ZyAIR

Wireless Gateway Series

User's Guide

Version 3.50

May 2004

ZyXEL

Unleash Networking Power

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Notice 1

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

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

Certifications

1. Go to www.zyxel.com
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

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

ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2. Do not use this product near water, for example, in a wet basement or near a swimming pool.

3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

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

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

METHOD	SUPPORT E-MAIL	TELEPHONE[1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX[1]	FTP SITE	
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase from the ZyAIR Wireless Gateway series.

A wireless gateway is an access point and router rolled into one. It is a cost-effect solution to share Internet access with multiple computers and expand your wired network.

Some features are not available in every model. Refer to the *Model Specific Features* table in Chapter 1 of this user's guide to see what features are specific to your ZyAIR model.

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

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

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

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.
- Quick Installation Guide

  Our Quick Installation Guide is designed to help you get up and running right away. It contains information on the configuration of key features and hardware connections and installation.
- ZyXEL Web Site

  The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- "Enter" means for you to type one or more characters (and press the carriage return). "Select" or "Choose" means for you to use one predefined choices.
- Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The ZyAIR Wireless Gateway series may be referred to simply as the ZyAIR in the user’s guide.

User Guide Feedback

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

Part I:

OVERVIEW

This part introduces the main features and applications of the ZyAIR and shows how to access the web configurator and use the Wizard to configure for Internet Access.

Chapter 1
Getting to Know Your ZyAIR

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

1.1 Introducing the ZyAIR Wireless Gateway Series

The ZyAIR Wireless Gateway provides wireless connectivity. As an Internet gateway, your ZyAIR can share an Internet connection (through a cable or xDSL modem) with multiple computers using SUA/NAT and DHCP. The ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption and MAC address filtering.

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

1.2 ZyAIR Features

The following sections describe the features of the ZyAIR Wireless Gateway series. Features vary by ZyAIR model. This table lists the difference between models; it does not include features that are common to all of the ZyAIR models.

Some features are not available in every model. Refer to the *Model Specific Features* table to see what features are specific to your ZyAIR model. These features are defined at the time of writing.

Table 1-1 Model Specific Features

ZYAIR MODEL FEATURES	B-2000	B-2000 V.2
Configurable Output Power	O	O
Two 2dBi Antennas	Detachable	Detachable
GUI Enable/Disable Capability of ZyAIR WLAN LED ON/OFF		O
Content Filtering		O
Limitation of Client Connections		O
Real-time WLAN status graphical display		O

Table 1-1 Model Specific Features

ZYAIR MODEL FEATURES	B-2000	B-2000 V.2
SPI/DoS prevention Firewall, including ACL		O
SSL Passthrough	O	O
Wi-Fi Protected Access (WPA)		O
Table Key: An "O" in a model's column shows that the model has the specified feature. A number specific to an individual model may alternately be displayed. The information in this table was correct at the time of writing, although it may be subject to change.		

4-Port Switch

A combination of switch and router makes your ZyAIR a cost-effective and viable network solution. You can connect up to four computers to the LAN ports on you ZyAIR without the cost of a hub.

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

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

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

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

10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router.

Reset Button

The ZyAIR reset button is built into the side panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP sever enabled with a pool of 32 IP addresses starting at 192.168.1.33.

Brute-Force Password Guessing Protection

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

ZyAIR LED

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

802.11b Wireless LAN Standard

ZyAIR products containing the letter "B" in the model name, such as ZyAIR B-2000, ZyAIR B-2000 v.2, comply with the 802.11b wireless standard.

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

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

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

Output Power Management

Power Management is the ability to set the level of output power.

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

Limit the number of Client Connections

You may set a maximum number of wireless stations that may connect to the ZyAIR. This may be necessary if for example, there is difficulty with channel assignment due to a high density of APs within a coverage area.

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.

Wi-Fi Protected Access

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

Firewall

The ZyAIR employs a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyAIR firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

IEEE 802.1x Network Security

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

Wireless LAN MAC Address Filtering

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

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyAIR and other UPnP-enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service.

PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyAIR is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. Use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translations of multiple IP addresses used within one network to different IP addresses known within another network.

NAT for Single-IP-address Internet Access

The ZyAIR's SUA (Single User Account) feature allows multiple-user Internet access for the cost of a single IP account. NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealPlayer, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyAIR also acts as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236). The ZyAIR supports versions 1 and 2.

IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet LAN interface with the ZyAIR itself as the gateway for each LAN network.

IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator.

SNMP

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

Full Network Management

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

Logging and Tracing

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

Diagnostics Capabilities

The ZyAIR can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- DRAM
- LAN port
- Wireless port

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

1.3 Application for the ZyAIR

Here is an application example of what you can do with your ZyAIR.

1.3.1 Internet Access Application

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

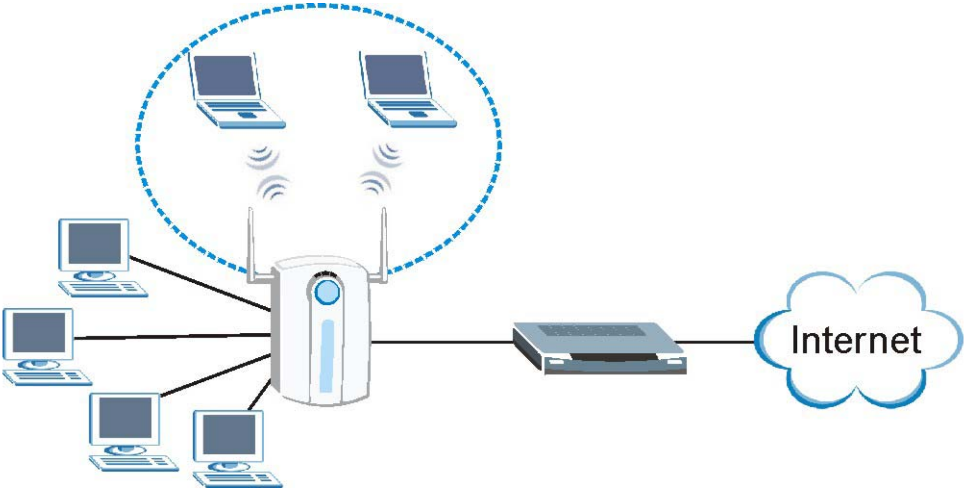


Figure 1-1 Internet Access Application Example

Chapter 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator makes it easy to configure and manage the ZyAIR. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual ZyAIR models or firmware versions.

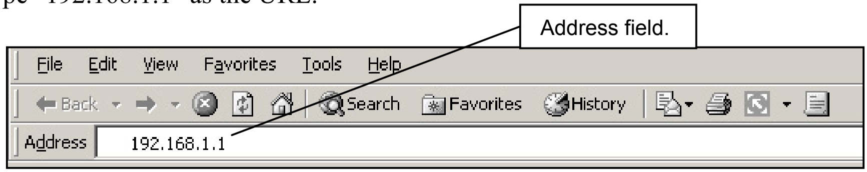
2.2 Accessing the ZyAIR Web Configurator

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

Step 2. Prepare your computer to connect to the ZyAIR (refer to the *Setting Up Your Computer's IP Address* appendix).

Step 3. Launch your web browser.

Step 4. Type "192.168.1.1" as the URL.

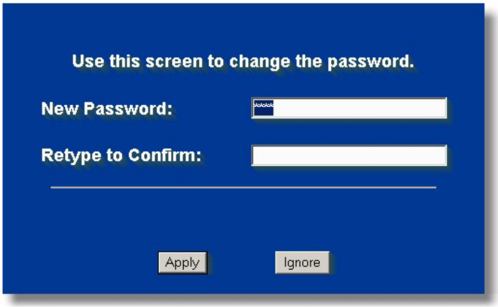


192.168.1.1

Figure 2-1 Web Browser Address Field

Step 5. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

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



Use this screen to change the password.

New Password: ****

Retype to Confirm:

Figure 2-2 Change Password Screen

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

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

2.3 Resetting the ZyAIR

If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file or use the **RESET** button on the side panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to "1234", also.

2.3.1 Procedure to Use the Reset Button

Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

Step 1. Press the **RESET** button for more than five seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyAIR restarts. Otherwise, go to step 2.

Step 2. Turn the ZyAIR off.

Step 3. While pressing the **RESET** button, turn the ZyAIR on.

Step 4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the ZyAIR is now restarting.

Step 5. Release the **RESET** button and wait for the ZyAIR to finish restarting.

2.3.2 Uploading a Configuration File via Console Port

This method is only applicable to ZyAIR models with a console port, such as the ZyAIR B-2000.

Step 1. Download the default configuration file from the ZyAIR FTP site, unzip it and save it in a folder.

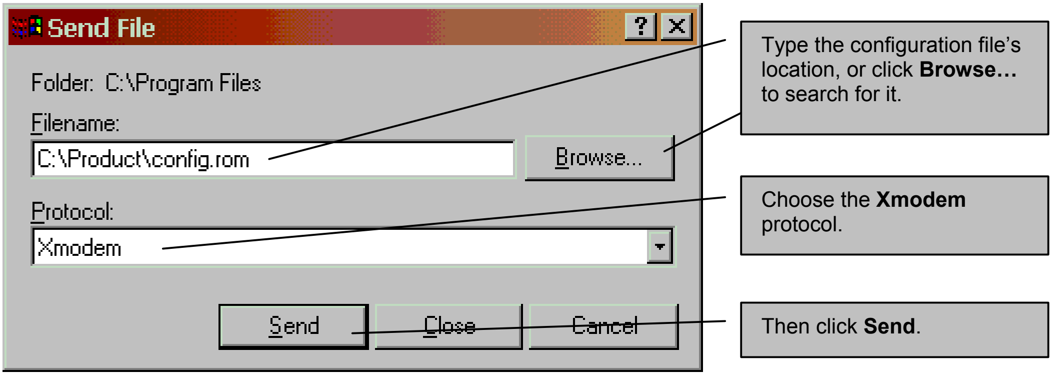
Step 2. Turn off the ZyAIR, begin a terminal emulation software session and turn on the ZyAIR again. When you see the message "Press any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

Step 3. Enter "y" at the prompt below to go into debug mode.

Step 4. Enter "atlc" after "Enter Debug Mode" message.

Step 5. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

Step 6. Click **Transfer**, then **Send File** to display the following screen.



Send File

Folder: C:\Program Files

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**.

Figure 2-3 Example Xmodem Upload

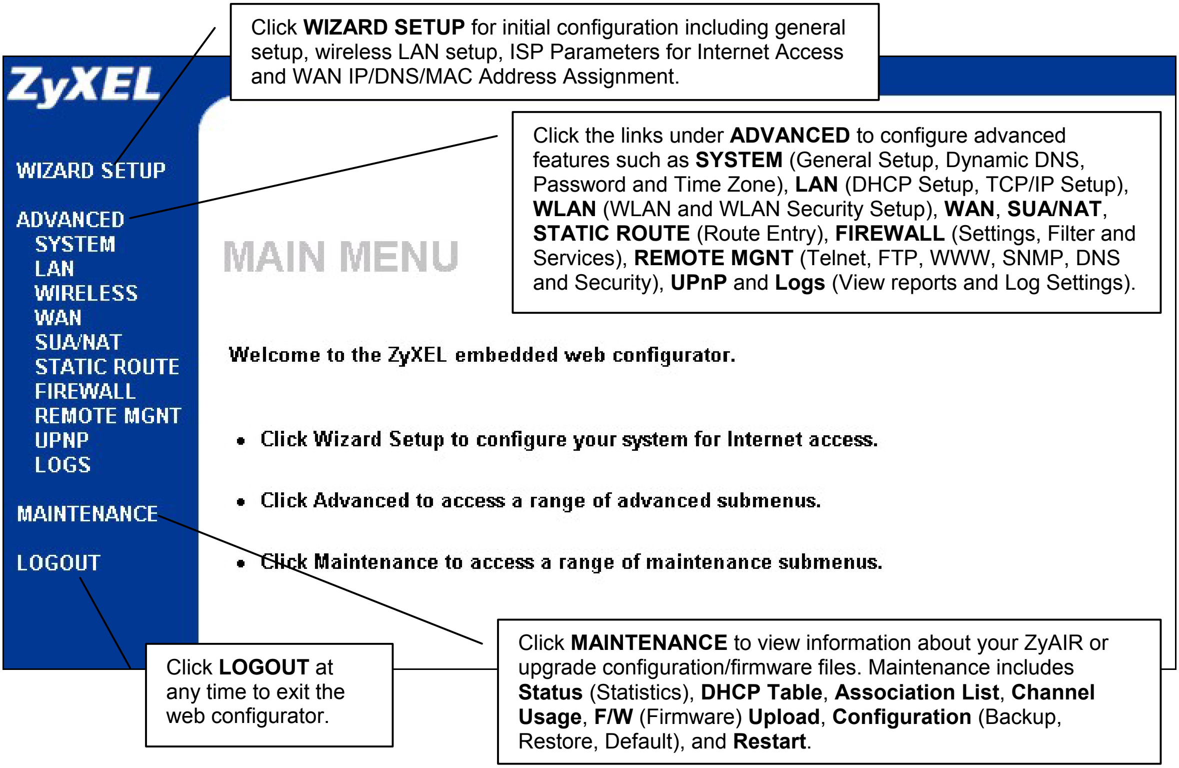
Step 7. After successful firmware upload, enter "atgo" to restart the ZyAIR.

2.4 Navigating the ZyAIR Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen. We use the ZyAIR B-2000v.2 web configurator in this guide as an example. The screen for your model may vary slightly for different ZyAIR models.

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.



Welcome to the ZyXEL embedded web configurator.

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

Click **WIZARD SETUP** for initial configuration including general setup, wireless LAN setup, ISP Parameters for Internet Access and WAN IP/DNS/MAC Address Assignment.

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Dynamic DNS, Password and Time Zone), **LAN** (DHCP Setup, TCP/IP Setup), **WLAN** (WLAN and WLAN Security Setup), **WAN**, **SUA/NAT**, **STATIC ROUTE** (Route Entry), **FIREWALL** (Settings, Filter and Services), **REMOTE MGNT** (Telnet, FTP, WWW, SNMP, DNS and Security), **UPnP** and **Logs** (View reports and Log Settings).

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

Click **MAINTENANCE** to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes **Status** (Statistics), **DHCP Table**, **Association List**, **Channel Usage**, **F/W** (Firmware) **Upload**, **Configuration** (Backup, Restore, Default), and **Restart**.

Figure 2-4 The MAIN MENU Screen of 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 Internet access and set up wireless LAN.

3.1.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel 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.

The ZyAIR's "Scan" function is especially designed to automatically scan for a channel with the least interference.

3.1.2 ESS ID

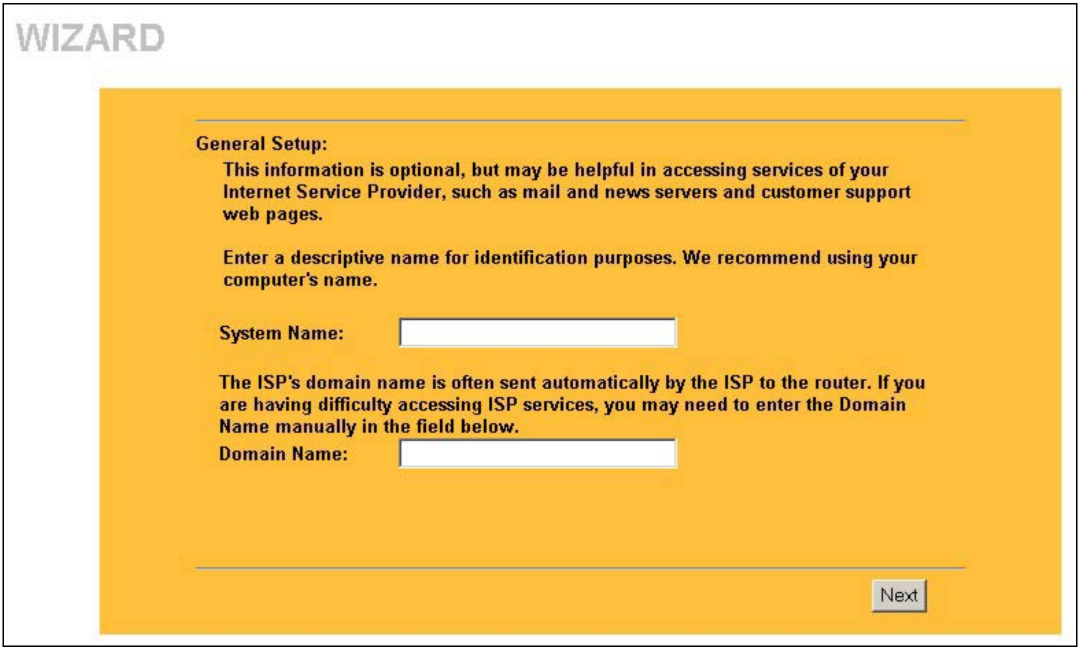
An Extended Service Set (ESS) is a group of access points or wireless gateways connected to a wired LAN on the same subnet. An ESS ID uniquely identifies each set. All access points or wireless gateways and their associated wireless stations in the same set must have the same ESSID.

3.1.3 WEP Encryption

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

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.



General Setup:

This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

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

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

Domain Name:

Figure 3-1 Wizard 1: General Setup

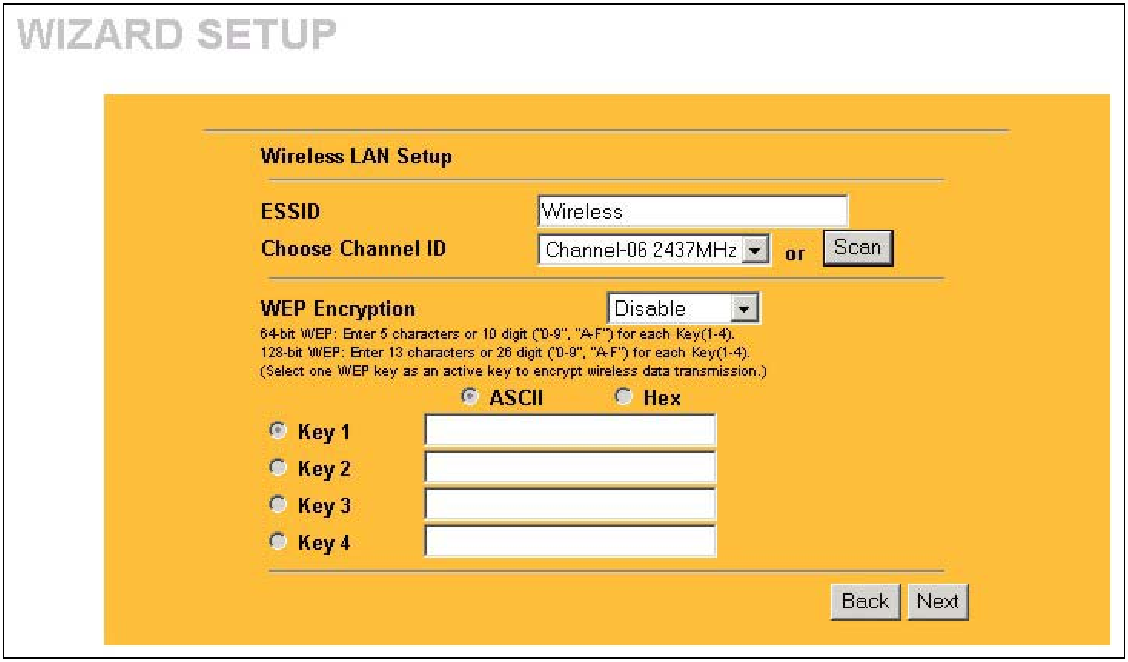
The following table describes the labels in this screen.

Table 3-1 Wizard 1: General Setup

LABEL	DESCRIPTION
System Name	It is recommended you type your computer's "Computer name". 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**, **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**. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Next	Click **Next** to proceed to the next screen.

3.3 Wizard Setup: Wireless LAN Setup

Set up your wireless LAN using the second wizard screen.



WIZARD SETUP

Wireless LAN Setup

ESSID: Wireless

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

Figure 3-2 Wizard 2: Wireless LAN Setup

The following table describes the labels in this screen.

Table 3-2 Wizard 2: Wireless LAN Setup

LABEL	DESCRIPTION
ESSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyAIR, make sure all wireless stations use the same ESSID in order to access the network.
Choose Channel ID	To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Open the **Channel Usage Table** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click **Scan** instead.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.

Table 3-2 Wizard 2: Wireless LAN Setup

LABEL	DESCRIPTION
WEP Encryption	Select **Disable** allows all wireless computers to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
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. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

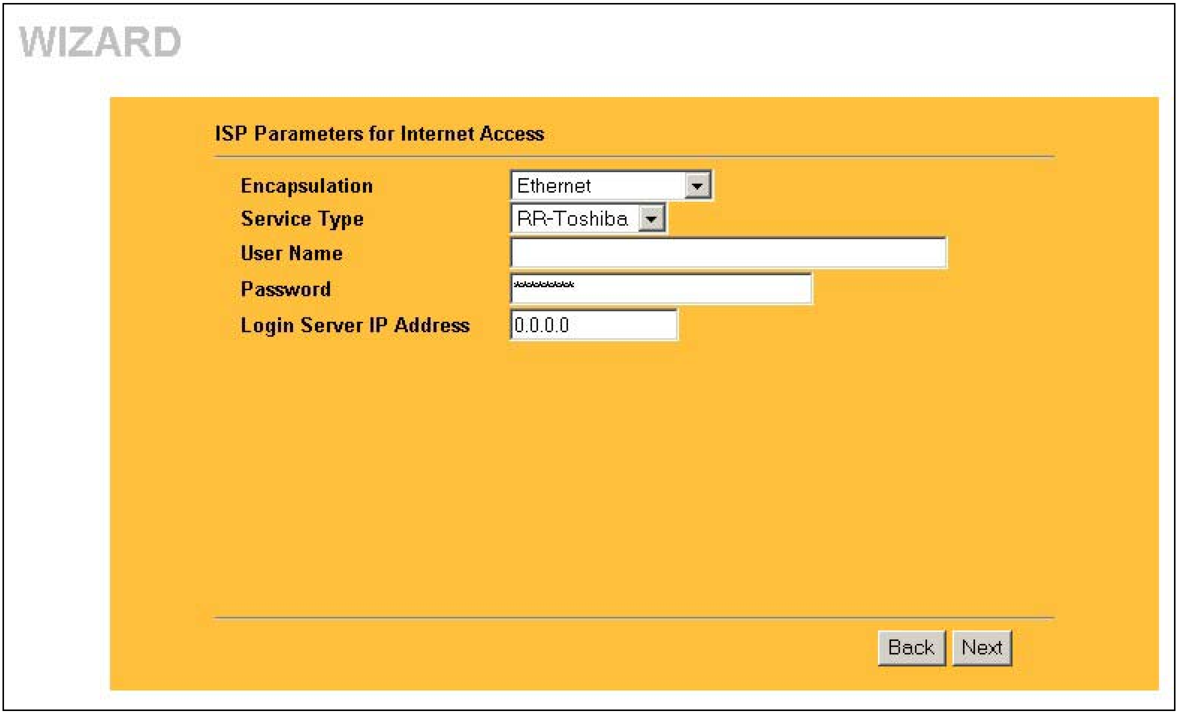
Refer to the chapter on wireless LAN for more information.

3.4 Wizard Setup: ISP Parameters

The ZyAIR offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE.** The screen varies depending upon the type chosen.

3.4.1 Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.



WIZARD

ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	RR-Toshiba
User Name	
Password	********
Login Server IP Address	0.0.0.0

Figure 3-3 Wizard 3: Ethernet Encapsulation

The following table describes the labels in this screen.

Table 3-3 Wizard 3: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
Service Type	Select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose **Standard**. The **User Name**, **Password** and **Login Server IP Address** fields are not applicable (**N/A**) for the **Standard** service type.

Table 3-3 Wizard 3: Ethernet Encapsulation

LABEL	DESCRIPTION
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the username above.
Login Server IP Address	The ZyAIR will find the Roadrunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example "login1.telia.com". This field is not available on all models.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyAIR to wait between logins. This field is not available on all models.
Next	Click **Next** to proceed to the next page.
Back	Click **Back** to go back to the previous page.

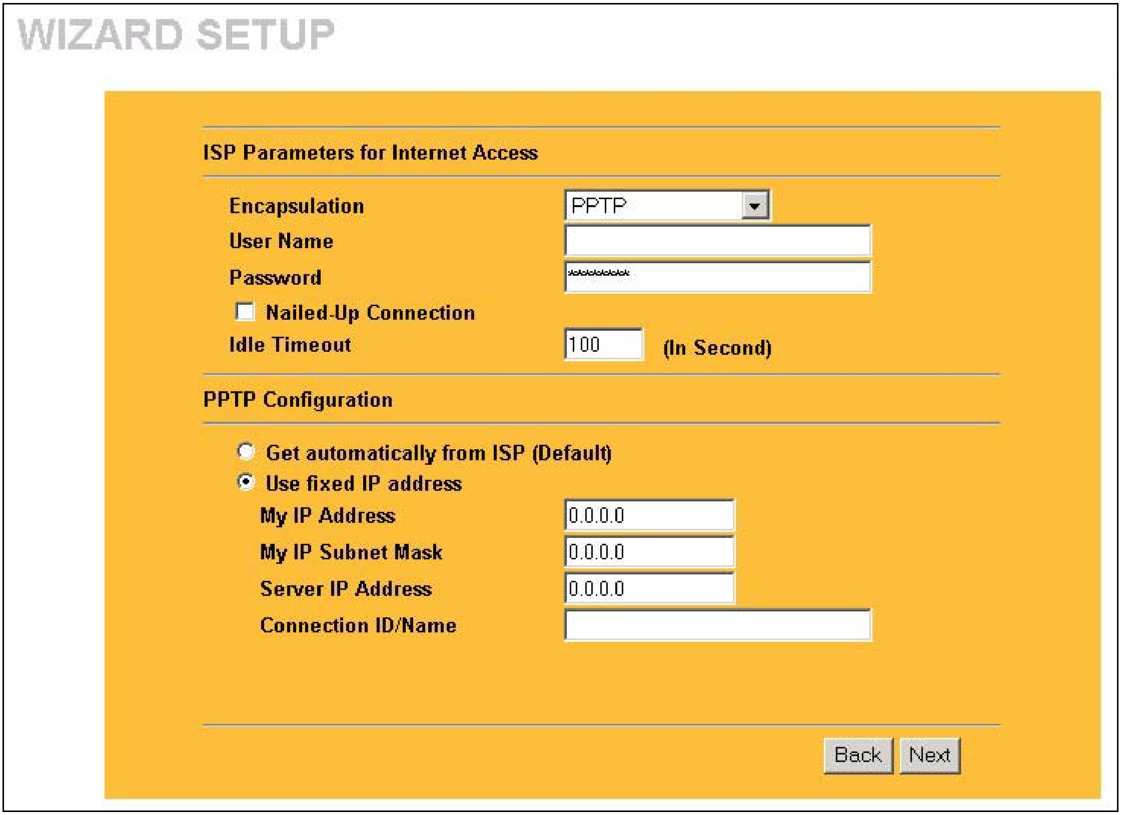
3.4.2 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

The ZyAIR supports one PPTP server connection at any given time.



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: PPTP
User Name:
Password: *********
□ Nailed-Up Connection
Idle Timeout: 100 (In Second)

PPTP Configuration

○ Get automatically from ISP (Default)
● Use fixed IP address
My IP Address: 0.0.0.0
My IP Subnet Mask: 0.0.0.0
Server IP Address: 0.0.0.0
Connection ID/Name:

Figure 3-4 Wizard 3: PPTP Encapsulation

The following table describes the labels in this screen.

Table 3-4 Wizard 3: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.

Table 3-4 Wizard 3: PPTP Encapsulation

LABEL	DESCRIPTION
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the ZyAIR automatically disconnects from the PPTP server.
PPTP Configuration	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP in this field if you selected **Use Fixed IP Address**.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given) in this field if you selected **Use Fixed IP Address**.
Server IP Address	Type the IP address of the PPTP server in this field.
Connection ID/Name	If your ISP has provided a connection ID name, enter it in this field exactly as provided.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.4.3 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

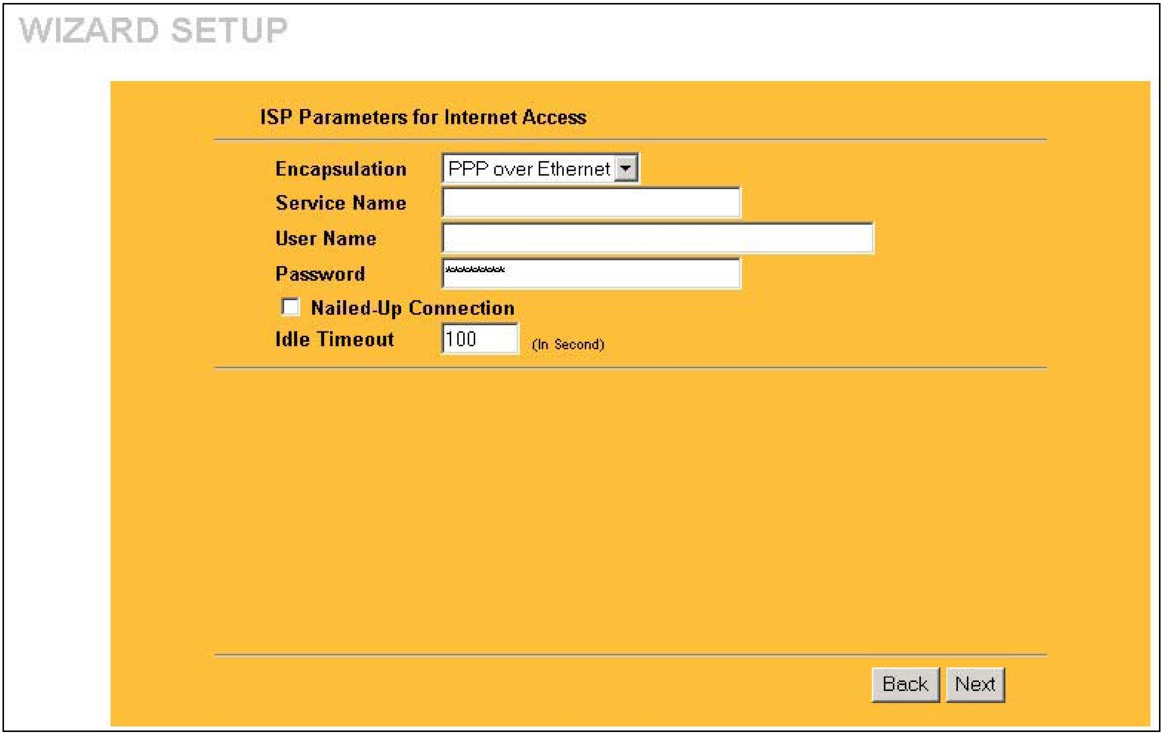
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the ZyAIR (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyAIR does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet
Service Name:
User Name:
Password: ********
□ Nailed-Up Connection
Idle Timeout: 100 (In Second)

Figure 3-5 Wizard 3: PPPoE Encapsulation

The following table describes the labels in this screen.

Table 3-5 Wizard 3: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	

Table 3-5 Wizard 3: PPPoE Encapsulation

LABEL	DESCRIPTION
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the ZyAIR automatically disconnects from the PPPoE server.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.

3.5 Wizard Setup: WAN and DNS

The fourth wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.5.1 WAN IP Address Assignment

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

Table 3-6 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

3.5.2 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. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyAIR. 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, 192.168.1.1, 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.

3.5.3 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.

There are two ways that an ISP disseminates the DNS server addresses.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The ZyAIR acts as a DNS proxy when this field is blank.

3.5.4 WAN MAC Address

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.

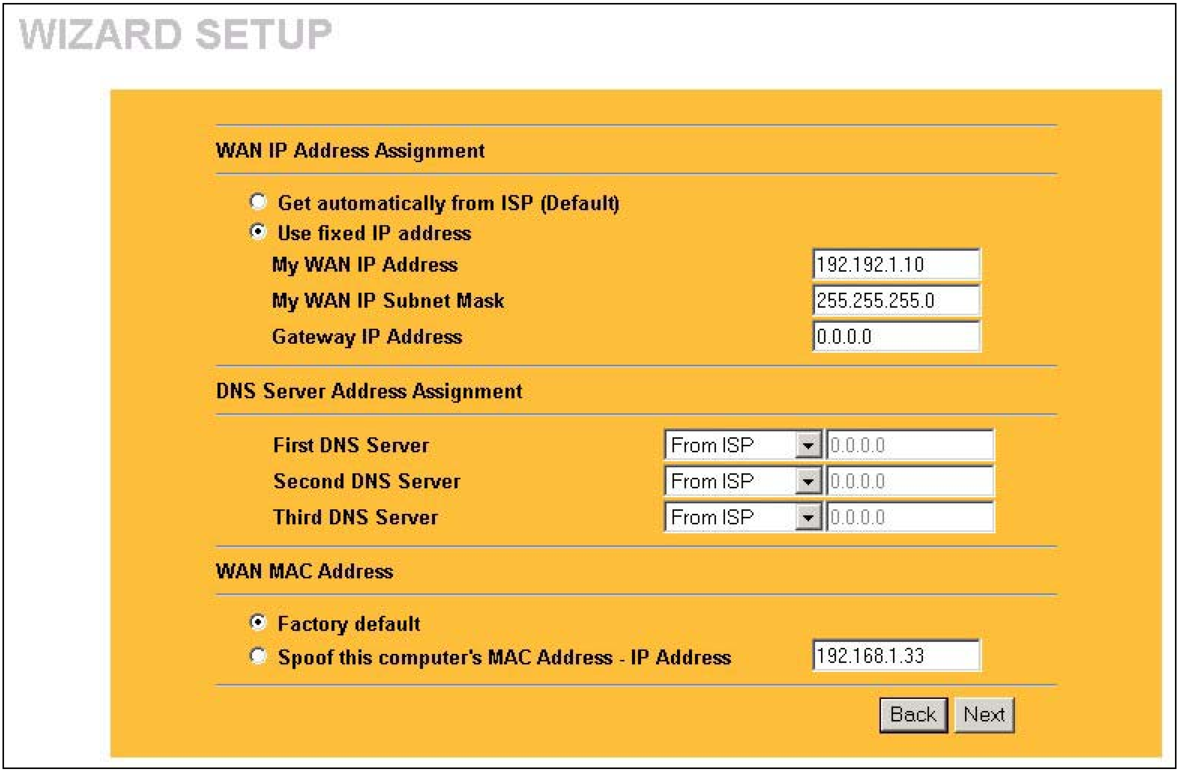
You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a workstation on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

ZyXEL recommends you clone the MAC address from a workstation on your LAN even if your ISP does not require MAC address authentication.

Your ZyAIR WAN port is always set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your ZyAIR supports full duplex mode on the LAN side.

Table 3-7 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyAIR LAN IP)



WIZARD SETUP

WAN IP Address Assignment

○ Get automatically from ISP (Default)

● Use fixed IP address

My WAN IP Address: 192.192.1.10

My WAN IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

DNS Server Address Assignment

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

WAN MAC Address

● Factory default

○ Spoof this computer's MAC Address - IP Address: 192.168.1.33

Figure 3-6 Wizard 4: WAN and DNS

The following table describes the labels in this screen.

Table 3-8 Wizard 4: WAN and DNS

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**

Table 3-8 Wizard 4: WAN and DNS

LABEL	DESCRIPTION
My WAN IP Subnet Mask	Enter the IP subnet mask in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE and PPTP encapsulation in the previous wizard screen.
Gateway/Remote IP Address	Enter the gateway IP address in this field if you selected **Use Fixed IP Address**. This field is not available when you select PPPoE encapsulation in the previous wizard screen.
Remote IP Subnet Mask	Enter the gateway IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. This field is available only when you select PPTP encapsulation in the previous wizard screen.
DNS Server Address Assignment	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Next**. 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 **Next**. 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. These fields are not available on the ZyAIR B-2000.
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default. This field is only available on the ZyAIR B-2000.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address. This field is only available on the ZyAIR B-2000.
Primary/Secondary DNS Server	If you selected the **Use fixed IP address – Primary/Secondary DNS Server** option, enter the provided DNS addresses in these fields. This field is only available on the ZyAIR B-2000.
WAN MAC Address: The MAC address field allows you to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a workstation on your LAN.	
Factory Default	Select this option to use the factory assigned default MAC address.

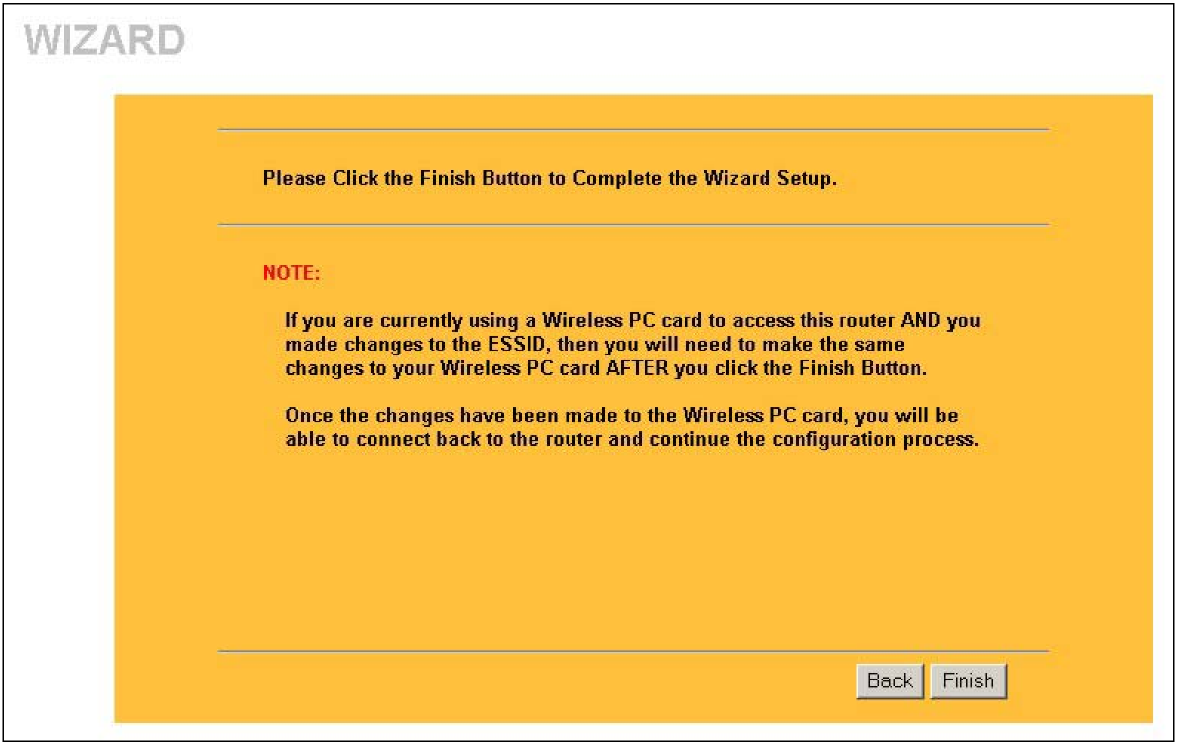
Table 3-8 Wizard 4: WAN and DNS

LABEL	DESCRIPTION
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC address you are cloning. Once it is successfully configured, the MAC address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.6 Basic Setup Complete

Click **Finish** to complete and save the wizard setup.

If you are currently using a wireless (LAN) adapter to access this ZyAIR and you made changes to the ESSID, then you will need to make the same changed to your wireless (LAN) adapter after you click the **Finish** button.



Please Click the Finish Button to Complete the Wizard Setup.

NOTE:

If you are currently using a Wireless PC card to access this router AND you made changes to the ESSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.

Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.

Figure 3-7 Setup Complete

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

Part II:

SYSTEM, LAN AND WIRELESS

This part discusses the System, LAN, and Wireless setup screens.

Chapter 4
System Screens

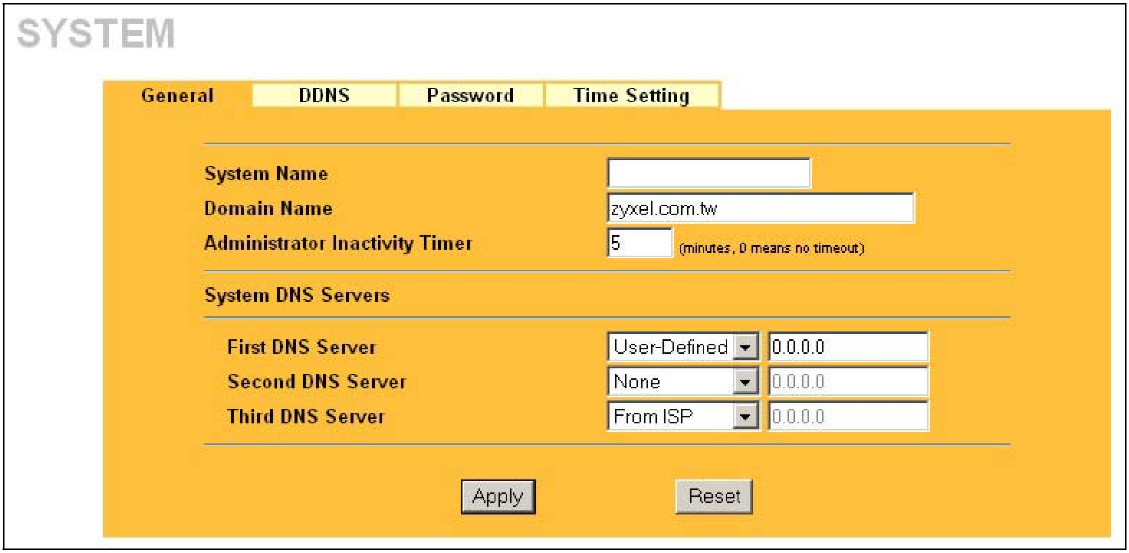
This chapter provides information on the System screens.

4.1 System Overview

This section provides information on general system setup.

4.2 Configuring General Setup

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



SYSTEM

General | DDNS | Password | Time Setting

System Name:

Domain Name: zyxel.com.tw

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

System DNS Servers

First DNS Server: User-Defined 0.0.0.0

Second DNS Server: None 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

Figure 4-1 System General Setup

The following table describes the labels in this screen.

Table 4-1 System General Setup

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

4.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or web site on your own computer using a DNS-like address (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The dynamic DNS service provider will give you a password or key.

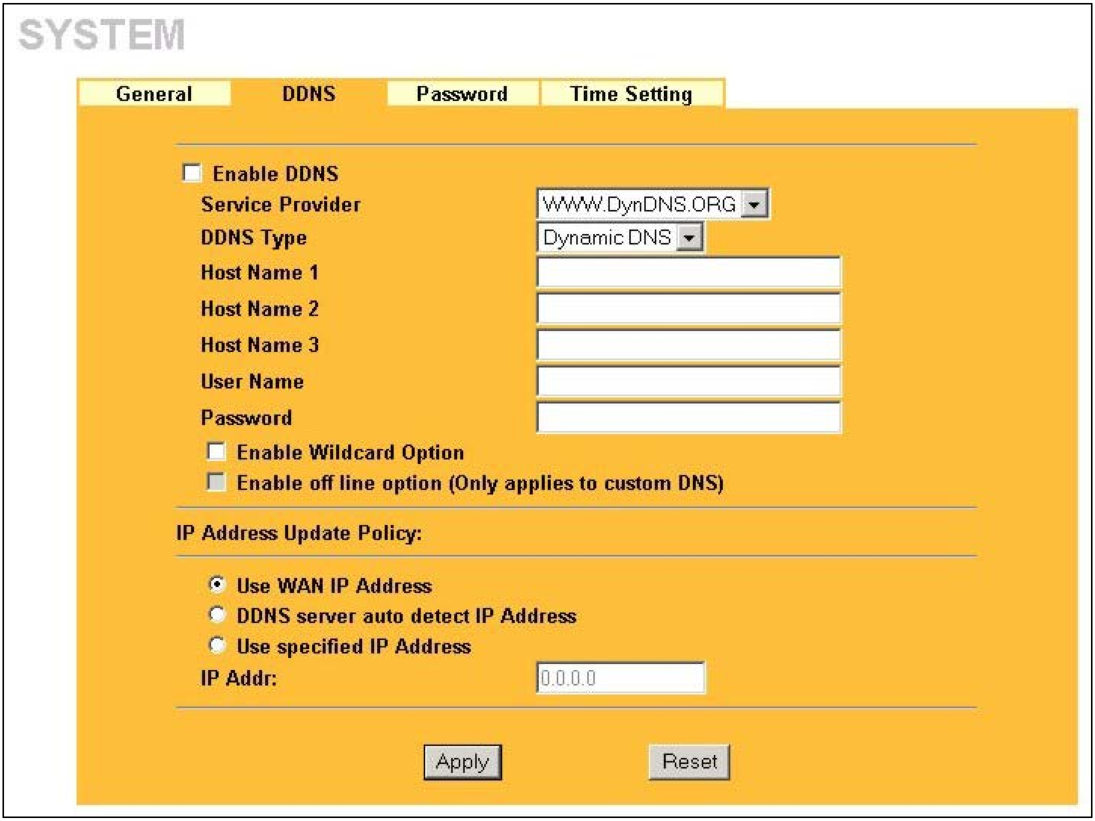
4.3.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

4.4 Configuring Dynamic DNS

To change your ZyAIR’s DDNS, click **ADVANCED**, **SYSTEM** and then the **DDNS** tab. The screen appears as shown.



SYSTEM

☐ Enable DDNS

Service Provider	WWW.DynDNS.ORG
DDNS Type	Dynamic DNS
Host Name 1	
Host Name 2	
Host Name 3	
User Name	
Password	

☐ Enable Wildcard Option

☐ Enable off line option (Only applies to custom DNS)

IP Address Update Policy:

● Use WAN IP Address

○ DDNS server auto detect IP Address

○ Use specified IP Address

IP Addr: 0.0.0.0

Figure 4-2 DDNS

The following table describes the labels in this screen.

Table 4-2 DDNS

LABEL	DESCRIPTION
Enable DDNS	Select this check box to activate DDNS.
Service Provider	Select the name of your DDNS service provider.
DDNS Type	Select the type of service that you are registered for from your DDNS service provider. Options are **Dynamic DNS**, **Static DNS** or **Custom DNS**.
Host Names 1~3	Enter your host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").

Table 4-2 DDNS

LABEL	DESCRIPTION
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Your ZyAIR supports DYNDNS wildcard. Select the check box to enable.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP address	Select this option to update the IP address of the host name(s) to the WAN IP address.
DDNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr	Enter the IP address if you select the **Use specified IP Address** option.
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 Password

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

If you forget your password (or the ZyAIR IP address), you will need to reset the ZyAIR or upload the default configuration file via console port (on ZyAIR B-2000 only). See the *Resetting the ZyAIR* section for details.

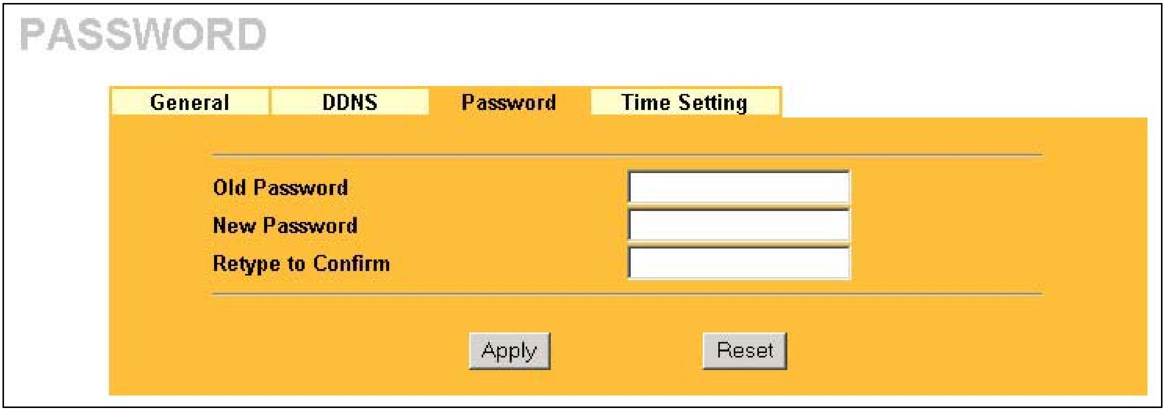


Figure 4-3 Password

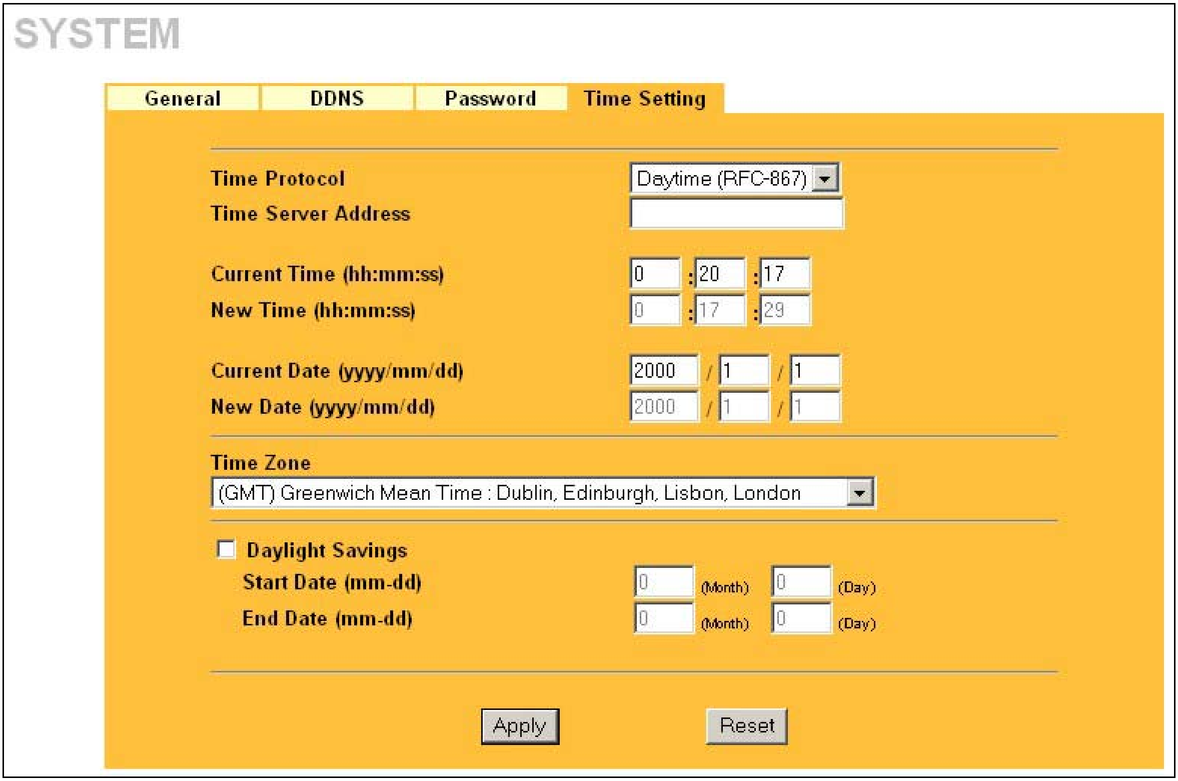
The following table describes the labels in this screen.

Table 4-3 Password

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

4.6 Configuring Time Setting

To change your ZyAIR's time and date, click **ADVANCED**, **SYSTEM** 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.



Time Protocol: Daytime (RFC-867)

Time Server Address:

Current Time (hh:mm:ss): 0 : 20 : 17

New Time (hh:mm:ss): 0 : 17 : 29

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

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

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

□ Daylight Savings

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

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

Figure 4-4 Time Setting

The following table describes the labels in this screen.

Table 4-4 Time Setting

LABEL	DESCRIPTION
Time Protocol	Select 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 difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.

Table 4-4 Time Setting

LABEL	DESCRIPTION
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 (the default is tick.stdtime.gov.tw).
Current Time (hh:mm:ss)	This field displays the time of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**.
Current Date (yyyy/mm/dd)	This field displays the date of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field 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 savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

Chapter 5
LAN Screens

This chapter describes how to configure LAN settings.

5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Please see the *Wizard Setup* chapter for the background information about Primary and Secondary DNS Server and IP Address and Subnet Mask.

5.2 LANs and WANs

A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

5.2.1 LANs, WANs and the ZyAIR

The actual physical connection determines whether the ZyAIR ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:

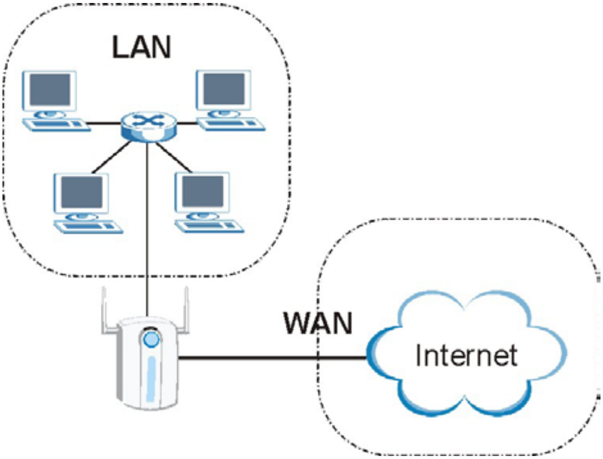


Figure 5-1 LAN & WAN IPs

5.3 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyAIR as a DHCP server or disable it. When configured as a server, the ZyAIR provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

5.4 Factory LAN Defaults

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

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

IP Pool Setup

The ZyAIR is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyAIR itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

5.5 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to:

1. **Both -** the ZyAIR will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the ZyAIR will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the ZyAIR will send out RIP packets but will not accept any RIP packets received.
4. **None -** the ZyAIR will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

5.6 Multicast

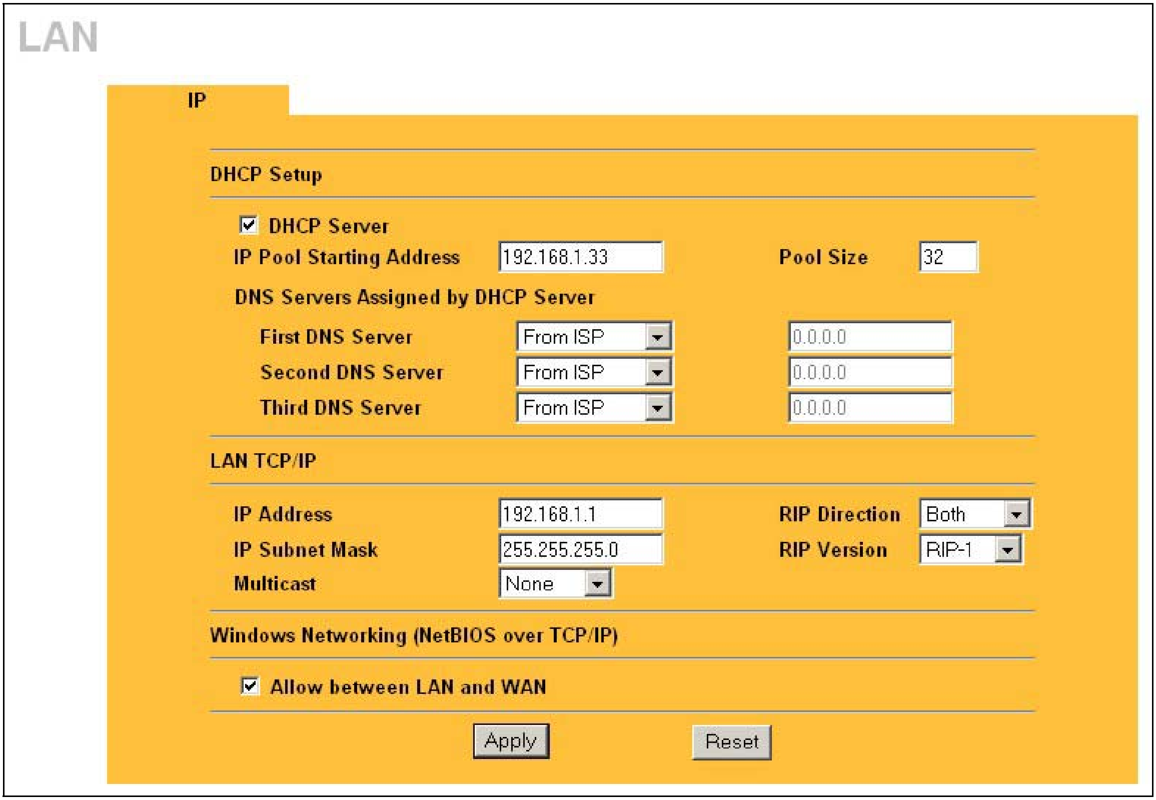
Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyAIR supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyAIR queries all directly connected networks to gather group membership. After that, the ZyAIR periodically updates this information. IP multicasting can be enabled/disabled on the ZyAIR LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

5.7 Configuring the LAN IP Screens

Click **ADVANCED** and then **LAN** to open the **IP** screen.



LAN

IP

DHCP Setup

☑ DHCP Server

IP Pool Starting Address: 192.168.1.33

Pool Size: 32

DNS Servers Assigned by DHCP Server

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

LAN TCP/IP

IP Address: 192.168.1.1

RIP Direction: Both

IP Subnet Mask: 255.255.255.0

RIP Version: RIP-1

Multicast: None

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between LAN and WAN

Figure 5-2 IP

The following table describes the labels in this screen.

Table 5-1 IP

LABEL	DESCRIPTION
DHCP Setup	
DHCP Server	Select this option to allow your ZyAIR to assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. When DHCP is used, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 5-1 IP

LABEL	DESCRIPTION
Pool Size	This field specifies the size or count of the IP address pool.
DNS Servers Assigned by DHCP Server	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyAIR's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyAIR act as a DNS proxy. The ZyAIR's LAN IP address displays in the field to the right (read-only). The ZyAIR tells the DHCP clients on the LAN that the ZyAIR itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyAIR, the ZyAIR forwards the query to the ZyAIR's system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
LAN TCP/IP	
IP Address	Type the IP address of your ZyAIR in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ZyAIR supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this option to forward NetBIOS packets between the LAN port and the WAN port.
Apply	Click **Apply** to save your changes back to the ZyAIR.

Table 5-1 IP

LABEL	DESCRIPTION
Reset	Click **Reset** to reload the previous configuration for this screen.

Chapter 6
Wireless Configuration and Roaming

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

6.1 Wireless LAN Overview

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

6.1.1 IBSS

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

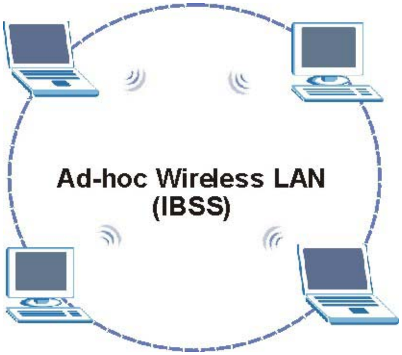


Figure 6-1 IBSS (Ad-hoc) Wireless LAN

6.1.2 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.

