ZyAIR G-1000

Wireless 54 Mbps Access Point

User's Guide

Version 3.50

July 2003

ZyXEL
Unleash Networking Power

Manual abstract:

All rights reserved. @@@@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. ii Copyright ZyAIR G-1000 Access Point User's Guide 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. 2. 3. 4.
Reorient or relocate the receiving antenna. Increase the separation between the equipment and the receiver. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. Consult the dealer or an experienced radio/TV technician for help. Notice 1 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. FCC Statements iii ZyAIR G-1000 Access Point User's Guide 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. iv ZyXEL Limited Warrenty ZyAIR G-1000 Access Point User's Guide 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 E-MAIL SUPPORT/SALES TELEPHONE/FAX WEB SITE/ FTP SITE REGULAR MAIL LOCATION WORLDWIDE support@zyxel.com.tw +886-3-578-3942 www.zyxel.com www.europe.zyxel.com sales@zyxel.com.tw NORTH AMERICA support@zyxel.com sales@zyxel.

com SCANDINAVIA support@zyxel.dk sales@zyxel.dk FINLAND sales@zyxel.fi +45-3955-0700 +45-3955-0707 +359-9-4780-8400 +359-9-4780-8448 GERMANY support@zyxel.de sales@zyxel.de +49-2405-6909-0 +49-2405-6909-99 www.zyxel.de +886-3-578-2439 1-800-255-4101 ftp.europe.zyxel.com www.us.zyxel.com ftp.zyxel.com www.zyxel.dk ftp.zyxel.dk http://www.zyxel.fi/ ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark ZyXEL Communications Oy, Malminkaari 10 00700 Helsinki, Finland ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany ZyXEL Communications Corp., 6 Innovation Road II, ScienceBased Industrial Park, Hsinchu 300, Taiwan Customer Support v ZyAIR G-1000 Access Point User's Guide Table of Contents Copyright .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
5-1 Table of Contents vii ZyAIR G-1000 Access Point User's Guide 5.1.3 ESS ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....5-2 5.

2 Wireless LAN Basics.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
...5-3 5.2.1 RTS/CTS.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
.....

.....
.....

.19-2 xvi List of Tables ZyAIR G-1000 Access Point User's Guide Preface Congratulations on your purchase of the ZyAIR G-1000. ZyAIR G-1000 is an IEEE802.11g-compliant 54 Mbps Ethernet wireless LAN Access Point (AP). It is suited for wireless connection to the wired network in the home and small office environment allowing users to enjoy the convenience of wireless LAN access. An AP acts as a bridge between the wireless and wired networks, extending your existing wired network without any additional wiring. This user's guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT. Background information on features configurable by both is in web configuration parts and on features configurable by SMT only is in the part about SMT configuration. Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your ZyAIR. Not all features can be configured through all interfaces.

Related Documentation Supporting Disk Refer to the included CD for support documents. Quick Installation Guide Our Quick Installation Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access. ZyXEL Web Site The ZyXEL download library at www.zyxel.

com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms. User Guide Feedback Help us help you.

E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you. Syntax Conventions · · "Enter" means for you to type one or more characters (and press the carriage return). "Select" or "Choose" means for you to use one predefined choices. Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys. Preface xvii ZyAIR G-1000 Access Point User's Guide · Mouse action sequences are denoted using a comma.

For example, "click the Apple icon, Control Panels and then Modem" means first click the Apple icon, then point your mouse pointer to Control Panels and then click Modem. For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual. The ZyAIR G-1000 Access Point may be referred to simply as the "ZyAIR", the "access point" or the "ZyAIR G-1000" in the user's guide. · · xviii Preface Getting Started Part I: GETTING STARTED This part introduces the main features and applications of ZyAIR, hardware installation and setup and shows how to access the web configurator. I ZyAIR G-1000 Access Point User's Guide Chapter 1 Getting to Know Your ZyAIR This chapter introduces the main features and applications of the ZyAIR. 1.

1 Introducing the ZyAIR G-1000 Access Point The ZyAIR G-1000 Access Point extends the range of your existing wired network without any additional wiring efforts, providing easy network access to mobile users. The ZyAIR incorporates the IEEE 802.11g standard for high-speed (up to 54 Mbps) wireless transmission. In line with the standard, your ZyAIR is backward compatible with IEEE 802.11b-enabled devices.

