

ZyAIR B-2000 v.2

Broadband Wireless Sharing Router

Quick Installation Guide

Version 3.50

July 2003



Table of Contents

1	<i>Introducing the ZyAIR</i>	4
2	<i>Hardware Connections</i>	5
2.1	Side Panel and Connections	5
2.2	The Front Panel	5
3	<i>Setting Up Your Computer's IP Address</i>	7
3.1	Windows 2000/NT/XP	8
3.2	Checking/Updating Your Computer's IP Address	9
3.3	Testing the Connection to the ZyAIR.....	9
4	<i>Internet Access Setup Using the Web Configurator Wizard</i>	10
4.1	Accessing the ZyAIR via the Web Configurator	10
4.2	Common Screen Command Buttons.....	12
4.3	Configuring the ZyAIR Using the Wizard.....	12
4.4	Test Your Internet Connection	15
5	<i>Key Features</i>	15
5.1	Wireless LAN Overview	15
5.2	Configuring Wireless LAN	16
5.3	Configuring Roaming.....	18
5.4	Configuring IEEE 802.1x Authentication	19
5.5	Local User Database and RADIUS Overview	22
5.6	Enabling Firewall	22
5.7	Define Content Filtering.....	24
5.8	Configuring Firewall Services	26
5.9	Remote Management Overview	28
5.10	UPnP Overview	29
5.11	Configuring UPnP	29
6	<i>Hardware Installation</i>	30
6.1	Attaching Antennas	30
6.2	Hardware Mounting Installation	31
7	<i>Troubleshooting</i>	34

1 Introducing the ZyAIR

The ZyAIR B-2000 v.2 is a broadband sharing gateway with a built-in wireless LAN access point and four-port switch that makes it easy for people to set up a small home/office network and share Internet access via a broadband (cable/DSL) modem. Key features of the ZyAIR include 802.1x wireless LAN security, Firewall, remote management and UPnP. See your *User's Guide* for more details on all ZyAIR features.

You should have an Internet account already set up and have been given most of the following information.

INTERNET ACCOUNT CHECKLIST	
Your device's WAN IP Address (if given): _____	
Encapsulation:	
<input type="checkbox"/> Ethernet	Service Type: _____ Login Server IP Address: _____ User Name: _____ Password: _____
<input type="checkbox"/> PPTP	User Name: _____ Password: _____ Your WAN IP Address: _____ PPTP Server IP Address: _____ Connection ID (if required): _____
<input type="checkbox"/> PPPoE	(PPPoE) Service Name: _____ User Name: _____ Password: _____

2 Hardware Connections

2.1 Side Panel and Connections



LABEL	DESCRIPTION AND FUNCTION
1. LAN	Use an Ethernet cable to connect at least one computer for initial ZyAIR configuration. These ports are auto-negotiating (can connect at 10 or 100Mbps) and auto-crossover (automatically adjust to the type of Ethernet cable you use (straight-through or crossover)).
2. WAN	Connect your cable/DSL modem to this port with the cable that came with your modem.
3. POWER	Connect the end of the included power adaptor (use only this adaptor) to this power socket.
After you've made the connections, connect the power cable to a power supply and look at the front panel LEDs.	
RESET	You only need to use this button if you've forgotten the ZyAIR's password. It returns the ZyAIR to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc. see your <i>User's Guide</i> for details).

2.2 The Front Panel

The **PWR** LED turns steady on when the power cord is connected. The **SYS** LED blinks while performing system testing and then turns steady on if the testing is successful. The link LED and the ZyAIR LED turn steady on while the wireless card on the ZyAIR is working. The **LAN** and **WAN** LEDs turn on, if they are properly connected. Refer to the *User's Guide* for more detailed LED descriptions.



Table 1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
ZyAIR	Blue	On	The ZyAIR is ready, but is not sending/receiving data through the wireless LAN.
		Blinking (Breathing)	The ZyAIR is sending/receiving data through the wireless LAN.

Table 1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4	Green	On	The ZyAIR has a successful 10Mbps Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have a 10Mbps Ethernet connection.
	Orange	On	The ZyAIR has a successful 100Mbps Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have a 100Mbps Ethernet connection.
WAN	Green	On	The ZyAIR has a successful 10Mbps WAN connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 10Mbps WAN connection.
	Orange	On	The ZyAIR has a successful 100Mbps WAN connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have a 100Mbps WAN connection.
SYS	Green	On	The ZyAIR is functioning properly.
		Off	The ZyAIR is not ready or has malfunctioned.
	Red	Blinking	The ZyAIR is rebooting.
PWR	Green	On	The ZyAIR is receiving power.
		Off	The ZyAIR is not receiving power.

3 Setting Up Your Computer's IP Address

Skip this section if your computer is already set up to accept a dynamic IP address. This is the default for most new computers.

The ZyAIR is already set up to assign your computer an IP address. Use this section to set up your computer to receive an IP address or assign it a static IP address in the 192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0. This is necessary to ensure that your computer can communicate with your ZyAIR.

Your computer must have a network card and TCP/IP installed. TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems. Refer to the *Setting Up Your Computer's IP Address* appendix in the *User's Guide* for configuring the IP address in other operating systems.

