# G-1000

*802.11g Wireless Access Point*

# *User's Guide*

Version 3.50
11/2005

ZyXEL
Unleash Networking Power

# Copyright

## Disclaimer

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

## Trademarks

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

# Federal Communications Commission (FCC) Interference Statement

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

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

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

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

- 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.

## Caution

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Notice 1

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

## Information for Canadian Users

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

Cet appareil numerique de la classe B est conforme a la norme NMB-003 du Canada.

## Certifications

Go to www.zyxel.com

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

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

# Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

# 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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 to the purchaser.

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

# Customer Support

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

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

| METHOD | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| LOCATION | SALES E-MAIL | FAX | FTP SITE | |
| CORPORATE HEADQUARTERS (WORLDWIDE) | support@zyxel.com.tw | +886-3-578-3942 | www.zyxel.com<br>www.europe.zyxel.com | ZyXEL Communications Corp.<br>6 Innovation Road II<br>Science Park<br>Hsinchu 300<br>Taiwan |
| | sales@zyxel.com.tw | +886-3-578-2439 | ftp.zyxel.com<br>ftp.europe.zyxel.com | |
| CZECH REPUBLIC | info@cz.zyxel.com | +420-241-091-350 | www.zyxel.cz | ZyXEL Communications<br>Czech s.r.o.<br>Modranská 621<br>143 01 Praha 4 - Modrany<br>Ceská Republika |
| | info@cz.zyxel.com | +420-241-091-359 | | |
| DENMARK | support@zyxel.dk | +45-39-55-07-00 | www.zyxel.dk | ZyXEL Communications A/S<br>Columbusvej<br>2860 Soeborg<br>Denmark |
| | sales@zyxel.dk | +45-39-55-07-07 | | |
| FINLAND | support@zyxel.fi | +358-9-4780-8411 | www.zyxel.fi | ZyXEL Communications Oy<br>Malminkaari 10<br>00700 Helsinki<br>Finland |
| | sales@zyxel.fi | +358-9-4780 8448 | | |
| FRANCE | info@zyxel.fr | +33-4-72-52-97-97 | www.zyxel.fr | ZyXEL France<br>1 rue des Vergers<br>Bat. 1 / C<br>69760 Limonest<br>France |
| | | +33-4-72-52-19-20 | | |
| GERMANY | support@zyxel.de | +49-2405-6909-0 | www.zyxel.de | ZyXEL Deutschland GmbH.<br>Adenauerstr. 20/A2 D-52146<br>Wuerselen<br>Germany |
| | sales@zyxel.de | +49-2405-6909-99 | | |
| HUNGARY | support@zyxel.hu | +36-1-3361649 | www.zyxel.hu | ZyXEL Hungary<br>48, Zoldlomb Str.<br>H-1025, Budapest<br>Hungary |
| | info@zyxel.hu | +36-1-3259100 | | |
| KAZAKHSTAN | http://zyxel.kz/support | +7-3272-590-698 | www.zyxel.kz | ZyXEL Kazakhstan<br>43, Dostyk ave.,Office 414<br>Dostyk Business Centre<br>050010, Almaty<br>Republic of Kazakhstan |
| | sales@zyxel.kz | +7-3272-590-689 | | |
| NORTH AMERICA | support@zyxel.com | 1-800-255-4101<br>+1-714-632-0882 | www.us.zyxel.com | ZyXEL Communications Inc.<br>1130 N. Miller St.<br>Anaheim<br>CA 92806-2001<br>U.S.A. |
| | sales@zyxel.com | +1-714-632-0858 | ftp.us.zyxel.com | |
| NORWAY | support@zyxel.no | +47-22-80-61-80 | www.zyxel.no | ZyXEL Communications A/S<br>Nils Hansens vei 13<br>0667 Oslo<br>Norway |
| | sales@zyxel.no | +47-22-80-61-81 | | |

| METHOD | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| **LOCATION** | **SALES E-MAIL** | **FAX** | **FTP SITE** | |
| **POLAND** | info@pl.zyxel.com | +48-22-5286603 | www.pl.zyxel.com | ZyXEL Communications<br>ul.Emilli Plater 53<br>00-113 Warszawa<br>Poland |
| | | +48-22-5206701 | | |
| **RUSSIA** | http://zyxel.ru/support | +7-095-542-89-29 | www.zyxel.ru | ZyXEL Russia<br>Ostrovityanova 37a Str.<br>Moscow, 117279<br>Russia |
| | sales@zyxel.ru | +7-095-542-89-25 | | |
| **SPAIN** | support@zyxel.es | +34-902-195-420 | www.zyxel.es | ZyXEL Communications<br>Alejandro Villegas 33<br>1º, 28043 Madrid<br>Spain |
| | sales@zyxel.es | +34-913-005-345 | | |
| **SWEDEN** | support@zyxel.se | +46-31-744-7700 | www.zyxel.se | ZyXEL Communications A/S<br>Sjöporten 4, 41764 Göteborg<br>Sweden |
| | sales@zyxel.se | +46-31-744-7701 | | |
| **UKRAINE** | support@ua.zyxel.com | +380-44-247-69-78 | www.ua.zyxel.com | ZyXEL Ukraine<br>13, Pimonenko Str.<br>Kiev, 04050<br>Ukraine |
| | sales@ua.zyxel.com | +380-44-494-49-32 | | |
| **UNITED KINGDOM** | support@zyxel.co.uk | +44-1344 303044<br>08707 555779 (UK only) | www.zyxel.co.uk | ZyXEL Communications UK<br>Ltd.,11 The Courtyard,<br>Eastern Road, Bracknell,<br>Berkshire, RG12 2XB,<br>United Kingdom (UK) |
| | sales@zyxel.co.uk | +44-1344 303034 | ftp.zyxel.co.uk | |

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

# Table of Contents

# List of Figures

# List of Tables

# Preface

Congratulations on your purchase of the ZyXEL G-1000 - 802.11g Wireless Access Point.