Additionally, the ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption and MAC address filtering. The ZyAIR is easy to install and configure. The embedded web-based configurator and SNMP network management enables remote configuration and management. 1.

2 ZyAIR Features Your ZyAIR has a number of features that give it the flexibility to provide a complete wireless networking solution. 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface This auto-negotiating feature allows the ZyAIR to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. 10/100M Auto-crossover Ethernet/Fast Ethernet Interface The Etherent interface automatically adjusts to either a crossover or straight-through Ethernet cable. Reset Button The ZyAIR reset button is built into the top panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.2, subnet mask to 255.255.

255.0. Getting to Know Your ZyAIR 1-1 ZyAIR G-1000 Access Point User's Guide ZyAIR LED The blue ZyAIR LED (also known as the Breathing LED) is on (dimmed) when the ZyAIR is on and blinks brightly when data is being transmitted to/from its wireless stations. You may use the web configurator to turn this LED off even when the ZyAIR is on and data is being transmitted/received.

802.11g Wireless LAN Standard ZyAIR products containing the letter "G" in the model name, such as ZyAIR G-1000, ZyAIR G-2000, support the 802.11g wireless standard. 802.11g will be fully compatible with the 802.11b standard.

This means an 802.11b radio card can interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates.

The 802.11g data rate and modulation are as follows: 802.11g Data Rate (Mbps) 1 ~ 54 Data Rate (Mbps) 1 ~ 54 The ZyAIR may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs. Wireless LAN MAC Address Filtering Your ZyAIR checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

IEEE 802.1x Network Security The ZyAIR supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication. Brute-Force Password Guessing Protection The ZyAIR has a special protection mechanism to discourage brute-force password guessing attacks on the ZyAIR's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendix for details about this feature. 1-2 Getting to Know Your ZyAIR ZyAIR G-1000 Access Point User's Guide SNMP SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices.

SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manger station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c). Full Network Management The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyAIR's management settings. Most functions of the ZyAIR are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection. Logging and Tracing Built-in message logging and packet tracing. Unix syslog facility support. Embedded FTP and TFTP Servers The ZyAIR's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration. Wireless Association List With the wireless association list, you can see the list of the wireless stations that are currently using the ZyAIR to access your wired network. 1.3 Applications for the ZyAIR Here are some applications examples of what you can do with your ZyAIR. 1.3.1 Internet Access Application The ZyAIR is an ideal access solution for wireless Internet connection.

A typical Internet access application for your ZyAIR is shown as follows. Getting to Know Your ZyAIR 1-3 ZyAIR G-1000 Access Point User's Guide Figure 1-1 Internet Access Application 1.3.2 Corporation Network Application In situations where users are always on the move in the coverage area but still need access to corporate network access, the ZyAIR is an ideal solution for wireless stations to connect to the corporate network without expensive network cabling. The following figure depicts a typical application of the ZyAIR in an enterprise environment.

The two computers with wireless adapters are allowed to access the network resource through the ZyAIR after account validation by the network authentication server. Figure 1-2 Corporation Network Application 1-4 Getting to Know Your ZyAIR ZyAIR G-1000 Access Point User's Guide Chapter 2 Hardware Installation and Initial Setup This chapter describes the physical features of the ZyAIR and how to make cable connections. 2.1 Front Panel of the ZyAIR The LEDs on the front panel indicate the operational status of your ZyAIR. Link LED ZyAIR LED ETHN LED PWR LED Figure 2-1 ZyAIR Front Panel Getting to Know Your ZyAIR 2-1 ZyAIR G-1000 Access Point User's Guide Table 2-1 Front Panel LED Description LED Link COLOR Red STATUS Blinking Off ZyAIR (WLAN ACK) ETHN Blue Breathing On (dim) Green On Blinking Off Orange On Blinking Off PWR Green On Off DESCRIPTION The ZyAIR is not ready or rebooting. The ZyAIR is working properly. The ZyAIR is sending/receiving data. The ZyAIR is ready, but is not sending/receiving data. The ZyAIR has a successful 10Mb Ethernet connection. The ZyAIR is sending/receiving data.