3.1 Windows 2000/NT/XP

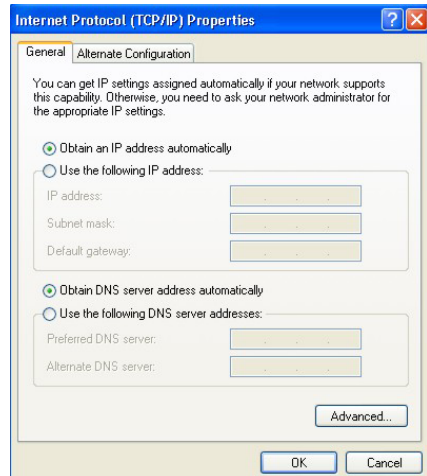
1. In Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.
2. In Windows XP, click **Network Connections**.
In Windows 2000/NT, click **Network and Dial-up Connections**.
3. Right-click **Local Area Connection** and then click **Properties**.
4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

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

-To have your computer accept a dynamic IP address, click **Obtain an IP address automatically**.

-If you want a static IP address, click **Use the following IP Address** and fill in the **IP address** (use one between 192.168.1.2 and 192.168.1.254), **Subnet mask** (255.255.255.0), and **Default gateway** (192.168.1.1) fields.

Click **Advanced**.



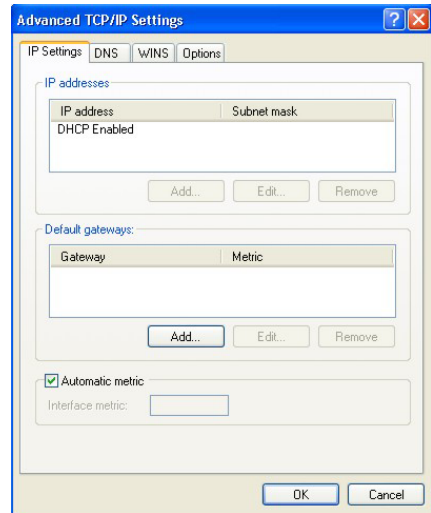
6. Remove any previously installed gateways in the **IP Settings** tab and click **OK** to go back to the **Internet Protocol TCP/IP Properties** screen.

7. 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.



Refer to your *User's Guide* for detailed IP address configuration for other Windows and Macintosh computer operating systems.

3.2 Checking/Updating Your Computer's IP Address

1. In the computer, click **Start, (All) Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer's static IP address is in the correct subnet (in the range between 192.168.1.2 and 192.168.1.254 if using the default ZyAIR LAN IP address). Alternatively, to have the ZyAIR assign your computer a new IP address (from the IP pool), make sure your ZyAIR is turned on, type "ipconfig/renew" and then press **ENTER**.

3.3 Testing the Connection to the ZyAIR

The default IP address of the ZyAIR is 192.168.1.1.

1. Click **Start, (All) Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ping" followed by a space and the IP address of the ZyAIR.

3. Press **ENTER** and the reply messages displays.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

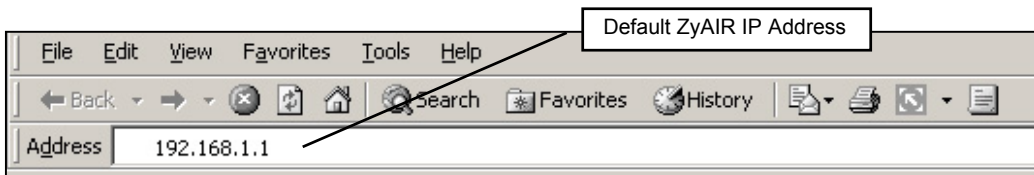
Your computer can now communicate with the ZyAIR using the LAN port.

4 Internet Access Setup Using the Web Configurator Wizard

The *Compact Guide* shows you how to use the web configurator Wizard and introduces the ZyAIR's key features. See your *User's Guide* for configuration details and background information on all ZyAIR features using the SMT (System Management Terminal) and web configurator.

4.1 Accessing the ZyAIR via the Web Configurator

1. Launch your web browser. Enter "192.168.1.1" as the web site address.



2. The default password (“1234”) is already in the password field (in non-readable format). Click **Login** to proceed to a screen asking you to change your password. Click **Reset** to revert to the default password in the password field.



3. It is highly recommended you change the default password! Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the **MAIN MENU** screen if you do not want to change the password now.



4. You should now see the web configurator **MAIN MENU** screen.



4.2 Common Screen Command Buttons

The following table shows common command buttons found on many web configurator screens.

Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

4.3 Configuring the ZyAIR Using the Wizard

The wizard consists of a series of screens to help you configure your ZyAIR for wireless stations to access your wired LAN and set up Internet access. Refer to your *User's Guide* for more background information.

1. Click **WIZARD SETUP** in the main menu to display the first wizard screen. Refer to your *User's Guide* for more background information on each field.

WIZARD

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

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

System Name:

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

Domain Name:

System Name is a unique name to identify the ZyAIR in the Ethernet network. Enter a descriptive name.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. Click **Next** to continue.

2. Use the second wizard screen to set up the wireless LAN.

WIZARD

Wireless LAN Setup

ESSID

Choose Channel ID or

WEP Encryption

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
 (Select one WEP key as an active key to encrypt wireless data transmission.)

ASCII Hex

Key 1

Key 2

Key 3

Key 4

ESSID is a unique name to identify the ZyAIR in the wireless LAN. Enter a descriptive name.