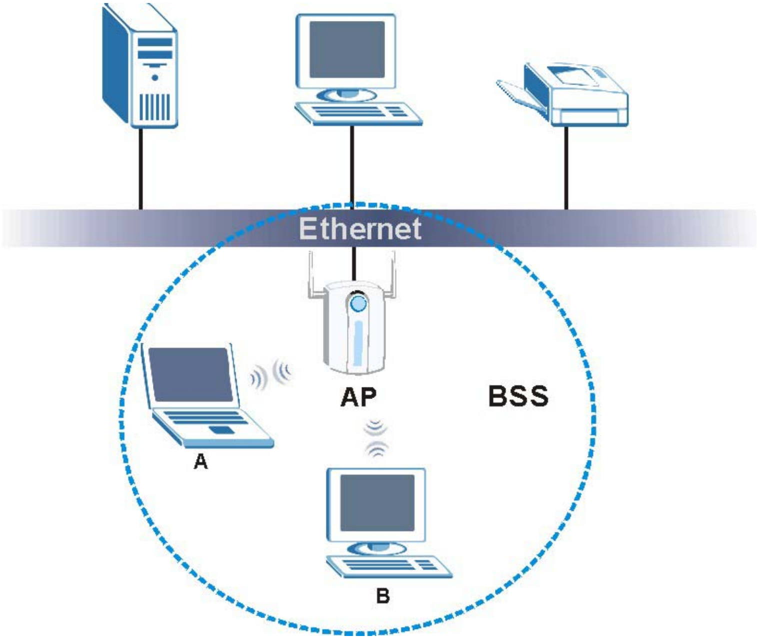


Figure 6-2 Basic Service set

6.1.3 ESS

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

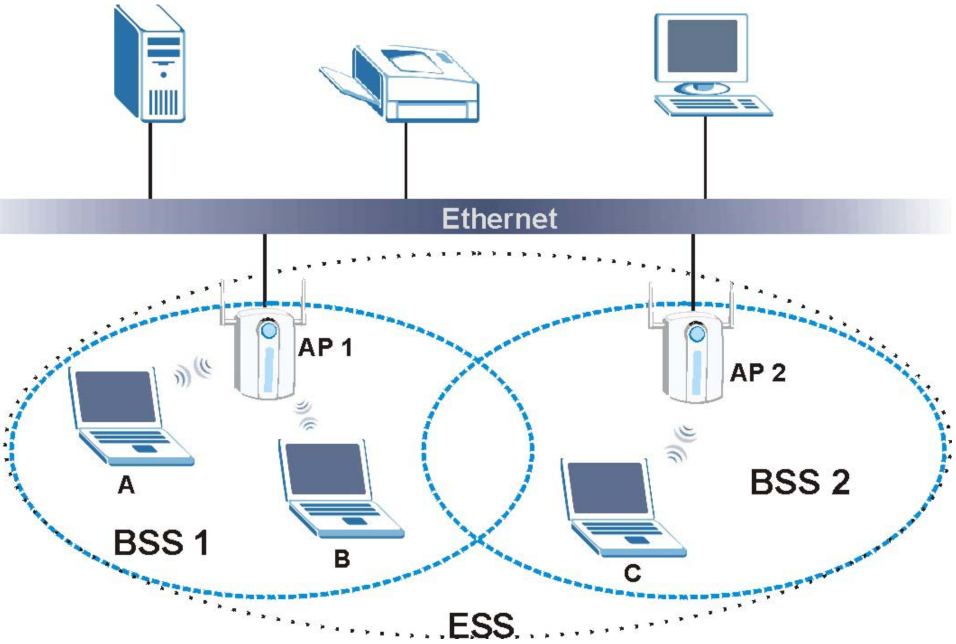


Figure 6-3 Extended Service Set

6.2 Wireless LAN Basics

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

6.2.1 RTS/CTS

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

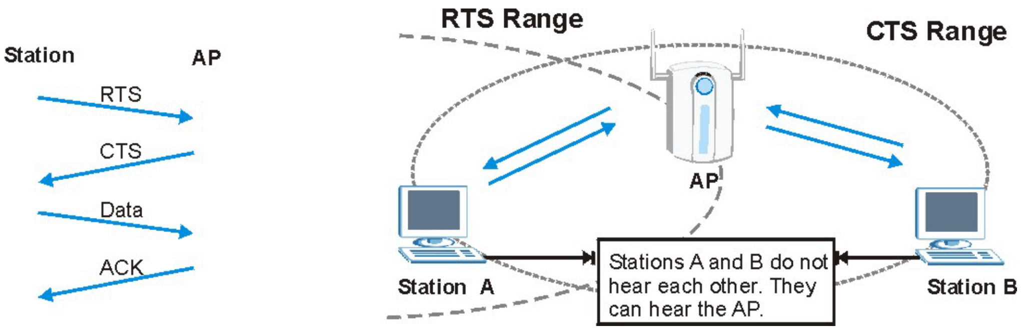

Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

Figure 6-4 RTS/CTS

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

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

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

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

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

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

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

6.2.2 Fragmentation Threshold

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

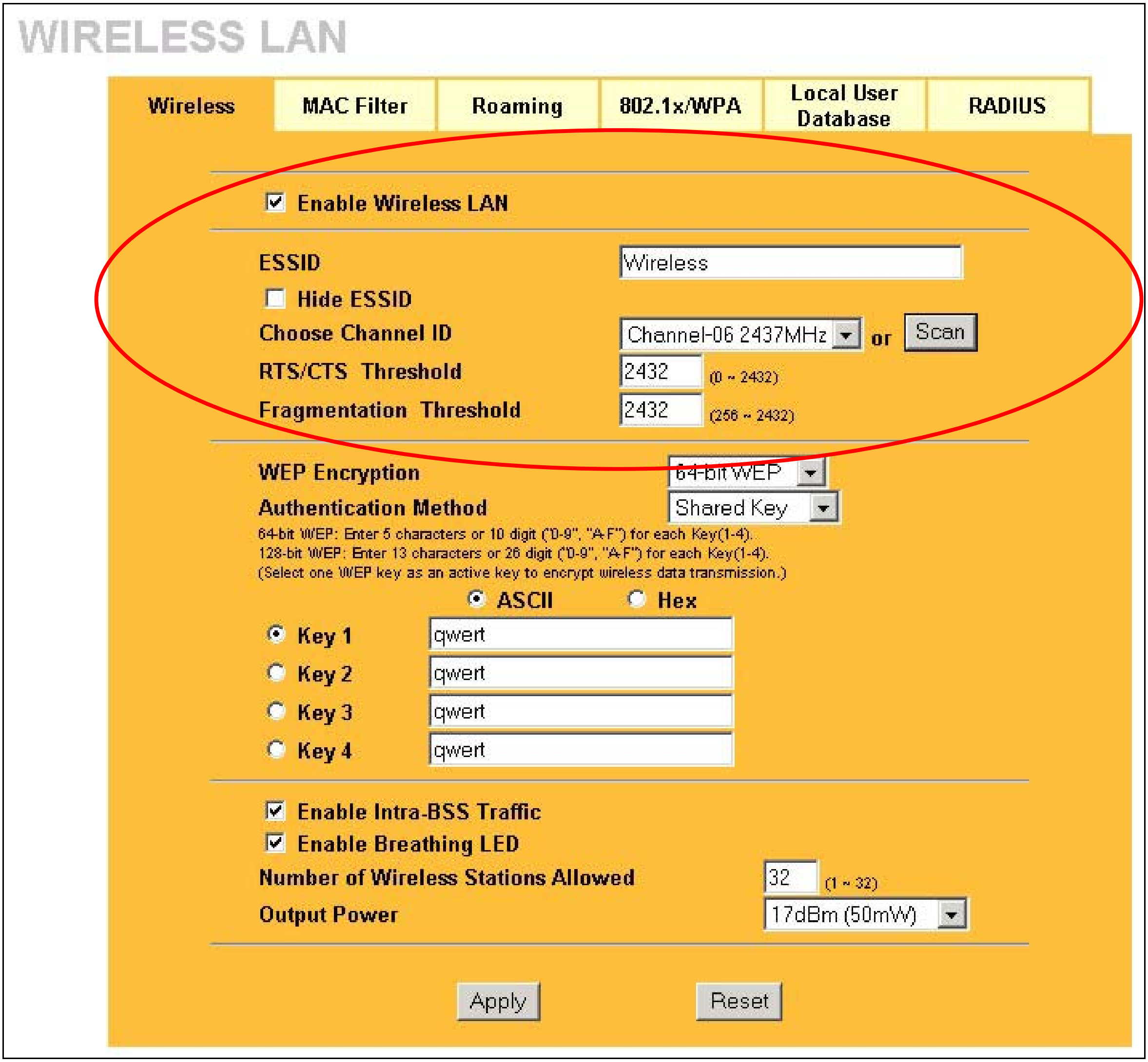
A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

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

6.3 Configuring Wireless

If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.

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



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: 64-bit WEP

Authentication Method: Shared Key

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: qwert
○ Key 2: qwert
○ Key 3: qwert
○ Key 4: qwert

☑ Enable Intra-BSS Traffic

☑ Enable Breathing LED

Number of Wireless Stations Allowed: 32 (1 ~ 32)

Output Power: 17dBm (50mW)

Figure 6-5 Wireless

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

Table 6-1 Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.**
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE**, **WIRELESS** 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. To have the ZyAIR automatically select a channel, click **Scan** instead. Refer to the *Wizard Setup* chapter for more information on channels.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.
RTS/CTS Threshold	Enter a value between 0 and 2432. The default is **2432**.
Fragmentation Threshold	Enter a value between 256 and 2432. The default is **2432**. It is the maximum data fragment size that can be sent.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

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

6.4 Configuring Roaming

A wireless station is a device with an IEEE 802.11b 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 6-6*.

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). 802.1x authentication information is not exchanged (at the time of writing).

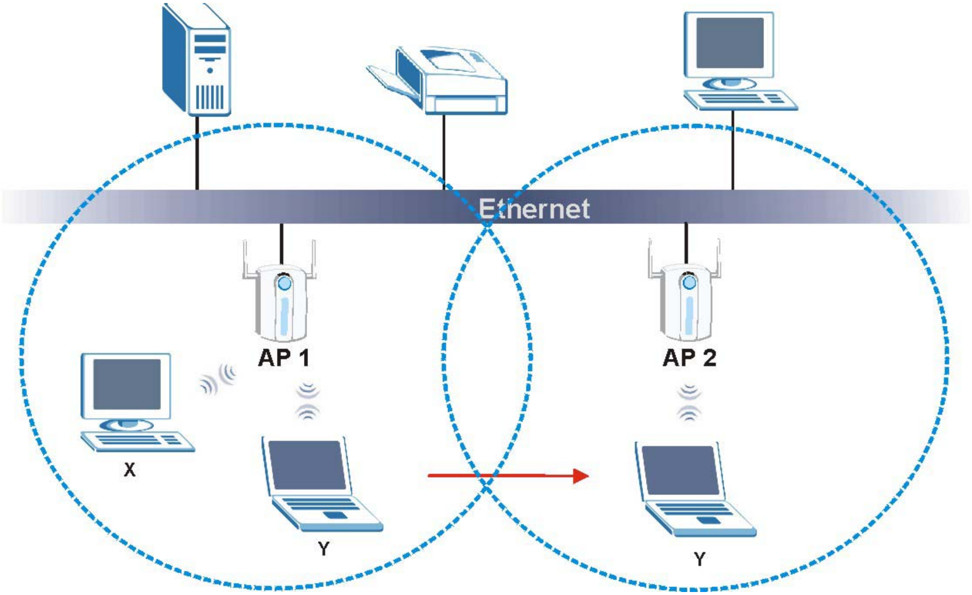


Figure 6-6 Roaming Example

The steps below describe the roaming process.

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

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

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

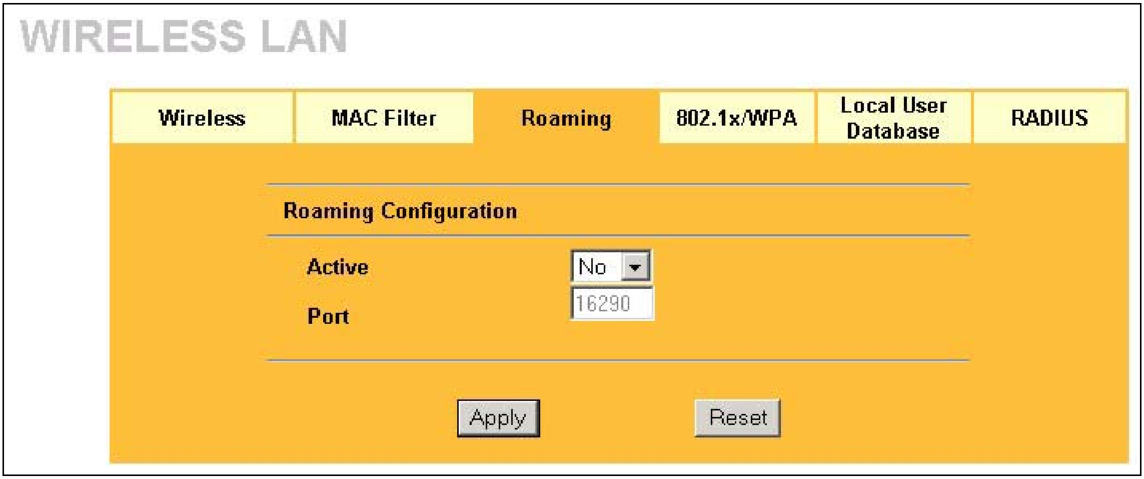
Step 4. Wireless station **Y** sends a request to access point **AP 2** for re-authentication.

6.4.1 Requirements for Roaming

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

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

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



WIRELESS LAN

Roaming Configuration

Active: No

Port: 16290

Figure 6-7 Roaming

The following table describes the labels in this screen.

Table 6-2 Roaming

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

Chapter 7
Wireless Security

This Chapter describes how to use the MAC Filter, 802.1x, Local User Database and RADIUS to configure wireless security on your ZyAIR.

7.1 Wireless Security Overview

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

The figure below shows the possible wireless security levels on your ZyAIR. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations. Dynamic WEP key exchange is not available on the ZyAIR B-2000.

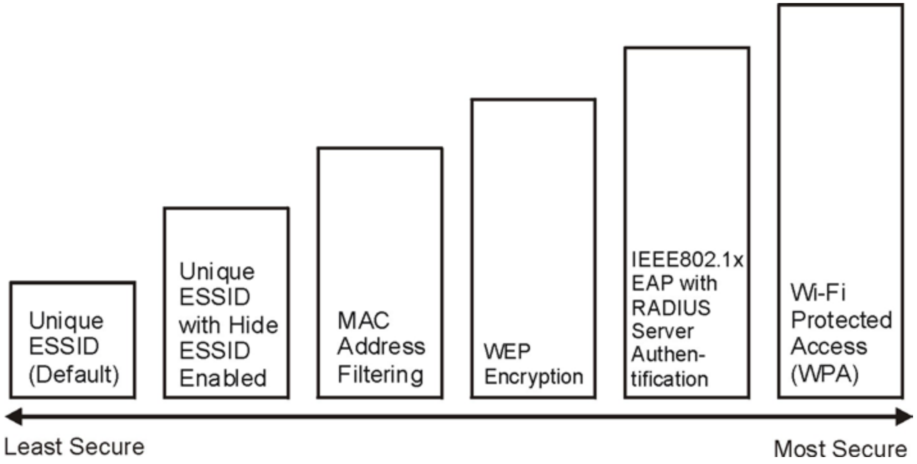

Unique ESSID (Default)
Unique ESSID with Hide ESSID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

Figure 7-1 ZyAIR Wireless Security Levels

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

7.2 WEP Overview

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

7.2.1 Data Encryption

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

7.2.2 Authentication

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

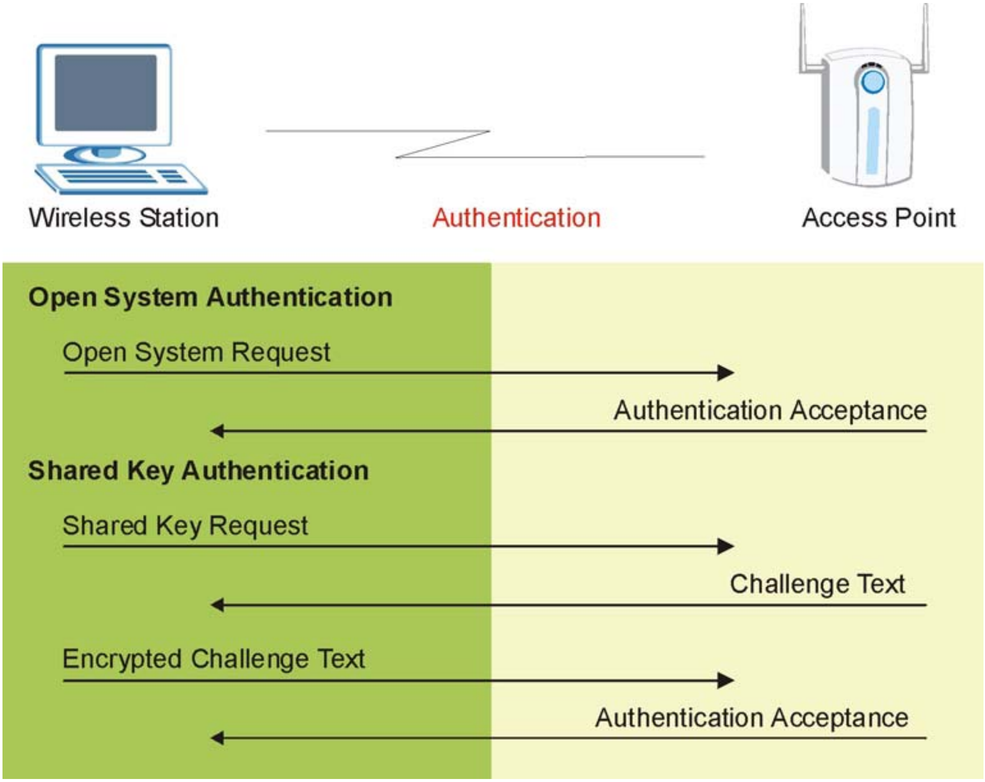


Figure 7-2 WEP Authentication Steps

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

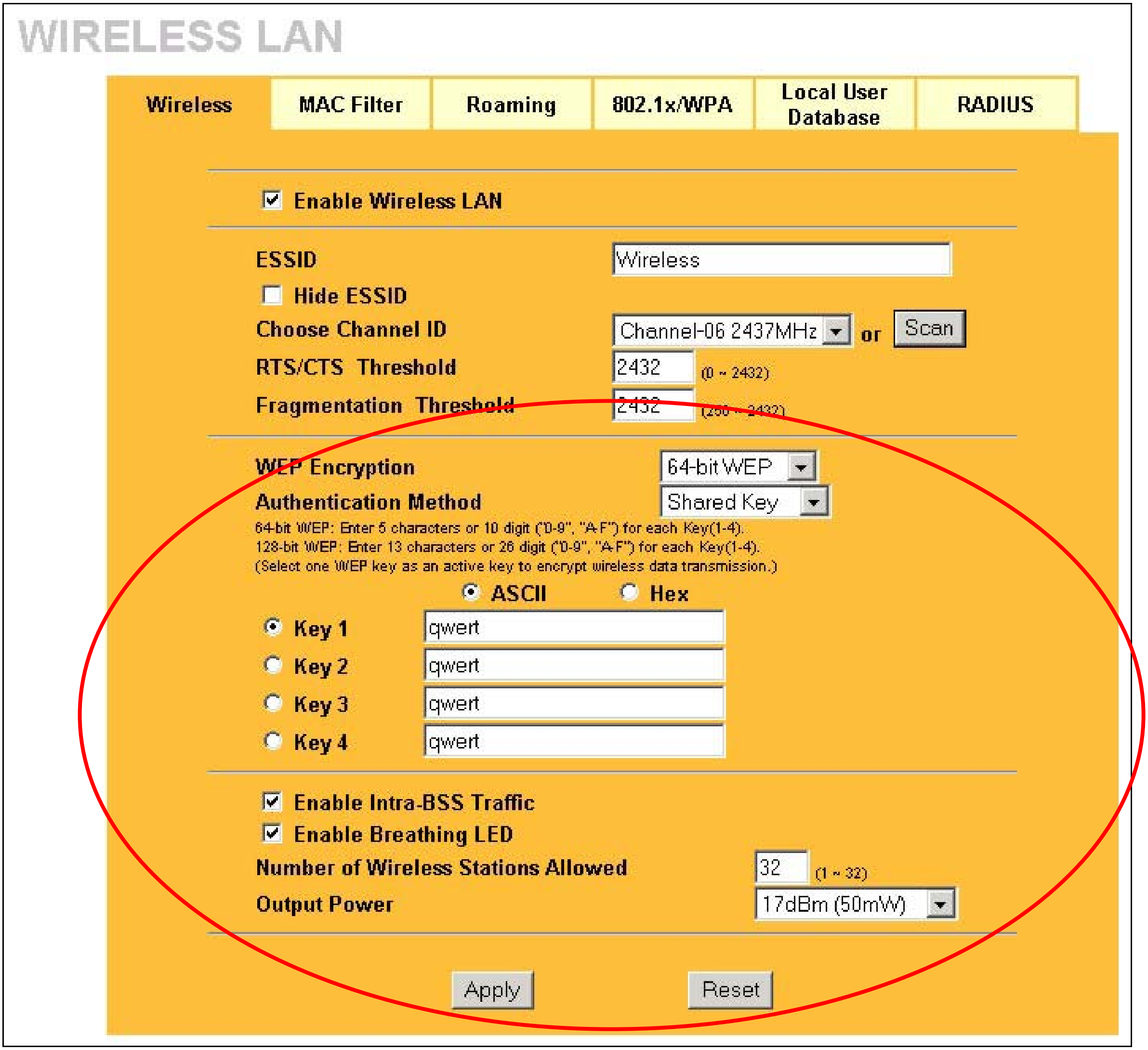
Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

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

7.3 Configuring WEP Encryption

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

The WEP Encryption, Authentication Method and the WEP key fields are not visible when you enable Dynamic WEP Key, WPA or WPA-PSK in the 802.1x/WPA screen.



WIRELESS LAN

☑ Enable Wireless LAN

ESSID: Wireless

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: 64-bit WEP

Authentication Method: Shared Key

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: qwert

○ Key 2: qwert

○ Key 3: qwert

○ Key 4: qwert

☑ Enable Intra-BSS Traffic

☑ Enable Breathing LED

Number of Wireless Stations Allowed: 32 (1 ~ 32)

Output Power: 17dBm (50mW)

Figure 7-3 Wireless

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

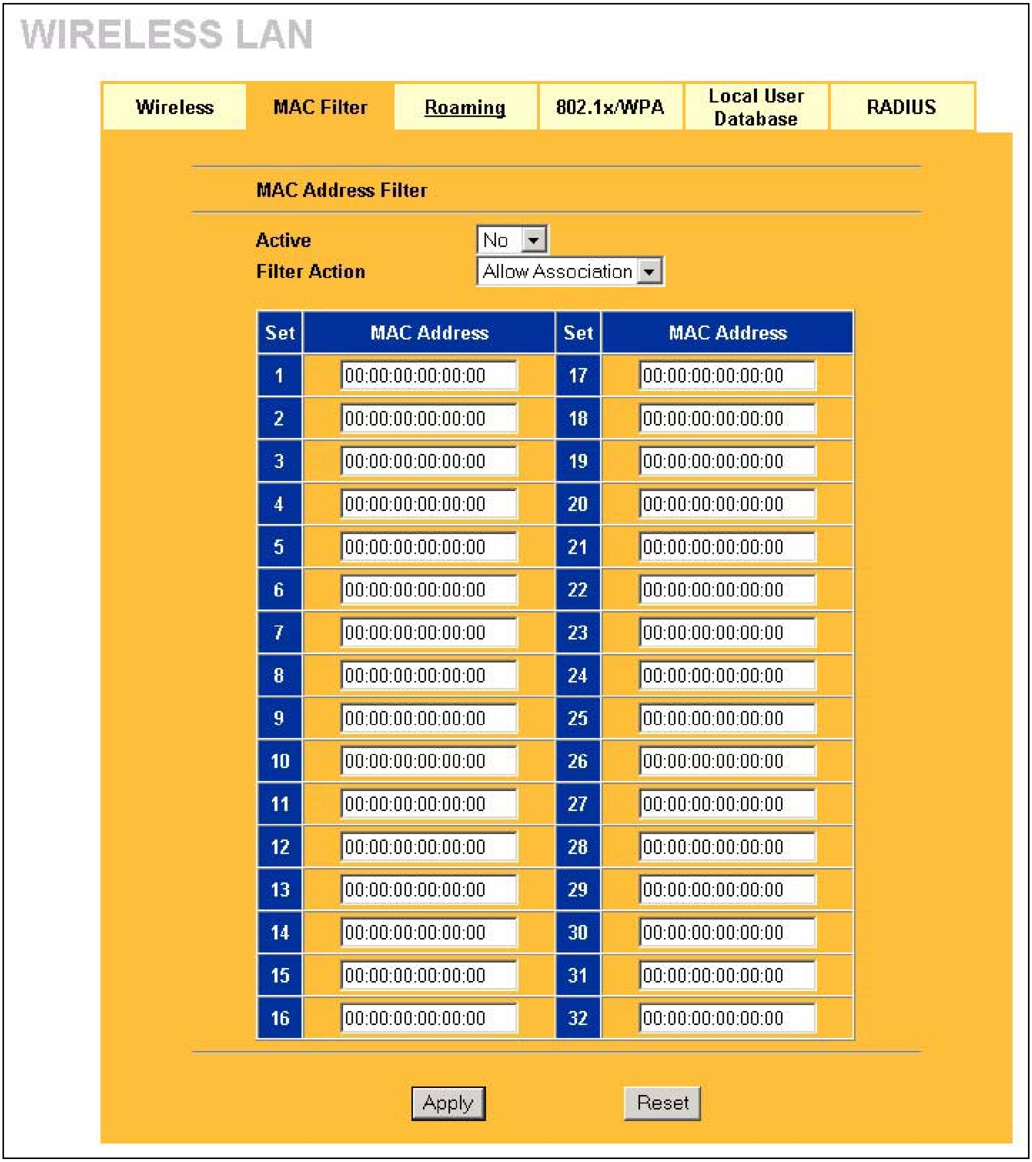
Table 7-1 Wireless : WEP Fields

LABEL	DESCRIPTION
WEP Encryption	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto**, **Open System** or **Shared Key** from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the BSS. Select this check box to enable Intra-BSS Traffic.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Number of Wireless Stations Allowed	Use this field to set a maximum number of wireless stations that may connect to the ZyAIR. Enter the number (from 1 to 32) of wireless stations allowed.
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 **17dBm (50mW)**, **15dBm (32mW)**, **13dBm (20mW)** or **11dBm (12.6mW)**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4 MAC Filter

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

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



MAC Address Filter

Active: No

Filter Action: Allow Association

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

Figure 7-4 MAC Address Filter

The following table describes the labels in this menu.

Table 7-2 MAC Address Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the ZyAIR, MAC addresses not listed will be allowed to access the ZyAIR Select **Allow Association** to permit access to the ZyAIR, MAC addresses not listed will be denied access to the ZyAIR.
Set	This is the index number of the MAC address.
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 reload the previous configuration for this screen.

7.5 802.1x Overview

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

7.6 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.

To use Dynamic WEP, enable and configure the RADIUS server (see *section 7.15*) and enable Dynamic WEP Key Exchange in the 802.1x screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

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

7.7 Introduction to WPA

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

7.7.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the ZyAIR's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

7.7.2 Encryption

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

Temporal Key Integrity Protocol (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 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. This all happens in the background automatically.

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

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode 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.

7.8 WPA-PSK Application Example

A WPA-PSK application looks as follows.

Step 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).

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

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

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

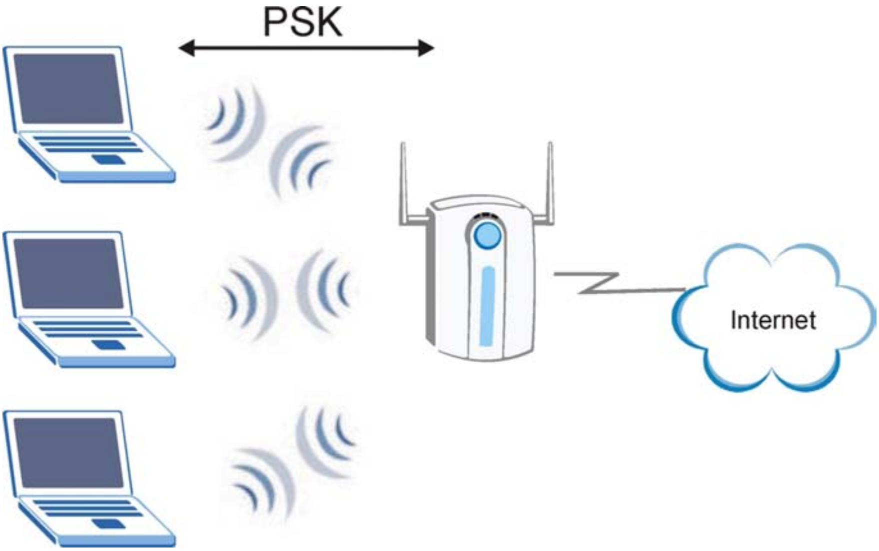


Figure 7-5 WPA - PSK Authentication

7.9 WPA with RADIUS Application Example

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

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

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

Step 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.

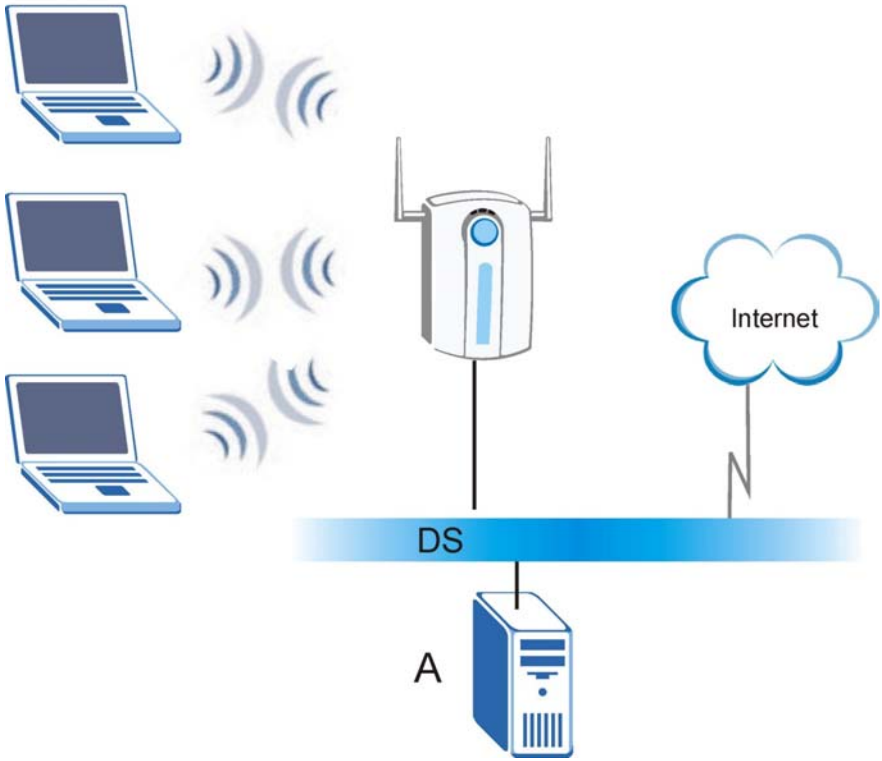


Figure 7-6 WPA with RADIUS Application Example

7.10 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 7-3 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
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	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

7.11 Wireless Client WPA Supplicants

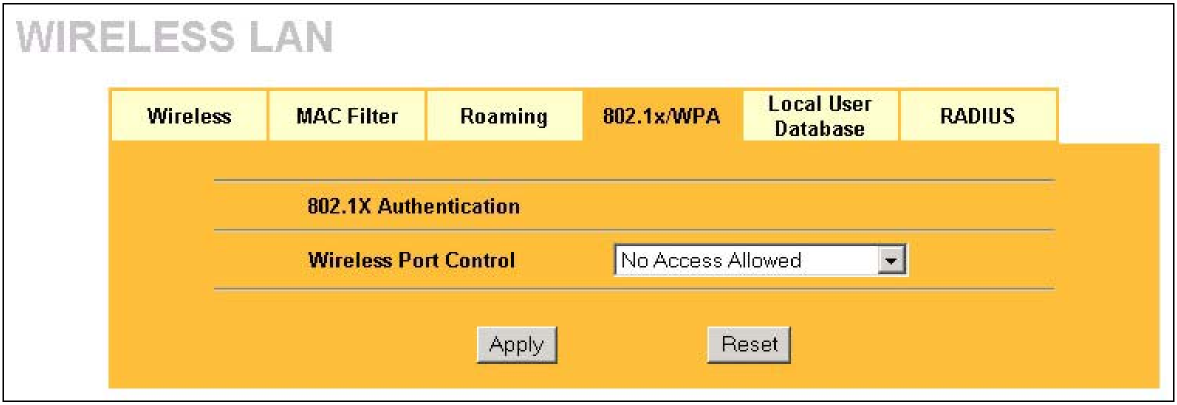
A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

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.

7.12 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.



802.1X Authentication

Wireless Port Control: No Access Allowed

Figure 7-7 Wireless LAN: 802.1x/WPA

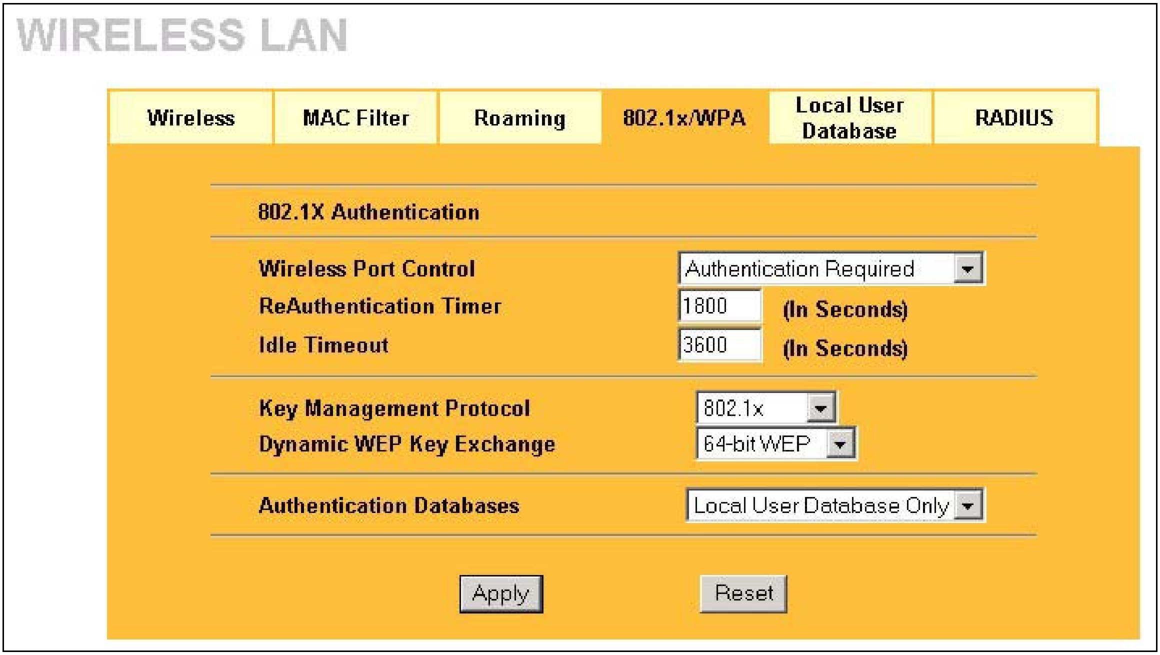
The following table describes the labels in this screen.

Table 7-4 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**. **No Access Allowed** blocks all wireless stations access to the wired network. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **Authentication Required** to configure **Key Management Protocol** and other related fields.

7.12.1 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.



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: 64-bit WEP

Authentication Databases: Local User Database Only

Figure 7-8 Wireless LAN: 802.1x/WPA for 802.1x Protocol

The following table describes the labels in this screen.

Table 7-5 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**. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. **No Access Allowed** blocks all wireless stations access to the wired network. The following fields are only available when you select **Authentication Required**.

Table 7-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol

LABEL	DESCRIPTION
ReAuthentication Timer (In Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). **If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**
Idle Timeout (In Seconds)	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (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. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**. This feature is not available on the ZyAIR B-2000.

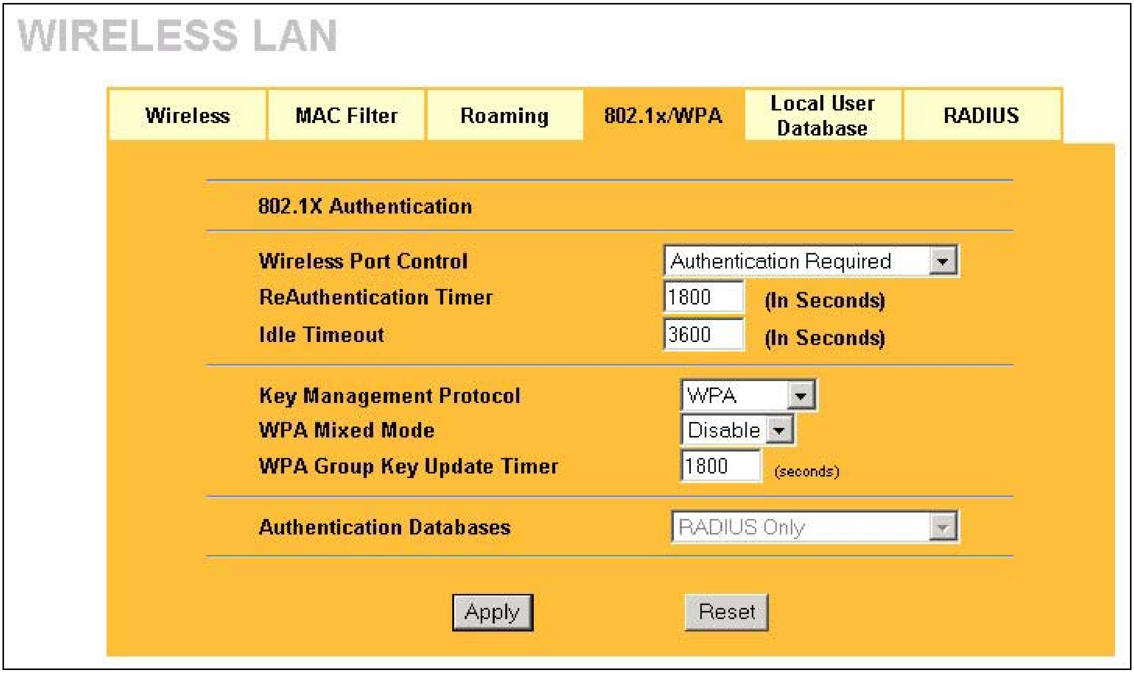
Table 7-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol

LABEL	DESCRIPTION
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 drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password. Select **RADIUS Only** to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

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

7.12.2 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.



WIRELESS LAN

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: RADIUS Only

Figure 7-9 Wireless LAN: 802.1x/WPA for WPA Protocol

The following table describes the labels not previously discussed

Table 7-6 Wireless LAN: 802.1x/WPA for WPA Protocol

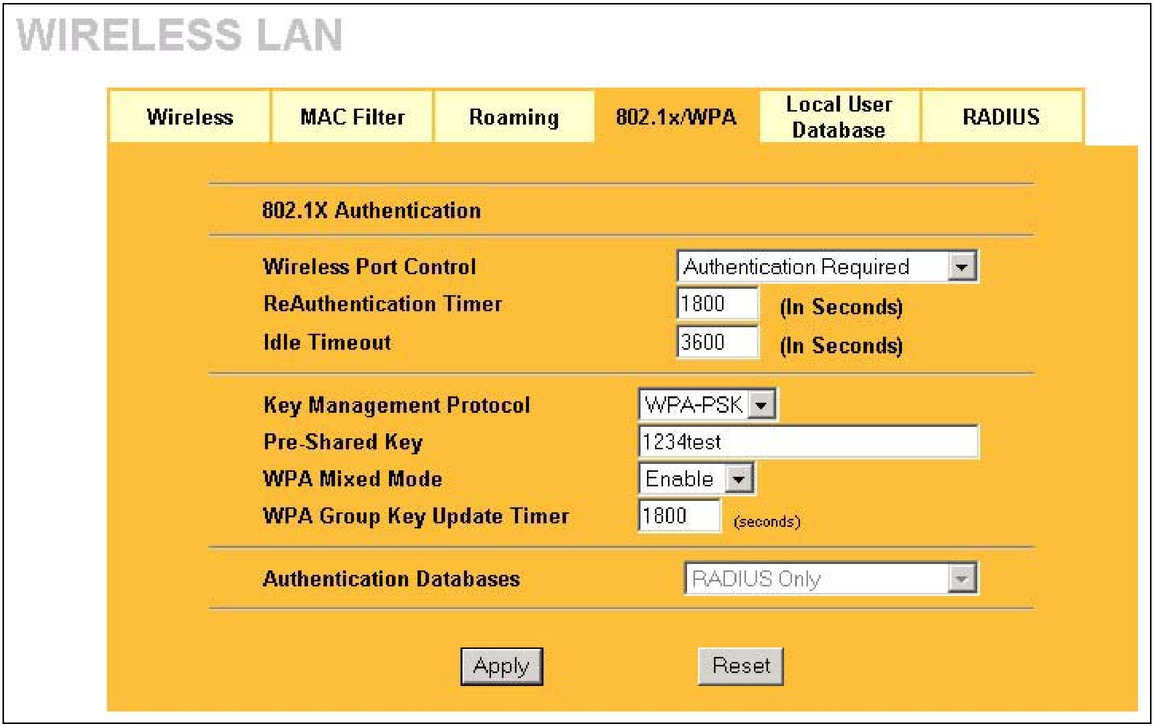
LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The ZyAIR can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select **Enable** to activate WPA mixed mode. 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).

Table 7-6 Wireless LAN: 802.1x/WPA for WPA Protocol

LABEL	DESCRIPTION
Authentication Databases	When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database Only** with **802.1x Key Management Protocol**.

7.12.3 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.



WIRELESS LAN

802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA-PSK

Pre-Shared Key: 1234test

WPA Mixed Mode: Enable

WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases: RADIUS Only

Figure 7-10 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

The following table describes the labels not previously discussed.

Table 7-7 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

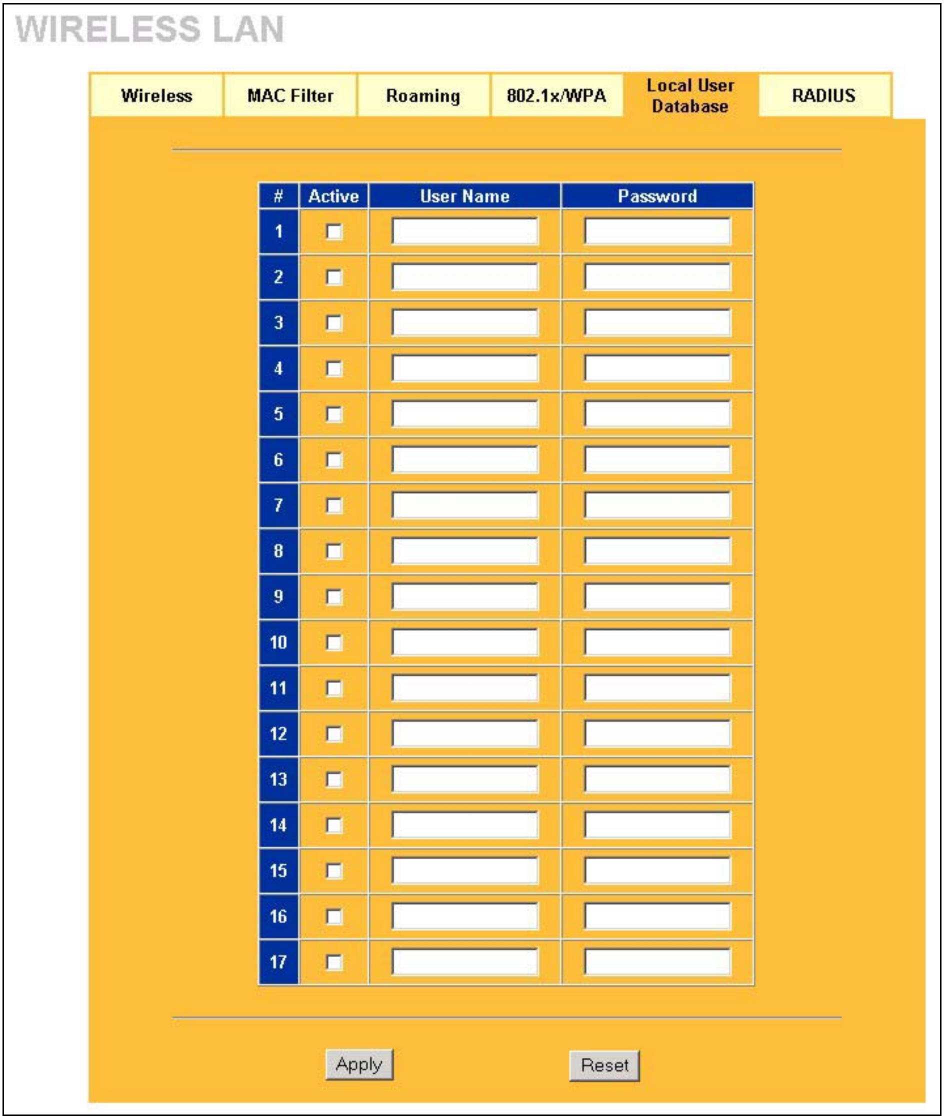
LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA-PSK** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
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 802.1x in the same Wi-Fi network. 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).
Authentication Databases	This field is only visible when **WPA Mixed Mode** is enabled. When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database Only** with **802.1x Key Management Protocol**.

7.13 Introduction to Local User Database

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

7.14 Configuring Local User Database

To change your ZyAIR's local user database, click **ADVANCED**, **WIRELESS** and then the **Local User Database** tab. The screen appears as shown (some of the screen's blank rows are not shown).



#	Active	User Name	Password
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		
11	□		
12	□		
13	□		
14	□		
15	□		
16	□		
17	□		

Figure 7-11 Local User Database

The following table describes the labels in this screen.

Table 7-8 Local User Database

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

7.15 Introduction to RADIUS

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

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

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

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

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

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

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

7.15.1 EAP Authentication Overview

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

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

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

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

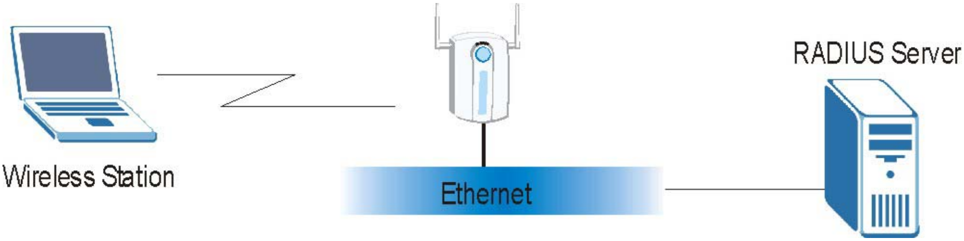


Figure 7-12 EAP Authentication

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

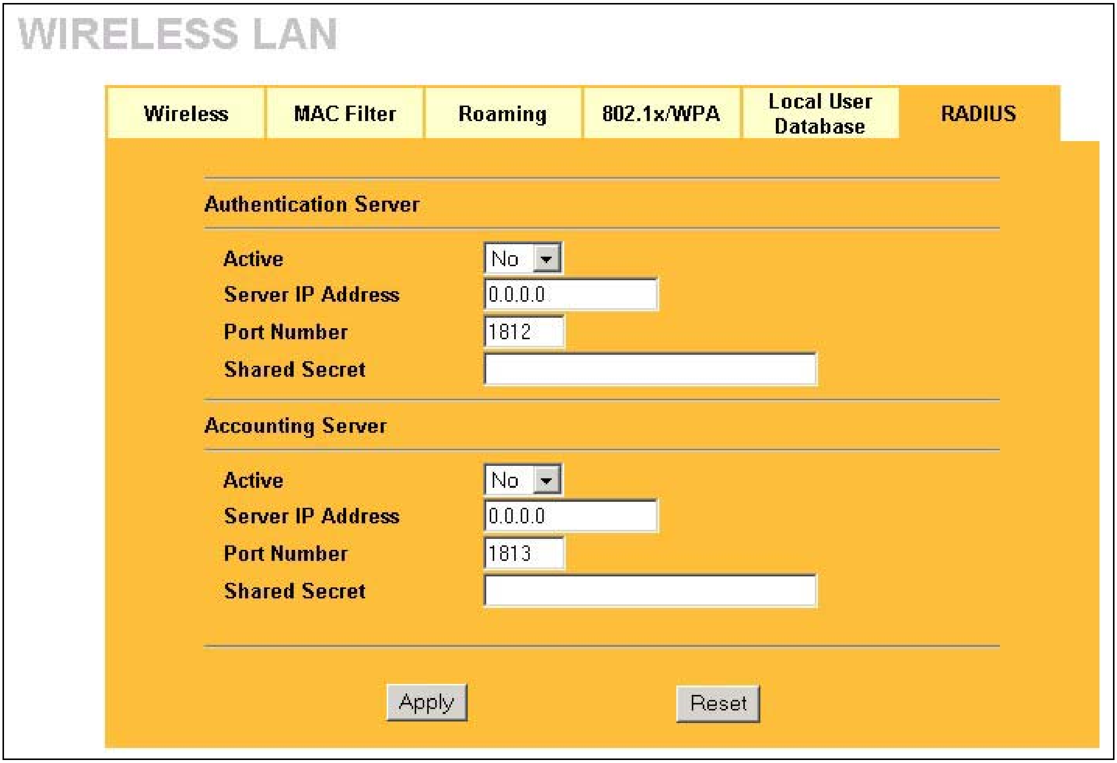
- The wireless station sends a “start” message to the ZyAIR.

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

7.16 Configuring RADIUS

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

To specify a RADIUS server, click **ADVANCED**, **WIRELESS** and then the **RADIUS** tab. The screen appears as shown.



WIRELESS LAN

Authentication Server

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

Accounting Server

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

Figure 7-13 RADIUS

The following table describes the labels in this screen.

Table 7-9 RADIUS

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

Part III:

WAN

This part covers the web configurator screen and information about WAN.

Chapter 8
WAN Screens

This chapter describes how to configure the ZyAIR WAN screens.

8.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

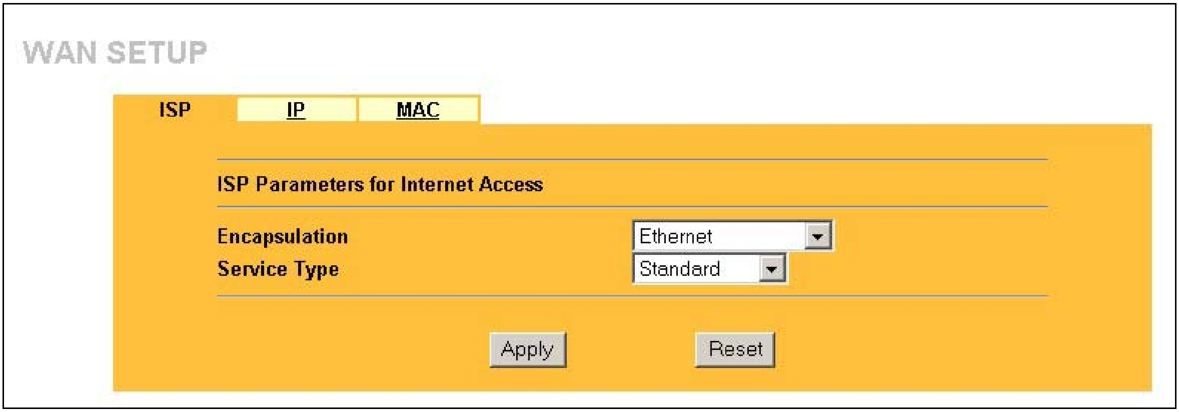
See the *Wizard Setup* chapter for more background information on most fields in the WAN screens. Background information on WAN fields not included in the Wizard is described here.

8.2 Configuring WAN ISP

To change your ZyAIR's WAN ISP settings, click **ADVANCED**, **WAN** and then the **ISP** tab. The screen differs by the encapsulation.

8.2.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.



ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard

Figure 8-1 Ethernet Encapsulation

The following table describes the labels in this screen.

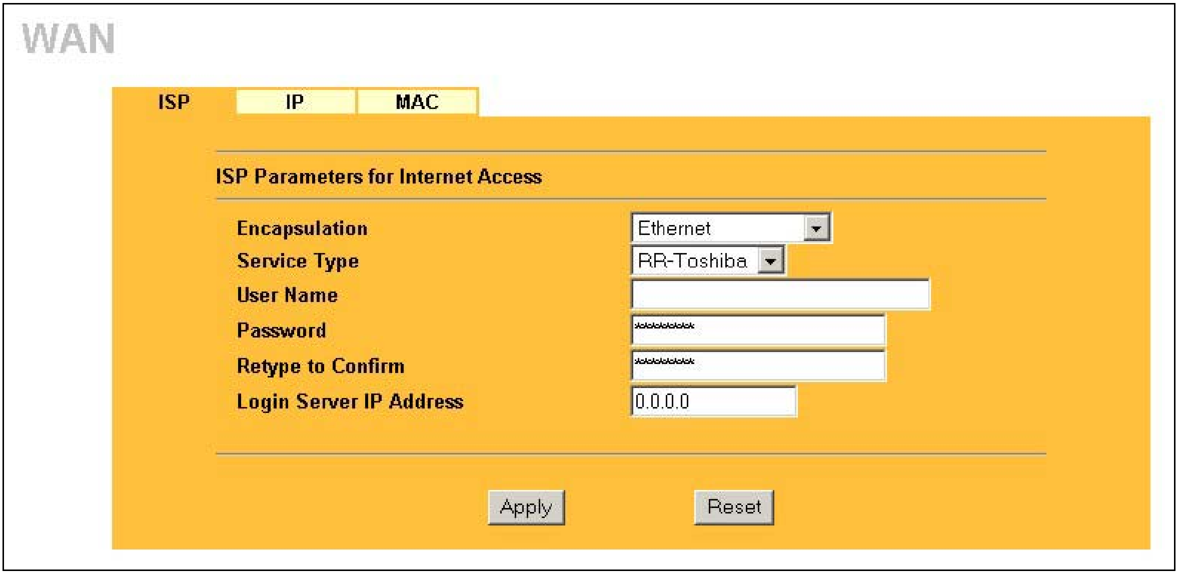
Table 8-1 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose **Standard**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Service Type

The screen varies according to the service type you select.

You need a username and password if your ISP is Time Warner's Roadrunner.



ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	RR-Toshiba
User Name	
Password	********
Retype to Confirm	********
Login Server IP Address	0.0.0.0

Figure 8-2 Service Type

The following table describes the labels in this screen.

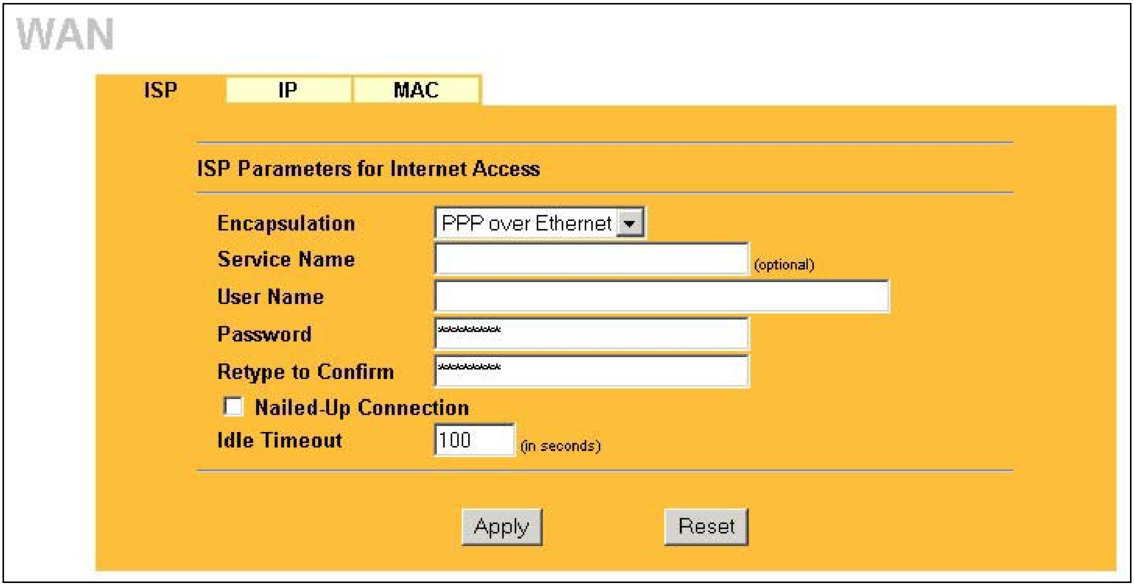
Table 8-2 Service Type

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (Roadrunner Manager authentication method) **RR-Telstra** or **Telia Login**. Choose a Roadrunner service type if your ISP is Time Warner's Roadrunner; otherwise choose **Standard**.
User Name	Enter the username given to you by your ISP.
Password	Enter the password associated with the login name above.
Retype to Confirm	Type your password again here to ensure that what you entered in the **Password** field above was what you intended.
Login Server IP Address	The ZyAIR will find the Roadrunner Server IP address if this field is left blank. If it does not, then you must enter the authentication server IP address.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example "login1.telia.com". This field is not available on all models.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyAIR out if the ZyAIR does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyAIR to wait between logins. This field is not available on all models.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.2 PPPoE Encapsulation

PPPoE (Point-to-Point Protocol over Ethernet) is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

The screen shown next is for **PPP over Ethernet** encapsulation.



WAN

ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet

Service Name: (optional)

User Name:

Password: *********

Retype to Confirm: *********

□ Nailed-Up Connection

Idle Timeout: 100 (in seconds)

Figure 8-3 PPPoE Encapsulation

The following table describes the labels in this screen.

Table 8-3 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The ZyAIR supports PPPoE (Point-to-Point Protocol over Ethernet).
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the username given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again here to ensure that what you entered in the **Password** field above was what you intended.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Specify the time in seconds that elapses before the ZyAIR automatically disconnects from the PPPoE server.

Table 8-3 PPPoE Encapsulation

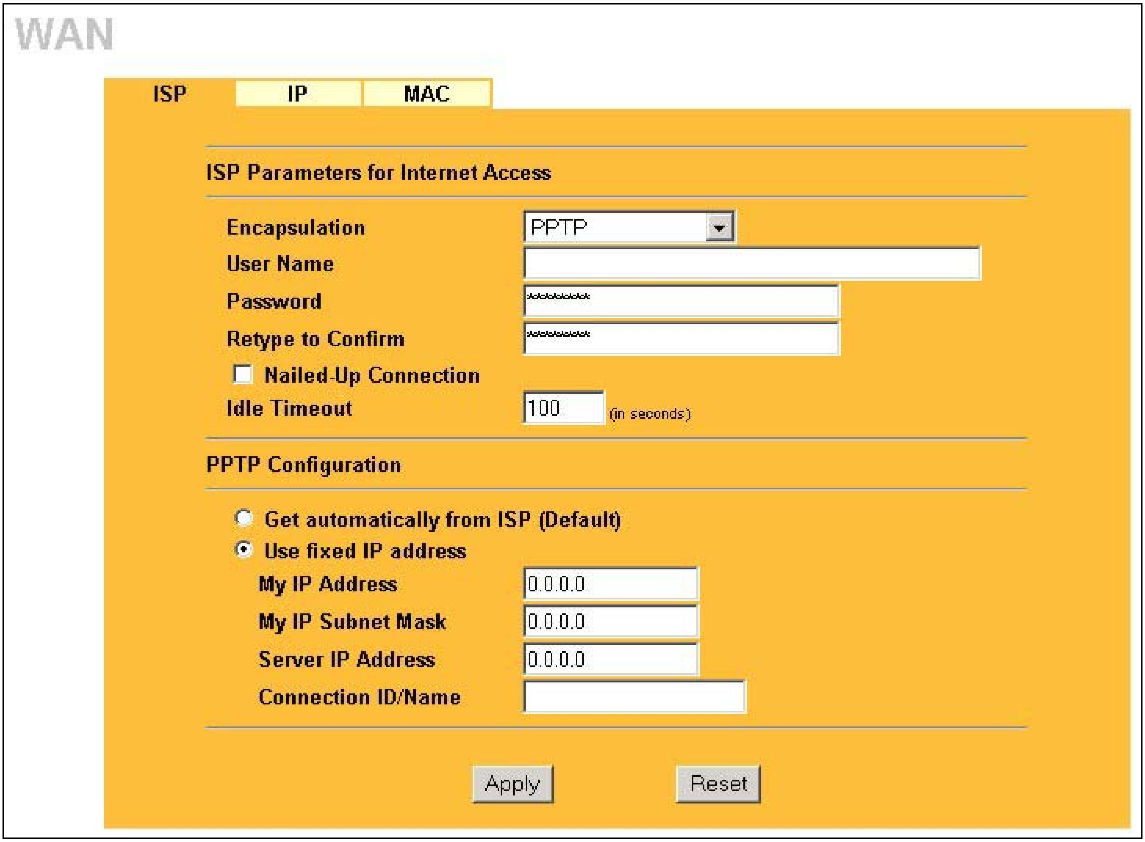
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.



WAN

ISP Parameters for Internet Access

Encapsulation: PPTP
User Name:
Password: *********
Retype to Confirm: *********
□ Nailed-Up Connection
Idle Timeout: 100 (in seconds)

PPTP Configuration

○ Get automatically from ISP (Default)
● Use fixed IP address
My IP Address: 0.0.0.0
My IP Subnet Mask: 0.0.0.0
Server IP Address: 0.0.0.0
Connection ID/Name:

Figure 8-4 PPTP Encapsulation

The following table describes the labels in this screen.