An AP acts as a bridge between the wireless and wired networks, extending your existing wired network without any additional wiring.

Your G-1000 is easy to install and configure.

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

## About This User's Guide

This User’s Guide is designed to guide you through the configuration of your G-1000 using the web configurator or the SMT. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator

**Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your G-1000. Not all features can be configured through all interfaces.

## Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Compact Guide

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

- Web Configurator Online Help

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

- ZyXEL Glossary and Web Site

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

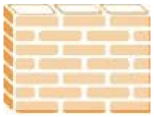
## User Guide Feedback

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

## Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted by right angle brackets (>). For example, "**Start** > **Settings** > **Control Panel** > **System**" means click the **Start** button, move the mouse over **Settings**, move the mouse over or click on **Control Panel**, and then click on **System**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The ZyXEL G-1000 may be referred to simply as the G-1000 in the user's guide.

## Graphics Icons Key

| | | |
|---|---|---|
| G-1000<br> | Computer<br> | Notebook computer<br> |
| Server<br> | DSLAM<br> | Firewall<br> |
| Modem<br> | Switch<br> | Router<br> |
| Wireless Signal<br> | | |

# CHAPTER 1
# Getting to Know Your G-1000

This chapter introduces the main features and applications of the G-1000.

## 1.1 Introducing the G-1000

The 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 G-1000 incorporates the IEEE802.11g standard for high-speed wireless transmission. In line with the standard, your G-1000 is backward-compatible with IEEE802.1b-enabled devices.

Additionally, the G-1000 offers highly-secure wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption and MAC address filtering.

The G-1000 is easy to install and configure. The embedded web-based configurator enables easy operation and configuration.

## 1.2 G-1000 Features

The following sections describe the features of the G-1000

### 1.2.1 Physical Features

#### 1.2.1.1 10/100M Auto-negotiating Ethernet/Fast Ethernet Interface

This auto-negotiating feature allows the G-1000 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.

#### 1.2.1.2 10/100M Auto-crossover Ethernet/Fast Ethernet Interface

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

#### 1.2.1.3 Reset Button

The G-1000 reset button is built into the side panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.2, subnet mask to 255.255.255.0.

#### 1.2.1.4 G-1000 LED

The blue G-1000 LED (also known as the Breathing LED) is on when the G-1000 is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. You may use the web configurator to turn this LED off even when the G-1000 is on and data is being transmitted/received.

### 1.2.2 Firmware Features

#### 1.2.2.1 Internal RADIUS Server

The G-1000 has a built-in RADIUS server that can authenticate wireless clients or other AP's in other wireless networks.The G-1000 can also function as an AP and as a RADIUS server at the same time.

#### 1.2.2.2 Wi-Fi Protected Access

The G-1000 supports WPA and WPA2. Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. WPA supports user authentication, and it provides better data encryption than WEP. WPA2 is similar to WPA but provides even stronger data encryption than WPA.

#### 1.2.2.3 802.11b Wireless LAN Standard

The G-1000 complies with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are shown in the table below. The modulation technique defines how bits are encoded onto radio waves.

**Table 1** IEEE 802.11b

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

### 1.2.2.4 802.11g Wireless LAN Standard

The G-1000 complies with the 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g device (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:.

**Table 2** IEEE 802.11g

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

**Note:** The G-1000 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.

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

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

### 1.2.2.6 Limit the number of Client Connections

You may set a maximum number of wireless stations that may connect to the G-1000. This may be necessary if for example, there is interference or difficulty with channel assignment due to a high density of APs within a coverage area.

### 1.2.2.7 Brute-Force Password Guessing Protection

The G-1000 has a special protection mechanism to discourage brute-force password guessing attacks on the G-1000'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.

### 1.2.2.8 Wireless LAN MAC Address Filtering

Your G-1000 checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

### 1.2.2.9 WEP Encryption

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

#### 1.2.2.10 IEEE 802.1x Network Security

The G-1000 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.

#### 1.2.2.11 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 G-1000 supports SNMP agent functionality, which allows a manger station to manage and monitor the G-1000 through the network. The G-1000 supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

#### 1.2.2.12 Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the G-1000's management settings. Most functions of the G-1000 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.

#### 1.2.2.13 Logging and Tracing

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

#### 1.2.2.14 Embedded FTP and TFTP Servers

The G-1000's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

#### 1.2.2.15 Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the G-1000 to access your wired network.

## 1.3 Applications for the G-1000

Here are some G-1000 application examples.

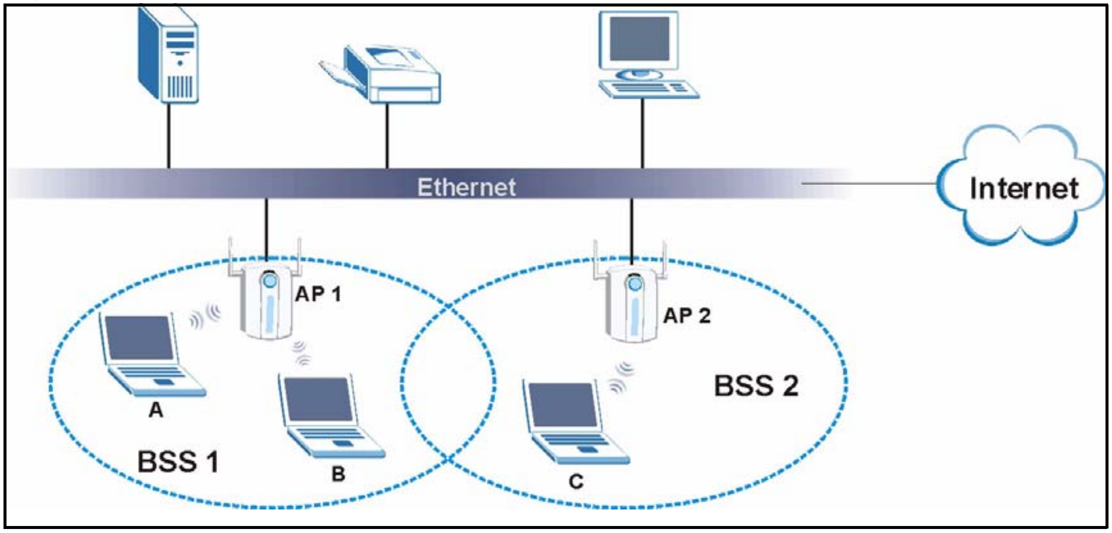
.

