 9600 bps and the password to
             "1234".
                         Do You Wish To Proceed:(Y/N)
```

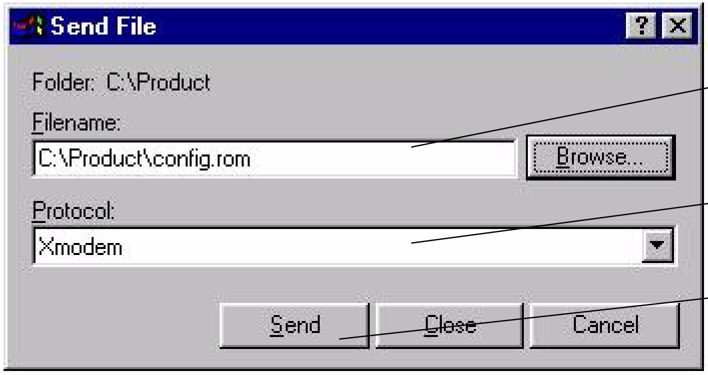
**2** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

**3** Enter “atgo” to restart the ZyAIR.

## 20.4.10 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 114 Example Xmodem Upload



Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

After the configuration upload process has completed, restart the ZyAIR by entering "atgo"

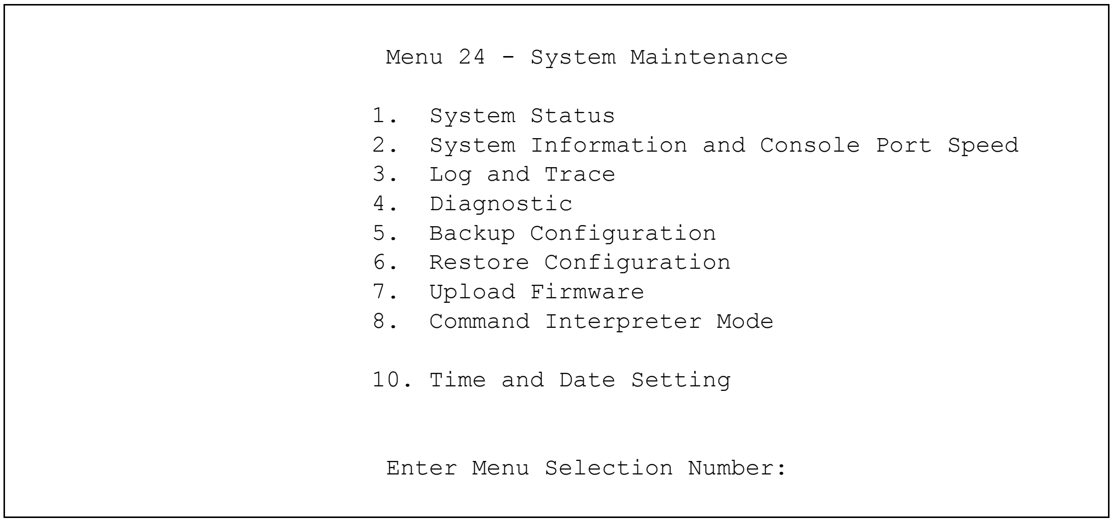
# CHAPTER 21 System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

## 21.1 Command Interpreter Mode

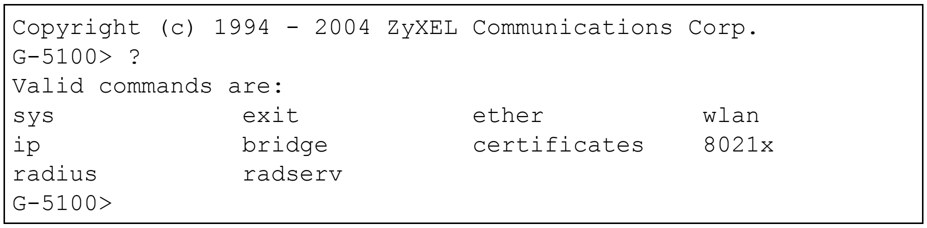
The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed 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.

**Figure 115** Menu 24 System Maintenance



```
                  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


                  Enter Menu Selection Number:
```

**Figure 116** Valid CI Commands



```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
G-5100> ?
Valid commands are:
sys             exit            ether           wlan
ip              bridge          certificates    8021x
radius          radserv
G-5100>
```

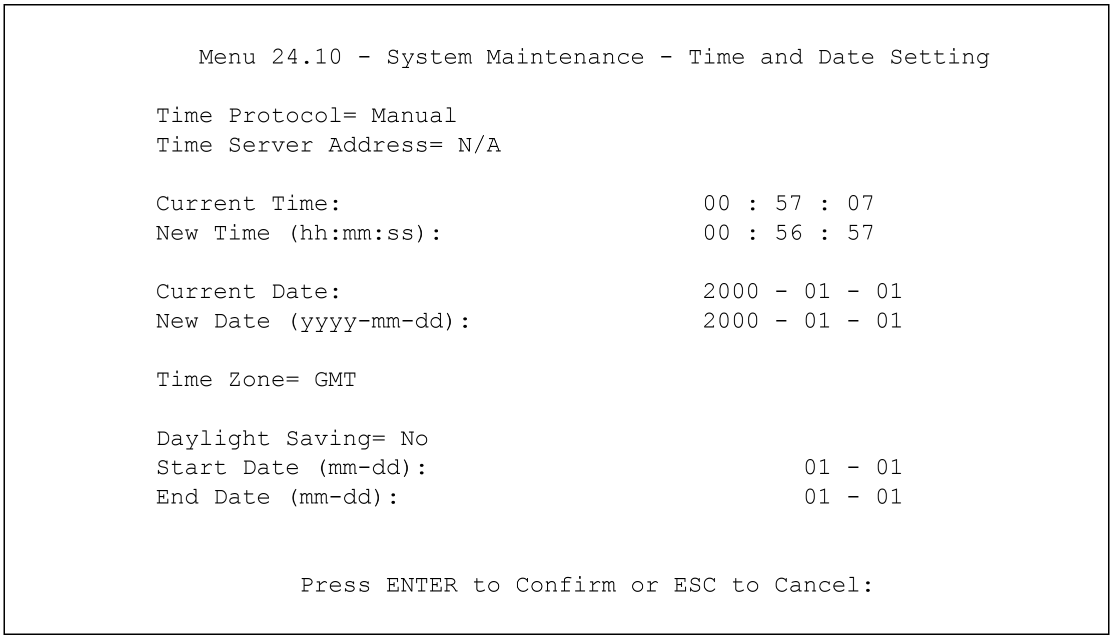
## 21.2 Time and Date Setting

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.

1 Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.

2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyAIR as shown in the following screen.

**Figure 117** Menu 24.10 System Maintenance: Time and Date Setting



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

          Time Protocol= Manual
          Time Server Address= N/A

          Current Time:                         00 : 57 : 07
          New Time (hh:mm:ss):                  00 : 56 : 57

          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:
```

The following table describes the fields in this menu.

**Table 65** System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Time Protocol | 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.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**NTP (RFC-1305)** is similar to **Time (RFC-868)**.<br>**None** The default, enter the time manually. |
| 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 saving time, then choose **Yes**. |
| Start Date | If using daylight saving time, enter the month and day that it starts on. |
| End Date | If using daylight saving 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. | |

### 21.2.1 Resetting the Time

The ZyAIR resets the time in three instances:

1. On leaving menu 24.10 after making changes.
2. When the ZyAIR starts up, if there is a timeserver configured in menu 24.10.
3. 24-hour intervals after starting.

# CHAPTER 22 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.

## 22.1 Problems Starting Up the ZyAIR

**Table 66** Troubleshooting the Start-Up of Your ZyAIR

| | |
|---|---|
| The power injector's **POWER** and **ACTIVE** LEDs are off. | Make sure the power cord is connected to an adequate power supply and that the power supply is turned on.<br>Disconnect and reconnect the power supply. If the error persists, you may have a hardware problem. In this case, you should contact your vendor. |
| The **ACTIVE** LED on the power injector is off. | Check the cable connection to the ZyAIR's special Ethernet port. The outdoor Ethernet cable must be straight-through and no longer than 80 m. |
| The ZyAIR reboots automatically sometimes. | The supplied power to the ZyAIR is too low. Check that the ZyAIR is receiving enough power.<br>Make sure the power source is working properly. |

## 22.2 Problems with Console Port Access

**Table 67** Troubleshooting Console Port Access

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| I cannot access the ZyAIR via the console port. | 1. Check to see if the ZyAIR is connected to your computer's console port. |
| | 2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:<br>VT100 terminal emulation.<br>9,600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.<br>No parity, 8 data bits, 1 stop bit, data flow set to none. |