The range of radio frequencies used by IEEE 802.11b wireless devices is called a channel.

Click **Scan** to have the ZyAIR automatically select a channel. The selected channel automatically appears in the **Channel ID** field.

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select either **64-bit** or **128-bit** from the **WEP Encryption** drop-down list box to activate WEP encryption. Select **Disable** to turn off WEP data encryption.

Select **ASCII** or **HEX** WEP key input method and then follow the on-screen instructions to set up the WEP keys. Click **Next** to continue.

The wireless stations and ZyAIR must use the same ESSID, channel ID and WEP encryption key (if WEP is enabled) for wireless communication.

3. The third wizard screen has three variations depending on what encapsulation type you use. Use the information in the *Internet Account Checklist* table and the online help to fill in the fields. Click **Next** in each screen to continue.

WIZARD

ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard
User Name	N/A
Password	N/A
Login Server IP Address	N/A

Back Next

Choose **Ethernet** when the WAN port is used as a regular Ethernet. Choose from **Standard** or a RoadRunner version. You'll need **User Name**, **Password** and **Login Server IP Address** for some Roadrunner versions.

Point-to-Point Protocol over Ethernet (**PPPoE**) also functions as a dial-up connection. Therefore you'll also need a username and password and possibly the PPPoE service name. Your ISP will give you all needed information.

Choose **PPTP** if your service provider uses a DSL terminator with PPTP login. The ZyAIR must have a static IP address in this case. You'll also need a login name, associated password, the DSL terminator IP address and possibly a connection ID.

Click **Next** to continue.

4. Fill in the fields in the last wizard configuration screen.

WIZARD

WAN IP Address Assignment

Get automatically from ISP (Default)
 Use fixed IP address

My WAN IP Address
 My WAN IP Subnet Mask
 Remote IP Address

DNS Server Address Assignment

Get automatically from ISP (Default)
 Use fixed IP Address - DNS Server IP Address

Primary DNS Server
 Secondary DNS Server

WAN MAC Address

Factory default
 Spoof this computer's MAC Address - IP Address

Back Next

WAN IP Address Assignment
 Select **Get automatically from ISP** to have the ZyAIR obtain an IP address automatically from the ISP. Select **Use fixed IP address** to give the ZyAIR a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable.

DNS Server Assignment
 Select **Get automatically from ISP** if your ISP does not give you DNS server addresses.

If you selected the **Use fixed IP address – Primary/Secondary DNS Server** option, enter the provided DNS addresses in these fields.

WAN MAC Address

The WAN MAC address field allows you to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select **Factory Default** to use the factory assigned default MAC address. Alternatively, select **Spoof this Computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC address you are cloning

5. In the final screen, click **Finish** and change the wireless parameter settings in the wireless stations to match those of the ZyAIR. Refer to the user's guide for your wireless adapter.

4.4 Test Your Internet Connection

Launch your web browser and navigate to www.zyxel.com. You don't need a dial-up program such as Dial Up Networking. Internet access is just the beginning. Refer to the *User's Guide* for more detailed information on the complete range of ZyAIR features.

5 Key Features

This section shows you how to configure some of the advanced features of the ZyAIR.

Refer to your *User's Guide* for more information on ZyAIR configurations.

5.1 Wireless LAN Overview

This section introduces the wireless LAN and some basic configurations. A wireless LAN can be as simple as two computers with wireless adapters communicating in a peer-to-peer network or as complex as a

number of computers with wireless adapters communicating through access points (APs) which bridge network traffic to the wired LAN.

5.2 Configuring Wireless LAN

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

WIRELESS LAN

Wireless	MAC Filter	Roaming	802.1x	Local User Database	RADIUS
----------	------------	---------	--------	---------------------	--------

Enable Wireless LAN

ESSID

Hide ESSID

Choose Channel ID or

RTS/CTS Threshold (0 ~ 2432)

Fragmentation Threshold (256 ~ 2432)

WEP Encryption

Authentication Method

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

ASCII **Hex**

Key 1

Key 2

Key 3

Key 4

Enable Intra-BSS Traffic

Enable Breathing LED

Number of Wireless Stations Allowed (1 ~ 32)

Output Power

Figure 1 Wireless LAN

The following table describes the fields in this screen.

Table 2 Wireless LAN

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
ESSID	ESSID (Extended Service Set ID) is a unique name to identify the ZyAIR in the wireless LAN. Enter a descriptive name.
Hide ESSID	Click this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
Choose Channel ID	Adjacent access points (APs) should use a channel different from what you selected to reduce interference. The wireless stations connected to the ZyAIR must use the same channel you selected.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.
RTS /CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432 .
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432 .
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	Select Auto , Open System or Shared Key from the drop-down list box.
Key 1 to Key 4	<p>If you chose 64-bit WEP in the WEP Encryption field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose 128-bit WEP in the WEP Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.</p> <p>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>