**Note:** A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

### 1.3.1 Internet Access Application

The G-1000 is an ideal access solution for wireless Internet connection. A typical Internet access application for your G-1000 is shown as follows. Stations A, B and C can access the wired network through the G-1000s.

**Figure 1** Internet Access Application

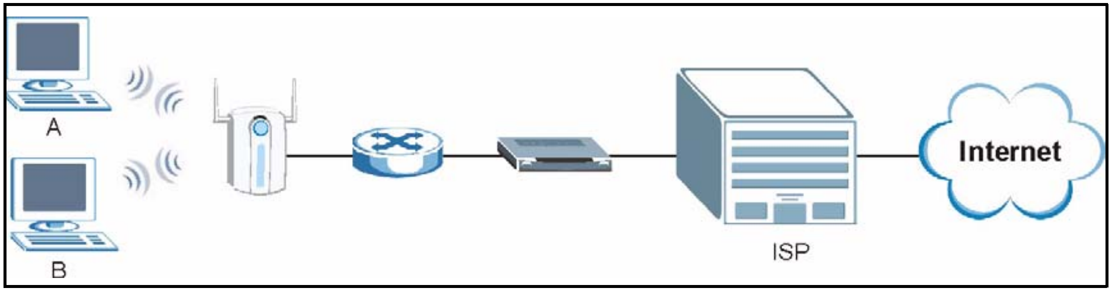


### 1.3.2 Corporation Network Application

In situations where users are always on the move in the coverage area but still need access to corporate network access, the G-1000 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 G-1000 in an enterprise environment. Stations A and B with wireless adapters are allowed to access the network resource through the G-1000 after account validation by the network authentication server.

**Figure 2** Corporation Network Application



# CHAPTER 2 Hardware Installation and Initial Setup

This chapter describes the physical features of the G-1000 and how to make cable connections.

## 2.1 Front Panel of the G-1000

The LEDs on the front panel indicate the operational status of your G-1000.

