ZyAIR B-4000

Hot Spot Gateway

User's Guide

Version 1.00

July 2003

ZyXEL

Unleash Networking Power

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

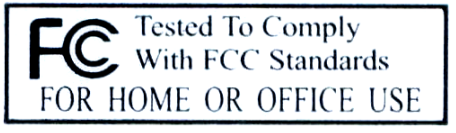
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

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



ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

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

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

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

Customer Support

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

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

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyXEL ZyAIR B-4000 Hot Spot Gateway.

The ZyAIR Hot Spot Gateway combines an 802.11b wireless access point, router, 4-port switch and service gateway in one box. An "exclusive printer" connects directly to the ZyAIR, allowing you to easily print subscriber statements. The ZyAIR is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.

This user's guide is designed to guide you through the configuration of your ZyAIR using 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 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.

User Guide Feedback

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

Syntax Conventions

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

- The ZyXEL ZyAIR B-4000 Hot Spot Gateway may be referred to as the “ZyAIR” in this manual.
- The ZyXEL ZyAIR SP-100 Statement Printer may be referred to as the “statement printer” or the “exclusive printer” in this manual.

Part I:

Getting Started

This part introduces the ZyAIR, the web configurator and general system setup.

Chapter 1
Getting to Know Your ZyAIR

This chapter introduces the features and applications of the ZyAIR.

1.1 Introducing the ZyAIR

The ZyAIR Hot Spot Gateway combines an 802.11b wireless access point, router, 4-port switch and service gateway in one box. An "exclusive printer" connects directly to the ZyAIR, allowing you to easily print subscriber statements. The ZyAIR is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.

1.2 Features

Your ZyAIR provides the following features to accommodate subscribers with a variety of network configurations with little or no technical support.

Plug-and-Play Internet Access

The ZyAIR provides Internet access to attached computer(s) without extra software installation or computer configuration. In addition, with transparent proxy, the ZyAIR resolves any incompatible proxy settings.

WEP Data Encryption

WEP (Wired Equivalent Privacy) data encryption helps ensure the security of data on the wireless LAN. The ZyAIR supports 64, 128 and 256 bit WEP encryption.

VPN (Virtual Private Network) Pass Through

The ZyAIR allows subscribers to create VPN networks (which use data encryption and the Internet to provide secure communications) that go through the ZyAIR.

VLAN

The ZyAIR can use VLANs (Virtual Local Area Network) to partition the physical network into multiple logical networks in order to stop subscribers from seeing each other's data. The ZyAIR also provides a port-based VLAN via the four 10/100Mbps auto-negotiating Ethernet ports.

SSL Secure Login

With Secure Socket Layer (SSL) activated upon login, data exchanged between the ZyAIR and client computers are encrypted and protected.

PPTP Support

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.

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.

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.

DHCP Support

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

E-mail Forwarding

The ZyAIR is able to forward and retrieve e-mail messages when the subscriber’s default email server is down or behind a firewall.

DNS Proxy

With DNS proxy, the ZyAIR provides DNS redirection when a subscriber’s configured DNS server is behind a firewall or located in a private Intranet.

Local Subscriber Database

The ZyAIR allows you to maintain a subscriber database on the ZyAIR without setting up an external RADIUS server. Subscriber accounting and authentication are done using the local subscriber database.

Accounting

Accounting can be done using the built-in accounting feature.

Local Content and Advertising Links

Once connected to the network, the ZyAIR directs the subscriber to a specified web site and display advertisement links. This can be a source of extra online advertising revenues and increased business exposure.

Access Control (Walled Garden)

With the walled garden feature, subscribers are able to access predetermined web sites without logging in. The ZyAIR blocks full Internet access until the subscribers log in.

Subscriber Login Page Customization

You can customize the subscriber login page according to your business needs. The advanced settings allows you to include welcome messages, company logo and basic formatting.

Web Configurator Management

The ZyAIR comes with an embedded web-based configurator. It offers advanced management features and allows you to manage the ZyAIR remotely using Internet Explorer.

Watchdog

The ZyAIR can continue working by resetting itself after a system crash.

Upgrade Firmware

The firmware of the ZyAIR can be upgraded via the web configurator or the SMT menu.

Syslog

The ZyAIR's syslog function allows network administrators to monitor the usage status of subscribers from a remote site. You can set up a syslog server to receive the log of information on current logged-in subscribers that the ZyAIR sends periodically.

802.11b Wireless LAN Standard

The ZyAIR complies 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.

Table 1-1802.11B

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.

Antennas

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

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

Table 1-2 ZyAIR Wireless LAN Coverage

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

4-Port Switch

A combination of switch and Internet gateway makes your ZyAIR a cost-effective and viable network solution. You can connect up to four computers to the LAN ports on the ZyAIR without the cost of a hub. To connect more than four Ethernet devices, attach a hub or switch.

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.

Reset Button

Use the reset button to restore the ZyAIR back to its factory defaults.

Statement Printer

A compact Statement Printer comes with your ZyAIR. The Statement Printer allows you to generate subscriber accounts on the ZyAIR and print out the account information on-site without using a computer.

The Statement Printer is also known as an Account Generator or Exclusive Printer.

Ease of Installation

Your ZyAIR is designed for quick, intuitive and easy installation. It can be mounted on a desktop or a wall.

1.3 Applications

The following sections describe network application examples in which the ZyAIR is used.

1.3.1 Internet Access for LAN Networks

With a broadband service account set up, the ZyAIR allows the attached computers to enjoy high speed Internet access.

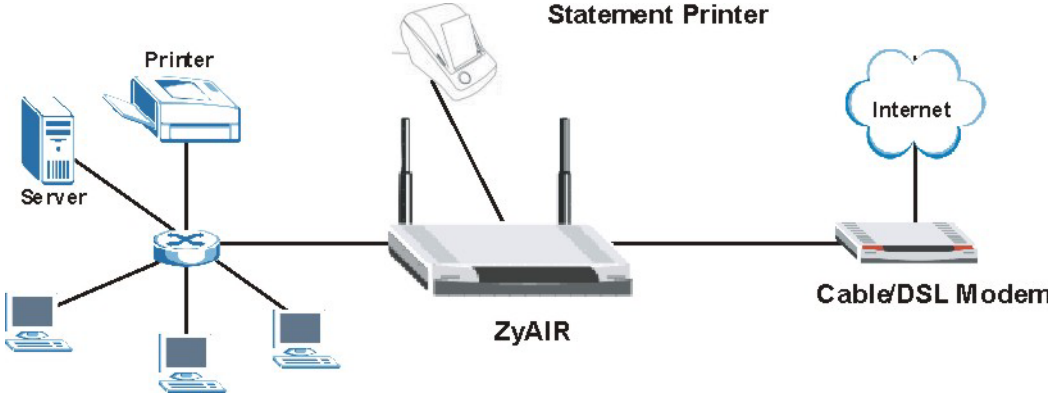


Figure 1-1 Application: Internet Access for LAN Networks

1.3.2 Internet Access in Public Areas

In public areas, such as a hotel, the ZyAIR provides high speed Internet access to subscribers. Account billing and authentication can be done using the built-in billing function and local subscriber database.

The ZyAIR functions as an access point (AP) to bridge the wired and the wireless network allowing wireless stations to access the Internet through the ZyAIR.

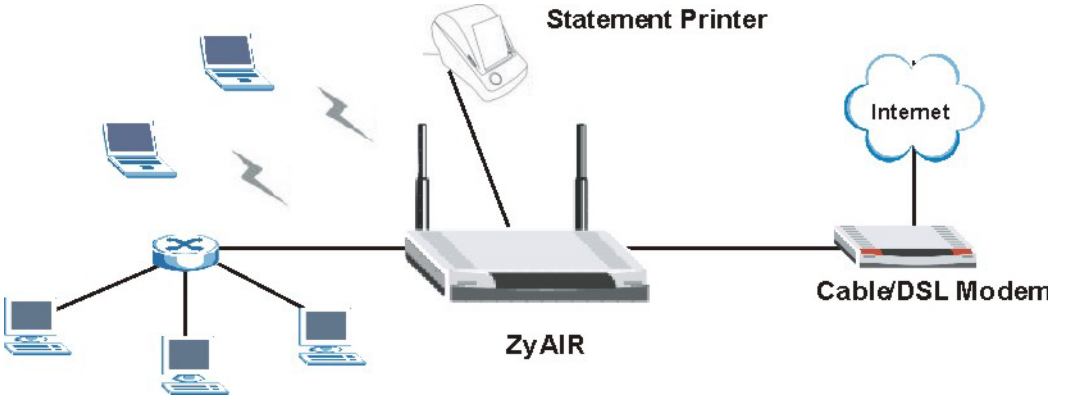


Figure 1-2 Application: Internet Access in Public Areas

Chapter 2
The Web Configurator

This chapter introduces how to access the web configurator to perform general system configuration.

2.1 Introducing the Web Configurator

The web configurator is best viewed with Internet Explorer (version 4.0 or above) or Netscape Navigator (version 6.0 or above). Your browser must have JavaScript support enabled.

2.2 Accessing the Web Configurator

Follow the steps below to access the web configurator.

The ZyAIR allows only one web configurator session at any one time.

Step 1. Make sure your ZyAIR is properly connected (refer to instructions in the *Quick Installation Guide* on hardware installtion and connections).

Step 2. Launch your web browser and type the WAN or LAN IP address of the ZyAIR as the web address (it is recommended that you connect your computer to the LAN and use the LAN IP address for initial configuration). **192.168.1.1** is the default IP address for the LAN port.
If you are using a different port number (between 8000 and 8099) for the web server, you must also append the port number to the LAN IP address seperated with a colon ":", for example, http://192.168.1.1:8080.

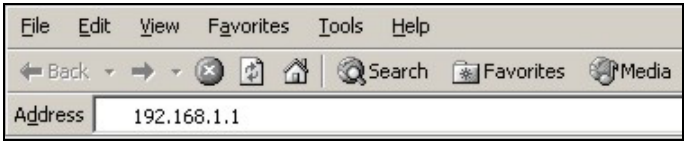


Figure 2-1 Entering ZyAIR IP Address in Internet Explorer

Step 3. A login screen displays. Type "admin" (default) as the user name and "1234" (default) as the password and click **Getting Started ►►**.

The user name and password are case sensitive.

Figure 2-2 Web Configurator: Login

Step 4. You should see the first screen of the Wizard Setup. Refer to the *Quick Installation Guide* for more information on configuring the Wizard Setup screens.

The ZyAIR automatically logs you out if there is no activity for longer than 20 minutes after you log in. If this happens, simply log back in again.

2.3 Wizard Setup Screens

The Wizard Setup screens display when you first access the ZyAIR. Refer to the *Quick Installation Guide* for information on how to configure the Wizard Setup screens.

2.4 Navigating the Web Configurator

After you finish the Wizard Setup screens, the ZyAIR web configurator provides two levels of navigation: the navigation tabs and sub-menu panels.

2.4.1 The Navigation Tabs

The navigation tabs at the top of the screen correspond to menus of screens grouped by category. Click a navigation tab to display the tab's sub-menu panel.

2.4.2 Sub-menu Panels

The sub-menu panel on the left of each web configurator screen provides a consistent way to access the configuration screens in a navigation tab. Click a link to open the corresponding screen.

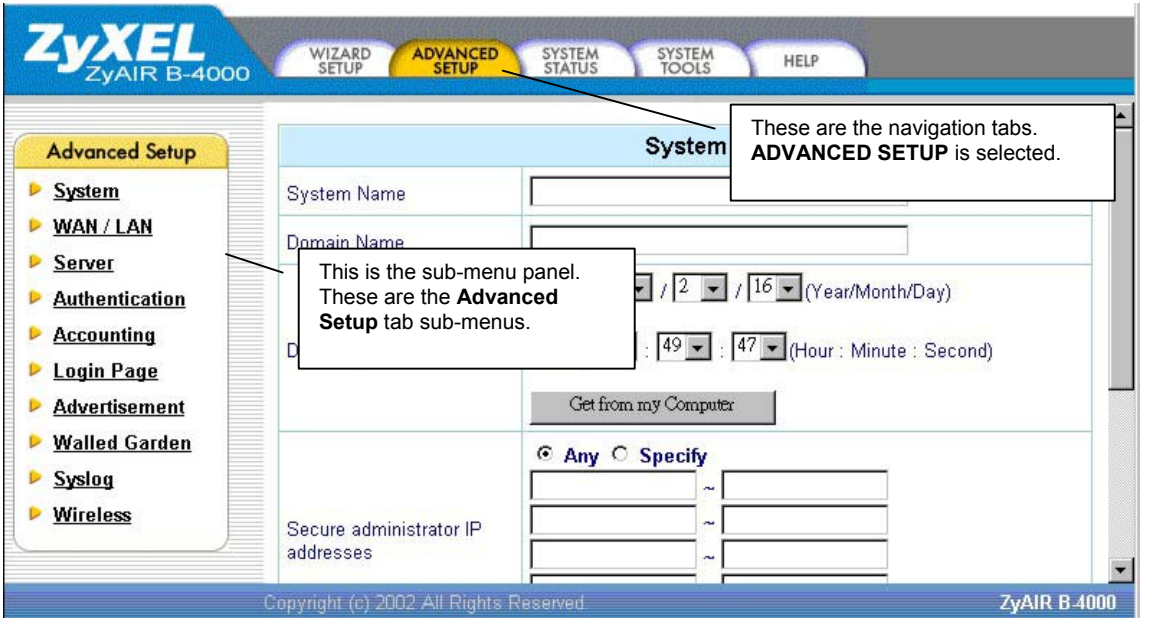


Figure 2-3 Web Configurator Navigation

2.5 Login Accounts

There are four system accounts that you can use to log in to the ZyAIR: administrator, account manager, supervisor and super subscriber.

The administrator account allows you full access to all system configurations. The default administrator user name is “admin” and the default password is “1234”.

The account manager account is used for proprietary subscriber account management only. No system configuration is allowed. This account is useful for front desk personnel (such as in a hotel) for setting up subscriber accounts without tampering with the system configuration. The account manager default user name and password are “account”.

With the supervisor account, you can only view the system status and change the supervisor account password. The default supervisor account user name and password are “supervisor”.

Use the super subscriber account to test the Internet connection between the ZyAIR and the ISP. The ZyAIR does not impose time limitations or charges on this account. Thus, anyone who logs in with this account is able to gain Internet access for free. The default super subscriber user name and password are "super".

You can only log in using the super subscriber account in the subscriber login screen.

2.5.1 Changing Login Account Usernames and Passwords

It is recommended you change the account passwords.

Click the **SYSTEM TOOLS** tab and **System Account**.

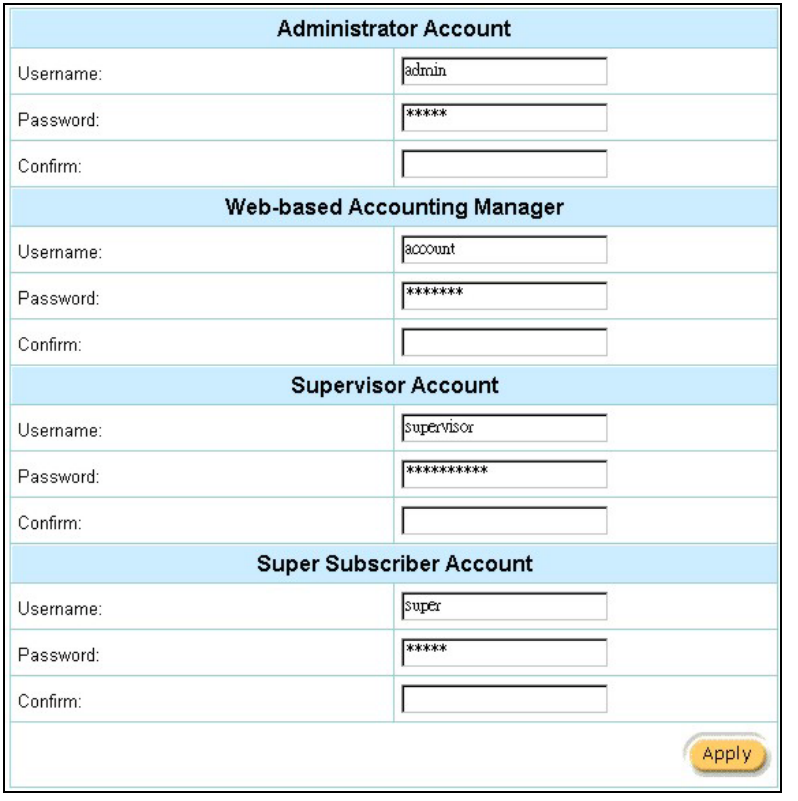


Figure 2-4 System Tools: System Account

The account user names and passwords are case sensitive.

Table 2-1 System Tools: System Account

LABEL	DESCRIPTION
Administrator Account	
Username	Enter the user name for the administrative account. The default is **admin**.
Password	Enter a new administrative account password.
Confirm	Enter the new administrator password again for confirmation.
Web-based Accounting Manager	
Username	Enter the user name for the account manager account. The default is **account**.
Password	Enter a new account manager password.
Confirm	Enter the new account manager password again for confirmation.
Supervisor Account	
Username	Enter the user name for the supervisor account. The default is **supervisor**.
Password	Enter a new supervisor password.
Confirm	Enter the new supervisor password again for confirmation.
Super Subscriber Account **You can only log in using the super subscriber account in the subscriber login screen.**	
Username	Enter the user name for the super subscriber account. The default is **super**.
Password	Enter a new super subscriber account password.
Confirm	Enter the new super subscriber account password again for confirmation.
Apply	Click **Apply** to save the changes back to the ZyAIR.

2.6 Methods of Restoring Factory-Defaults

There are two methods you can use to erase the current configuration and restore factory defaults.

2.6.1 The Reset Button

The reset button is located on the left side panel. Use a pointed object to press this button in once to reset the ZyAIR back to the factory defaults.

All of your custom configuration including the local subscriber database will be erased.

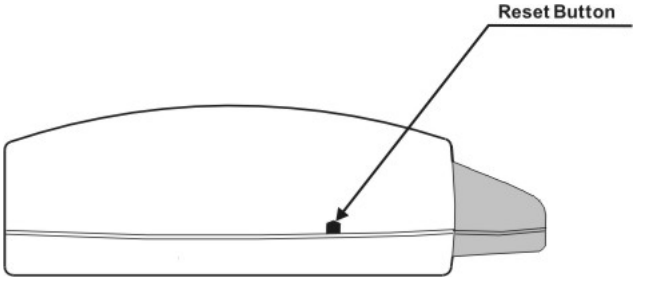


Figure 2-5 Side Panel

2.6.2 Web Configurator

To reset the ZyAIR back to the factory defaults, click the **SYSTEM TOOLS** tab and **Default Settings** to display the screen as shown next.

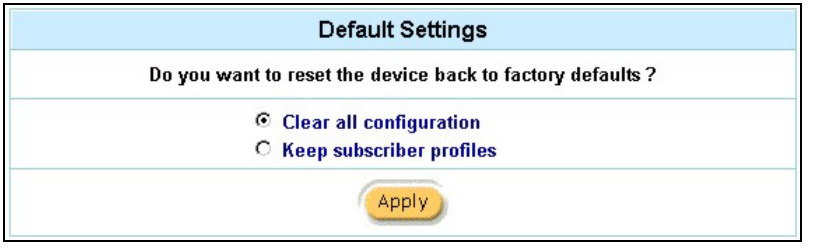


Figure 2-6 Default Settings

The following table describes the labels in this screen.