Table 2 Wireless LAN

LABEL	DESCRIPTION
Enable Intra-BSS Traffic	<p>Select this check box to enable Intra-BSS Traffic.</p> <p>Intra-BSS traffic is traffic between wireless stations in the BSS. If two wireless stations connect to the Internet via the ZyAIR, then when Intra-BSS is enabled, both can access the wired network and communicate with each other. When Intra-BSS is disabled, both can still access the wired network but cannot communicate with each other</p>
Enable Breathing LED	<p>Select this check box to enable the Breathing LED, also known as the ZyAIR LED.</p> <p>The blue ZyAIR LED is on (dimmed) when the ZyAIR is on and blinks brightly (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.</p>
Number of Wireless Stations Allowed	<p>Use this field to set a maximum number of wireless stations that may connect to the ZyAIR. This may be necessary if for example, there is difficulty with channel assignment due to a high density of APs within a coverage area.</p> <p>Enter the number (from 1 to 32) of wireless stations allowed.</p>
Output Power	<p>Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference from other APs.</p> <p>The options are 11dBm (50mW), 13dBm (32mW), 15dBm (20mW) or 17dBm (12.6mW).</p>

5.3 Configuring Roaming

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

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

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

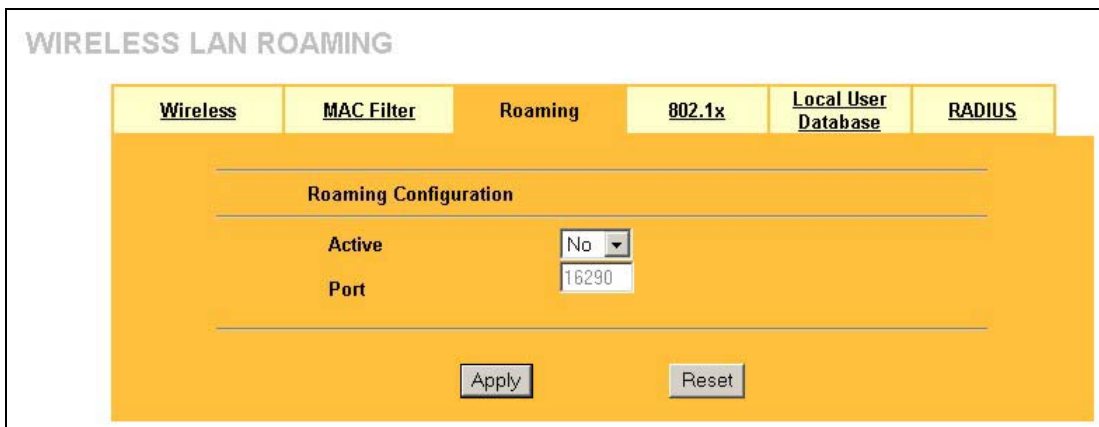


Figure 2 Roaming

The following table describes the fields in this screen.

Table 3 Roaming

LABEL	DESCRIPTION
Active	Select Yes from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center;"> All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming. </div>
Port	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 16290 . Make sure this port is not used by other services.

5.4 Configuring IEEE 802.1x Authentication

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

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

WIRELESS LAN

Wireless MAC Filter Roaming **802.1X** Local User Database RADIUS

802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

Dynamic WEP Key Exchange: 64-bit WEP

Apply Reset

Figure 3 Wireless 802.1x Authentication

The following table describes the fields in this screen.

Table 4 Wireless 802.1x Authentication

LABEL	DESCRIPTION
Wireless Port Control	<p>To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from No Authentication Required, Authentication Required and No Access Allowed.</p> <p>No Authentication Required allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.</p> <p>Authentication Required means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>No Access Allowed blocks all wireless stations access to the wired network.</p>
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select Authentication Required in the Wireless Port Control field.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p>Note: If wireless authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>

Table 4 Wireless 802.1x Authentication

LABEL	DESCRIPTION
Idle Timeout	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>This field is activated only when you select Authentication Required in the Wireless Port Control field. The default time interval is 3600 seconds (or 1 hour).</p>
Authentication Databases	<p>This field is activated only when you select Authentication Required in the Wireless Port Control field.</p> <p>The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach RADIUS, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.</p>

Table 4 Wireless 802.1x Authentication

LABEL	DESCRIPTION
Dynamic WEP Key Exchange	<p>This field is activated only when you select Authentication Required in the Wireless Port Control field. Also set the Authentication Databases field to RADIUS Only. Local user database may not be used.</p> <p>Select Disable to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.</p> <p>Select 64-bit WEP or 128-bit WEP to enable data encryption.</p> <p>Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange.</p>

5.5 Local User Database and RADIUS Overview

EAP is an authentication protocol designed originally to run over PPP (Point-to-Point Protocol) frame in order to support multiple types of user authentication. RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point (ZyAIR) is the client and the server is the RADIUS server. RADIUS is a simple package exchange in which your ZyAIR acts as a message relay between the wireless station and the network RADIUS server. In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server to perform mutual authentication.

To authenticate wireless users without interacting with a network RADIUS server, you can store user profiles locally. To change your ZyAIR's local user list, click **ADVANCED**, **WIRELESS** and then the **Local User Database** tab.

If you do enable the EAP authentication, you need to specify the local user database or the external sever for remote user authentication. To set up your ZyAIR's local user database, click **ADVANCED**, **WIRELESS** and then the **Local User Database** tab. To set up your ZyAIR's RADIUS server settings, click **WIRELESS**, then the **RADIUS** tab.