Table 8-4 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyAIR supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

Table 8-4 PPTP Encapsulation

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again here to ensure that what you entered in the **Password** field above was what you intended.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	Specify the time in seconds that elapses before the ZyAIR automatically disconnects from the PPTP server.
PPTP Configuration	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP in this field if you selected **Use Fixed IP Address**.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given) in this field if you selected **Use Fixed IP Address**.
Server IP Address	Type the IP address of the PPTP server in this field.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

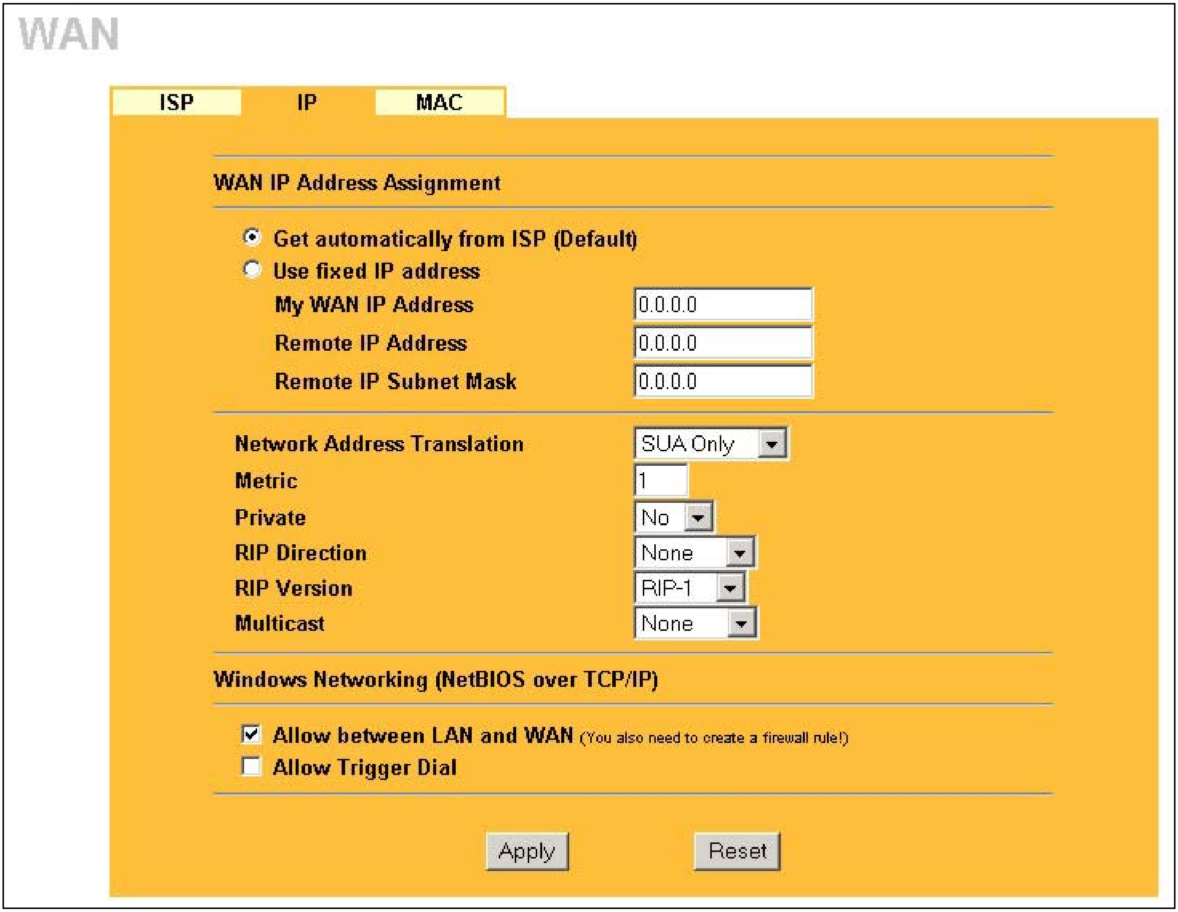
8.3 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyAIR's routes to the Internet. If any two of the default routes have the same metric.

8.4 Configuring WAN IP

To change your ZyAIR's WAN IP settings, click **ADVANCED**, **WAN** and then the **IP** tab.



WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use fixed IP address

My WAN IP Address: 0.0.0.0

Remote IP Address: 0.0.0.0

Remote IP Subnet Mask: 0.0.0.0

Network Address Translation: SUA Only

Metric: 1

Private: No

RIP Direction: None

RIP Version: RIP-1

Multicast: None

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between LAN and WAN (You also need to create a firewall rule!)

□ Allow Trigger Dial

Figure 8-5 IP Setup

The following table describes the labels in this screen.

Table 8-5 IP Setup

LABEL	DESCRIPTION
WAN IP Address Assignment	

Table 8-5 IP Setup

LABEL	DESCRIPTION
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter the ZyAIR WAN IP address in this field if you selected **Use Fixed IP Address.**
My WAN IP Subnet Mask (Ethernet encapsulation)	Enter the ZyAIR WAN IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Remote IP Address (or Gateway IP Address)	Type the IP address of the remote network or gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the remote nodes.
Remote IP Subnet Mask (PPPoE and PPTP encapsulation)	When using a LAN to LAN application, type the IP subnet mask of the destination network. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255, in the subnet mask field, to force the network number to be identical to the host ID.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. **SUA** (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. When you select this option the ZyAIR will use Address Mapping Set 255 in the SMT. Choose **SUA Only** if you have just one public WAN IP address for your ZyAIR. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyAIR. For more information about NAT refer to the *NAT* chapter in this *User's Guide*.
Metric (PPPoE and PPTP only)	Type a number that approximates the cost for this link. Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

Table 8-5 IP Setup

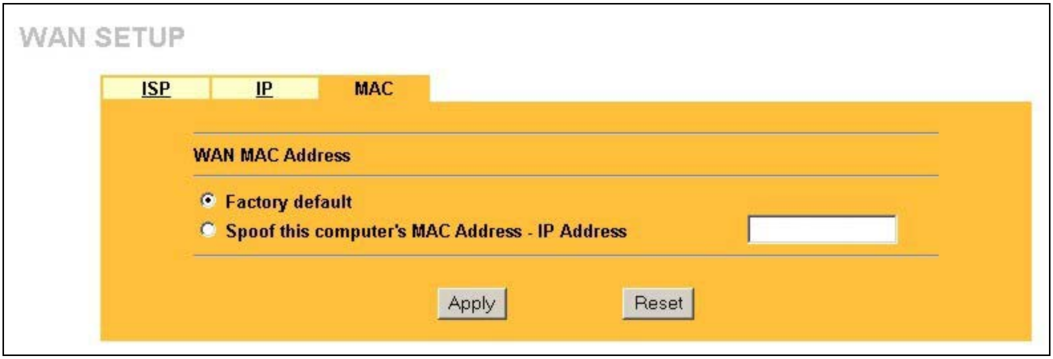
LABEL	DESCRIPTION
Private (PPPoE and PPTP only)	This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If select **Yes**, this route is kept private and not included in RIP broadcast. If select **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyAIR will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyAIR will incorporate RIP information that it receives. When set to **None**, the ZyAIR will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.	

Table 8-5 IP Setup

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Configuring WAN MAC

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



WAN SETUP

WAN MAC Address

● Factory default

○ Spoof this computer's MAC Address - IP Address

Figure 8-6 MAC Setup

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC address.

Part IV:

SUA/NAT AND STATIC ROUTE

This part covers the information about SUA/NAT and Static Route setup.

Chapter 9
Single User Account (SUA) / Network Address Translation (NAT)

This chapter discusses how to configure SUA/NAT on the ZyAIR.

9.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

9.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyAIR. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 9-1 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside **host.**

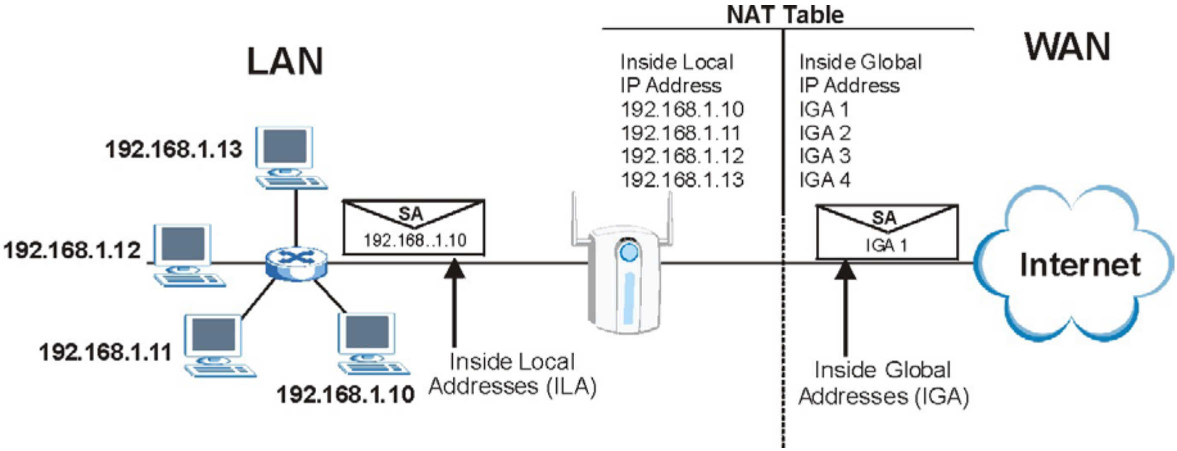
9.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyAIR filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

9.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyAIR keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.



NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

Figure 9-1 How NAT Works

9.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyAIR can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

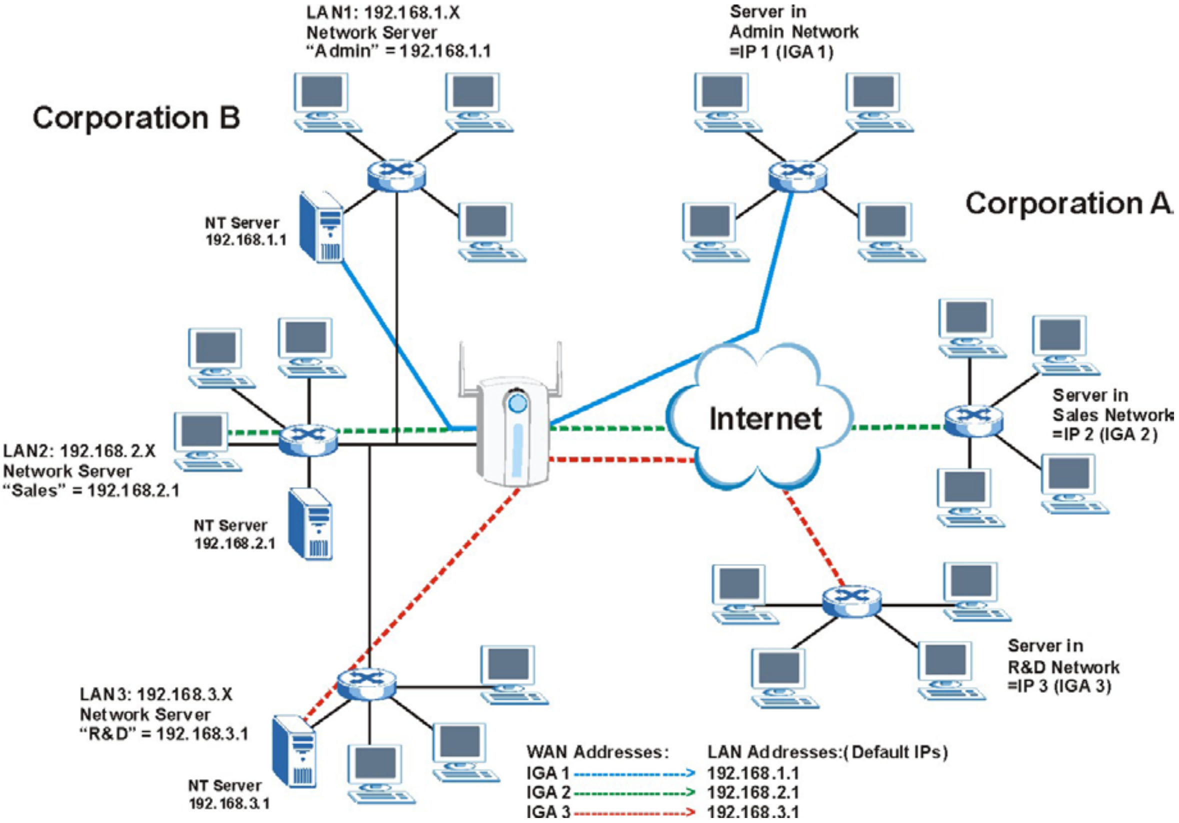


Figure 9-2 NAT Application with IP Alias

9.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyAIR maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyAIR maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyAIR maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyAIR maps each local IP address to a unique global IP address.

- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do not change for One-to-One and Many-One-to-One NAT mapping types.

The following table summarizes these types.

Table 9-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1-1

Many-to-One (SUA/PAT)	ILA1←→ IGA1
	ILA2←→ IGA1
	…
		M-1

Many-to-Many Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA1
	ILA4←→ IGA2
	…
		M-M Ov

Many-One-to-One	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		M-1-1

Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

9.1.6 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyAIR also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

9.2 SUA Server

An SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a Default Server **IP address, the ZyAIR discards all packets received for ports that are not specified here or in the remote management setup.**

9.2.1 Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

Table 9-3 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119

Table 9-3 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

9.2.2 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server, port 80 to another (A in the example) and assign a default server IP address of 192.168.1.35 to a third (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet

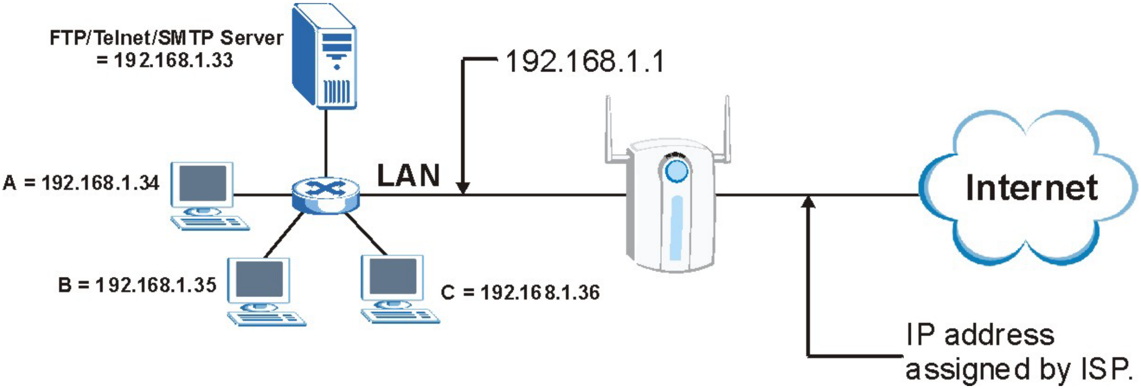


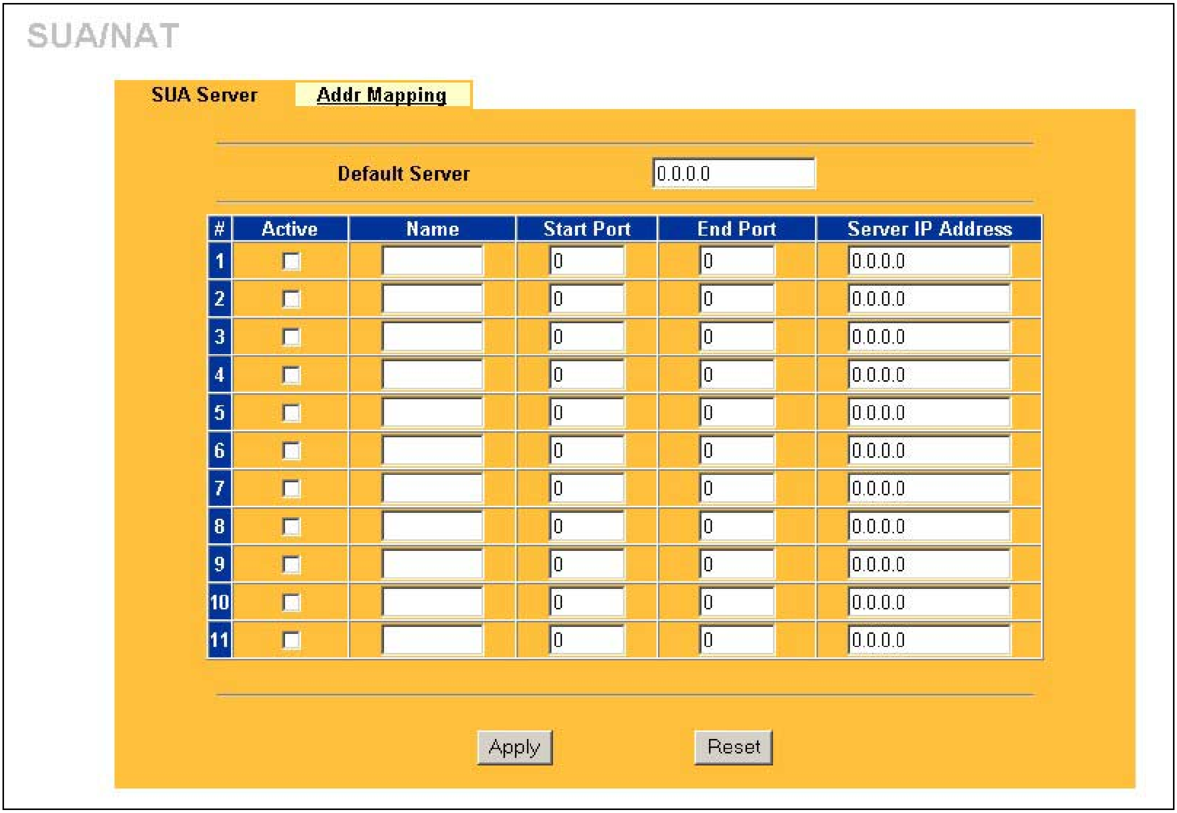
Figure 9-3 Multiple Servers Behind NAT Example

9.3 Configuring SUA Server

If you do not assign a Default Server **IP address, the ZyAIR discards all packets received for ports that are not specified here or in the remote management setup.**

Click **ADVANCED** and then **SUA/NAT** to open the **SUA Server** screen.

Refer to the *Table 9-3* for port numbers commonly used for particular services.



Default Server: 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	□		0	0	0.0.0.0
2	□		0	0	0.0.0.0
3	□		0	0	0.0.0.0
4	□		0	0	0.0.0.0
5	□		0	0	0.0.0.0
6	□		0	0	0.0.0.0
7	□		0	0	0.0.0.0
8	□		0	0	0.0.0.0
9	□		0	0	0.0.0.0
10	□		0	0	0.0.0.0
11	□		0	0	0.0.0.0

Figure 9-4 SUA/NAT Setup

The following table describes the labels in this screen.

Table 9-4 SUA/NAT Setup

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen.
#	This field displays the number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.

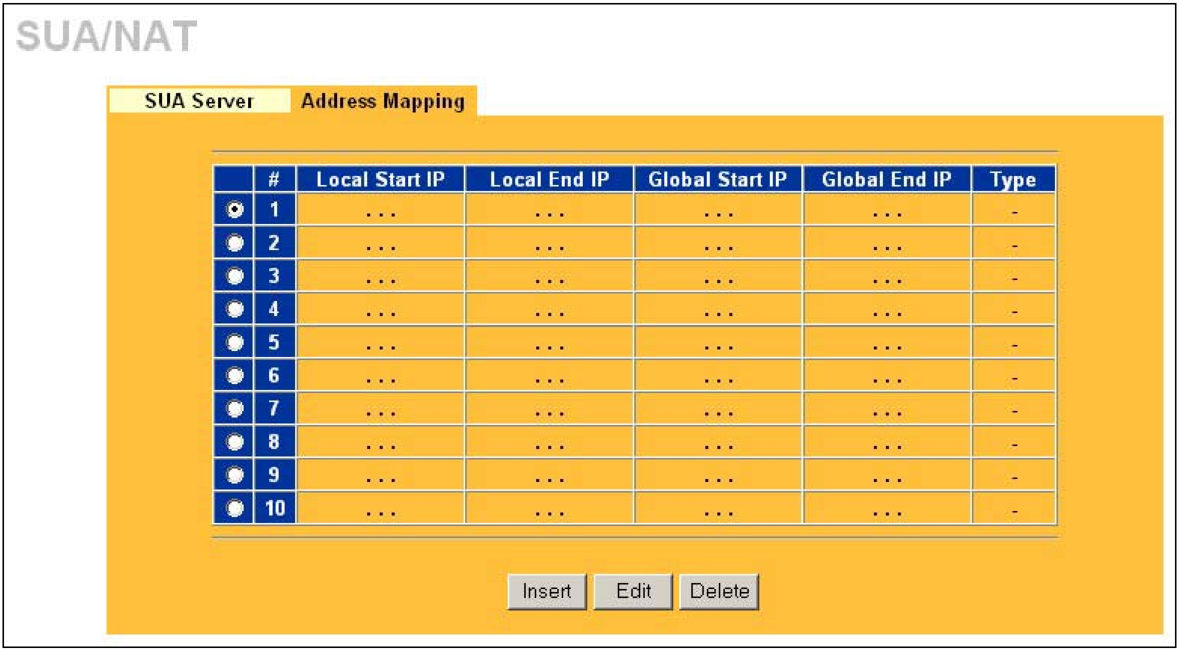
Table 9-4 SUA/NAT Setup

LABEL	DESCRIPTION
Start Port End Port	Enter a port number here. To forward only one port, enter the port number in the **Start Port** field and then type it again in the **End Port** field. To specify a range of ports, enter the start port number in the **Start Port** field and the last port to be forwarded in the **End Port** field.
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 Configuring Address Mapping

Ordering your rules is important because the ZyAIR applies the rules in the order that you specify. When a rule matches the current packet, the ZyAIR takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyAIR's address mapping settings, click **ADVANCED**, **SUA/NAT** and then the **Address Mapping** tab. The screen appears as shown.



	#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
◉	1	...	...	...	...	-
○	2	...	...	...	...	-
○	3	...	...	...	...	-
○	4	...	...	...	...	-
○	5	...	...	...	...	-
○	6	...	...	...	...	-
○	7	...	...	...	...	-
○	8	...	...	...	...	-
○	9	...	...	...	...	-
○	10	...	...	...	...	-

Figure 9-5 Address Mapping

The following table describes the labels in this screen.

Table 9-5 Address Mapping

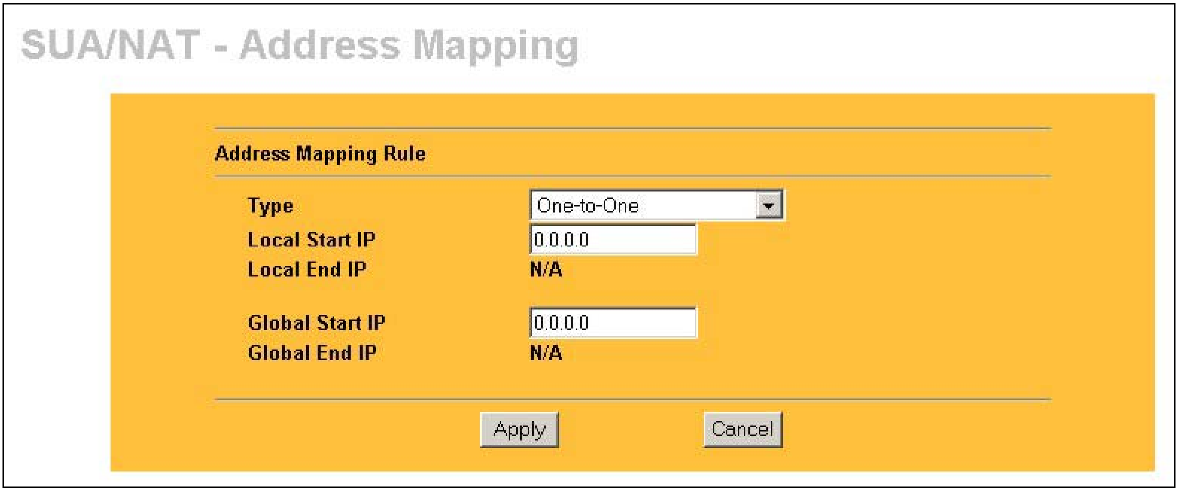
LABEL	DESCRIPTION
#	This field displays the index number of the address mapping rule.
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	Choose the port mapping type from the drop down list.

Table 9-5 Address Mapping

LABEL	DESCRIPTION
Insert	Click **Insert** to insert a new mapping rule before an existing one.
Edit	Click **Edit** to go to the **Address Mapping Rule** screen.
Delete	Click **Delete** to delete an address mapping rule.

9.4.1 Configuring Address Mapping Rule

To edit an address mapping rule, click the **Edit** button to display the screen shown next.



SUA/NAT - Address Mapping

Address Mapping Rule

Type	One-to-One
Local Start IP	0.0.0.0
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A

Figure 9-6 Address Mapping Rule

The following table describes the labels in this screen.

Table 9-6 Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from the drop down list.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.

Table 9-6 Address Mapping Rule

LABEL	DESCRIPTION
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Cancel	Click **Cancel** to exit this screen without saving.

Chapter 10
Static Route

This chapter shows you how to configure static routes for your ZyAIR.

10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyAIR has no knowledge of the networks beyond. For instance, the ZyAIR knows about network N2 in the following figure through remote node Router 1. However, the ZyAIR is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyAIR about the networks beyond the remote nodes.

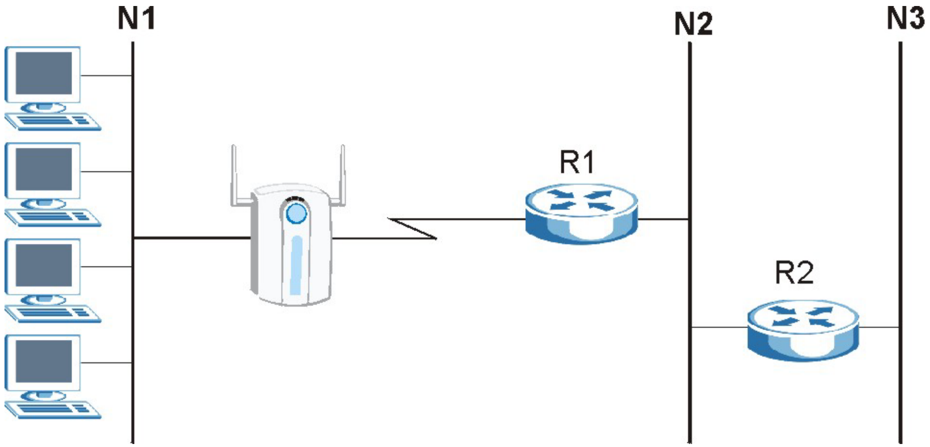
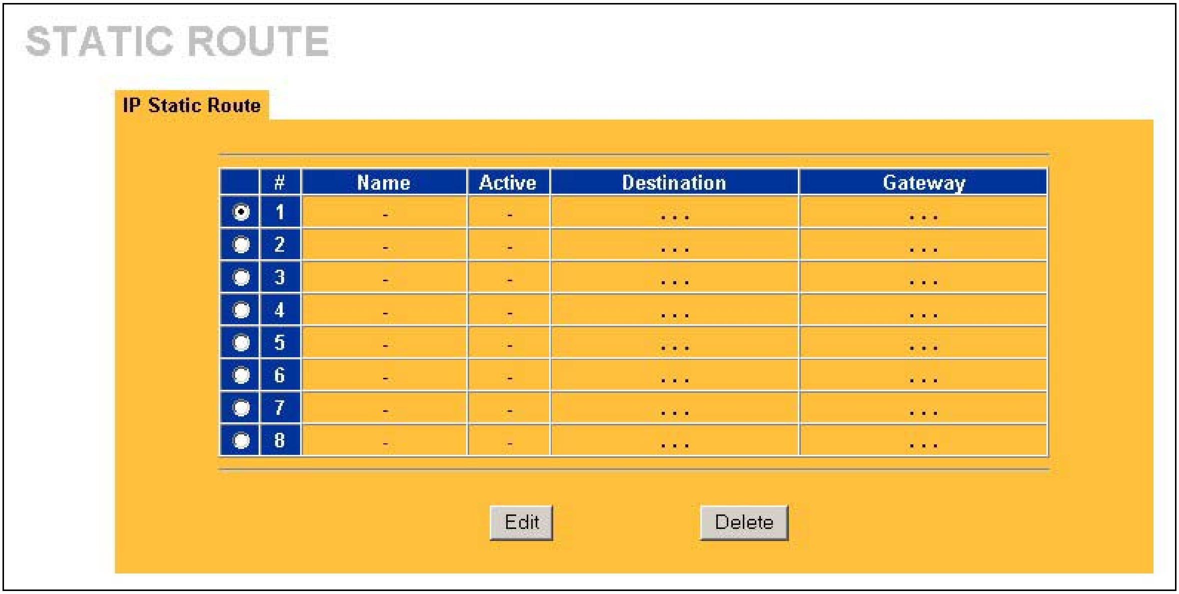


Figure 10-1 Example of Static Routing Topology

10.2 Configuring IP Static Route

Click **ADVANCED** and then **STATIC ROUTE** to open the screen shown next.



	#	Name	Active	Destination	Gateway
●	1	-	-	...	...
○	2	-	-	...	...
○	3	-	-	...	...
○	4	-	-	...	...
○	5	-	-	...	...
○	6	-	-	...	...
○	7	-	-	...	...
○	8	-	-	...	...

Figure 10-2 IP Static Route Summary

The following table describes the labels in this screen.

Table 10-1 IP Static Route Summary

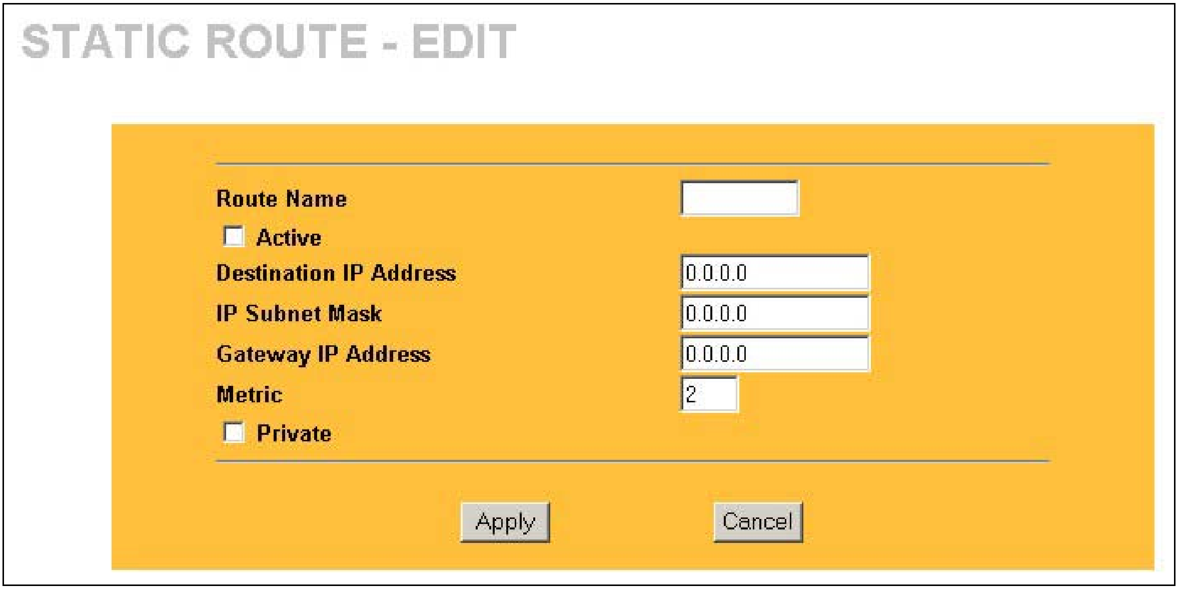
LABEL	DESCRIPTION
#	This field displays an individual static route index number.
Name	This field displays the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	To set up a static route on the ZyAIR, click the radio button next to the static route index number you want to configure, then click **Edit** to go to the **Static Route -Edit** screen.

Table 10-1 IP Static Route Summary

LABEL	DESCRIPTION
Delete	To remove a static route on the ZyAIR, click the radio button next to the static route index number you want to remove, then click **Delete**.

10.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.



STATIC ROUTE - EDIT

Route Name	
□ Active	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Metric	2
□ Private	

Figure 10-3 Edit IP Static Route

The following table describes the labels in this screen.

Table 10-2 Edit IP Static Route

LABEL	DESCRIPTION
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	Select this check box to activate this static route.

Table 10-2 Edit IP Static Route

LABEL	DESCRIPTION
Destination IP Address	Type the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the IP subnet mask here.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Type a number that approximates the cost for this link. Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If this check box is selected, this route is kept private and not included in RIP broadcast. If it is not selected, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Cancel	Click **Cancel** to exit this screen without saving.

Part V:

FIREWALL AND REMOTE MANAGEMENT

This part introduces firewalls in general and the ZyAIR firewall. It also explains custom ports and gives example firewall rules and information on Remote Management.

Chapter 11
Introduction to Firewalls

This chapter gives some background information on firewalls and introduces the ZyAIR firewall. This chapter is not applicable to the ZyAIR B-2000.

11.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

11.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

11.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

11.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

11.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See *section 11.5* for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

11.3 Introduction to ZyXEL's Firewall

The ZyAIR firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyAIR's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyAIR can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyAIR also has packet-filtering capabilities.

11.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyAIR is pre-configured to automatically detect and thwart all known DoS attacks.

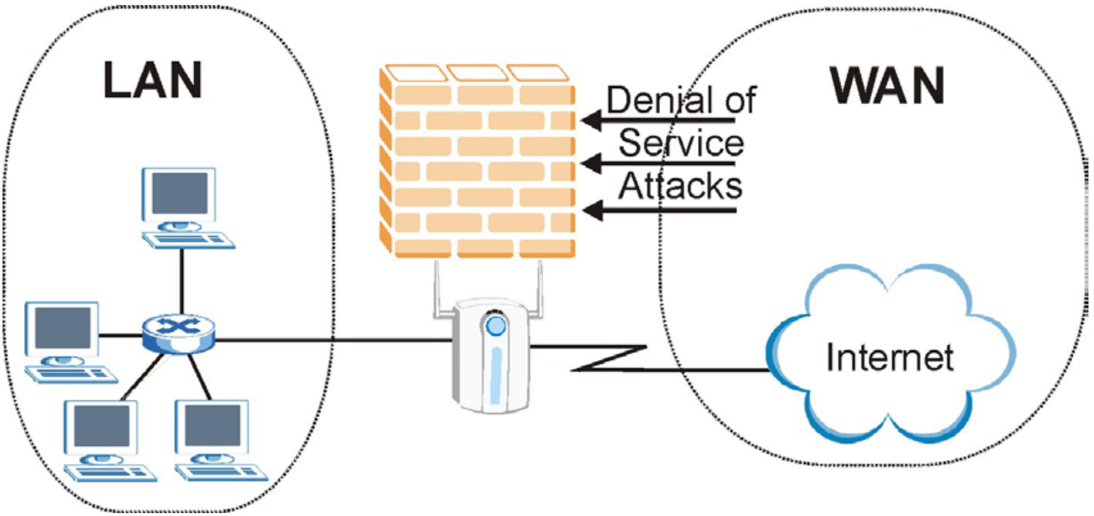


Figure 11-1 Firewall Application

11.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 11-1 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

11.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

   1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

   1-b Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

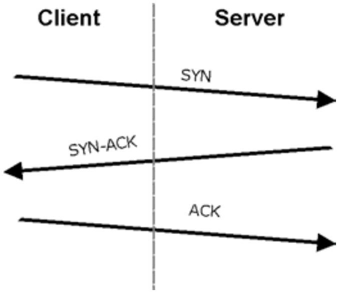


Figure 11-2 Three-Way Handshake

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

2-a **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

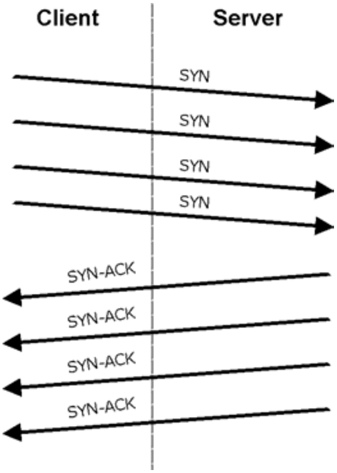


Figure 11-3 SYN Flood

2-b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

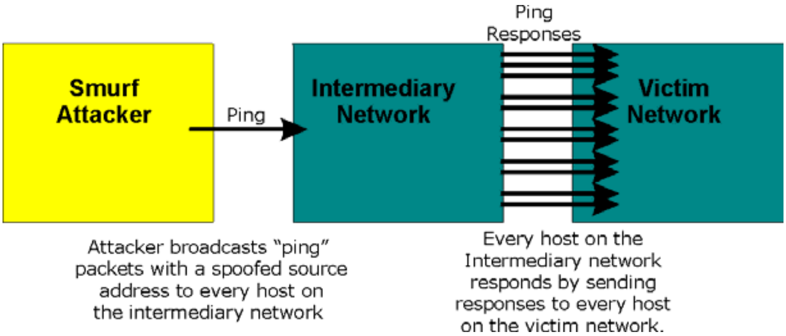

Smurf Attacker
Ping
Intermediary Network
Ping Responses
Victim Network
Attacker broadcasts "ping" packets with a spoofed source address to every host on the intermediary network
Every host on the Intermediary network responds by sending responses to every host on the victim network.

Figure 11-4 Smurf Attack

- ❑ ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 11-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- ❑ Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 11-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 11-4 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

❑ Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyAIR blocks all IP Spoofing attempts.

11.5 Stateful Inspection

Stateful inspection means the ZyAIR records packet information, such as port number and source/destination addresses and then allows or denies the response depending on your firewall rules.

The default rules allow LAN-to-WAN traffic and deny traffic initiated from WAN-to-LAN.

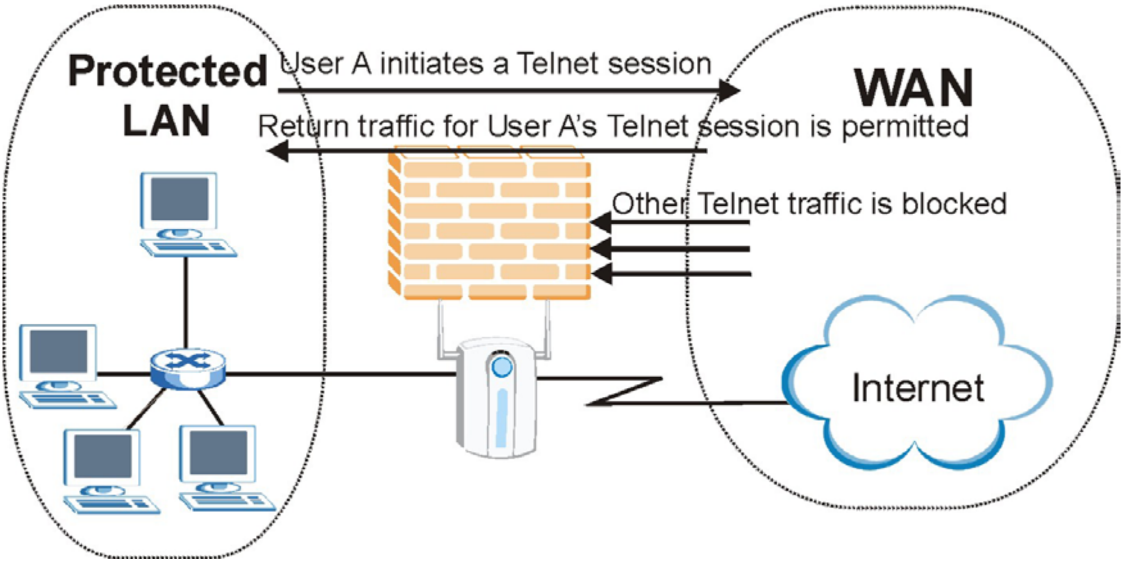

Protected LAN
User A initiates a Telnet session
Return traffic for User A's Telnet session is permitted
WAN
Other Telnet traffic is blocked
Internet

Figure 11-5 Stateful Inspection

The previous figure shows the ZyAIR's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

Chapter 12
Firewall Screens

This chapter shows you how to configure your ZyAIR firewall. This chapter is not applicable to the ZyAIR B-2000.

12.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyAIR has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall.

12.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ZyAIR
- LAN to WAN
- WAN to LAN
- WAN to WAN/ZyAIR

By default, the ZyAIR's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyAIR

  This allows computers on the LAN to manage the ZyAIR and communicate between networks or subnets connected to the LAN interface.

- LAN to WAN

By default, the ZyAIR's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyAIR

  This prevents computers on the WAN from using the ZyAIR as a gateway to communicate with other computers on the WAN and/or managing the ZyAIR.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyAIR's default rules.

12.3 Rule Logic Overview

Study these points carefully before configuring rules.

12.3.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to (refer to *12.2*)?
4. What IP services will be affected?
5. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.3.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

12.3.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 12.6.3* for more information on predefined services.

12.4 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

12.5 Connection Direction Examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ZyAIR and WAN to WAN/ZyAIR rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/ZyAIR means policies for LAN-to-ZyAIR (the policies for managing the ZyAIR through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN).

12.5.1 LAN to WAN Rules

LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

How can you block certain LAN to WAN traffic?

You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are "higher priority logs" that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/ZyAIR means the LAN to the ZyAIR LAN interface. This is always allowed, as this is how you manage the ZyAIR from your local computer.

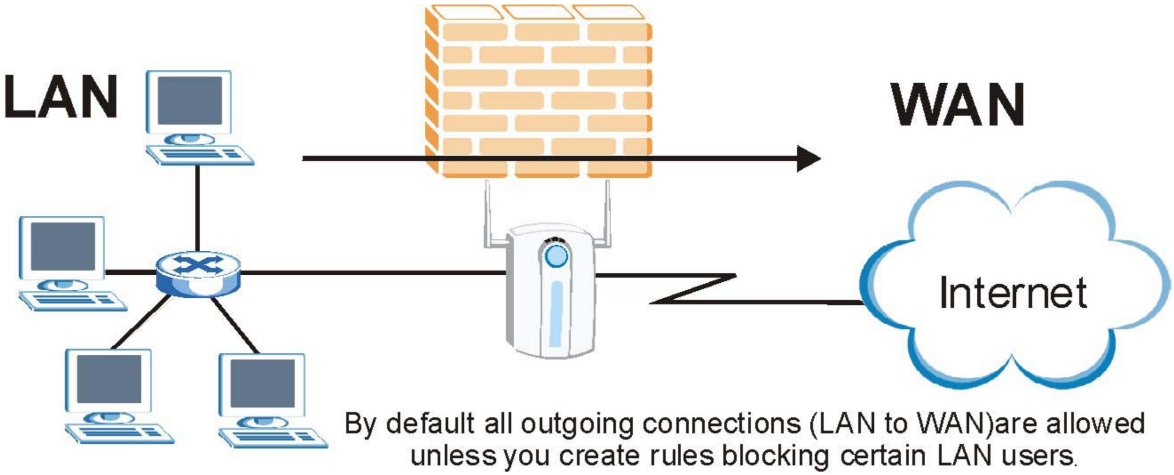

LAN
WAN
Internet
By default all outgoing connections (LAN to WAN)are allowed unless you create rules blocking certain LAN users.

Figure 12-1 LAN to WAN Traffic

12.5.2 WAN to LAN Rules

WAN-to-LAN rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/ZyAIR firewall rules. WAN-to-WAN/ZyAIR firewall rules are Internet to the ZyAIR WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what WAN-to-LAN and WAN-to-WAN/ZyAIR packets to log.
- Allow NetBIOS traffic from the WAN to the LAN using the **WAN IP** web screen or SMT menu 24.8 commands.

Forwarded **WAN-to-LAN** packets are not considered alerts.

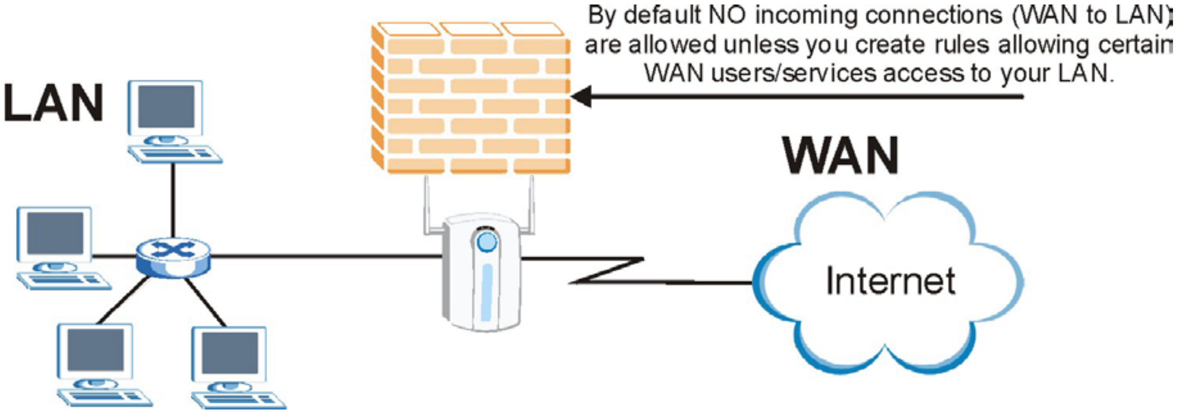

By default NO incoming connections (WAN to LAN)
are allowed unless you create rules allowing certain
WAN users/services access to your LAN.
LAN
WAN
Internet

Figure 12-2 WAN to LAN Traffic

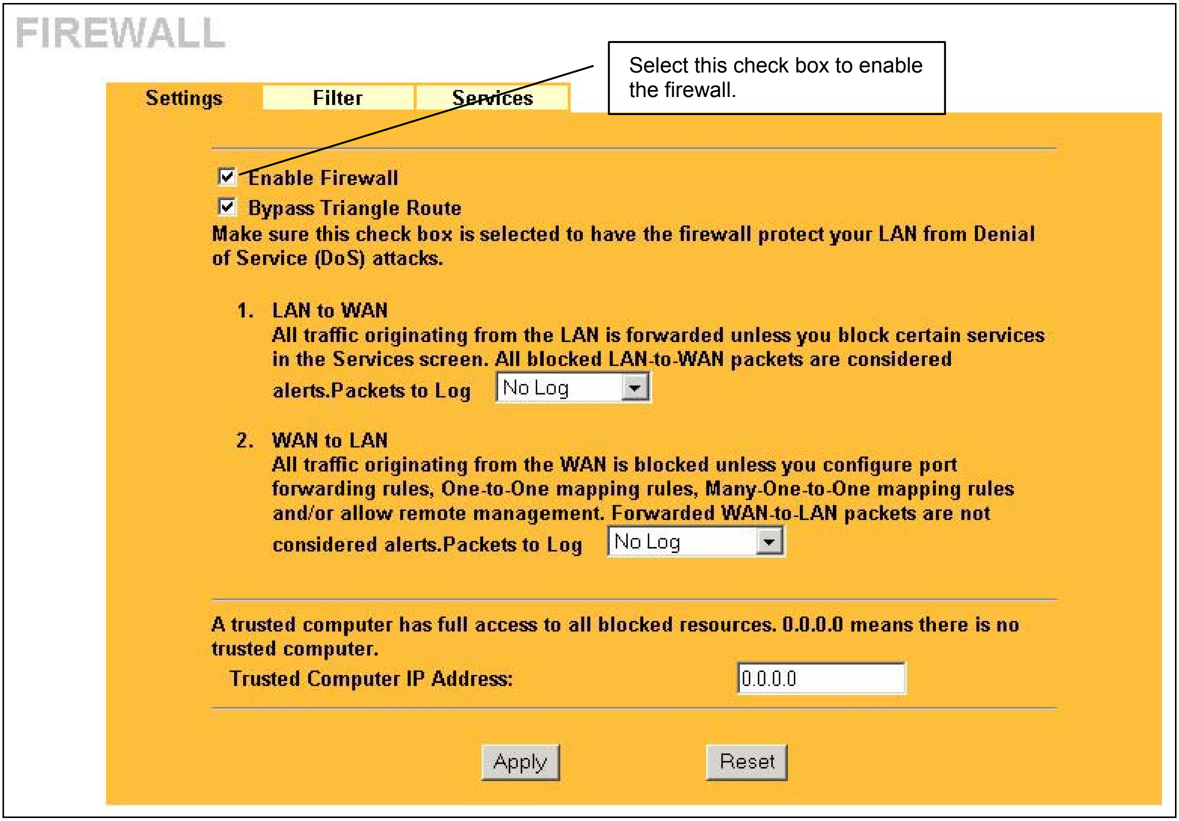
12.6 Enabling Firewall

The ordering of your rules is very important as rules are applied in turn.

The default rules allow LAN-to-WAN traffic and deny traffic initiated from WAN-to-LAN. You may block traffic initiated from the LAN by configuring blocked services in the **Services** screen. You may allow traffic initiated from the WAN by configuring port-forwarding rules, one-to-one/many one-to-one mapping rules and/or allow remote management.

The firewall is automatically enabled when you configure blocked services. When you configure a remote management menu to allow access to the ZyAIR, a firewall rule (WAN-to-WAN) is automatically created.

Click **ADVANCED** and **FIREWALL** to open the **Settings** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.



Select this check box to enable the firewall.

☑ Enable Firewall

☑ Bypass Triangle Route

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. LAN to WAN
   All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts.Packets to Log No Log
2. WAN to LAN
   All traffic originating from the WAN is blocked unless you configure port forwarding rules, One-to-One mapping rules, Many-One-to-One mapping rules and/or allow remote management. Forwarded WAN-to-LAN packets are not considered alerts.Packets to Log No Log

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

Figure 12-3 Firewall Settings

The following table describes the labels in this screen.

Table 12-1 Firewall Settings

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyAIR performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyAIR firewall ignore the use of triangle route topology on the network. See the appendix for more on triangle route topology.
LAN to WAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.

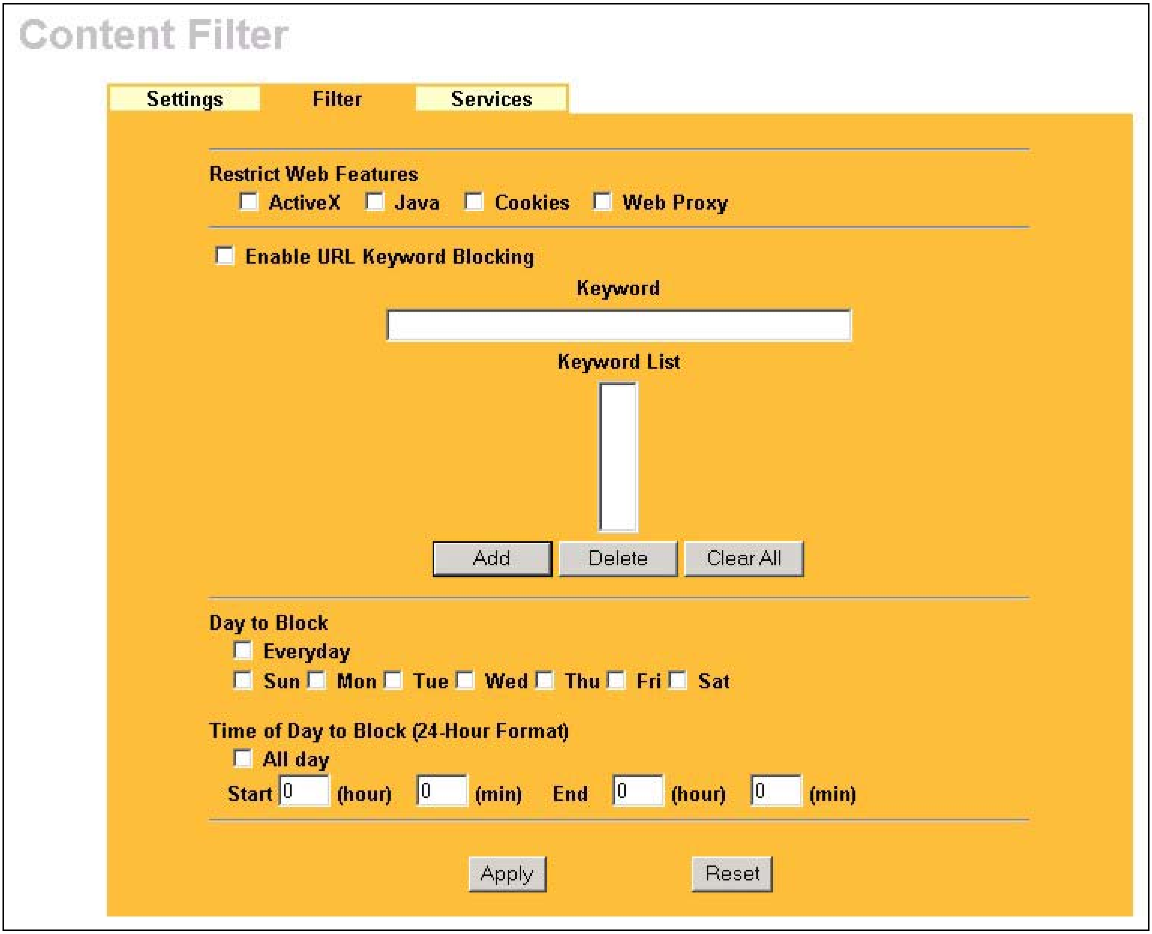
Table 12-1 Firewall Settings

LABEL	DESCRIPTION
Packets to Log	Choose what **LAN to WAN** packets to log. Choose from: • **No Log** • **Log Blocked** (blocked LAN to WAN services appear in the **Blocked Services** textbox in the **Services** screen (with **Enable Services Blocking** selected)) • **Log All** (log all **LAN to WAN** packets)
WAN to LAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.
Packets to Log	Choose what **WAN to LAN** and WAN to WAN/ZyAIR packets to log. Choose from: • **No Log** • **Log Forwarded** • **Log All** (log all **WAN to LAN** packets).
Allow one specific computer full access to all blocked resources.	
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

12.6.1 Configuring Content Filtering

Content filtering allows you to block web sites by URL keywords that you specify, for example, you can block access to all web sites with the word "bad" in the URL by specifying "bad' as a keyword. You can also block access to web proxies and pages containing Active X components, Java applets and cookies. Finally you can schedule when the ZyAIR performs content filtering by day and time.

Click **ADVANCED**, **FIREWALL** and then the **Filter** tab to open the **Filter** screen.



Restrict Web Features
□ ActiveX □ Java □ Cookies □ Web Proxy

□ Enable URL Keyword Blocking

Keyword

Keyword List

Day to Block
□ Everyday
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)
□ All day
Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Figure 12-4 Firewall Filter

The following table describes the labels in this screen.

Table 12-2 Firewall Filter

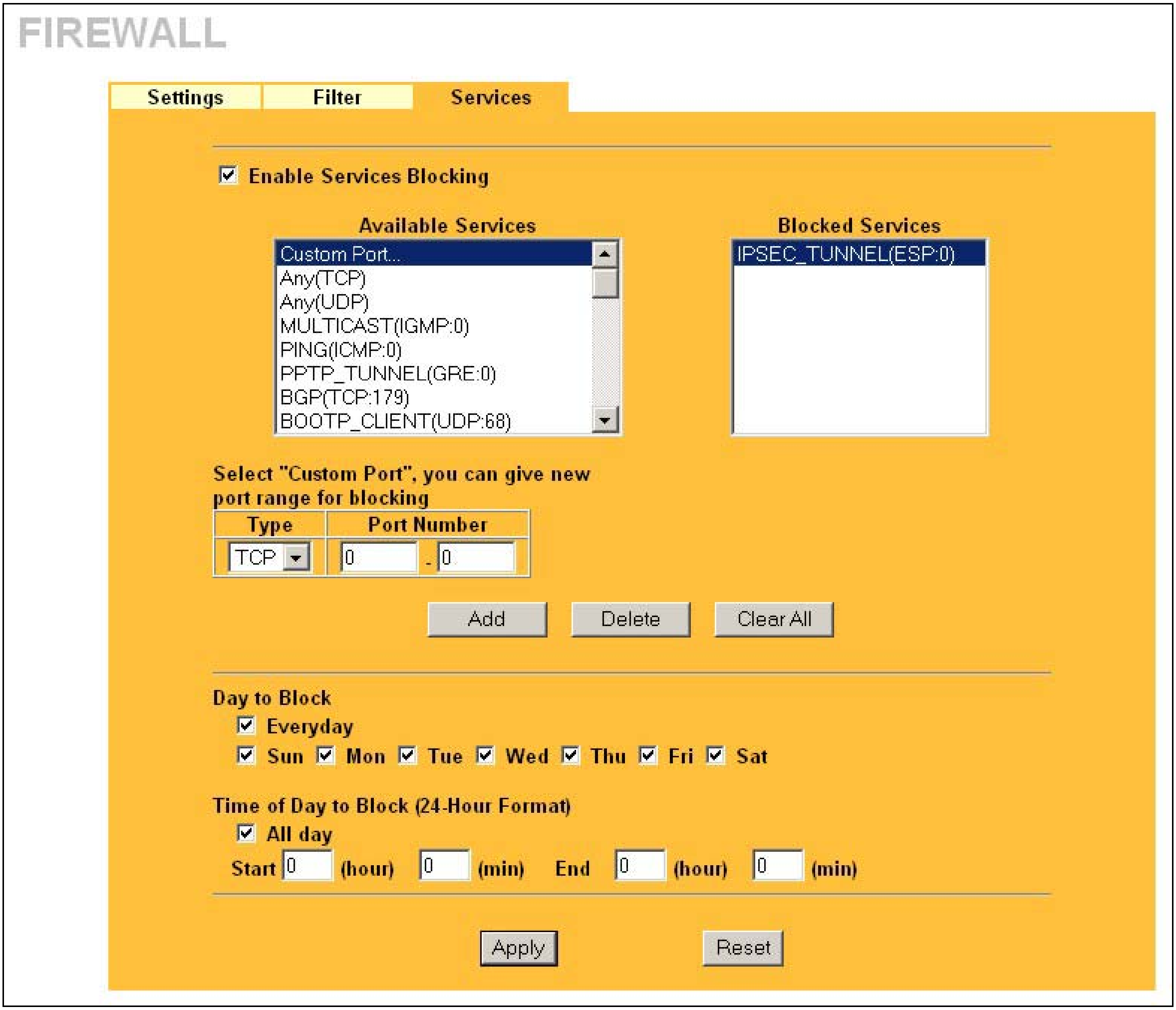
LABEL	DESCRIPTION
Restrict Web Features	Select the categories of web features that you want to restrict.

Table 12-2 Firewall Filter

LABEL	DESCRIPTION
ActiveX	ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Web servers that track usage and provide service based on ID use cookies.
Web Proxy	This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	Select this check box to block the URL containing the keywords in the keyword list
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Keyword List	This is a list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Add	Type a keyword in the **Keyword** field and click then **Add** to add a keyword to the **Keyword List**.
Delete	Select a keyword from the **Keyword List** and then click **Delete** to remove this keyword from the list.
Clear All	Click **Clear All** to empty the **Keyword List**.
Day to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to activate blocking.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to reload the previous configuration for this screen.

12.6.2 Configuring Firewall Services

Click **ADVANCED**, **FIREWALL** and then the **Services** tab to open the **Services** screen. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.



FIREWALL

☑ Enable Services Blocking

Available Services

- Custom Port...
- Any(TCP)
- Any(UDP)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)

Blocked Services

- IPSEC_TUNNEL(ESP:0)

Select "Custom Port", you can give new port range for blocking

Type	Port Number
TCP	0 - 0

Day to Block

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Block (24-Hour Format)

☑ All day

Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Figure 12-5 Firewall Services

The following table describes the labels in this screen.

Table 12-3 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Enable Services Blocking	Select the check box to activate service blocking.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Service** field. Please see *Table 12-4* for more information on services available
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port (**TCP**, **UDP** or **TCP**/**UDP**) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.
Type	Services are either **TCP** and/or **UDP**. Select from either **TCP** or **UDP**.
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the Blocked Service.
Delete	Select a service from the **Blocked Services List** and then click **Delete** to remove this service from the list.
Clear All	Click **Clear All** to empty the **Blocked Service**.
Day to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the **All Day** check box. You can also configure specific times that by entering the start time in the **Start (hr)** and **Start (min)** fields and the end time in the **End (hr)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to reload the previous configuration for this screen.

12.6.3 Predefined Services

The **Available Services** list box in the **Services** screen (see *Figure 12-5*) displays all predefined services that the ZyAIR already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 12-4 Predefined Services

SERVICE	DESCRIPTION
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME (TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
HTTP(TCP:80)	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.

Table 12-4 Predefined Services

SERVICE	DESCRIPTION
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 12-4 Predefined Services

SERVICE	DESCRIPTION
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

Chapter 13 Remote Management

This chapter provides information on the Remote Management screens. This chapter is not applicable to the ZyAIR B-2000.

13.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your ZyAIR from a remote location via:

- Internet (WAN only)
- LAN only,
- ALL (LAN and WAN)
- Neither (Disable).

When you Choose WAN only **or** ALL **(LAN & WAN), you still need to configure a firewall rule to allow access.**

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

You may only have one remote management session running at a time. The ZyAIR automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. Telnet
3. HTTP

13.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
5. There is a firewall rule that blocks it.

13.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

13.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyAIR automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen.

13.2 Telnet

You can telnet into the ZyAIR to perform remote management.

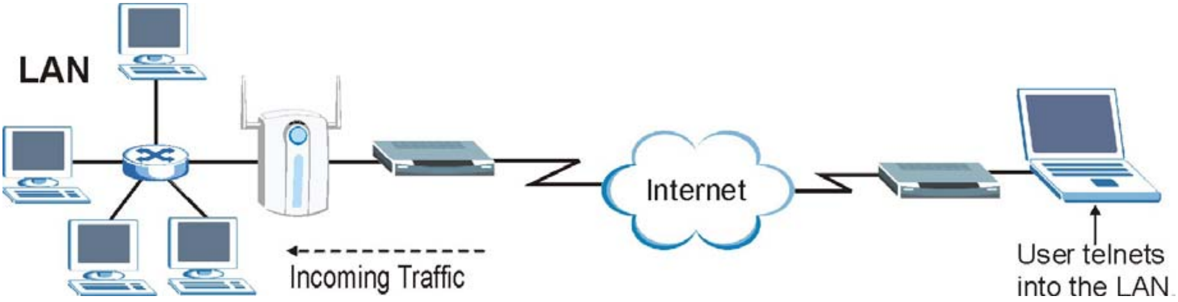
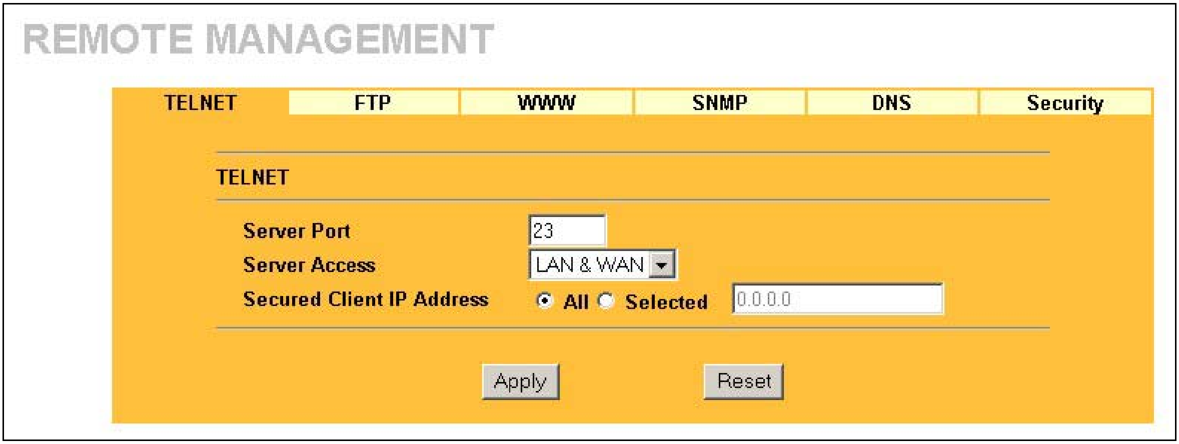


Figure 13-1 Telnet Configuration on a TCP/IP Network

13.3 Configuring TELNET

Click **ADVANCED** and then **REMOTE MGNT** to open the **TELNET** screen.