Table 2-2 Default Settings

LABEL	DESCRIPTION
Clear all configuration	Select this option to reset system configuration back to the factory defaults and erase all custom configuration (including as subscriber account information).
Keep subscriber profile	Select this option to reset the system configuration back to the factory default but retain subscriber account information. All other custom configuration is erased.
Apply	Click **Apply** to reset the ZyAIR.

2.7 Restarting the ZyAIR

You *must* restart the ZyAIR every time you change the system IP address or upload a firmware or configuration file.

Click the **SYSTEM TOOLS** tab, **Restart** and then **Apply**.

Figure 2-7 Restart

When the ZyAIR restarts, all connections will be terminated. Subscribers need to log in again.

2.8 Logging Out of the Web Configurator

Click the **SYSTEM TOOLS** tab, **Logout** and **Apply** to exit from the web configurator.

Figure 2-8 Logging Out

Chapter 3
General System Setup

*This chapter describes how to configure the **System** and **LAN/WAN** advanced setup screens.*

3.1 General System Settings

Click the **ADVANCED SETUP** tab and then **System** to open this screen.

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 a DHCP server 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.

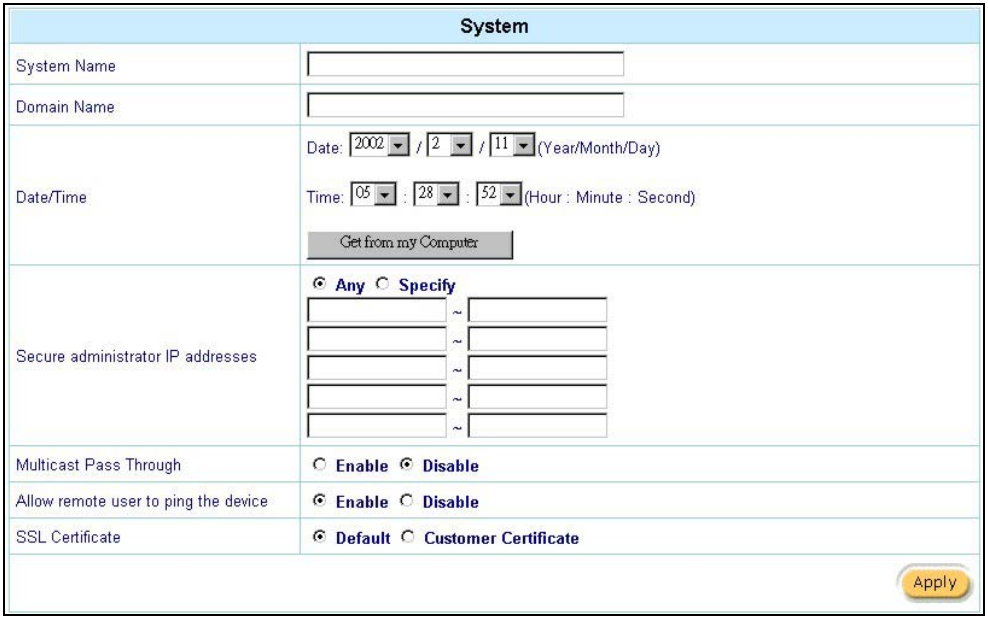


Figure 3-1 System

The following table describes the labels in this screen.

Table 3-1 System

LABEL	DESCRIPTION
System Name	Enter a descriptive name (up to 40 characters) for identification purposes.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ZyAIR may obtain a domain name from a DHCP server. The domain name entered by you is given priority over the DHCP server assigned domain name.
Date/Time	Set the system date and time by selecting the appropriate choices from the drop-down list boxes. Click **Get from my Computer** to set the time and date on the ZyAIR to be the same as the management computer.
Secure administrator IP addresses	Select **Any** to use any computer to access the web configurator on the ZyAIR. Select **Specify** and then enter the IP address(es) or ranges of IP addresses of the computer(s) that are allowed to log in to configure the ZyAIR.
Multicast Pass Through	Select **Enable** to allow multicast traffic to pass through the ZyAIR. This may affect your network performance. Select **Disable** to prevent any multicast traffic from passing through the ZyAIR. This is the default setting.
Allow remote user to ping the device	Select **Enable** to respond to Ping requests. Select **Disable** to not respond to Ping requests.
SSL Certificate	Secure Socket Layer (SSL) security allows you to create a secure connection between the ZyAIR and the client computer(s). Select **Default** to use the default system-generated SSL certificate. Select **Customer Certificate** to use a certificate obtained from a certificate authority. Refer to the *SSL (Secure Socket Layer) Security* chapter for more information.
Apply	Click **Apply** to save the changes.

Chapter 4
WAN, LAN and Server Setup

This chapter shows you how to configure LAN and WAN ports and server settings.

4.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyAIR are preset to the following values:

- Dynamic WAN IP address.
- LAN IP address of 192.168.1.1 with subnet mask of 255.255.255.0
- DHCP server enabled on the LAN with a 252 client IP address pool starting from 192.168.1.2.

These parameters should work for the majority of installations. If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

4.2 LANs and WANs

A LAN (Local Area Network) 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.

4.3 IP Address Assignment

A static IP is a fixed IP that the ZyAIR obtains from a DHCP server on a network. A dynamic IP is not fixed; the DHCP server provides an IP address to the ZyAIR each time it connects to the network. When an Ethernet device is configured to obtain a dynamic IP address from a DHCP server, it is known as a DHCP client.

4.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (Ethernet device) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability, which means it can assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client when this feature is activated. The ZyAIR can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

4.4.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the computers on a LAN share one common network number.

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

The Internet Assigned Number Authority (IANA) reserved a block of addresses specifically for private use (refer to *Section 4.4.2*); 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.

The subnet mask specifies the network number portion of an IP address.