**Figure 3** G-1000 Front Panel

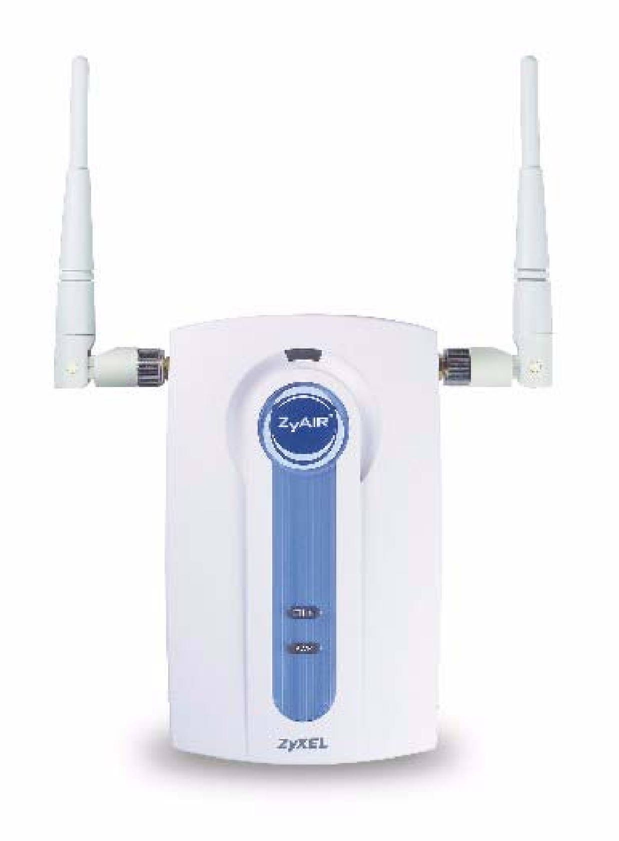


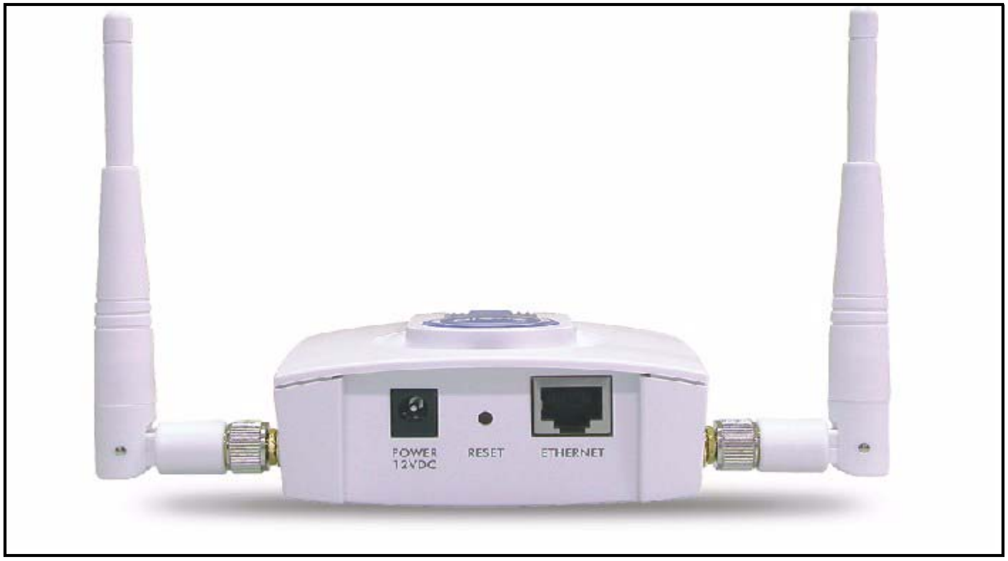
**Table 3** Front Panel LED Description

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| BRI/RPT | Green | On | The wireless card on the G-1000 is working properly. |
| | | Off | The wireless card on the G-1000 is not ready or has a malfunction. |
| | Red | On | The G-1000 is not ready or rebooting. |
| G-1000(WLAN ACK) | Blue | Breathing | The G-1000 is sending or receiving data. |
| | | On (dim) | The G-1000 is ready, but is not sending or receiving data. |
| ETHN | Green | On | The G-1000 has a successful 10Mb Ethernet connection. |
| | | Blinking | The G-1000 is sending/receiving data. |
| | | Off | The G-1000 does not have 10Mb Ethernet connection. |
| | Orange | On | The G-1000 has a successful 100Mb Ethernet connection. |
| | | Blinking | The G-1000 is sending or receiving data. |
| | | Off | The G-1000 does not have 100Mb Ethernet connection. |
| PWR | Green | On | The G-1000 is receiving power. |
| | | Off | The G-1000 is not receiving power. |

## 2.2 Top Panel and Connections of the G-1000

The following figure shows the top panel of your G-1000.

**Figure 4** G-1000 Top Panel



### 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 G-1000 to a computer/external hub.

**Note:** When the G-1000 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 G-1000 which then automatically turns on.

**Note:** The G-1000 will reboot if the supplied power is too low. This is a normal operation.
**Note:** To avoid damage to the G-1000, 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 ten seconds (or until the Link LED turns red) to reboot and restore your G-1000 to factory default values.

**Note:** All custom settings will be lost once you reset to the default settings.

### 2.2.4 Antennas

The G-1000 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 G-1000's coverage (in meters) using the included antennas. The distance may differ depending on the network environment.

**Table 4** G-1000 Wireless LAN Coverage

| | ≤ **11 MBPS** | ≤ **5.5 MBPS OR LOWER** |
|---|---|---|
| Indoor | 50 m | 80 m |
| Outdoor | 200 m | 300 m |

Refer to the Quick Installation Guide for instructions on how to attach the antennas to the G-1000.

## 2.3 Hardware Mounting Options

The G-1000 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 G-1000 in a high position free of obstructions.

Refer to the Quick Start Guide for hardware mounting procedure.

## 2.4 Additional Installation Requirements

- A computer(s) with an installed network card or an IEEE 802.11b-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 G-1000

Configure your G-1000 using the Web configurator or SMT (System Management Terminal). You can access the SMT using Telnet.

# CHAPTER 3 Introducing the Web Configurator

This chapter describes how to access the G-1000 web configurator and provides an overview of its screens. The default IP address of the G-1000 is 192.168.1.2.

## 3.1 Accessing the G-1000 Web Configurator

1 Make sure your G-1000 hardware is properly connected and prepare your computer/ computer network to connect to the G-1000 (refer to the Quick Start Guide).

2 Launch your web browser.

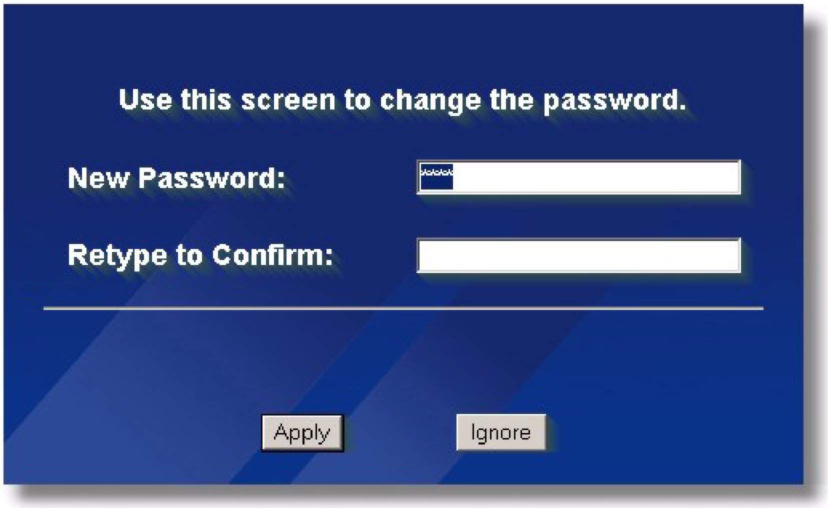
3 Type "192.168.1.2" as the URL.

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

5 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**.

**Note:** If you do not change the password, the following screen appears every time you login.

**Figure 5** Change Password Screen



Use this screen to change the password.

New Password: ****

Retype to Confirm:

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

**Note:** The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the G-1000 if this happens to you.

## 3.2 Resetting the G-1000

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the side panel of the G-1000. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to 1234.

### 3.2.1 Procedure To Use The Reset Button

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

1 Press the **RESET** button for ten seconds or until the **SYS** LED, **LINK** LED or **BDG/ RPT** LED turns red, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the G-1000 restarts. Otherwise, go to step 2.

2 Turn the G-1000 off.

3 While pressing the **RESET** button, turn the G-1000 on.

4 Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the G-1000 is now restarting.