5.6 Enabling Firewall

The ZyAIR contains a stateful inspection firewall designed to protect against Denial of Service (DoS) attacks. Stateful inspection means the ZyAIR records packet information, such as port number and source/destination addresses and then allows or denies the response depending on your firewall rules.

The default rules allow LAN-to-WAN traffic and deny traffic initiated from WAN-to-LAN. You may block traffic initiated from the LAN by configuring blocked services in the **Services** screen. You may allow

traffic initiated from the WAN by configuring port-forwarding rules, one-to-one/many one-to-one mapping rules and/or allow remote management.

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

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

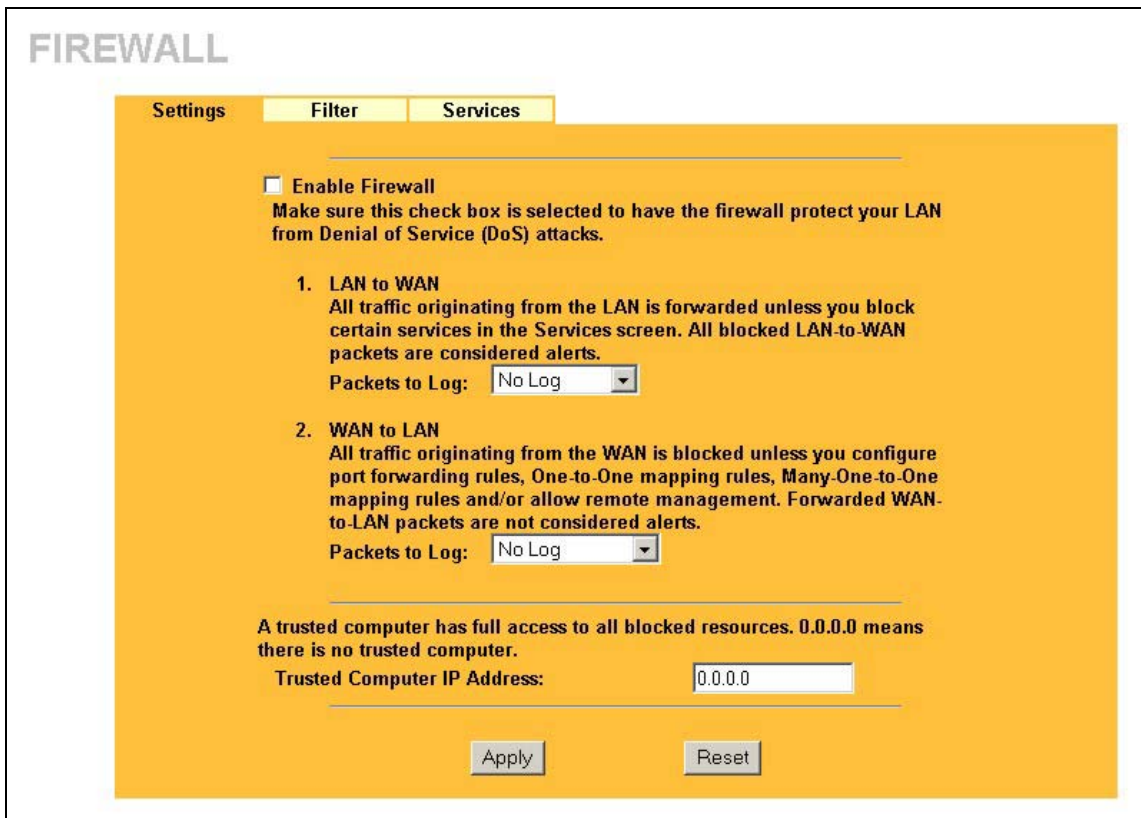


Figure 4 Firewall Settings

The following table describes the fields in this screen.

Table 5 Firewall Settings

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyAIR performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
LAN to WAN	To log packets related to firewall rules, make sure that Access Control under Log is selected in the Logs, Log Settings screen.
Packets to Log	Choose what LAN to WAN packets to log. Choose from: <ul style="list-style-type: none"> • No Log • Log Blocked (blocked LAN to WAN services appear in the Blocked Services textbox in the Services screen (with Enable Services Blocking selected)) • Log All (log all LAN to WAN packets)
WAN to LAN	To log packets related to firewall rules, make sure that Access Control under Log is selected in the Logs, Log Settings screen.
Packets to Log	Choose what WAN to LAN and WAN to WAN/Prestige packets to log. Choose from: <ul style="list-style-type: none"> • No Log • Log Forwarded • Log All (log all WAN to LAN packets).
Allow one specific computer full access to all blocked resources.	
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.

5.7 Define Content Filtering

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

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

CONTENT FILTER

Settings
Filter
Services

Restrict Web Features ActiveX Java Cookies Web Proxy

Enable URL Keyword Blocking

Keyword

Keyword List

Add
Delete
Clear All

Day to Block

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Block (24-Hour Format)

All day

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

Apply
Reset

Figure 5 Firewall Filter

The following table describes the fields in this screen.

Table 6 Firewall Filter

LABEL	DESCRIPTION
Restrict Web Features	Select the categories of web features that you want to restrict.
ActiveX	ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.

Table 6 Firewall Filter

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

5.8 Configuring Firewall Services

Click **ADVANCED**, **FIREWALL** and then the **Services** tab to open the **Services** screen. Use this screen to block LAN-to-WAN services (all are allowed when the firewall is enabled) and the date/time you want to block them.