4.4.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, 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:

```
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 it can be assigned from 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.*

4.5 DNS Server Address

DNS (Domain Name System) is for mapping 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. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The

DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. The second is to obtain the DNS server information automatically when a computer is set as a DHCP client.

4.6 PPPoE

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.

4.6.1 PPP MTU

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

4.6.2 TCP MSS

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU).

4.7 PPTP

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.

4.8 Configuring the WAN and LAN Settings

To configure the LAN and WAN settings on the ZyAIR, click the **ADVANCED SETUP** tab and **LAN/WAN** to display the screen as shown. The **WAN/LAN** screen varies depending on the **WAN Port Mode** setting.

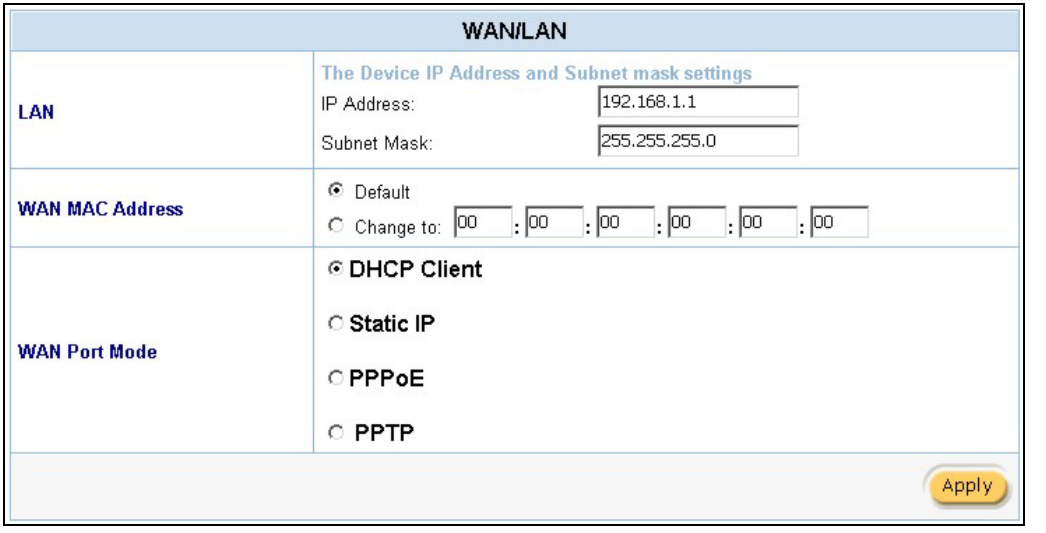


Figure 4-1 WAN/LAN

The following table describes the labels in this screen.

Table 4-1 WAN/LAN

LABEL	DESCRIPTION
LAN	
IP Address	Enter the LAN IP address of the ZyAIR in dotted decimal notation. The default is **192.168.1.1**.
Subnet Mask	Enter the LAN subnet mask in dotted decimal notation. The default is **255.255.255.0**.
WAN MAC Address	Select **Default** to use the factory assigned MAC address. If your ISP requires MAC address authentication, select **Change to** and enter the MAC address of a computer on the LAN in the fields provided.
WAN Port Mode	
DHCP Client	Select this option to set the ZyAIR to act as a DHCP client on the WAN. The ZyAIR obtains TCP/IP information (IP address, DNS server information, etc.) from a DHCP server. This is the default setting.
Static IP Settings	Select this option to set the ZyAIR to use a static (or fixed) IP address.
IP Address	Enter the static IP address in dotted decimal notation.
Subnet Mask	Enter the subnet mask in dotted decimal notation.
Default IP Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the primary and/or secondary DNS servers.
PPPoE	Select this option to activate **PPPoE** support. Refer to *Section 4.6* for more information.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Service Name	Enter the name of your PPPoE service.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.

Table 4-1 WAN/LAN

LABEL	DESCRIPTION
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the ZyAIR will attempt to bring up the connection after the redial period.
PPTP	Select this option to activate **PPTP** support. Refer to *Section 4.7* for more information.
My IP Address	Enter the IP address assigned to you.
My Subnet Mask	Enter the subnet mask assigned to you.
Gateway IP Address	Enter the IP address of the gateway device.
PPTP Server IP Address	Enter the IP address of your ISP's PPTP server.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Connections ID/Name	Enter your identification name of the PPTP server assigned to you by the ISP.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the ZyAIR will attempt to bring up the connection after the redial period.
Apply	Click **Apply** to save the changes.

4.9 Server Configuration

Use the **Server** screen to set the embedded web server, the LAN DHCP server and specify the e-mil server for e-mail redirection on the ZyAIR.

Click the **ADVANCED SETUP** and **Server** to display the screen as shown next.

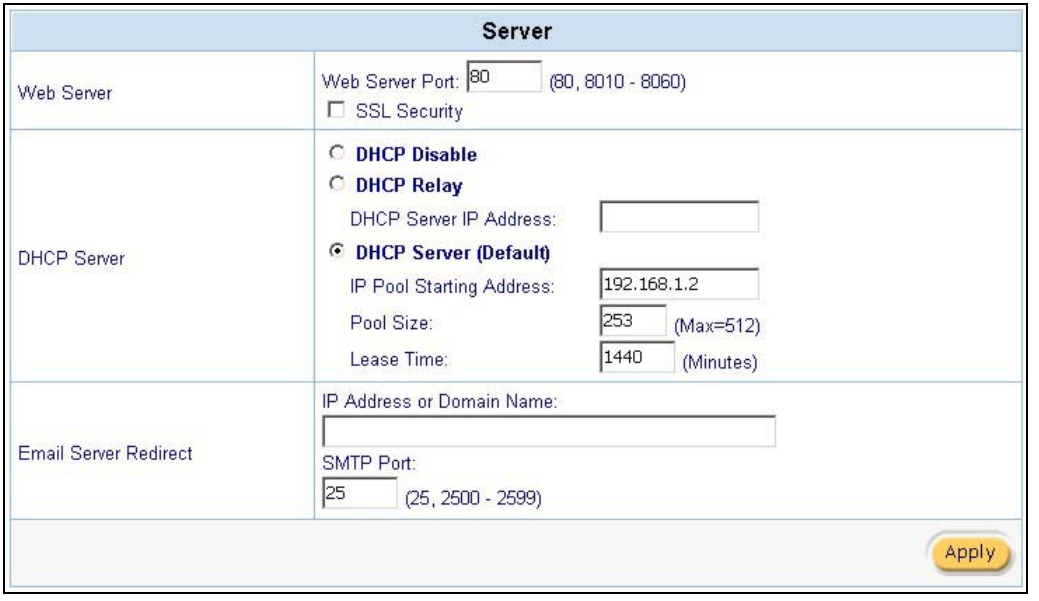


Figure 4-2 Server

The following table describes the fields in this screen.

Table 4-2 Server

LABEL	DESCRIPTION
Web Server	
Web Server Port	Specify the port number of the embedded web server on the ZyAIR for accessing the web configurator. The default port number is **80**. Enter a number between 8010 and 8060 to access the web configurator behind a NAT-enabled network. If you enter a number between 8000 and 8099, you need to append the port number to the **WAN** or **LAN** port IP address to access the web configurator. For example, if you enter “8010” as the web server port number, then you must enter “http://www.192.168.1.1:8010” where 192.168.1.1 is the WAN or LAN port IP address.

Table 4-2 Server

LABEL	DESCRIPTION
SSL Security	Secure Socket Layer (SSL) security allows you to create a secure connection between the ZyAIR and the client computer(s). Refer to the *SSL (Secure Socket Layer) Security* chapter for more information. Select this check box to activate SSL security.
DHCP Server Select the DHCP mode on the LAN.	
DHCP Disable	Select this option to disable DHCP server on the LAN.
DHCP Relay	Select this option to set the ZyAIR to forward network configuration requests to a DHCP server on the LAN network. Then configure the **DHCP Server IP Address** field.
DHCP Server IP Address	If you select **DHCP Relay**, enter the IP address of the real DHCP server.
DHCP Server (Default)	Select this option to set the ZyAIR to assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the **LAN** port(s). This is the default setting.
DHCP Pool Start IP Address	Enter the first of the continuous addresses in the IP address pool. The default is **192.168.1.2**.
DHCP Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 512. The default is **253**.
Lease Duration	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Primary/Secondary DNS IP Address	Enter the IP address of the DNS server(s) in the **Primary DNS IP Address** and/or **Secondary DNS IP Address** fields. **You *must* specify a DNS server.**
E-mail Server Redirect	Specify the IP address or the domain name of the e-mail server to which the ZyAIR forwards e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
Apply	Click **Apply** to save the settings.

Part II:

Subscriber Account Management

This part covers the **ADVANCED SETUP** tab's **Authentication**, **Accounting** and **Login** screens.

Chapter 5 Authentication

This chapter shows you how to set up subscriber authentication on the ZyAIR.

5.1 About the Built-in Authentication

You can use the built-in subscriber database to manage the subscribers. The ZyAIR also provides a simple, built-in billing mechanism to set up accounting information without using an accounting software or an accounting server (such as RADIUS).

5.2 Authentication Settings

Click the **ADVANCED SETUP** tab and **Authentication** to display the screen as shown next.

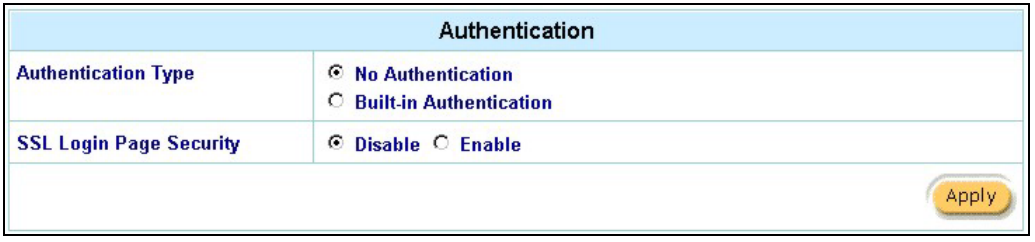


Figure 5-1 System Settings: Authentication

The following table describes the labels in this screen.

Table 5-1 System Settings: Authentication

LABEL	DESCRIPTION
No Authentication	Select this option to disable subscriber authentication. Subscribers can access the Internet without entering user names and passwords. This is the default setting.
Built-in Authentication	Select this option to authenticate the subscribers using the local subscriber database. **When you select this option, you *must* also configure the** Accounting **screen.**

Table 5-1 System Settings: Authentication

LABEL	DESCRIPTION
SSL Login Page Security	Select **Enable** to activate SSL security upon accessing the login screen so that user names and passwords are encrypted before being transmitted to the ZyAIR. Select **Disable** to de-activate SSL security for the subscriber login screen. Refer to the *SSL (Secure Socket Layer) Security* chapter for more information.
Apply	Click **Apply** to save the changes.

Chapter 6
Accounting

This chapter shows you how to set up and manage subscriber accounts.

6.1 About Subscriber Accounts

Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list. Accounts are automatically generated either by pressing the connected exclusive printer's button or using the web configurator (the **Account Generator Panel** screen).

6.1.1 Time-to-finish Accounting Method

The time-to-finish accounting method is good for one-time logins. Once a subscriber logs in, the ZyAIR stores the MAC address of the subscriber's computer for the duration of the time allocated. Thus the subscriber does not have to enter the user name and password again for re-login within the allocated time.

Once activated, the subscriber account is valid until the allocated time is reached even if the subscriber disconnects Internet access for a certain period within the allocated time. For example, Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects his Internet access to go to a 20-minute meeting. After the meeting, he only has 20 minutes left on his account.

6.2 Accounting Settings

Click the **ADVANCED SETUP** tab and **Accounting** to display the screen as shown next.

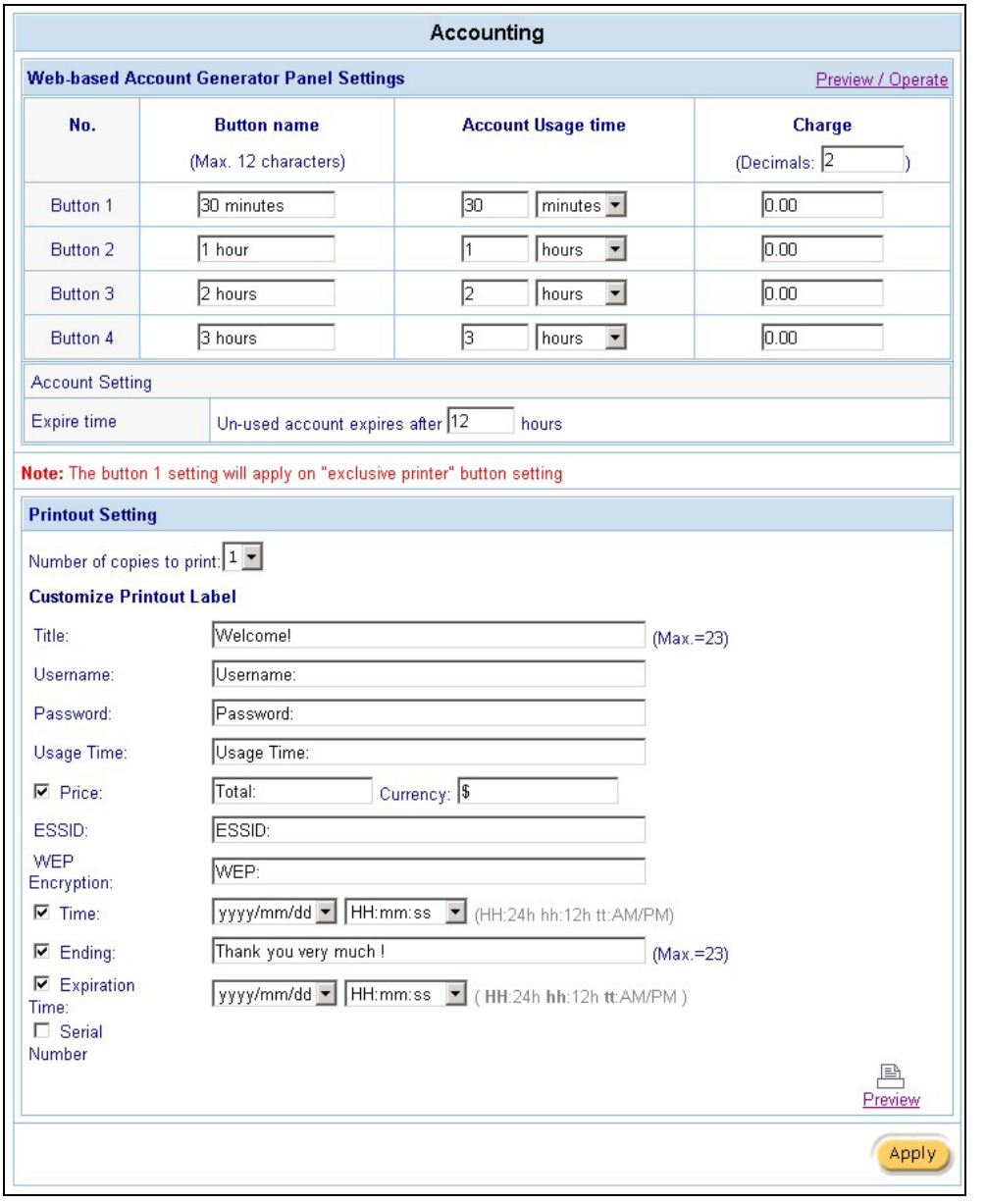


Figure 6-1 Accounting

The following table describes the labels in this screen.

Table 6-1 Accounting

LABEL	DESCRIPTION
Preview/Operate	Click **Preview/Operate** to open the **Account Generator Panel** (see *Figure 6-3*).
No.	This read-only field displays the button index number (Button 1..4). The button numbers correspond to the buttons displayed in the **Account Generator Panel** (see *Figure 6-3*). The button 1 settings will apply to the “exclusive printer” button setting.
Button name	A button is a subscriber “profile” defining maximum Internet access time and charge per time unit. The button 1 settings also apply to the button on the “exclusive printer”. The button numbers correspond to the buttons displayed in the **Account Generator Panel**. Type up to 12 characters to specify the names that appear on the buttons. The defaults are **30 minutes**, **1 hour**, **2 hours** and **3 hours**.
Account Usage Time	Select a time period (**minutes**, **hours**, or **days**) and enter the time unit in the field provided to define each “profile’s” maximum Internet access time. The defaults are **Button 1** 30 minutes, **Button 2** 1hour, **Button 3** 2hours and **Button 4** 3hours.
Charge	Define each “profile’s” charge, up to 999999, per time unit (configured in the **Account Usage Time** field). The default is 0.00.
Decimals	Define the number of decimal places allowed (up to 3) for the total amount charged that appears in the subscriber’s statement in the **Decimals** field.
Account Setting	
Expire Time	Specify the number of hours (1 to 168) to wait before the ZyAIR deletes an inactive account (default 12).
Printout Setting	
Number of copies to print	Select how many copies of subscriber statements you want to print (1 is the default).
Customize Printout Label	
Title	Enter a title (up to 24 characters) for the printout.

Table 6-1 Accounting

LABEL	DESCRIPTION
Username	Enter the label name for the field that displays the account username.
Password	Enter the label name for the field that displays the account password.
Usage Time	Type a label name for the maximum time allowed for a subscriber to access the Internet via the ZyAIR.
Price	Select this check box and type a label for the field displaying the total charge to the subscriber in the statement.
Currency	Type a currency prefix that displays before the total charge amount in the statement.
ESSID	Type a label name for the field displaying the wireless LAN's Extended Service Set Identifier (**ESSID**).
WEP	Type a label name for the field displaying the Wired Equivalent Privacy (**WEP Encryption**) key.
Time	Select this check box to display the time an account is created and then select date and time formats from the drop-down list boxes.
Ending	Select this check box to display (in the statement) the ending subscription validity date and time and then select the date and time formats from the drop-down list boxes.