The ZyAIR does not have 10Mb Ethernet connection. The ZyAIR has a successful 100Mb Ethernet connection. The ZyAIR is sending/receiving data. The ZyAIR does not have 100Mb Ethernet connection. The ZyAIR is receiving power. The ZyAIR is not receiving power. 2.2 Top Panel and Connections of the ZyAIR The following figure shows the top panel of your ZyAIR. Figure 2-2 ZyAIR Top Panel 2-2 Getting to Know Your ZyAIR ZyAIR G-1000 Access Point User's Guide 2.2.

1 One 10/100M Ethernet Port Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. The ETHERNET port is auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your ZyAIR to a computer/external hub. When the ZyAIR is turned on and properly connected to a computer or a hub, the ETHN LED on the front panel turns on. 2.2.

2 Power Port Connect the power adapter to the port labeled POWER 12VDC on the top panel of your ZyAIR which then automatically turns on. The ZyAIR will reboot if the supplied power is too low. This is a normal operation. To avoid damage to the ZyAIR , make sure you use the supplied power adapter. Refer to the Power Adapter Specification appendix for more information.

2.2.3 The RESET Button Hold this button in for about 10 seconds (or until the Link LED turns red) to reboot and restore your ZyAIR to factory default values. All custom settings will be lost once you reset to the default settings. 2.2.4 Antennas The ZyAIR is equipped with two reverse SMA connectors and two detachable omni-directional 2dBi antennas to provide clear radio signal between the wireless stations and the access points. Refer to the Antenna Selection and Positioning Recommendations appendix for more information. The following table shows the ZyAIR's coverage (in meters) using the included antennas. The distance may differ depending on the network environment.

Getting to Know Your ZyAIR 2-3 ZyAIR G-1000 Access Point User's Guide Table 2-2 ZyAIR G-1000 Wireless LAN Coverage 11 Mbps Indoor Outdoor 50 m 200 m 5.

5 Mbps or lower 80 m 300 m Refer to the Quick Installation Guide for instructions to attach the antennas to the ZyAIR. 2.3 Hardware Mounting Options The ZyAIR may be placed on a flat surface or wall mounted. In general, the best place for the access point is at the center of your intended wireless coverage area. For better performance, mount the ZyAIR in a high position free of obstructions. Refer to the Quick Installation Guide for hardware mounting procedure. 2.4 Additional Installation Requirements A computer(s) with an installed network card or an IEEE 802.11g-compliant PCMCIA wireless LAN card.

To enable remote RADIUS authentication for wireless clients, you need A wireless client computer running IEEE 802.1x-compliant client software. Currently, this is bundled with Windows XP. A network RADIUS server for remote user authentication and accounting. 2.

5 Configuring Your ZyAIR Web configurator SMT (System Management Terminal). Access the SMT using Telnet. Configure your ZyAIR using: 2-4 Getting to Know Your ZyAIR ZyAIR G-1000 Access Point User's Guide Chapter 3 Introducing the Web Configurator This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens. The default IP address of the ZyAIR is 192.168.

1.2. 3.1 Step 1. Step 2. Step 3. Step 4. Step 5. Step 6. Accessing the ZyAIR Web Configurator Make sure your ZyAIR hardware is properly connected.

Prepare your computer/computer network to connect to the ZyAIR (refer to the Quick Installation Guide. Launch your web browser. Type "192.168.1.2" (default) as the URL. Type "1234" (default) as the password and click Login. In some versions, the default password appears automatically - if this is the case, click Login. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click Apply or click Ignore.

Figure 3-1 Change Password Screen Step 7. You should now see the MAIN MENU screen. Introducing the Web Configurator 3-1 ZyAIR G-1000 Access Point User's Guide The ZyAIR automatically times out after five minutes of inactivity. Simply log back into the ZyAIR if this happens to you. 3.

2 Resetting the ZyAIR If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file or use the RESET button on the top panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to "1234", also. 3.