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

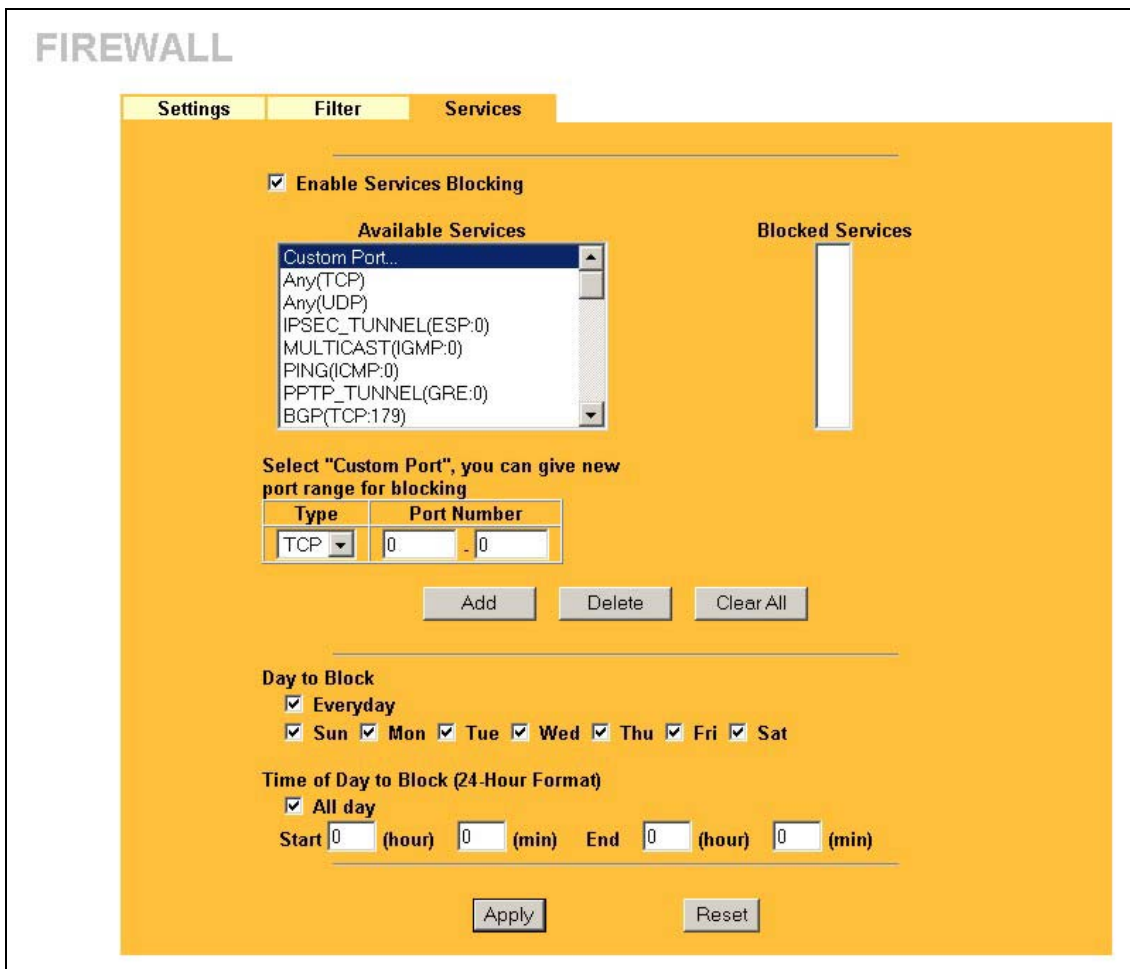


Figure 6 Firewall Services

The following table describes the fields in this screen.

Table 7 Firewall Services

LABEL	DESCRIPTION
Enable Services Blocking	Select the check box to enable this feature.

Table 7 Firewall Services

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

5.9 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers.

To configure your ZyAIR for remote management, click **ADVANCED** and then **REMOTE MANAGEMENT**.

5.10 UPnP Overview

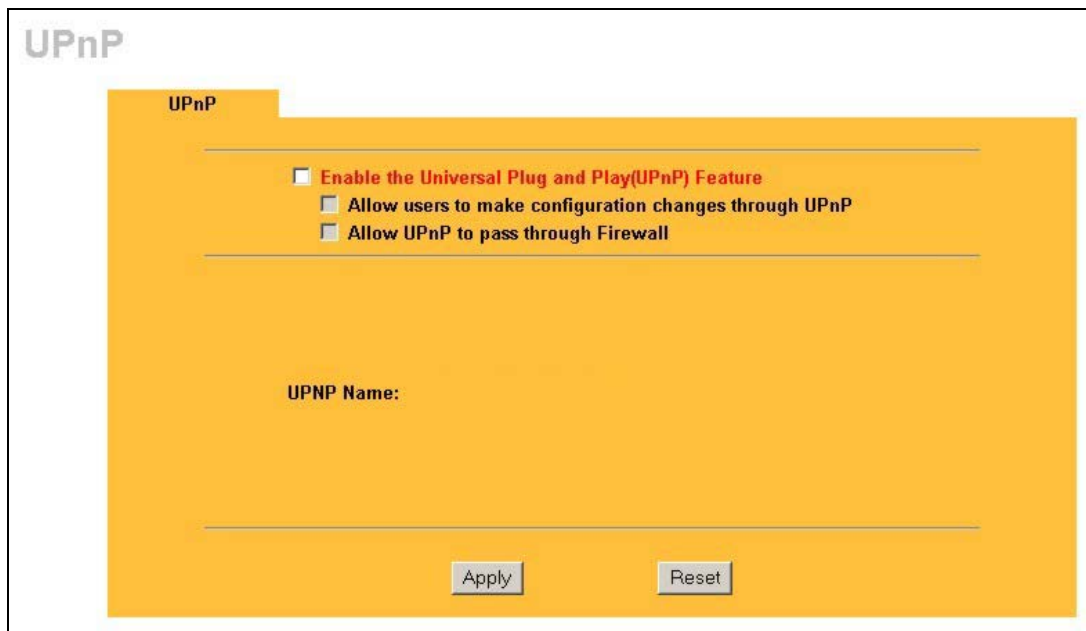
Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn,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