Expiration Time	Select this check box to display (in the statement) the ending subscription validity date and time and then select the date and time formats from the drop-down list boxes.
Serial Number	Select this check box to generate and display (in the statement) a number for each subscriber account that you use the ZyAIR to generate.
Preview	Click **Preview** to display a sample of the statement layout in a new window (see *Figure 6-2*). If you modify the settings on this page, click **Apply** before you click **Preview** if you want to see how the changed settings will affect the statement layout.
Apply	Click **Apply** to save your settings to the ZyAIR.

The following is an example of how your custom statement printout will look. Close this window when you are finished viewing it.

Figure 6-2 Printout Label Preview Example

6.3 Creating Accounts

There are two ways to create subscriber accounts: using the **Account Generator Panel** screen in the web configurator or using the exclusive printer.

6.3.1 Creating Accounts in the Web Configurator

To create subscriber accounts, click **Preview/Operate** in the **Accounting** screen to display the **Account Generator Panel** screen shown next.

Figure 6-3 Account Generator Panel

The settings for the first button apply to the button on the exclusive printer. [1]

Click a button to generate an account based on the settings you configure for the button in the **Accounting** screen. A window displays showing a printout preview of the account generated.

The following figure shows an example.

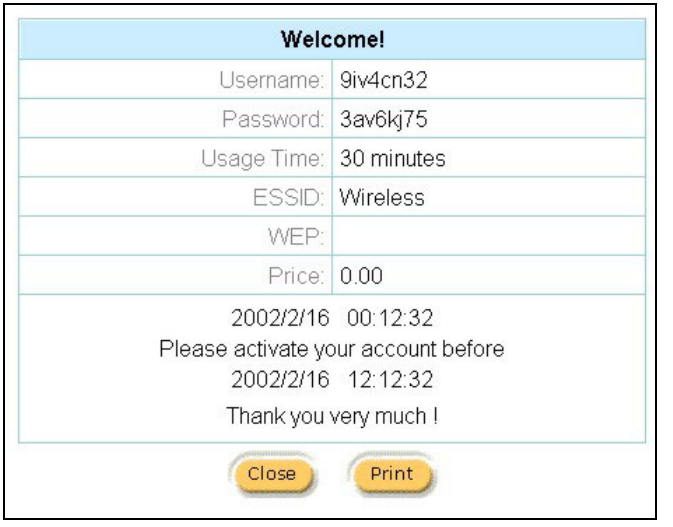


Figure 6-4 Account Information Printout Example

6.3.2 Using the Exclusive Printer to Create and Print Subscriber Statements

Follow the steps below to setup and create subscriber accounts and print subscriber statements using an external statement printer.

Step 1. Make sure that the printer's is connected to the appropriate power and the ZyAIR, and that there is printing paper in the statement printer. Refer to the printer's *User's Guide* for details.

Step 2. Press the button on the Statement Printer. The ZyAIR generates a dynamic account and the printer prints the subscriber's statement. Refer to *Figure 6-4* for a printout example.

[1] The web-based account generator and the exclusive printer do not function together at the time of writing.

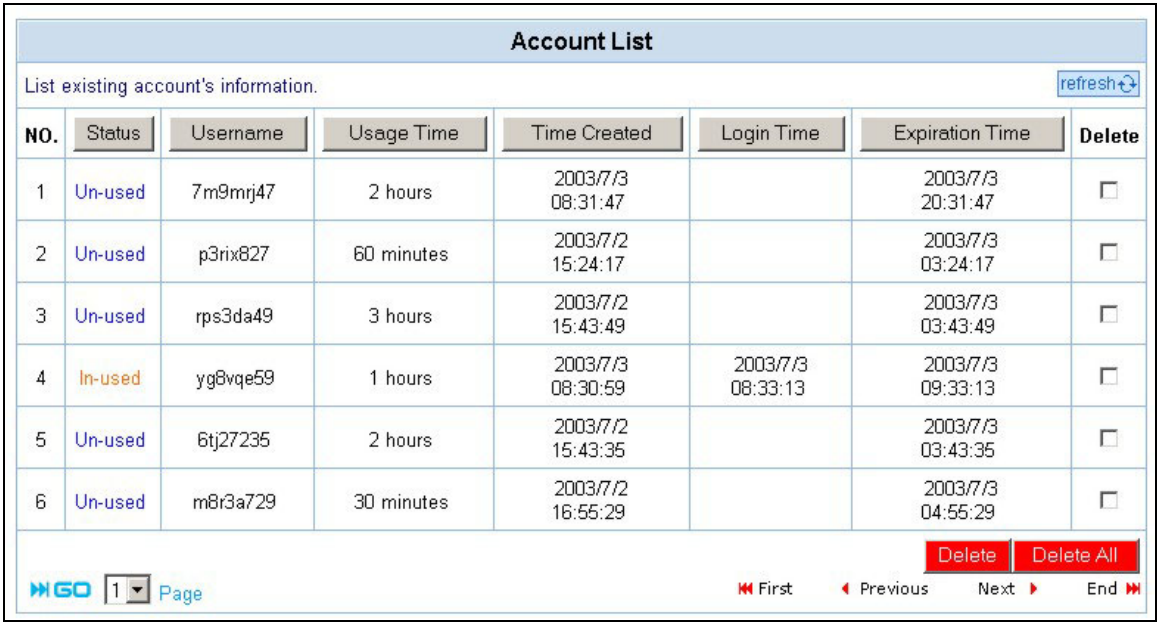
The settings of the button on the statement printer correspond to the first button in the *Account Operator Panel* screen. Refer to *Figure 6-3*.

Refer to section *6.2* to configure the printout page.

6.4 Viewing the Account List

Do one of the following to view the account list.

- From the **Account Generator Panel** screen (refer to *Figure 6-3*) and click **View Account List**.
- From the **SYSTEM STATUS** sub-menus, click **Account List**.



Account List

List existing account's information. refresh

NO.	Status	Username	Usage Time	Time Created	Login Time	Expiration Time	Delete
1	Un-used	7m9mrj47	2 hours	2003/7/3 08:31:47		2003/7/3 20:31:47	
2	Un-used	p3rix827	60 minutes	2003/7/2 15:24:17		2003/7/3 03:24:17	
3	Un-used	rps3da49	3 hours	2003/7/2 15:43:49		2003/7/3 03:43:49	
4	In-used	yg8vqe59	1 hours	2003/7/3 08:30:59	2003/7/3 08:33:13	2003/7/3 09:33:13	
5	Un-used	6tj27235	2 hours	2003/7/2 15:43:35		2003/7/3 03:43:35	
6	Un-used	m8r3a729	30 minutes	2003/7/2 16:55:29		2003/7/3 04:55:29	

Delete Delete All

GO 1 Page First Previous Next End

Figure 6-5 Account List

The following table describes the labels in this screen.

Table 6-2 Account List

LABEL	DESCRIPTION
Refresh	Click **Refresh** to update this screen.

Table 6-2 Account List

LABEL	DESCRIPTION
NO	This field displays the index number of an entry. The maximum number of subscriber account entries is 512.
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **UN-Used**.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.
Create Time	This field displays when the account was created (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Expire Time	This field displays when the subscriber's account becomes invalid (in yyyy/mm/dd HH/mm/ss format). When the subscriber has already logged into the account, this field displays the time until which the subscriber can continue to use the account to access the Internet. When the subscriber has not yet logged into the account, this field displays the time that the account expires if the subscriber does not log into it. Click the heading to sort the entries in ascending or descending order based on this column.
Delete All	Click **Delete All** to remove all accounts.
Delete	Click **Delete** to remove the selected account.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.

Refer to the *Subscriber Login* appendix for more information on logging in as a subscriber.

Chapter 7
Subscriber Login Screen

This chapter shows you how to customize the subscriber login screen when subscriber control is activated.

7.1 About the Subscriber Login Screen

When subscriber authentication is activated in the **Authentication** screen, the subscriber login screen is the first screen that all subscribers see when trying to access the Internet. You can configure walled garden web addresses for web sites that all subscribers are allowed to access without logging in (refer to the chapter on advertisement links and walled garden).

The ZyAIR provides different formats in which you can customize the login screen: **Standard**, **Redirect**, **Advanced** and **Frame**.

7.2 Customizing the Subscriber Login Screen

To customize the subscriber login screen, click the **ADVANCED SETUP** tab and **Login Page** to display the screen as shown next.

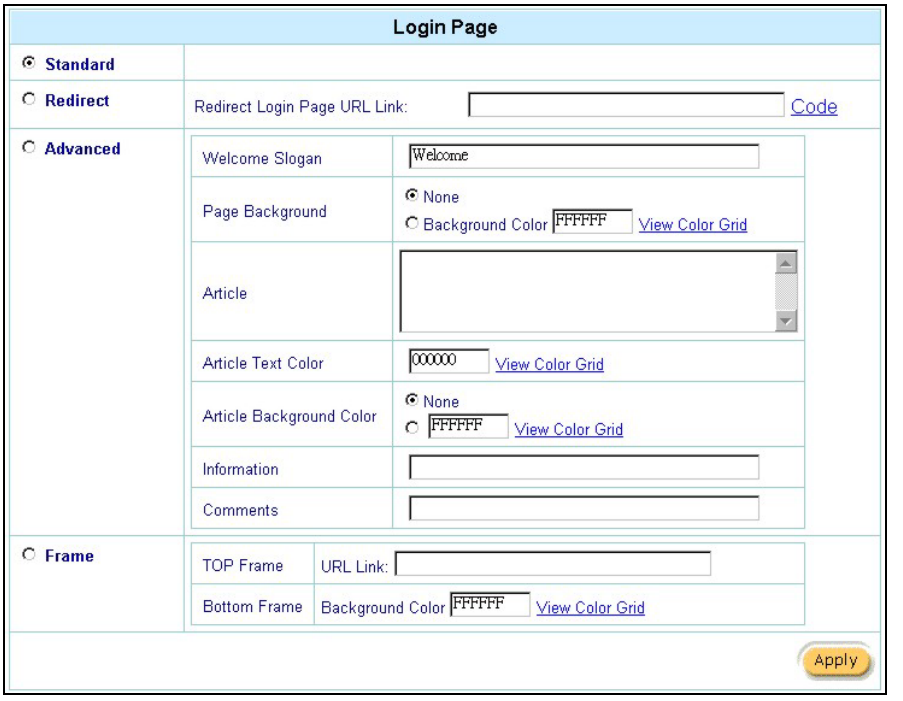


Figure 7-1 Login Page

7.2.1 Standard Subscriber Login Screen

The standard subscriber login screen is the ZyAIR's pre-configured, default simple login screen. In **Login Screen**, select **Standard**. The following figure shows an example of what a subscriber sees when logging in.

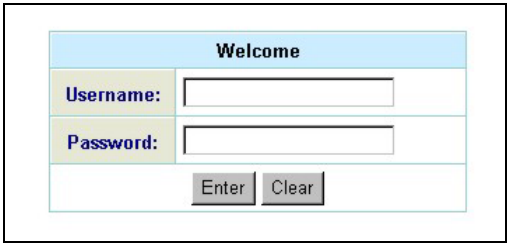


Figure 7-2 Subscriber Login Screen Example: Standard

7.2.2 Redirect Subscriber Login Screen

You can set the ZyAIR to redirect the subscribers to another login screen.

In the **Login Screen Configuration** screen, select **Redirect**.

Figure 7-3 Subscriber Login Screen: Redirect

The following table describes the related labels.

Table 7-1 Subscriber Login Screen: Redirect

LABEL	DESCRIPTION
Redirect	Select this option to direct the subscriber to another login screen.
Redirect Login Page URL Link	Specify the web site address to which the ZyAIR directs the subscribers for logins.
Code	Click **Code** to display the source code of the web page you specify above (see *Figure 7-4*).

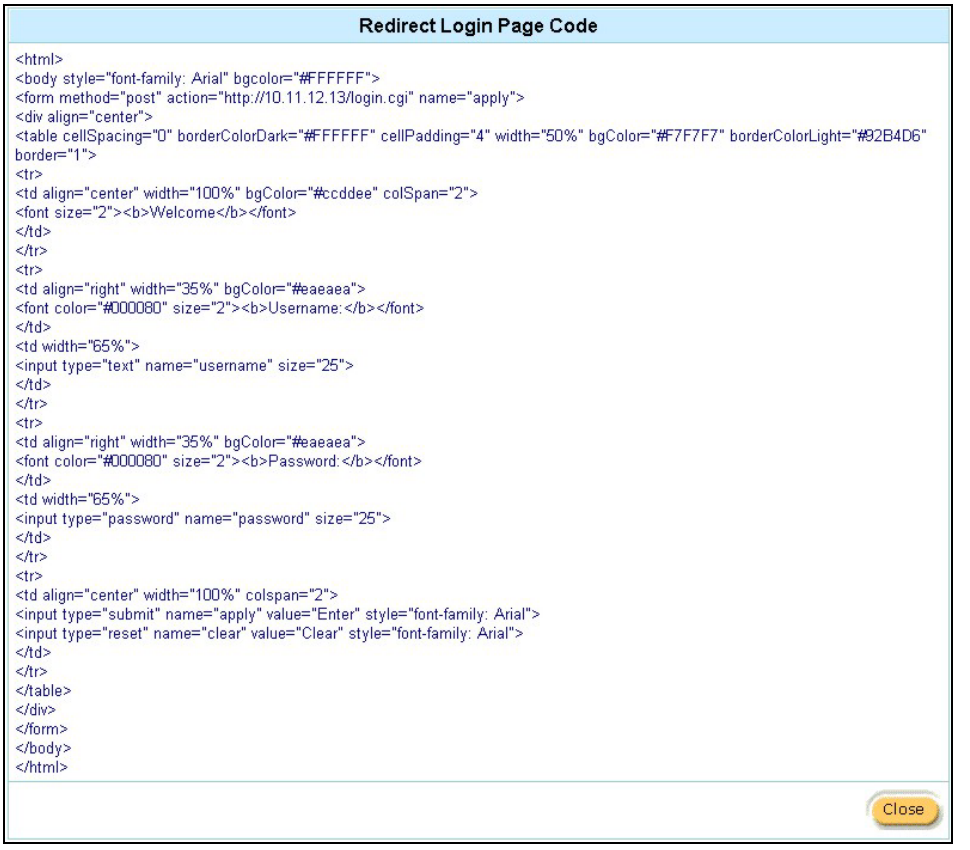


Figure 7-4 Subscriber Login Screen: Redirect Code

7.2.3 Advanced Subscriber Login Screen

Use the **Advanced** login screen option to customize a login screen where you can create a welcome slogan and add advertising information.

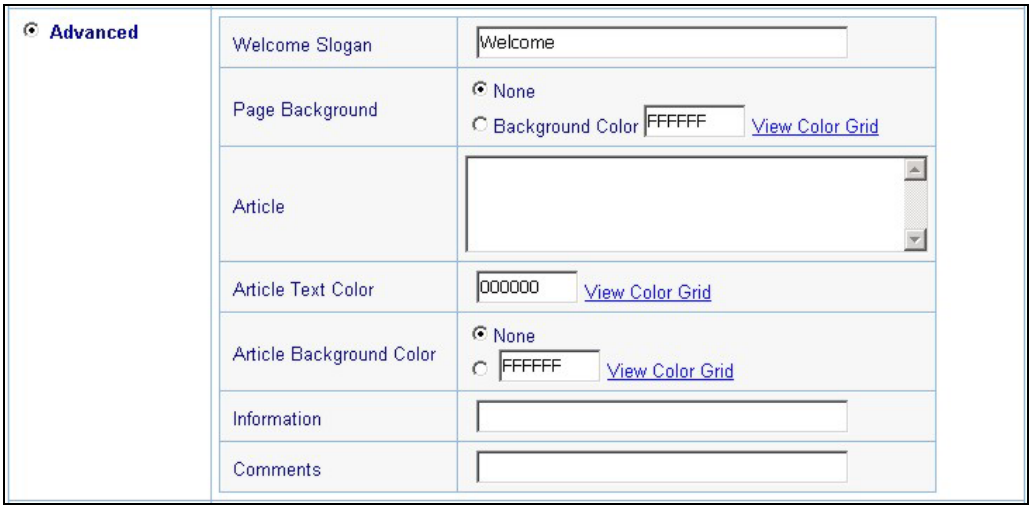


Figure 7-5 Subscriber Login Screen: Advanced

The following table describes the related labels.

Table 7-2 Subscriber Login Screen: Advanced

LABEL	DESCRIPTION
Advanced	Select this option to set the ZyAIR to display the advanced subscriber login screen.
Welcome Slogan	Enter a welcome message (up to 80 characters long) in the text box provided.
Page Background	Select **None** to set the background color of the login screen to white (the default). Select **Background Color** to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 1024 characters long) in the text box. This is useful for advertisements or announcements.
Article Text Color	Select **None** to set the article text color of the login screen to white (the default). Select and set the color of the article text block background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Information	Enter information such address and telephone or fax numbers in the text box provided. Up to 80 characters allowed.

Table 7-2 Subscriber Login Screen: Advanced

LABEL	DESCRIPTION
Comments	Enter any comments (up to 80 characters long) in the text box provided.

The web-friendly color sets are displayed in the figure shown.

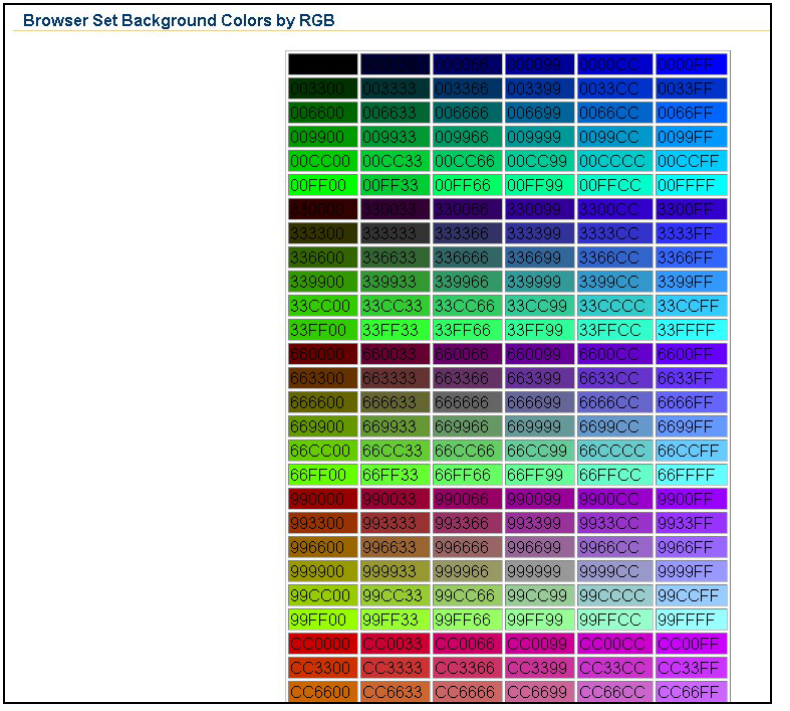


Figure 7-6 Subscriber Login Screen: Color Grid

The following figure shows an advanced subscriber login screen example.

Figure 7-7 Subscriber Login Screen Example: Advanced

7.2.4 Framed Subscriber Login Screen

The **Frame** login screen splits the login screen into two frames: top and bottom. You can specify a web site to be displayed in the top frame with the user name and password prompt displayed in the bottom frame. The frame login screen is useful for you to link to a web site (such as the company web site) as your welcome screen. In addition, you can externally design a web page with images and/or advanced multimedia features.

Figure 7-8 Subscriber Login Screen: Frame

The following table describes the related labels.

Table 7-3 Subscriber Login Screen: Frame

LABEL	DESCRIPTION
Frame	Select this option to configure and set the ZyAIR to display the subscriber login screen in two frames.
TOP Frame	Enter a web site address in the **URL Link** field, for example, http://www.zyxel.com.
Bottom Frame Background Color	Specify the color of the frame background. For example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly color and corresponding hexadecimal values. The default is white ("FFFFFF").

The following figure shows a framed subscriber login screen example.

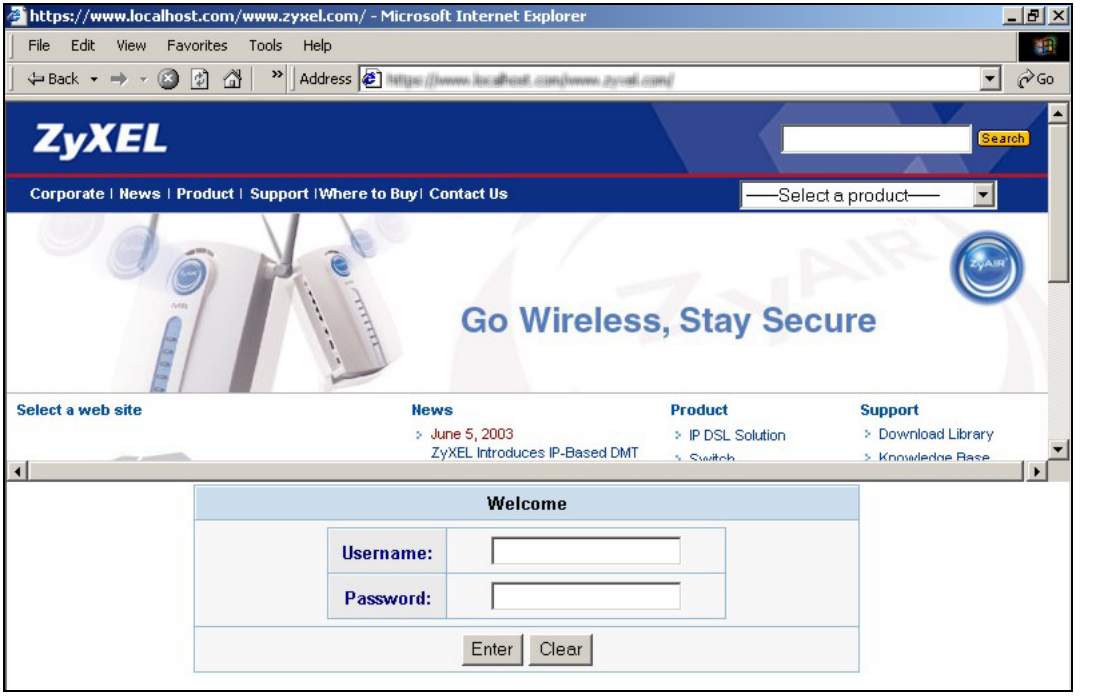


Figure 7-9 Subscriber Login Screen Example: Frame

Part III:

Advanced Subscriber Account Management

This part covers the **ADVANCED SETUP** tab's **Advertisement**, **Walled Garden**, **Syslog** and **Wireless** screens.

Chapter 8
Advertisement Links and Walled Garden

This chapter shows you how to set advertisement links and create walled garden web sites.

8.1 Advertisement Links and Walled Garden Overview

When you enable subscriber authentication in the **Authentication** screen, you can set the ZyAIR to display advertisement links or activate the walled garden feature for generating on-line advertising revenues.

8.2 Advertisement Links

You can set the ZyAIR to display an advertisement web page as the first web page whenever the subscriber connects to the Internet. Click **ADVANCED SETUP** and **Advertisement** to display the screen as shown next.

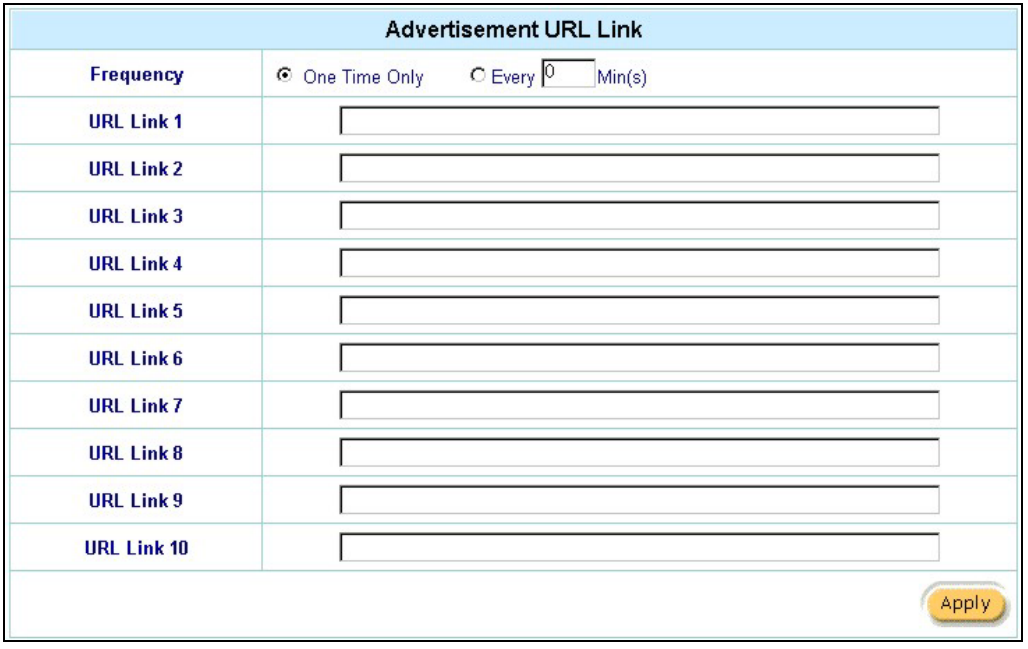


Figure 8-1 Advertisement

The following table describes the labels in this screen.

Table 8-1 Advertisement

LABEL	DESCRIPTION
Frequency	Select **One Time Only** to display an advertisement web site in an active browser window once after a subscriber logs in successfully. Select **Every … Min(s)** to display an advertisement web site in an active browser window once every time period specified (in minutes) after a subscriber logs in successfully. **The advertisement links are displayed randomly one at a time.**
URL Link 1 .. 10	Enter the web site addresses in the fields provided.
Apply	Click **Apply** to save the changes.

8.3 Walled Garden

A subscriber must log in before the ZyAIR allows the subscriber access to the Internet. However, with a walled garden, you can define a web site address(es) which all subscribers can access without logging in.

Click **ADVANCED SETUP** and then **Walled Garden** to display the screen as shown.

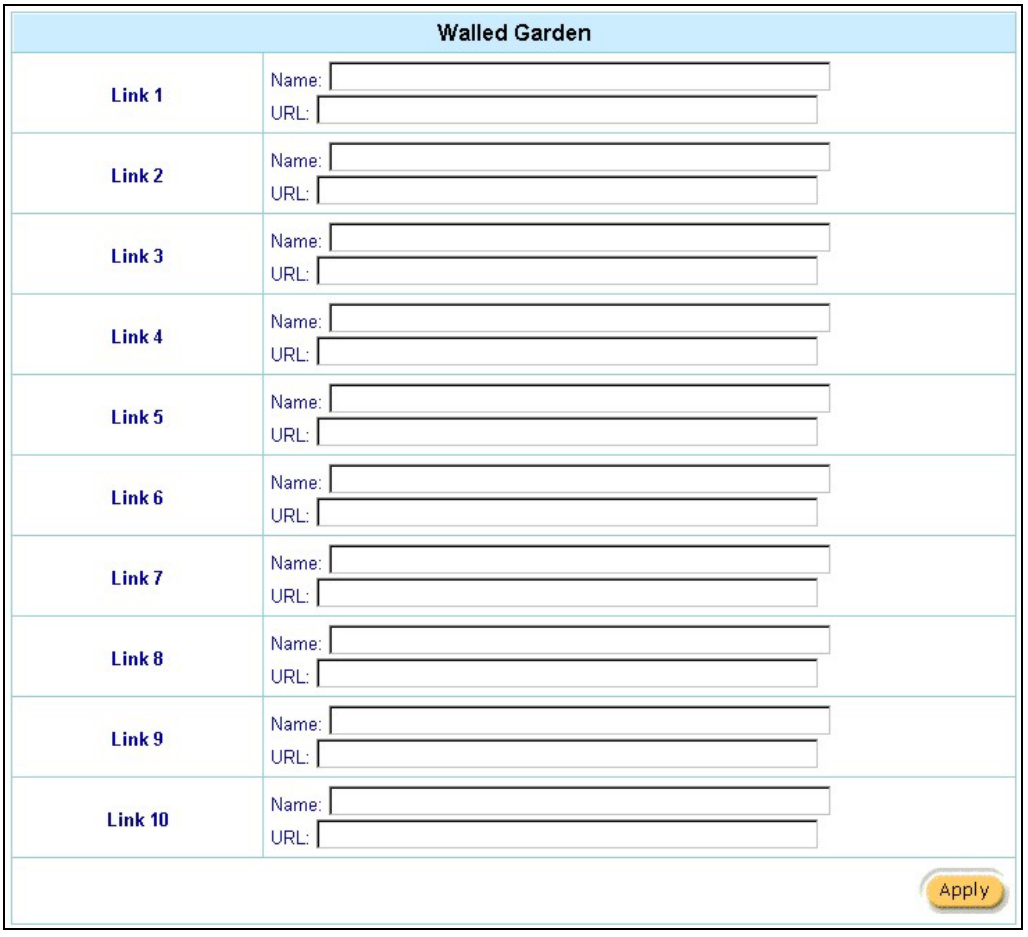


Figure 8-2 Walled Garden

The following table describes the labels in this screen.

Table 8-2 Walled Garden

LABEL	DESCRIPTION