## 22.3 Problems with the Ethernet Interface

**Table 68** Troubleshooting the Ethernet Interface

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the ZyAIR from the LAN. | If all of the LEDs on the inline power injector are on, check the Ethernet cable connection between your ZyAIR and the computer connected to the **DATA IN** port on the inline power injector.<br>Use a cross-over Ethernet cable to connect the power injector to a computer. Use a straight through Ethernet cable to connect the power injector to a switch or router.<br>Check for faulty Ethernet cables.<br>Make sure the computer’s Ethernet adapter is installed and working properly.<br>If directly connected to the ZyAIR, verify that the IP addresses and the subnet masks of the ZyAIR and the computer are on the same subnet. |
| | Ping the ZyAIR. Make sure your computer’s Ethernet card is installed and functioning properly.<br>In the computer, click **Start**, (**All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the ZyAIR’s IP address (192.168.1.2 is the default) and then press [ENTER]. The ZyAIR should reply. |
| Cannot access the web configurator. | You must connect to the ZyAIR’s current IP address and your computer’s IP address must be in the same subnet as the ZyAIR’s IP address.<br>If you don’t know the ZyAIR’s IP address, you can check the IP address in the System Management Terminal (SMT). Use the included console cable to connect the ZyAIR’s console port to a computer running a terminal emulation program set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 9600 bps port speed.<br>If the ZyAIR is set to get an IP address via DHCP, you can check the DHCP server to see which IP address it assigned to the ZyAIR. |
| | You may also need to clear your Internet browser’s cache.<br>In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen.<br>In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.<br>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer’s ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device’s MAC address).<br>In Windows, use **arp -d** at the command prompt to delete all entries in your computer’s ARP table. |
| I cannot ping any computer on the LAN. | If the LEDs on the inline power injector are on, check the Ethernet cable connection between your ZyAIR and the computer connected to the **DATA IN** port on the inline power injector.<br>Verify that the IP addresses and the subnet masks of the ZyAIR and the computers are on the same subnet. |

## 22.4 Problems with the Password

**Table 69** 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.<br>If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file. 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 baud rate of 9,600 bps, with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to '1234', also. |

## 22.5 Problems with Telnet

**Table 70** Troubleshooting Telnet

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| I cannot access the ZyAIR through Telnet. | Refer to Section 22.3 on page 186" section for instructions on checking your Ethernet connection. |

## 22.6 Problems with the WLAN Interface

**Table 71** Troubleshooting the WLAN Interface

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| I cannot ping any computer on the WLAN. | Make sure the wireless adapter on the wireless station is working properly.<br>Check that both the ZyAIR and wireless station(s) are using the same SSID, channel and WEP keys (if WEP encryption is activated). |

# APPENDIX A Specifications

## General Specifications

**Table 72** Device Specifications

| | |
|---|---|
| Default IP Address | 192.168.1.2 |
| Default Subnet Mask | 255.255.255.0 (24 bits) |
| Default Password | 1234 |

**Table 73** Performance

| | |
|---|---|
| WLAN Connection Distance | IEEE 802.11g, up to 500 m<br>IEEE 802.11g, up to 5 km |

**Table 74** Firmware Features

| | |
|---|---|
| System Management | Embedded Web Configurator (HTTP)<br>Menu-driven SMT (System Management Terminal) management<br>CLI (Command Line Interpreter)<br>Remote Management via Telnet or Web<br>Diagnostic tool (built-in)<br>SNMP Manageable<br>Firmware Upgrade (web configurator, TFTP/FTP)<br>RADIUS client |
| Wireless | IEEE 802.11b Compliant<br>IEEE 802.11g Compliant<br>Can support simultaneous IEEE 802.11b and IEEE 802.11g connections or can be configured to only use one or the other.<br>2 ESSID/VLANs of for the WLANs (one for each WLAN card)<br>Frequency Range: 2.4 GHz<br>Roaming (IAPP) support based on IEEE 802.11f (can't roam across subnets, without re-authentication)<br>Advanced Orthogonal Frequency Division Multiplexing (OFDM)<br>64/128-bits WEP support, dynamic WEP key exchange included<br>WPA (Wi-Fi Protected Access), WPA-PSK support,<br>IEEE 802.1x security (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP)<br>Mixed WEP & WPA mode (support both 802.1x/WEP & WPA clients)<br>Built-in RADIUS server (MD5 / PEAP, 32 entries)<br>Backup RADIUS server<br>RADIUS client<br>MAC address filtering through WLAN (support 32 entries)<br>Access point and Bridge/Repeater mode (concurrent)<br>WDS (including Bridge/Repeater mode configurable per link individually & support simultaneously)<br>Auto scan for channel with least interference<br>Configurable WLAN adapter output power<br>Intra-BSS traffic blocking |
| Logging/Monitoring | Logs<br>System status monitoring<br>Syslog |
| Other Protocol Support and Standards Compliance | IEEE 802.3 and 802.3u 10Base-T and 100Base-TX physical layer specification<br>IEEE 802.1d Rapid Spanning Tree Protocol<br>IPSec, PPTP and L2TP pass through<br>SIP pass through<br>Transparent bridging for unsupported network layer protocols<br>DHCP Client/Relay<br>SNMP v1 and v2c with MIB II support (RFC 1213) |

**Table 75** Environmental Conditions

| | TEMPERATURE RANGE IN DEGREES CELSIUS |
|---|---|
| Operation | +15 ~ +35 |
| Normal | ~ +35 |
| Extreme | ~ +70 |
| Storage | -40 to +80 |

HUMIDITY (non-condensing): 5% to 95% RH (typical)

**Table 76** Inspection Channel (CH1, CH7, CH13)

| | TX/RX FREQUENCY MHZ | 1ST LO FREQUENCY MHZ | 2ND LO FREQUENCY MHZ |
|---|---|---|---|
| CH1 | 2412 | 2038 | |
| CH7 | 2442 | 2068 | |
| CH13 | 2472 | 2098 | |
| VCO | | | 748 |
| IF | | | 374 |

# Hardware Specifications

**Table 77** Hardware Specifications

| | |
|---|---|
| Ethernet Interface | One MIL-C-5015 style Ethernet port |
| Ethernet Interface (Power Injector) | Two RJ-45 Ethernet ports |
| Console Port | One MIL-C-5015 style RS-232 console port |
| WLAN Adapters | Two embedded IEEE 802.11g wireless LAN cards |
| Antenna Connectors | Three standard-N type (female) jacks |
| Access Protocol | CSMA/CA |
| Roaming | IAPP compliant (based on IEEE 802.11f) |
| Radio Data Rate | 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and 1 Mbps, Auto Fall-Back |
| Regulatory & Safety Certifications | FCC Part 15, Class BR&TTE Directive 1999/5/ECEN 300 328-2EN 301 489-1EN 301 489-17EN 60950IP68 |
| Compatibility | Fully interoperable with IEEE802.11g and IEEE802.11b compliant products |
| Power Supply (for the Power Injector) | Input 100 ~ 240 VAC, 2 A, 50/60 Hz. Output 800 mA at -48 VDC |

**Table 77** Hardware Specifications (continued)

| | |
|---|---|
| Dimensions | 246(L) x 202(D) x 73(H) mm |
| Weight | ZyAIR G-5100 without accessories, 2.6 kg |

# Radio Specifications

**Table 78** Radio Specifications

| FREQUENCY BAND | 2.4 ~ 2.4835 (GHZ) |
|---|---|
| **RADIO TYPE** | Direct Sequence Spread Spectrum (DSSS) |
| **MODULATION TYPE** | (Mbps) |
| CCK | 11, 5.5 |
| DQPSK | 2 |
| DBPSK | 1 |
| **OPERATION CHANNELS** | (CH) |
| North American (FCC) | 11 |
| European Community (ETSI) | 13 |
| **RF OUTPUT POWER** | (measured in dBm) |
| FCC (Excluding antenna gain) | 18 ± 2 |
| ETSI (Excluding antenna gain) | 14 |
| **BAND EDGE** | (dBc) |
| **FCC** | >30 |
| **ETSI** | >30 |

**Table 79** Rx Sensitivity (@ FER = 0.08)

| MBPS/<br>MODULATION | 54<br>OFDM | 48<br>OFDM | 36<br>OFDM | 18<br>OFDM | 12<br>OFDM | 9<br>OFDM | 6<br>OFDM | 11<br>CCK | 5.5<br>CCK | 2<br>QPSK | 1<br>QPSK |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FCC (dBm) | -68 | -68 | -75 | -82 | -84 | -87 | -88 | -82 | -85 | -86 | -89 |
| ETSI (dBm) | -68 | -68 | -75 | -82 | -84 | -87 | -88 | -82 | -85 | -86 | -89 |

# System Test

**Table 80** Transmitting System

| PARAMETER | TEST CONDITION | SPECIFICATION | TEMP. DEG. C. |
|---|---|---|---|
| Tx Power | Modulation: OFDM Data Rate: 54 Mbps | FCC: 18 dBm ± 2 dB | 25-20 ~ +70 |
| | | ETSI: 14 dBm ± 1 dB | 25-20 ~ +70 |
| Spectrum Mask | ±11MHz ~ 22MHz±22MHz ~ 33MHz | < -30 dBr< -45 dBr | -20 ~ +70 |
| Frequency Error | Modulation: Carrier Only | ± 60 KHz± 120 KHz | 25-20 ~ +70 |
| Power Ramp On | Tx power on 90% of Pmax | 3 us | -20 ~ +70 |
| Power Ramp Off | Tx power off 10% of Pmax | 3 us | -20 ~ +70 |
| Carrier Suppression | Modulation: Carrier Suppression | 20 dBr | -20 ~ +70 |
| Spurious Emission | 1 GHz ~ 16 GHz | -41 dBm | 25 |