**5** Release the **RESET** button and wait for the G-1000 to finish restarting.

### 3.2.2 Method of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

Use the **RESET** button on the side panel of the G-1000 to upload the default configuration file (hold this button in for about 10 seconds or until the **SYS** LED, **LINK** LED or **BDG/RPT** LED turns red). Use this method for cases when the password or IP address of the G-1000 is not known.

Use the web configurator to restore defaults (refer to Chapter 10).

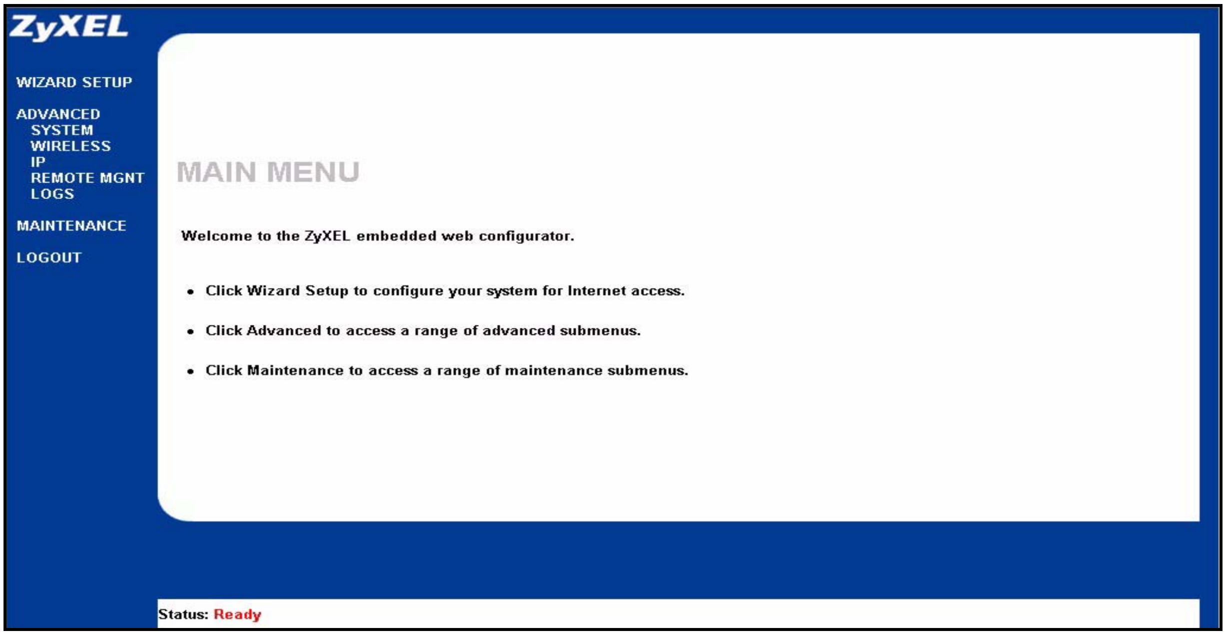
Transfer the configuration file to your G-1000 using FTP. See later in the part on SMT configuration for more information.

## 3.3 Navigating the G-1000 Web Configurator

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

**Note:** Follow the instructions you see in the MAIN MENU screen or click the HELP ? icon (located in the top right corner of most screens) to view online help.
**Note:** The HELP ? icon does not appear in the MAIN MENU screen.

**Figure 6** The MAIN MENU Screen of the Web Configurator



Welcome to the ZyXEL embedded web configurator.

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

Status: Ready

Click **WIZARD SETUP** for initial configuration including general setup, Wireless LAN setup and IP address assignment.

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Password and Time Zone), **WIRELESS** (Wireless, MAC Filter, Roaming and 802.1x/WPA), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), Internal RADIUS Server (Settings, Trusted AP and Trusted User databases), and **LOGS** (View reports and Log Settings).

Click **MAINTENANCE** to view information about your G-1000 or upgrade configuration/ firmware files. Maintenance includes **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**

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

# CHAPTER 4 Wizard Setup

This chapter provides information on the Wizard Setup screens in the web configurator.

## 4.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your G-1000 for wireless stations to access your wired LAN.

### 4.1.1 Channel

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

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

The G-1000's "Scan" function is especially designed to automatically scan for a channel with the least interference.

### 4.1.2 ESS ID

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

### 4.1.3 WEP Encryption

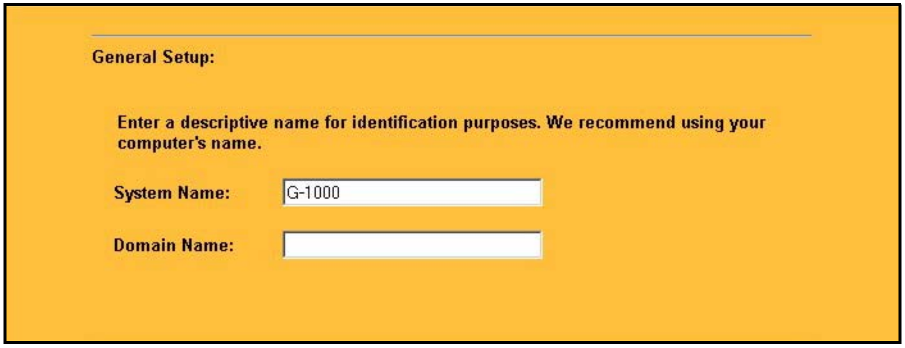
WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both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

## 4.2 Wizard Setup: General Setup

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

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the G-1000 via DHCP.

**Figure 7** Wizard 1: General Setup



General Setup:

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

System Name: G-1000

Domain Name:

The following table describes the labels in this screen.