Link 1 … 10	In the **Name** field, enter a descriptive name (up to 80 characters) for the walled garden link to be displayed in the web browser. In the **URL** field, enter the web site address (up to 200 characters) of the web site. See the chapter on login setup for a sample display of the login screen.
Apply	Click **Apply** to save the changes.

8.3.1 Walled Garden Login Example

The following figure shows the subscriber login screen with four walled garden links (the links are named **Walled Garden Link 1** through **4** for demonstration purposes, see *Table 8-2* to configure your own custom link names).

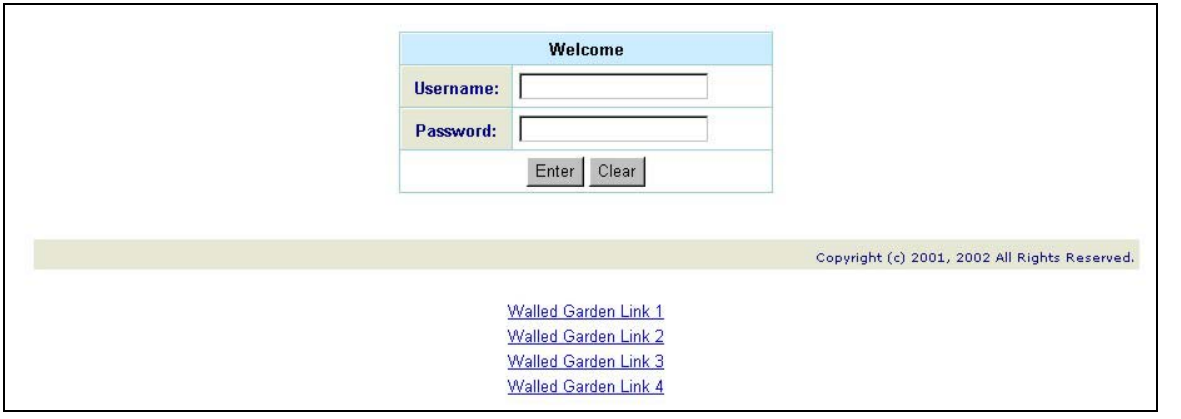


Figure 8-3 Walled Garden Login Example

Chapter 9
Syslog

This chapter shows you how to configure syslog on the ZyAIR.

9.1 Syslog Configuration

Use the **Syslog Configuration** screen to configure to where the ZyAIR is to send logs; which logs the ZyAIR is to send and the schedule for when the ZyAIR is to send the logs.

To configure the syslog settings, click **ADVANCED SETUP**, **Syslog** to display the screen as shown next.

Figure 9-1 Syslog Configuration

The following table describes the labels in this screen.

Table 9-1 Syslog Configuration

LABEL	DESCRIPTION
Syslog	Select **Enable** to activate the syslog function. Select **Disable** to de-activate the syslog function.
Syslog Server	
Syslog on LAN	Select this check box to specify a syslog server on the LAN.
Server IP Address	Enter the IP address (in dotted decimal notation) of the syslog server on the LAN.
Server MAC Address	Enter the MAC address of the syslog server on the LAN.
Syslog on WAN	Select this check box to specify a syslog server on the WAN.
Server 1 IP Address	Enter the IP address of the first syslog server on the WAN in dotted decimal notation.
Server 2 IP Address	Enter the IP address of the second syslog server on the WAN in dotted decimal notation.
Log Settings	
Syslog Name	This field displays the name (or type) of the syslog. Select the check box(es) to send the syslog.
Description	This field displays a short description about the syslog.
Interval Time	This field displays when or how often the ZyAIR sends the syslog. If available, enter the number of minutes the ZyAIR waits between sending the syslog.
Apply	Click **Apply** to save the settings.

Chapter 10
Wireless LAN

This chapter shows you how to configure wireless LAN settings on the ZyAIR and set up WEP encryption keys.

10.1 Wireless LAN Overview

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

10.1.1 IBSS

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

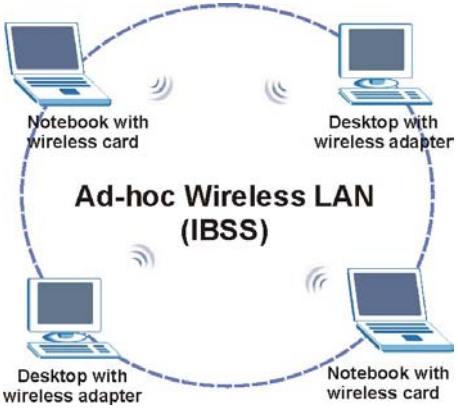


Figure 10-1 IBSS (Ad-hoc) Wireless LAN

10.1.2 BSS

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

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

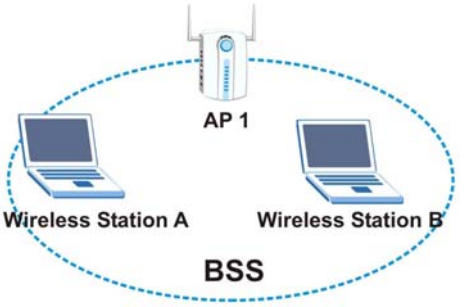


Figure 10-2 Basic Service set

10.1.3 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.

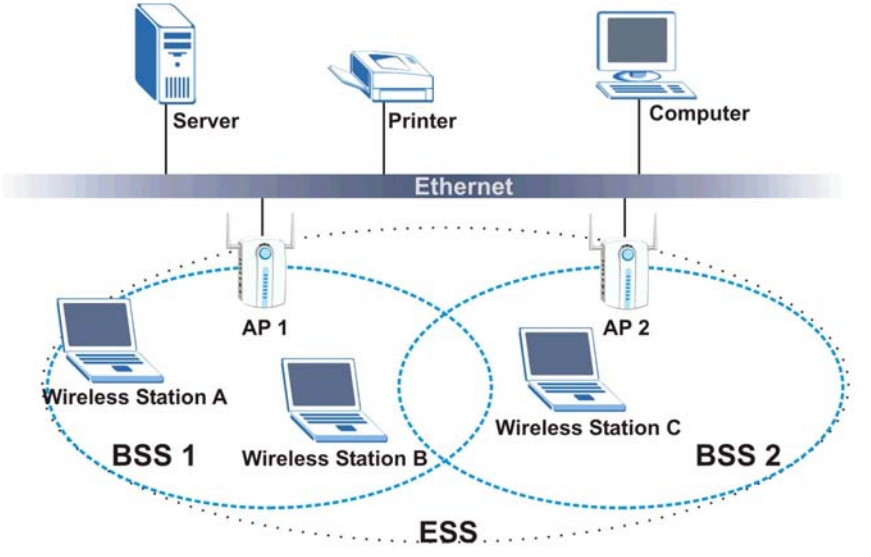


Figure 10-3 Extended Service Set

10.2 Wireless LAN Basics

This section provides background information on Wireless LAN features.

10.2.1 Channel

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

Adjacent channels partially overlap however. To avoid interference due to overlap, your 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 and 11.

10.2.2 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. WEP degrades performance.

10.2.3 RTS/CTS

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

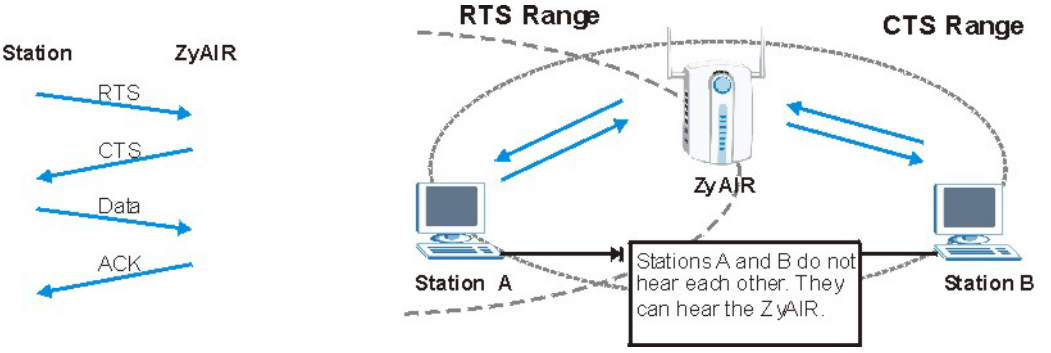


Figure 10-4 RTS/CTS

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.

10.2.4 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.

10.2.5 Preamble Type

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

Long preamble mode allows more processing time for each transmitted data packet. Short preamble mode allows less processing time for the transmitted data packets.

Using short preamble mode may minimize overhead and maximize network throughput. However, short preamble mode is supported by IEEE 802.11b compliant wireless devices, thus wireless stations using short preamble mode cannot communicate with wireless stations using the original IEEE 802.11 standard.

10.3 Wireless LAN Setup

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 SETUP** and then **WIRELESS** to open the **Wireless** screen.

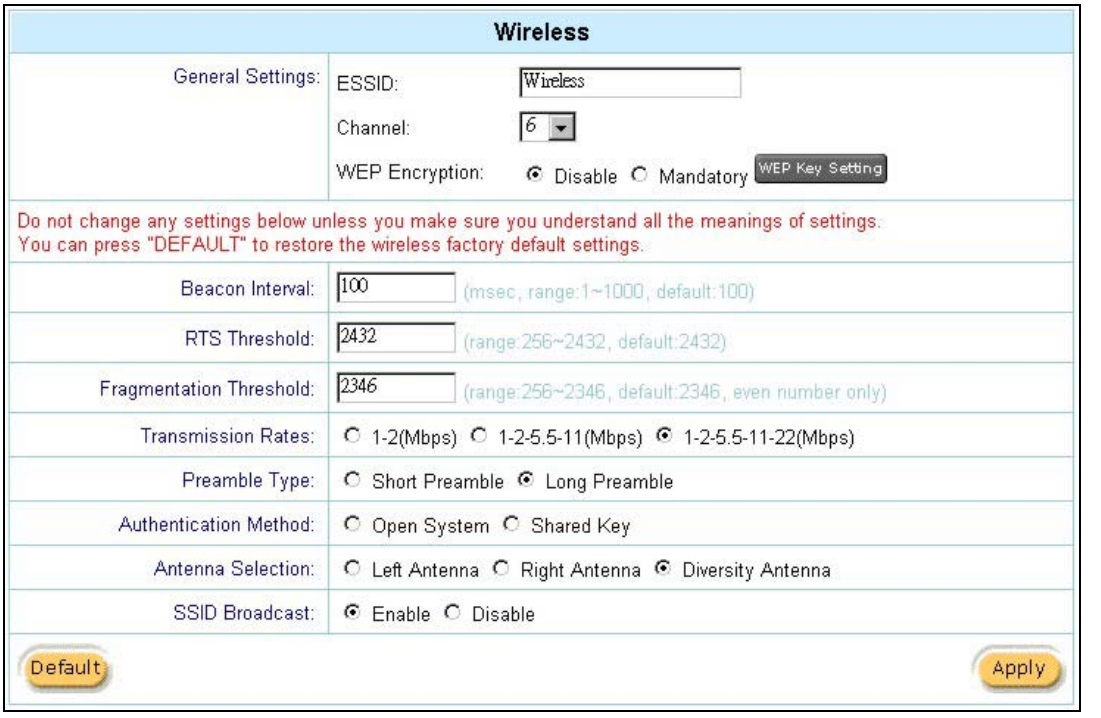


Figure 10-5 Wireless

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

Table 10-1 Wireless

LABEL	DESCRIPTION
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 click **Apply**. You must then change the wireless settings of your computer to match the ZyAIR's new settings.
Channel	Select a channel from the drop-down list box depending on your particular region.

Table 10-1 Wireless

LABEL	DESCRIPTION
WEP Encryption	Select **Disable** to allow all wireless computers to communicate with the access points without any data encryption. Select **Mandatory** to enable WEP data encryption. Then click **WEP Key Setup** to open a screen where you can configure the WEP keys on the ZyAIR. Refer to *Section 10.3.1*.
Beacon Interval	Set the number of milliseconds that should pass between sending out a beacon. Enter a time period between 1 and 1000. The default is **100**.
RTS Threshold	Enter a value between 0 and 2442 to enable an RTS/CTS handshake to avoid retransmitting due to hidden nodes. The default is **2432**.
Fragmentation Threshold	Enter a value between 256 and 2446 to enable a fragmentation threshold. This sets the maximum size of data fragments that can be sent. The default is **2432**. Use a low setting if there is a great deal of radio interference.
DTIM Interval	This setting, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells client devices that are set to power-save that a packet is waiting for them. The DTIM Interval's valid range is 1 to 65535.
Transmission Rates	The basic transfer rates should be set depending on the speed of your wireless network. The default setting is 1-2-5.5-22 (Mbps).
Preamble Type	Select either **Short Preamble** or **Long Preamble**.
Antenna Selection	Select **Left Antenna** if your device has removable antennas and you install a high-gain antenna on the connector on the left (when you look at the device's rear panel). Select **Right Antenna** if your device has removable antennas and you install a high-gain antenna on the connector on the right (when you look at the device's rear panel). Select **Diversity Antenna** (default) to have the device use the antenna that receives the best signal.

Table 10-1 Wireless

LABEL	DESCRIPTION
Authentication Method	Select **Open System** to allow any device to authenticate and then attempt to communicate with the ZyAIR. Using open authentication, any wireless device can authenticate with the ZyAIR, but the device can only communicate if its WEP keys match the ZyAIR. Devices not using WEP do not attempt to authenticate with a ZyAIR that is using WEP. Open authentication does not rely on a RADIUS server on your network. Select **Shared Key** to have the ZyAIR use shared key authentication. The ZyAIR sends an unencrypted challenge text string to any device attempting to communicate with the ZyAIR. The device-requesting authentication encrypts the challenge text and sends it back to the ZyAIR. If the challenge text is encrypted correctly, the ZyAIR allows the requesting device to authenticate. However, both the unencrypted challenge and the encrypted challenge can be monitored; thus leaving the ZyAIR open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network. Select **Both** to allow subscribers to communicate with or without data encryption.
SSID Broadcast	Select **Enable** to allow devices that do not specify an SSID (Service Set Identity) to associate with the ZyAIR. Select **Disable** to stop devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) from associating with the ZyAIR. The SSID on the subscriber's device must match the ZyAIR's SSID exactly.
Default	Click this button to load the factory default wireless LAN settings.
Apply	Click **Apply** to save the settings.

10.3.1 Configuring WEP Keys

When you select **Mandatory** in the **WEP Encryption** field in the **Wireless** screen, click **WEP Key Setting** to display the screen as shown.

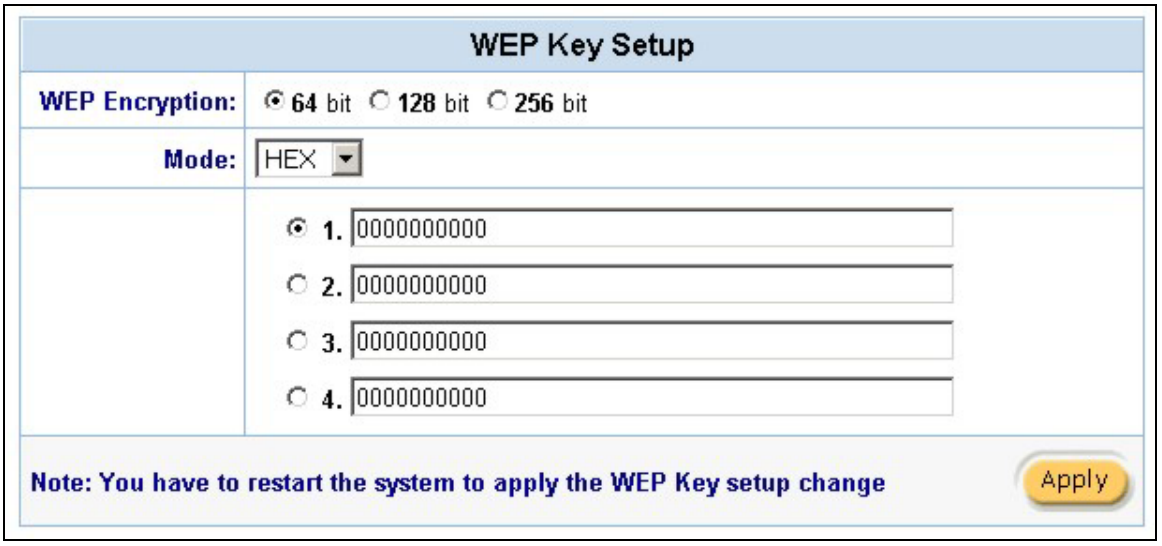


Figure 10-6 WEP Key Setup

The following table describes the labels in this screen.

Table 10-2 WEP Key Setup

LABEL	DESCRIPTION
WEP Encryption	Select **64 bit**, **128 bit** or **256 bit** for the WEP key length.
Mode	Select the type of input mode from the drop-down list box. Choices are **HEX** and **ASCII**. Select **ASCII** to enter the WEP keys as ASCII characters. Select **HEX** to enter the WEP keys as hexadecimal characters.

Table 10-2 WEP Key Setup

LABEL	DESCRIPTION
1 … 4	Enter the WEP keys in the fields provided and select a key as the default key to use. If you select **64 bit** in the **WEP Encryption** field. ◆ Enter either 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (e.g. 11AA22BB33) for HEX key type or ◆ Enter 5 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (e.g. MyKey) for ASCII key type. If you select **128 bit** in the **WEP Encryption** field, ◆ Enter either 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for HEX key type or ◆ Enter 13 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type. If you select **256 bit** in the **WEP Encryption** field, ◆ Enter either 58 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” for HEX key type or ◆ Enter 29 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” for ASCII key type. **ASCII WEP keys are case sensitive.** **You *must* configure all four WEP keys the first time you use the ZyAIR.**
Apply	Click **Apply** to save the changes.

Part IV:

System Status, System Tools and Troubleshooting

This part covers the sub-menus in **SYSTEM STATUS** and **SYSTEM TOOLS** and troubleshooting.

Chapter 11
System Status

*This chapter describes the screens under **System Status**.*

11.1 About System Status

The screens in **SYSTEM STATUS** show the current state of the ZyAIR.

11.2 View System Information

Click **SYSTEM STATUS** and **System** to display the screen as shown next.

System		
Display the WAN connection status, firmware and hardware version.		
System Status	System Name:	
	Bootrom Version:	1.03
	Firmware Version:	1.00.05
	Wireless Version:	1.00a
	Concurrent Users Limitation:	100
	WAN MAC Address:	00:A0:CF:41:E0:CB
	LAN MAC Address:	00:A0:CF:41:E0:CA
WAN IP Settings	WAN Port Mode:	DHCP Client
	IP Address:	None
	Subnet Mask:	None
	Gateway IP address:	None
DNS	Primary DNS Server:	
	Secondary DNS Server:	
LAN DHCP	DHCP Status	Server
	Start IP Address:	192.168.1.2
	End IP Address:	192.168.1.254
	Lease Time:	1440
E-Mail	Server IP Address:	
SSL Certificate	Country	00
	State	Local State
	Local City	Local City
	Organization	Local Group
	Organization Unit	Local Host
	Common Name	10.11.12.13
	Email Address	mail@localhost.com

Figure 11-1 System

The following table describes the labels in this screen.

Table 11-1 System

LABEL	DESCRIPTION
System Status	
System Name	This field displays the description name of the ZyAIR for identification purposes.
Bootrom Version	This field displays the version of the bootbase in the ZyAIR.
Firmware Version	This field displays the version of the firmware on the ZyAIR.
Wireless Version	This field displays the version of the wireless features on the ZyAIR.
Concurrent Users Limitation	This field displays the maximum number of users that can connect to the ZyAIR at the same time.
WAN MAC Address	This field displays the MAC address of the ZyAIR on the WAN.
LAN MAC Address	This field displays the MAC address of the ZyAIR on the LAN.
WAN IP Settings	