**Table 81** Receiving System

| PARAMETER | TEST CONDITION | SPECIFICATION | TEMP. DEG. C. |
|---|---|---|---|
| Rx Sensitivity (FER) | FER 8% | Pin  -85 dBmPin  -83 dBm | 25-20 ~ +70 |
| Rx Sensitivity (Throughput) | THP 3 Mbps | Pin  -83 dBmPin  -80 dBm | 25-20 ~ +70 |
| RSSI | Pin -80 dBm | 16 (CR62) | 25 |
| Adjacent Channel Rejection | Carrier  -80 dBmTHP   3 Mbps | 35 dB | 25 |
| Spurious Emission | 1 GHz ~ 16 GHz | -46 dBm | 25 |

**Table 82** Current Consumption

| PARAMETER | TEST CONDITION | SPECIFICATION | TEMP. DEG. C. |
|---|---|---|---|
| Tx Current | Tx continue | 150 mA (-48V) | 25 |
| Rx Current | Rx continue | 80 mA (-48V) | 25 |
| Standby Current | Standby | 50 mA (-48V) | 25 |

**Figure 118** Inspection Cosmetic and Function

| TEST ITEM | TEST | CONDITION | CRITERIA |
|---|---|---|---|
| High Temperature Operation | Temp.<br>Storage<br>Test<br>Spec. | +70 Deg. C<br>24 hours<br>Operation mode in the chamber<br>The same as +25 Deg. C | No Damage In Cosmetics or Error In Function |
| Low Temperature Operation | Temp.<br>Storage<br>Test<br>Spec. | -20 Deg. C<br>24 hours<br>Operation mode in the chamber<br>The same as +25 Deg. C | No Damage In Cosmetics or Error In Function |
| High Temperature Storage | Temp.<br>Storage<br>Test<br>Spec. | +80 Deg. C2<br>4 hours<br>Operation mode in room temperature 4 hours after the storage<br>The same as +25 Deg. C | No Damage In Cosmetics or Error In Function |
| Low Temperature Storage | Temp.<br>Storage<br>Test:<br>Spec. | -40 Deg. C<br>24 hours<br>Operation mode in room temperature 4 hours after the storage<br>The same as +25 Deg. C | No Damage In Cosmetics or Error In Function |
| High Temperature High Humidity | Temp.<br>Humidity<br>Storage Test<br>Spec. | +40 Deg. C<br>95%RH (non-condensing) 72 hours<br>Operation mode in room temperature 4 hours after the storage<br>The same as +25 Deg. C | No Damage In Cosmetics or Error In Function |
| Temperature Recycle | Temp. Cycle<br>Test | +20->0->-20->0->+20->40->+60->+40->+20<br>Operation in the chamber 1 hour after arriving at the test temperature | No Damage On Electrical or Error In Function |
| ESD | Discharge By Air<br>Discharge By Contact | ±15KV (Each polarity 10 times)<br>±8KV (Each polarity 10 times) | No Damage On Electrical Performance |

# Approvals

**Table 83** Approvals

| | | |
|---|---|---|
| **SAFETY** | North America | ANSI/UL-1950 3rdCSA C22.2 No. 950 3rd |
| | European Union (CE mark) | EN60950 (1992+A1+A2+A3+A4+A11)IEC 60950 3rd |

**Table 83** Approvals

| | | |
|---|---|---|
| **EMI** | North America | FCC Part 15 Class B |
| | European Union (CE mark) | EN55022 Class BEN61000-3-2EN61000-3-3 |
| **EMS** | European Union (CE mark) | |
| **ELECTROSTATIC DISCHARGE** | | EN61000-4-2 |
| **RADIO-FREQUENCY ELECTROMAGNETIC FIELD** | | EN61000-4-3 |
| **EFT/BURST** | | EN61000-4-4 |
| **SURGE** | | EN61000-4-5 |
| **CONDUCTED SUSCEPTIBILITY** | | EN61000-4-6 |
| **POWER MAGNETIC** | | EN61000-4-8 |
| **VOLTAGE DIPS/ INTERRUPTION** | | EN61000-4-11 |
| **EM FIELD FROM DIGITAL TELEPHONES** | | ENV50204 |
| **LAN COMPATIBILITY** | | SmartBit |
| **FOR WIRELESS PC CARD** | | FCC Part15C, Sec15.247 |
| | | ETS300 328ETS300 826 |
| | | CE mark |

# APPENDIX B
# Packaging Specifications

**Table 84** Packaging Specifications

| ITEMS | SPECIFICATION/DESCRIPTION | QUANTITY |
|---|---|---|
| Inline Power Injector (PoE) | Input 100 ~ 240 VAC, 2 A, 50/60 Hz. Output 800 mA at -48 VDC | 1 |
| Wall-plug AC Power Cord | (1.8 m) | 1 |
| RS232 Console Cable | MIL-C-5015 STP (2.0 m) | 1 |
| Uplink Ethernet Cable | MIL-C-5015 UTP (1.8 m) | 1 |
| Grounding Cable | UL1015 (3.0m) | 1 |
| RJ45 Ethernet Cable | MIL-C-5015 STP (30.0 m) | 1 |
| Waterproofing Strip | 15 cm | 3 |
| Antennas | 5dBi omni-direction rubber antenna | 2 |
| Antenna Cable | LMR-400 (1 m) | 1 |
| Mounting Brackets | Wall mount brackets<br>Mast mount brackets | 1 pair<br>1 pair |
| Installation Tool | Wrench | 1 |
| CD-ROM | Quick Start Guide and User's Guide | 1 |

Table 85 Mounting Hardware Specifications

| ITEM | QUANTITY |
|---|---|
| U Bolt, 1/4-20" (1/4" diameter with 20 threads per inch) | 2 |
| Screw, M6*12(ISO), HEX Head (6 mm diameter and 12 mm long) | 4 |
| eNut, HEX, 1/4-20" (1/4" internal diameter with 20 threads per inch) | 4 |
| Washer | 8 |
| Split Lock Washer | 8 |
| Anchor Bolt | 4 |
| Mast Mounting Bracket | 2 |
| Wall Mounting Bracket | 2 |

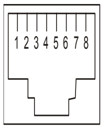
# APPENDIX C
# Power over Ethernet Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

**Table 86** Power over Ethernet Injector Specifications

| | |
|---|---|
| Power Output | 15.4 Watts maximum |
| Power Current | 400 mA maximum |

**Table 87** Power over Ethernet Injector RJ-45 Port Pin Assignments

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

# APPENDIX D
# Setting up Your Computer's IP Address

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

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

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

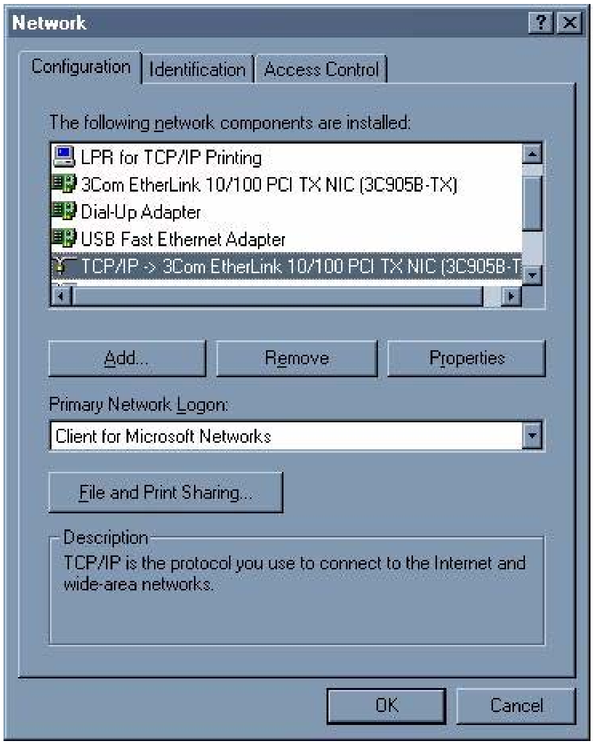
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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

## Windows 95/98/Me

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

**Figure 119** WIndows 95/98/Me: Network: Configuration



The following network components are installed:

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

Primary Network Logon: Client for Microsoft Networks

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

## Installing Components

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

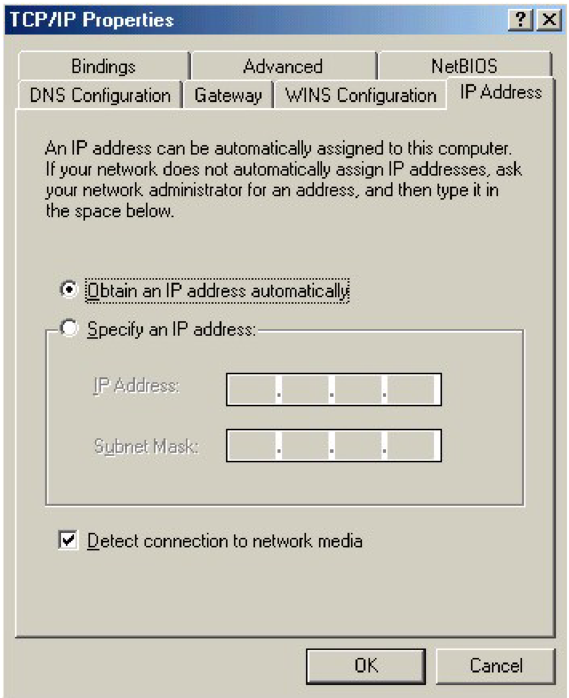
## Configuring

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

**2** Click the **IP Address** tab.

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

**Figure 120** Windows 95/98/Me: TCP/IP Properties: IP Address



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

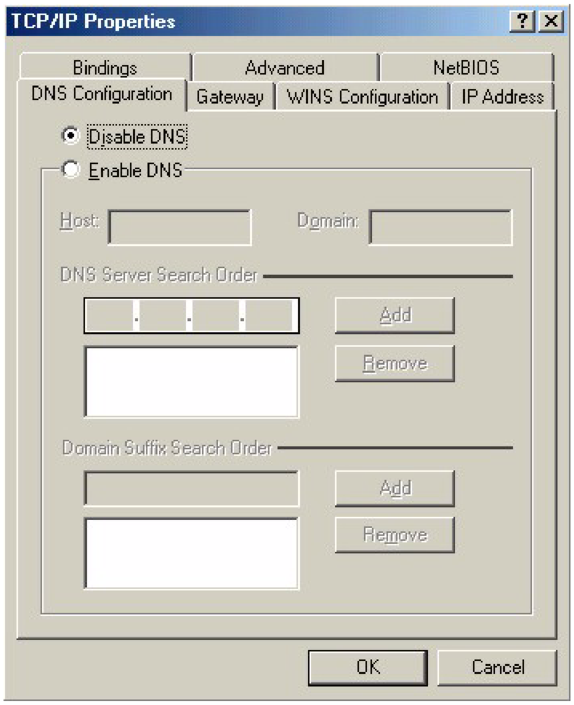
Subnet Mask: . . .

☑ Detect connection to network media

**3** Click the **DNS** Configuration tab.

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

**Figure 121** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

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

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

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

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

## Verifying Settings

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

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

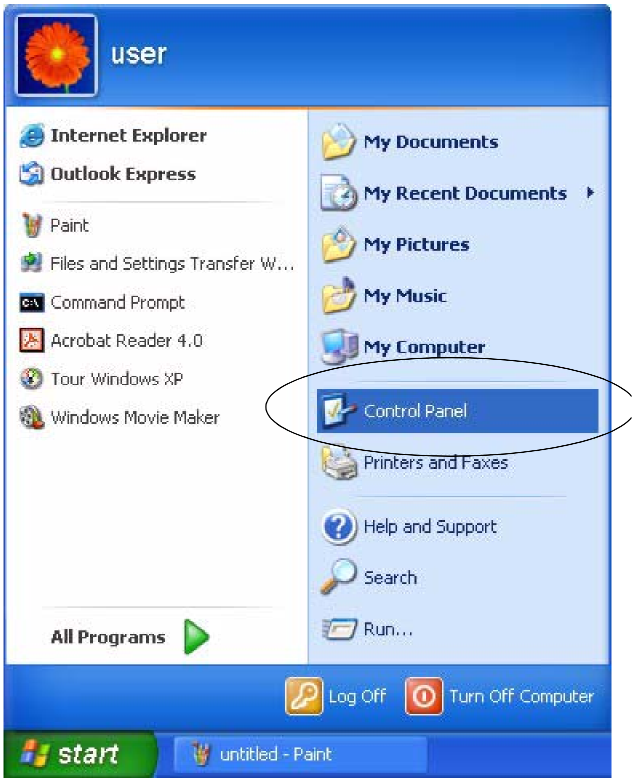
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

# Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

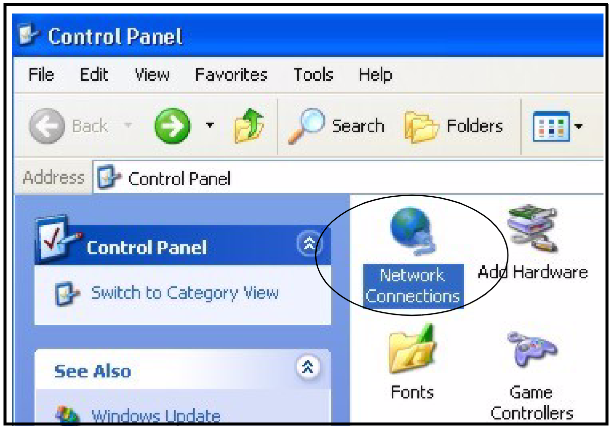
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 122** Windows XP: Start Menu



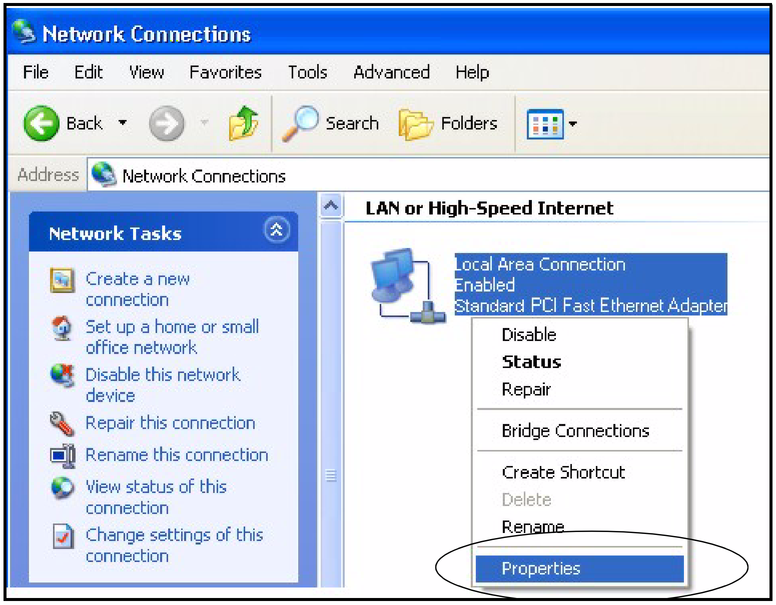
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 123** Windows XP: Control Panel



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

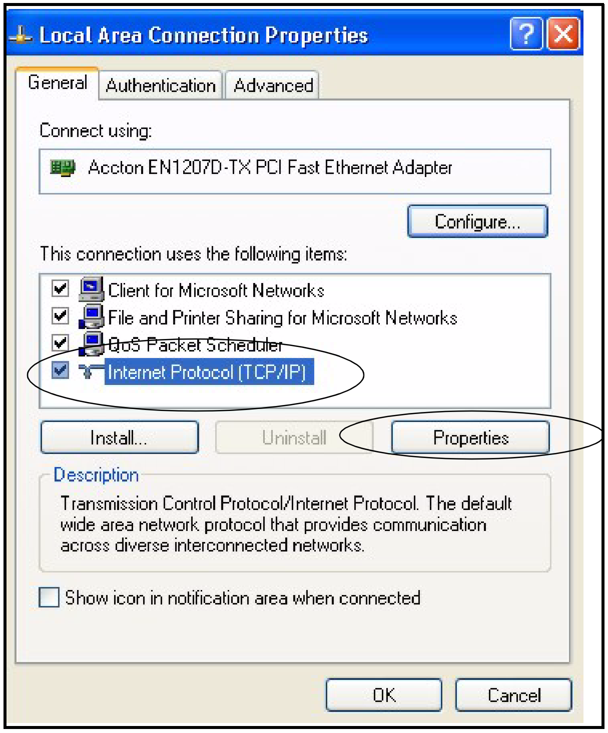
**Figure 124** Windows XP: Control Panel: Network Connections: Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

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

**Figure 125** Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

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

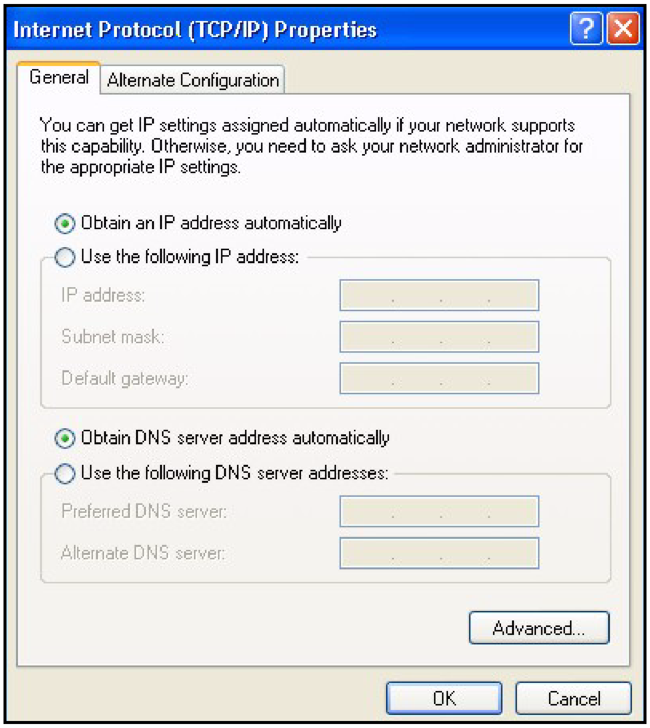
☐ Show icon in notification area when connected