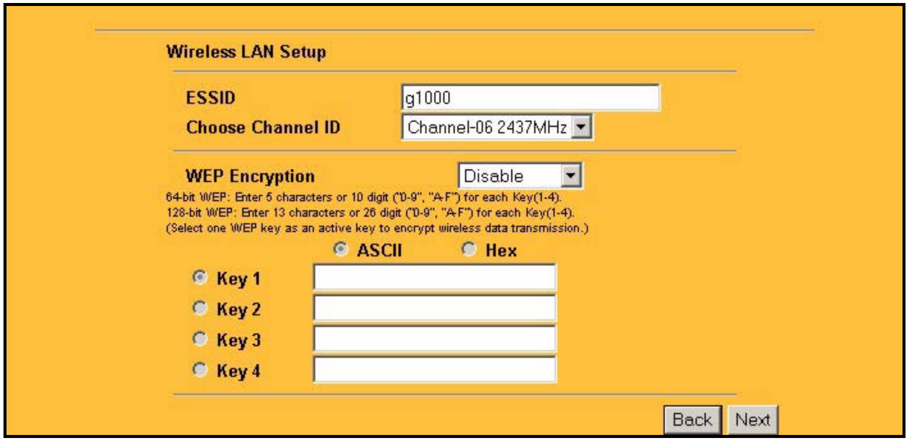
**Table 5** Wizard 1: General Setup

| LABEL | DESCRIPTION |
|---|---|
| System Name | It is recommended you type your computer's "Computer name".<br>In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.<br>In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.<br>In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the G-1000 **System Name**.<br>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | This is not a required field. Leave this field blank or enter the domain name here if you know it. |
| Next | Click **Next** to proceed to the next screen. |

## 4.3 Wizard Setup: Wireless LAN

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

**Figure 8** Wizard 2: Wireless LAN Setup



Wireless LAN Setup

ESSID: g1000

Choose Channel ID: Channel-06 2437MHz

WEP Encryption: Disable

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

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

The following table describes the labels in this screen.

**Table 6** Wizard 2: Wireless LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| Wireless LAN Setup | |
| WLAN Adaptor | Select **Built-in** from the drop down list box to configure your G-1000 using the internal WLAN card. Select **Removable** from the drop down list box to configure your G-1000 using a WLAN card adaptor using the extension card slot.<br>**Note:** This field is only available when you have an external wireless card inserted in the G-1000. |
| ESSID | Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>If you change this field on the G-1000, make sure all wireless stations use the same Name (ESSID) in order to access the network. |
| Choose Channel ID | To manually set the G-1000 to use a channel, select a channel from the drop-down list box. Open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.<br>To have the G-1000 automatically select a channel, click **Scan** instead. |
| Scan | Click this button to have the G-1000 automatically scan for and select a channel with the least interference. |
| WEP Encryption | Select **Disable** allows all wireless computers to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to allow data encryption. |
| ASCII | Select this option in order to enter ASCII characters as the WEP keys. |
| Hex | Select this option to enter hexadecimal characters as the WEP keys.<br>The preceding 0x is entered automatically. |
| Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the G-1000 and the wireless stations must use the same WEP key for data transmission.<br>If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. |

**Table 6** Wizard 2: Wireless LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.4 Wizard Setup: IP Address

The third wizard screen allows you to configure IP address assignment.

### 4.4.1 IP Address Assignment

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

**Table 7** Private IP Address Ranges

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

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

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

### 4.4.2 IP Address and Subnet Mask

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

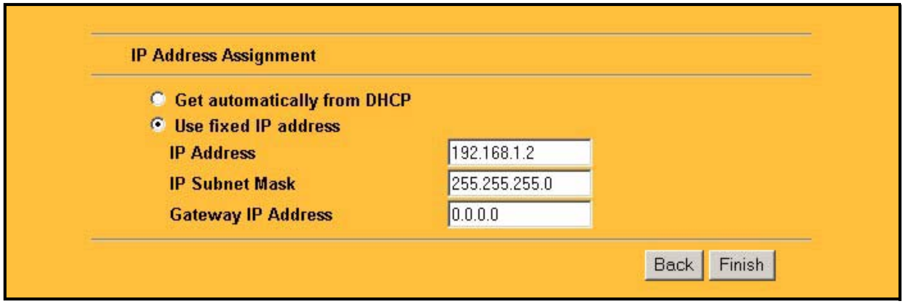
Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your G-1000, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your G-1000 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the G-1000 unless you are instructed to do otherwise.

**Figure 9** Wizard 3: IP Address Assignment



IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

| | |
|---|---|
| IP Address | 192.168.1.2 |
| IP Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 0.0.0.0 |

The following table describes the labels in this screen.

**Table 8** Wizard 3: IP Address Assignment

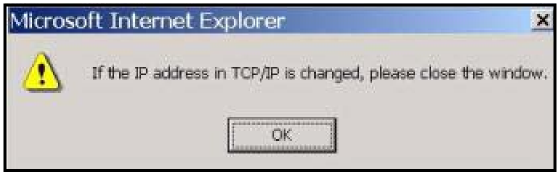
| LABEL | DESCRIPTION |
|---|---|
| IP Address Assignment | |
| Get automatically from DHCP | Select this option if your G-1000 is using a dynamically assigned IP address from a DHCP server each time.<br>**Note:** You must know the IP address assigned to the G-1000 (by the DHCP server) to access the G-1000 again. |
| Use fixed IP address | Select this option if your G-1000 is using a static IP address. When you select this option, fill in the fields below. |
| IP Address | Enter the IP address of your G-1000 in dotted decimal notation.<br>**Note:** If you changed the G-1000's IP address, you must use the new IP address if you want to access the web configurator again. |
| IP Subnet Mask | Type the subnet mask. |
| Gateway IP Address | Type the IP address of the gateway. The gateway is an immediate neighbor of your G-1000 that will forward the packet to the destination. The gateway must be a router on the same segment as your G-1000's LAN or WLAN port. |

**Table 8** Wizard 3: IP Address Assignment

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to return to the previous screen. |
| Finish | Click **Finish** to proceed to complete the Wizard setup. |

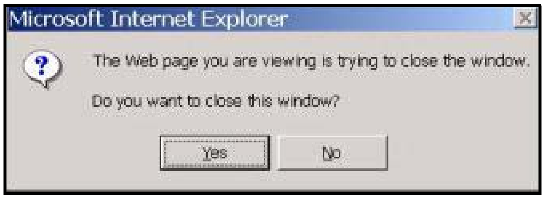
## 4.5 Basic Setup Complete

When you click **Finish** in the **Wizard 3 IP Address Assignment** screen, a warning window display as shown. Click **OK** to close the window and log in to the web configurator again using the new IP address if you change the default IP address (192.168.1.2).