2.1 Method of Restoring Factory-Defaults You can erase the current configuration and restore factory defaults in three ways: 1. Use the RESET button on the top panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the Link LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known. Use the web configurator to restore defaults. Transfer the configuration file to your ZyAIR using the SMT menus. See the part on SMT configuration for more information. 2. 3. 3.

3 Navigating the ZyAIR Web Configurator Follow the instructions you see in the MAIN MENU screen or click the icon (located in the top right corner of most screens) to view online help. The icon does not appear in the MAIN MENU screen. The following summarizes how to navigate the web configurator from the MAIN MENU screen. 3-2 Introducing the Web Configurator ZyAIR G-1000 Access Point User's Guide Click WIZARD SETUP for initial configuration including general setup, Wireless LAN setup and IP address assignment. Refer to the Quick Installation Guide for information. Click ADVANCED to configure advanced features such as SYSTEM (General, Password and Time settings), WIRELESS LAN (Wireless, MAC Filter, Roaming, 802.1x, Local User Database and RADIUS), IP, and Logs (View reports and Log Settings). Click LOGOUT at any time to exit the web configurator. Click MAINTENANCE to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes SYSTEM STATUS (Statistics), Wireless (Association List), F/W (firmware) UPLOAD, CONFIGURATION (Backup, Restore and Default).

Figure 3-2 Web Configurator: Main Menu Refer to the Quick Installation Guide for information on configuring the Wizard screens. Introducing the Web Configurator 3-3 System and Wireless LAN Part II: SYSTEM AND WIRELESS LAN This part covers the System and Wireless LAN screens. II ZyAIR G-1000 Access Point User's Guide Chapter 4 System Screens This chapter provides information on the System screens. 4.1 4.

2 System Overview Configuring General Setup This section provides information on general system setup. Click ADVANCED and then SYSTEM to open the General screen. Figure 4-1 System General Setup The following table describes the labels in this screen. System Screens 4-1 ZyAIR G-1000 Access Point User's Guide Table 4-1 System General Setup LABEL System Name DESCRIPTION Type a descriptive name to identify the ZyAIR in the Ethernet network. This name can be up to 30 alphanumeric characters long.

Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This is not a required field. Leave this field blank or enter the domain name here if you know it. Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). Domain Name Administrator Inactivity Timer System DNS Servers First DNS Server Second DNS Server Third DNS Server Select From DHCP if your DHCP server dynamically assigns DNS server information (and the ZyAIR's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.

If you chose From DHCP, but the ZyAIR has a fixed Ethernet IP address, From DHCP changes to None after you click Apply. If you chose From DHCP for the second or third DNS server, but the DHCP server does not provide a second or third IP address, From DHCP changes to None after you click Apply. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second UserDefined changes to None after you click Apply.

Select None if you do not want to configure DNS servers.
If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is None. Click Apply to save your changes back to the ZyAIR. Click Reset to reload the previous configuration for this screen. Apply Reset 4.
3 Configuring Password To change your ZyAIR's password (recommended), click ADVANCED, SYSTEM and then the Password tab. The screen appears as shown. This screen allows you to change the ZyAIR's password. 4-2 System Screens ZyAIR G-1000 Access Point User's Guide If you forget your password (or the ZyAIR IP address), you will need to reset the ZyAIR. See the Resetting the ZyAIR section in for details.
Figure 4-2 Password The following table describes the labels in this screen. Table 4-2 Password LABEL Old Password New Password Retype to Confirm Apply Reset DESCRIPTION Type in your existing system password (1234 is the default password). Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type. Retype your new system password for confirmation. Click Apply to save your changes back to the ZyAIR. Click Reset to reload the previous configuration for this screen. 4.4 Setting the Time To set the time and date on your ZyAIR, click ADVANCED, SYSTEM and then the Time Setting tab. The screen appears as shown.