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

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

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

**Figure 126** Windows XP: 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: . . .

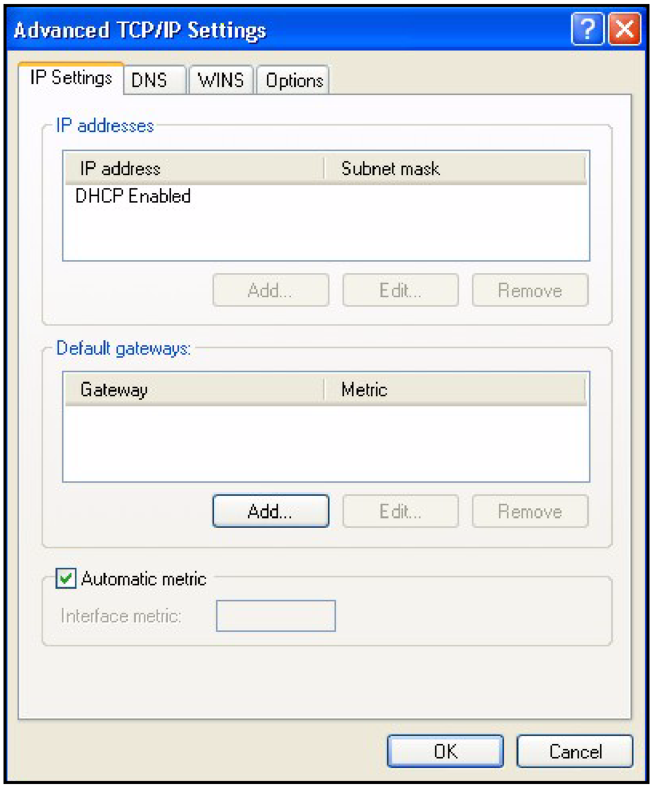
Alternate DNS server: . . .

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

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

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

**Figure 127** Windows XP: Advanced TCP/IP Properties



DHCP Enabled

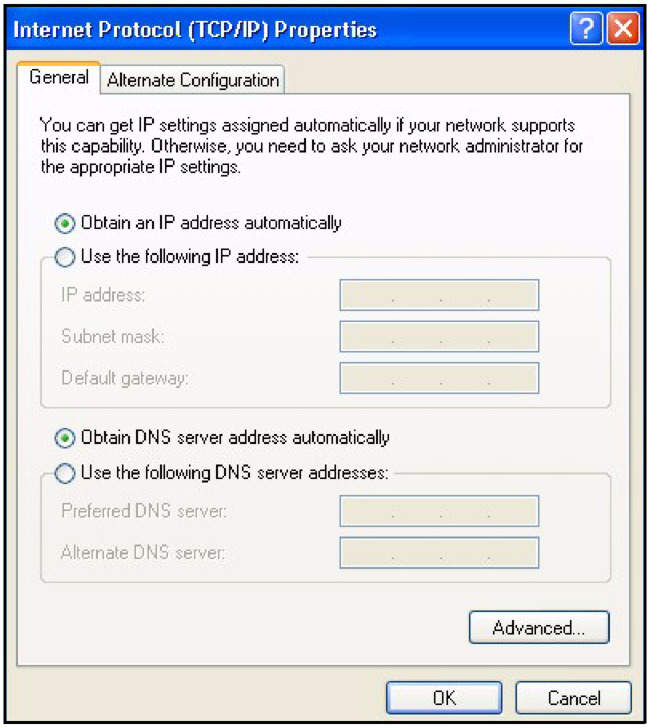
☑ Automatic metric

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

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

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

**Figure 128** Windows XP: Internet Protocol (TCP/IP) Properties



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:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

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

**9** Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

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

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

## Verifying Settings

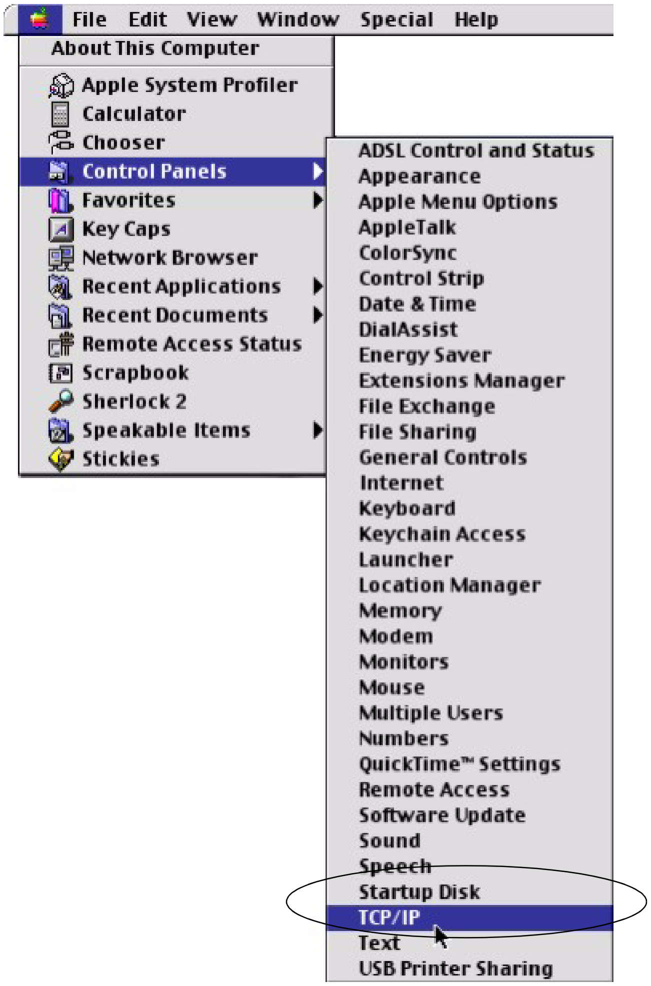
**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

# Macintosh OS 8/9

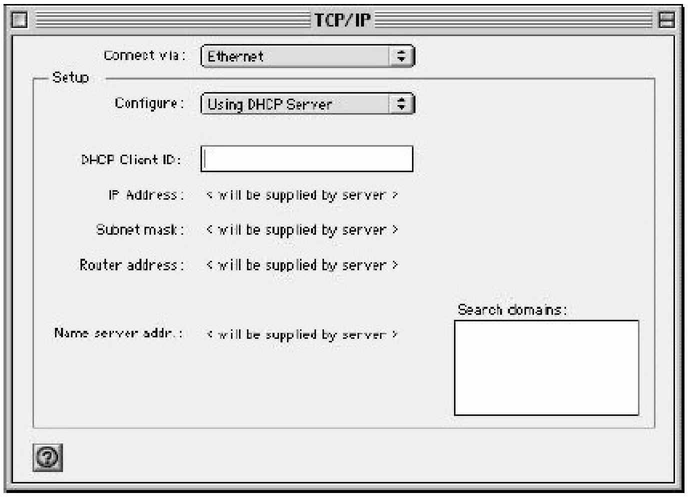
**1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 129** Macintosh OS 8/9: Apple Menu



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

**Figure 130** Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

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

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

4 For statically assigned settings, do the following:

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

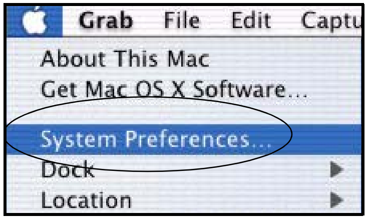
## Verifying Settings

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

# Macintosh OS X

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

**Figure 131** Macintosh OS X: Apple Menu

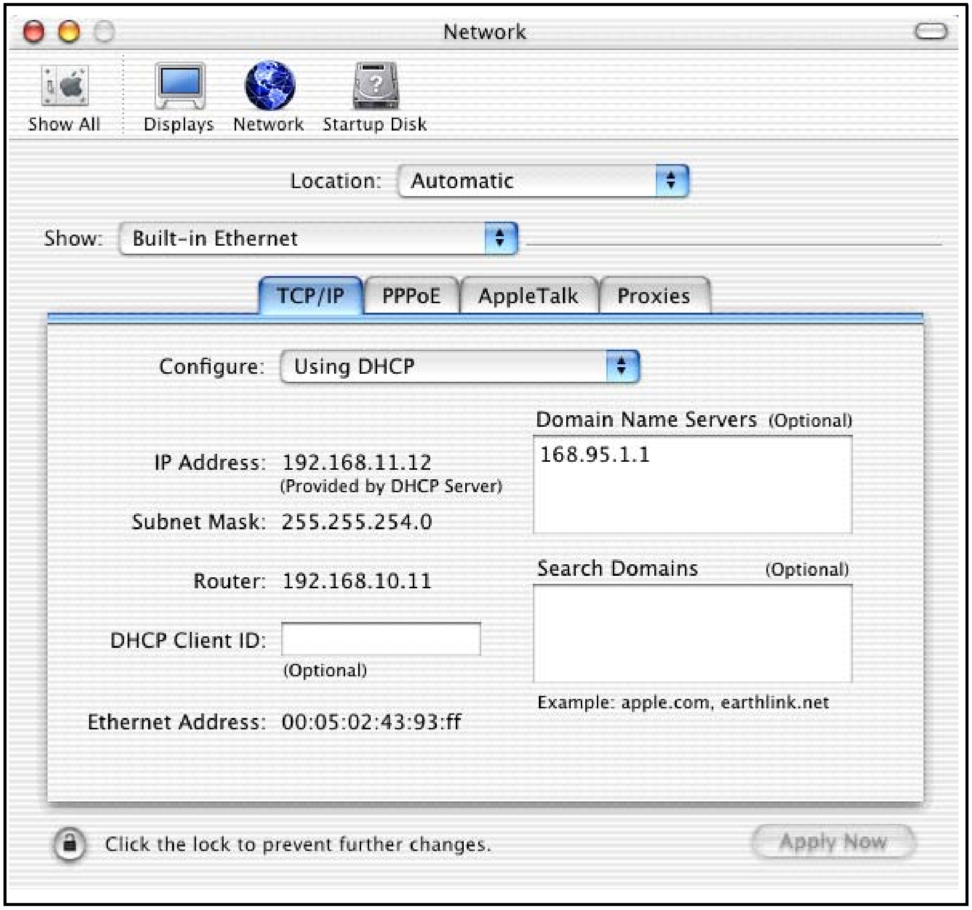


2 Click **Network** in the icon bar.

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

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

Figure 132 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

Domain Name Servers (Optional)

168.95.1.1

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

Search Domains (Optional)

DHCP Client ID:
(Optional)

Example: apple.com, earthlink.net

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

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 Settings

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

# Appendix E
# 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.)

**Table 88** 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 |

**Note:** 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.

**Table 89** 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  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.