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

Windows ME and Windows XP support UPnP. See the Microsoft website for information about other Microsoft operating systems.

5.11 Configuring UPnP

Click **UPnP** to open the **UPnP** screen.



The screenshot shows a web-based configuration interface for UPnP. The interface is titled "UPnP" and has a yellow background. It contains the following elements:

- A tab labeled "UPnP" at the top left.
- A section with three checkboxes:
 - Enable the Universal Plug and Play(UPnP) Feature
 - Allow users to make configuration changes through UPnP
 - Allow UPnP to pass through Firewall
- A text input field labeled "UPnP Name:".
- Two buttons at the bottom: "Apply" and "Reset".

Figure 7 UPnP

The following table describes the fields in this screen.

Table 8 Configuring UPnP

FIELD	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyAIR's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyAIR so that they can communicate through the ZyAIR, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	<p>Select this check box to create a static LAN to LAN/ZyAIR rule that allows forwarding of ports 1900 and 80. Selecting this check box also creates a dynamic firewall rule every time a NAT forwarding port is reserved for UPnP. This setting remains active until you disable UPnP or clear this check box.</p> <p>Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets) instead of creating a firewall rule for them.</p>
UPnP Name	This identifies the ZyAIR in UPnP applications.

6 Hardware Installation

6.1 Attaching Antennas

Follow the steps below to connect the supplied antennas.

1. Locate the antenna connectors on the sides of your ZyAIR.
2. Screw the antennas clockwise onto the antenna connectors. The antennas should be perpendicular to the ground and parallel to each other.

Make sure the antennas are securely screwed onto the antenna connectors.



Figure 8 Attaching Antenna

6.2 Hardware Mounting Installation

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

Free-standing

Place your ZyAIR on a flat, level surface (on a desk or shelf) that is strong enough to support the weight of the ZyAIR with connection cables.

With the Desktop Holder

The included desktop holder helps you organize the ZyAIR's connection cables.

- 1.** Secure the desktop holder to the back of the ZyAIR with the included screw.

2. Turn the desktop holder up to the right.
3. Refer to the *Hardware Connections* section. Connect the cables to the ports on the ZyAIR through the desktop holder.
4. Turn the desktop holder down and place the unit on a flat, sturdy surface (on a desk or shelf).

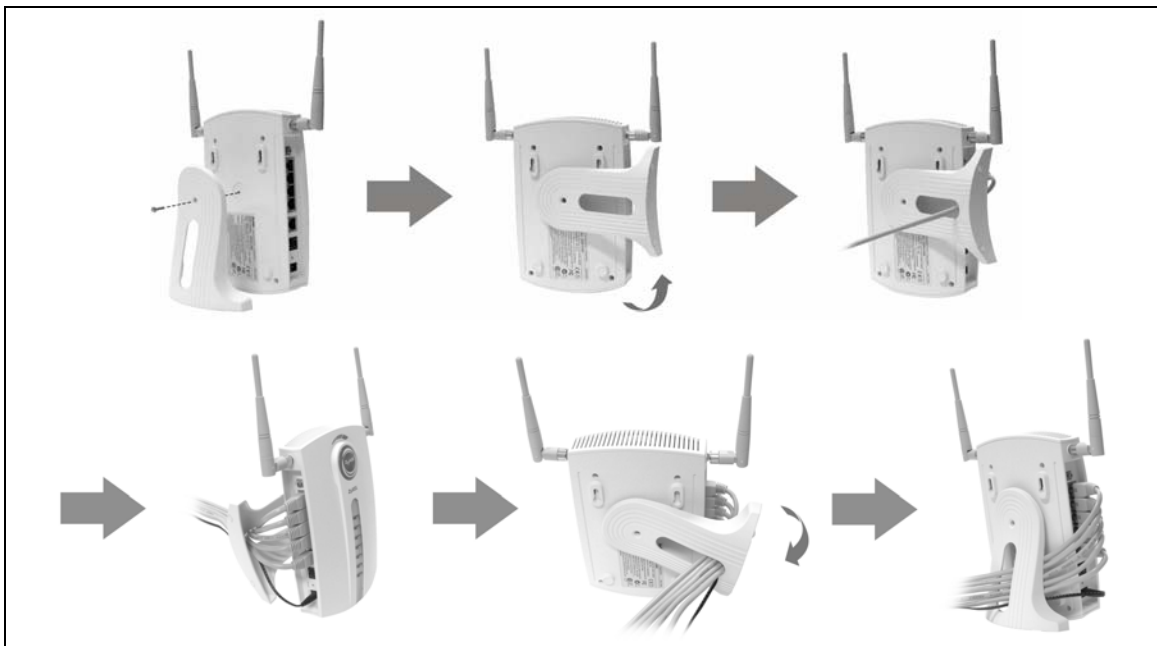


Figure 9 Instructions using the Desktop Holder

Wall-mounted

Follow the steps to attach your ZyAIR to a wall.