System Screens 4-3 ZyAIR G-1000 Access Point User's Guide Figure 4-3 Time Setting The following table describes the labels in this screen. Table 4-3 Time/Date LABEL Time Protocol DESCRIPTION Select the time protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305), is similar to Time (RFC 868). Select None to enter the time and date manually. 4-4 System Screens ZyAIR G-1000 Access Point User's Guide Table 4-3 Time/Date LABEL Time Server Address Current Time (hh:mm:ss) New Time (hh:mm:ss) Current Date (yy/mm/dd) New Date (yy/mm/dd) Time Zone Daylight Savings DESCRIPTION Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information (the default is tick.
stdtime.gov.tw). This field displays the time of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
This field displays the last updated time from the time server. When you select None in the Time Protocol field, enter the new time in this field. This field displays the date of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server. This field displays the last updated date from the time server.
When you select None in the Time Protocol field, enter the new date in this field. Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Enter the month and day that your daylight-savings time starts on if you selected Daylight Savings. Enter the month and day that your daylight-savings time ends on if you selected Daylight Savings. Click Apply to save your changes back to the ZyAIR. Click Reset to begin configuring this screen afresh. Start Date (mm-dd) End Date (mm-dd) Apply Reset System Screens 4-5 ZyAIR G-1000 Access Point User's Guide Chapter 5 Wireless Configuration and Roaming This chapter discusses how to configure Wireless and Roaming screens on the ZyAIR.

. 5.1 Wireless LAN Overview This section introduces the wireless LAN (WLAN) and some basic scenarios. 5.1.1 IBSS An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other and can set up an independent (wireless) network without the need of an access point (AP). Figure 5-1 IBSS (Ad-hoc) Wireless LAN 5.1.2 BSS A Basic Service Set (BSS) is when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).
Intra-BSS traffic is traffic between wireless stations in the BSS. Wireless Configuration and Roaming 5-1 ZyAIR G-1000 Access Point User's Guide Figure 5-2 Basic Service set 5.1.3 ESS An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).
An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate. 5-2 Wireless Configuration and Roaming ZyAIR G-1000 Access Point User's Guide Figure 5-3 Extended Service Set 5.2 Wireless LAN Basics Refer also to the Wizard Setup chapter for more background information on Wireless LAN features, such as channels. 5.
2.1 RTS/CTS A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other. Wireless Configuration and Roaming 5-3 ZyAIR G-1000 Access Point User's Guide Figure 5-4 RTS/CTS When station A sends data to the ZyAIR, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations. RTS/CTS is designed to prevent collisions due to hidden nodes. An RTS/CTS defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked. When a data frame exceeds the RTS/CTS value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it.

The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission.

It also reserves and confirms with the requesting station the time frame for the requested transmission. Stations can send frames smaller than the specified RTS/CTS directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake. You should only configure RTS/CTS if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake. If the RTS/CTS value is greater than the Fragmentation Threshold value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. 5.2.2 Fragmentation Threshold A Fragmentation Threshold is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyAIR will fragment the packet into smaller data frames. 5-4 Wireless Configuration and Roaming ZyAIR G-1000 Access Point User's Guide A large Fragmentation Threshold is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the Fragmentation Threshold value is smaller than the RTS/CTS value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. 5.3 Configuring Wireless Click ADVANCED and then WIRELESS to display the Wireless screen. Figure 5-5 Wireless The following table describes the general wireless LAN labels in this screen. Wireless Configuration and Roaming 5-5 ZyAIR G-1000 Access Point User's Guide Table 5-1 Wireless LABEL ESSID DESCRIPTION (Extended Service Set IDentity) The ESSID identifies the Service Set with to which a wireless station is associated.

Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings. Hide ESSID Choose Channel ID RTS/CTS Threshold Fragmentation Threshold Apply Reset Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.

Set the operating frequency/channel depending on your particular region. RTS/CTS handshake avoids retransmitting due to hidden nodes. Enter a value between 0 and 2432. The default is 2432. Fragmentation threshold defines the maximum data fragment size that can be sent. Enter a value between 256 and 2432. Click Apply to save your changes back to the ZyAIR. Click Reset to begin configuring this screen afresh. See the Wireless Security chapter for information on the other fields in this screen. 5.

4 Configuring Roaming A wireless station is a device with an IEEE 802.11b or 802.11g-compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area. In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors. The roaming feature on the access points allows the access points to relay information about the wireless stations to each other.