**Table 90** "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.

**Table 91** 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.

**Table 92** Two Subnets Example

| | 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.

**Note:** 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.

**Table 93** 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 | |

**Table 94** 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).

**Table 95** 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 | |

**Table 96** 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 | |

**Table 97** Subnet 3

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

**Table 98** 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:<br>192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address:<br>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.

**Table 99** 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 | 225 | 254 | 255 |

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

**Table 100** 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 Table 88 on page 213) available for subnetting.

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

**Table 101** 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 |
| 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 F Wireless LAN

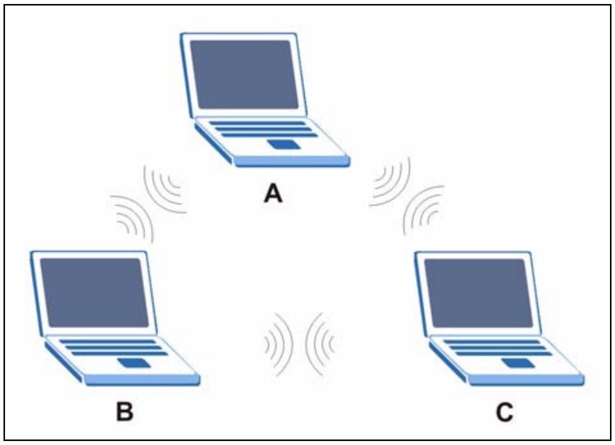
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). 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). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 133** Peer-to-Peer Communication in an Ad-hoc Network

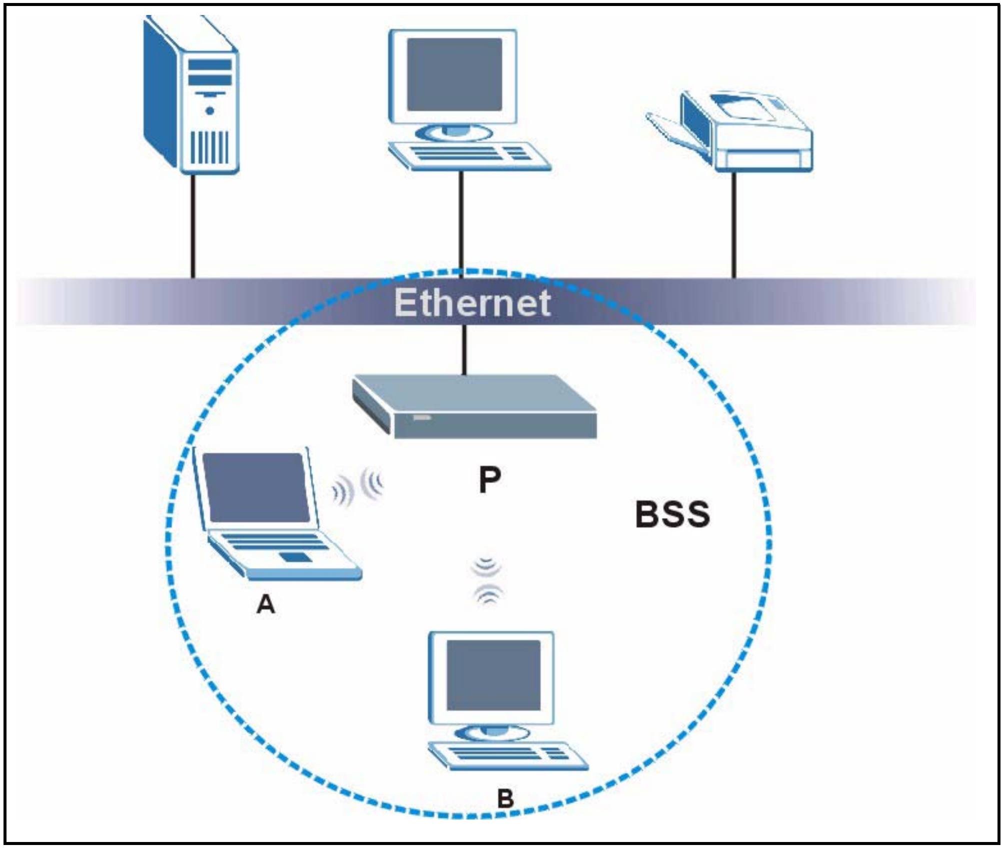


### BSS

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

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

**Figure 134** Basic Service Set



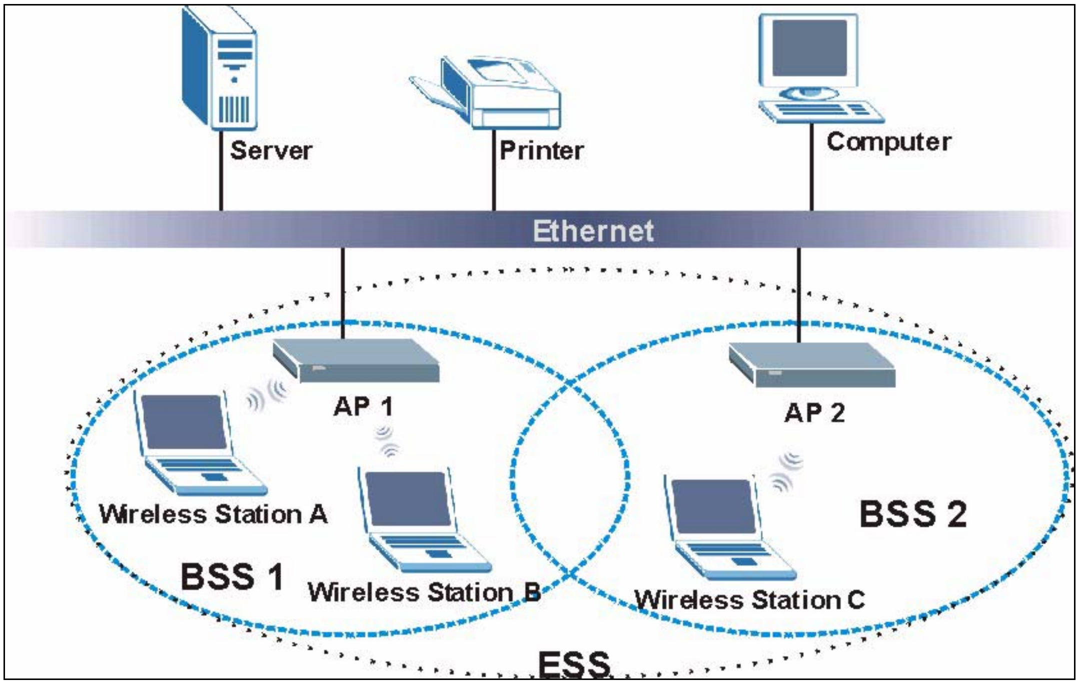
## ESS

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).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

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 135** Infrastructure WLAN



## Channel

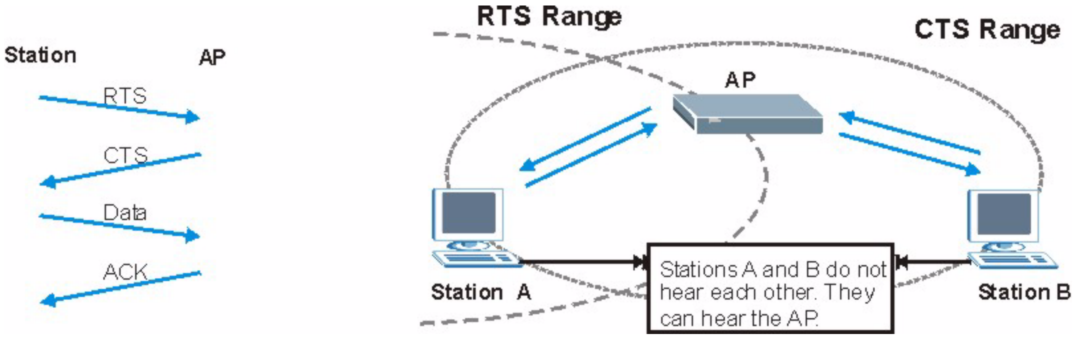
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs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

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

## 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 136** RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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

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

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

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

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

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

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

# 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 AP 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.

# Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a ‘noisy’ network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in ‘noisy’ networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

**Note:** The AP and the wireless stations MUST use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

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

**Table 102** IEEE802.11g

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 1 | DBPSK (Differential Binary Phase Shift Keyed) |
| 2 | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11 | CCK (Complementary Code Keying) |
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing) |

# 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. Some advantages of IEEE 802.1x are:

- 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

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

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP 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 network from unauthorized access.