REMOTE MANAGEMENT

TELNET

Server Port: 23

Server Access: LAN & WAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 13-2 Telnet

The following table describes the labels in this screen.

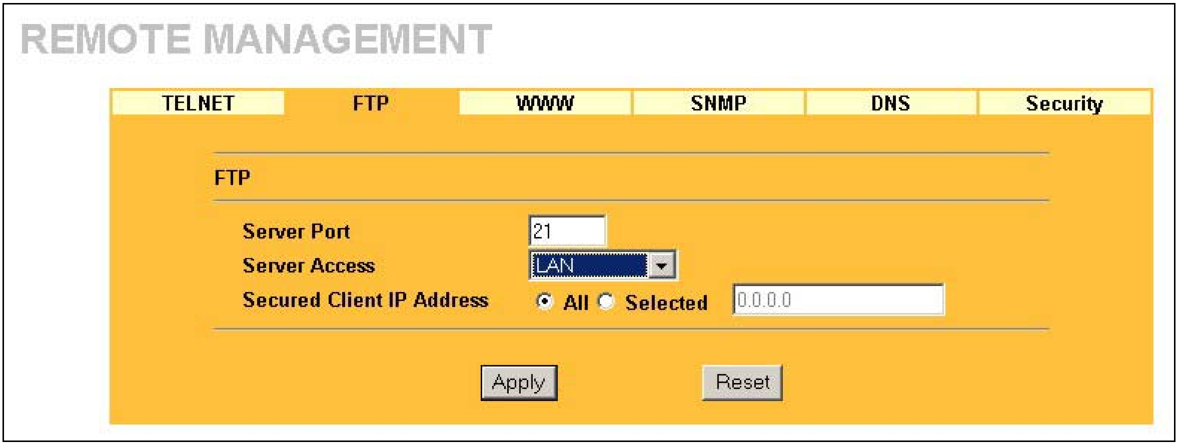
Table 13-1 Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select **All** to allow any computer to access the ZyAIR using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

13.4 Configuring FTP

You can upload and download the ZyAIR's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyAIR's FTP settings, click **ADVANCED**, **REMOTE MGNT** and then the **FTP** tab. The screen appears as shown.



FTP

Server Port: 21

Server Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 13-3 FTP

The following table describes the labels in this screen.

Table 13-2 FTP

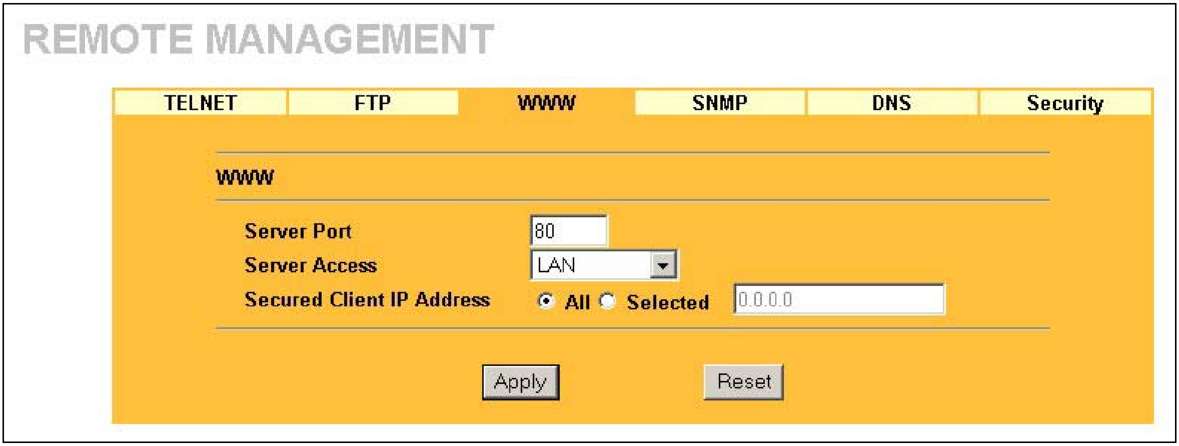
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select **All** to allow any computer to access the ZyAIR using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click **Apply** to save your changes back to the ZyAIR.

Table 13-2 FTP

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.

13.5 Configuring WWW

To change your ZyAIR's World Wide Web settings, click **ADVANCED**, **REMOTE MGNT** and then the **WWW** tab. The screen appears as shown.



WWW

Server Port 80

Server Access LAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

Figure 13-4 WWW

The following table describes the labels in this screen.

Table 13-3 WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.

Table 13-3 WWW

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select **All** to allow any computer to access the ZyAIR using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

13.6 Configuring 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.

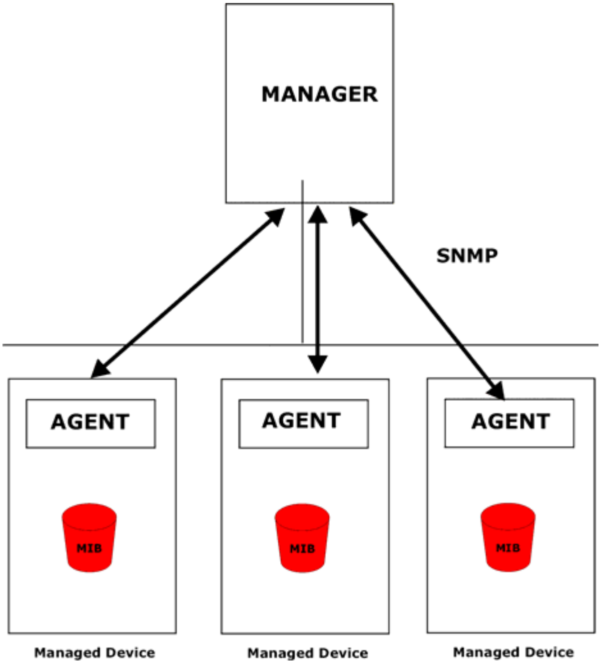


Figure 13-5 SNMP Management Model

An SNMP managed network consists of two main types of component: 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.

13.6.1 Supported MIBs

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

13.6.2 SNMP Traps

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

Table 13-4 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.

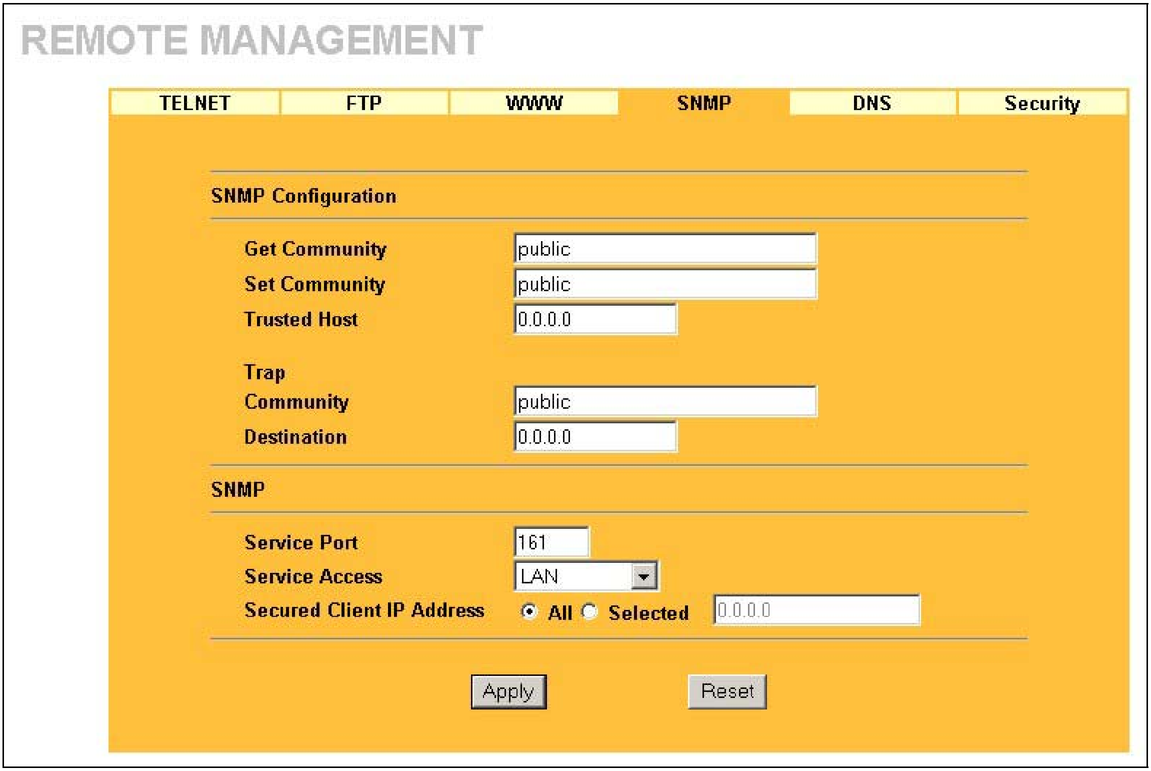
The following table maps the physical port and encapsulation to the interface type.

Table 13-5 Ports and Interface Types

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

13.6.3 REMOTE MANAGEMENT: SNMP

To change your ZyAIR’s SNMP settings, click **ADVANCED**, **REMOTE MGNT** and then the **SNMP** tab. The screen appears as shown.



SNMP Configuration

Get Community: public

Set Community: public

Trusted Host: 0.0.0.0

Trap

Community: public

Destination: 0.0.0.0

SNMP

Service Port: 161

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 13-6 SNMP

The following table describes the labels in this screen.

Table 13-6 SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.

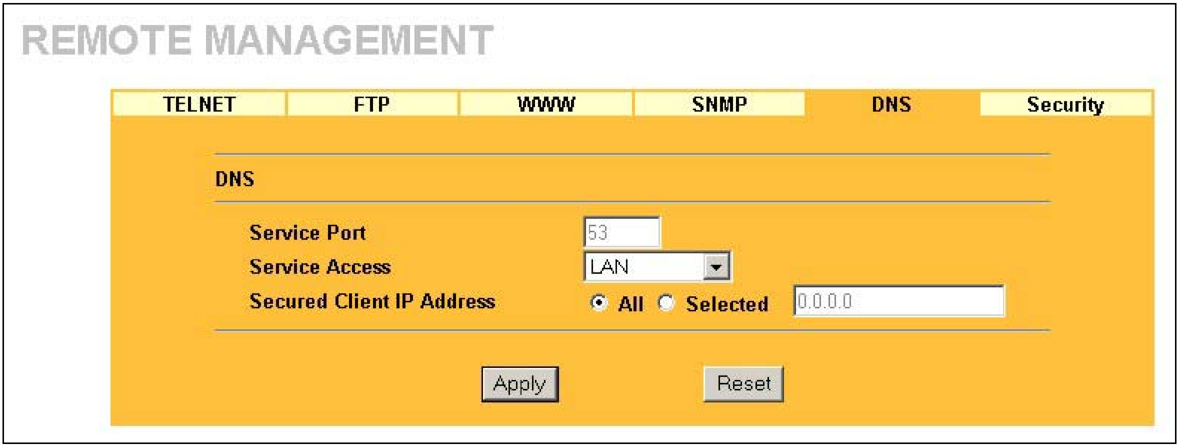
Table 13-6 SNMP

LABEL	DESCRIPTION
Set Community	Enter 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.
SNMP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select **All** to allow any computer to access the ZyAIR using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

13.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.zyxel.com is 204.217.0.2. Refer to the *Internet Access* chapter for more information.

To change your ZyAIR's DNS settings, click **ADVANCED**, **REMOTE MGNT** and then the **DNS** tab. The screen appears as shown.



REMOTE MANAGEMENT

DNS

Service Port: 53

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Figure 13-7 DNS

The following table describes the labels in this screen.

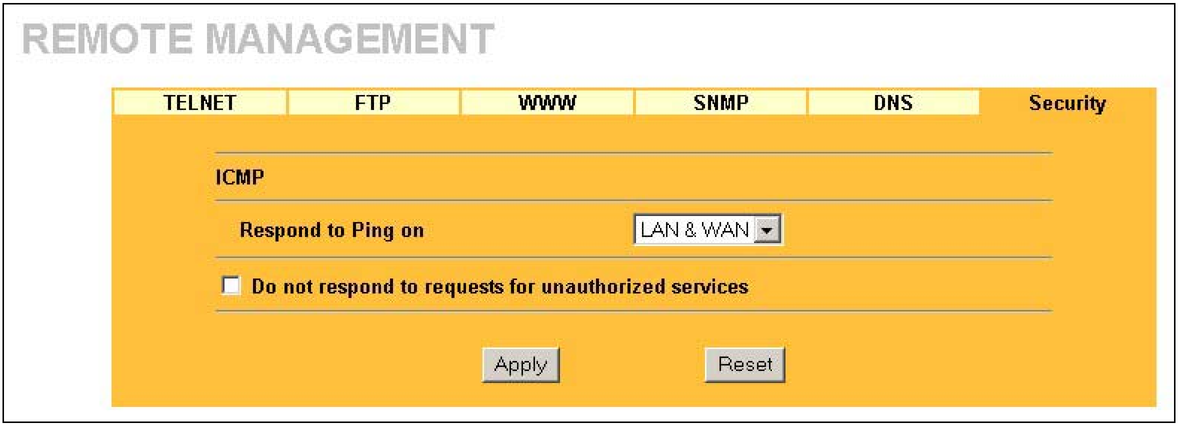
Table 13-7 DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the ZyAIR.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send DNS queries to the ZyAIR. Select **All** to allow any computer to send DNS queries to the ZyAIR. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyAIR.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

13.8 Configuring Security

To change your ZyAIR's security settings, click **ADVANCED**, **REMOTE MGNT** and then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyAIR, an ICMP response packet is automatically returned. This allows the outside user to know the ZyAIR exists. The ZyAIR series support anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyAIR when unsupported ports are probed.



Respond to Ping on: LAN & WAN

☐ Do not respond to requests for unauthorized services

Figure 13-8 Security

The following table describes the labels in this screen.

Table 13-8 Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyAIR will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN&WAN** to reply to both incoming LAN and WAN Ping requests.

Table 13-8 Security

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyAIR by probing for unused ports. If you select this option, the ZyAIR will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyAIR unseen. By default this option is not selected and the ZyAIR will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyAIR's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyAIR reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

Part VI:

UPNP AND LOGS

This part provides information and configuration instructions for UPnP (Universal Plug and Play) and the logs.

Chapter 14
UPnP Screen

This chapter introduces the Universal Plug and Play feature.

14.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

14.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

14.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *SUA/NAT* chapter for further information about NAT.

14.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

14.2 UPnP and ZyXEL

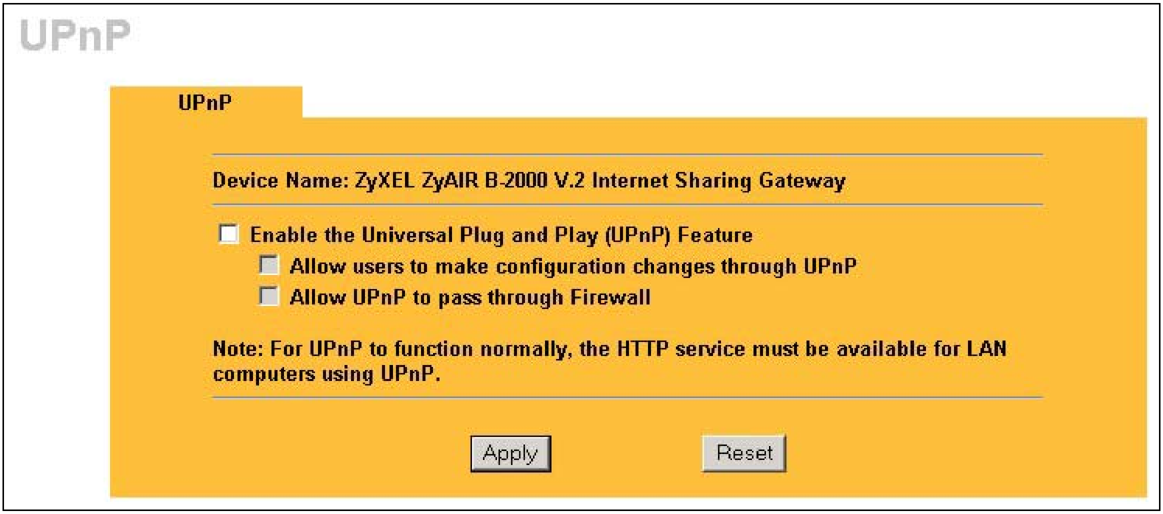
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

Please see your *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

14.3 Configuring UPnP

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



Device Name: ZyXEL ZyAIR B-2000 V.2 Internet Sharing Gateway

□ Enable the Universal Plug and Play (UPnP) Feature

□ Allow users to make configuration changes through UPnP

□ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Figure 14-1 Configuring UPnP

The following table describes the labels in this screen.

Table 14-1 Configuring UPnP

LABEL	DESCRIPTION
Device Name (or UPnP Name)	This identifies the ZyAIR in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyAIR's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyAIR so that they can communicate through the ZyAIR, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Table 14-1 Configuring UPnP

LABEL	DESCRIPTION
Allow UPnP to pass through Firewall	Select this check box to create a static LAN to LAN/ZyAIR rule that allows forwarding of ports 1900 and 80. Selecting this check box also creates a dynamic firewall rule every time a NAT forwarding port is reserved for UPnP. This setting remains active until you disable UPnP or clear this check box. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets) instead of creating a firewall rule for them.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

14.4 Installing UPnP in Windows Example

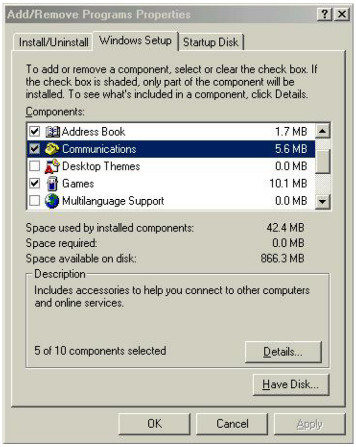
This section shows how to install UPnP in Windows Me and Windows XP.

14.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

Step 1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

Step 2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



Add/Remove Programs Properties

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Address Book	1.7 MB
☑ Communications	5.6 MB
☐ Desktop Themes	0.0 MB
☑ Games	10.1 MB
☐ Multilanguage Support	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

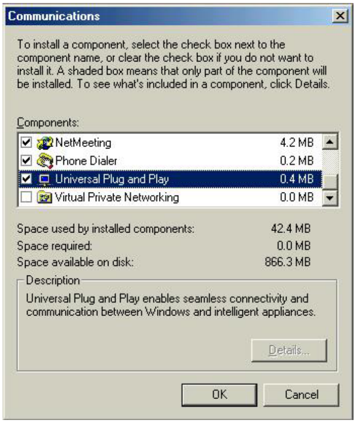
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

Step 3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Step 4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

Step 5. Restart the computer when prompted.



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ NetMeeting	4.2 MB
☑ Phone Dialer	0.2 MB
☑ Universal Plug and Play	0.4 MB
☐ Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

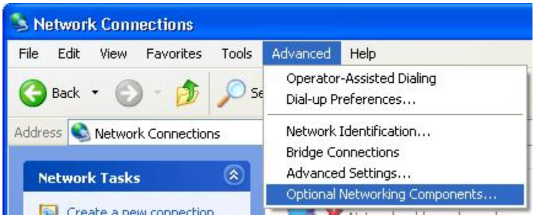
14.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

Step 1. Click **Start** and **Control Panel**.

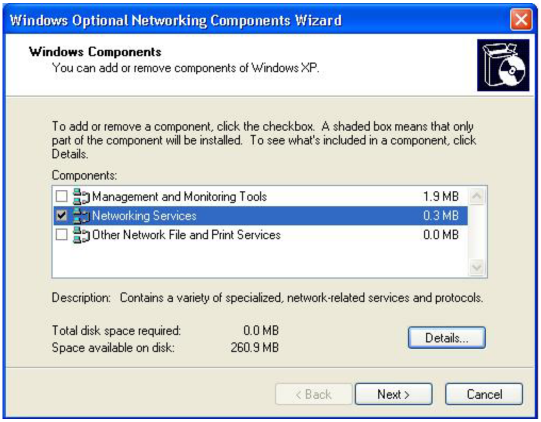
Step 2. Double-click **Network Connections**.

Step 3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components** ….
The **Windows Optional Networking Components Wizard** window displays.



Network Connections
File Edit View Favorites Tools Advanced Help
Back
Se
Address Network Connections
Network Tasks
Create a new connection
Operator-Assisted Dialing
Dial-up Preferences...
Network Identification...
Bridge Connections
Advanced Settings...
Optional Networking Components...

Step 4. Select **Networking Service** in the **Components** selection box and click **Details**.



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

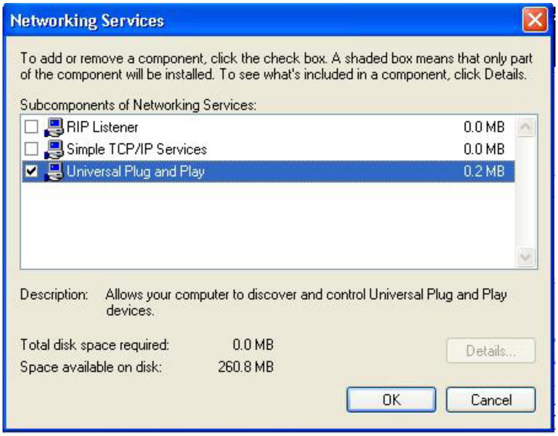
☐ Management and Monitoring Tools	1.9 MB
☑ Networking Services	0.3 MB
☐ Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

Step 5. In the **Networking Services** window, select the **Universal Plug and Play** check box.

Step 6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

14.5 Using UPnP in Windows XP Example

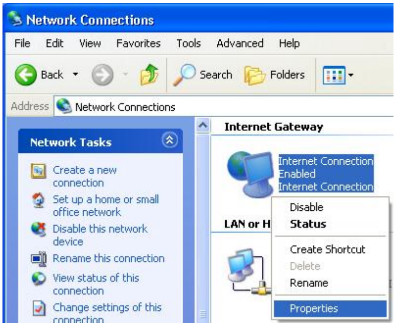
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyAIR.

Make sure the computer is connected to a LAN port of the ZyAIR. Turn on your computer and the ZyAIR.

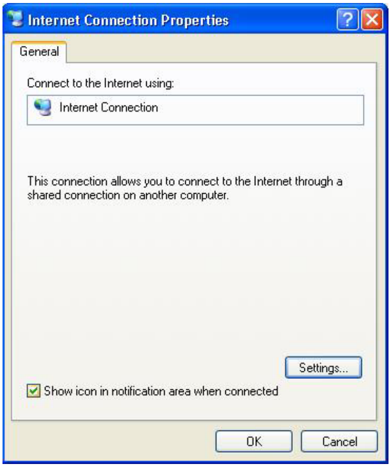
14.5.1 Auto-discover Your UPnP-enabled Network Device

Step 1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

Step 2. Right-click the icon and select **Properties**.



Step 3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.



Internet Connection Properties

General

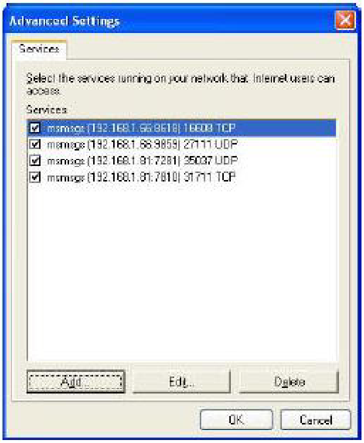
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

Step 4. You may edit or delete the port mappings or click **Add** to manually add port mappings.



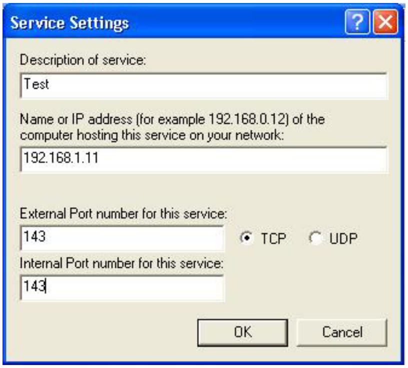
Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:9618) 16603 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP



Service Settings

Description of service:

Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:

192.168.1.11

External Port number for this service:

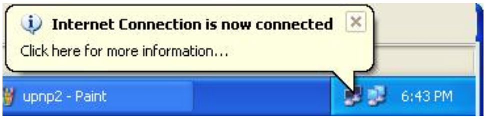
143 ● TCP ○ UDP

Internal Port number for this service:

143

When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

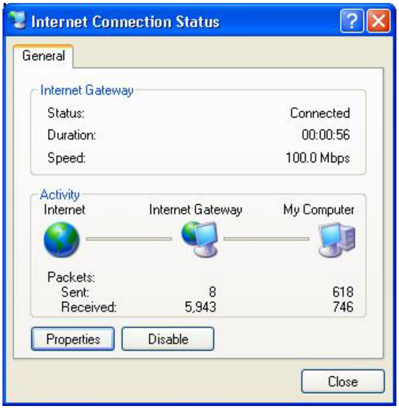
Step 5. Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



Internet Connection is now connected

Click here for more information...

Step 6. Double-click the icon to display your current Internet connection status.



Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

14.5.2 Web Configurator Easy Access

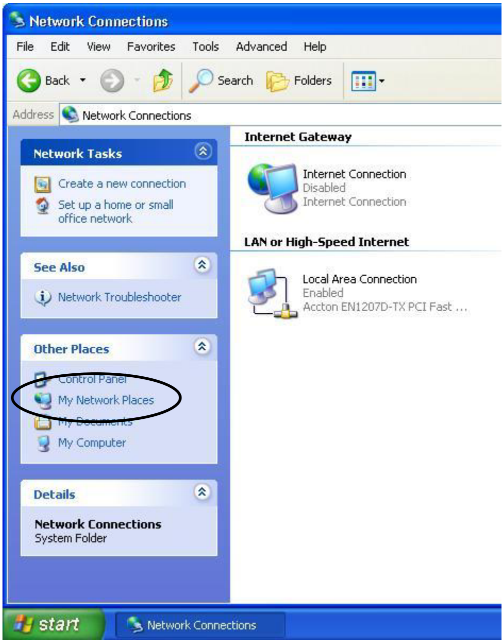
With UPnP, you can access the web-based configurator on the ZyAIR without finding out the IP address of the ZyAIR first. This is helpful if you do not know the IP address of the ZyAIR.

Follow the steps below to access the web configurator.

Step 1. Click **Start** and then **Control Panel**.

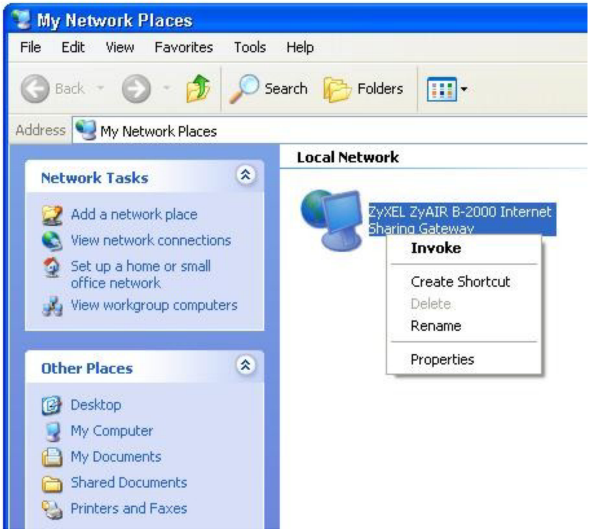
Step 2. Double-click **Network Connections**.

Step 3. Select **My Network Places** under **Other Places**.

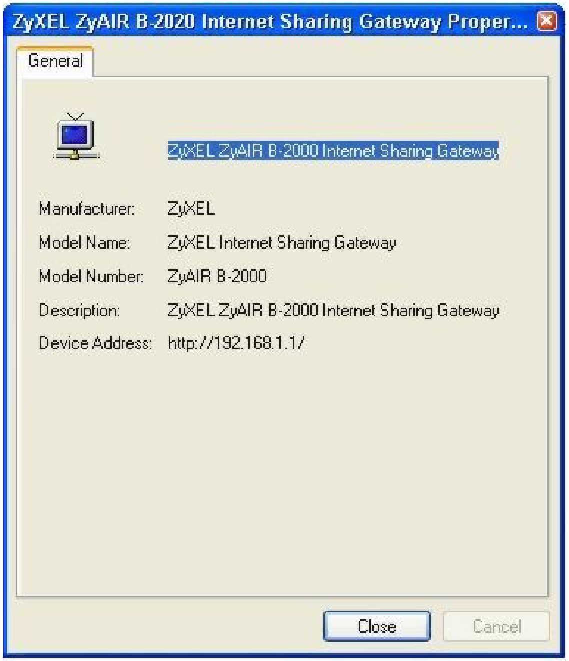


Step 4. An icon with the description for each UPnP-enabled device displays under **Local Network**.

Step 5. Right-click the icon for your ZyAIR and select **Invoke**. The web configurator login screen displays.



Step 6. Right-click the icon for your ZyAIR and select **Properties**. A properties window displays with basic information about the ZyAIR.



ZyXEL ZyAIR B-2020 Internet Sharing Gateway Proper...

ZyXEL ZyAIR B-2000 Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: ZyAIR B-2000

Description: ZyXEL ZyAIR B-2000 Internet Sharing Gateway

Device Address: http://192.168.1.1/

Chapter 15
Logs Screens

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

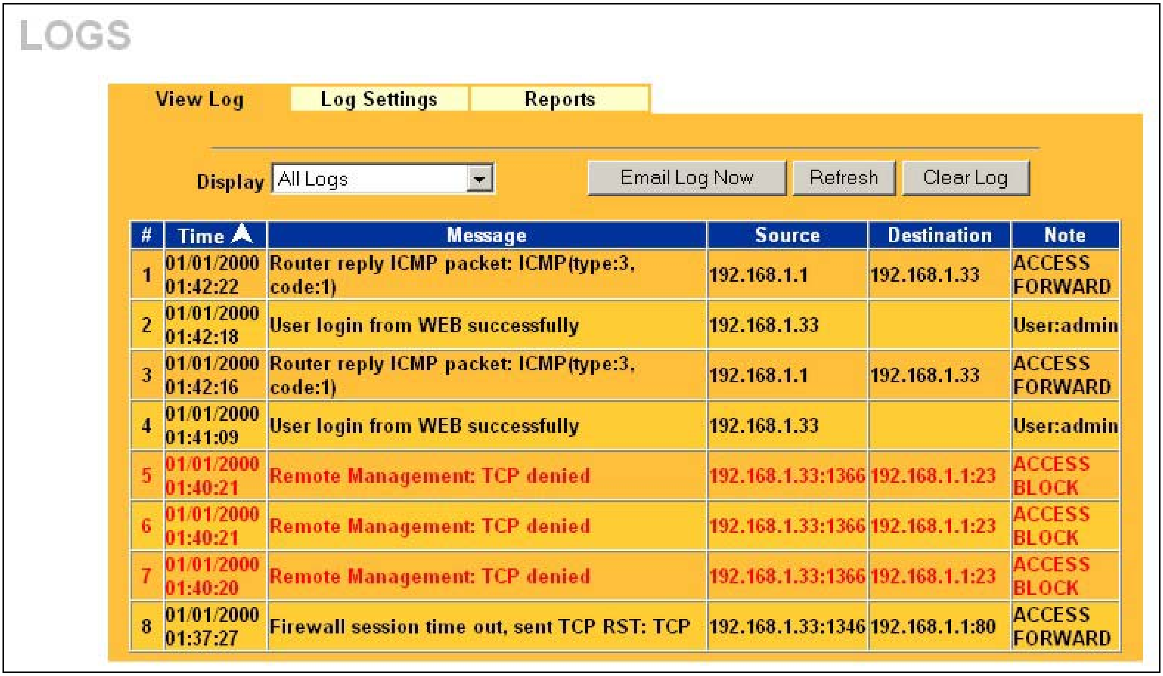
15.1 Using the View Log Screen

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

Click **ADVANCED** and then **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 15.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

You can view logs and alert messages in this page. Log entries in red indicate system error logs. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

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



#	Time	Message	Source	Destination	Note
1	01/01/2000 01:42:22	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
2	01/01/2000 01:42:18	User login from WEB successfully	192.168.1.33		User:admin
3	01/01/2000 01:42:16	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
4	01/01/2000 01:41:09	User login from WEB successfully	192.168.1.33		User:admin
5	01/01/2000 01:40:21	Remote Management: TCP denied	192.168.1.33:1366	192.168.1.1:23	ACCESS BLOCK
6	01/01/2000 01:40:21	Remote Management: TCP denied	192.168.1.33:1366	192.168.1.1:23	ACCESS BLOCK
7	01/01/2000 01:40:20	Remote Management: TCP denied	192.168.1.33:1366	192.168.1.1:23	ACCESS BLOCK
8	01/01/2000 01:37:27	Firewall session time out, sent TCP RST: TCP	192.168.1.33:1346	192.168.1.1:80	ACCESS FORWARD

Figure 15-1 View Log

The following table describes the labels in this screen.

Table 15-1 View Log

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

Table 15-1 View Log

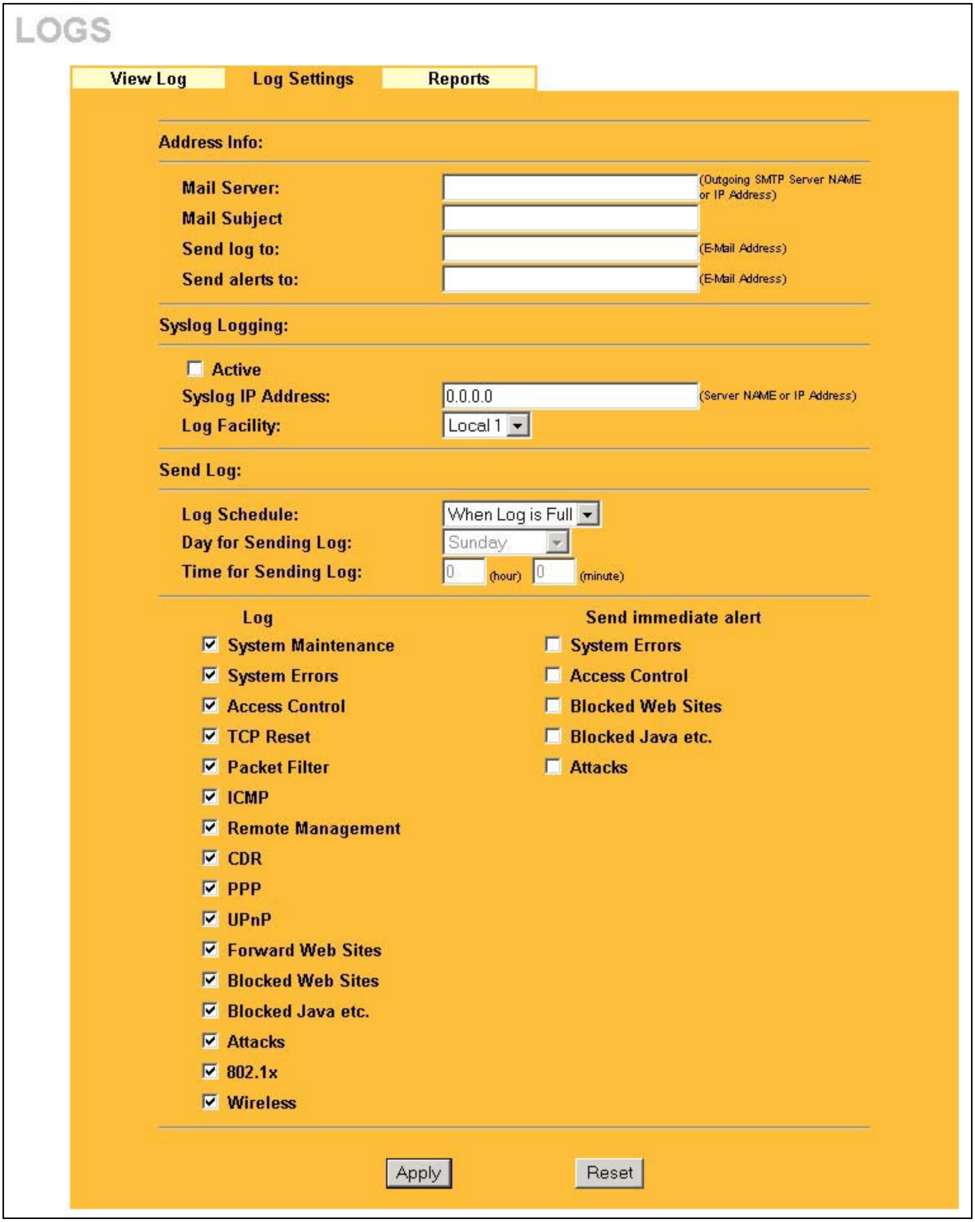
LABEL	DESCRIPTION
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

15.2 Configuring Log Settings

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

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

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, Active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.



LOGS

Address Info:

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

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

Syslog Logging:

□ Active

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

Log Facility: Local 1

Send Log:

Log Schedule: When Log is Full

Day for Sending Log: Sunday

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

Log	Send immediate alert
☑ System Maintenance	□ System Errors
☑ System Errors	□ Access Control
☑ Access Control	□ Blocked Web Sites
☑ TCP Reset	□ Blocked Java etc.
☑ Packet Filter	□ Attacks
☑ ICMP	
☑ Remote Management	
☑ CDR	
☑ PPP	
☑ UPnP	
☑ Forward Web Sites	
☑ Blocked Web Sites	
☑ Blocked Java etc.	
☑ Attacks	
☑ 802.1x	
☑ Wireless	

Figure 15-2 Log Settings

The following table describes the labels in this screen.

Table 15-2 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.
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. Alerts include system errors, attacks and attempted access to blocked web sites. 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 Server 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: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None.** If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.

Table 15-2 Log Settings

LABEL	DESCRIPTION
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record.
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 changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

15.3 Configuring Reports

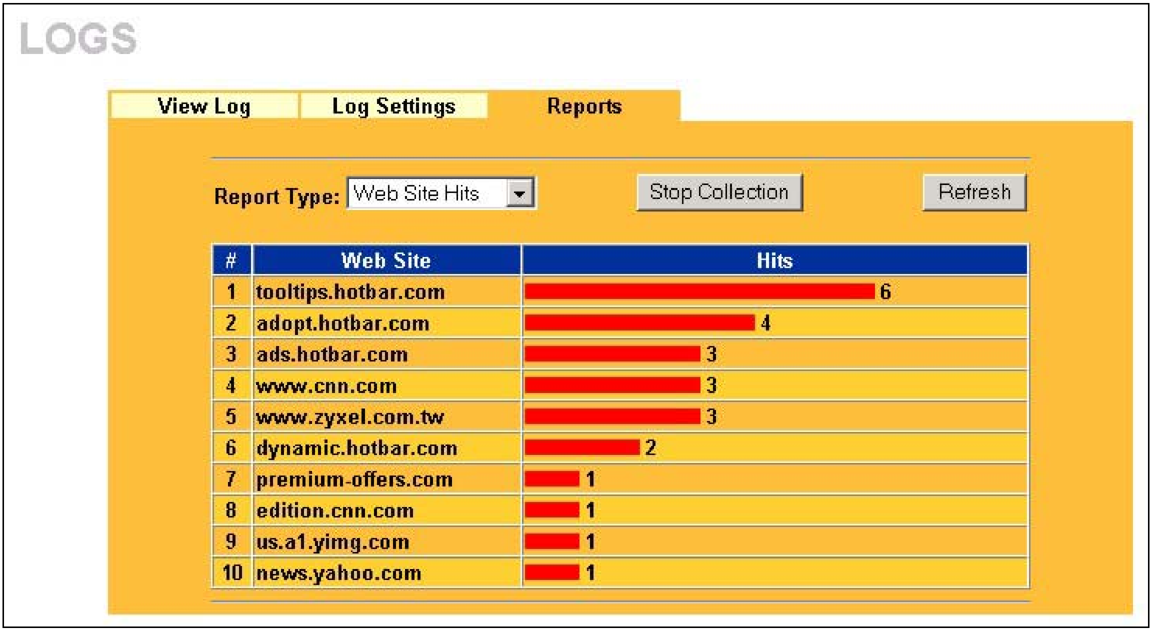
To change your ZyAIR's log reports, click **ADVANCED**, **LOGS** and then the **Reports** tab. The screen appears as shown.

The **Reports** screen displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to view information about bandwidth usage:

- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent

The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyAIR records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyAIR may count these as hits, thus the web hit count is not (yet) 100% accurate.



Report Type: Web Site Hits

#	Web Site	Hits
1	tooltips.hotbar.com	6
2	adopt.hotbar.com	4
3	ads.hotbar.com	3
4	www.cnn.com	3
5	www.zyxel.com.tw	3
6	dynamic.hotbar.com	2
7	premium-offers.com	1
8	edition.cnn.com	1
9	us.a1.yimg.com	1
10	news.yahoo.com	1

Figure 15-3 Reports

Enabling the ZyAIR's reporting function decreases the overall throughput by about 1 Mbps.

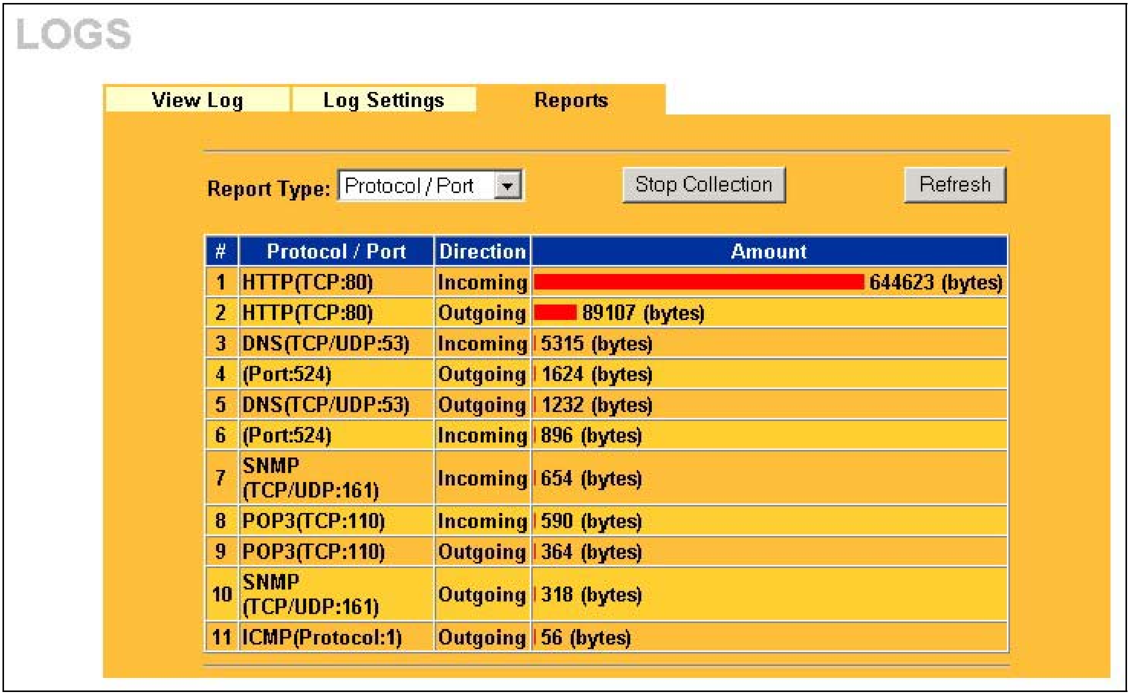
The following table describes the labels in this screen.

Table 15-3 Reports

LABEL	DESCRIPTION
Report Type	Use the drop-down list box to select the type of reports to display. **Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **LAN IP Address** displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Start Collection/ Stop Collection	The button text shows **Start Collection** when the ZyAIR is not recording report data and **Stop Collection** when the ZyAIR is recording report data. Click **Start Collection** to have the ZyAIR record report data. Click **Stop Collection** to halt the ZyAIR from recording more data.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
#	This field displays the index number of an individual web site.
Web Site	**Web Site** displays the web site address(es) that have been visited the most often from the LAN.
Hits	**Hits** displays the total number of visits to each web site.

15.3.1 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyAIR record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.



Report Type: Protocol / Port

#	Protocol / Port	Direction	Amount
1	HTTP(TCP:80)	Incoming	644623 (bytes)
2	HTTP(TCP:80)	Outgoing	89107 (bytes)
3	DNS(TCP/UDP:53)	Incoming	5315 (bytes)
4	(Port:524)	Outgoing	1624 (bytes)
5	DNS(TCP/UDP:53)	Outgoing	1232 (bytes)
6	(Port:524)	Incoming	896 (bytes)
7	SNMP (TCP/UDP:161)	Incoming	654 (bytes)
8	POP3(TCP:110)	Incoming	590 (bytes)
9	POP3(TCP:110)	Outgoing	364 (bytes)
10	SNMP (TCP/UDP:161)	Outgoing	318 (bytes)
11	ICMP(Protocol:1)	Outgoing	56 (bytes)

Figure 15-4 Protocol/Port Report

The following table describes the labels in this screen.

Table 15-4 Protocol/Port Report

LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyAIR. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Start Collection/ Stop Collection	The button text shows **Start Collection** when the ZyAIR is not recording report data and **Stop Collection** when the ZyAIR is recording report data. Click **Start Collection** to have the ZyAIR record report data. Click **Stop Collection** to halt the ZyAIR from recording more data.

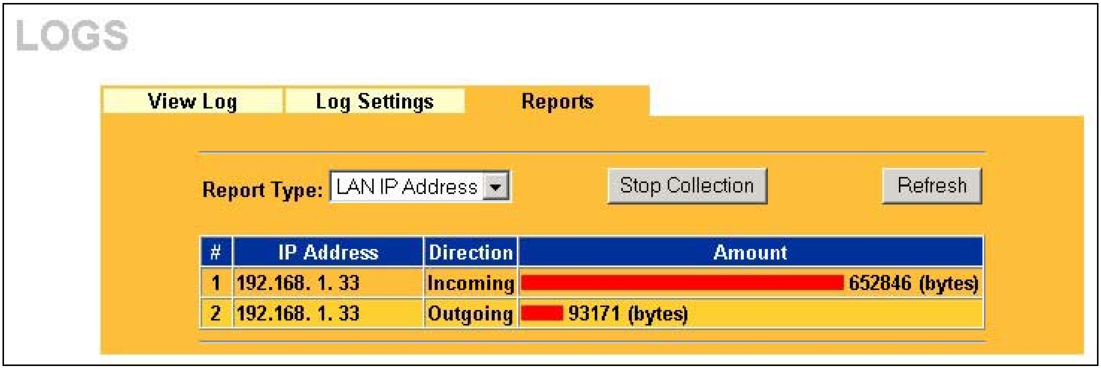
Table 15-4 Protocol/Port Report

LABEL	DESCRIPTION
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see *Table 15-6*).

15.3.2 Viewing LAN IP Address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list box to have the ZyAIR record and display the LAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

Computers take turns using dynamically assigned LAN IP addresses. The ZyAIR continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.



Report Type: LAN IP Address

#	IP Address	Direction	Amount
1	192.168. 1. 33	Incoming	652846 (bytes)
2	192.168. 1. 33	Outgoing	93171 (bytes)

Figure 15-5 LAN IP Address Report

The following table describes the labels in this screen.

Table 15-5 LAN IP Address Report

LABEL	DESCRIPTION
Start Collection/ Stop Collection	The button text shows **Start Collection** when the ZyAIR is not recording report data and **Stop Collection** when the ZyAIR is recording report data. Click **Start Collection** to have the ZyAIR record report data. Click **Stop Collection** to halt the ZyAIR from recording more data.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see *Table 15-6*).

15.3.3 Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 15-6 Report Specifications

LABEL	DESCRIPTION
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

Part VII:

MAINTENANCE

This part describes the Maintenance web configurator screens.

Chapter 16 Maintenance

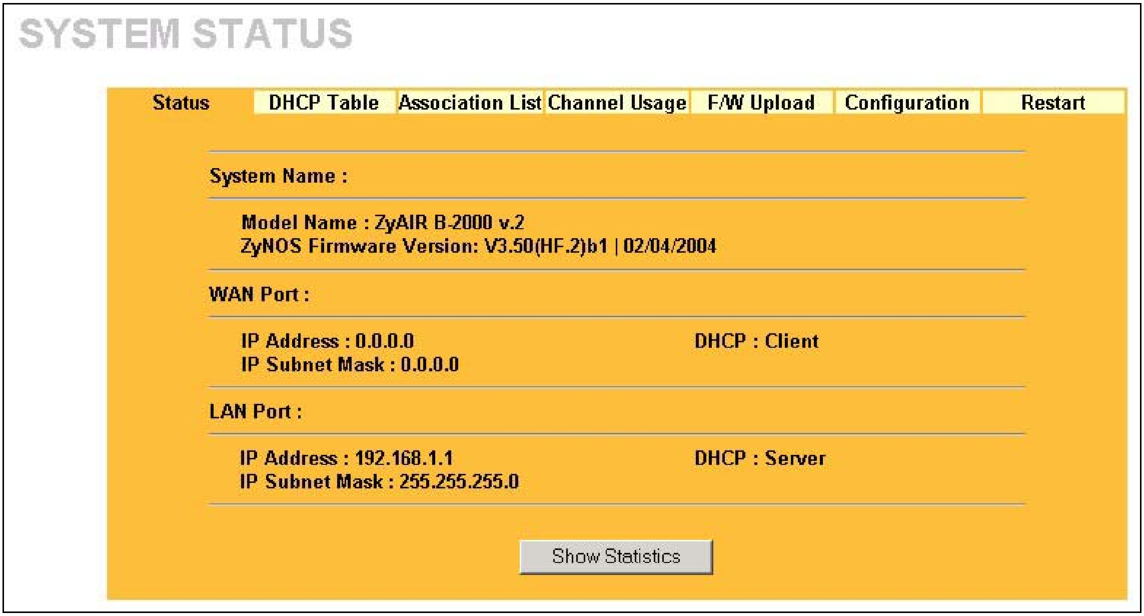
This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

16.1 Maintenance Overview

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

16.2 System Status Screen

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



System Name :

Model Name : ZyAIR B-2000 v.2
ZyNOS Firmware Version: V3.50(HF.2)b1 | 02/04/2004

WAN Port :

IP Address : 0.0.0.0 DHCP : Client
IP Subnet Mask : 0.0.0.0

LAN Port :

IP Address : 192.168.1.1 DHCP : Server
IP Subnet Mask : 255.255.255.0

Figure 16-1 Status

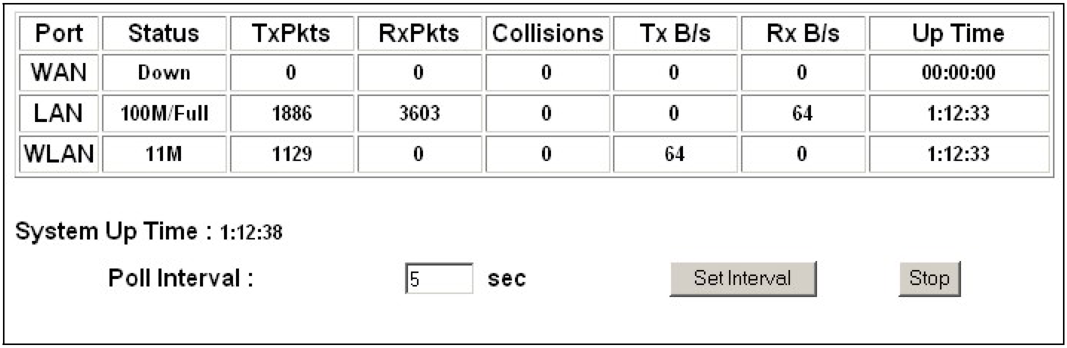
The following table describes the labels in this screen.

Table 16-1 Status

LABEL	DESCRIPTION
System Name	This is the **System Name** you enter in the first Internet Access Wizard screen. It is for identification purposes.
Model Name	The model name identifies your device type. The model name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol – **IP** for which the ZyAIR is configured. This field is not available on all models.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - **Client** or **None**.
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - **Server**, **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.

16.2.1 System Statistics

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



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	1886	3603	0	0	64	1:12:33
WLAN	11M	1129	0	0	64	0	1:12:33

System Up Time : 1:12:38

Poll Interval : 5 sec

Figure 16-2 Status: Show Statistics

The following table describes the labels in this screen.

Table 16-2 Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the LAN or WAN port.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission speed only for wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyAIR has been on.
Poll Interval	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.

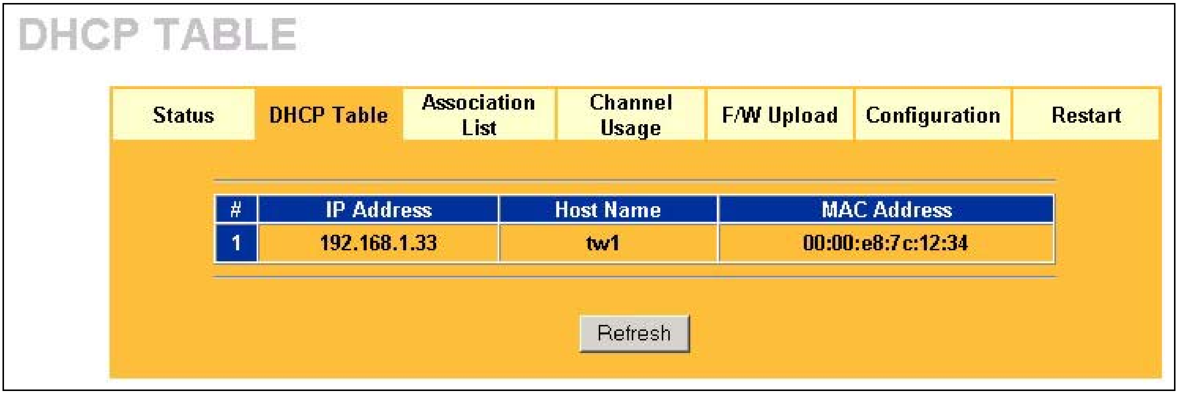
Table 16-2 Status: Show Statistics

LABEL	DESCRIPTION
Stop	Click this button to stop refreshing statistics.

16.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyAIR as a DHCP server or disable it. When configured as a server, the ZyAIR provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE** and then the **DHCP Table** tab (or **DHCP TABLE**). Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.



#	IP Address	Host Name	MAC Address
1	192.168.1.33	tw1	00:00:e8:7c:12:34

Figure 16-3 DHCP Table

The following table describes the labels in this screen.

Table 16-3 DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the **#** field listed above.
Host Name	This field displays the computer host name.

Table 16-3 DHCP Table

LABEL	DESCRIPTION
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Refresh	Click **Refresh** to reload the DHCP table.

16.4 Association List

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

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

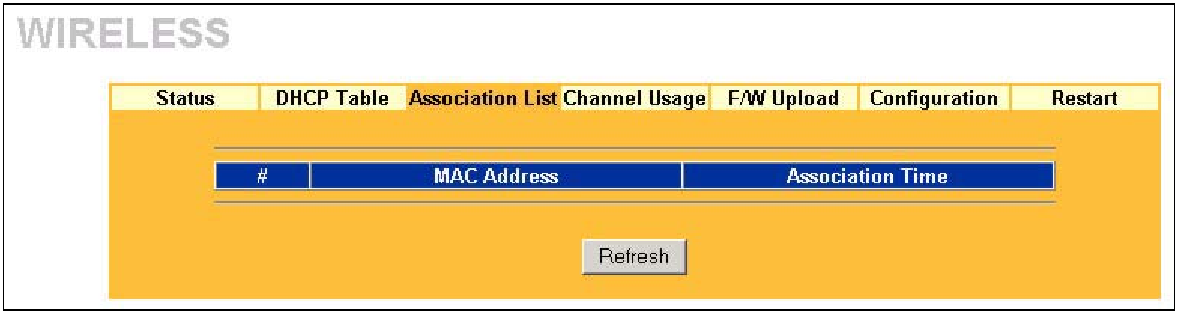


Figure 16-4 Association List

The following table describes the labels in this screen.

Table 16-4 Association List

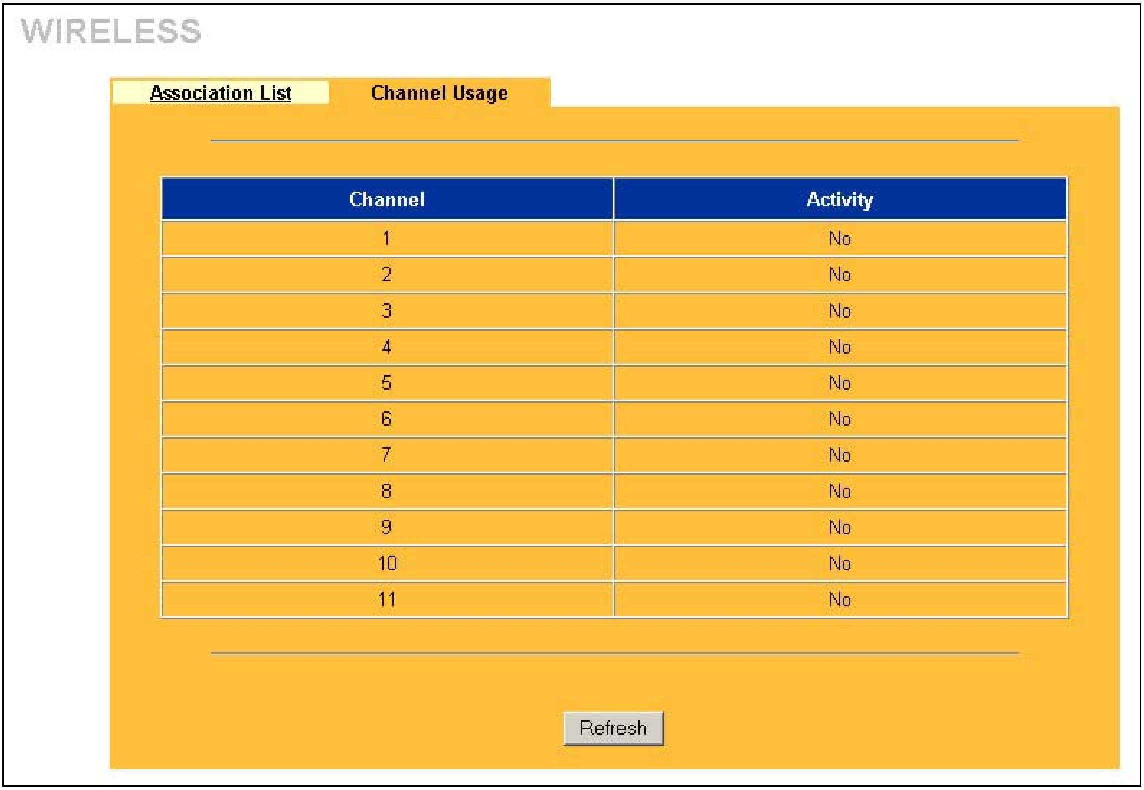
LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyAIR.
Refresh	Click **Refresh** to reload the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

16.5 Channel Usage

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

Click **MAINTENANCE**, (**WIRELESS**) and then the **Channel Usage** tab to display the screen shown next.

Wait a moment while the ZyAIR compiles the information.



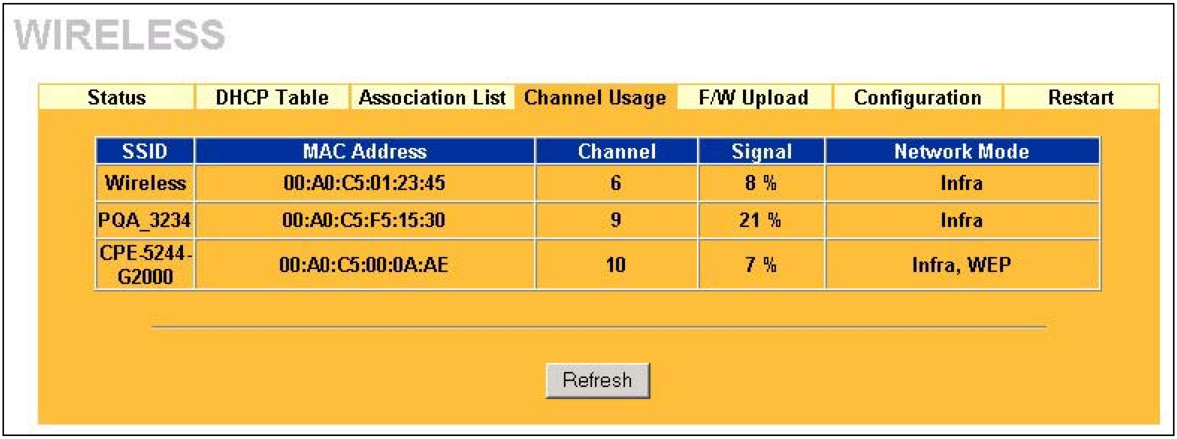
Channel	Activity
1	No
2	No
3	No
4	No
5	No
6	No
7	No
8	No
9	No
10	No
11	No

Figure 16-5 Channel Usage (ZyAIR B-2000)

The following table describes the labels in this screen.