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

You have successfully set up the G-1000. A screen displays prompting you to close the web browser.

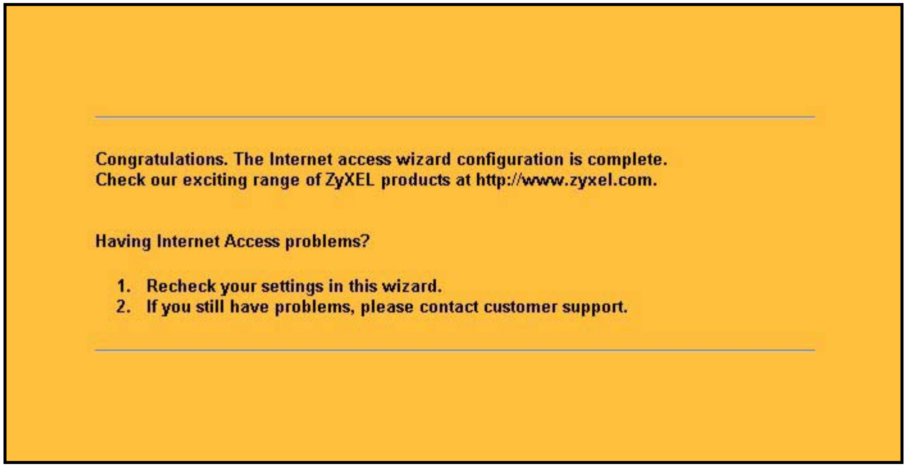


The Web page you are viewing is trying to close the window.

Do you want to close this window?

Click **Yes**. Otherwise, click **No** and the congratulations screen shows next.

**Figure 10** Wizard 4: Setup Complete



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

Having Internet Access problems?

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

Well done! You have successfully set up your G-1000 to operate on your network and access the Internet.

# Chapter 5 System Screens

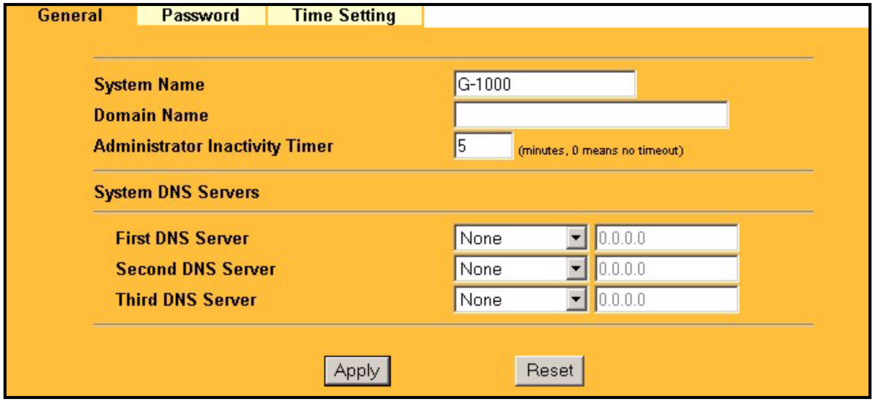
## 5.1 System Overview

This section provides information on general system setup.

## 5.2 Configuring General Setup

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

**Figure 11 System General Setup**



System Name: G-1000

Domain Name:

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

System DNS Servers

First DNS Server: None 0.0.0.0

Second DNS Server: None 0.0.0.0

Third DNS Server: None 0.0.0.0

The following table describes the labels in this screen.

**Table 9** System General Setup

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| System Name | Type a descriptive name to identify the G-1000 in the Ethernet network.<br>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | This is not a required field. Leave this field blank or enter the domain name here if you know it. |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out.<br>The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.<br>A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| System DNS Servers | |

**Table 9** System General Setup

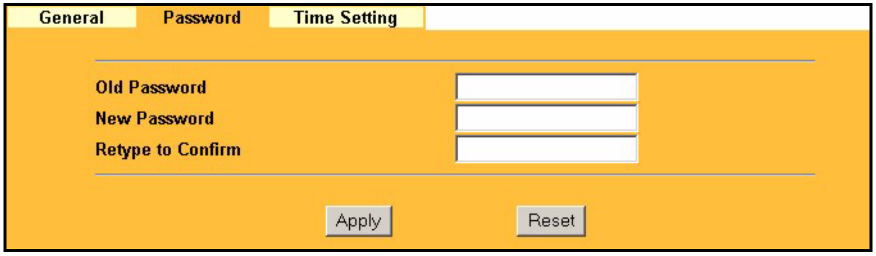
| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Select **From DHCP** if your DHCP server dynamically assigns DNS server information (and the G-1000's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns.<br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br>Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.<br>The default setting is **None**. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to reload the previous configuration for this screen. |

## 5.3 Configuring Password

To change your G-1000's password (recommended), click the **SYSTEM** link under **ADVANCED** and then the **Password** tab. The screen appears as shown. This screen allows you to change the G-1000's password.