- Step 1.** Locate a high position on the wall that is free of obstructions.
2. You can use the diagram at the end of this guide to help you mark the screw holes correctly. Use screws with 6mm ~7.5mm (0.24" ~ 0.30") wide heads. Connect two screws (not included) in the wall 80mm (3.15") apart. Do not screw the screws all the way into the wall. Leave a small gap between the head of the screws and the wall.

Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the ZyAIR with the connection cables.

3. Align the holes on the back of the ZyAIR with the screws on the wall. Hang the ZyAIR on the screws.

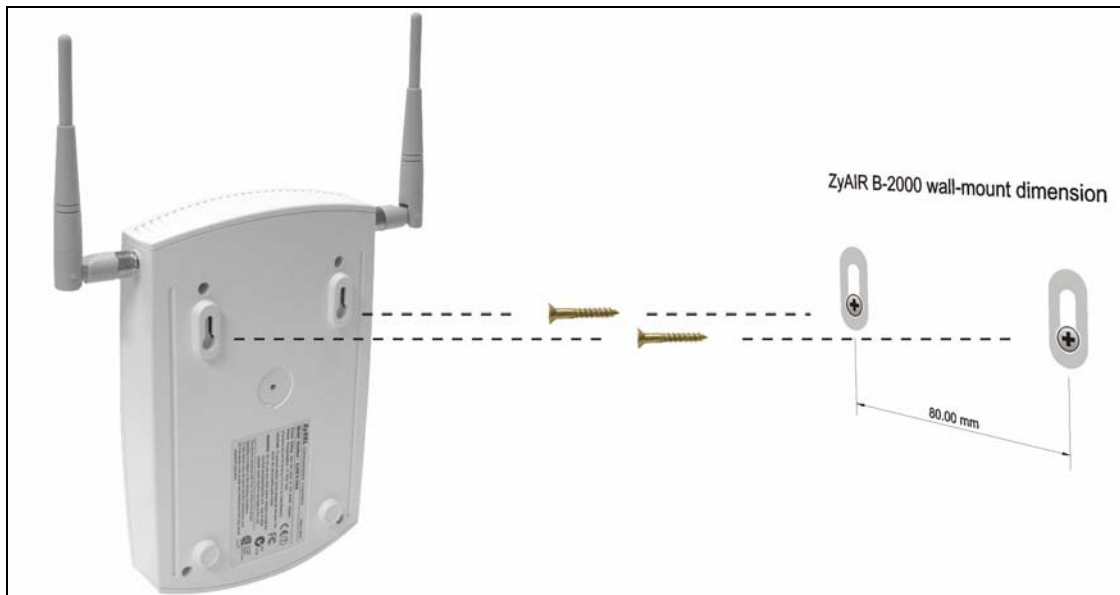


Figure 10 Wall Mounting your ZyAIR

7 Troubleshooting

PI OBLEM	CORRECTIVE ACTION
The PWR and/or SYS LED are off.	<p>Make sure you are using the correct power adaptor and the power adaptor is plugged into an adequate power supply.</p> <p>Turn the ZyAIR off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>
The LAN LED is off.	<p>Check the cable connection to the ZyAIR LAN port.</p> <p>Make sure your computer's network card is working properly.</p>
The ZyAIR LED is off.	<p>Turn the ZyAIR off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>
I cannot access the web configurator.	<p>Make sure the IP addresses and subnet masks of the ZyAIR and the computer are in the same IP address range. (For example, if the ZyAIR is using the default IP address and subnet mask, check that the IP address of the computer is in the range 192.168.1.2 ~192.168.1.254 and the subnet mask is 255.255.255.0). Refer to the <i>Setting Up Your Computer's IP Address</i> section.</p> <p>If you changed the ZyAIR default IP address, then enter the new IP address as the web site address.</p> <p>The default password is "1234". If you have changed the password and have now forgotten it, you will need to reset the ZyAIR. Refer to the <i>User's Guide</i> for how to use the RESET button.</p>
I cannot ping any computer on the LAN.	<p>If all of the LAN LEDs are off, check the cables between the ZyAIR and your computer or hub.</p> <p>Verify that the IP address and the subnet mask of the ZyAIR and the computers are on the same IP address range.</p>
I cannot get a WAN IP address from the ISP.	<p>The WAN IP is provided after the ISP verifies the MAC address, host name or user ID.</p> <p>Find out the verification method used by your ISP and configure the corresponding fields.</p>
I cannot access the Internet.	<p>Make sure the ZyAIR is turned on and connected to the network.</p> <p>Make sure you entered your username correctly. A username may be case-sensitive.</p>

Cut out this page to mark the points on the wall for the screws.