Table 16-5 Channel Usage (ZyAIR B-2000)

LABEL	DESCRIPTION
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.
Activity	This field display Yes if the channel is used by another AP or Ad-hoc network within the ZyAIR's transmission range.
Refresh	Click **Refresh** to reload the screen.



SSID	MAC Address	Channel	Signal	Network Mode
Wireless	00:A0:C5:01:23:45	6	8 %	Infra
PQA_3234	00:A0:C5:F5:15:30	9	21 %	Infra
CPE-5244-G2000	00:A0:C5:00:0A:AE	10	7 %	Infra, WEP

Figure 16-6 Channel Usage

The following table describes the labels in this screen.

Table 16-6 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the *Wireless Configuration and Roaming* chapter for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.

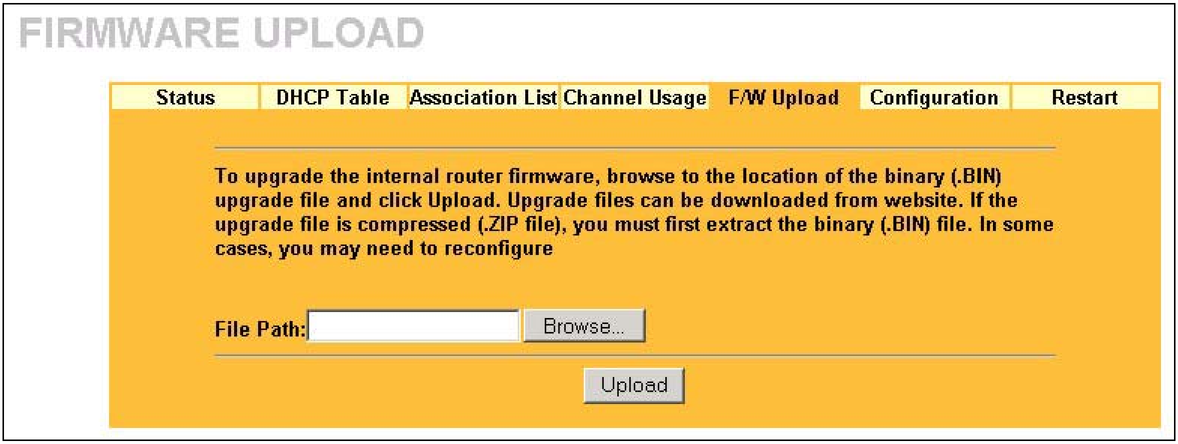
Table 16-6 Channel Usage

LABEL	DESCRIPTION
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 (refer to the *Wireless LAN* chapter) and WEP setup. Network modes are: **Infrastructure** (same as an extended service set ESS)), **Infrastructure with WEP** (WEP encryption is enabled), **Ad-Hoc** (same as an independent basic service set IBSS)), or **Ad-Hoc with WEP**.
Refresh	Click **Refresh** to reload the screen.

16.6 F/W Upload Screen

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

Click **MAINTENANCE**, and then the **F/W Upload** tab. Follow the instructions in this screen to upload firmware to your ZyAIR.



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

File Path:

Figure 16-7 Firmware Upload

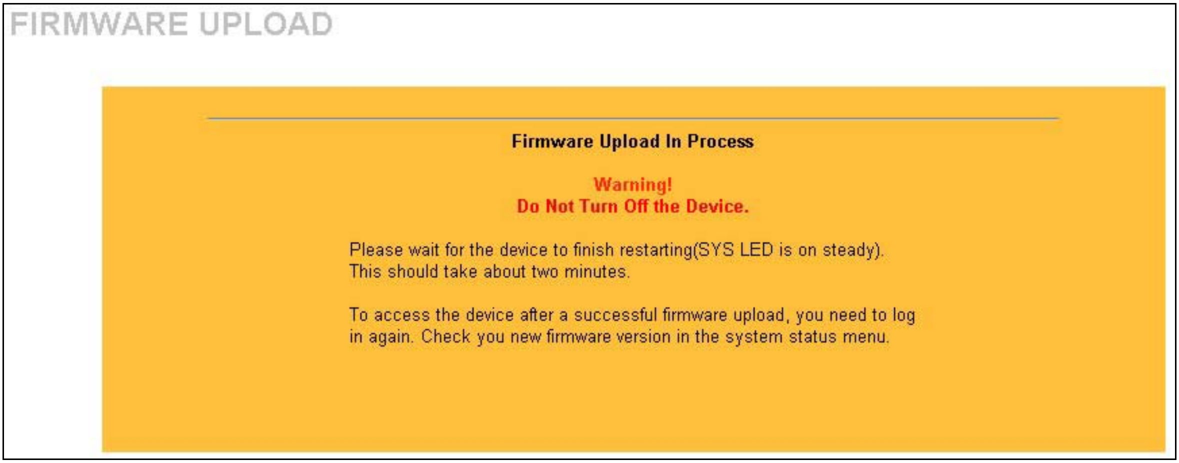
The following table describes the labels in this screen.

Table 16-7 Firmware Upload

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

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

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



FIRMWARE UPLOAD

Firmware Upload In Process

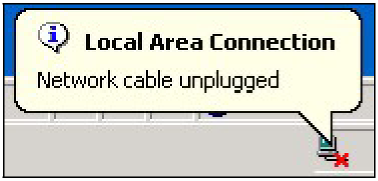
Warning!
Do Not Turn Off the Device.

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

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

Figure 16-8 Firmware Upload In Process

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



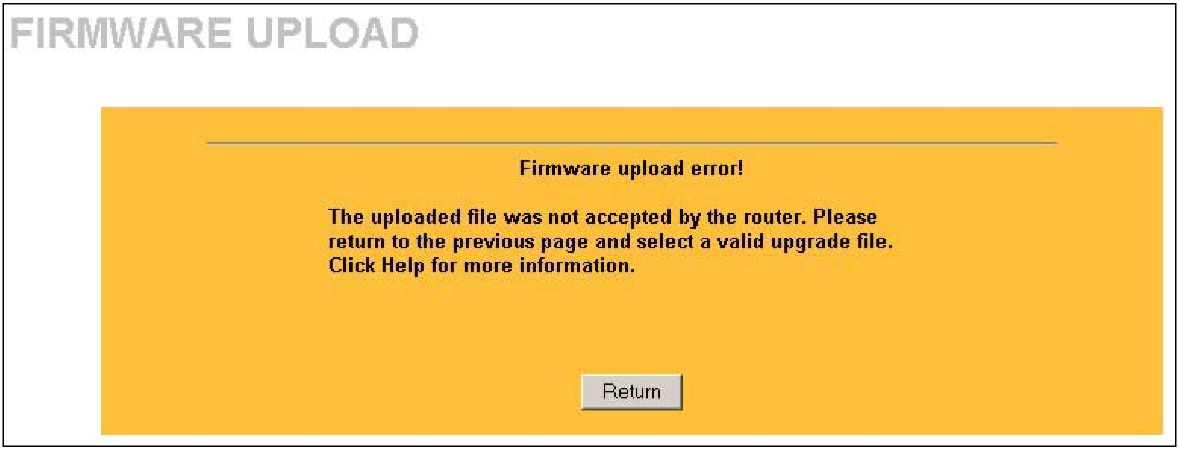
Local Area Connection

Network cable unplugged

Figure 16-9 Network Temporarily Disconnected

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

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



FIRMWARE UPLOAD

Firmware upload error!

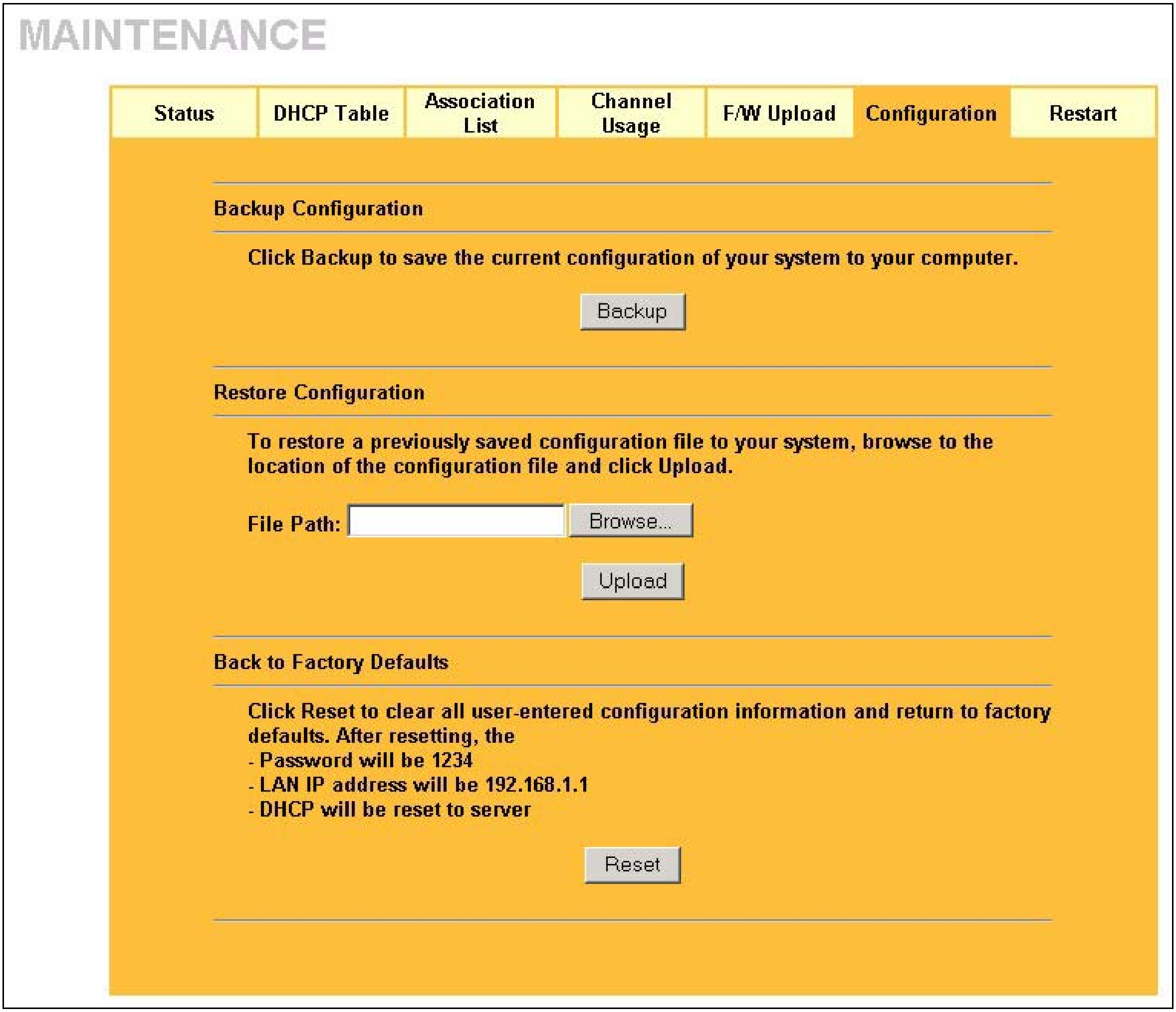
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

Figure 16-10 Firmware Upload Error

16.7 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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



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
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Figure 16-11 Configuration

16.7.1 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 your current ZyAIR configuration to your computer.

16.7.2 Restore Configuration

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

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

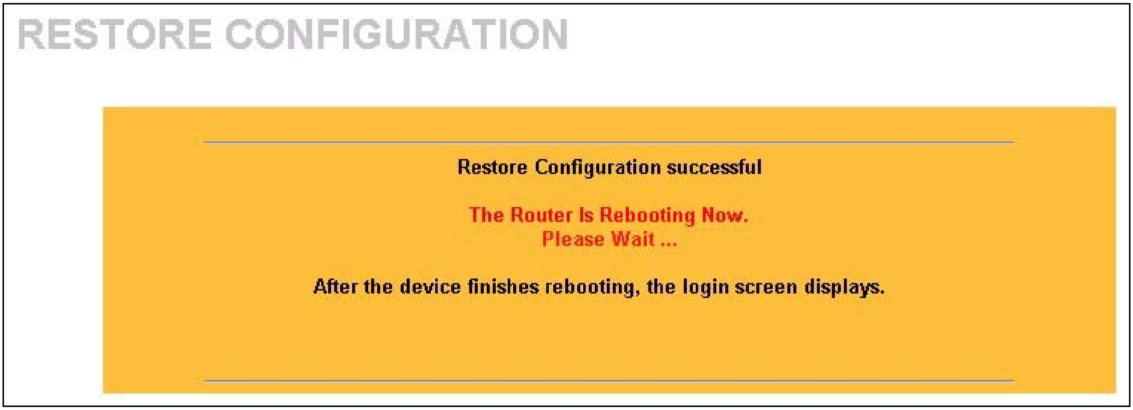
Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyAIR.

Table 16-8 Restore Configuration

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

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

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



RESTORE CONFIGURATION

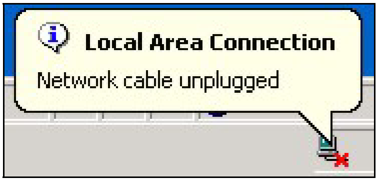
Restore Configuration successful

The Router Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

Figure 16-12 Configuration Upload Successful

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



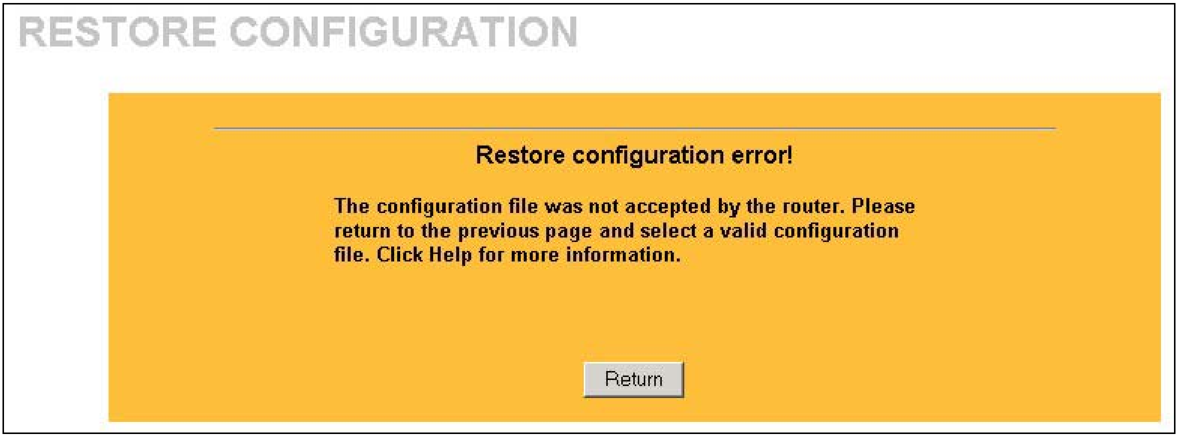
Local Area Connection

Network cable unplugged

Figure 16-13 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyAIR IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

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



RESTORE CONFIGURATION

Restore configuration error!

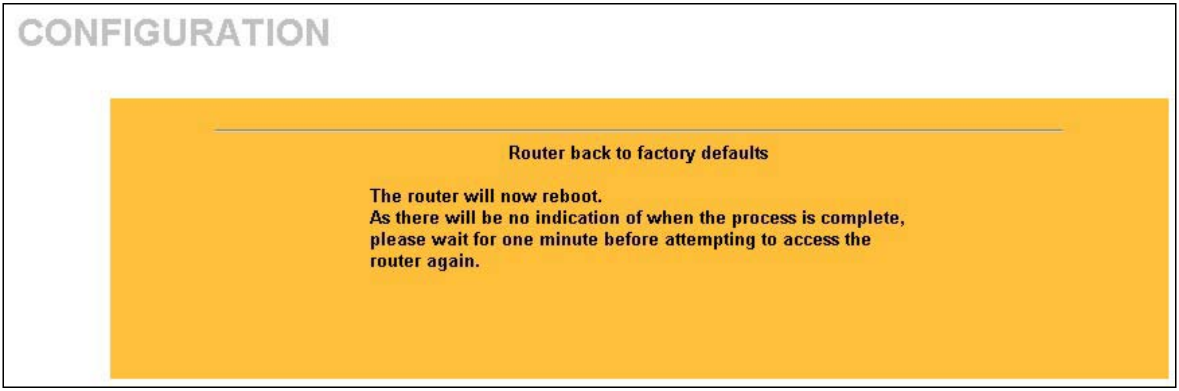
The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

Figure 16-14 Configuration Upload Error

16.7.3 Back to Factory Defaults

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

The following warning screen will appear.



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.

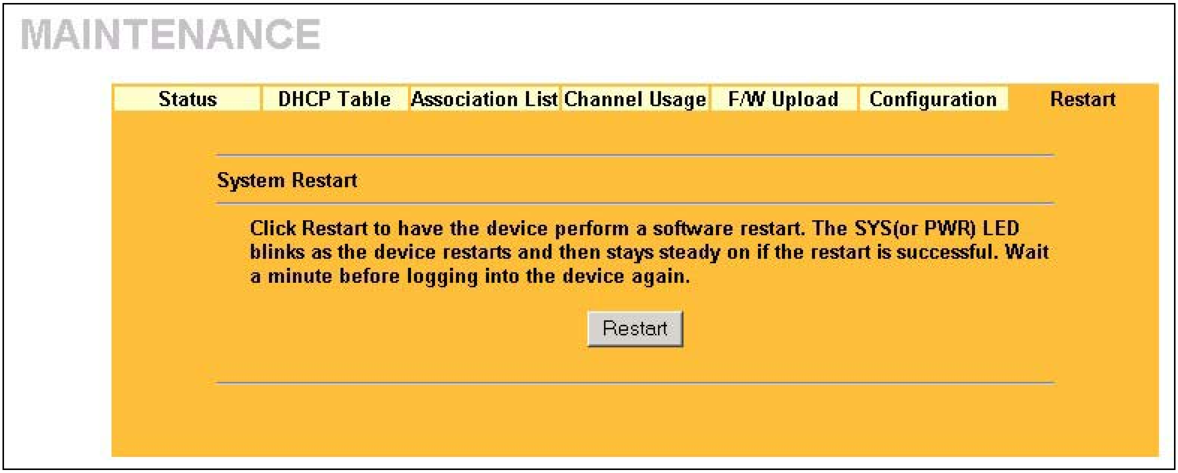
Figure 16-15 Reset Warning Message

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

16.8 Restart Screen

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

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



MAINTENANCE

System Restart

Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

Figure 16-16 Restart Screen

Part VIII:

SMT GETTING STARTED MENUS

This part introduces the SMT (System Management Terminal) and discusses the “Getting Started” SMT menus.

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

Chapter 17
Introducing the SMT

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

17.1 Connect to your ZyAIR Using Telnet

The following procedure details how to telnet into your ZyAIR.

Step 1. Make sure your computer IP address and the ZyAIR IP address are on the same subnet. Refer to the *Setting Up Your Computer IP Address* appendix.

Step 2. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.

Step 3. For your first login, enter 1234 in the **Password** field. As you type the password, the screen displays an "x" for each character you type.

Step 4. After entering the password you will see the main menu.

17.2 Connect to Your ZyAIR Using the Console Port

This method is only applicable to ZyAIR models with a console port, such as the ZyAIR B-2000.

Step 1. Connect the 7-pin male end of a console port cable to the port labelled **CONSOLE** on the ZyAIR and the 9-pin female end to an avaliable serial port on your computer.

Step 2. Run the communications software and configure the communication parameteres as follows:

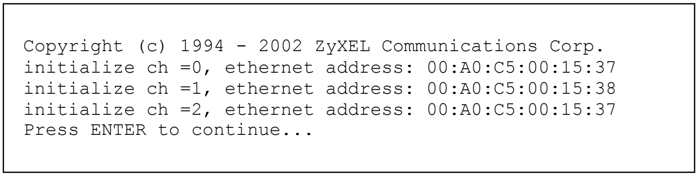
- VT100 terminal emulation
- 9600bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Step 3. Turn on your ZyAIR and you should see the initial screen shown next.

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.

17.2.1 Initial Screen

When you turn on your ZyAIR, it performs several internal tests as well as line initialization. After the initialization, the ZyAIR asks you to press [ENTER] to continue, as shown.



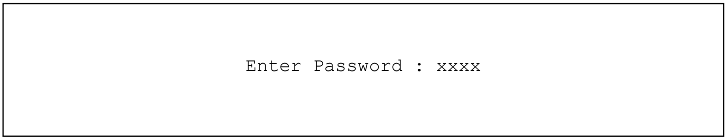
```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:00:15:37
initialize ch =1, ethernet address: 00:A0:C5:00:15:38
initialize ch =2, ethernet address: 00:A0:C5:00:15:37
Press ENTER to continue...
```

Figure 17-1 Consol Port Power-On Display

17.2.2 Entering Password

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

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



```
Enter Password : xxxx
```

Figure 17-2 Login Screen

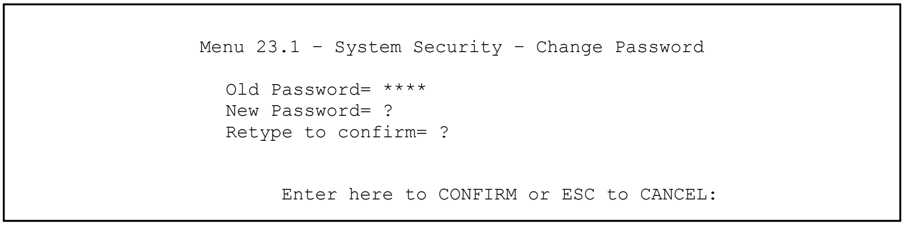
17.3 Changing the System Password

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

Step 1. Enter 23 in the main menu to open **Menu 23 - System Security**.

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

Step 3. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].



```
                  Menu 23.1 - System Security - Change Password

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


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

Figure 17-3 Menu 23.1 System Security : Change Password

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

Step 5. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

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

17.4 ZyAIR SMT Menu Overview Example

We use the ZyAIR B-2000 v.2 SMT menus in this guide as an example. The SMT menus for your model may vary slightly for different ZyAIR wireless gateway models.

The following figure gives you an example overview of the various SMT menu screens for your ZyAIR B-2000 v.2.

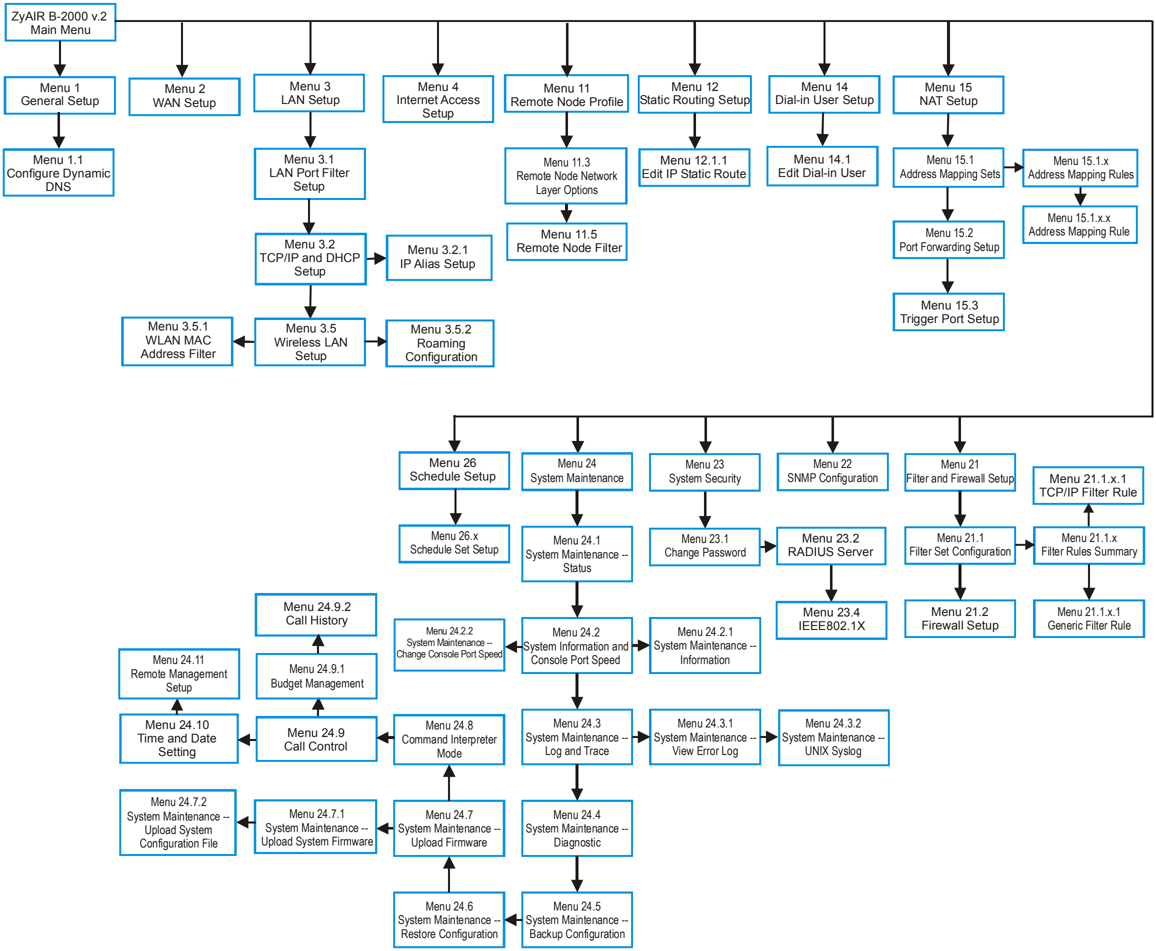

ZyAIR B-2000 v.2 Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 2 WAN Setup
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 3.5 Wireless LAN Setup
Menu 3.5.1 WLAN MAC Address Filter
Menu 3.5.2 Roaming Configuration
Menu 4 Internet Access Setup
Menu 11 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 12 Static Routing Setup
Menu 12.1.1 Edit IP Static Route
Menu 14 Dial-in User Setup
Menu 14.1 Edit Dial-in User
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.x Address Mapping Rules
Menu 15.1.x.x Address Mapping Rule
Menu 15.2 Port Forwarding Setup
Menu 15.3 Trigger Port Setup
Menu 26 Schedule Setup
Menu 26.x Schedule Set Setup
Menu 24 System Maintenance
Menu 24.1 System Maintenance -- Status
Menu 24.2 System Information and Console Port Speed
Menu 24.2.1 System Maintenance -- Information
Menu 24.2.2 System Maintenance -- Change Console Port Speed
Menu 24.3 System Maintenance -- Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance -- UNIX Syslog
Menu 24.4 System Maintenance -- Diagnostic
Menu 24.5 System Maintenance -- Backup Configuration
Menu 24.6 System Maintenance -- Restore Configuration
Menu 24.7 System Maintenance -- Upload Firmware
Menu 24.7.1 System Maintenance -- Upload System Firmware
Menu 24.7.2 System Maintenance -- Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Budget Management
Menu 24.9.2 Call History
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management Setup
Menu 23 System Security
Menu 23.1 Change Password
Menu 23.2 RADIUS Server
Menu 23.4 IEEE802.1X
Menu 22 SNMP Configuration
Menu 21 Filter and Firewall Setup
Menu 21.1 Filter Set Configuration
Menu 21.1.x Filter Rules Summary
Menu 21.1.x.1 TCP/IP Filter Rule
Menu 21.1.x.1 Generic Filter Rule
Menu 21.2 Firewall Setup

Figure 17-4 ZyAIR B-2000 v.2 SMT Menu Overview Example

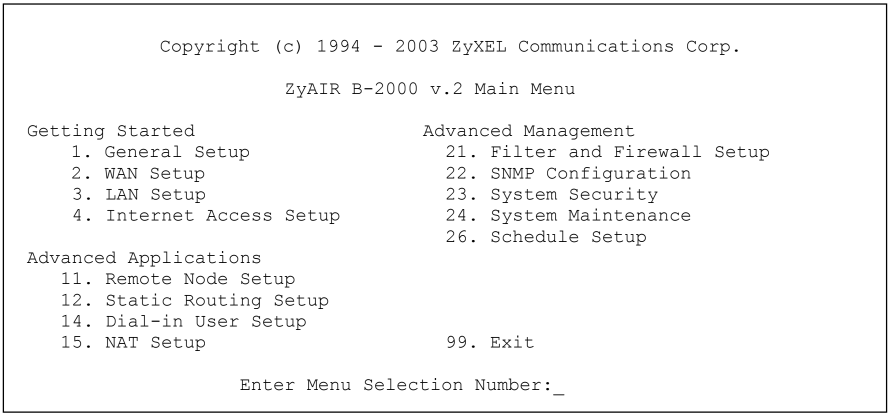
17.5 Navigating the SMT Interface

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

Table 17-1 Main Menu Commands

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

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



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

                       ZyAIR B-2000 v.2 Main Menu

Getting Started                    Advanced Management
    1. General Setup                 21. Filter and Firewall Setup
    2. WAN Setup                     22. SNMP Configuration
    3. LAN Setup                     23. System Security
    4. Internet Access Setup         24. System Maintenance
                                     26. Schedule Setup
Advanced Applications
   11. Remote Node Setup
   12. Static Routing Setup
   14. Dial-in User Setup
   15. NAT Setup                     99. Exit

                   Enter Menu Selection Number:_
```

Figure 17-5 ZyAIR B-2000 v.2 SMT Main Menu

17.5.1 System Management Terminal Interface Summary

Table 17-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to set up your WAN connection.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyAIR.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to set up filters and firewall to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password and set up wireless security.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.

Table 17-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
99	Exit	Use this to exit from SMT and return to a blank screen.

Chapter 18
General and WAN Setup

The chapter shows you the information on general setup and how to configure the WAN.

18.1 General Setup

Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

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

18.1.1 Dynamic DNS

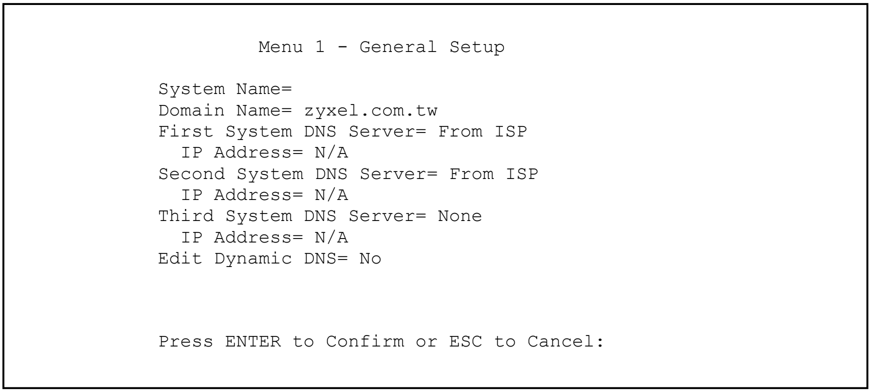
To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The ZyAIR supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

18.1.2 Procedure To Configure Menu 1

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



```
                  Menu 1 - General Setup

         System Name=
         Domain Name= zyxel.com.tw
         First System DNS Server= From ISP
           IP Address= N/A
         Second System DNS Server= From ISP
           IP Address= N/A
         Third System DNS Server= None
           IP Address= N/A
         Edit Dynamic DNS= No



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

Figure 18-1 Menu 1 General Setup

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

Table 18-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted.	**ZyAIR**
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	**zyxel.com.tw**
First System DNS Server Second System DNS Server Third System DNS Server	Press [SPACE BAR] to select **From ISP**, **User Defined** or **None** and press [ENTER].	**From ISP**
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select **User-Defined** in the field above.	**N/A**

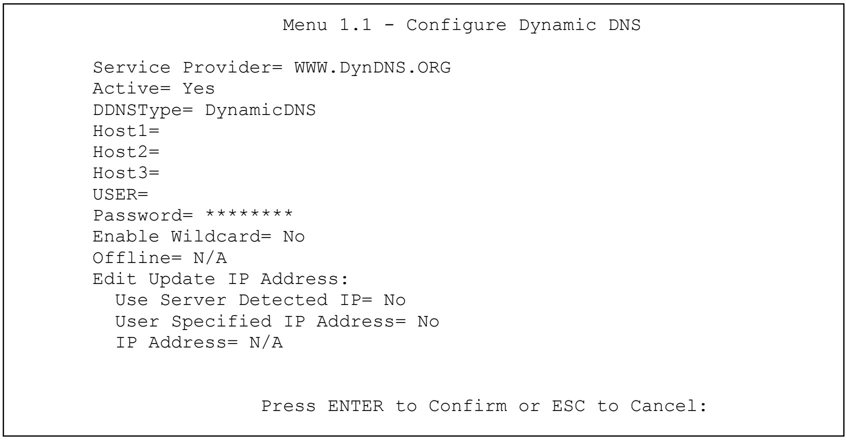
Table 18-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
Edit Dynamic DNS	Press [SPACE BAR] to select **Yes** and press [ENTER] to configure **Menu 1.1 – Configure Dynamic DNS** (discussed next).	**No**
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.		

18.1.3 Procedure to Configure Dynamic DNS

If you have a private WAN IP address, then you cannot use Dynamic DNS.

Step 1. To configure Dynamic DNS, go to **Menu 1 – General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1– Configure Dynamic DNS** as shown next.



```
                  Menu 1.1 - Configure Dynamic DNS

        Service Provider= WWW.DynDNS.ORG
        Active= Yes
        DDNSType= DynamicDNS
        Host1=
        Host2=
        Host3=
        USER=
        Password= ********
        Enable Wildcard= No
        Offline= N/A
        Edit Update IP Address:
          Use Server Detected IP= No
          User Specified IP Address= No
          IP Address= N/A


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

Figure 18-2 Menu 1.1 Configure Dynamic DNS

The following table describes the fields in this menu.

Table 18-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)

Table 18-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyAIR supports DYNDNS wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
Offline	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	**Yes**
Edit Update IP Address: You can select **Yes** in either the **Use Server Detected IP** field (recommended) or the **User Specified IP Addr** field, but not both. With the **Use Server Detected IP** and **User Specified IP Addr** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyAIR's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the ZyAIR must have a public WAN IP address in order for DDNS to work.		
Use Server Detected IP	Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the ZyAIR uses or is behind. You can set this field to **Yes** whether the IP address is public or private, static or dynamic.	**Yes**

Table 18-2 Menu 1.1 Configure Dynamic DNS

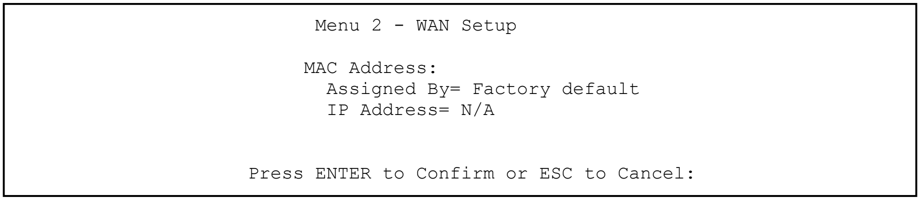
FIELD	DESCRIPTION	EXAMPLE
User Specified IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the ZyAIR uses or is behind a static public IP address.	**No**
IP Address	Enter the static public IP address if you select **Yes** in the **User Specified IP Addr** field.	**N/A**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

18.2 WAN Setup

The MAC address field allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file.

ZyXEL recommends you clone the MAC address from a workstation on your LAN even if your ISP does not require MAC address authentication.

From the main menu, enter 2 to display **Menu 2-WAN Setup** screen as shown.



```
                          Menu 2 - WAN Setup

                         MAC Address:
                           Assigned By= Factory default
                           IP Address= N/A


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

Figure 18-3 Menu 2 WAN Setup

The following table describes the fields in this menu.

Table 18-3 Menu 2 WAN Setup

FIELD	DESCRIPTION	EXAMPLE
MAC Address		

Table 18-3 Menu 2 WAN Setup

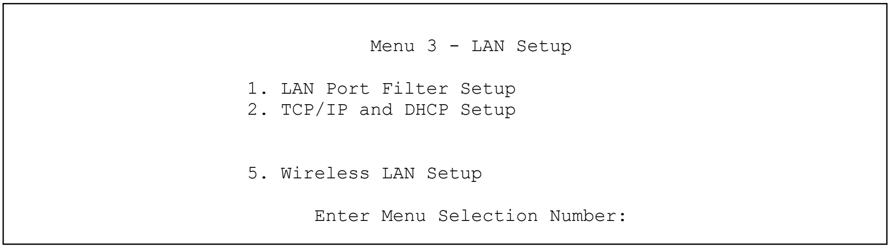
FIELD	DESCRIPTION	EXAMPLE
Assigned By	Press [SPACE BAR] to select **Factory default** and press [ENTER] to use the factory assigned MAC address. Select **IP address attached on LAN** and enter the IP address in the **IP Address** field below to clone the MAC address of the computer on the Ethernet.	**Factory default**
IP Address	Enter the IP address of the computer whose MAC address you are cloning. This field is available if you select **IP address attached on LAN** in the **Assigned By** field.	N/A
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 19
LAN Setup

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

19.1 LAN Setup

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



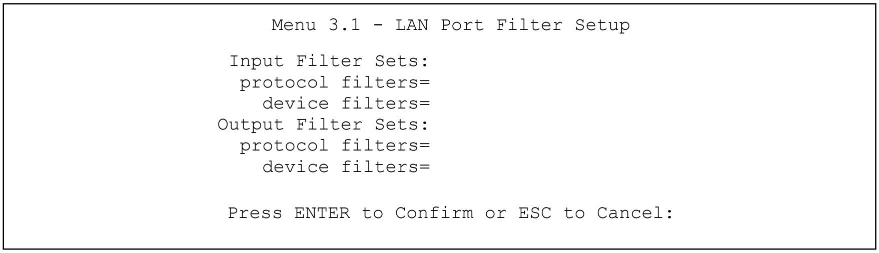
```
                                 Menu 3 - LAN Setup

                      1. LAN Port Filter Setup
                      2. TCP/IP and DHCP Setup


                      5. Wireless LAN Setup

                            Enter Menu Selection Number:
```

Figure 19-1 Menu 3 LAN Setup

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

19.1.1 General Ethernet Port Filter Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.



```
                           Menu 3.1 - LAN Port Filter Setup

                       Input Filter Sets:
                        protocol filters=
                          device filters=
                      Output Filter Sets:
                        protocol filters=
                          device filters=

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

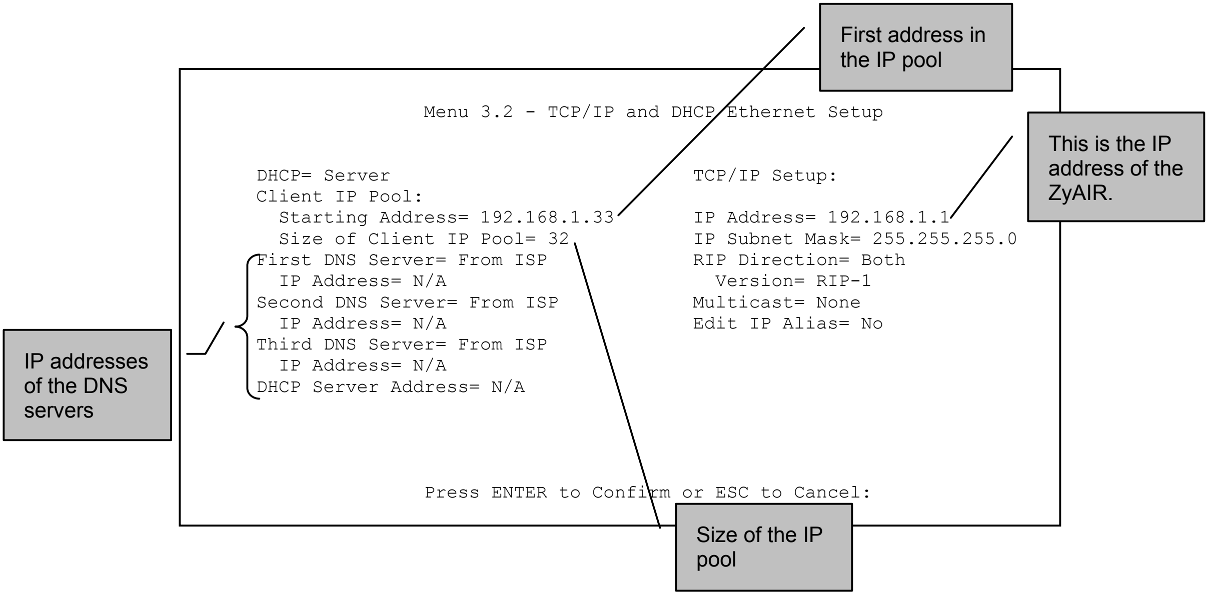
Figure 19-2 Menu 3.1 LAN Port Filter Setup

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

19.2 TCP/IP Ethernet and DHCP 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-Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP and DHCP Ethernet Setup**, as shown next:



```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup

   DHCP= Server                           TCP/IP Setup:
   Client IP Pool:
     Starting Address= 192.168.1.33       IP Address= 192.168.1.1
     Size of Client IP Pool= 32           IP Subnet Mask= 255.255.255.0
   First DNS Server= From ISP             RIP Direction= Both
     IP Address= N/A                        Version= RIP-1
   Second DNS Server= From ISP            Multicast= None
     IP Address= N/A                      Edit IP Alias= No
   Third DNS Server= From ISP
     IP Address= N/A
   DHCP Server Address= N/A



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

First address in the IP pool

This is the IP address of the ZyAIR.

IP addresses of the DNS servers

Size of the IP pool

Figure 19-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

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

Table 19-1 Menu 3.2 DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
DHCP	If set to **Server**, your ZyAIR can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyAIR acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP is used, the following items need to be set:	**Server** (default)
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	**192.168.1.33**
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
First DNS Server Second DNS Server Third DNS Server	Press [SPACE BAR] to select **From ISP**, **User Defined**, **DNS Relay** or **None** and press [ENTER]. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	**From ISP**
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select **User-Defined** in the field above.	**N/A**
DHCP Server Address	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 19-2 Menu3.2 TCP/IP Ethernet Setup

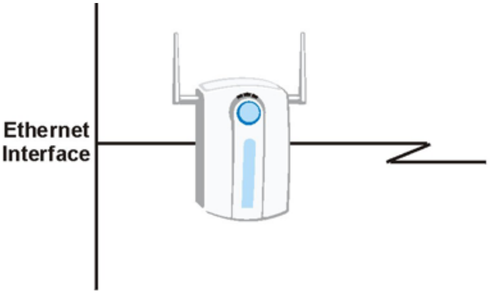
FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your ZyAIR in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both**

Table 19-2 Menu3.2 TCP/IP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyAIR supports both IGMP version 1(**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None**
Edit IP Alias	The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to menu 3.2.1.	**No**
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.		

19.3 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network.



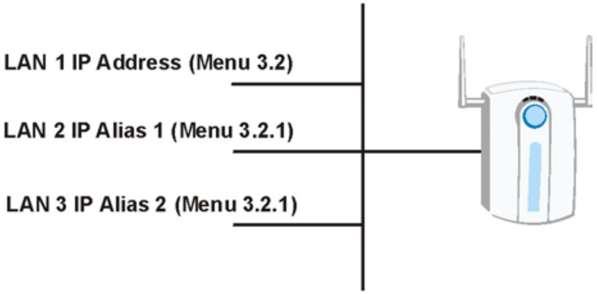
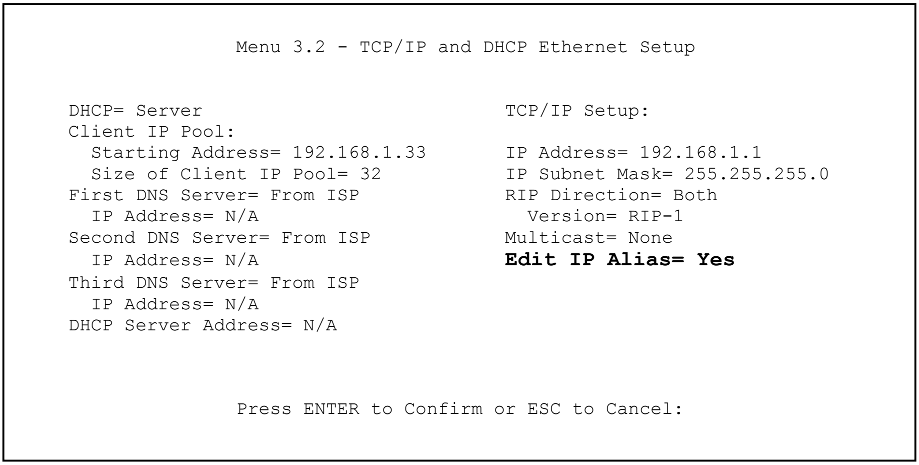

LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2.1)
LAN 3 IP Alias 2 (Menu 3.2.1)

Figure 19-4 Physical Network **Figure 19-5 Partitioned Logical Networks**

Use menu 3.2.1 to configure IP Alias on your ZyAIR.

19.3.1 IP Alias Setup

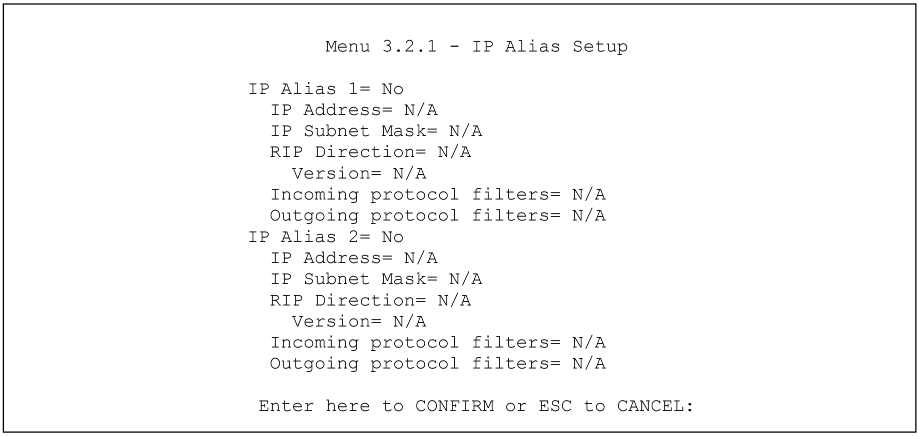
Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.



```
                      Menu 3.2 - TCP/IP and DHCP Ethernet Setup


      DHCP= Server                            TCP/IP Setup:
      Client IP Pool:
        Starting Address= 192.168.1.33        IP Address= 192.168.1.1
        Size of Client IP Pool= 32            IP Subnet Mask= 255.255.255.0
      First DNS Server= From ISP              RIP Direction= Both
        IP Address= N/A                         Version= RIP-1
      Second DNS Server= From ISP             Multicast= None
        IP Address= N/A                       Edit IP Alias= Yes
      Third DNS Server= From ISP
        IP Address= N/A
      DHCP Server Address= N/A



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

Figure 19-6 Menu 3.2 TCP/IP and DHCP Ethernet Setup

Press [ENTER] to display **Menu 3.2.1-IP Alias Setup**, as shown next.



```
                              Menu 3.2.1 - IP Alias Setup

                      IP Alias 1= No
                        IP Address= N/A
                        IP Subnet Mask= N/A
                        RIP Direction= N/A
                          Version= N/A
                        Incoming protocol filters= N/A
                        Outgoing protocol filters= N/A
                      IP Alias 2= No
                        IP Address= N/A
                        IP Subnet Mask= N/A
                        RIP Direction= N/A
                          Version= N/A
                        Incoming protocol filters= N/A
                        Outgoing protocol filters= N/A

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

Figure 19-7 Menu 3.2.1 IP Alias Setup

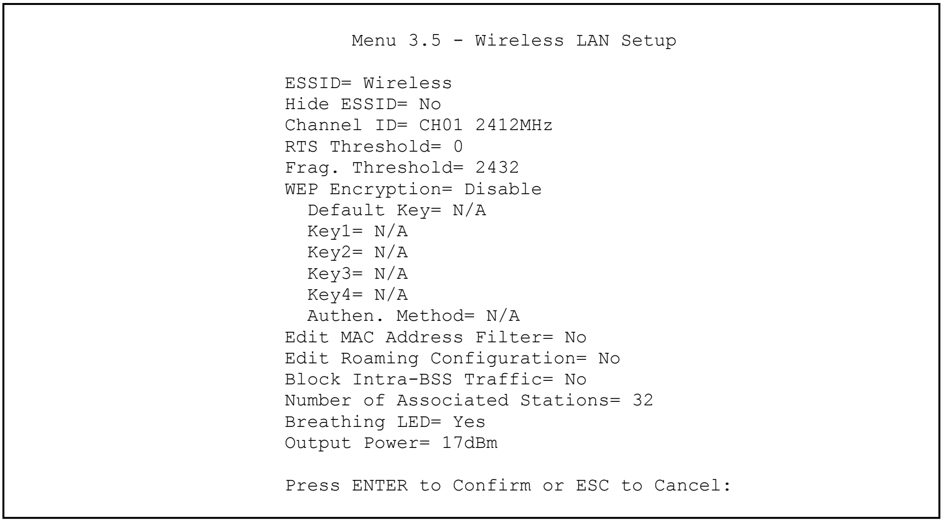
Follow the instructions in the table below to configure IP Alias parameters.

Table 19-3 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the ZyAIR.	**Yes**
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyAIR.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the 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.		

19.4 Wireless LAN Setup

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



```
                    Menu 3.5 - Wireless LAN Setup

              ESSID= Wireless
              Hide ESSID= No
              Channel ID= CH01 2412MHz
              RTS Threshold= 0
              Frag. Threshold= 2432
              WEP Encryption= Disable
                Default Key= N/A
                Key1= N/A
                Key2= N/A
                Key3= N/A
                Key4= N/A
                Authen. Method= N/A
              Edit MAC Address Filter= No
              Edit Roaming Configuration= No
              Block Intra-BSS Traffic= No
              Number of Associated Stations= 32
              Breathing LED= Yes
              Output Power= 17dBm

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

Figure 19-8 Menu 3.5 Wireless LAN Setup

The following table describes the fields in this menu.

Table 19-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
ESSID	The ESSID (Extended 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.	**Wireless**
Hide ESSID	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.	**No**
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	**CH01 2412MHz**
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	**2432**
Fragment Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	**2432**

Table 19-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
WEP	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.	**Disable**
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyAIR and the wireless stations to communicate.	1
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). **Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote a ASCII key.**	0x12345abcde
Authen. Method	Press [SPACE BAR] to select **Auto**, **Open System Only** or **Shared Key Only** and press [ENTER]. This field is **N/A** if WEP is not activated. If WEP encryption is activated, the default setting is **Auto**.	**Auto**
Block Intra-BSS Traffic	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER].	**No**
Number of Associated Stations	Enter the maximum number of wireless stations that may connect to the ZyAIR. The number should be from 1 to 32.	
Breathing LED	Press [SPACE BAR] to select **Yes** or **No** and press [ENTER].	**Yes**
Output Power	Press [SPACE BAR] to select **11dBm**, **13dBm**, **15dBm** or **17dBm** and press [ENTER].	**17dBm**

Table 19-4 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
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.		

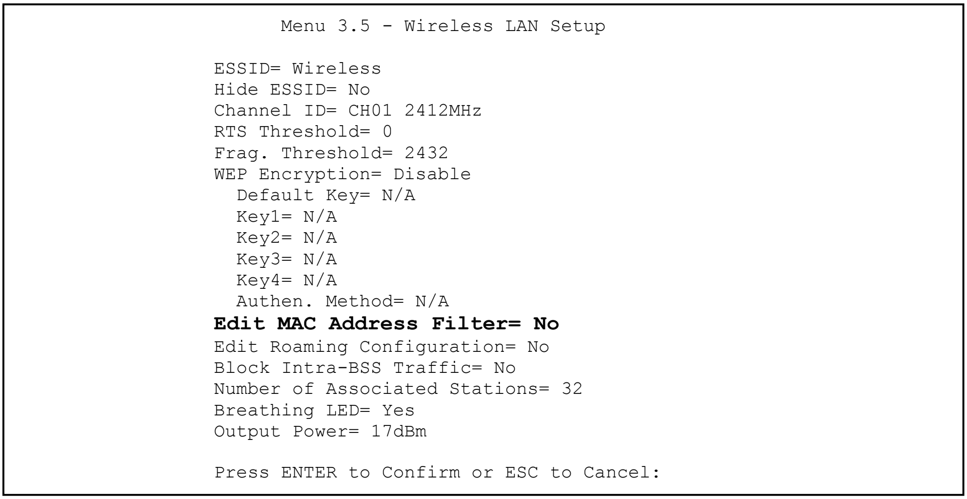
19.4.1 Configuring MAC Address Filter

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.

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

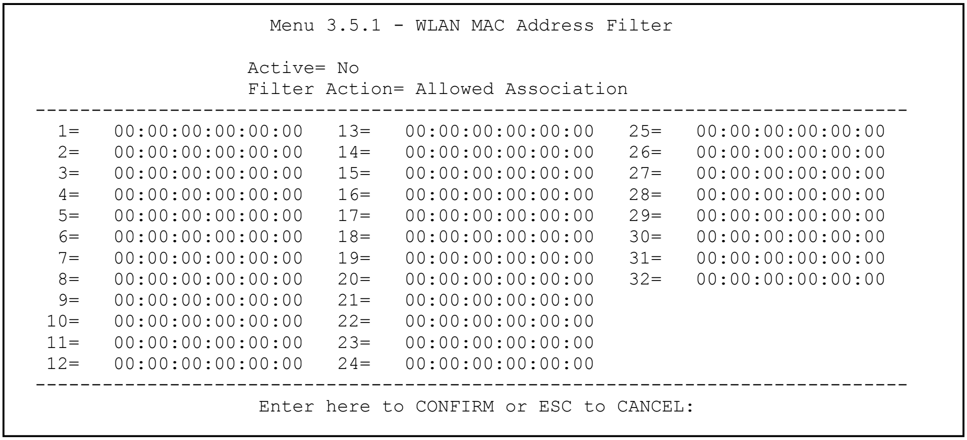
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
      Menu 3.5 - Wireless LAN Setup

ESSID= Wireless
Hide ESSID= No
Channel ID= CH01 2412MHz
RTS Threshold= 0
Frag. Threshold= 2432
WEP Encryption= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
  Authen. Method= N/A
Edit MAC Address Filter= No
Edit Roaming Configuration= No
Block Intra-BSS Traffic= No
Number of Associated Stations= 32
Breathing LED= Yes
Output Power= 17dBm

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

Figure 19-9 Menu 3.5 Wireless LAN Setup

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



```
                      Menu 3.5.1 - WLAN MAC Address Filter

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

Figure 19-10 Menu 3.5.1 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 19-5 Menu 3.5.1 WLAN MAC Address Filter

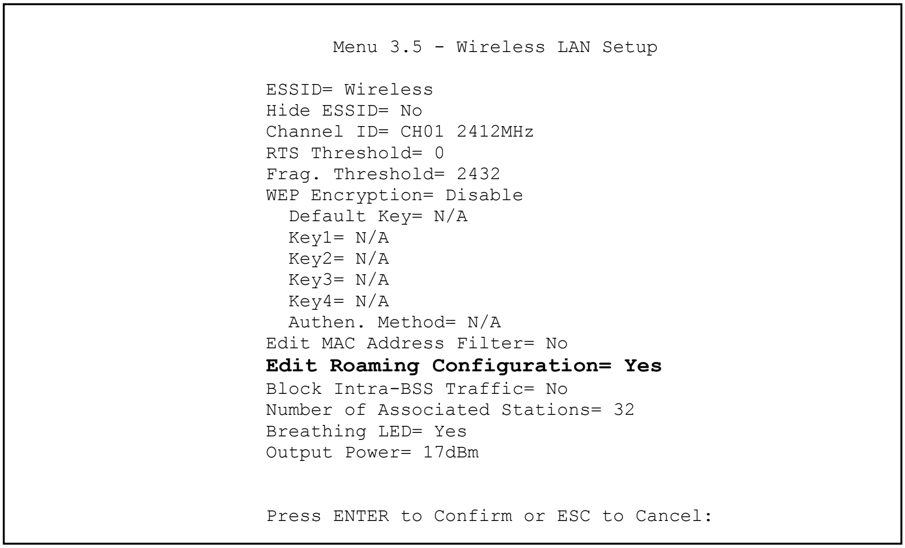
FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyAIR, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the ZyAIR. MAC addresses not listed will be denied access to the router.
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.	

19.4.2 Configuring Roaming on the ZyAIR

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

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

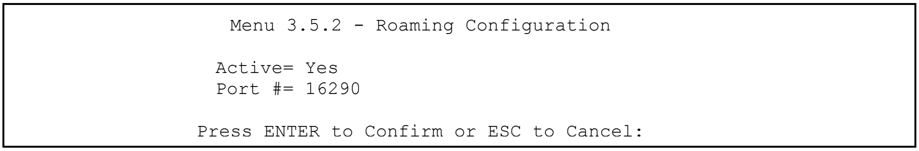
Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.



```
                      Menu 3.5 - Wireless LAN Setup

                ESSID= Wireless
                Hide ESSID= No
                Channel ID= CH01 2412MHz
                RTS Threshold= 0
                Frag. Threshold= 2432
                WEP Encryption= Disable
                  Default Key= N/A
                  Key1= N/A
                  Key2= N/A
                  Key3= N/A
                  Key4= N/A
                  Authen. Method= N/A
                Edit MAC Address Filter= No
                Edit Roaming Configuration= Yes
                Block Intra-BSS Traffic= No
                Number of Associated Stations= 32
                Breathing LED= Yes
                Output Power= 17dBm


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

Figure 19-11 Menu 3.5 Wireless LAN Setup

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



```
                   Menu 3.5.2 - Roaming Configuration

                  Active= Yes
                  Port #= 16290

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

Figure 19-12 Menu 3.5.2 Roaming Configuration

The following table describes the fields in this menu.

Table 19-6 Menu 3.5.2 Roaming Configuration

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **16290**. Make sure this port is not used by other services.
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 20
Internet Access

This chapter describes how to configure the ZyAIR for Internet Access.

20.1 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your ZyAIR for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information. Note that if you are using PPP or PPPoE encapsulation, then the only ISP information you need is a login name and password.

Table 20-1 Internet Account Information

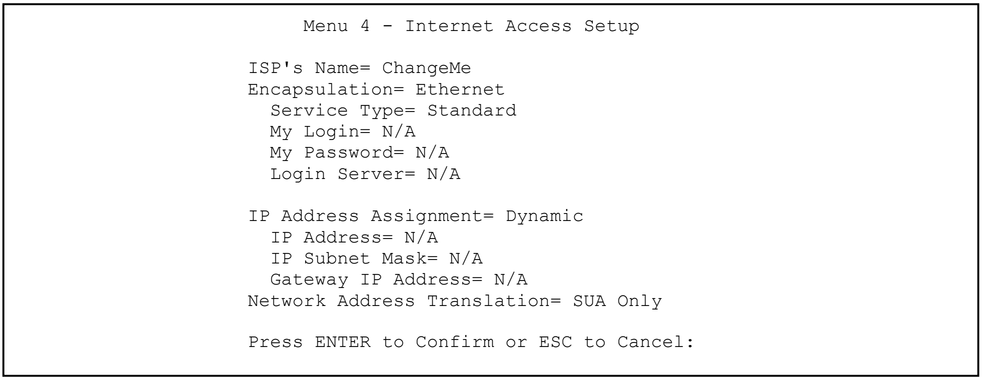
FIELD	DESCRIPTION	YOUR INFORMATION
System Name	Enter the name of the ZyAIR (optional).	
Service Name (PPPoE)	Enter the PPPoE service name if the ISP supplies one. Enter "any" if the ISP does not assign you one.	
Encapsulation	Select **Ethernet**, **PPPoE** or **PPTP**	
My Login	Enter the login name assigned by your ISP (for PPP/PPPoE only).	
My Password	Enter the password associated with your ISP assigned **My Login** (for PPP/PPPoE only).	
Idle Timeout (PPPoE or PPP)	Enter the time lapse, in seconds, before you automatically disconnect from the PPPoE or PPP server.	
IP Address	Enter if your IP address is not dynamically assigned.	
Network Address Translation	Select **Full Feature**, **SUA Only** or **None**.	

Table 20-1 Internet Account Information

FIELD	DESCRIPTION	YOUR INFORMATION
DNS Server Address Assignment	**Primary DNS server** **Secondary DNS server** Enter when using RFC 1483 Encapsulation or a static IP address.	

20.2 Internet Access Setup

From the main menu, type 4 to display **Menu 4 – Internet Access Setup**, as shown next.



```
     Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

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

Figure 20-1 Menu 4 Internet Access Setup

The following table contains instructions on how to configure your ZyAIR for Internet access.

Table 20-2 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	ChangeMe
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPP** or **Ethernet**.	**Ethernet**

Table 20-2 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
Service Type	This field is available if you select the **Ethernet** encapsulation. Press [SPACE BAR] to select the service type then press [ENTER]. Choose a RoadRunner flavor if your ISP is using Time Warner's RoadRunner; otherwise choose **Standard**. The **User Name**, **Password** and **Login Server** fields are not applicable (N/A) for the latter. Choose from **Standard**, **Telstra** (RoadRunner Telstra or BigPond authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Toshiba** (RoadRunner Toshiba authentication method).	**Standard**
My Login	Configure the **My Login** and **My Password** fields for PPP and PPPoE encapsulation only. Enter the login name exactly as your ISP gives you.	N/A
My Password	Enter the password associated with the login name above.	N/A
Login Server	Enter the IP address of the login server in dotted decimal notation.	10.11.12.13
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Static** or **Dynamic** address assignment.	Static
IP Address	Enter the IP address supplied by your ISP if applicable.	10.11.12.20
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you entered. 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 segment as your ZyAIR.	
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select **None**, **SUA Only** or **Full Feature**. Please see the *NAT Chapter* for more details.	**SUA Only**
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.		