WAN Port Mode	This field displays the DHCP mode of the WAN port. It displays either **DHCP Client** or **Static IP Setting**.
IP Address	This field displays the IP address of the WAN port on the ZyAIR.
Subnet Mask	This field displays the subnet mask of the WAN port on the ZyAIR.
Gateway IP address	This field displays the IP address of the default gateway of the WAN port on the ZyAIR.
DNS	
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
LAN DHCP	
DHCP Status	This field displays the DHCP mode on the LAN.
Start IP Address	This field displays the first of the continuous addresses in the IP address pool.
End IP Address	This field displays the last of the continuous addresses in the IP address pool.

Table 11-1 System

LABEL	DESCRIPTION
Lease Time	This field displays the time period (in minutes between 1 and 71582788) during which a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
E-mail	
Server IP Address	The field displays the IP address or the domain name of the SMTP server.
SSL Certification	
Country	This field displays the two-letter abbreviation of your country.
State	This field displays the name of the state or province where your organization is located.
Local City	This field displays the name of the city your organization is located.
Organization	This field displays the name of your organization.
Origination Unit	This field displays additional information about your organization.
Common Name	This field displays the fully qualified domain name of your web server.
Email Address	This field displays your e-mail address.

11.3 Account List

Refer to the *Accounting* chapter for an example and explanation of the **Account List** screen.

11.4 Account Log

The **Account Log** screen displays information on the ZyAIR's subscriber account logs.

Click **SYSTEM STATUS** and **Current Users** to display the screen as shown. Click a column heading to sort the entries if applicable.

Figure 11-2 Account Log

The following table describes the labels in this screen.

Table 2 Account Log

FIELD	DESCRIPTION
Clear Log	Click **Clear Log** to remove all of the log entries from the ZyAIR's memory and this screen.
Refresh	Click **Refresh** to update this screen.
NO	This field displays the index number of an entry. The maximum number of user account entries is 512.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Time Created	This field displays when the account was created (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.

Table 2 Account Log

FIELD	DESCRIPTION
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.
Charge	This field displays the total cost of the subscriber's account.
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **UN-Used**. This field displays **Finished** when a subscriber uses up the time allocated to an account.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.

11.5 Current Users

The **Current Users** screen displays a list of subscribers currently logged on to the ZyAIR for Internet access.

Click **SYSTEM STATUS** and **Current Users** to display the screen as shown. Click a column heading to sort the entries if applicable.

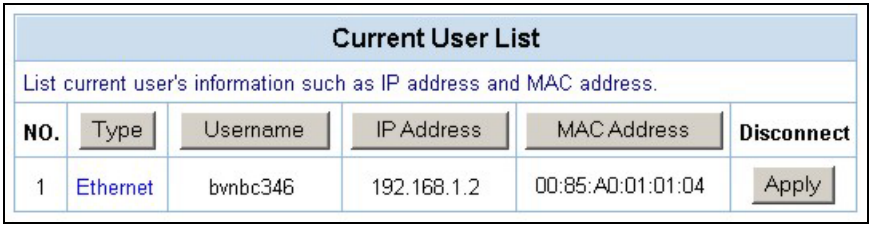


Figure 11-3 Current User List

The following table describes the labels in this screen.

Table 11-3 Current User List

LABEL	DESCRIPTION
No	This field displays the index number of the entry.
Username	This field displays the user name of an account.
IP Address	This field displays the IP address of a subscriber's computer.
MAC Address	This field displays the MAC address of the computer that is logged in using the account.
Disconnect	Click **Apply** to terminate the connection to the selected subscriber.

11.6 DHCP Clients

The DHCP client table shows current DHCP client information of all network clients using the DHCP server on the ZyAIR.

Click **SYSTEM STATUS** and **DHCP** to display the screen as shown.

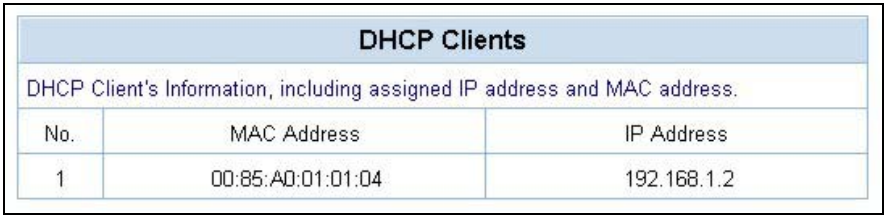


Figure 11-4 DHCP Clients

The following table describes the labels in this screen.

Table 11-4 DHCP Clients

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the client computer. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal characters). 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.
IP Address	This field displays the IP address assigned to the client computer.

11.7 Session List

To display a list of incoming and outgoing packet information, click **SYSTEM STATUS** and **Session List**.

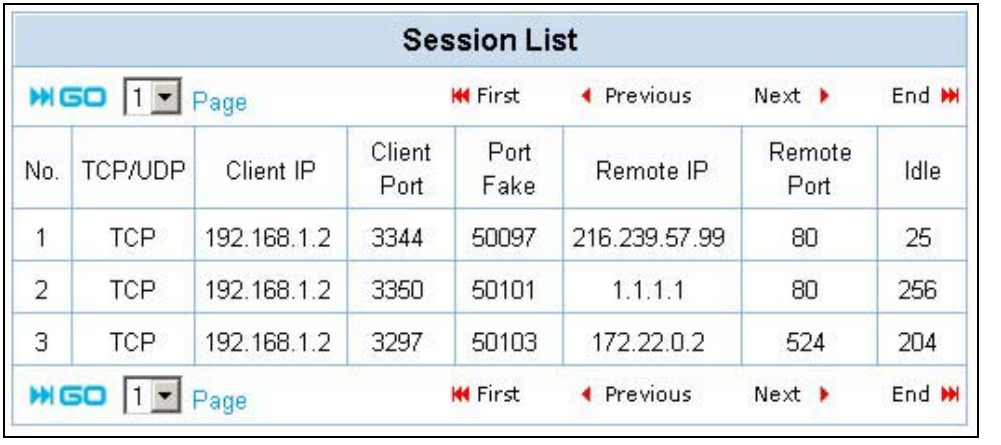


Figure 11-5 Session List

The following table describes the fields in this screen.

Table 11-5 Session List

LABEL	DESCRIPTION
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.
No	This field displays the index number of an entry.
TCP/UDP	This field displays the type of traffic (**TCP** or **UDP**).
IP Client	This field displays the IP address of the client computer.
Port Client	This field displays the port number through which the client computer transmits the traffic.
Port Fake	This field displays the NAT port to and from which the ZyAIR maps the session's traffic.

Table 11-5 Session List

LABEL	DESCRIPTION
Remote Port	This field displays the port number of a remote device the client computer accesses.
Idle	This field displays how many seconds are left before the session times out if there is no more traffic. The ZyAIR automatically times out idle TCP sessions after 5 minutes (300 seconds). The ZyAIR automatically times out idle UDP sessions after 1 minute (60 seconds).

Chapter 12
Configuration, Firmware and Accounting Log Maintenance

This chapter shows you how to upgrade the firmware and configuration file and back up configuration files and accounting logs.

12.1 Filename Conventions

The configuration file contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. Once you have customized the settings of the ZyAIR, they can be saved back to your computer under a filename of your choosing.

It is recommended to use the ".bin" file extension for the firmware file and ".rom" for the configuration file for management purposes.

Visit www.zyxel.com to download the latest version of firmware for your ZyAIR.

12.2 Firmware Upgrade

There are two ways to upgrade firmware to the ZyAIR: manually or scheduled.

To manually upgrade the firmware, you have to download the latest firmware first from www.zyxel.com and then upload it to the ZyAIR.

With scheduled firmware upgraded, you need to set up a TFTP server where the ZyAIR can automatically download the latest firmware at the specified time.

12.2.1 Manual Firmware Upgrade

Follow the steps below to upload the firmware using the web configurator.

Step 1. Click **SYSTEM TOOLS** and then **Firmware Upgrade** to display the screen as shown.

Figure 12-1 Firmware Upgrade

Step 2. Specify the name of the firmware file in the **File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The firmware must be a binary file and should have a .bin extension.

Step 3. When the file transfer is completed successfully, a restart message displays and the ZyAIR automatically restarts.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

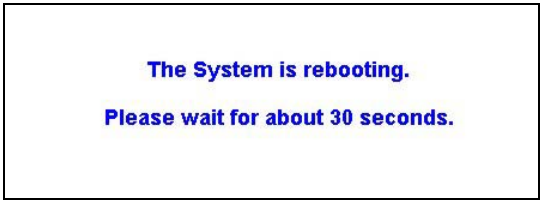


Figure 12-2 System Restart

Step 4. After the ZyAIR finishes restarting, access the web configurator again. Check the firmware version number in the **System** screen.

When the ZyAIR restarts, all connections terminate. Subscribers need to log in again.

12.2.2 Scheduled Firmware Upgrade

Click **SYSTEM TOOLS** and then **Scheduled Firmware Upgrade** to display the screen as shown.

Configure the screen to automatically download the latest firmware from a TFTP server.

Make sure that the TFTP server has the firmware and synchronization check file before you configure for scheduled firmware upgrades.

Make sure that you check new features or functionality enhancements in new firmware releases before you put the firmware on the TFTP server.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

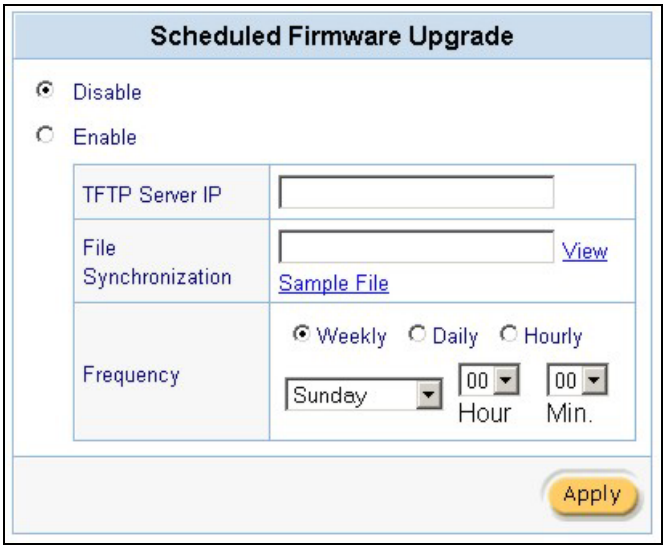


Figure 12-3 Scheduled Firmware Upgrade

When the ZyAIRs restart, all connections terminate. Subscribers need to log in again.

Table 12-1 Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Disable Enable	Select **Disable** or **Enable** to turn the scheduled firmware upgrade function on or off (disabled by default).
TFTP Server IP	Type the IP address of the TFTP server from which the ZyAIR can download new firmware files.
File Synchronization	A synchronization check file is a .txt file containing the latest firmware filename and version number on the TFTP server. Enter the name of the check file.
View Sample File	Click **View Sample File** to view an example synchronization check file (see *Figure 12-4*).

Table 12-1 Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Frequency	Set how often (**Weekly**, **Daily** or **Hourly**) you want to have the ZyAIR check for new firmware and upgrade to new firmware if available (default **Weekly**). Then select the day (applies only when you select **Weekly**), the hour (applies when you select **Daily** or **Hourly**) and the minute that you want the ZyAIR to do the check and upload.
Apply	Click **Apply** to save the changes.

The following figure shows an example of a check file's content.

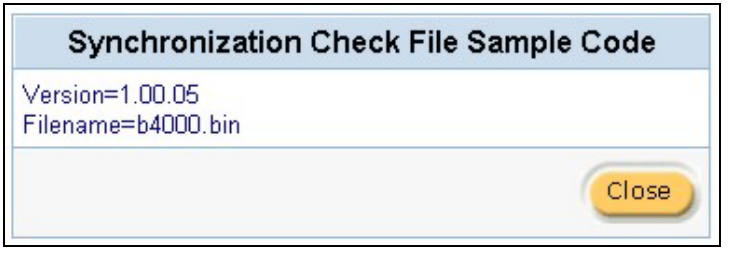


Figure 12-4 Synchronization Check File Example

12.3 Configuration File Maintenance

You can use the web configurator to perform configuration file backup and restore.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR DEVICE.

12.3.1 Backup Configuration

Backup is highly recommended once your ZyAIR is functioning properly.

Step 1. Click **SYSTEM TOOLS** and **Backup/Restore**. A screen displays as shown next.

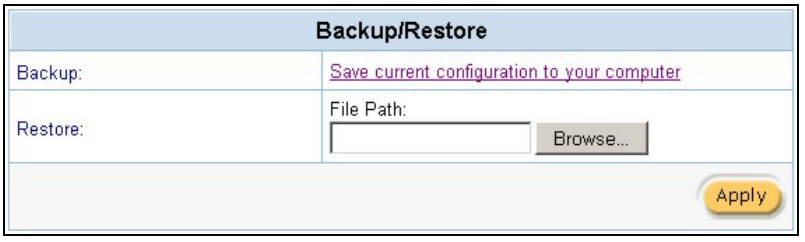


Figure 12-5 Backup/Restore

Step 2. Click S**ave current configuration to your computer**. A **File Download** window displays (an example is shown next).

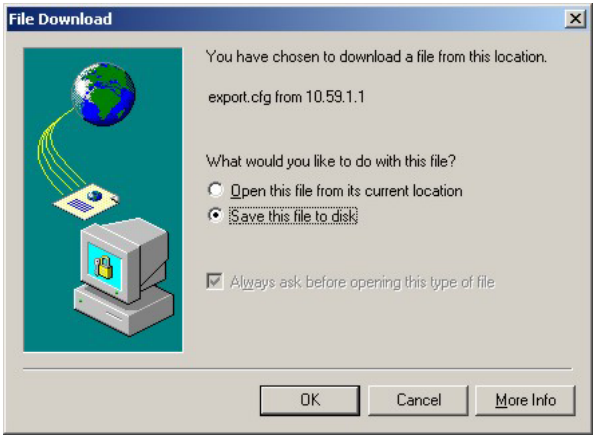


Figure 12-6 Configuration Backup: File Download Example

Step 3. Select the option to save the file to your computer and click **OK**. A **Save As** window displays.

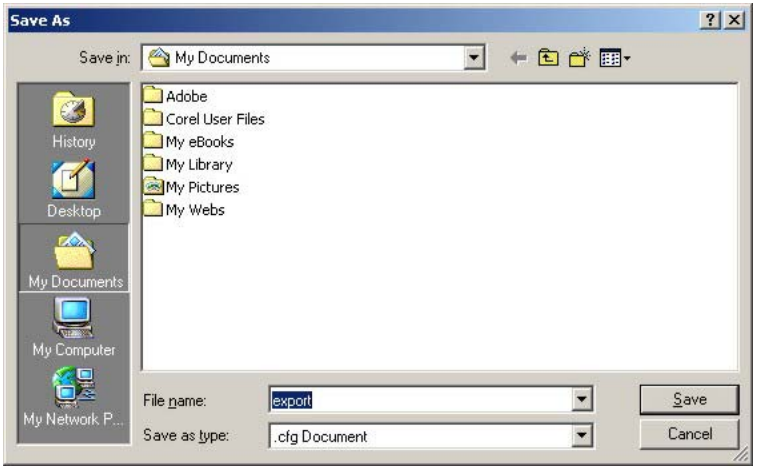


Figure 12-7 Configuration Backup: Save As

Step 4. Specify the file name and/or location and click **Save** to start the backup process.

12.3.2 Restore Configuration

This section shows you how to restore a previously saved configuration.

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.

Step 1. Click **SYSTEM TOOLS** and **Backup/Restore**. A screen displays as shown next.

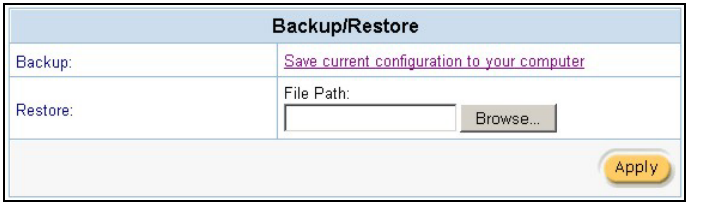


Figure 12-8 System Tools: Importing Configuration File

Step 2. Specify the location and filename of a configuration file in the **Restore** field or click **Browse**.

Step 3. Click **Apply** to start the configuration restore process. The ZyAIR automatically restarts after the restoration process is complete.

12.3.3 Backup Accounting Logs

Follow the steps below to back up accounting logs to a computer.

Step 1. In the web configurator, click **SYSTEM TOOLS** and **Backup Accounting Logs** to displays a screen as shown next.

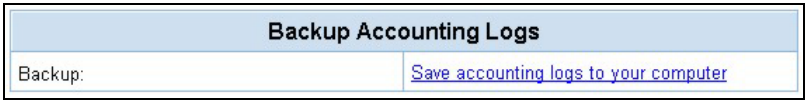


Figure 12-9 Backup Accounting Logs

Step 2. Click **Save accounting logs to your computer**. A **File Download** window displays (an example is shown next).

Figure 12-10 Backup Accounting Logs: File Download

Step 3. Select **Save this file to disk** and click **OK**. A **Save As** window displays.

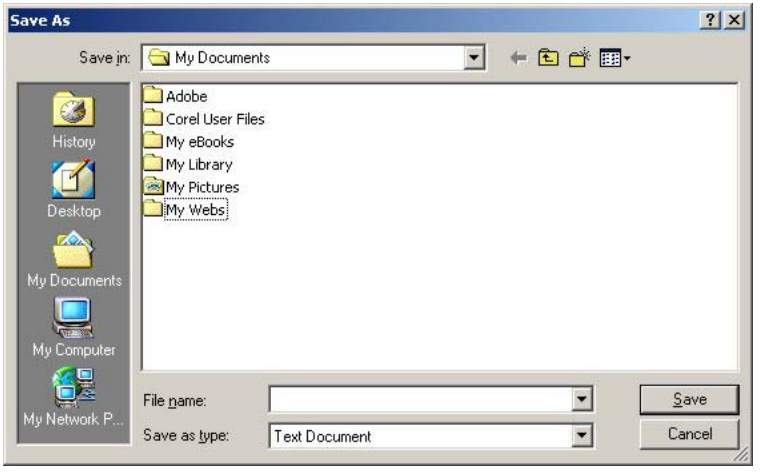


Figure 12-11 Backup Accounting Logs: Save As

Step 4. Specify the file name and/or location and click **Save** to start the backup process.

To view the accounting logs, open the log file using any text editor. The following figure shows an example.