When a wireless station moves from a coverage area to another, it scans and uses the 5-6 Wireless Configuration and Roaming ZyAIR G-1000 Access Point User's Guide channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 5-6. With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN. If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas.

The wireless station may not be able to communicate with other wireless stations on the network and vice versa. Figure 5-6 Roaming Example The steps below describe the roaming process. Step 1. As wireless station Y moves from the coverage area of access point AP 1 to that of access point AP 2, it scans and uses the signal of access point AP 2. Step 2.

Access point AP 2 acknowledges the presence of wireless station Y and relays this information to access point AP 1 through the wired LAN. Step 3. Access point AP 1 updates the new position of wireless station. Step 4. Wireless station Y sends a request to access point AP 2 for reauthentication. 5.4.1 Requirements for Roaming The following requirements must be met in order for wireless stations to roam between the coverage areas. 1. All the access points must be on the same subnet and configured with the same ESSID.

2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station. Wireless Configuration and Roaming 5-7 ZyAIR G-1000 Access Point User's Guide The adjacent access points should use different radio channels when their coverage areas overlap. All access points must use the same port number to relay roaming information. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment. To enable roaming on your ZyAIR, click ADVANCED, WIRELESS and then the Roaming tab. The screen appears as shown. 3. 4.

5. Figure 5-7 Roaming The following table describes the labels in this screen. Table 5-2 Roaming LABEL Active DESCRIPTION Select Yes from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming. Port Enter the port number to communicate roaming information between access points.

The port number must be the same on all access points. The default is 16290. Make sure this port is not used by other services. Click Apply to save your changes back to the ZyAIR.

Click Reset to begin configuring this screen afresh.
Apply Reset 5-8 Wireless Configuration and Roaming ZyAIR G-1000 Access Point User's Guide Chapter 6 Wireless Security This chapter describes how to configure WEP encryption, MAC filter, 802.1x, Local User Database and RADIUS to set up wireless security on your ZyAIR 6.1 Wireless Security Overview Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network. The figure below shows the possible wireless security levels on your ZyAIR. The highest security level relies on EAP (Extensible Authentication Protocol) for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations. Figure 6-1 ZyAIR Wireless Security Levels If you do not enable any wireless security on your ZyAIR, your network is accessible to any wireless networking device that is within range. 6.2 WEP Overview WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

6.2.1 Data Encryption WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your ZyAIR allows you to configure up to four 64bit or 128-bit WEP keys, but only one key can be enabled at any one time. Wireless Security 6-1 ZyAIR G-1000 Access Point User's Guide 6.2.2 Authentication Three different methods can be used to authenticate wireless stations to the network: Open System, Shared Key, and Auto. The following figure illustrates the steps involved. Wireless Station Open System Authentication Open System Request Authentication Access Point Authentication Acceptance Shared Key Authentication Shared Key Request Challenge Text Encrypted Challenge Text Authentication Acceptance Figure 6-2 WEP Authentication Steps Open System authentication involves an unencrypted two-message procedure.
A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network. Shared Key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key.
If the decrypted message matches the challenge text, the wireless station is authenticated. 6-2 Wireless Security ZyAIR G-1000 Access Point User's Guide When your ZyAIR's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the ZyAIR will accept either type of authentication request and the ZyAIR will fall back to use open authentication if the shared key does not match. 6.
3 Configuring WEP Data Encryption In order to configure and enable WEP encryption; click ADVANCED and then WIRELESS to display the Wireless screen. Figure 6-3 Wireless The following table describes the wireless LAN security fields in this screen. Wireless Security 6-3 ZyAIR G-1000 Access Point User's Guide Table 6-1 Wireless LABEL WEP Encryption Authentication Method DESCRIPTION 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. Select Auto, Open System or Shared Key from the drop-down list box. This field is N/A if WEP is not activated. If WEP encryption is activated, the default setting is Auto. Select this option to enter ASCII characters as the WEP keys. Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.