If all your settings are correct your ZyAIR should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Refer to the *System Security* chapter for the wireless LAN security setup.

Part IX:

SMT ADVANCED APPLICATION MENUS

This part shows how to configure Remote Node, Static Routing, Dial-in User and NAT.

Chapter 21
Remote Node Configuration

This chapter shows you how to set up remote nodes on the WAN side.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

21.1 Remote Node Profile

Use **Menu 11-Remote Node Profile** to setup the remote node.

From the main menu, enter 11 to display **Menu 11-Remote Node Profile** as shown in .

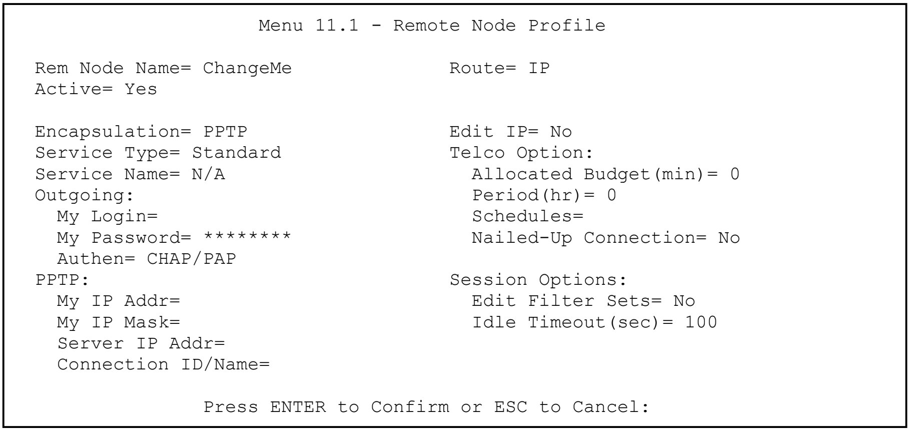
21.1.1 Encapsulation Scenarios

For Internet access you should use the encapsulation used by your ISP.

Nailed-Up Connection (PPPoE/PPTP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyAIR does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyAIR will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your ISP offers flat-rate service or you need a constant connection and the cost is of no concern.



```
                      Menu 11.1 - Remote Node Profile

  Rem Node Name= ChangeMe              Route= IP
  Active= Yes

  Encapsulation= PPTP                  Edit IP= No
  Service Type= Standard               Telco Option:
  Service Name= N/A                      Allocated Budget(min)= 0
  Outgoing:                              Period(hr)= 0
    My Login=                            Schedules=
    My Password= ********                Nailed-Up Connection= No
    Authen= CHAP/PAP
  PPTP:                                Session Options:
    My IP Addr=                          Edit Filter Sets= No
    My IP Mask=                          Idle Timeout(sec)= 100
    Server IP Addr=
    Connection ID/Name=

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

Figure 21-1 Menu 11.1 Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 21-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	ChangeMe
Active	Press [SPACE BAR] and then [ENTER] to select **No** to deactivate this node. Inactive nodes are displayed with a minus sign “–“ in SMT menu 11.	**Yes** (default)
Encapsulation	Press [SPACE BAR] to select from **Ethernet**, **PPPoE** or **PPTP** and press [ENTER].	Ethernet
Service Type	Press [SPACE BAR] and then [ENTER] to select the service type. Choose a RoadRunner flavor if your ISP is using Time Warner's RoadRunner; otherwise choose **Standard**. The User Name, Password and Login Server IP Address fields are not applicable (N/A) for the latter. Choose from **Standard**, **Telstra** (RoadRunner Telstra or BigPond authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Toshiba** (RoadRunner Toshiba authentication method).	Standard
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.	N/A

Table 21-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Outgoing:		
My Login	Type the login name assigned by your ISP when the ZyAIR calls this remote node.	
My Password	Type the password assigned by your ISP when the ZyAIR calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your ZyAIR will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.	**PAP**
PPTP:		
My IP Address	Type the (static) IP address assigned to you by your ISP in dotted decimal notation.	10.11.12.13
My IP Mask	Type the subnet mask of the PPTP server.	
Server IP Address	Type the IP address of the PPTP server in dotted decimal notation.	
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem.	
Route	This field determines the protocol used in routing. Options are **IP** and **None.**	**IP** (default)
Edit IP	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Telco Option:	**Telco Option** is available only for PPTP or PPPoE encapsulation.	
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)

Table 21-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).	0 (default)
Schedule	This field is only applicable for **PPPoE** and **PPPTP** encapsulation. You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed up Connection	This field is only applicable for **PPPoE** and **PPTP** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options		
Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the ZyAIR is idle (there is no traffic going to the remote node), before the ZyAIR automatically disconnects the remote node. 0 means that the session will not timeout. This field is available only for PPTP or PPPoE encapsulations.	100 (default)
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.		

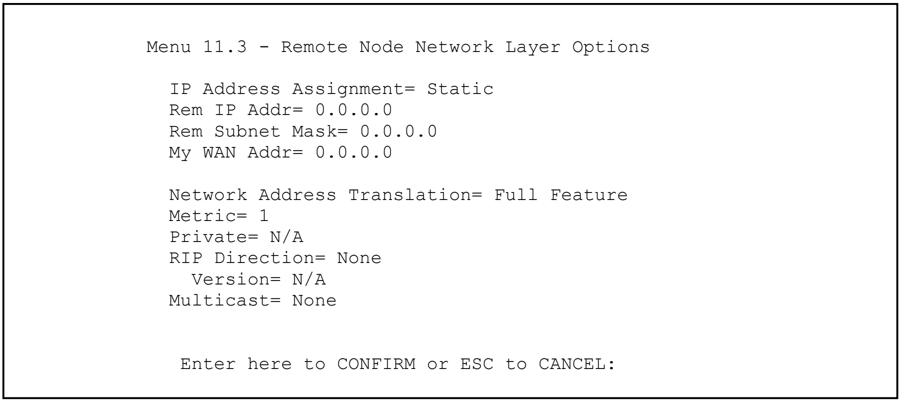
21.1.2 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

21.1.3 Remote Node Setup

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 - Remote Node Network Layer Options**.

Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3** – **Remote Node Network Layer Options** shown below.



```
            Menu 11.3 - Remote Node Network Layer Options

              IP Address Assignment= Static
              Rem IP Addr= 0.0.0.0
              Rem Subnet Mask= 0.0.0.0
              My WAN Addr= 0.0.0.0

              Network Address Translation= Full Feature
              Metric= 1
              Private= N/A
              RIP Direction= None
                Version= N/A
              Multicast= None


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

Figure 21-2 Menu 11.3 Remote Node Network Layer Options

The next table explains the fields in this menu.

Table 21-2 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.	**Static**
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your ZyAIR.	

Table 21-2 Menu 11.3 Remote Node Network Layer Options

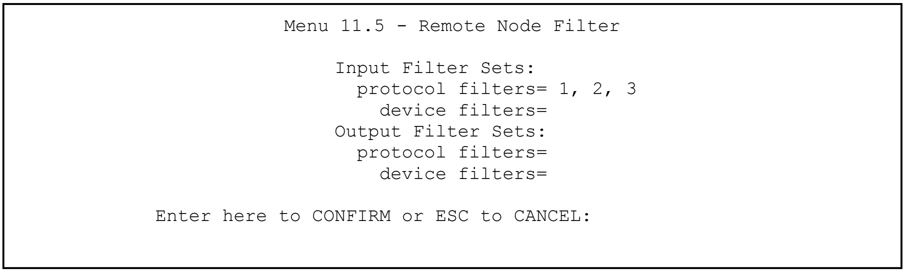
FIELD	DESCRIPTION	EXAMPLE
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your ZyAIR. Select **SUA Only** if you have just one public WAN IP address for your ZyAIR. The SMT uses Address Mapping Set 255 (menu 15.1 - see section *23.2.1*). Select **None** to disable NAT.	**Full Feature**
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**None**
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.		

21.2 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 - Remote Node Filter**.

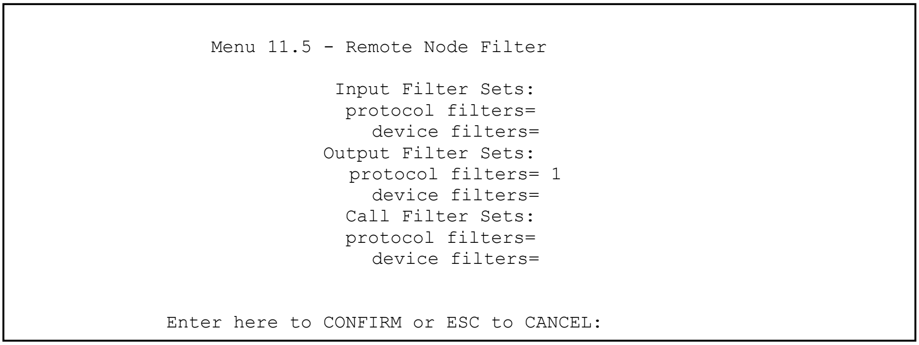
Use **Menu 11.5 - Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyAIR and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field.



```
            Menu 11.5 - Remote Node Filter

                Input Filter Sets:
                  protocol filters= 1, 2, 3
                    device filters=
                Output Filter Sets:
                  protocol filters=
                    device filters=

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

Figure 21-3 Menu 11.5 Remote Node Filter (Ethernet Encapsulation)



```
    Menu 11.5 - Remote Node Filter

               Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters= 1
                  device filters=
                Call Filter Sets:
                protocol filters=
                  device filters=


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

Figure 21-4 Menu 11.5 Remote Node Filter (PPTP or PPPoE Encapsulation)

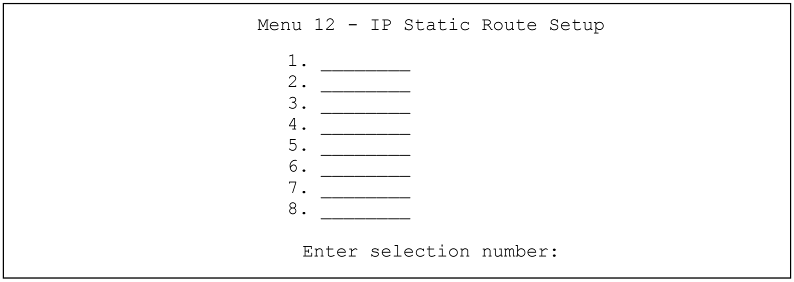
21.2.1 IP Static Route Setup

Static routes tell the ZyAIR routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the ZyAIR has no knowledge of the networks beyond. For instance, the ZyAIR knows about network N2 in the following figure through remote node Router 1. However, the ZyAIR is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the ZyAIR about the networks beyond the remote nodes.

Configuration

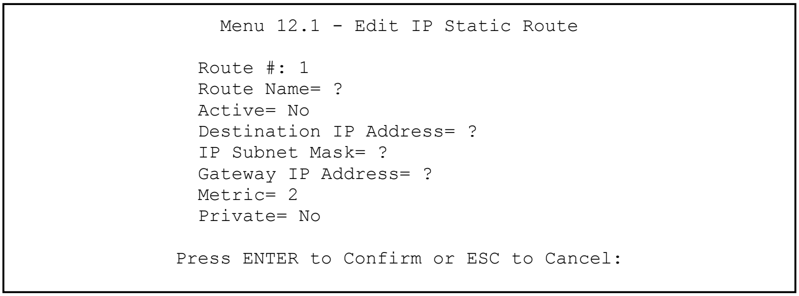
Step 1. To configure an IP static route, use **Menu 12 - Static Route Setup** as shwon next.



```
                   Menu 12 - IP Static Route Setup

                      1. ________
                      2. ________
                      3. ________
                      4. ________
                      5. ________
                      6. ________
                      7. ________
                      8. ________

                        Enter selection number:
```

Figure 21-5 Menu 12.1 IP Static Route Setup

Step 2. Now, type the route number of a static route you want to configure.



```
                 Menu 12.1 - Edit IP Static Route

               Route #: 1
               Route Name= ?
               Active= No
               Destination IP Address= ?
               IP Subnet Mask= ?
               Gateway IP Address= ?
               Metric= 2
               Private= No

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

Figure 21-6 Menu 12.1 Edit IP Static Route

The following table describes the fields in this menu.

Table 21-3 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.

Table 21-3 Menu 12.1 Edit IP Static Route

FIELD	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
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 22
Dial-in User Setup

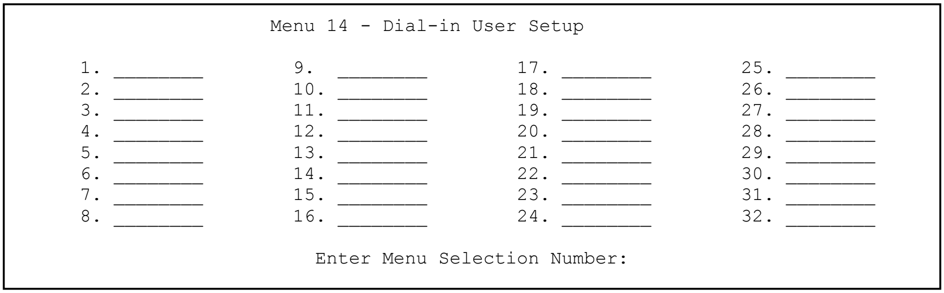
This chapter shows you how to create user accounts on the ZyAIR.

22.1 Dial-in User Setup

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

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

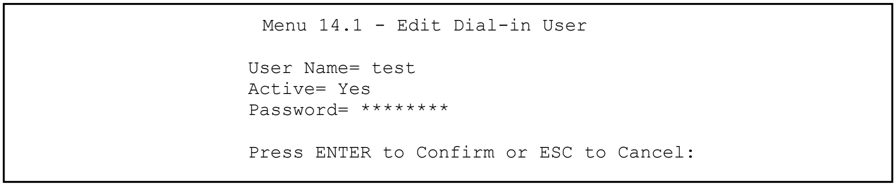
Step 1. From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.



```
                        Menu 14 - Dial-in User Setup

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

                            Enter Menu Selection Number:
```

Figure 22-1 Menu 14 Dial-in User Setup

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



```
                      Menu 14.1 - Edit Dial-in User

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

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

Figure 22-2 Menu 14.1 Edit Dial-in User

The following table describes the fields in this screen.

Table 22-1 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 23
Network Address Translation (NAT)

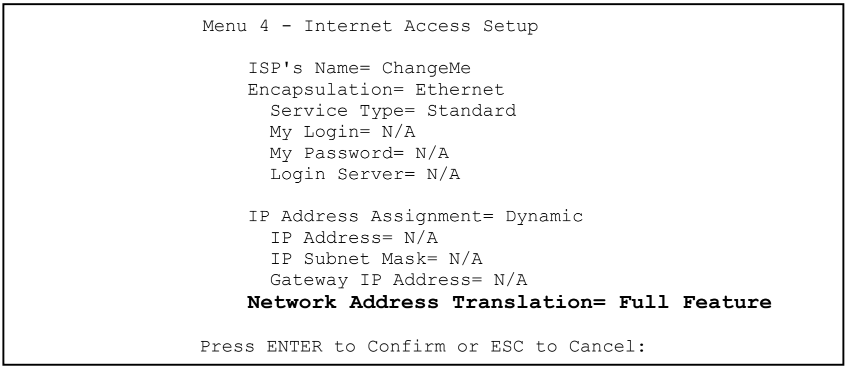
This chapter discusses how to configure NAT on the ZyAIR.

23.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

23.1.1 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.



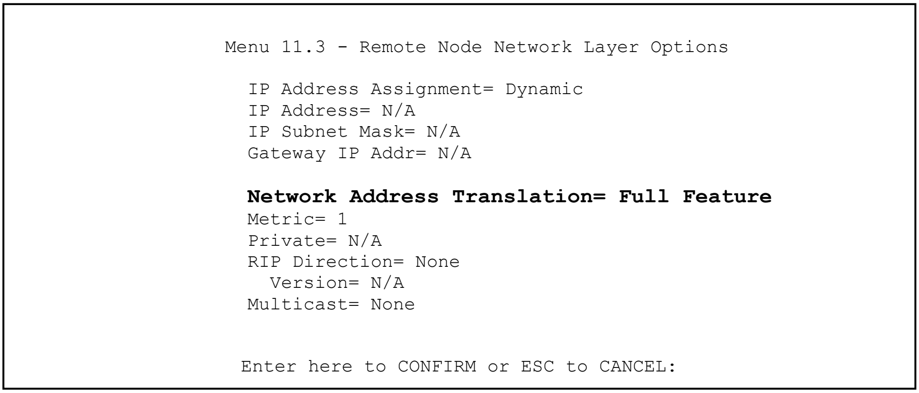
```
                 Menu 4 - Internet Access Setup

                     ISP's Name= ChangeMe
                     Encapsulation= Ethernet
                       Service Type= Standard
                       My Login= N/A
                       My Password= N/A
                       Login Server= N/A

                     IP Address Assignment= Dynamic
                       IP Address= N/A
                       IP Subnet Mask= N/A
                       Gateway IP Address= N/A
                     Network Address Translation= Full Feature

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

Figure 23-1 Menu 4 Internet Access Setup

The following figure shows how you apply NAT to the remote node in menu 11.1.

Step 1. Enter 11 from the main menu.

Step 2. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**



```
                    Menu 11.3 - Remote Node Network Layer Options

                      IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Addr= N/A

                      Network Address Translation= Full Feature
                      Metric= 1
                      Private= N/A
                      RIP Direction= None
                        Version= N/A
                      Multicast= None


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

Figure 23-2 Menu 11.3 Remote Node Network Layer Options

The following table describes the options for Network Address Translation.

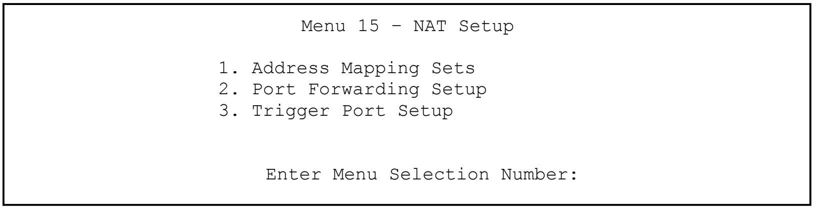
Table 23-1 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	EXAMPLE
Network Address Mapping	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your ZyAIR.	**Full Feature**
	Select **None** to disable NAT.	
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see *Section 23.2.1*). Choose **SUA Only** if you have just one public WAN IP address for your ZyAIR.	

23.2 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set, a server rule must be set up inside the NAT Address Mapping set. Please see *Section 23.3* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

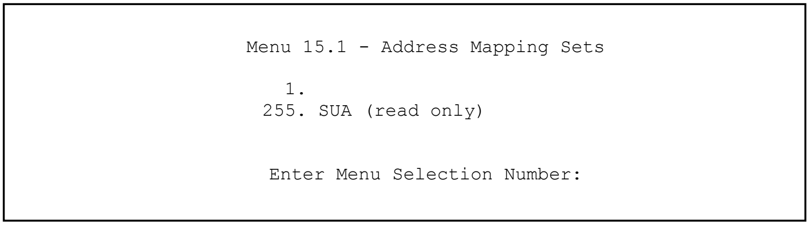


```
                          Menu 15 - NAT Setup

                   1. Address Mapping Sets
                   2. Port Forwarding Setup
                   3. Trigger Port Setup


                       Enter Menu Selection Number:
```

Figure 23-3 Menu 15 NAT Setup

23.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 – Address Mapping Sets**.



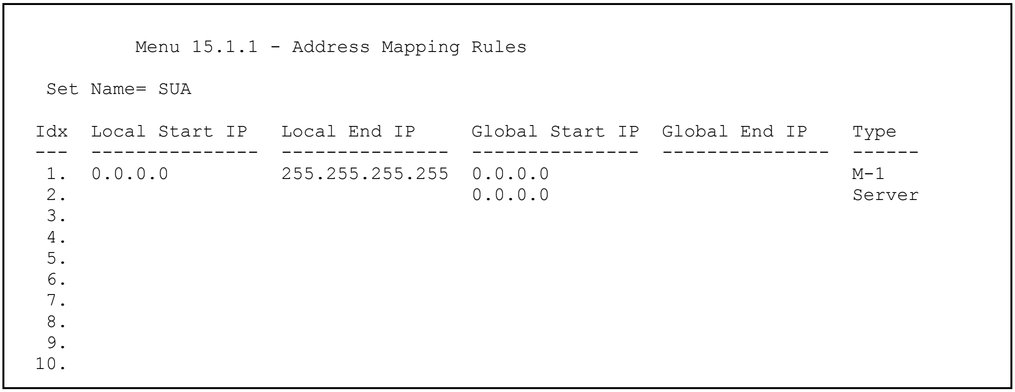
```
                   Menu 15.1 - Address Mapping Sets

                       1.
                     255. SUA (read only)


                      Enter Menu Selection Number:
```

Figure 23-4 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen. The fields in this menu cannot be changed.

Menu 15.1.255 is read-only.



```
        Menu 15.1.1 - Address Mapping Rules

 Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
```

Figure 23-5 Menu 15.1.255 SUA Address Mapping Rules

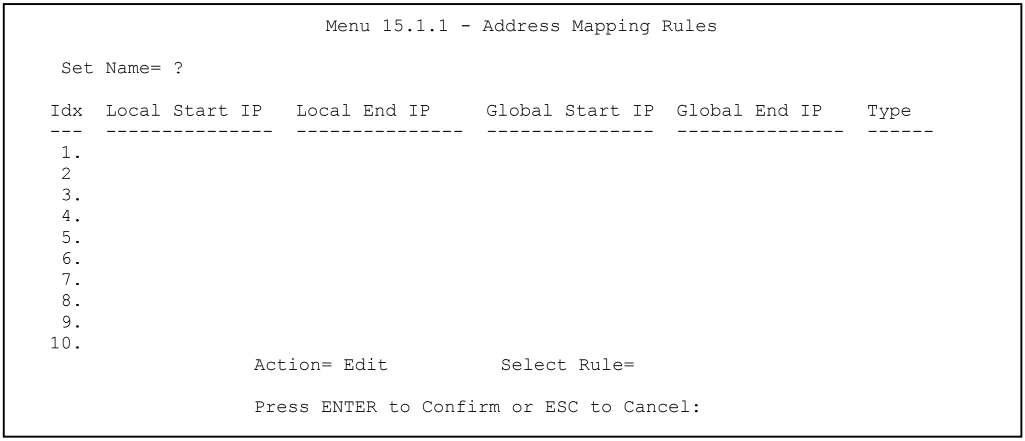
The following table explains the fields in this menu.

Table 23-2 Menu 15.1.255 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA).	0.0.0.0
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the "?" in the **Set Name** field means that this is a required field and you must enter a name for the set.



```
                          Menu 15.1.1 - Address Mapping Rules

     Set Name= ?

    Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
    ---  ---------------  ---------------  ---------------  ---------------  ------
     1.
     2
     3.
     4.
     5.
     6.
     7.
     8.
     9.
    10.
                      Action= Edit          Select Rule=

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

Figure 23-6 Menu 15.1.1 Address Mapping Rules

The table below describes the fields for configuration in this menu.

Table 23-3 Menu 15.1.1 Address Mapping Rules

FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

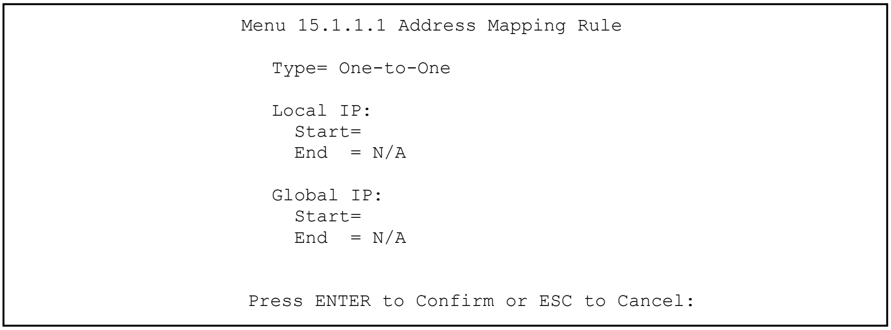
You must press [ENTER] **at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.**

An End IP address must be numerically greater than its corresponding IP Start address.

If the Set Name **field is left blank, the entire set will be deleted.**

23.2.2 Configuring Individual Rule

In **Menu 15.1.1-Address Mapping Rules**, select **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.



```
                    Menu 15.1.1.1 Address Mapping Rule

                      Type= One-to-One

                      Local IP:
                        Start=
                        End  = N/A

                      Global IP:
                        Start=
                        End  = N/A


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

Figure 23-7 Menu 15.1.1.1 Address Mapping Rule

The table below describes the fields for configuration in this menu.

Table 23-4 Menu 15.1.1.1 Address Mapping Rule

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *Section 23.4.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0

Table 23-4 Menu 15.1.1.1 Address Mapping Rule

FIELD	DESCRIPTION	EXAMPLE
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.	
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

Ordering Your Rules

Ordering your rules is important because the ZyAIR applies the rules in the order that you specify. When a rule matches the current packet, the ZyAIR takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

23.3 Port Forwarding Setup - NAT Server Sets

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 23-5 Services & Port Numbers

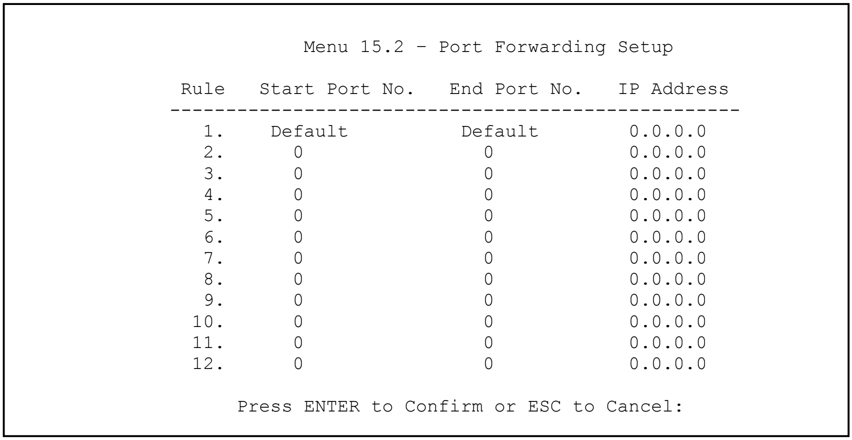
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

23.3.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to display **Menu 15.2 – Port Forwarding Setup** as shown next.



```
                Menu 15.2 - Port Forwarding Setup

     Rule   Start Port No.   End Port No.   IP Address
    ---------------------------------------------------
       1.     Default          Default        0.0.0.0
       2.       0                0            0.0.0.0
       3.       0                0            0.0.0.0
       4.       0                0            0.0.0.0
       5.       0                0            0.0.0.0
       6.       0                0            0.0.0.0
       7.       0                0            0.0.0.0
       8.       0                0            0.0.0.0
       9.       0                0            0.0.0.0
      10.       0                0            0.0.0.0
      11.       0                0            0.0.0.0
      12.       0                0            0.0.0.0

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

Figure 23-8 Menu 15.2 Port Forwarding Setup

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

23.4 General NAT Examples

23.4.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

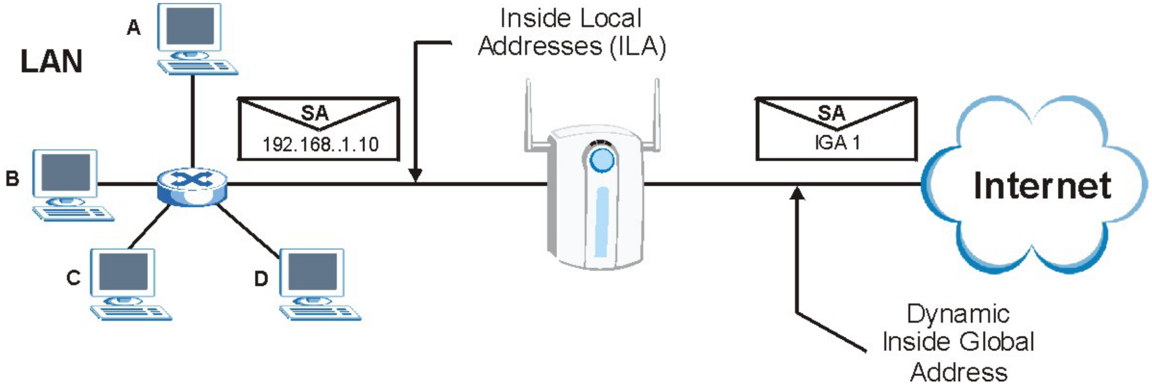
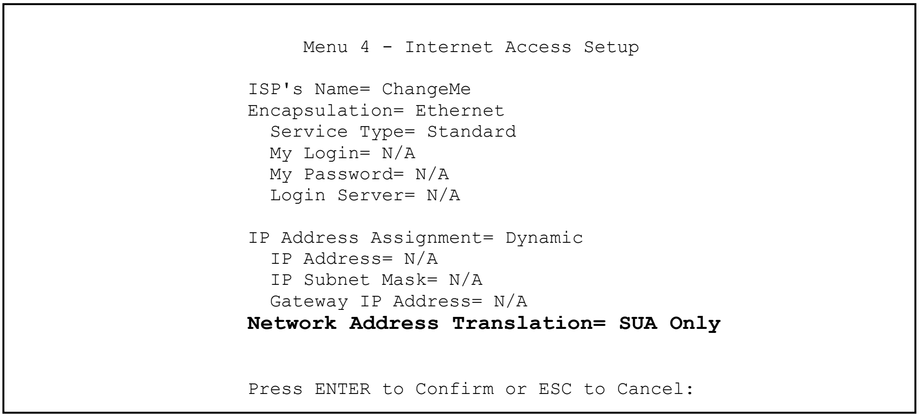


Figure 23-9 NAT Example 1



```
     Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only


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

Figure 23-10 Menu 4 Internet Access Setup

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 23.4.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

23.4.2 Example 2: Internet Access with an Inside Server

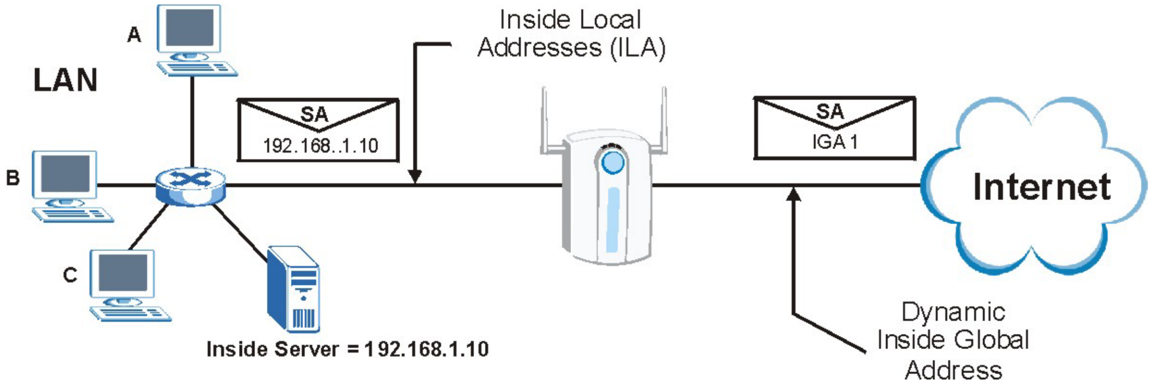
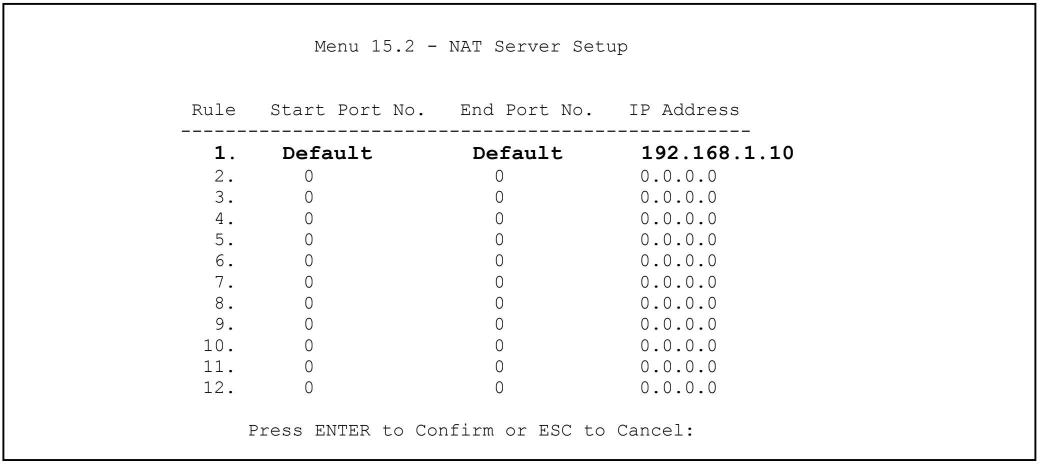


Figure 23-11 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and then go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.



```
                    Menu 15.2 - NAT Server Setup


          Rule   Start Port No.   End Port No.   IP Address
         ---------------------------------------------------
            1.     Default          Default       192.168.1.10
            2.       0                0           0.0.0.0
            3.       0                0           0.0.0.0
            4.       0                0           0.0.0.0
            5.       0                0           0.0.0.0
            6.       0                0           0.0.0.0
            7.       0                0           0.0.0.0
            8.       0                0           0.0.0.0
            9.       0                0           0.0.0.0
           10.       0                0           0.0.0.0
           11.       0                0           0.0.0.0
           12.       0                0           0.0.0.0

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

Figure 23-12 Menu 15.2.1 NAT Server Setup

23.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

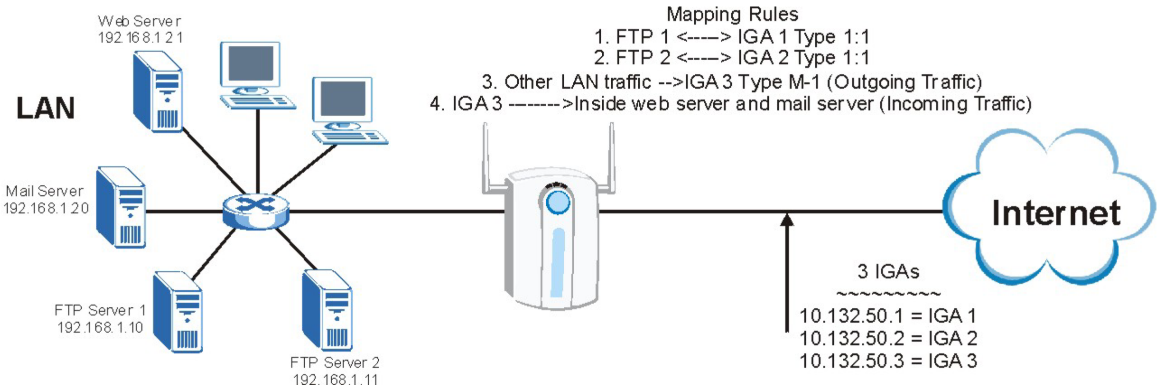
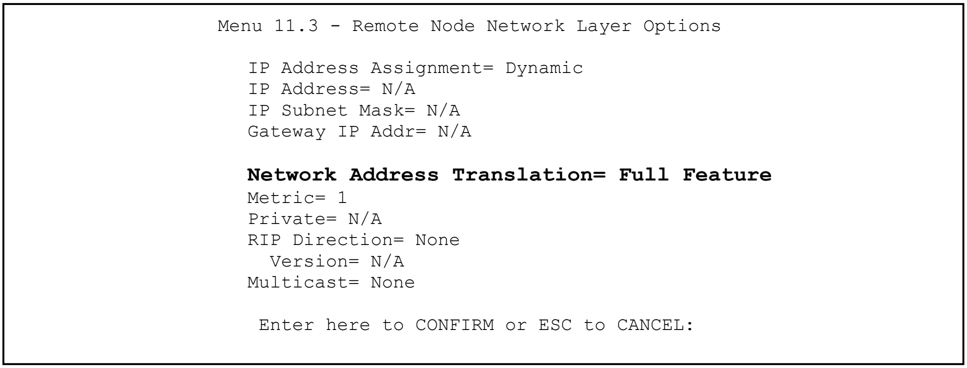


Figure 23-13 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) as shown in the finger below.



```
              Menu 11.3 - Remote Node Network Layer Options

                 IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Addr= N/A

                 Network Address Translation= Full Feature
                 Metric= 1
                 Private= N/A
                 RIP Direction= None
                   Version= N/A
                 Multicast= None

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

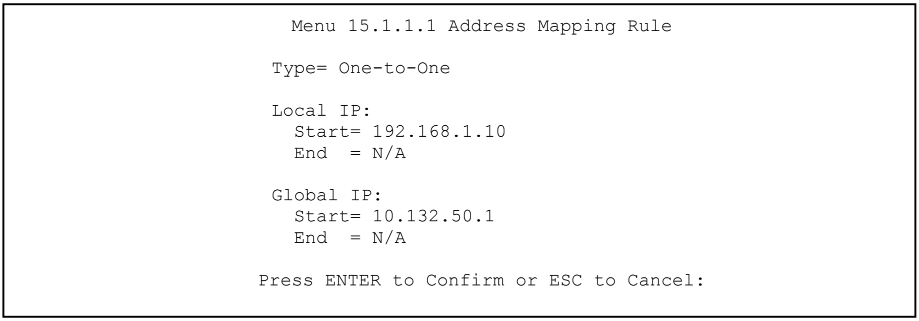
Figure 23-14 Menu 11.3 Remote Node Network Layer Options

Step 2. Then enter 15 from the main menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). The following figure shows how to configure the first rule.

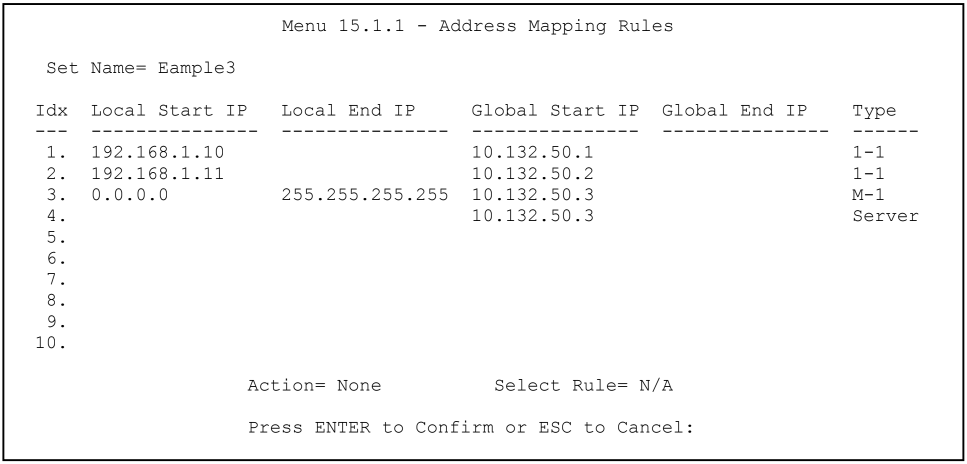


```
                  Menu 15.1.1.1 Address Mapping Rule

                 Type= One-to-One

                 Local IP:
                   Start= 192.168.1.10
                   End  = N/A

                 Global IP:
                   Start= 10.132.50.1
                   End  = N/A

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

Figure 23-15 Menu 15.1.1.1 Address Mapping Rule

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown next.



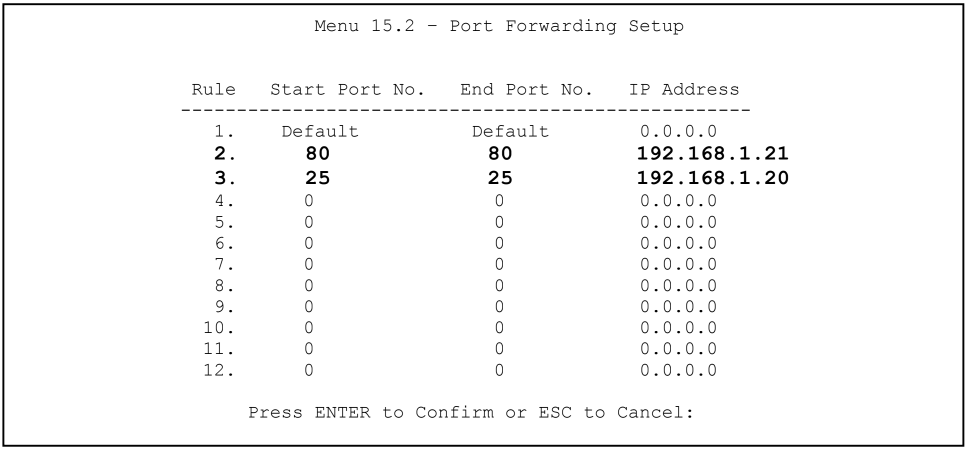
```
                        Menu 15.1.1 - Address Mapping Rules

   Set Name= Eample3

  Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
  ---  ---------------  ---------------  ---------------  ---------------  ------
   1.  192.168.1.10                      10.132.50.1                       1-1
   2.  192.168.1.11                      10.132.50.2                       1-1
   3.  0.0.0.0          255.255.255.255  10.132.50.3                       M-1
   4.                                    10.132.50.3                       Server
   5.
   6.
   7.
   8.
   9.
  10.

                     Action= None          Select Rule= N/A

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

Figure 23-16 Menu 15.1.1 Address Mapping Rules

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 1. Enter 15 from the main menu.

Step 2. Enter 2 to display **Menu 15.2 – Port Forwarding Setup** and configure it as shown.



```
                          Menu 15.2 - Port Forwarding Setup


                 Rule   Start Port No.   End Port No.   IP Address
                ---------------------------------------------------
                   1.    Default          Default        0.0.0.0
                   2.      80               80           192.168.1.21
                   3.      25               25           192.168.1.20
                   4.      0                0            0.0.0.0
                   5.      0                0            0.0.0.0
                   6.      0                0            0.0.0.0
                   7.      0                0            0.0.0.0
                   8.      0                0            0.0.0.0
                   9.      0                0            0.0.0.0
                  10.      0                0            0.0.0.0
                  11.      0                0            0.0.0.0
                  12.      0                0            0.0.0.0

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

Example 3: Menu 15.2 Port Forwarding Setup

23.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many One-to-One** mapping as port numbers do *not* change for **Many One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

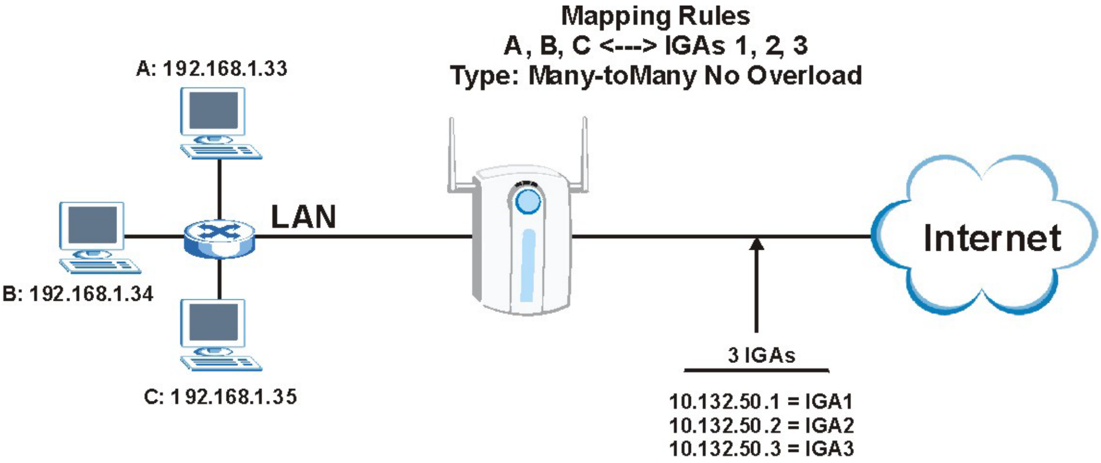
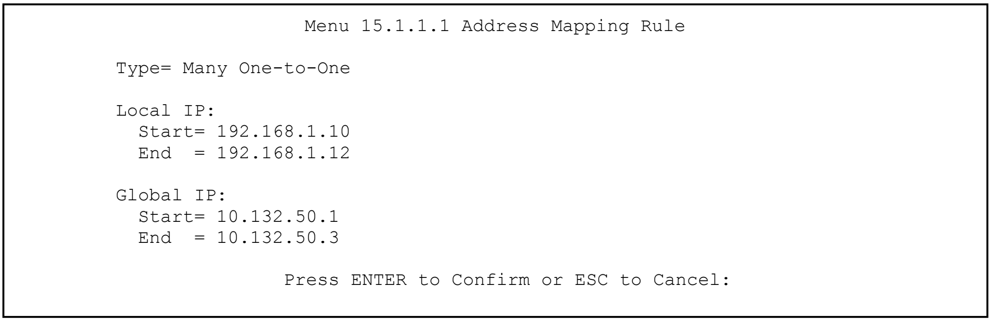


Figure 23-17 NAT Example 4

> **Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using** One-to-One **and** Many One-to-One **mapping types.**

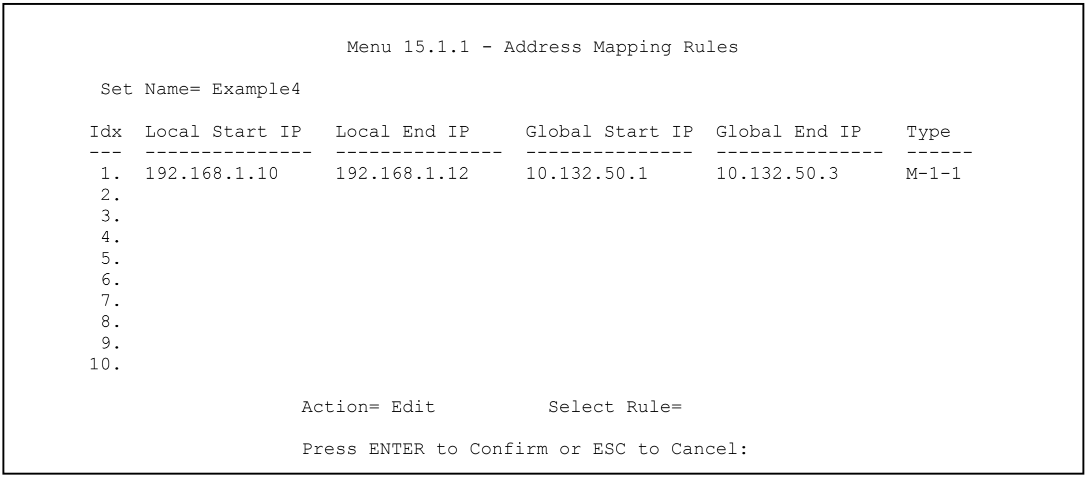
Follow the steps outlined in example 3 to configure these two menus as follows.



```
                        Menu 15.1.1.1 Address Mapping Rule

          Type= Many One-to-One

          Local IP:
            Start= 192.168.1.10
            End  = 192.168.1.12

          Global IP:
            Start= 10.132.50.1
            End  = 10.132.50.3

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

Figure 23-18 Menu 15.1.1.1 Address Mapping Rule

After you’ve configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.



```
                       Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-1-1
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                   Action= Edit         Select Rule=

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

Figure 23-19 Menu 15.1.1 Address Mapping Rules

23.5 Trigger Port Setup

The ZyAIR records the IP address of a LAN computer that requests a service that you have defined as a “trigger port”. The response from the Internet can then be forwarded directly to the LAN computer. Trigger ports are transient; they only exist while in use or are timed out. The following is a trigger port example.

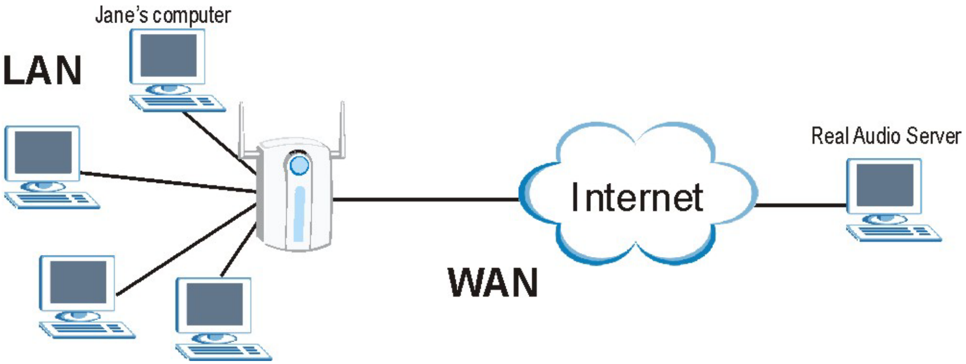


Figure 23-20 Trigger Port Forwarding Process: Example

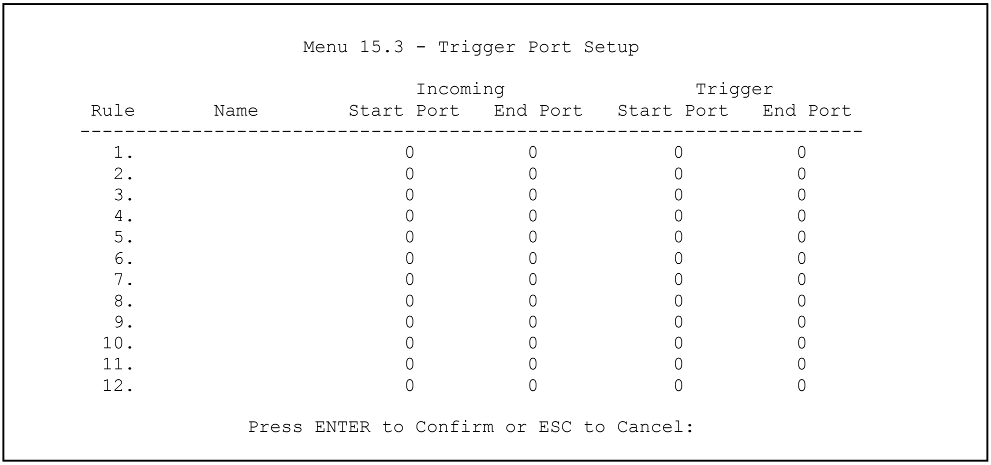
1. Jane requests a file from the Real Audio server (port 7070).

2. Port 7070 is a "trigger" port and causes the ZyAIR to record Jane's computer IP address. The ZyAIR associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyAIR forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyAIR times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Two Points To Remember About Trigger Ports

1. Trigger events only happen on outgoing data (from the ZyAIR to the WAN).
2. Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.



```
                    Menu 15.3 - Trigger Port Setup

                              Incoming                 Trigger
 Rule       Name        Start Port   End Port   Start Port   End Port
----------------------------------------------------------------------
   1.                        0          0            0          0
   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
   7.                        0          0            0          0
   8.                        0          0            0          0
   9.                        0          0            0          0
  10.                        0          0            0          0
  11.                        0          0            0          0
  12.                        0          0            0          0

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

Figure 23-21 Menu 15.3 Trigger Port Setup

The table below describes the fields for configuration in this menu.

Table 23-6 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio

Table 23-6 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyAIR forwards the traffic with this port (or range of ports) to the wireless station on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyAIR to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Part X:

SMT ADVANCED MANAGEMENT MENUS

This part discusses Filtering and Firewall setup, SNMP, System Security, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, Call Scheduling and Remote Management.

Chapter 24
Filter and Firewall Configuration

This chapter shows you how to create and apply filters and setup firewall.

24.1 About Filtering

Your ZyAIR uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your ZyAIR has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your ZyAIR applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

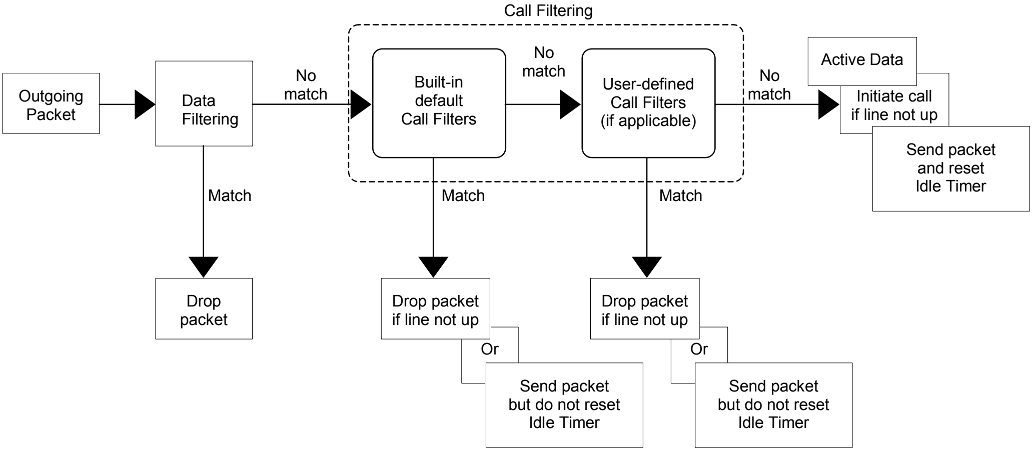

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

Figure 24-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

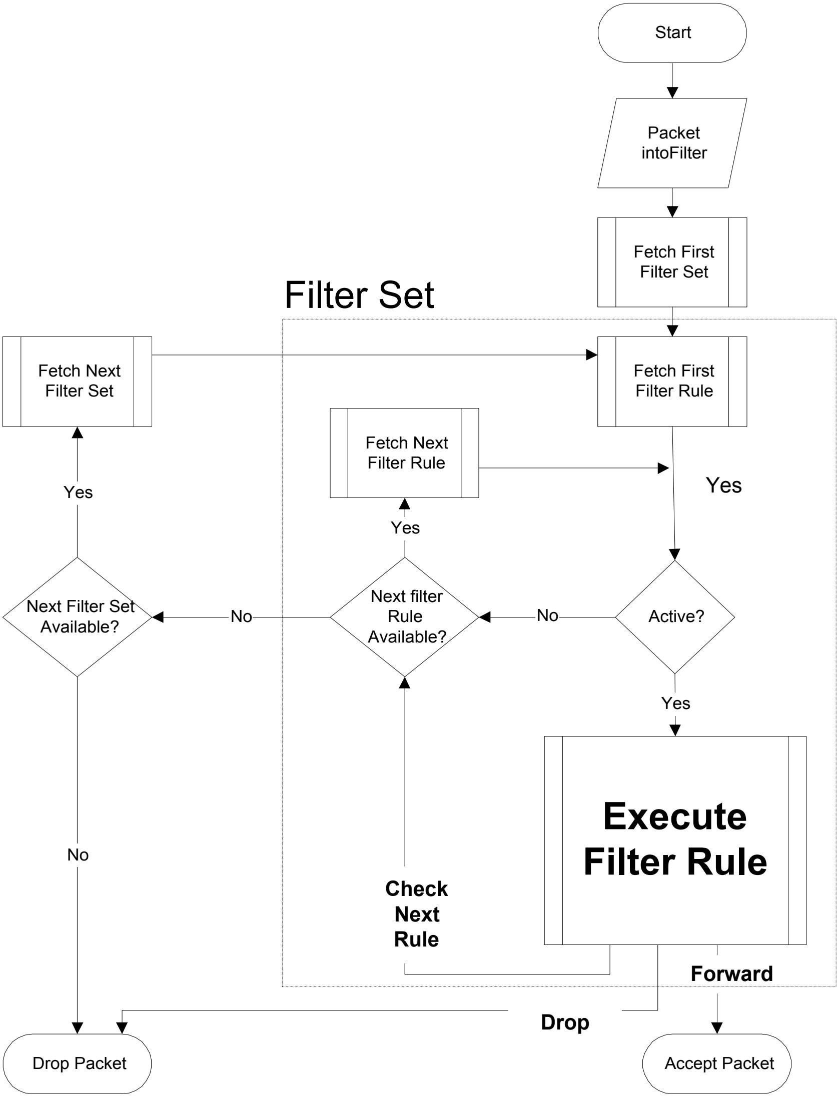


Figure 24-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your ZyAIR applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the ZyAIR

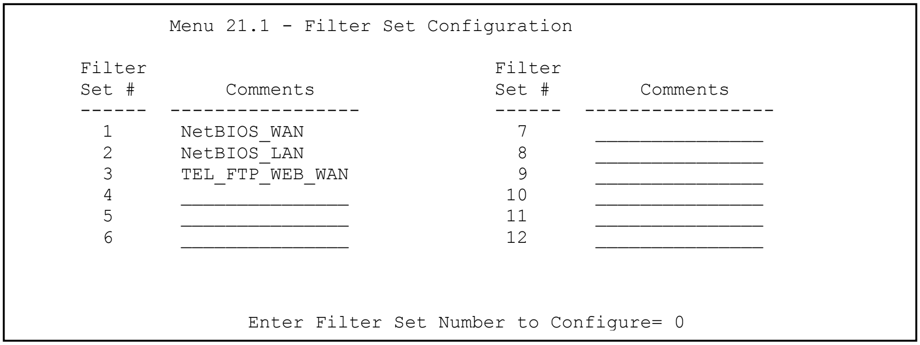
A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

24.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 from the main menu.

Step 2. Enter 1 to display **Menu 21.1 – Filter Set Configuration**.



```
                Menu 21.1 - Filter Set Configuration

        Filter                              Filter
        Set #       Comments                Set #       Comments
        ------  -----------------           ------  -----------------
          1      NetBIOS_WAN                  7      _______________
          2      NetBIOS_LAN                  8      _______________
          3      TEL_FTP_WEB_WAN              9      _______________
          4      _______________             10      _______________
          5      _______________             11      _______________
          6      _______________             12      _______________



                       Enter Filter Set Number to Configure= 0
```

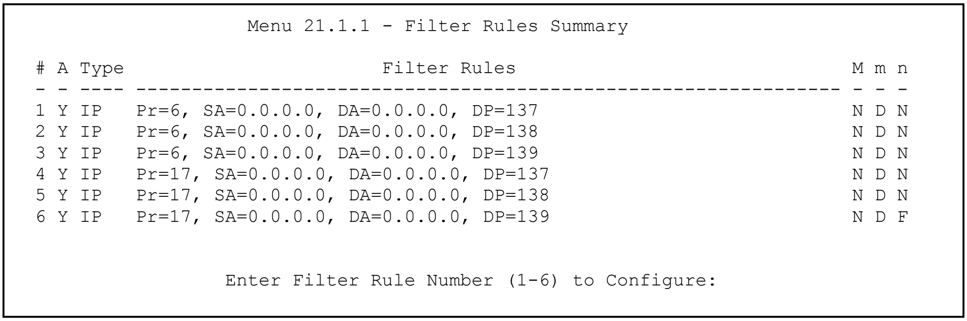
Figure 24-3 Menu 21.1 Filter Set Configuration

Step 3. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Step 4. Type a descriptive name or comment in the **Comments** field and press [ENTER].

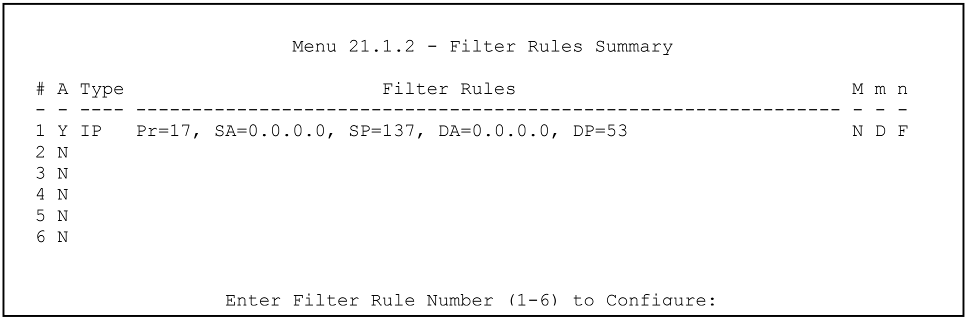
Step 5. Press [ENTER] at the message "Press ENTER to confirm…" to display **Menu 21.1.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21.1).

The following figures show the summary of three filter sets of your ZyAIR.



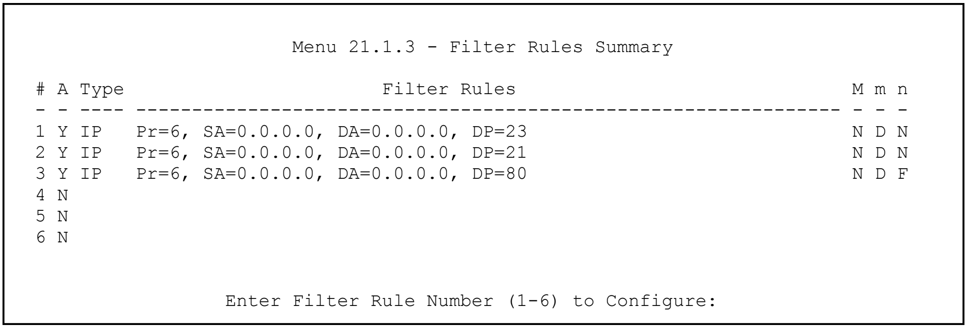
```
                   Menu 21.1.1 - Filter Rules Summary

# A Type                       Filter Rules                              M m n
- - ---- --------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                            N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                            N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                            N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                           N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                           N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                           N D F


                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 24-4 NetBIOS_WAN Filter Rules Summary



```
                       Menu 21.1.2 - Filter Rules Summary

# A Type                       Filter Rules                              M m n
- - ---- --------------------------------------------------------------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                    N D F
2 N
3 N
4 N
5 N
6 N


                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 24-5 NetBIOS_LAN Filter Rules Summary



```
                       Menu 21.1.3 - Filter Rules Summary

# A Type                       Filter Rules                              M m n
- - ---- --------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                             N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                             N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                             N D F
4 N
5 N
6 N


                 Enter Filter Rule Number (1-6) to Configure:
```

Figure 24-6 TEL_FTP_WEB_WAN Filter Rules Summary

24.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1.x.