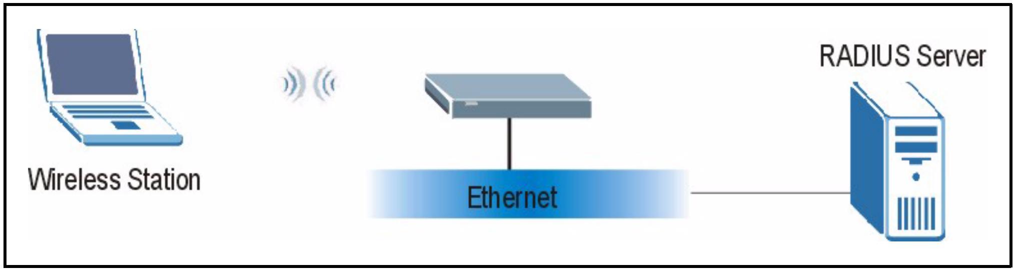
# EAP Authentication

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

**Figure 137** 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.

1. The wireless station sends a "start" message to the device.
2. The device sends a "request identity" message to the wireless station for identity information.

3 The wireless station replies with identity information, including username and password.

4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## Types of  Authentication

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

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

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

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

### EAP-TLS (Transport Layer Security)

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

### EAP-TTLS (Tunneled Transport Layer Service)

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

### PEAP (Protected EAP)

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

### LEAP

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

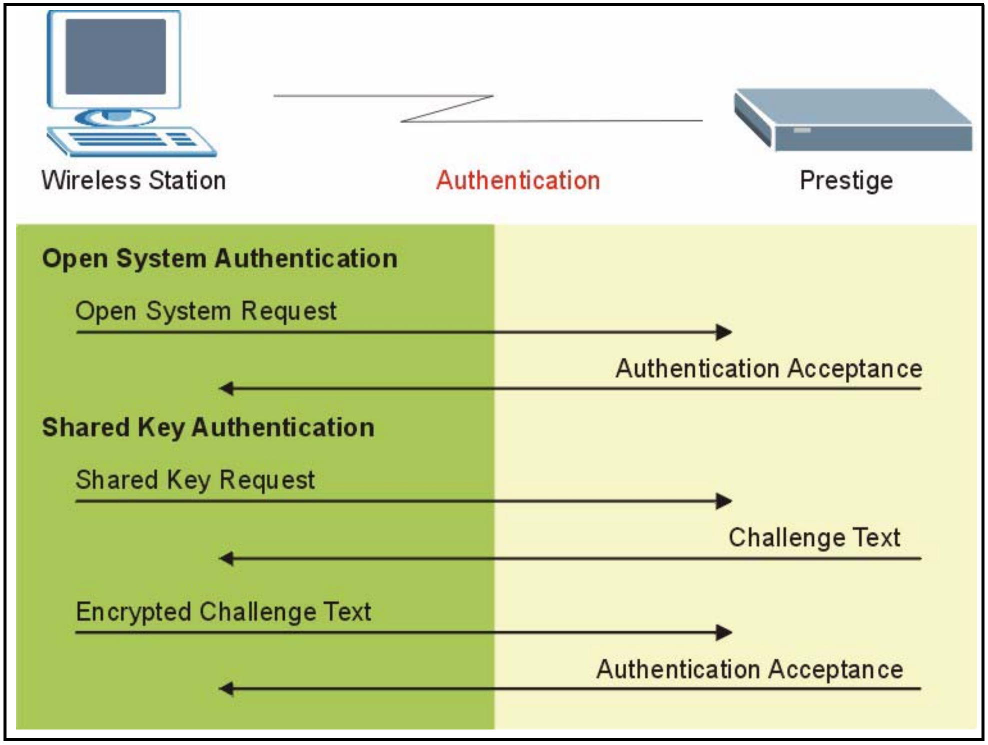
### WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

## WEP Authentication Steps

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 138** 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 device 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 device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

## Dynamic WEP Key Exchange

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

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

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

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

**Table 103** Comparison of EAP Authentication Types

| | EAP-MD5 | EAP-TLS | EAP-TTLS | PEAP | LEAP |
|---|---|---|---|---|---|
| Mutual Authentication | No | Yes | Yes | Yes | Yes |
| Certificate – Client | No | Yes | Optional | Optional | No |
| Certificate – Server | No | Yes | Yes | Yes | No |
| Dynamic Key Exchange | No | Yes | Yes | Yes | Yes |
| Credential Integrity | None | Strong | Strong | Strong | Moderate |
| Deployment Difficulty | Easy | Hard | Moderate | Moderate | Moderate |
| Client Identity Protection | No | No | Yes | Yes | No |

# WPA

## User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

## Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

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

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

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

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

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

## Security Parameters Summary

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

**Table 104** Wireless Security Relational Matrix

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

## Roaming

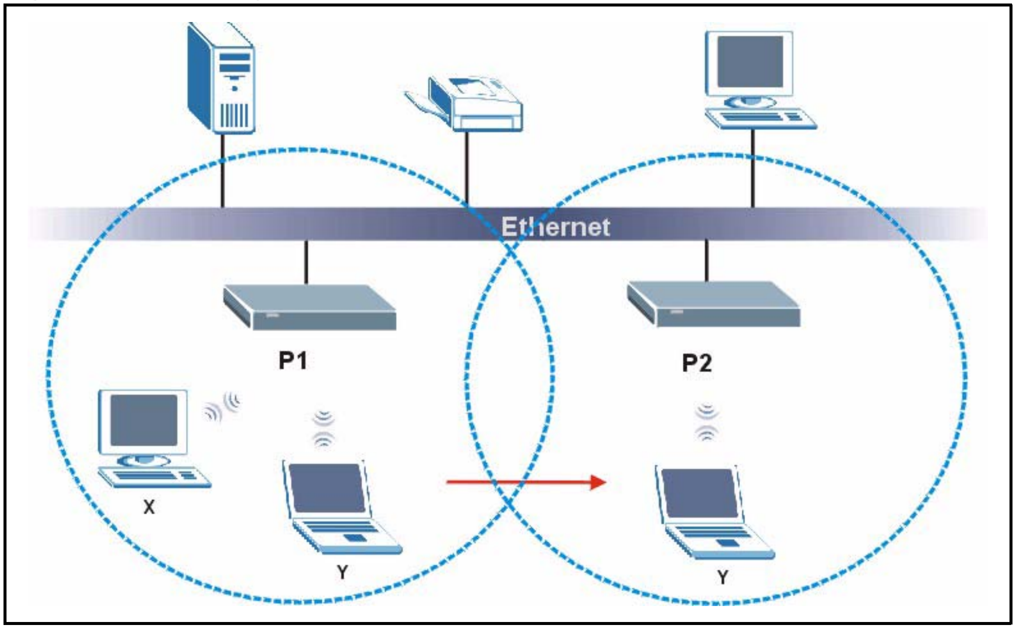
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access 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 139.

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.

**Figure 139** Roaming Example



The steps below describe the roaming process.

1. As wireless station **Y** moves from the coverage area of access point **P1** to that of access point
2. **P2**, it scans and uses the signal of access point **P2**.
3. Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
4. Access point **P1** updates the new position of wireless station.
5. Wireless station **Y** sends a request to access point **P2** for re-authentication.

## 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.

# Appendix G
# Outdoor Site Planning

This appendix provides information on site planning requirements for the installation of your outdoor wireless device.

## Introduction

The installation of a wireless network requires some additional planning over a wired network. This planning includes RF (Radio Frequency) path planning, site preparation, and installation of outdoor components such as outdoor units, antennas, lightning protection devices, and cabling suitable for outdoor conditions. Furthermore, you also need to investigate the zoning laws as well as Federal Communications Commission (FCC) and European Telecommunications Standards Institute (ETSI) regulations.

## General Considerations

A basic consideration is the physical location outdoor wireless device. Because microwave signals travel in a straight line, a clear line of sight between antennas is ideal. Frequently, however, the locations of the desired links are fixed. When a clear line of sight cannot be achieved, you have to plan accordingly.

Other general site considerations include:

- Is there a structure already in place on which you can mount the outdoor wireless device or would you be required to construct one, for example, a mast for the sole purpose of mounting the outdoor wireless device?
- Would there be permit requirements for this?
- Possibility of future obstructions
    - If trees grow too high will they interfere with the signal?
    - Are there plans to erect buildings between the sites, which may inadvertently obstruct the signal path?
- Availability of grounding, good grounding is important in all areas of the world, but in areas prone to lightning, it is especially critical.
- Whether or not strong RF interference exists in the neighborhood, within or adjacent to the operating frequency.

# Specific Considerations

The following information will help you determine site characteristics that are most applicable to your outdoor wireless device and the actions that should be taken.

## Weather

It is important to research any unusual weather conditions that are common to the site location. These conditions include extreme

- Rainfall
- Fog
- Wind
- Temperature Ranges.

If extreme conditions exist that may affect the integrity of the radio link, the effects of these conditions should be considered early in the planning process.