```
[Account Log Profile]
NO.  Username Time Created        Login Time          Usage Time      Charge      Status
1    p3rix827 2003/7/2 15:24:17                      60 minutes      0.0         Un-used
2    6tj27235 2003/7/2 15:43:35                      2 hours         0.00        Un-used
3    rps3da49 2003/7/2 15:43:49                      3 hours         0.00        Un-used
4    m8r3a729 2003/7/2 16:55:29                      30 minutes      0.0         Un-used
5    yg8vqe59 2003/7/3 08:30:59   2003/7/3 08:33:13  1 hours         0.00        Finished
6    7m9mrj47 2003/7/3 08:31:47                      2 hours         0.00        Un-used
7    bvnbc346 2003/7/3 09:35:46   2003/7/3 09:37:20  3 hours         0.00        In-used
```

Figure 12-12 Backup Accounting Logs: Example

Chapter 13
SSL (Secure Socket Layer) Security

This chapter shows you how to setup and enable Secure Socket Layer (SSL) security on the ZyAIR.

13.1 About SSL

SSL (Secure Socket Layer) security is a standard Internet protocol for secure communications that uses a combination of certificate-based authentication and public-key encryption. SSL protects data transfer between the web configurator on the ZyAIR and the web browser on a connected computer.

With SSL security activated, data (such as user name and password) transferred between the ZyAIR and the computer is protected when you access the ZyAIR using a web browser that supports SSL.

13.2 Activating SSL Security for Management Connections

Follow the steps below to activate the SSL security for management connections to the ZyAIR.

Step 1. Click the **ADVANCED SETUP** tab and then **Server**. Select the **SSL Security** check box in the **Web Server** field.

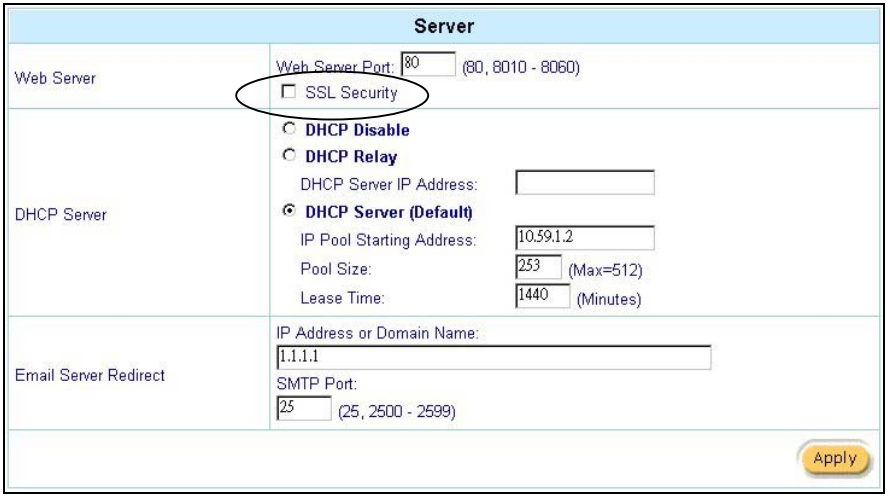


Figure 13-1 System Settings: Server Configuration: Enable SSL Security

Step 2. Click **Apply** to save the changes and restart the ZyAIR when prompted. See section *13.3* for details on how to install the SSL security certificate in order to access the web configurator through a secure connection.

13.3 Viewing and Installing the SSL Security Certificate

After you enable and activate the SSL security on the ZyAIR, you can access the web configurator through a secure connection.

Follow the steps below to view and install the default SSL security certificate on your computer.

Step 1. Access the ZyAIR. A **Security Alert** window displays. Click **OK** to continue and close the window.

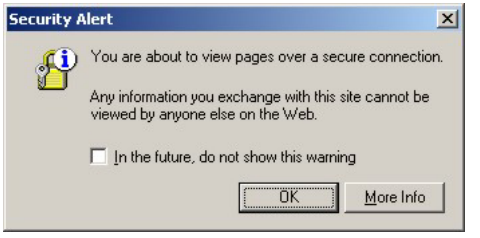


Figure 13-2 Install the SSL Security Certificate: First Security Alert

Step 2. A second **Security Alert** window displays.

Figure 13-3 Install the SSL Security Certificate: Second Security Alert

Step 3. Click **View Certificate** to display the **Certificate** window as shown.

Figure 13-4 Install the SSL Security Certificate: View Certificate

Step 4. Click **Install Certificate** to install the certificate to your computer. A **Certificate Import Wizard** window displays. Click **Next**.

Figure 13-5 Install the SSL Security Certificate: Certificate Import Wizard

Step 5. Accept the default or specify the location to store the certificate. Click **Next**.

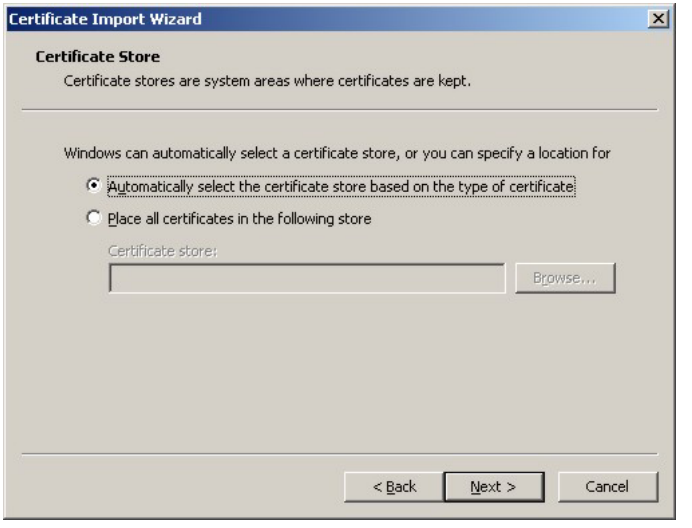


Figure 13-6 Certificate Import Wizard: Location

Step 6. Click **Finish** to import the certificate.

Figure 13-7 Certificate Import Wizard: Finish

Step 7. A **Root Certificate Store** window displays as shown. Click **Yes** to store the certificate to the computer.

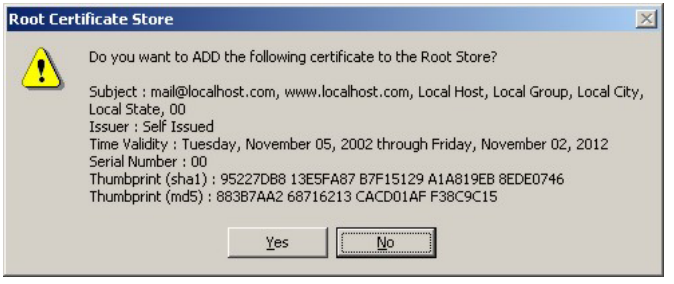


Figure 13-8 Root Certificate Store

Step 8. When the certificate is saved successfully, a **Certificate Import Wizard** window displays. Click **OK**.

Figure 13-9 Certificate Import Wizard

Step 9. A **Certificate** window displays the detail information.

Figure 13-10 Certificate: Details

Step 10. Click **OK** in the **Certificate** window to return to the **Security Alert** window as shown. Notice that the first item in the list changed to inform you that the certificate is from a trusted host. Click **OK** to proceed to the login screen in secure mode.

Figure 13-11 Security Alert: Trusted

13.4 Activating SSL Security for Subscriber Logins

Follow the steps below to activate the SSL security for subscriber login connections to the ZyAIR.

Step 1. Click the **ADVANCED SETUP** tab, **Authentication** and select **Enable** in the **SSL Login Page Security** field

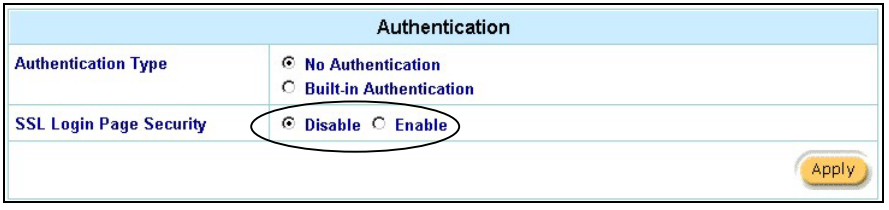


Figure 13-12 Authentication: Activate SSL Login

Step 2. Click **Apply** to save the changes and restart the ZyAIR when prompted.

13.5 SSL Certificate Download

You can register for a certificate from a CA (Certificate Authority). A CA issues digital certificates and guarantees the identity of the certificate owner.

Click **SYSTEM TOOLS**, **SSL Certificate Download** to open the **SSL Certificate Download** screen. Use the **SSL Certificate Download** screen to download a CA registered certificate from a computer connected to the ZyAIR.

You must save the certificate and private key files from the CA on a computer that is connected to the ZyAIR.

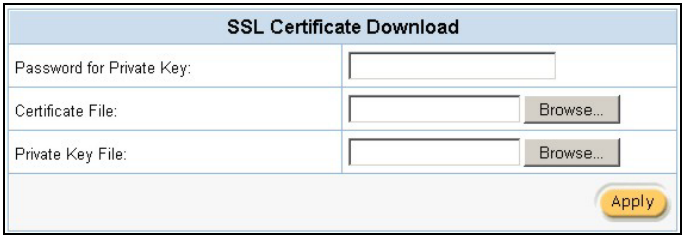


Figure 13-13 SSL Certificate Download

The following table describes the labels in this screen.

Table 13-1 SSL Certificate Download

LABEL	DESCRIPTION
Password for Private Key	Enter the private key password from the CA. Make sure you enter it exactly as the CA provides.
Certificate File	Specify the name and/or location of the file containing the certificate. Or click **Browse** to locate the file.
Private Key File	Specify the name and/or location of the file containing the private key, Or click **Browse** to locate the file.
Apply	Click **Apply** to transfer the certificate and private key files from the computer to the ZyAIR.

After you download the certificate files, click **Apply** to restart the ZyAIR.

See the chapter on general system setup for how to set the ZyAIR to use the certificate that you download.

Chapter 14
Troubleshooting

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

14.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

14.1.1 The Power LED

The **PWR** LED on the front panel does not light up.

Table 14-1 Troubleshooting Power LED

STEPS	CORRECTIVE ACTION
1	Check the connection from the ZyAIR to the power source. Make sure you are using the supplied power supply. Refer to the product specifications.
2	Make sure the power source is turned on and that the ZyAIR is receiving sufficient power.
3	If these steps fail to correct the problem, contact your local distributor for assistance.

14.1.2 The LAN Port LEDs

None of the LEDs for the LAN port(s) light up when connected to an Ethernet device.

Table 14-2 Troubleshooting LAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure the ZyAIR is turned on.
2	Verify that the attached device(s) is turned on and properly connected to the ZyAIR.
3	Verify that the Ethernet cable length does not exceed 100 meters.
4	Make sure the network adapters are working on the attached device(s).

14.1.3 The WAN Port LED

The LED for the WAN port does not light up when connected to an Ethernet device.

Table 14-3 Troubleshooting WAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure you connect your cable or DSL modem or router to this port using the Ethernet cable that came with your cable or DSL modem or router.
2	Verify that the attached device is turned on and properly connected to the ZyAIR.
3	Verify that the Ethernet cable length does not exceed 100 meters.

14.2 Web Configurator

I cannot access the web configurator.

Table 14-4 Troubleshooting the Web Configurator

STEPS	CORRECTIVE ACTION
1	Make sure you are using either Internet Explorer (version 4.0 and later) or Netscape Navigator (version 6.0 and later).
2	Make sure you are using the correct WAN or LAN IP address. The default LAN IP address is **192.168.1.1**.
3	Make sure you entered the correct username and password. The default administrator username is “admin” and the default password is “1234”. The username and password are case-sensitive. If you have forgotten the administrator user name and/or password, you must reset the ZyAIR back to the factory defaults using the reset button. Use a pointed object to press the reset button on the side panel to reset the ZyAIR. All of your custom configuration will be lost.
4	Ping the ZyAIR from your computer on the WAN or LAN. If you cannot ping the ZyAIR, check the IP addresses of the ZyAIR and your computer. Make sure that both IP addresses are in the same subnet.
5	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.) In Netscape, click **Edit**, **Preference**. Under **Advanced** category, click **Cache**. Click **Clear Memory Cache** and **Clear Disk Cache**. (Steps may vary depending on the version of your Internet browser.)

The web configurator does not display properly.

Table 14-5 Troubleshooting the Internet Browser Display

STEPS	CORRECTIVE ACTION
1	Make sure you are using either Internet Explorer (version 4.0 or above) or Netscape Navigator (6.0 or above). Make sure that your browser has JavaScript support enabled.
2	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.) In Netscape, click **Edit**, **Preference**. Under **Advanced** category, click **Cache**. Click **Clear Memory Cache** and **Clear Disk Cache**. (Steps may vary depending on the version of your Internet browser.)

14.3 Internet Access

A subscriber cannot connect to the Internet through the ZyAIR.

Table 14-6 Troubleshooting Internet Access

STEPS	CORRECTIVE ACTION
1	Check your Internet settings on your modem and/or router.
2	Make sure the subscriber enters the correct user name and password to log in to the ZyAIR. The user name and password are case sensitive.
3	Verify that the IP addresses and the subnet masks of the ZyAIR and the computers are on the same subnet.
4	Make sure the account is still valid.
5	Make sure there is no conflict in IP address assignment. Refer to the appendix.
7	For wireless clients, check that both the ZyAIR and wireless client(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

14.4 The Statement Printer

This section is applicable when you use an external statement printer.

I cannot print subscriber statements using the statement printer.

Table 14-7 Troubleshooting the Statement Printer

STEPS	CORRECTIVE ACTION
1	Make sure the statement printer is connected to a power source and is turned on.
2	Check that the statement printer is connected to the port labeled **DEVICE PORT**.
3	Make sure there is enough printing paper in the statement printer.
4	Make sure you set the ZyAIR to require authentication before allowing Internet access, see the Wizard Setup screens or the **Authentication** chapter.

Part V:

ADDITIONAL INFORMATION

This part provides contains background information on setting up your computer's IP address, IP address assignment conflicts, wireless LAN, PPPoE, PPTP, IP subnetting, subscriber login, and cable types and cable pin assignments. It also provides an index of key terms.

Appendix A
Setting up Your Computer's IP Address

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

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

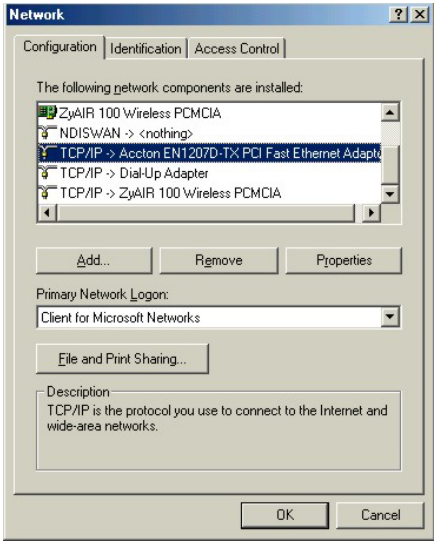
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

Windows 95/98/Me