Table 24-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 24-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	

Table 24-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
Off	Offset
Len	Length

24.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1.x for the rule.

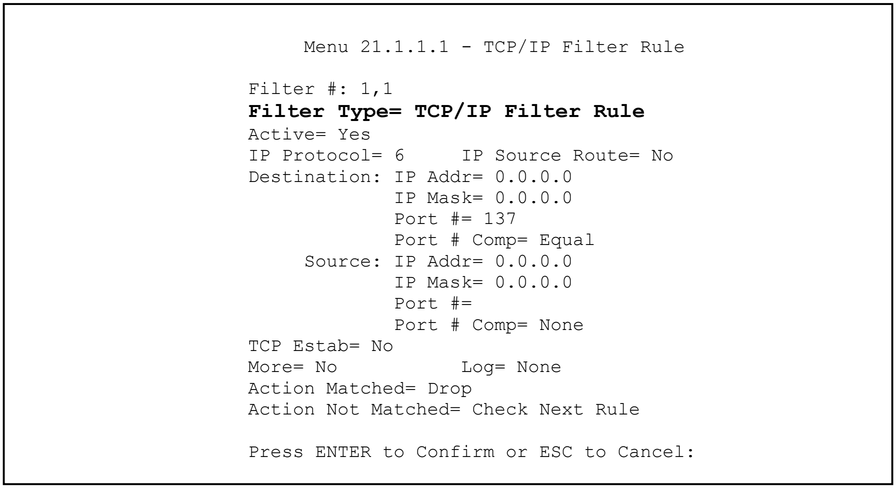
There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the ZyAIR will warn you and will not allow you to save.

24.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 – TCP/IP Filter Rule**, as shown next.



```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

               Filter #: 1,1
               Filter Type= TCP/IP Filter Rule
               Active= Yes
               IP Protocol= 6     IP Source Route= No
               Destination: IP Addr= 0.0.0.0
                            IP Mask= 0.0.0.0
                            Port #= 137
                            Port # Comp= Equal
                    Source: IP Addr= 0.0.0.0
                            IP Mask= 0.0.0.0
                            Port #=
                            Port # Comp= None
               TCP Estab= No
               More= No           Log= None
               Action Matched= Drop
               Action Not Matched= Check Next Rule

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

Figure 24-7 Menu 21.1.1 TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 24-3 Menu 21.1.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Press [SPACE BAR] and the [ENTER] to select filter type. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule**
Active	Select **Yes** to activate or **No** to deactivate the filter rule.	**No**
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)
Destination:		

Table 24-3 Menu 21.1.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source:		
IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**

Table 24-3 Menu 21.1.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
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.		

The following figure illustrates the logic flow of an IP filter.

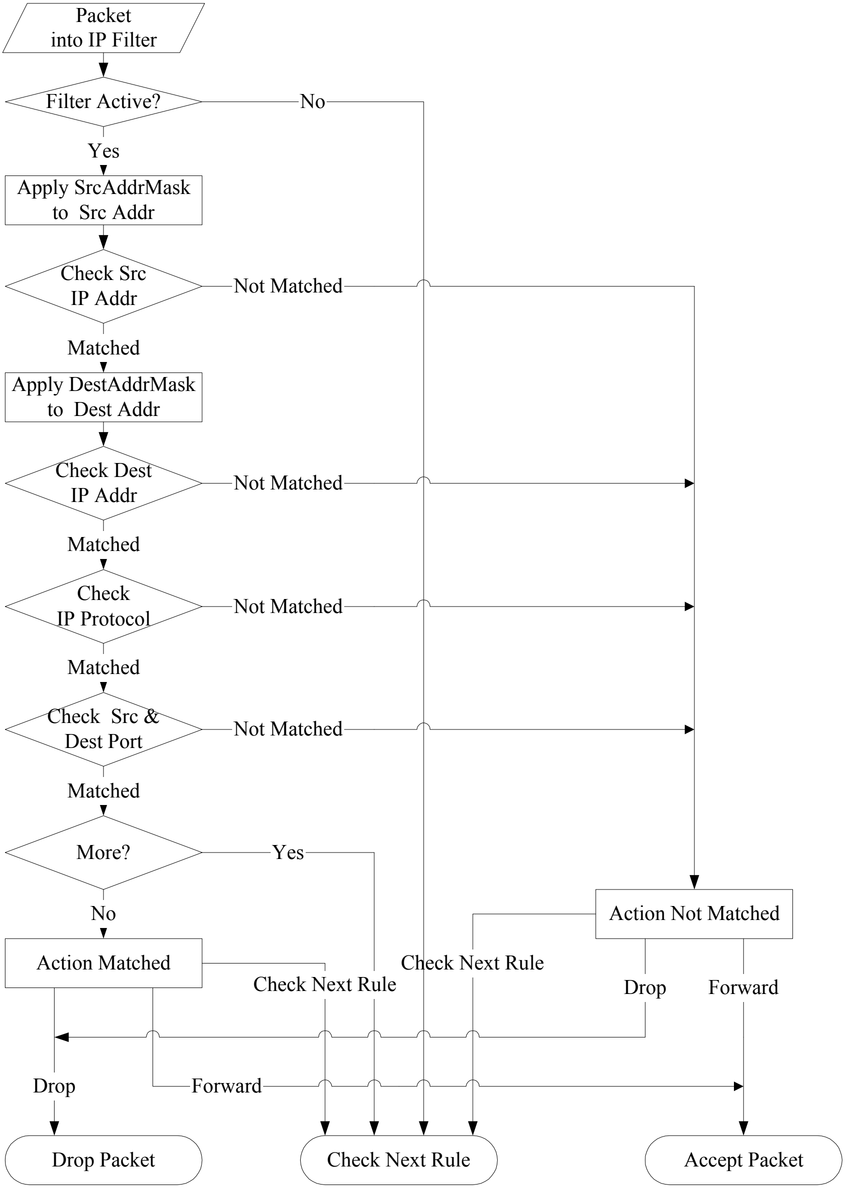


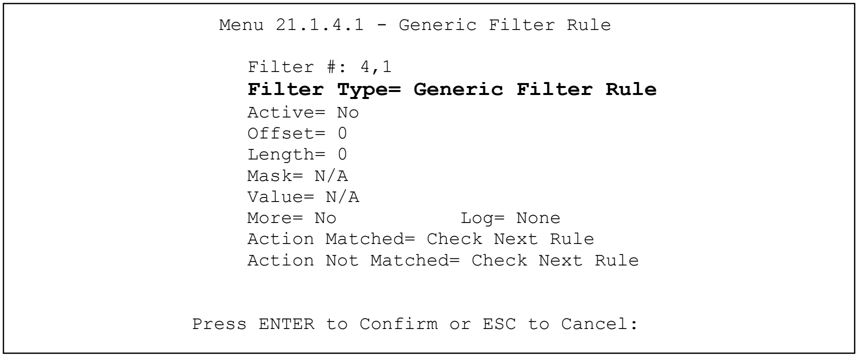
Figure 24-8 Executing an IP Filter

24.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyAIR treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyAIR applies the **Mask** (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21.1, for example 4. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.4.1 – Generic Filter Rule**, as shown in the following figure.



```
                    Menu 21.1.4.1 - Generic Filter Rule

                      Filter #: 4,1
                      Filter Type= Generic Filter Rule
                      Active= No
                      Offset= 0
                      Length= 0
                      Mask= N/A
                      Value= N/A
                      More= No           Log= None
                      Action Matched= Check Next Rule
                      Action Not Matched= Check Next Rule


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

Figure 24-9 Menu 21.1.4.1 Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 24-4 Menu 21.1.4.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	4,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to turn on the filter rule.	**No** (default)

Table 24-4 Menu 21.1.4.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	Check Next Rule
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	Check Next Rule
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.		

24.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyAIR applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the ZyAIR is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

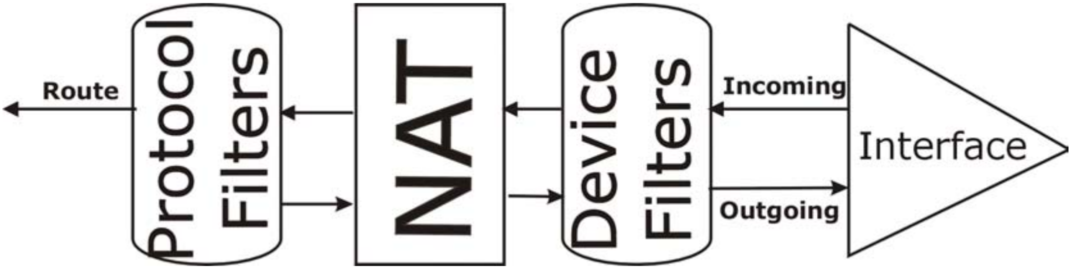


Figure 24-10 Protocol and Device Filter Sets

24.5 Example Filter

Let's look at an example to block outside users from telnetting into the ZyAIR.

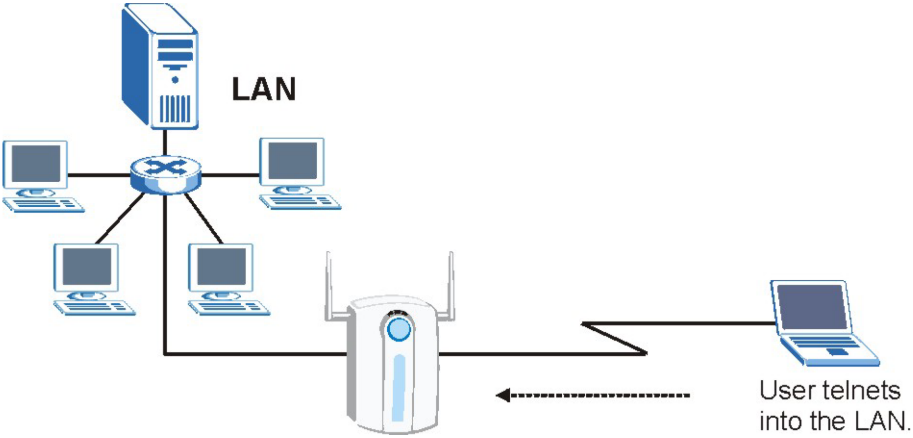


Figure 24-11 Sample Telnet Filter

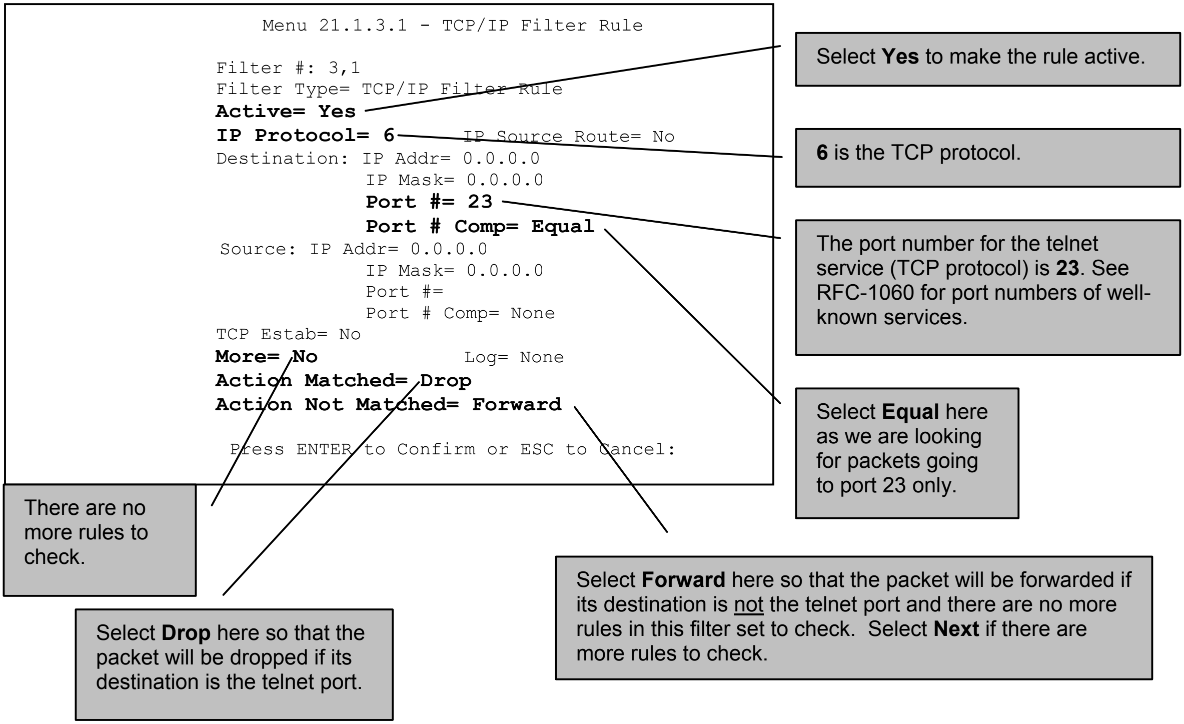
Step 1. Enter 1 in menu 21 to open **Menu 21.1 – Filter Set Configuration**.

Step 2. Enter the index number of the filter set you want to configure (in this example, 3).

Step 3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].

Step 4. Press [ENTER] at the message "Press ENTER to confirm or ESC to cancel" to open **Menu 21.1.3.1 – TCP/IP Filter Rule**.

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.



```
                    Menu 21.1.3.1 - TCP/IP Filter Rule

                Filter #: 3,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6       IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 23
                             Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #=
                             Port # Comp= None
                TCP Estab= No
                More= No              Log= None
                Action Matched= Drop
                Action Not Matched= Forward

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

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See RFC-1060 for port numbers of well-known services.

Select **Equal** here as we are looking for packets going to port 23 only.

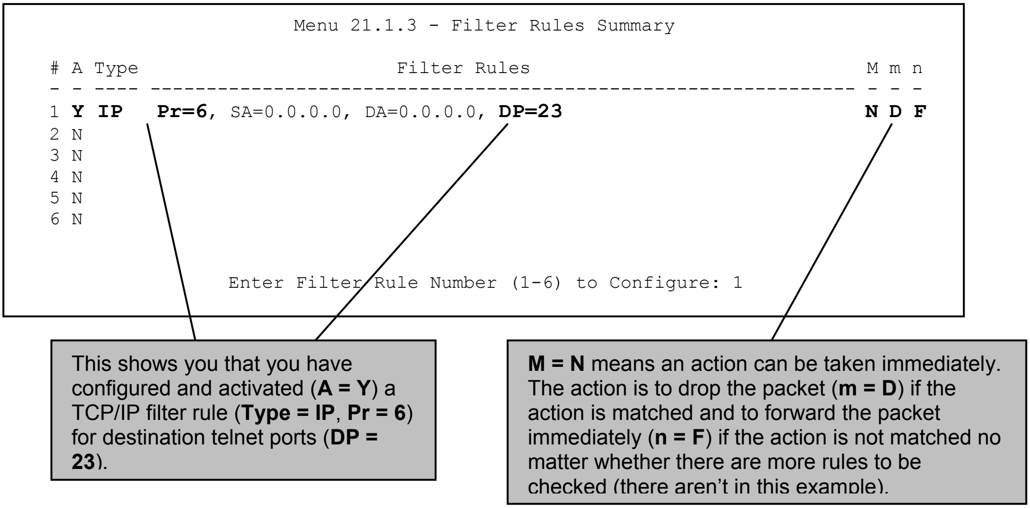
There are no more rules to check.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

Figure 24-12 Sample Filter - Menu 21.1.3.1

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.



```
                         Menu 21.1.3 - Filter Rules Summary

 # A Type                      Filter Rules                                M m n
 - - ---- --------------------------------------------------------------- - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                               N D F
 2 N
 3 N
 4 N
 5 N
 6 N


                     Enter Filter Rule Number (1-6) to Configure: 1
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 24-13 Sample Filter Rules Summary - Menu 21.1.3

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

24.6 Applying Filters and Factory Defaults

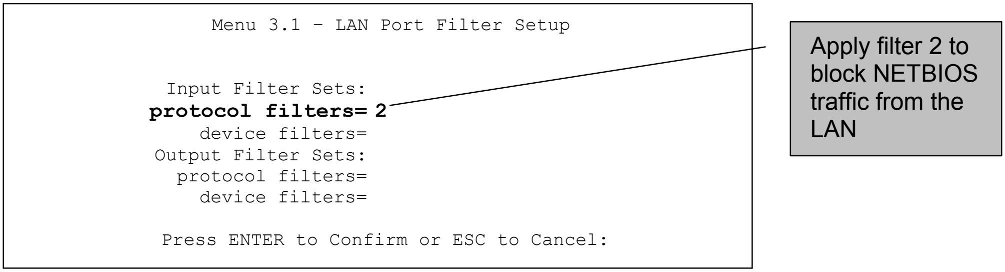
This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 24-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the ZyAIR. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

24.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.



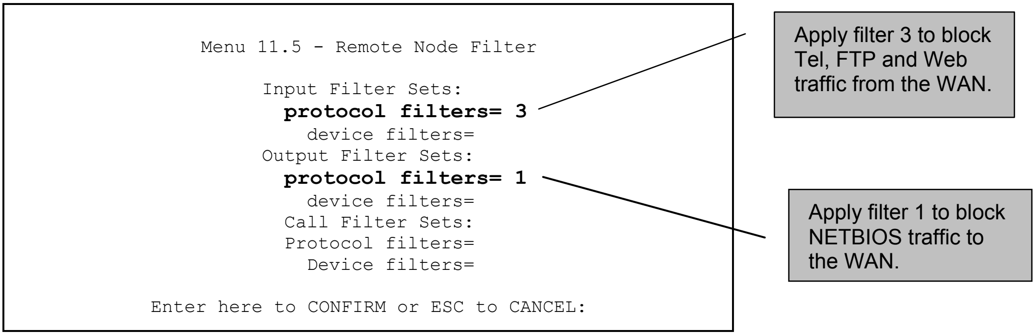
```
                  Menu 3.1 - LAN Port Filter Setup


              Input Filter Sets:
            protocol filters= 2
                 device filters=
             Output Filter Sets:
               protocol filters=
                 device filters=

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

Apply filter 2 to block NETBIOS traffic from the LAN

Figure 24-14 Filtering Ethernet Traffic

24.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.



```
                 Menu 11.5 - Remote Node Filter

                      Input Filter Sets:
                        protocol filters= 3
                          device filters=
                      Output Filter Sets:
                        protocol filters= 1
                          device filters=
                        Call Filter Sets:
                        Protocol filters=
                          Device filters=

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

Apply filter 3 to block Tel, FTP and Web traffic from the WAN.

Apply filter 1 to block NETBIOS traffic to the WAN.

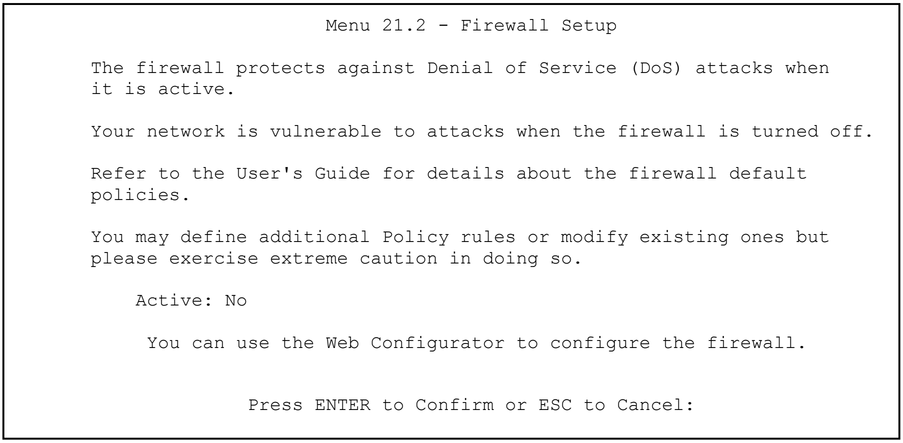
Figure 24-15 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPTP or PPPoE encapsulation.

24.7 Firewall Setup

The ZyAIR wireless gateways employ a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyAIR firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Enter 2 in menu 21 to display **Menu 21.2 — Firewall Setup**, shown next.



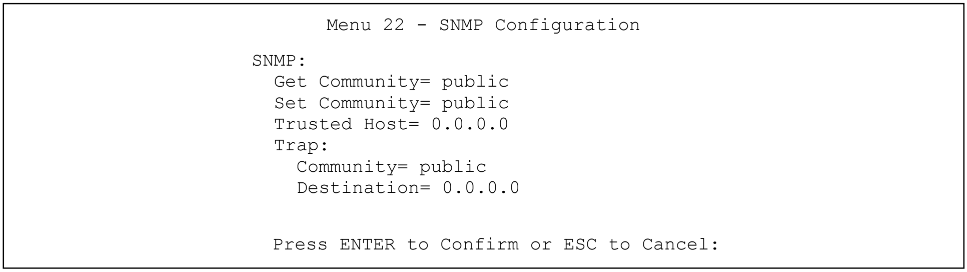
```
                         Menu 21.2 - Firewall Setup

       The firewall protects against Denial of Service (DoS) attacks when
       it is active.

       Your network is vulnerable to attacks when the firewall is turned off.

       Refer to the User's Guide for details about the firewall default
       policies.

       You may define additional Policy rules or modify existing ones but
       please exercise extreme caution in doing so.

           Active: No

            You can use the Web Configurator to configure the firewall.


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

Chapter 25
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

25.1 SNMP Configuration

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



```
                           Menu 22 - SNMP Configuration

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


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

Figure 25-1 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 25-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set Community**, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		

Table 25-1 Menu 22 SNMP Configuration

<table>
<tr><th>FIELD</th><th>DESCRIPTION</th><th>EXAMPLE</th></tr>
<tr><td>Community</td><td>Type the trap community, which is the password sent with each trap to the SNMP manager.</td><td>public</td></tr>
<tr><td>Destination</td><td>Type the IP address of the station to send your SNMP traps to.</td><td>0.0.0.0</td></tr>
<tr><td colspan="3">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.</td></tr>
</table>

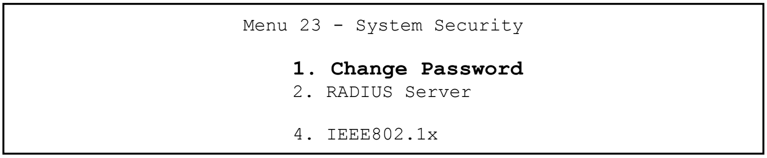
Chapter 26
System Security

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

26.1 System Security

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

26.1.1 System Password



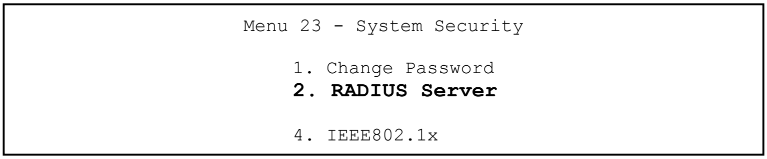
```
                    Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x
```

Figure 26-1 Menu 23 System Security

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

26.1.2 Configuring External RADIUS Server

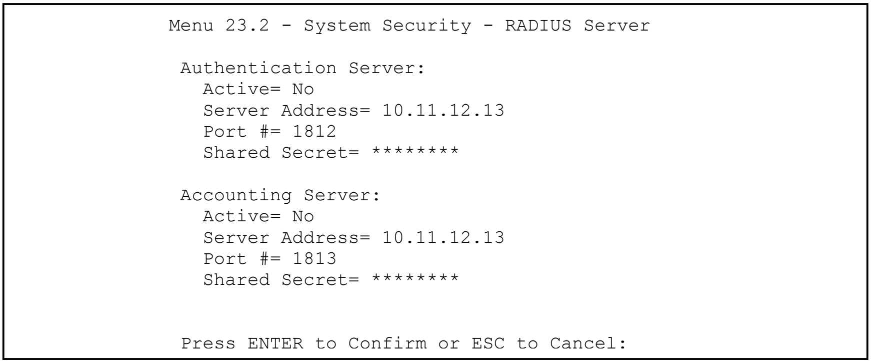
Enter 23 in the main menu to display **Menu 23 – System Security**.



```
                    Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x
```

Figure 26-2 Menu 23 System Security

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



```
                Menu 23.2 - System Security - RADIUS Server

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

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


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

Figure 26-3 Menu 23.2 System Security : RADIUS Server

The following table describes the fields in this screen.

Table 26-1 Menu 23.2 System Security : RADIUS Server

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

Table 26-1 Menu 23.2 System Security : RADIUS Server

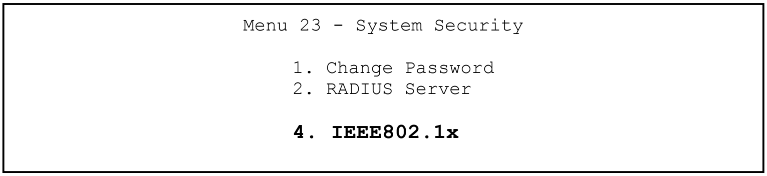
FIELD	DESCRIPTION	EXAMPLE
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1813**
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyAIR.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

26.1.3 IEEE802.1x

The IEEE802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

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

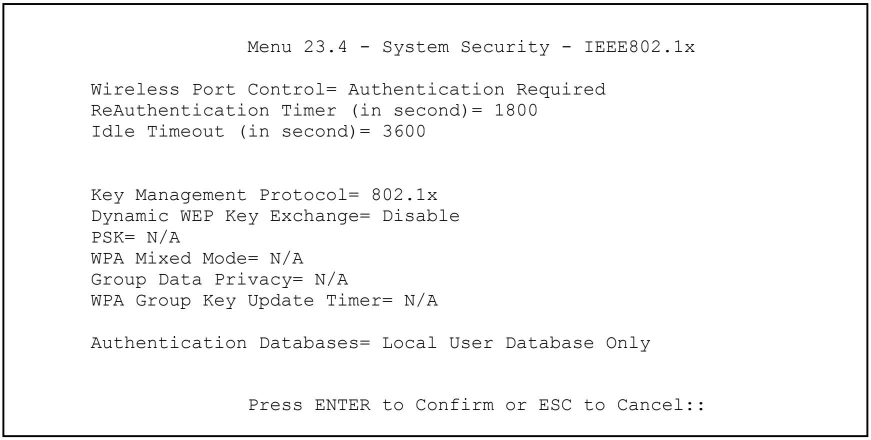
Step 1. From the main menu, enter 23 to display **Menu23 – System Security**.



```
                    Menu 23 - System Security

                        1. Change Password
                        2. RADIUS Server

                        4. IEEE802.1x
```

Figure 26-4 Menu 23 System Security

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



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

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


    Key Management Protocol= 802.1x
    Dynamic WEP Key Exchange= Disable
    PSK= N/A
    WPA Mixed Mode= N/A
    Group Data Privacy= N/A
    WPA Group Key Update Timer= N/A

    Authentication Databases= Local User Database Only


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

Figure 26-5 Menu 23.4 System Security : IEEE802.1x

The following table describes the fields in this menu.

Table 26-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **No Access Allowed** to block all wireless stations access to the wired network. 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. 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).

Table 26-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
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. 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].
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange. This feature is not available on the ZyAIR B-2000.
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 **Group Data Privacy** field.
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
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).

Table 26-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
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. Before you specify the priority, make sure you have set up the corresponding database correctly first. 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**. Select **Local User Database Only** to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password. Select **RADIUS Only** to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.
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.	

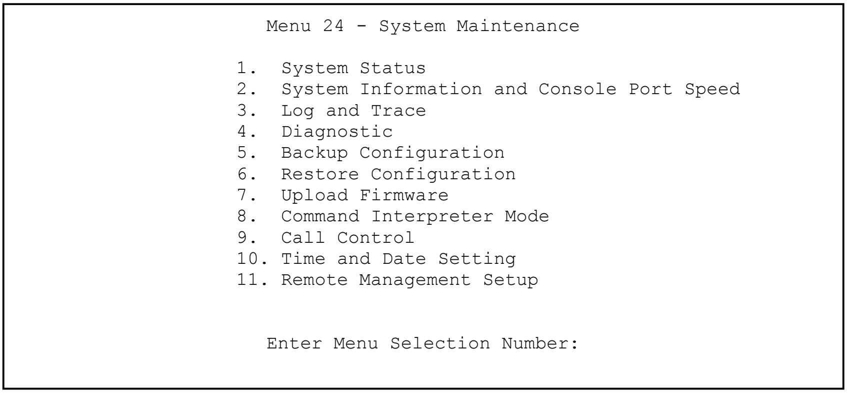
Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication.

Chapter 27 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 to open **Menu 24** - **System Maintenance**, as shown in the following figure.



```
                 Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode
              9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup


                 Enter Menu Selection Number:
```

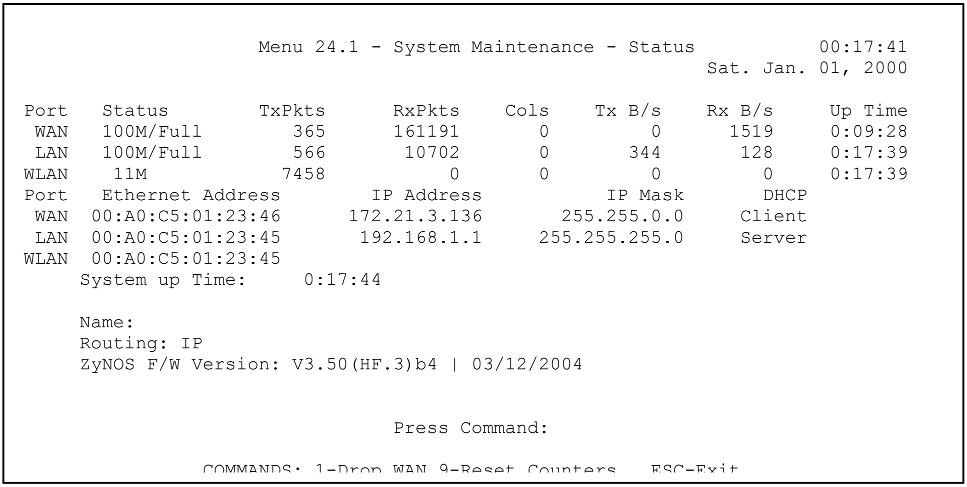
Figure 27-1 Menu 24 System Maintenance

27.1 System Status

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

To display menu 24.1 properly, make sure you use the console cable supplied to connect to the ZyAIR.



```
                      Menu 24.1 - System Maintenance - Status           00:17:41
                                                                Sat. Jan. 01, 2000

Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
 WAN   100M/Full        365      161191       0         0      1519     0:09:28
 LAN   100M/Full        566       10702       0       344       128     0:17:39
WLAN    11M            7458           0       0         0         0     0:17:39
Port   Ethernet Address        IP Address           IP Mask       DHCP
 WAN  00:A0:C5:01:23:46      172.21.3.136       255.255.0.0     Client
 LAN  00:A0:C5:01:23:45       192.168.1.1     255.255.255.0     Server
WLAN  00:A0:C5:01:23:45
     System up Time:     0:17:44

     Name:
     Routing: IP
     ZyNOS F/W Version: V3.50(HF.3)b4 | 03/12/2004


                                 Press Command:

                 COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

Figure 27-2 Menu 24.1 System Maintenance : Status

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

Table 27-1 Menu 24.1 System Maintenance : Status

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

Table 27-1 Menu 24.1 System Maintenance : Status

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

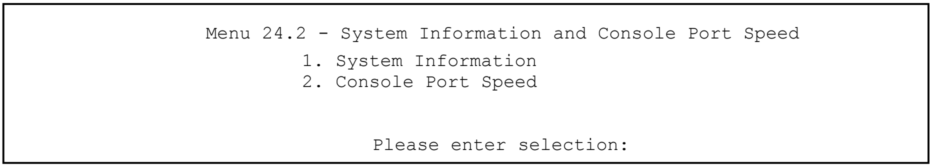
27.2 System Information

To get to the System Information:

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

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

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



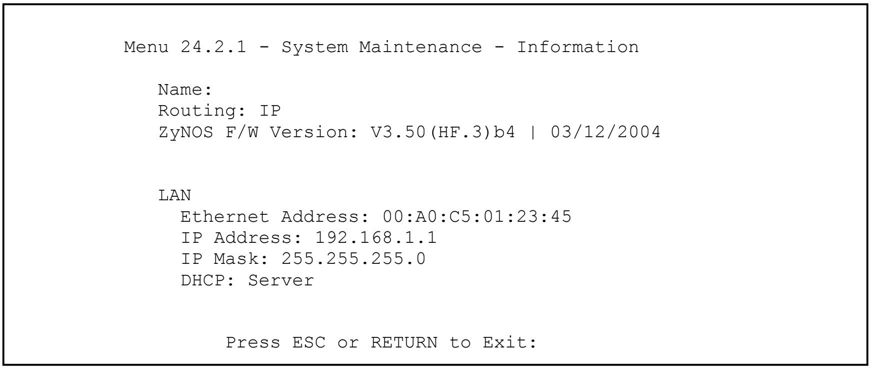
```
                  Menu 24.2 - System Information and Console Port Speed
                           1. System Information
                           2. Console Port Speed


                                 Please enter selection:
```

Figure 27-3 Menu 24.2 System Information and Console Port Speed

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

27.2.1 System Information

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



```
          Menu 24.2.1 - System Maintenance - Information

             Name:
             Routing: IP
             ZyNOS F/W Version: V3.50(HF.3)b4 | 03/12/2004


             LAN
               Ethernet Address: 00:A0:C5:01:23:45
               IP Address: 192.168.1.1
               IP Mask: 255.255.255.0
               DHCP: Server


                   Press ESC or RETURN to Exit:
```

Figure 27-4 Menu 24.2.1 System Maintenance : Information

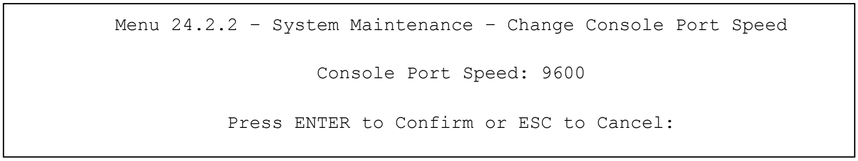
The table below describes the fields for configuration in this menu.

Table 27-2 Menu 24.2.1 System Maintenance – Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
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.	

27.2.2 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.



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

                           Console Port Speed: 9600

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

Figure 27-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

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

27.3 Log and Trace

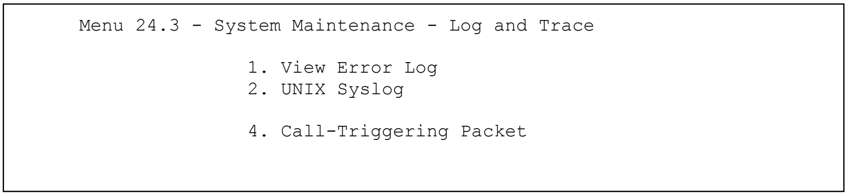
There are two logging facilities in the ZyAIR. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

27.3.1 Viewing Error Log

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

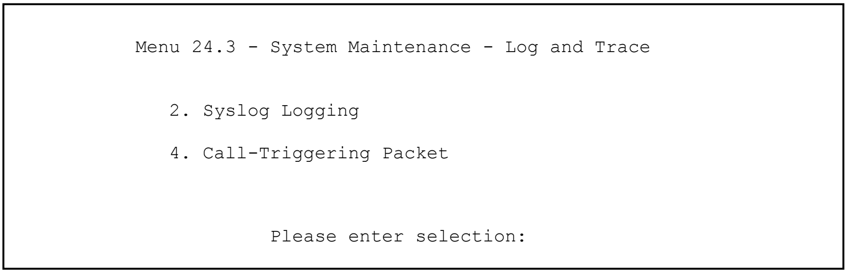
Step 1. Type 24 in the main menu to display **Menu 24** – **System Maintenance**.

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



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

                     1. View Error Log
                     2. UNIX Syslog

                     4. Call-Triggering Packet
```

Figure 27-6 Menu 24.3 System Maintenance : Log and Trace (ZyAIR B-2000)

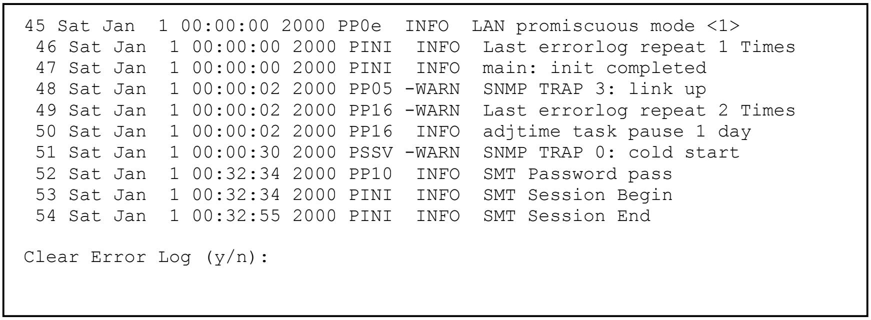


```
             Menu 24.3 - System Maintenance - Log and Trace


                 2. Syslog Logging

                 4. Call-Triggering Packet



                            Please enter selection:
```

Figure 27-7 Menu 24.3 System Maintenance : Log and Trace

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

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

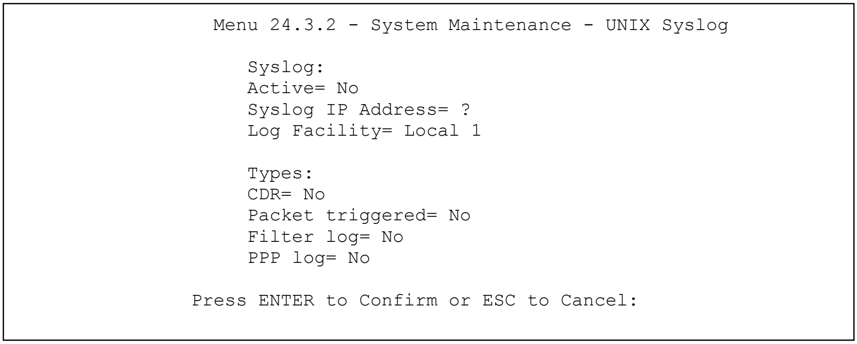


```
45 Sat Jan  1 00:00:00 2000 PP0e  INFO  LAN promiscuous mode <1>
 46 Sat Jan  1 00:00:00 2000 PINI  INFO  Last errorlog repeat 1 Times
 47 Sat Jan  1 00:00:00 2000 PINI  INFO  main: init completed
 48 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
 49 Sat Jan  1 00:00:02 2000 PP16 -WARN  Last errorlog repeat 2 Times
 50 Sat Jan  1 00:00:02 2000 PP16  INFO  adjtime task pause 1 day
 51 Sat Jan  1 00:00:30 2000 PSSV -WARN  SNMP TRAP 0: cold start
 52 Sat Jan  1 00:32:34 2000 PP10  INFO  SMT Password pass
 53 Sat Jan  1 00:32:34 2000 PINI  INFO  SMT Session Begin
 54 Sat Jan  1 00:32:55 2000 PINI  INFO  SMT Session End

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

Figure 27-8 Sample Error and Information Messages

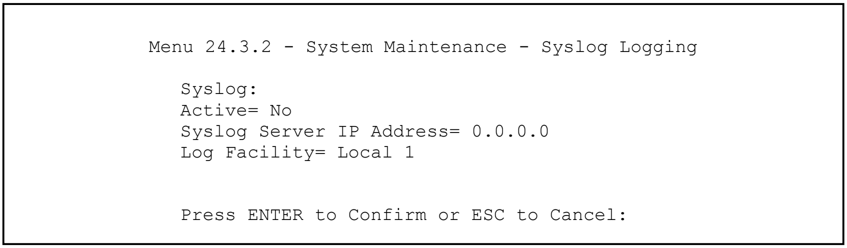
27.3.2 Syslog Logging

The ZyAIR uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog can be configured in **Menu 24.3.2** – **System Maintenance** – **UNIX Syslog**, as shown next.



```
                 Menu 24.3.2 - System Maintenance - UNIX Syslog

                    Syslog:
                    Active= No
                    Syslog IP Address= ?
                    Log Facility= Local 1

                    Types:
                    CDR= No
                    Packet triggered= No
                    Filter log= No
                    PPP log= No

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

Figure 27-9 Menu 24.3.2 System Maintenance : UNIX Syslog (ZyAIR B-2000)



```
          Menu 24.3.2 - System Maintenance - Syslog Logging

             Syslog:
             Active= No
             Syslog Server IP Address= 0.0.0.0
             Log Facility= Local 1


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

Figure 27-10 Menu 24.3.2 System Maintenance : Syslog Logging

You need to configure the UNIX syslog parameters described in the following table to activate syslog and then choose what you want to log.

Table 27-3 Menu 24.3.2 System Maintenance : Syslog Logging

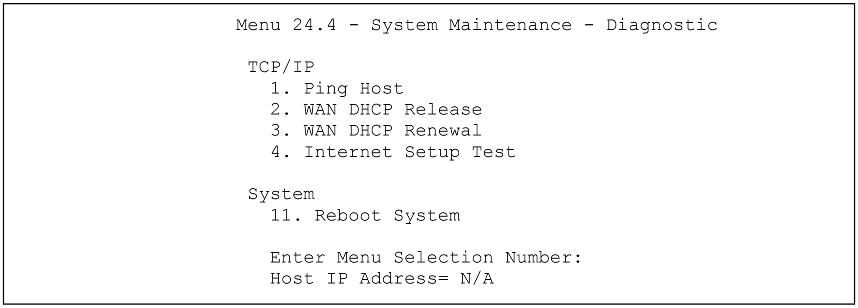
FIELD	DESCRIPTION
Syslog:	Syslog logging sends a log to an external syslog server used to store logs.
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select one of seven different local options. 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.
Types:	The following fields are not available on all models.
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter Log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** are logged when this field is set to **Yes**.
PPP Log	PPP events are logged when this field is set to **Yes**.
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.	

27.3.3 Call-Triggering Packet

Call-triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hexadecimal format.

27.4 Diagnostic

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



```
                    Menu 24.4 - System Maintenance - Diagnostic

                     TCP/IP
                       1. Ping Host
                       2. WAN DHCP Release
                       3. WAN DHCP Renewal
                       4. Internet Setup Test

                     System
                       11. Reboot System

                       Enter Menu Selection Number:
                       Host IP Address= N/A
```

Figure 27-11 Menu 24.4 System Maintenance : Diagnostic

Follow the procedure next to get to display this menu:

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

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

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

Table 27-4 Menu 24.4 System Maintenance : 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.
Internet Setup Test	Use this option to test your Internet connection.
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 28 Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

28.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, 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) may 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. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

Table 28-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	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.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyAIR.	*.bin

28.2 Backup Configuration

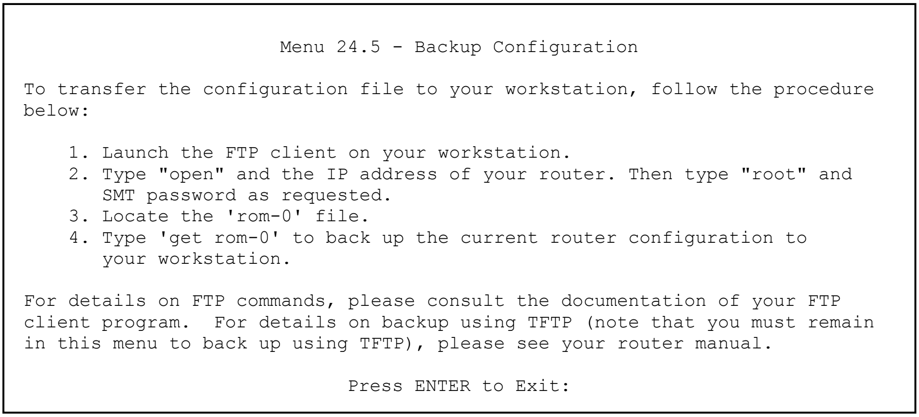
The ZyAIR displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

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 methods for backing up your current configuration to your computer since they are faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that 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.

28.2.1 Backup Configuration

Follow the instructions as shown in the next screen.



```
                       Menu 24.5 - Backup Configuration

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

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

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

                             Press ENTER to Exit:
```

Figure 28-1 Telnet in Menu 24.5

28.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your ZyAIR.

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

Step 4. Enter your password as requested (the default is "1234").

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

Step 6. Use "get" to transfer files from the ZyAIR to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyAIR to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

28.2.3 Example of FTP Commands from the Command Line

```
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: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 28-2 FTP Session Example

28.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 28-2 General Commands for GUI-based FTP Clients

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

28.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

3. The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyAIR will disconnect the Telnet session immediately.

4. You have an SMT console session running.

28.2.6 Backup Configuration Using TFTP

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

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

Step 1. Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.

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

Step 3. Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

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

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

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

28.2.7 TFTP Command Example

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.

28.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 28-3 General Commands for GUI-based TFTP Clients

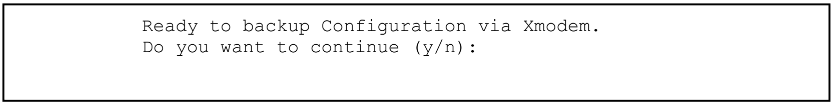
COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.1 is the ZyAIR’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyAIR and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyAIR. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 28.2.5* to read about configurations that disallow TFTP and FTP over WAN.

28.2.9 Backup Via Console Port (only for ZyAIR B-2000)

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

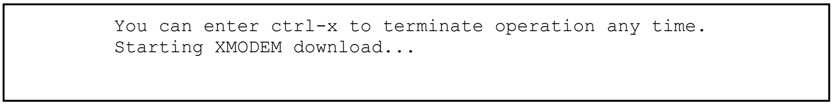
Step 1. Display menu 24.5 and enter “y” at the following screen.



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

Figure 28-3 System Maintenance : Backup Configuration

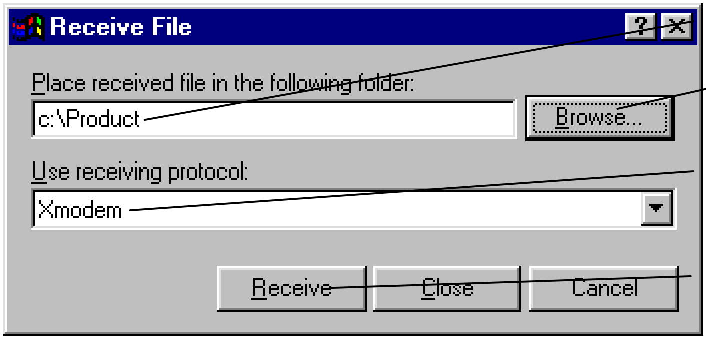
Step 2. The following screen indicates that the Xmodem download has started.



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

Figure 28-4 System Maintenance : Starting Xmodem Download Screen

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



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**.

Figure 28-5 Backup Configuration Example

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

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

Figure 28-6 Successful Backup Confirmation Screen

28.3 Restore Configuration

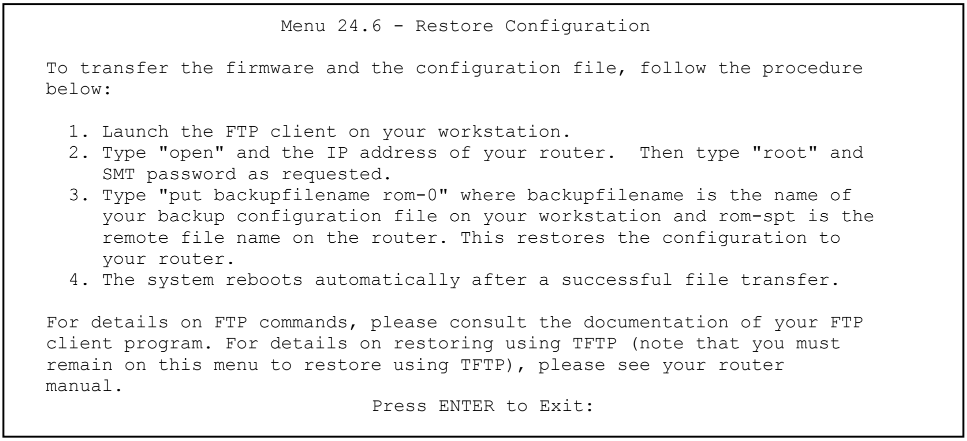
This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your ZyAIR since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYAIR. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE ZYAIR WILL AUTOMATICALLY RESTART.

28.3.1 Restore Using FTP

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



```
                       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 on this menu to restore using TFTP), please see your router
  manual.
                              Press ENTER to Exit:
```

Figure 28-7 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your ZyAIR.

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

Step 4. Enter your password as requested (the default is "1234").

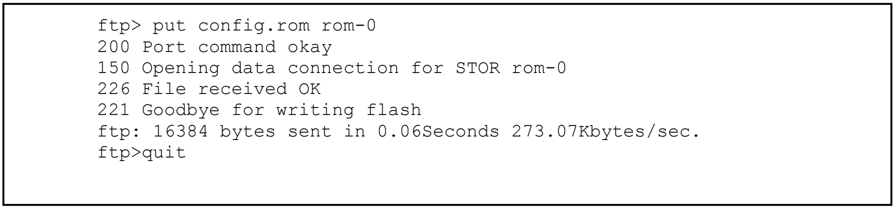
Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Find the "rom" file (on your computer) that you want to restore to your ZyAIR.

Step 7. Use "put" to transfer files from the ZyAIR to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the ZyAIR. See earlier in this chapter for more information on filename conventions.

Step 8. Enter "quit" to exit the ftp prompt. The ZyAIR will automatically restart after a successful restore process.

28.3.2 Restore Using FTP Session Example



```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

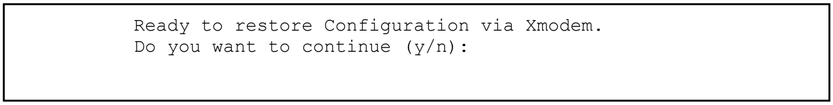
Figure 28-8 Restore Using FTP Session Example

Refer to *section 28.2.5* to read about configurations that disallow TFTP and FTP over WAN.

28.3.3 Restore Via Console Port (only for ZyAIR B-2000)

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

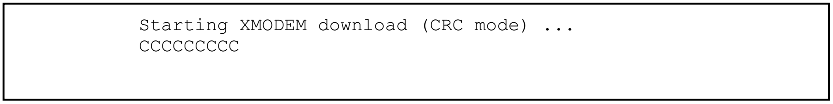
Step 1. Display menu 24.6 and enter “y” at the following screen.



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

Figure 28-9 System Maintenance : Restore Configuration

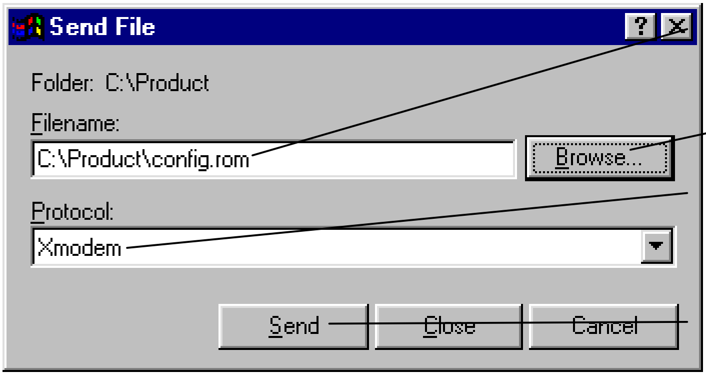
Step 2. The following screen indicates that the Xmodem download has started.



```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 28-10 System Maintenance : Starting Xmodem Download Screen

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



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**.

Figure 28-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the ZyAIR and return to the SMT menu.

```
                Save to ROM
                Hit any key to start system reboot.
```

Figure 28-12 Successful Restoration Confirmation Screen

28.4 Uploading Firmware and Configuration Files

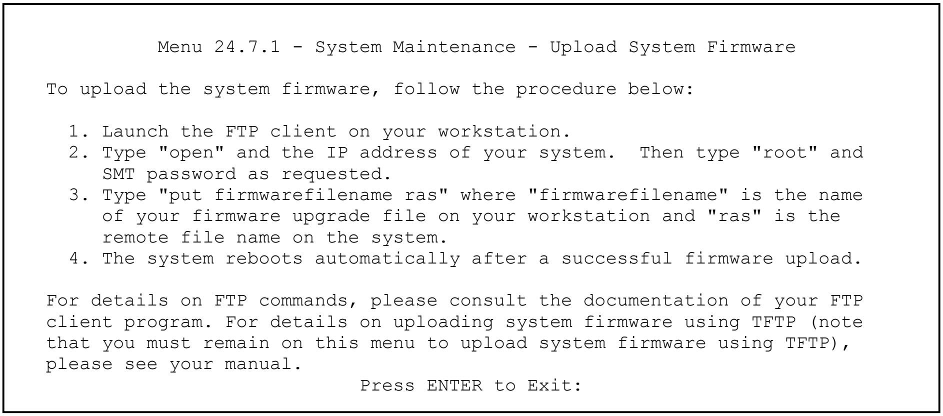
This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYAIR.

28.4.1 Firmware File Upload

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

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

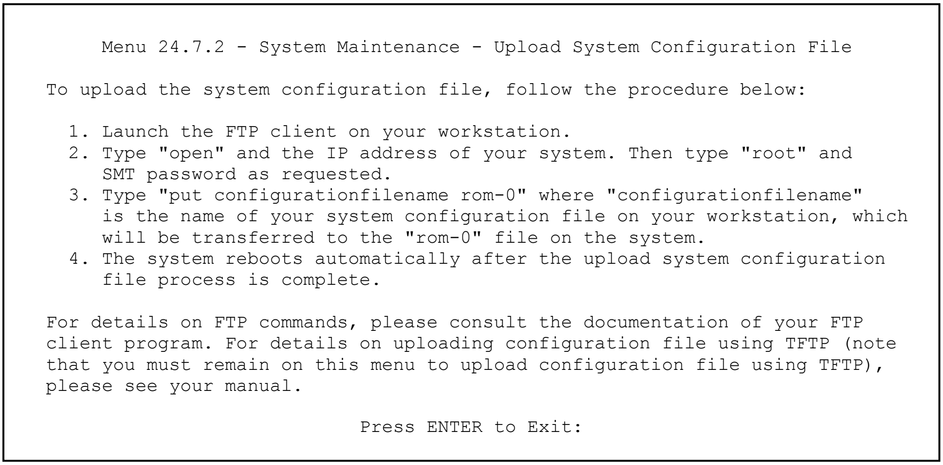


```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

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

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

Figure 28-13 Telnet Into Menu 24.7.1 Upload System Firmware

28.4.2 Configuration File Upload

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



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

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

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

                              Press ENTER to Exit:
```

Figure 28-14 Telnet Into Menu 24.7.2 System Maintenance

To upload the firmware and the configuration file, follow these examples

28.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyAIR.

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

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the ZyAIR, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyAIR and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyAIR and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

28.4.4 FTP Session Example of Firmware File Upload

```
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: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 28-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 28.2.5* to read about configurations that disallow TFTP and FTP over WAN.

28.4.5 TFTP File Upload

The ZyAIR also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

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

Step 1. Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.

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

Step 3. Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

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

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the ZyAIR 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.

28.4.6 TFTP Upload Command Example

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 and "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 GUI-based TFTP clients are listed earlier in this chapter.

28.4.7 Uploading Via Console Port (only for ZyAIR B-2000)

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.

28.4.8 Uploading Firmware File Via Console Port (only for ZyAIR B-2000)

Step 1. 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.

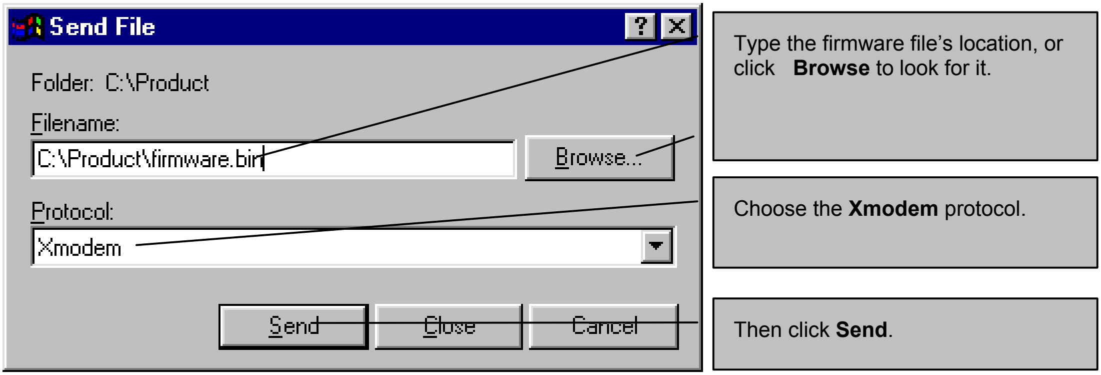
```
                 Menu 24.7.1 - System Maintenance - Upload System Firmware


              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)
```

Figure 28-16 Menu 24.7.1 as seen using the Console Port

Step 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.

28.4.9 Example Xmodem Firmware Upload Using HyperTerminal

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



Folder: C:\Product

Filename: C:\Product\firmware.bin

Protocol: Xmodem

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

Choose the **Xmodem** protocol.

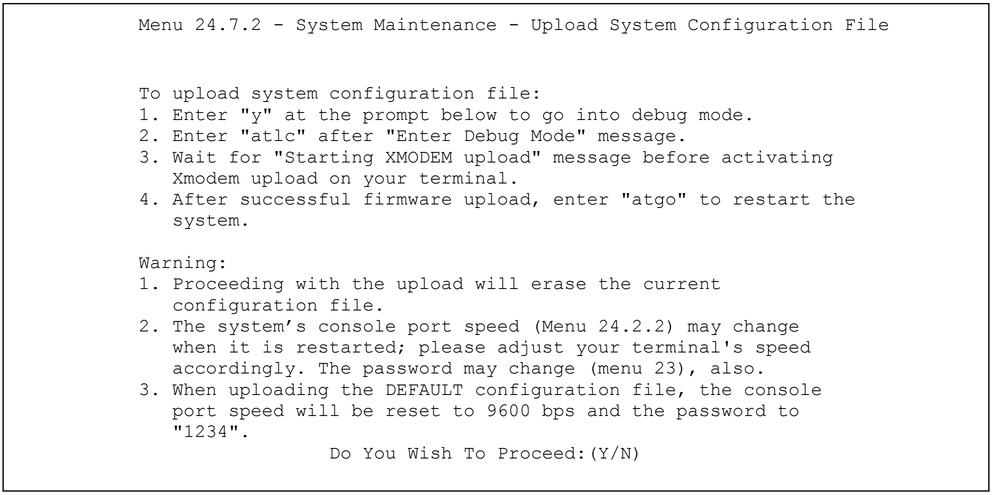
Then click **Send**.

Figure 28-17 Example Xmodem Upload

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

28.4.10Uploading Configuration File Via Console Port (only for ZyAIR B-2000)

Step 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.



```
            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)
```

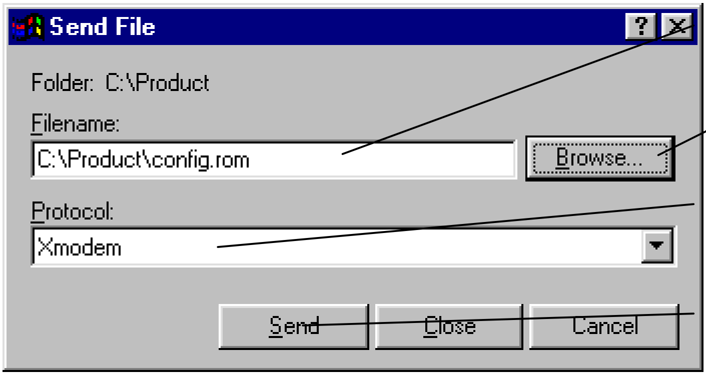
Figure 28-18 Menu 24.7.2 as seen using the Console Port

Step 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.

Step 3. Enter "atgo" to restart the ZyAIR.

28.4.11Example Xmodem Configuration Upload Using HyperTerminal

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



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**.

Figure 28-19 Example Xmodem Upload

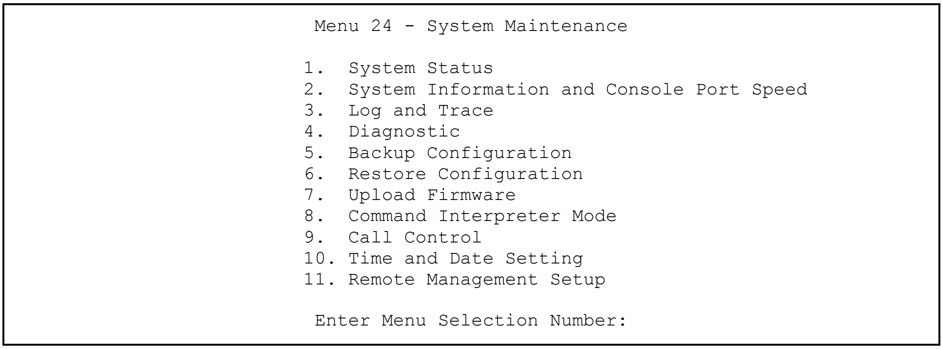
After the configuration upload process has completed, restart the ZyAIR by entering "atgo".