## Rainfall

Except in extreme conditions, attenuation (weakening of the signal) due to rain does not present a serious problem for frequencies up to the range of 6 to 8 GHz. When microwave frequencies are at 11 GHz and above, attenuation due to rain becomes more of a concern, especially in areas where rainfall is of high density and long duration. If this is the case, shorter paths may be required.

## Fog

In most cases, the effects of fog are considered to be much the same as rain.

However, fog can adversely affect the radio link when it is accompanied by atmospheric conditions such as temperature inversion, or very still air accompanied by stratification.

- Temperature inversions and stratification can cause ducting, which may increase the potential for interference between systems that do not normally interfere with each other.
- Stratification along with still air can cause severe refractive or reflective conditions with unpredictable results.

Where either temperature inversion or stratification exists, shorter paths and adequate clearances are recommended.

## Wind

Any system components mounted outdoors will be subject to the effects of wind. It is important to know the direction and velocity of the wind common to the site. The mounting structure must be able to withstand these forces as well as protect against damage to the outdoor wireless device components.

Antenna designs react differently to wind forces, depending on the location. This is known as wind loading. Most antenna manufacturers will specify wind loading for each type of antenna manufactured.

## Temperature Ranges

Temperature can adversely affect the radio link when phenomena such as temperature inversion or very still air accompanied by stratification occur

See the section on *Fog* for further detail.

## Lightning

The potential for lightning damage to radio equipment should always be considered when planning a wireless link. There are a variety of lightning protection and grounding devices, whether located inside or outside the site, which could potentially be damaged by a lightning strike.

Lightning protection requirements are based on the level of site exposure, the cost in the event of a link downtime, local building codes and electrical codes. If the link is critical and the site is in an active lightning area, attention to thorough lightning protection and grounding is critical.

## Lightning Protection

To provide adequate lightning protection,

- Install antennas in locations that are unlikely to receive direct lightning strikes.
- Install lightning rods to protect antennas from direct strikes.
- Make sure that cables and equipment are properly grounded to provide low-impedance paths for lightning currents.
- Install surge suppressors on telephone lines and power lines.

## Interference

An important part of planning a site for your outdoor wireless device is the avoidance of interference.

Effects within the system or outside the system can cause interference. Good planning for frequencies and antennas can overcome most interference challenges.

Co-Channel and Adjacent Channel Interference

Co-channel interference results when another RF link is using the same channel frequency.

Adjacent-channel interference results when another RF link is using an adjacent channel frequency.

A spectrum analyzer can be used to determine if there is any strong signals present at the site and determine how close they are to the desired frequency. The further away from your proposed frequency, the less likely they are to cause a problem.

Antenna placement and polarization, is the most effective method of reducing this type of interference.

## Antennas

Antennas play a key role in reducing the potential for interference. They come in a variety of configurations that have different performance characteristics in the areas of gain and direction. Antennas that transmit/receive in all directions are known as omni-directional, while those that transmit/receive in one specific direction are categorized as directional.

Antennas are tuned to operate on a specific group of frequencies. The manufacturer also fixes other specific attributes such as beam width and gain. Antennas should be selected and placed according to your site and your application.

## 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 does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Antenna Polarization

The orientation of the antenna will change the orientation of the signal. The transmitting and receiving antennas should be both polarized either horizontally or vertically. Adjacent antennas on different frequencies can be cross-polarized to help reduce interference between the two, if your operating license permits this.

## Towers

When planning antenna placement, it might be necessary to build a freestanding tower for the antenna. Regulations and limitations define the height and location of these towers with respect to airports, runways, and airplane approach paths. The Federal Aviation Administration (FAA) controls these regulations. In some circumstances, the FAA, the FCC, or both, must approve the tower installations.

To ensure compliance, review the current FCC regulations regarding antenna structures. These regulations (along with examples) can be viewed on the FCC web site at http://www.fcc.gov/antenna.

## Path Planning

To get the most value from a wireless system, path planning is essential. In addition to the fact that radio signals dissipate as they travel, many other factors operate on a microwave signal as it moves through space. All of these must be taken into account, to avoid attenuation of the signal by path obstruction.

## Calculating a Link Budget

A link budget is a rough calculation of all known elements of the link, to determine if the signal will have the proper strength when it reaches the other end of the link.

To make this calculation, consider the following information.

- A signal degrades as it moves through space. The longer the path, the more loss it experiences. This free-space path loss is a factor in calculating the link viability. Free-space path loss is easily calculated for miles or kilometers.
- Availability represents the quality of a link. It is the ratio of the time that the link is available to the total time. This serves as a guide to the service that you can expect, on average, over a period of one year.

## Availability

Your application determines what availability is required. A critical application where downtime adversely affects business and revenue requires a high percentage of availability. Somewhat lower availability might be acceptable by an application used to gather data, where occasional outages can be tolerated.

Availability is largely a function of fade margins and the amount of signal fading. Paths obstructed by trees have larger fades than paths with no trees. Longer paths tend to have more fading than shorter paths. Larger fade margins yield better link availability.

The International Telecommunications Union (ITU) publishes a reference for link planning, which is available at http://www.itu.ch/.

ITU Recommendation G.826 contains definitions for "availability" and related terms used to describe link quality. It also contains recommendations for link quality objectives.

ITU Recommendation P.530 contains information on how to plan for high reliability in clear, line-of-sight links.

Availability is much more difficult to predict for non-line-of-sight links. It is best determined by field measurements.

## Unlicensed Frequencies (U-NII)

The FCC has identified the frequencies from 5.725 to 5.825 GHz as Unlicensed National Information Infrastructure (U-NII). This band can be used by anyone without having to obtain a license. However, you must use radio equipment that is "type approved" by the FCC for use within the specific band. If you are installing a U-NII band link between two buildings, across a parking lot, or across town, you will find that this type of system is much simpler to implement than licensed systems. By using very directional antennas in the installation, you are not likely to experience interference.

# APPENDIX H
# Outdoor Installation Recommendations

This appendix provides information on site requirements for the installation of your outdoor wireless device See the Quick Start Guide for more information on site installation.

## Mounting

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.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

A wall (side) mount allows for mounting an antenna (mast) on the side of a building or on the side of an elevated penthouse. This will provide a convenient mounting location when the roof overhang is not excessive and/or the location is high enough to provide a clear line of sight.

In most situations mounting an antenna directly to the wall will not allow you to properly align the antenna with the corresponding antenna at the opposite end of your wireless link. As poor alignment will typically result in poor performance, you are advised to always mount the outdoor wireless device to a mast.

### Antenna Mast/Antenna Requirements

To accommodate the outdoor wireless device, the mast must satisfy the following requirements:

- The construction of the mast must be of a sturdy, weatherproof and non-corrosive material, for example, galvanized or stainless steel construction pipe.
- The diameter of the mast may vary, see the *Hardware Specifications* for details.
- The height of the antenna mast must be sufficient to allow the antenna to be installed at least 1.5 m (5’) above the peak of roof. If the roof is metal, then the height of the antenna should be a minimum of 3m (10’) above the roof.
- The mast or wall-bracket must be free from any substance that may prevent a good electrical connection with the antenna, for example, paint.

## Grounding

A safe grounding system is necessary to protect your outdoor installation from lightning strikes and the build-up of static electricity.

Direct grounding of the antenna mast and outdoor wireless device. The outdoor wireless device should be connected to the same grounding system as the antenna mast and the AC wall outlet.

The grounding system must comply with the National Electrical Code and safety standards that apply in your country. Always check with a qualified electrician if you are in doubt as to whether your outdoor installation is properly grounded.

# Lightning Protection

All outdoor electronic equipment is susceptible to lightning damage. Proper grounding to national and local codes is instrumental in providing human safety. Lightning Protection is used when a customer wants to maximize the reliability of the electronic system by diverting the excess energy that can be induced on any transmission lines (data, power) though a series of surge protection devices. The energy is dissipated through heat and is also diverted to the ground.

## Additional Protection

Lightning, even with the built-in protection, can still damage the outdoor wireless device. This can occur for any number of reasons, such as an improperly grounded installation or if the amount of transient energy from nearby lightning exceeds what the device can handle.

If the outdoor wireless device fails due to damage from lightning, the link is out-of-service until the unit is replaced or repaired. An external, reverting protection device can provide a higher level of protection, and greater probability of surviving lightning strikes without damage to the outdoor wireless device.

## Antenna Alignment

For optimal performance of your wireless link, make sure that the antennas are properly aligned (facing one another "eye-to-eye"). To align the antennas:

- Use a pair of binoculars and/or a map of the area and compass to point the antennas to one another.
- Optimize antenna alignment if required, by making small modifications in the antenna orientation.
- Alternatively, consult a professional Antenna Installation Service to optimize the antenna alignment.

Omni-directional antennas are characterized by a wide radiation pattern. Therefore alignment of this type of antennas is less critical than for directional antennas.

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.

# APPENDIX I
# 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.

**Note:** 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 J
# Brute-Force Password Guessing Protection

Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix I on page 245 for information on the command structure.

**Table 105** 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. The brute-force password guessing protection is turned off by default. |
| 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.

# APPENDIX K
# Log Descriptions

This appendix provides descriptions of example log messages.

**Table 106** 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. |
| `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. |

**Table 107** 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 |
| | 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 |

**Table 107** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| | 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 |

**Table 108** 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

**Table 109** Log Categories and Available Settings

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

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

## Displaying Logs

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

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

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

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

# Log Command Example

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

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

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

# Index