The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on (dimmed) when the ZyAIR is on and blinks brightly (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received. Click Apply to save your changes back to the ZyAIR.
Click Reset to begin configuring this screen afresh. ASCII Hex Key 1 to Key 4 Enable Breathing LED Apply Reset 6.4 MAC Filter The MAC filter screen allows you to configure the ZyAIR to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the ZyAIR (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
You need to know the MAC address of the devices to configure this screen. To change your ZyAIR's MAC filter settings, click ADVANCED, WIRELESS and then the MAC Filter tab. The screen appears as shown. 6-4 Wireless Security ZyAIR G-1000 Access Point User's Guide Figure 6-4 MAC Address Filter The following table describes the fields in this screen. Wireless Security 6-5 ZyAIR G-1000 Access Point User's Guide Table 6-2 MAC Address Filter LABEL MAC Address Filter Active Filter Action Select Yes from the drop down list box to enable MAC address filtering.
@@Select Deny Association to block access to the router, MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router, MAC addresses not listed will be denied access to the router. Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the ZyAIR in these address fields. Click Apply to save your changes back to the ZyAIR. Click Reset to begin configuring this screen afresh. DESCRIPTION MAC Address Apply Reset 6.5 802.1x Overview The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the ZyAIR (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

6.6 Introduction to RADIUS RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others: · · Authentication Determines the identity of the users. Accounting Keeps track of the client's network activity. RADIUS user is a simple package exchange in which your ZyAIR acts as a message relay between the wireless station and the network RADIUS server. Types of RADIUS Messages The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication: 6-6 Wireless Security ZyAIR G-1000 Access Point User's Guide · · · · Access-Request Sent by an access point requesting authentication. Access-Reject Sent by a RADIUS server rejecting access. Access-Accept Sent by a RADIUS server allowing access. Access-Challenge Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting: · · Accounting-Request Sent by the access point requesting accounting. Accounting-Response Sent by the RADIUS server to indicate that it has started or stopped accounting. In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

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

The type of authentication you use depends on the RADIUS server or the AP. The ZyAIR supports EAPTLS, EAP-TTLS and DEAP with RADIUS. Refer to the Types of EAP Authentication appendix for descriptions on the four common types. Your ZyAIR supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database and RADIUS. The following figure shows an overview of authentication when you specify a RADIUS server on your access point. Wireless Security 6-7 ZyAIR G-1000 Access Point User's Guide AP RADIUS Server Wireless Station Ethernet Figure 6-5 EAP Authentication The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix. · · · · The wireless station sends a "start" message to the ZyAIR.

The ZyAIR sends a "request identity" message to the wireless station for identity information. The wireless station replies with identity information, including username and password. The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station. 6.7 Dynamic WEP Key Exchange The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed. If this feature is enabled, it is not necessary to configure a default WEP encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled. To use Dynamic WEP, enable and configure the RADIUS server (see section 6.

11) and enable Dynamic WEP Key Exchange in the 802.1x screen. Ensure that the wireless station's EAP type is configured to one of the following: · · · EAP-TLS EAP-TTLS PEAP EAP-MD5 cannot be used with Dynamic WEP Key Exchange. 6-8 Wireless Security ZyAIR G-1000 Access Point User's Guide 6.8 Introduction to Local User Database By storing user profiles locally on the ZyAIR, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server.

However, there is a limit on the number of users you may authenticate in this way. 6.9 Configuring 802.1x To change your ZyAIR's authentication settings, click ADVANCED, WIRELESS and then the 802.1x tab.

The screen appears as shown. Figure 6-6 802.1x Authentication The following table describes the fields in this screen. Wireless Security 6-9 ZyAIR G-1000 Access Point User's Guide Table 6-3 802.1x Authentication LABEL Wireless Port Control DESCRIPTION To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from No Authentication Required, Authentication Required and No Access Allowed. No Authentication Required allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. Authentication Required means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. No Access Allowed blocks all wireless stations access to the wired network.

Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select Authentication Required in the Wireless Port Control field. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). ReAuthentication Timer (in seconds) If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. Idle Timeout (in seconds) The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select Authentication Required in the Wireless Port Control field. The default time interval is 3600 seconds (1 hour). 6-10 Wireless Security ZyAIR G-1000 Access Point User's Guide Table 6-3 802.

1x Authentication LABEL Authentication Databases DESCRIPTION This field is activated only when you select Authentication Required in the Wireless Port Control field. The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first.