Chapter 29
System Maintenance and SMT Menu 24.8 to 24.10

This chapter leads you through SMT menus 24.8 to 24.10.

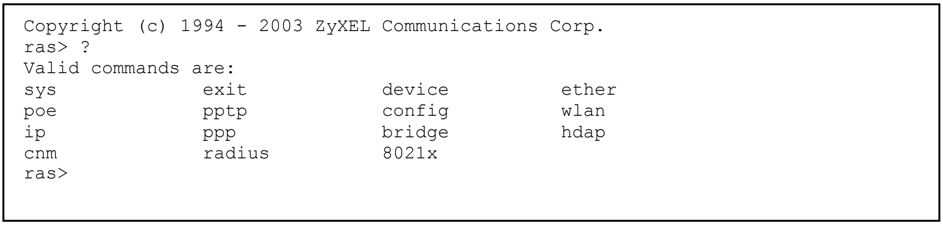
29.1 Command Interpreter Mode

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



```
                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Upload Firmware
                         8.  Command Interpreter Mode
                         9.  Call Control
                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

Figure 29-1 Menu 24 System Maintenance



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

Figure 29-2 Valid CI Commands

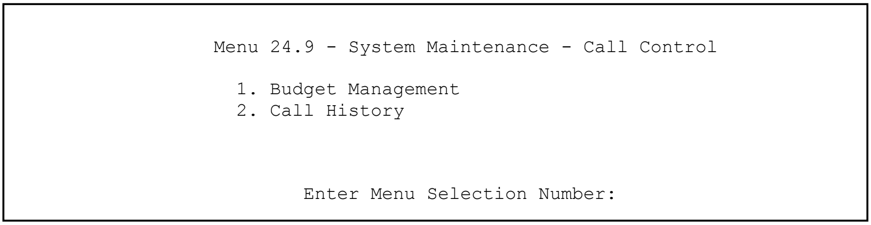
29.2 Call Control Support

The ZyAIR provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyAIR within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

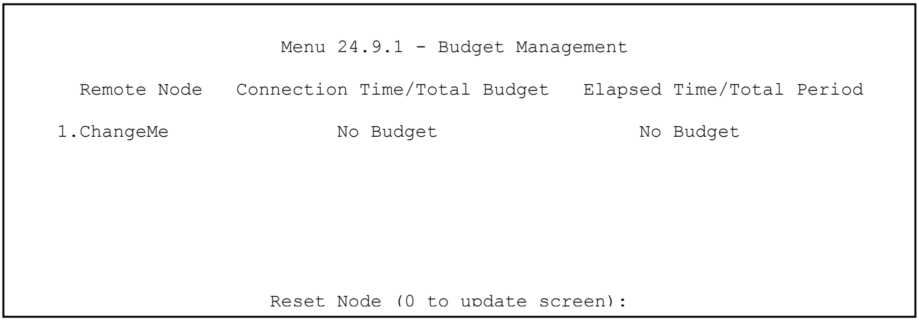


```
                Menu 24.9 - System Maintenance - Call Control

                  1. Budget Management
                  2. Call History



                        Enter Menu Selection Number:
```

Figure 29-3 Menu24.9 System Maintenance : Call Control

29.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                        Menu 24.9.1 - Budget Management

      Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

    1.ChangeMe               No Budget                   No Budget






                       Reset Node (0 to update screen):
```

Figure 29-4 Menu 24.9.1 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked.

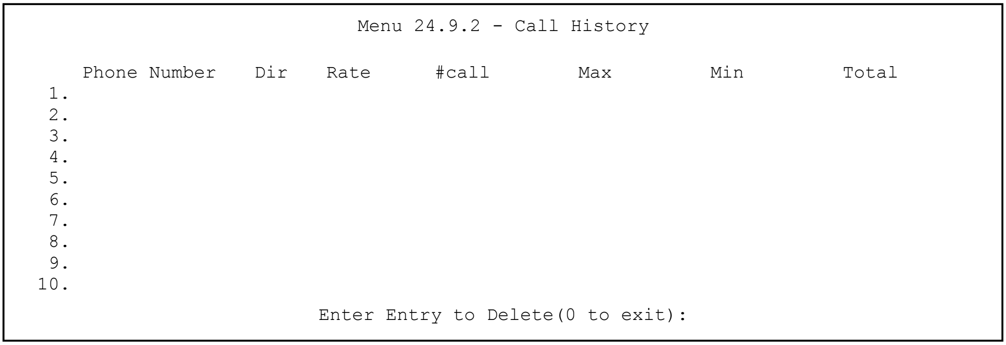
After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 29-1 Menu 24.9.1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

29.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                         Menu 24.9.2 - Call History

     Phone Number   Dir    Rate     #call       Max        Min        Total
  1.
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                      Enter Entry to Delete(0 to exit):
```

Figure 29-5 Menu 24.9.2 Call History

The following table describes the fields in this menu.

Table 29-2 Menu 24.9.2 Call History

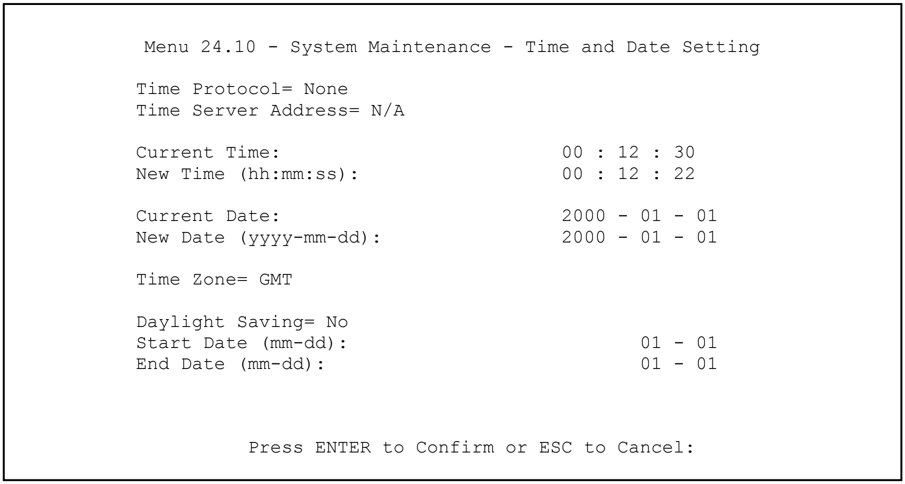
FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or '"0" to exit.	

29.3 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.

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

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



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

Time Protocol= None
Time Server Address= N/A

Current Time:                          00 : 12 : 30
New Time (hh:mm:ss):                   00 : 12 : 22

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

Time Zone= GMT

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



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

Figure 29-6 Menu 24.10 System Maintenance : Time and Date Setting

The following table describes the fields in this menu.

Table 29-3 Menu 24.10 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. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.
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 (hh:mm:ss)	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in hour, minute and second format.

Table 29-3 Menu 24.10 System Maintenance : Time and Date Setting

FIELD	DESCRIPTION
Current Date	This field displays an updated date only when you re-enter this menu.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date (mm-dd)	If using daylight savings time, enter the month and day that it starts on.
End Date (mm-dd)	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

29.3.1 Resetting the Time

The ZyAIR resets the time in three instances:

i. On leaving menu 24.10 after making changes.

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

iii. 24-hour intervals after starting.

Chapter 30
Remote Management

This chapter covers remote management (SMT menu 24.11).

30.1 Telnet

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

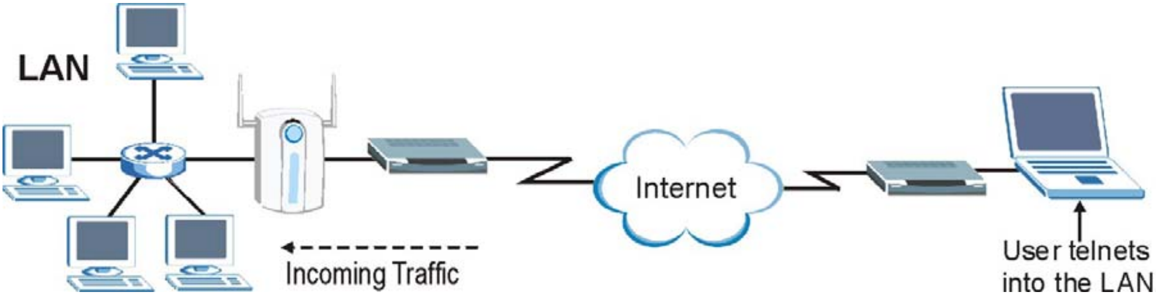


Figure 30-1 Telnet Configuration on a TCP/IP Network

30.2 FTP

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

30.3 Web

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

30.4 Remote Management

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

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

30.4.1 Remote Management Setup

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

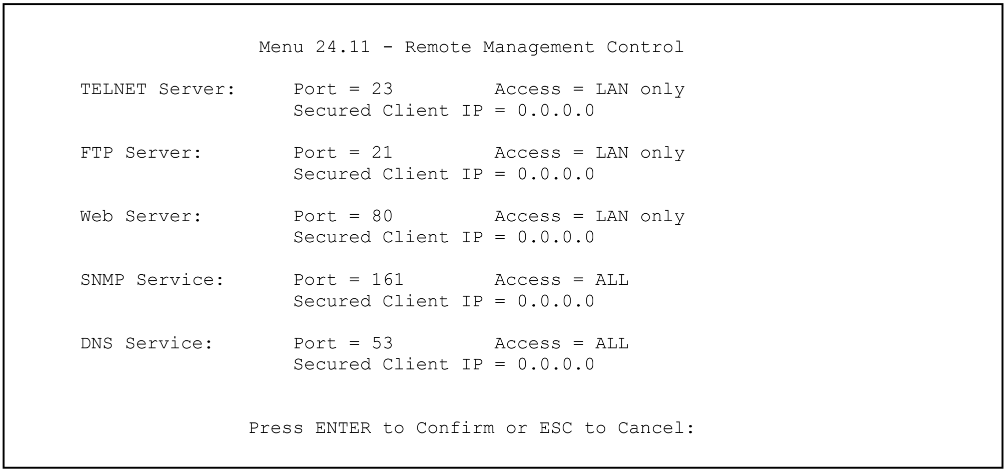
You may manage your ZyAIR from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

- WAN only (Internet)
- LAN only
- ALL (LAN and WAN)
- Disable (Neither)

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

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



```
                   Menu 24.11 - Remote Management Control

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

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

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

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

     DNS Service:       Port = 53         Access = ALL
                        Secured Client IP = 0.0.0.0


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

Figure 30-2 Menu 24.11 Remote Management Control

The following table describes the fields in this menu.

Table 30-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyAIR.	
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management. The DNS Service port number is 53. This cannot be changed.	
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.	LAN only
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

30.4.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

30.5 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

30.6 System Timeout

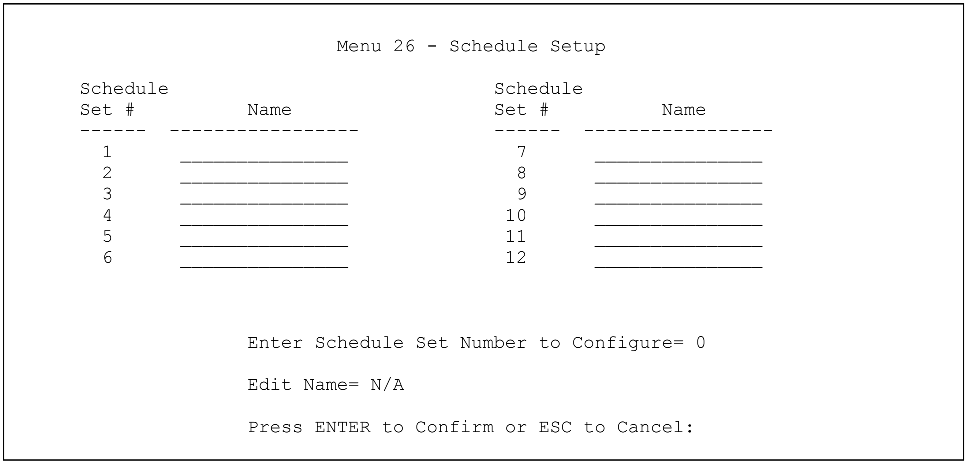
There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyAIR will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Chapter 31
Call Scheduling

Call scheduling (applicable for PPPoE or PPTP encapsulation only) allows you to dictate when a remote node should be called and for how long.

31.1 Introduction

The call scheduling feature allows the ZyAIR to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 – Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 – Schedule Setup** as shown next.



```
                      Menu 26 - Schedule Setup

      Schedule                             Schedule
      Set #          Name                  Set #          Name
      ------  -----------------            ------  -----------------
        1      _______________               7      _______________
        2      _______________               8      _______________
        3      _______________               9      _______________
        4      _______________              10      _______________
        5      _______________              11      _______________
        6      _______________              12      _______________



                     Enter Schedule Set Number to Configure= 0

                     Edit Name= N/A

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

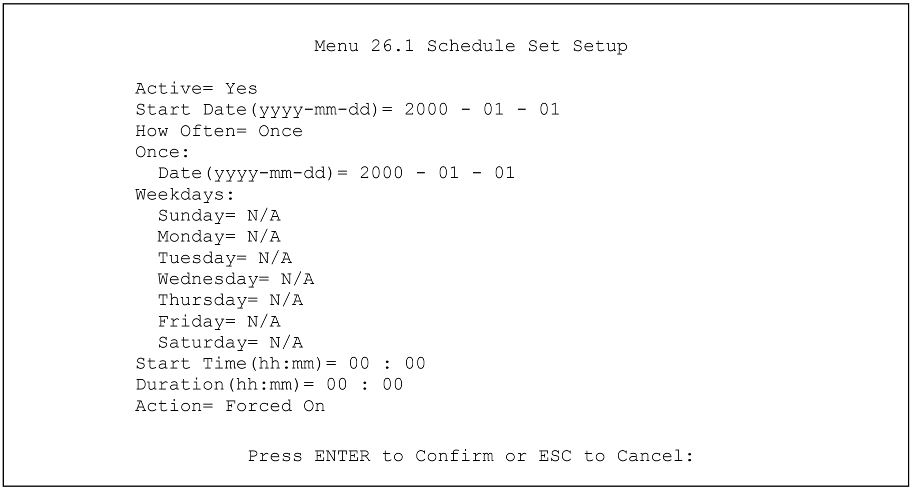
Figure 31-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the ZyAIR, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] **and then** [ENTER] **(or delete) in the** Edit Name **field.**

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.



```
                        Menu 26.1 Schedule Set Setup

            Active= Yes
            Start Date(yyyy-mm-dd)= 2000 - 01 - 01
            How Often= Once
            Once:
              Date(yyyy-mm-dd)= 2000 - 01 - 01
            Weekdays:
              Sunday= N/A
              Monday= N/A
              Tuesday= N/A
              Wednesday= N/A
              Thursday= N/A
              Friday= N/A
              Saturday= N/A
            Start Time(hh:mm)= 00 : 00
            Duration(hh:mm)= 00 : 00
            Action= Forced On

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

Figure 31-2 Menu 26.1 Schedule Set Setup

If a connection has been already established, your ZyAIR will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

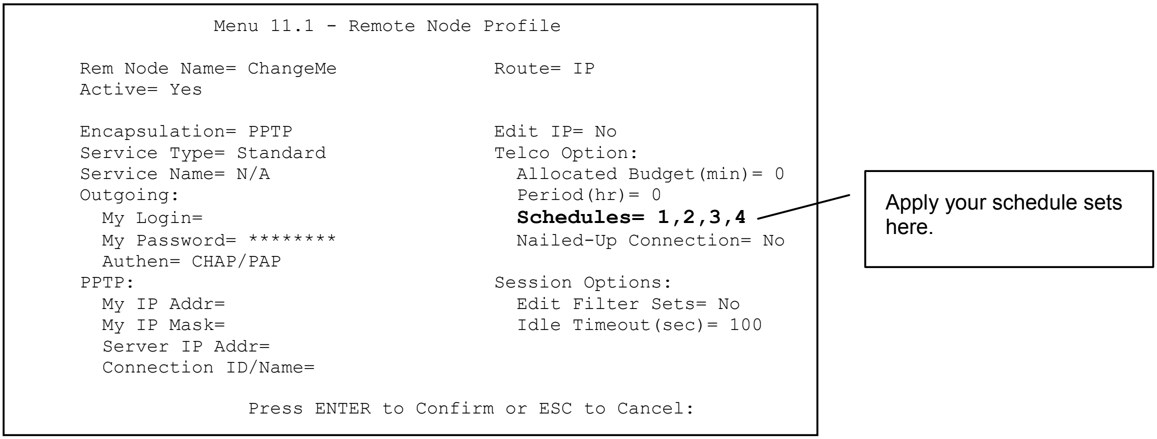
Table 31-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to **No** and press [ENTER] to disable the schedule set.	**Yes**
Start Date	Enter the start date when you wish the set to take effect in year - month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once**

Table 31-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Once:		
Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday:		
Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
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.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPTP** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.



```
                Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe             Route= IP
      Active= Yes

      Encapsulation= PPTP                 Edit IP= No
      Service Type= Standard              Telco Option:
      Service Name= N/A                     Allocated Budget(min)= 0
      Outgoing:                             Period(hr)= 0
        My Login=                           Schedules= 1,2,3,4
        My Password= ********               Nailed-Up Connection= No
        Authen= CHAP/PAP
      PPTP:                               Session Options:
        My IP Addr=                         Edit Filter Sets= No
        My IP Mask=                         Idle Timeout(sec)= 100
        Server IP Addr=
        Connection ID/Name=

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

Apply your schedule sets here.

Figure 31-3 Applying Schedule Set(s) to a Remote Node (PPTP)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Part XI:

APPENDICES

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

Appendix A
Troubleshooting

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

Problems Starting Up the ZyAIR

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

<table>
<tr><th>PROBLEM</th><th colspan="2">CORRECTIVE ACTION</th></tr>
<tr><td>None of the LEDs turn on when I plug in the power adaptor.</td><td colspan="2">Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on.
If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.</td></tr>
<tr><td rowspan="4">I cannot access the ZyAIR via the console port.</td><td colspan="2">1. Check to see if the ZyAIR is connected to your computer's console port.</td></tr>
<tr><td rowspan="3">2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:</td><td>VT100 terminal emulation.</td></tr>
<tr><td>9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.</td></tr>
<tr><td>No parity, 8 data bits, 1 stop bit, data flow set to none.</td></tr>
</table>

Problems with the Password

Chart A-2 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the **RESET** button on the side panel of the ZyAIR to restore the factory default configuration file (hold this button in for more than five seconds). This will restore all of the factory defaults including the password.

Problems with the Ethernet Interface

Chart A-3 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR from the Ethernet	If all of the **LAN** LEDs on the front panel are off, check the Ethernet cable connection between your ZyAIR and the computer connected to the **LAN** port. Check for faulty Ethernet cables. Make sure the computer's Ethernet adapter is installed and working properly. Verify that the IP addresses and the subnet masks of the ZyAIR and the computer are on the same subnet.
I cannot ping any computer on the LAN.	If all of the **LAN** LEDs on the front panel are off, check the Ethernet cable connection between your ZyAIR and the computer connected to the **LAN** port. Verify that the IP addresses and the subnet masks of the ZyAIR and the computers are on the same subnet.

Problems with the WAN Interface

Chart A-4 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPTP encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the *WAN Screens* chapter (web configurator) or the *Internet Access* chapter (SMT). Clone the MAC address from your computer on the LAN as the ZyAIR's WAN MAC address. Refer to the *WAN Screens* chapter (web configurator) or the *General and WAN Setup* chapter (SMT). It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication. Configure your computer's name as the ZyAIR's system name. Refer to the *Wizard Setup* chapter (web configurator) or the *General and WAN Setup* chapter (SMT).

Problems with Internet Access

Chart A-5 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Connect your cable/DSL modem to the ZyAIR using the appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because for some devices may require a crossover cable and others a straight-through Ethernet cable. Verify your WAN settings. Refer to the *WAN* chapter (web configurator) or the *Internet Access* chapter (SMT). Make sure you entered the correct user name and password. For wireless stations, check that both the ZyAIR and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
Internet connection disconnects	If you use PPTP or PPPoE encapsulation, check the idle time-out setting. Refer to the *WAN* chapter (web configurator) or the *Remote Node Configuration* chapter (SMT). Contact your ISP.

Problems with Telnet

Chart A-6 Troubleshooting Telnet

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

Problems with the WLAN Interface

Chart A-7 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot ping any computer on the WLAN.	Make sure the wireless card is properly inserted in the ZyAIR and the **WLAN** LED is on. Make sure the wireless adapter on the wireless station is working properly. Check that both the ZyAIR and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Appendix B
Brute-Force Password Guessing Protection

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

Chart B-1 Brute-Force Password Guessing Protection Commands

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

Example

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

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

Appendix C
Setting up Your Computer's IP Address

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

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

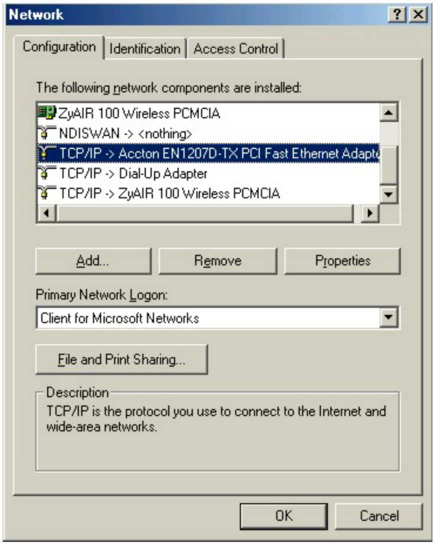
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

Windows 95/98/Me

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


The following network components are installed:
- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

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

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

a. Click **Add**.

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

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

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

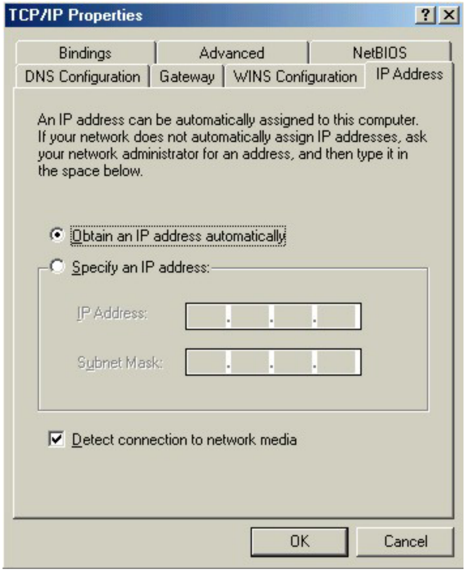
e. Restart your computer so the changes you made take effect.

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

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

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

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



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

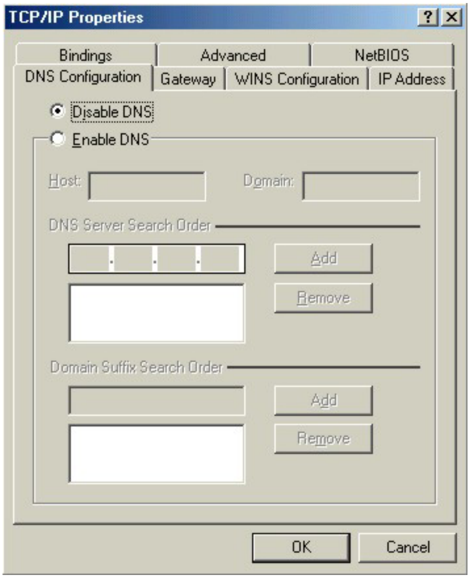
Subnet Mask: . . .

☑ Detect connection to network media

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

   -If you do not know your DNS information, select **Disable DNS**.

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



● Disable DNS

○ Enable DNS

Host:

Domain:

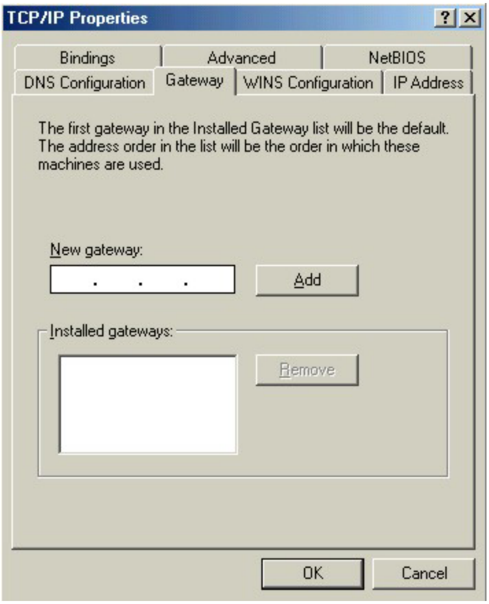
DNS Server Search Order

Domain Suffix Search Order

3. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



TCP/IP Properties

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

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

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

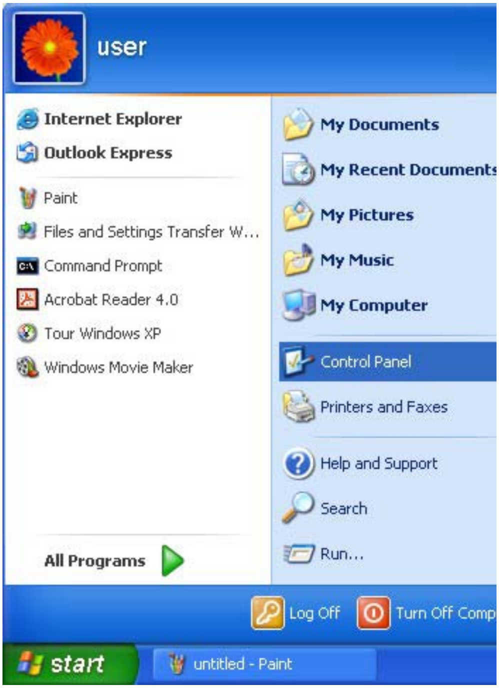
6. Turn on your ZyAIR and restart your computer when prompted.

Verifying Your Computer's IP Address

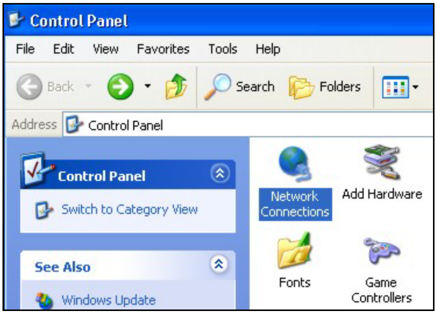
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

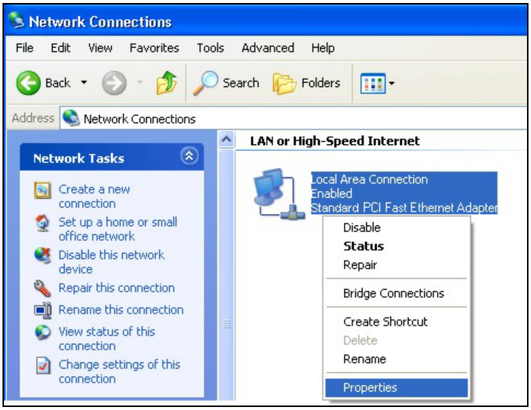
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



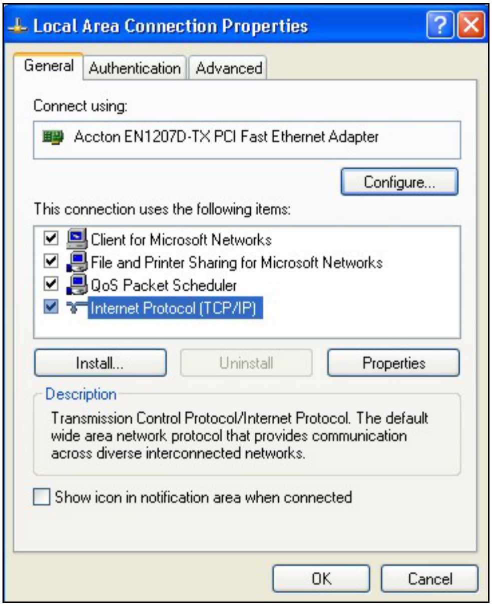
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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



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



Local Area Connection Properties

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

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

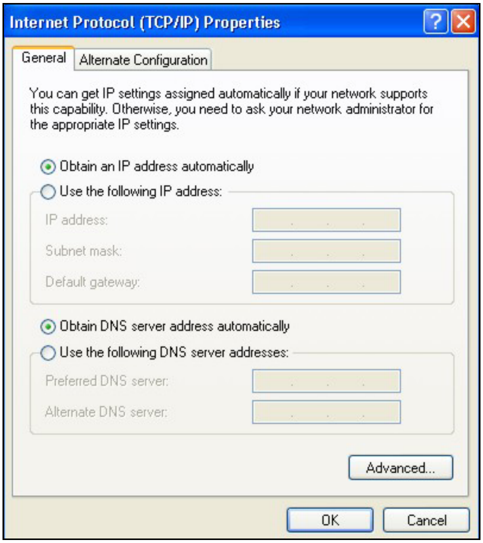
☐ Show icon in notification area when connected

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

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

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

   Click **Advanced**.



Internet Protocol (TCP/IP) Properties

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 Settin**gs tab and click **OK**.

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

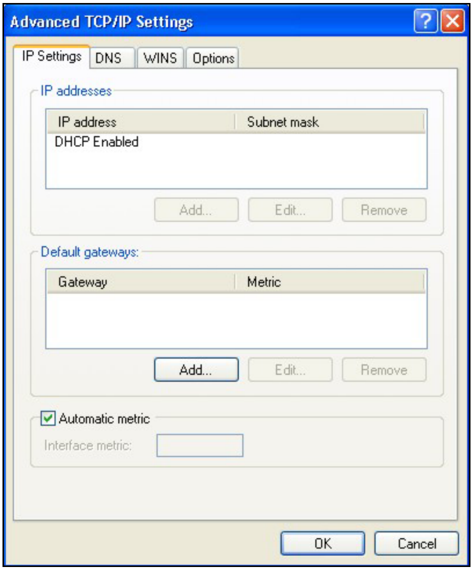
   -In the **IP Settings** tab, in IP addresses, click **Add**.

   -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**.



IP address	Subnet mask
DHCP Enabled	

☑ Automatic metric

Interface metric:

   -Click **Add**.

   -Repeat the previous three steps for each default gateway you want to add.

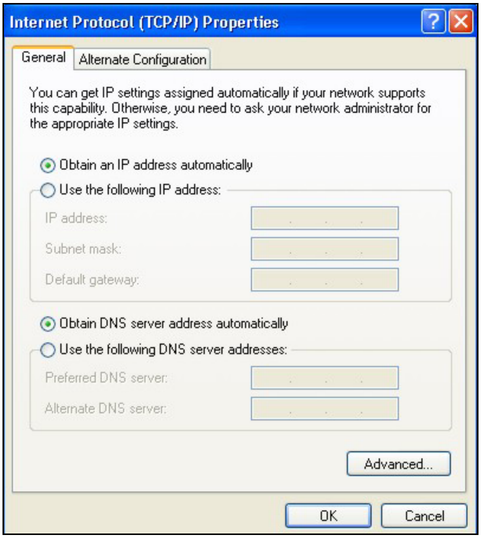
   -Click **OK** when finished.

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

   -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

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

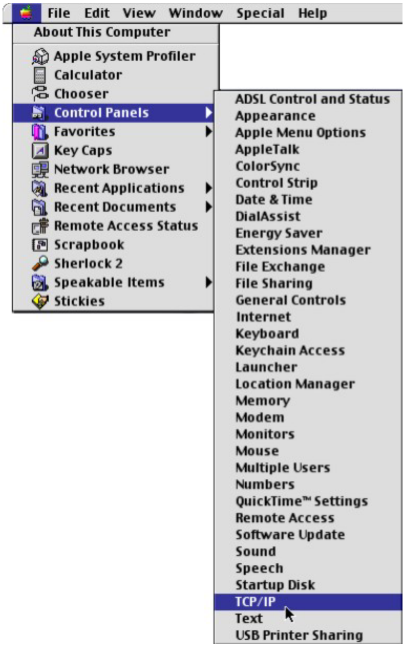
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer’s IP Address

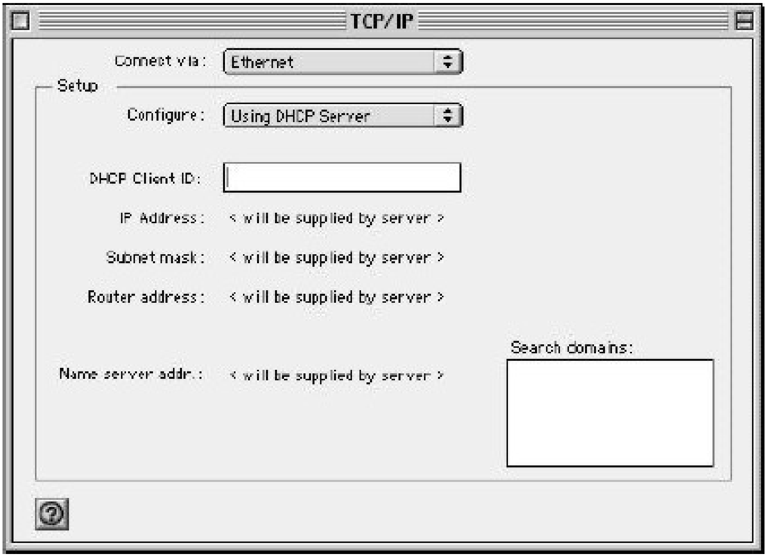
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

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

Search domains:

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

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your ZyAIR in the **Router address** box.

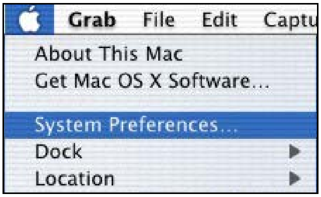
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

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

Macintosh OS X

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

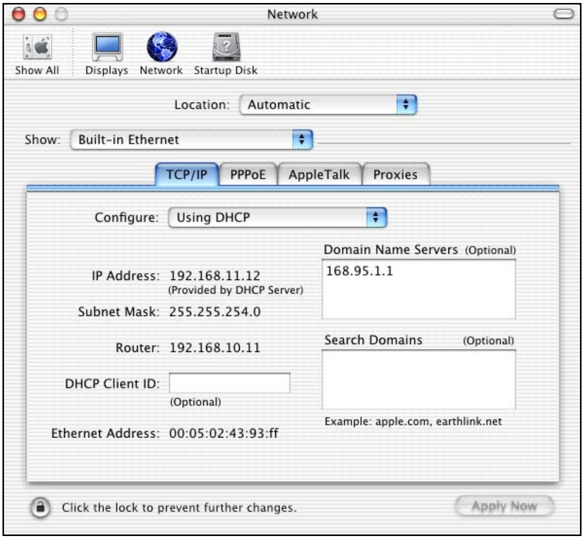


2. Click **Network** in the icon bar.

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

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

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



Network

Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

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

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your ZyAIR in the **Router address** box.

5. Click **Apply Now** and close the window.

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

Verifying Your Computer’s IP Address

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

Appendix D Wireless LAN and IEEE 802.11

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

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

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

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

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

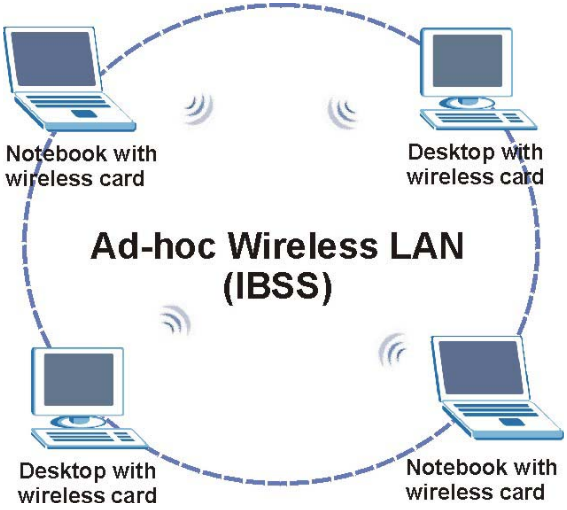

Notebook with wireless card
Desktop with wireless card
Ad-hoc Wireless LAN (IBSS)
Desktop with wireless card
Notebook with wireless card

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

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

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

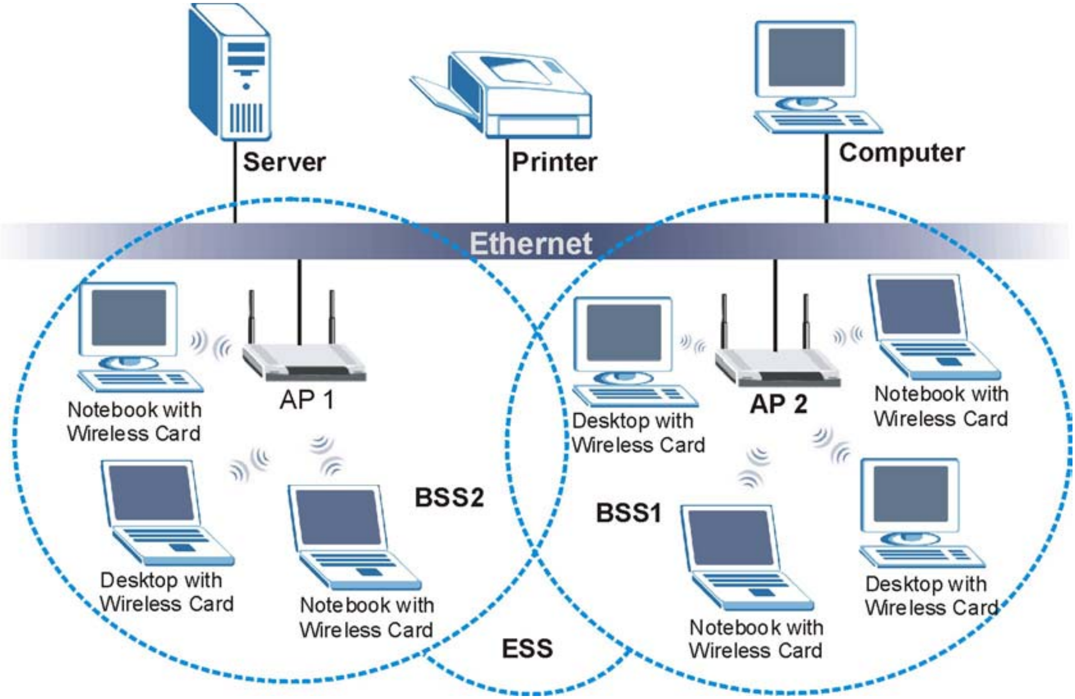

Server
Printer
Computer
Ethernet
Notebook with Wireless Card
AP 1
Desktop with Wireless Card
Notebook with Wireless Card
BSS2
Desktop with Wireless Card
AP 2
Notebook with Wireless Card
BSS1
Notebook with Wireless Card
Desktop with Wireless Card
ESS

Diagram D-2 ESS Provides Campus-Wide Coverage

Appendix E
Wireless LAN With IEEE 802.1x

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

Security Flaws with IEEE 802.11

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

Deployment Issues with IEEE 802.11

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

IEEE 802.1x

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

Advantages of the IEEE 802.1x

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

RADIUS Server Authentication Sequence

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

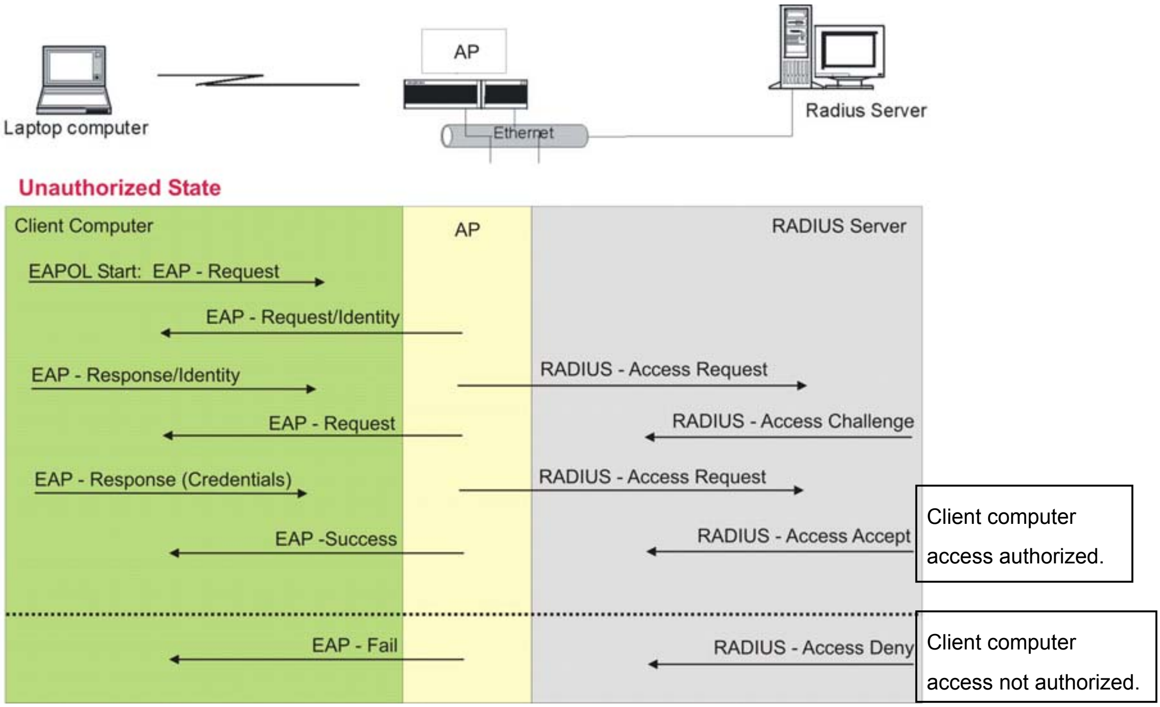


Diagram E-1 Sequences for EAP MD5–Challenge Authentication

Appendix F
Types of EAP Authentication

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

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

Comparison of EAP Authentication Types

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

Appendix G Antenna Selection and Positioning Recommendation

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

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

Antenna Characteristics

➢ Frequency

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

➢ Radiation Pattern

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

➢ Antenna Gain

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

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

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

Types of Antennas For WLAN

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

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

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

Positioning Antennas

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

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

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

Connector Type

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

Appendix H PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit), which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

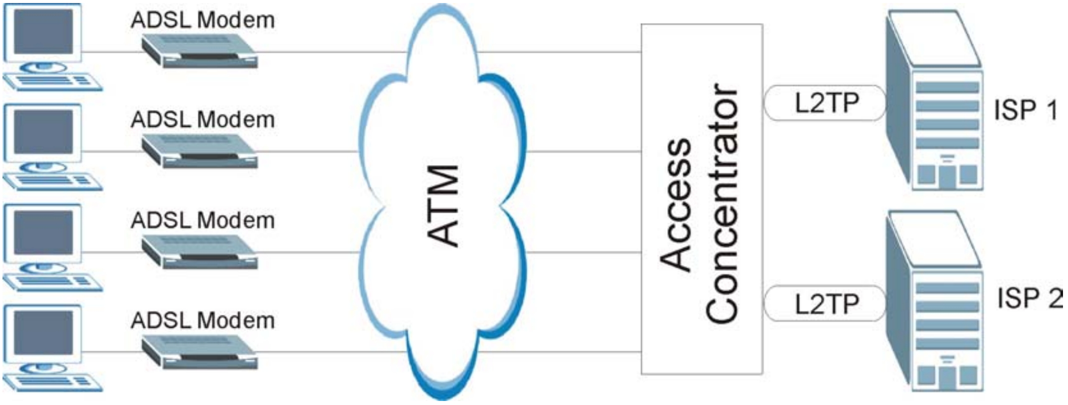


Diagram H-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

ZyAIR as a PPPoE Client

When using the ZyAIR as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

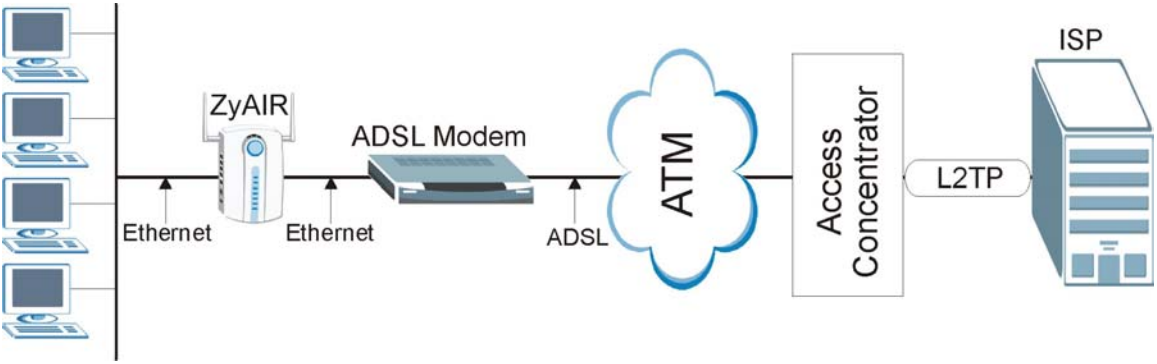


Diagram H-2 ZyAIR as a PPPoE Client

Appendix I PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

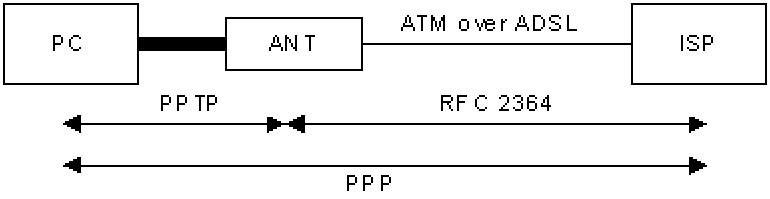


Diagram I-1 Transport PPP frames over Ethernet

PPTP and the ZyAIR

When the ZyAIR is deployed in such a setup, it appears as a PC to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyAIR's Internet connection. In NAT mode, the ZyAIR is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyAIR initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

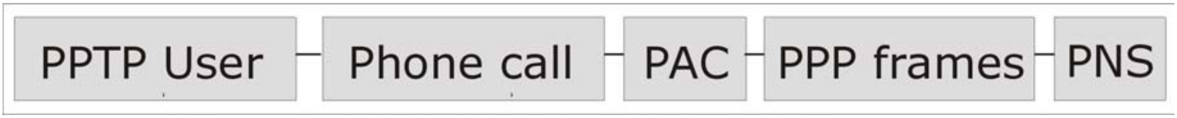


Diagram I-2 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the ZyAIR, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

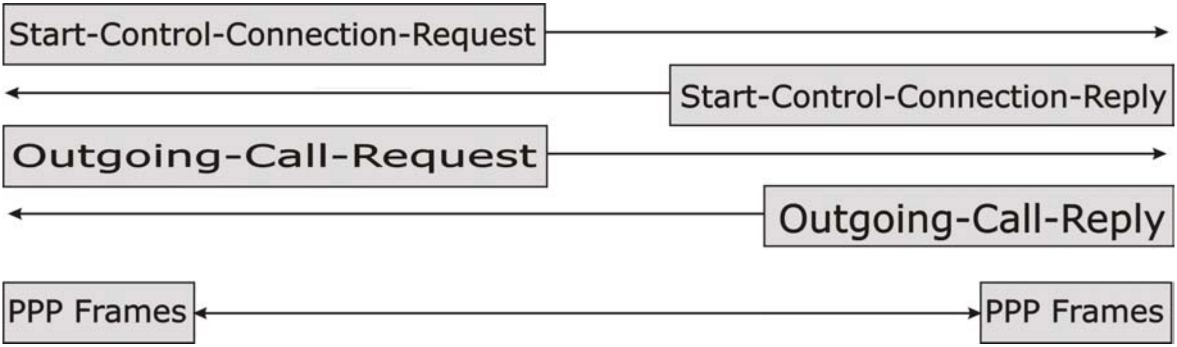

Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

Diagram I-3 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix J IP Subnetting

IP Addressing

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

IP Classes

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

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

Chart J-1 Classes of IP Addresses

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

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

Therefore:

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

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

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

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

Chart J-2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

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

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

Chart J-3 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

Chart J-4 Alternative Subnet Mask Notation

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

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

Example: Two Subnets

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

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

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

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

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

Chart J-5 Subnet 1

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

Chart J-6 Subnet 2

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

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

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart J-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Chart J-8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart J-9 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

Chart J-10 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

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

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

Chart J-11 Eight Subnets

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

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

Chart J-12 Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

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

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

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

Chart J-13 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126

Chart J-13 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 K
Command Interpreter

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

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

Command Syntax

The command keywords are in `courier new` font.

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

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

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

The `|` symbol means "or".

For example,

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

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

Command Usage

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

Appendix L
NetBIOS Filter Commands

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

Introduction

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

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

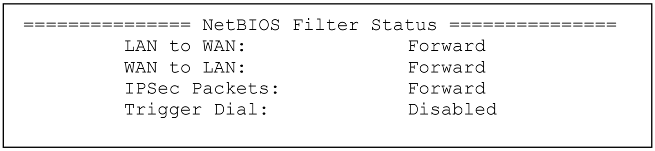
You can configure NetBIOS filters to do the following :

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

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

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



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

Diagram L-1 NetBIOS Display Filter Settings Command Without DMZ Example

The filter types and their default settings are as follows.

Chart L-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
LAN to WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN.	Forward

Chart L-1 NetBIOS Filter Default Settings

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

NetBIOS Filter Configuration

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

`<type> =` Identify which NetBIOS filter (numbered 0-3) to configure.

`0` = LAN to WAN

1 = WAN to LAN

6 = IPSec packet pass through

7 = Trigger Dial

`<on|off> =` For types `0` and `1`, use `on` to enable the filter and block NetBIOS packets. Use `off` to disable the filter and forward NetBIOS packets.

For type `7`, use `on` to allow NetBIOS packets to initiate dial backup calls. Use `off` to block NetBIOS packets from initiating dial backup calls.

Example commands

Command:

```
sys filter netbios config 0 on
```

This command blocks LAN to WAN NetBIOS packets

Command:

```
sys filter netbios config 1 off
```

This command forwards WAN to LAN NetBIOS packets

Command:

```
sys filter netbios config 6 on
```

This command blocks IPSec NetBIOS packets

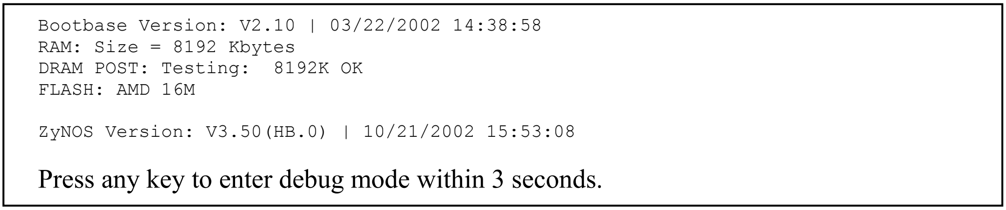
Command:

```
sys filter netbios config 7 off
```

This command stops NetBIOS commands from initiating calls.

Appendix M
Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware (ZyNOS) is started. When you start up your ZyAIR, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the *Firmware and Configuration File Maintenance* chapter.



```
Bootbase Version: V2.10 | 03/22/2002 14:38:58
RAM: Size = 8192 Kbytes
DRAM POST: Testing:  8192K OK
FLASH: AMD 16M

ZyNOS Version: V3.50(HB.0) | 10/21/2002 15:53:08

Press any key to enter debug mode within 3 seconds.
```

Diagram M-1 Option to Enter Debug Mode

Enter ATHE to view all available ZyAIR boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

```
AT              just answer OK
ATHE            print help
ATBAx           change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)       set BootExtension Debug Flag (y=password)
ATSE            show the seed of password generator
ATTI(h,m,s)     change system time to hour:min:sec or show current time
ATDA(y,m,d)     change system date to year/month/day or show current date
ATDS            dump RAS stack
ATDT            dump Boot Module Common Area
ATDUx,y         dump memory contents from address x for length y
ATWBx,y         write address x with  8-bit value y
ATWWx,y         write address x with 16-bit value y
ATWLx,y         write address x with 32-bit value y
ATRBx           display the  8-bit value of address x
ATRWx           display the 16-bit value of address x
ATRLx           display the 32-bit value of address x
ATGO(x)         run program at addr x or boot router
ATGR            boot router
ATGT            run Hardware Test Program
AT%Tx           Enable Hardware Test Program at boot up
ATBTx           block0 write enable (1=enable, other=disable)
ATRTw,x,y(,z)   RAM test level w, from address x to y (z iterations)
ATWEa(,b,c,d)   write MAC addr, Country code, EngDbgFlag, FeatureBit to flash ROM
ATCUx           write Country code to flash ROM
ATCB            copy from FLASH ROM to working buffer
ATCL            clear working buffer
ATSB            save working buffer to FLASH ROM
ATBU            dump manufacturer related data in working buffer
ATSH            dump manufacturer related data in ROM
ATWMx           set MAC address in working buffer
ATCOx           set country code in working buffer
ATFLx           set EngDebugFlag in working buffer
ATSTx           set ROMRAS address in working buffer
ATSYx           set system type in working buffer
ATVDx           set vendor name in working buffer
ATPNx           set product name in working buffer
ATFEx,y,...     set feature bits in working buffer
ATMP            check & dump memMapTab
ATDOx,y         download from address x for length y to PC via XMODEM
ATTD            download router configuration to PC via XMODEM
ATUPx,y         upload to RAM address x for length y from PC via XMODEM
ATUR            upload router firmware to flash ROM
ATLC            upload router configuration file to flash ROM
ATUXx(,y)       xmodem upload from flash block x to y
ATERx,y         erase flash rom from block x to y
ATWFx,y,z       copy data from addr x to flash addr y, length z
ATXSx           xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATLOa,b,c,d     Int/Trap Log Cmd
ATSR            system reboot
ATBR            Reset to default Romfile
ATDC            Disable check model mechanism
```

Diagram M-2 Boot Module Commands

Appendix N Triangle Route

The Ideal Setup

When the firewall is on, your ZyAIR acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyAIR to protect your LAN against attacks.

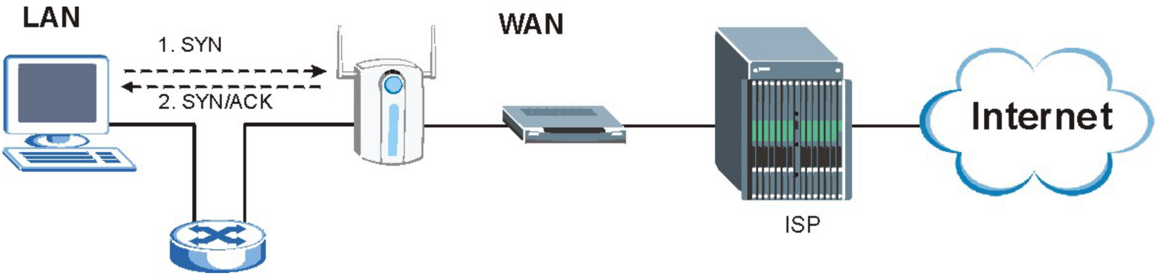


Diagram N-1 Ideal Setup

The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

Step 1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

Step 2. The ZyAIR reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

Step 3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyAIR.

As a result, the ZyAIR resets the connection, as the connection has not been acknowledged.

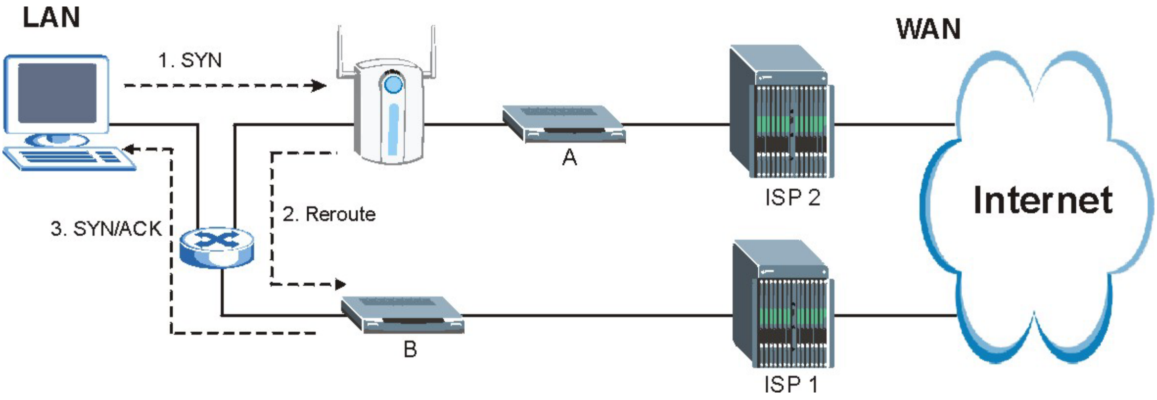


Diagram N-2 "Triangle Route" Problem

The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyAIR supports up to three logical LAN interfaces with the ZyAIR being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the ZyAIR to your LAN. The following steps describe such a scenario.

Step 1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

Step 2. The ZyAIR reroutes the packet to Gateway **B** in Subnet 2.

Step 3. The reply from WAN goes through the ZyAIR to the computer on the LAN in Subnet 1.

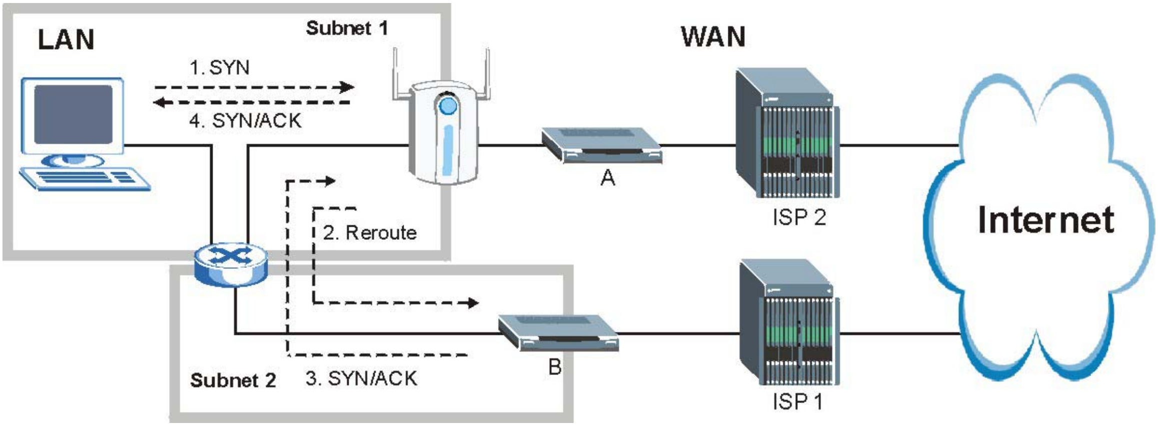


Diagram N-3 IP Alias

Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyAIR to your LAN. Therefore your LAN is protected.

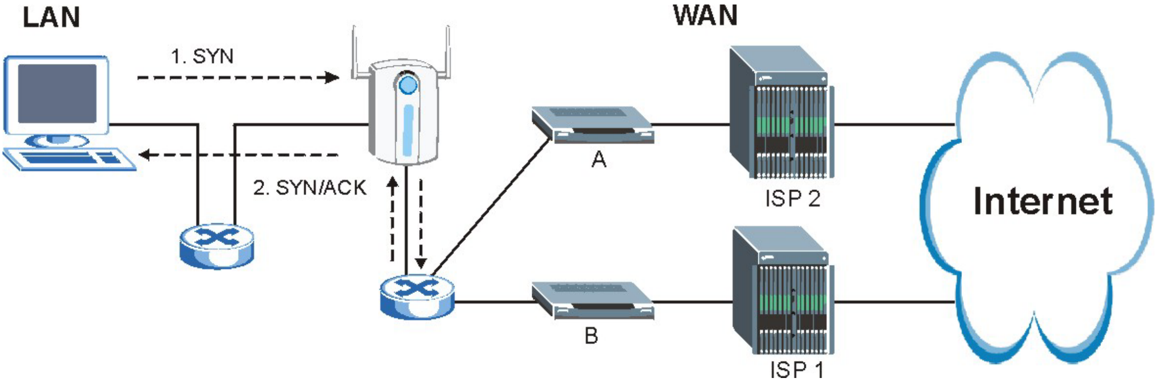


Diagram N-4 Gateways on the WAN Side

Appendix O
Log Descriptions

Chart O-1 System Error Logs

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

Chart O-2 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.

Chart O-2 System Maintenance Logs

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

Chart O-3 UPnP Logs

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

Chart O-4 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench

Chart O-4 ICMP Notes

TYPE	CODE	DESCRIPTION
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Chart O-5 Sys log

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

Log Commands

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

Configuring What You Want the ZyAIR to Log

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

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

Chart O-6 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
`error`	`0, 1, 2, 3`
`mten`	`0, 1`
`upnp`	`0, 1`
`8021x`	`0, 1`
`urlforward`	`0, 1`
`urlblocked`	`0, 1, 2, 3`
`javablocked`	`0, 1, 2, 3`
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

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

Displaying Logs

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

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

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

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

Log Command Example

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

```
ras> sys logs load

ras> sys logs category error 3

ras> sys logs save

ras> sys logs display access


#  .time                 source                 destination
notes

    message

  0|11/11/2002 15:10:12 |172.22.3.80:137       |172.22.255.255:137
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

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

    Firewall default policy: UDP(set:8)

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

    Firewall default policy: IGMP(set:8)

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

    Firewall default policy: UDP(set:8)
  4|11/11/2002 15:10:10 |192.168.10.1:520      |192.168.10.255:520
|ACCESS BLOCK

    Firewall default policy: UDP(set:8)

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

Appendix P
Power Adaptor Specifications

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

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

Appendix Q
Index