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



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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

a. Click **Add**.

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

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

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

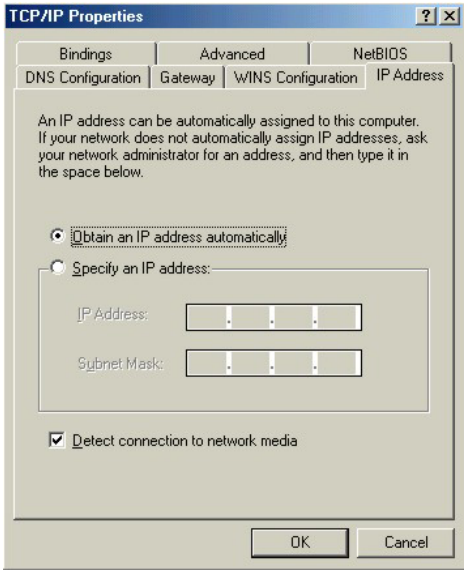
e. Restart your computer so the changes you made take effect.

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

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

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

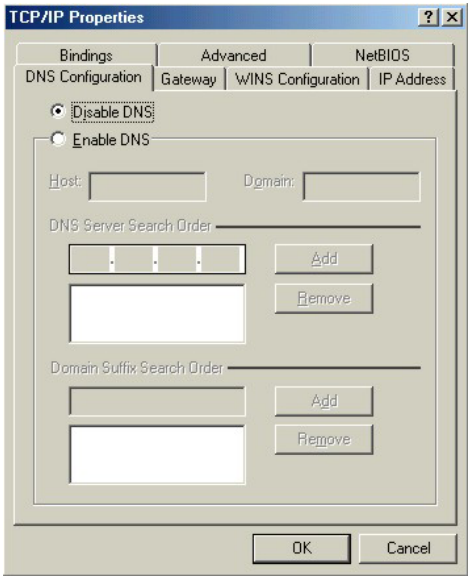
   -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



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

   -If you do not know your DNS information, select **Disable DNS**.

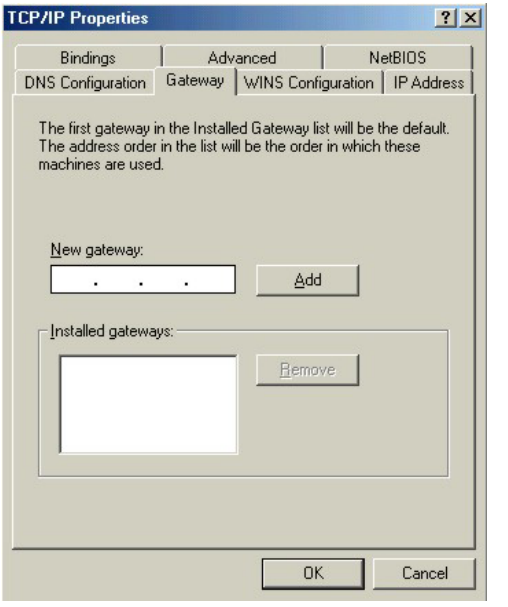
   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



3. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



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

Verifying Your Computer's IP Address

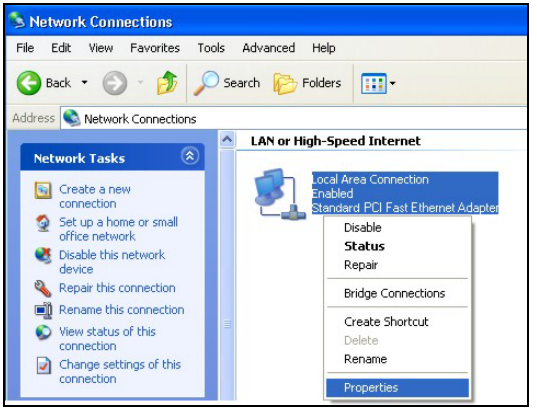
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

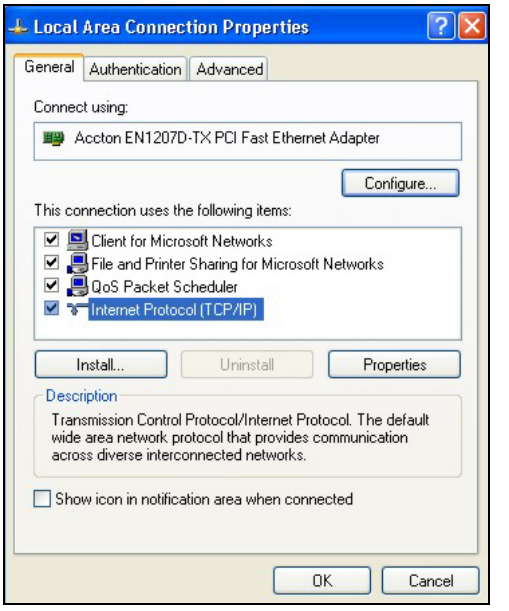
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

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

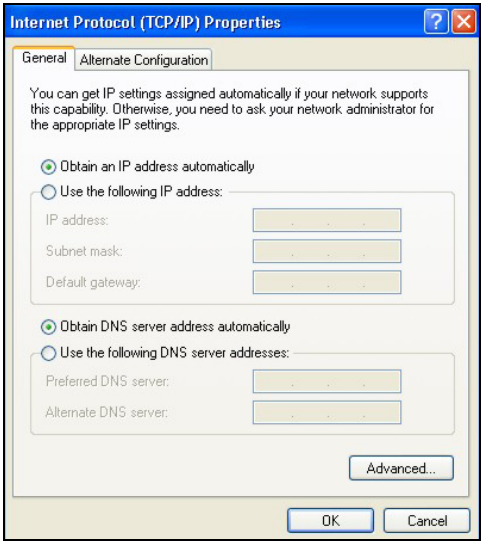


5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

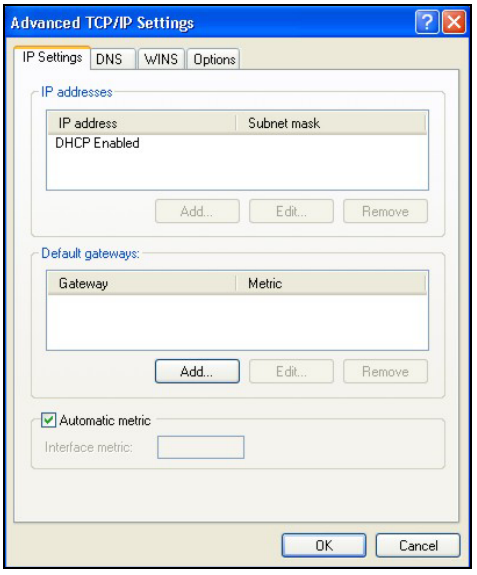
   -If you have a dynamic IP address click **Obtain an IP address automatically**.

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

   Click **Advanced**.



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



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

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

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

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

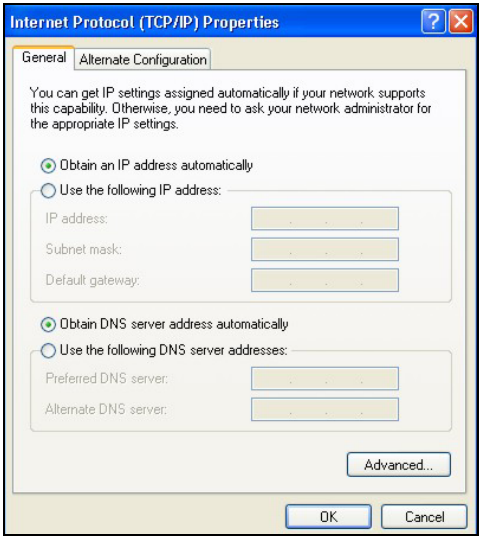
-Click **OK** when finished.

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

   -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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



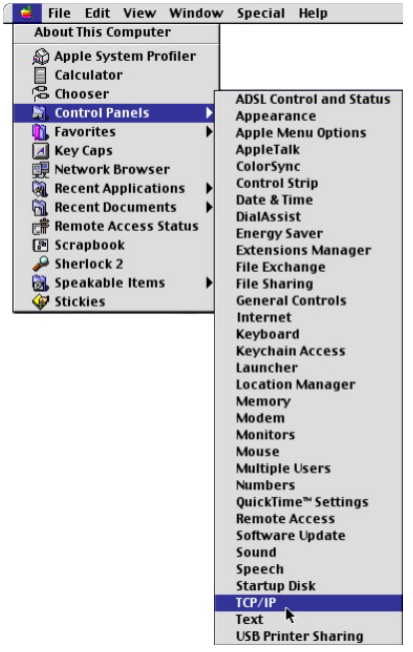
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

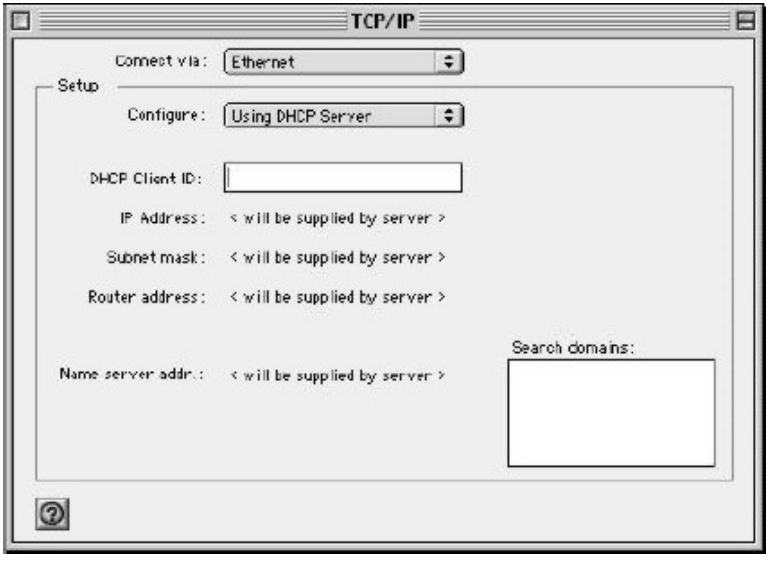
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



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

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your ZyAIR in the **Router address** box.

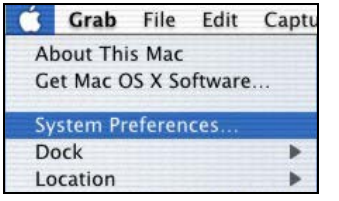
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

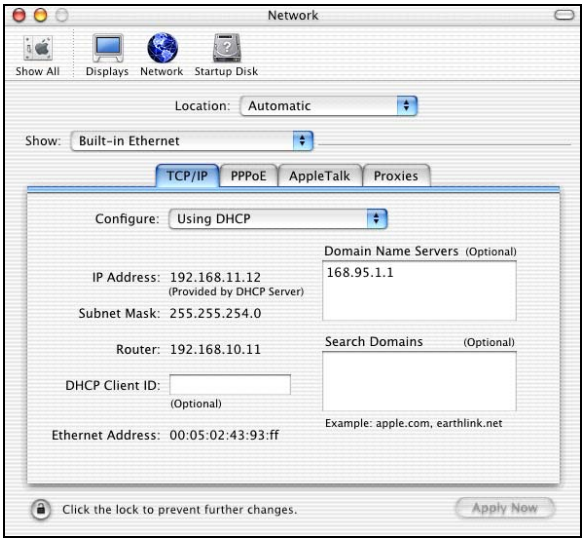
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

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



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



3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.
4. For statically assigned settings, do the following:
   -From the **Configure** box, select **Manually**.
   -Type your IP address in the **IP Address** box.
   -Type your subnet mask in the **Subnet mask** box.
   -Type the IP address of your ZyAIR in the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

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

Appendix B
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyAIR is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyAIR is using a WAN IP address that is the same as the IP address of a computer on the LAN.

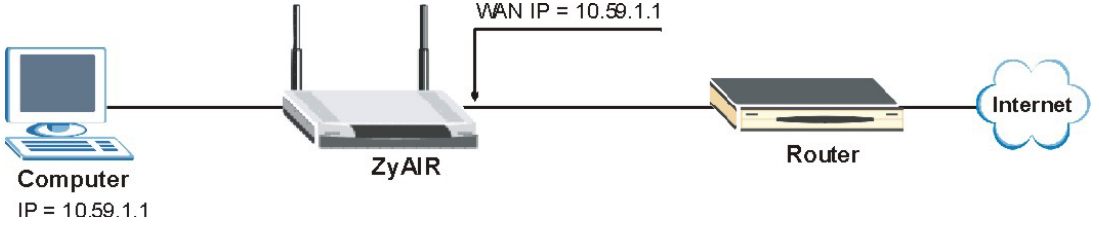


Diagram B-1 IP Address Conflicts: Case A

You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case B: The ZyAIR LAN IP address conflicts with the DHCP client IP address

In the following figure, the ZyAIR is acting as a DHCP server. The ZyAIR assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

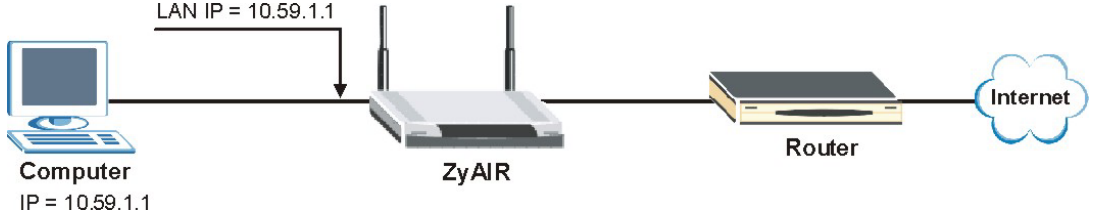


Diagram B-2 IP Address Conflicts: Case B

To solve this problem, make sure the ZyAIR LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyAIR.

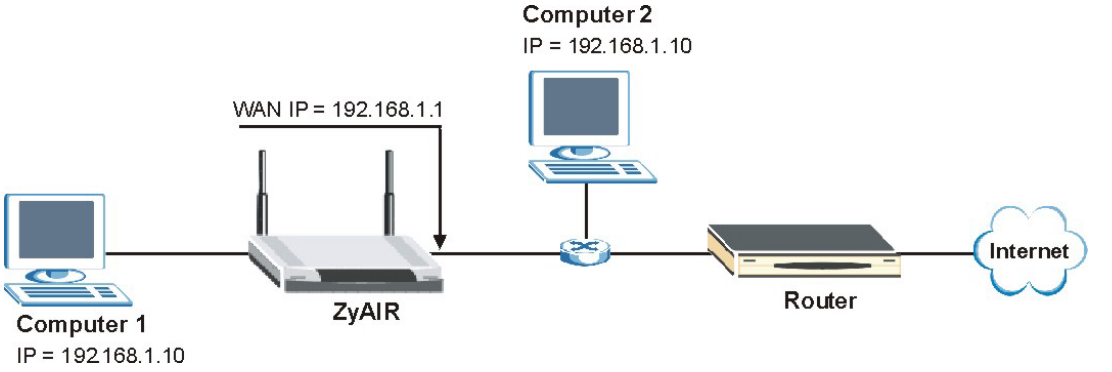


Diagram B-3 IP Address Conflicts: Case C

You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyAIR allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyAIR DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

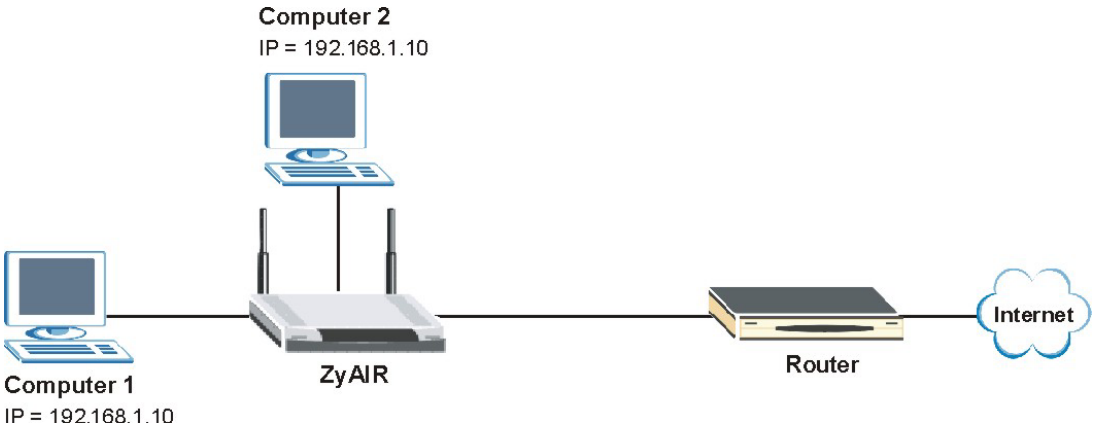


Diagram B-4 IP Address Conflicts: Case D

This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

Appendix C
Wireless LAN and IEEE 802.11

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

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

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

IEEE 802.11

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

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

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

Ad-hoc Wireless LAN Configuration

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

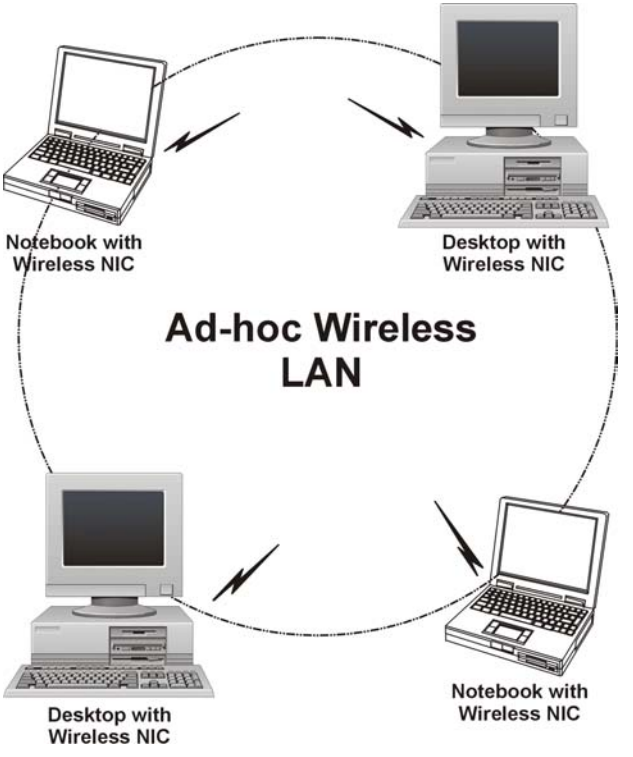


Diagram C-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

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

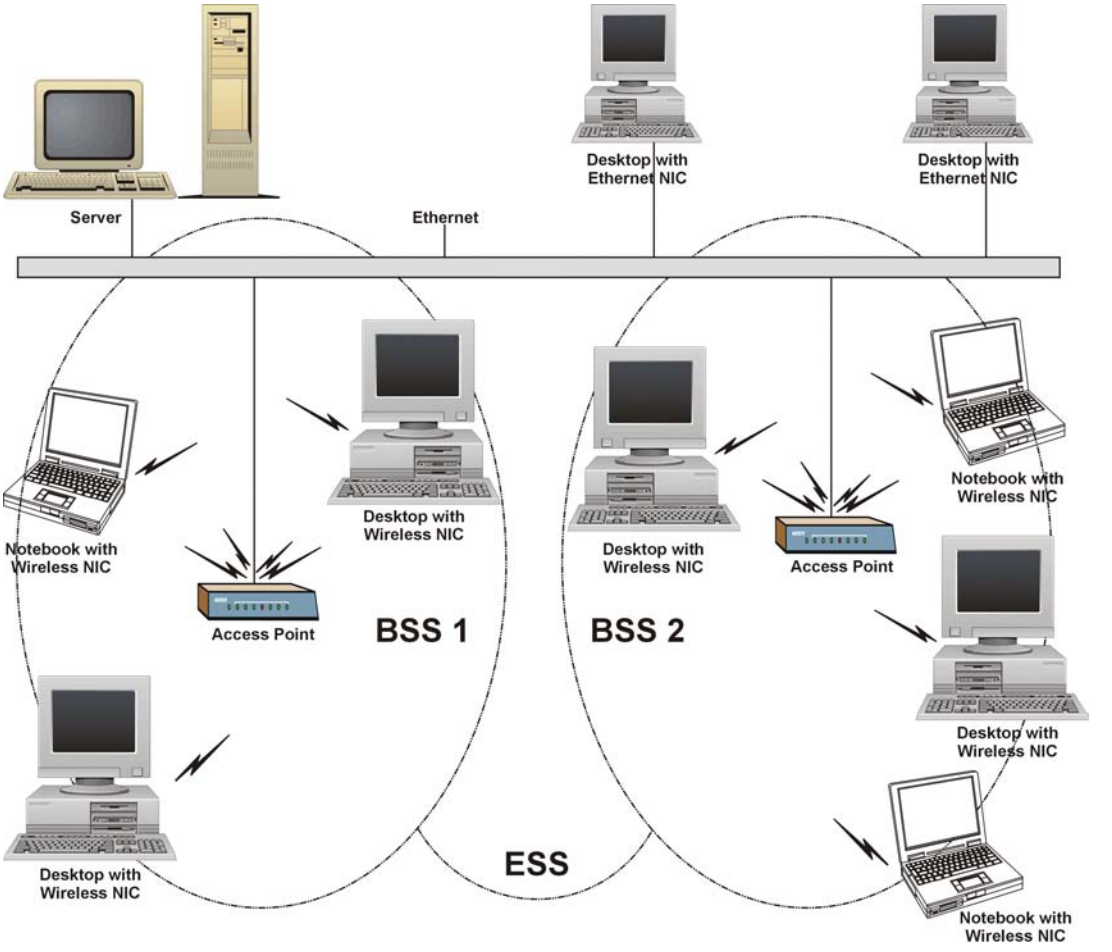


Diagram C-2 ESS Provides Campus-Wide Coverage

Appendix D
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 E
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.

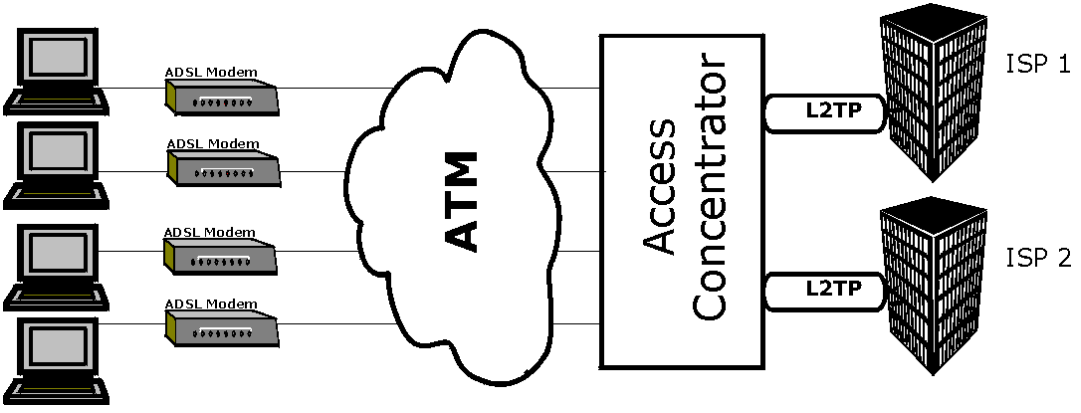


Diagram E-1 Single-PC per Modem Hardware Configuration

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.

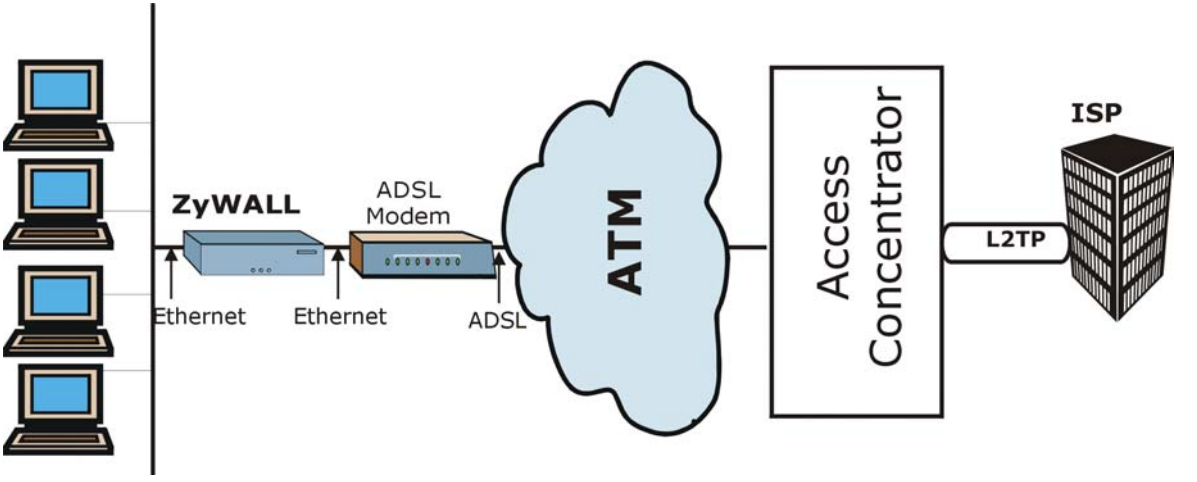


Diagram E-2 ZyAIR as a PPPoE Client

Appendix F
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.

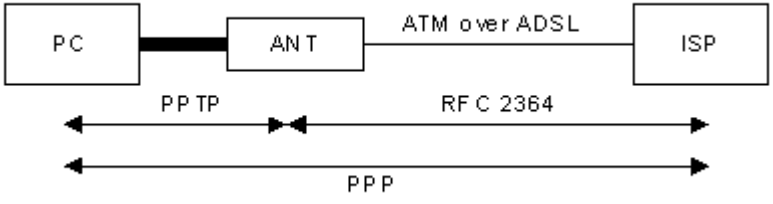


Diagram F-1 Transport PPP frames over Ethernet

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 F-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.

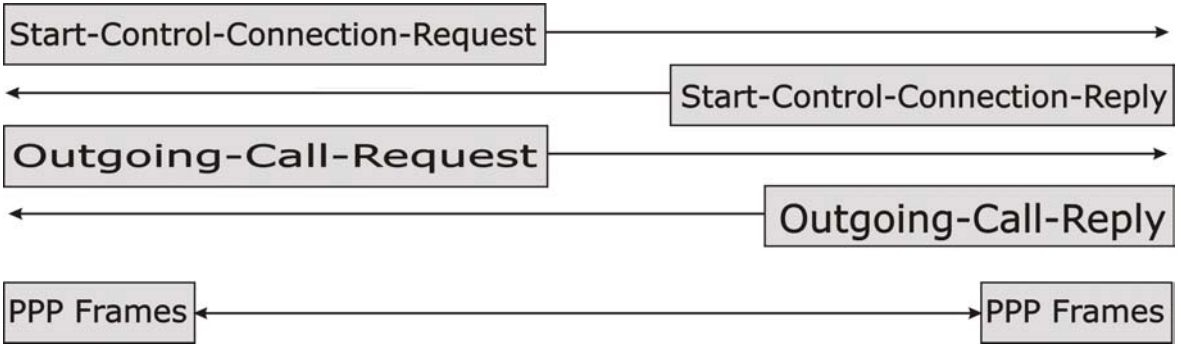


Diagram F-3 Example Message Exchange between PC and an ANT

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 G
IP Subnetting

IP Addressing

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

IP Classes

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

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

Chart G-1 Classes of IP Addresses

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

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

Therefore:

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

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

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

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

Chart G-2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**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 G-3 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

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

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

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

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

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

Chart G-4 Alternative Subnet Mask Notation

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

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

Example: Two Subnets

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

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

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

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

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

Chart G-5 Subnet 1

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

Chart G-6 Subnet 2

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

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

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

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

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**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 G-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 G-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 G-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 G-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 G-11 Eight Subnets

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

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

Chart G-12 Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

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

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

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

Chart G-13 Class B Subnet Planning

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

Chart G-13 Class B Subnet Planning

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

Appendix H
Subscriber Login

To log in as a subscriber, enter a web site address such as www.zyxel.com in a web browser.

If user authentication is activated, the login screen displays prompting you to enter the user name and password. A standard subscriber login screen is shown in the figure below.

Diagram H-1 Subscriber Login Screen

Enter a user name and password and click **Enter**. Depending on the settings in the ZyAIR, either the specified web page or an advertisement web page displays. A **Time Window** screen also displays showing the amount of time remaining on the account for Internet access.

Diagram H-2 Subscriber Login: Time Windows

Appendix I
Cable Types and Cable Pin Assignments

RJ-45 Ethernet Port

The following table describes the types of network cable used for the different connection speeds.

Make sure the Ethernet cable length between connections does not exceed 100 meters (328 feet).

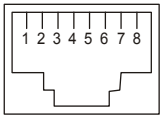
Chart I-1Network Cable Types

SPEED	NETWORK CABLE TYPE
10 Base-TX	100Ω 2-pair UTP/STP Category 3, 4 or 5
100 Base-TX	100Ω 2-pair UTP/STP Category 5

The WAN Port

The following table describes the Ethernet cable pin assignments for the WAN port.

Chart I-2 WAN Port Cable Ping Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
	1	Output Transmit Data +	TD+
	2	Output Transmit Data -	TD-
	3	Input Transmit Data +	RD+
	4	Unused	N/U
	5	Unused	N/U
	6	Input Transmit Data -	RD-
	7	Unused	N/U
	8	Unused	N/U

Make sure that the Ethernet cable connection between the ZyAIR and the hub or router conforms to the following pin assignments.

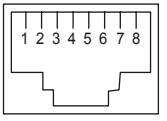
Chart I-3 WAN Port Cable Pin Assignments

ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)			ZYAIR	
1	RD+	———	1	TD+
2	RD-	———	2	TD-
3	TD+	———	3	RD+
6	TD-	———	6	RD-

The LAN Port

The following table describes the Ethernet cable pin assignments for the LAN port.

Chart I-4 LAN Port Cable Pin Assignments



PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
1	Input Transmit Data +	RD+
2	Input Transmit Data -	RD-
3	Output Transmit Data +	TD+
4	Unused	N/U
5	Unused	N/U
6	Output Transmit Data -	TD-
7	Unused	N/U
8	Unused	N/U

Make sure that the Ethernet cable connection between the ZyAIR and a computer or switch uplink port conforms to the following pin assignments.

Chart I-5 LAN Port Cable Pin Assignments

ETHERNET DEVICE (COMPUTER/ UPLINK PORT)			ZYAIR	
1	TD+	———	1	RD+
2	TD-	———	2	RD-
3	RD+	———	3	TD+
6	RD-	———	6	TD-

The DEVICE Port

The following table describes the printer cable pin assignments that the ZyAIR's device port uses with the exclusive printer.

Chart I-6 Device Port Cable Pin Assignments

ZYAIR DB25		EXCLUSIVE PRINTER RJ-11
2	———	2
3	———	3
7	———	4
5	———	5

Appendix J
Index