If you forget your password (or the G-1000 IP address), you will need to reset the G-1000. See the Resetting the G-1000 section for details

**Figure 12** **Password**.



Old Password

New Password

Retype to Confirm

The following table describes the labels in this screen.

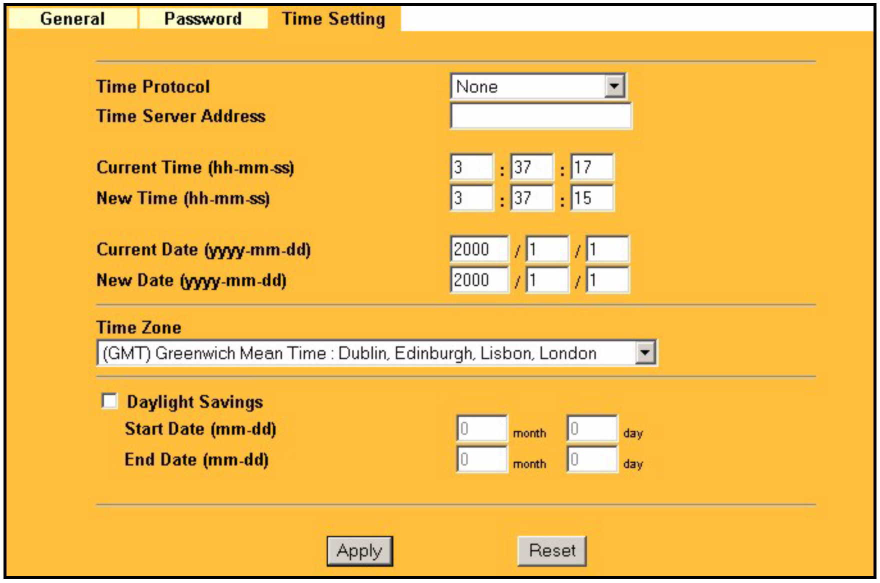
**Table 10** Password

| LABEL | DESCRIPTIONS |
|---|---|
| Old Password | Type in your existing system password (1234 is the default password). |
| New Password | Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type. |
| Retype to Confirm | Retype your new system password for confirmation. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to reload the previous configuration for this screen. |

## 5.4 Configuring Time Setting

To change your G-1000’s time and date, click the **SYSTEM** link under **ADVANCED** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the G-1000’s time based on your local time zone.

**Figure 13** Time Setting



Time Protocol: None
Time Server Address:

Current Time (hh-mm-ss): 3 : 37 : 17
New Time (hh-mm-ss): 3 : 37 : 15

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

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

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

The following table describes the labels in this screen.

**Table 11** Time Setting

| LABEL | DESCRIPTION |
|---|---|
| Time Protocol | Select the time service protocol that your time server sends when you turn on the G-1000. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC 1305),** is similar to Time (RFC 868).<br>Select **None** to enter the time and date manually. |
| Time Server Address | Enter the IP address or the URL of your time server. Check with your ISP/ network administrator if you are unsure of this information. |
| Current Time (hh:mm:ss) | This field displays the time of your G-1000.<br>Each time you reload this page, the G-1000 synchronizes the time with the time server. |
| New Time (hh:mm:ss) | This field displays the last updated time from the time server.<br>When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**. |

**Table 11** Time Setting

| LABEL | DESCRIPTION |
|---|---|
| Current Date (yyyy/mm/dd) | This field displays the date of your G-1000.<br>Each time you reload this page, the G-1000 synchronizes the date with the time server. |
| New Date (yyyy/mm/dd) | This field displays the last updated date from the time server.<br>When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**. |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Savings | Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. |
| Start Date (mm-dd) | Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**. |
| End Date (mm-dd) | Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to reload the previous configuration for this screen. |

# CHAPTER 6 Wireless LAN

This chapter discusses how to configure Wireless LAN.

## 6.1 Introduction

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

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

## 6.2 Wireless Security Overview

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

Wireless security methods available on the G-1000 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the G-1000 identity.

### 6.2.1 Encryption

- Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA(2) has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don’t have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can enter 64-bit or 128-bit WEP keys.

### 6.2.2 Authentication

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

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the G-1000.

- Use the Local User Database if you have less than 32 wireless clients in your network. The G-1000 uses MD5 encryption when a client authenticates with the Local User Database

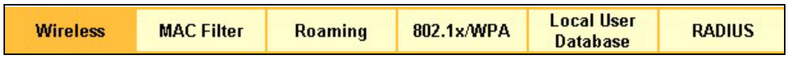
### 6.2.3 Restricted Access

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

### 6.2.4 Hide G-1000 Identity

If you hide the ESSID, then the G-1000 cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the G-1000 may be inconvenience for some valid WLAN clients.

### 6.2.5 Configuring Wireless LAN on the G-1000



1 Configure the **ESSID** and **WEP** in the **Wireless** screen. If you configure **WEP**, you can't configure **WPA(2)** or **WPA(2)-PSK**.

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

3 Use the **Roaming** screen to configure the G-1000 so that 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.

4 Configure **WPA(2)** or **WPA(2)-PSK** in the **802.1x/WPA** screen. Configure 802.1x wireless client authentication in the **802.1x/WPA** screen.

5 Configure the built-in authentication database in the **Local User Database** screen.

6 Configure the authentication and accounting servers for RADIUS in the **RADIUS** screen.

The following figure shows the relative effectiveness of these wireless security methods available on your G-1000.

The figure below shows the possible wireless security levels on your G-1000. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations

**Table 12** G-1000 Wireless Security Levels

| Security Level | Security Type |
|---|---|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| ↓ | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| Most Secure | Wi-Fi Protected Access (WPA) |
| | WPA2 |

If you do not enable any wireless security on your G-1000, your network is accessible to any wireless networking device that is within range.

# 6.3 Configuring the Wireless Screen

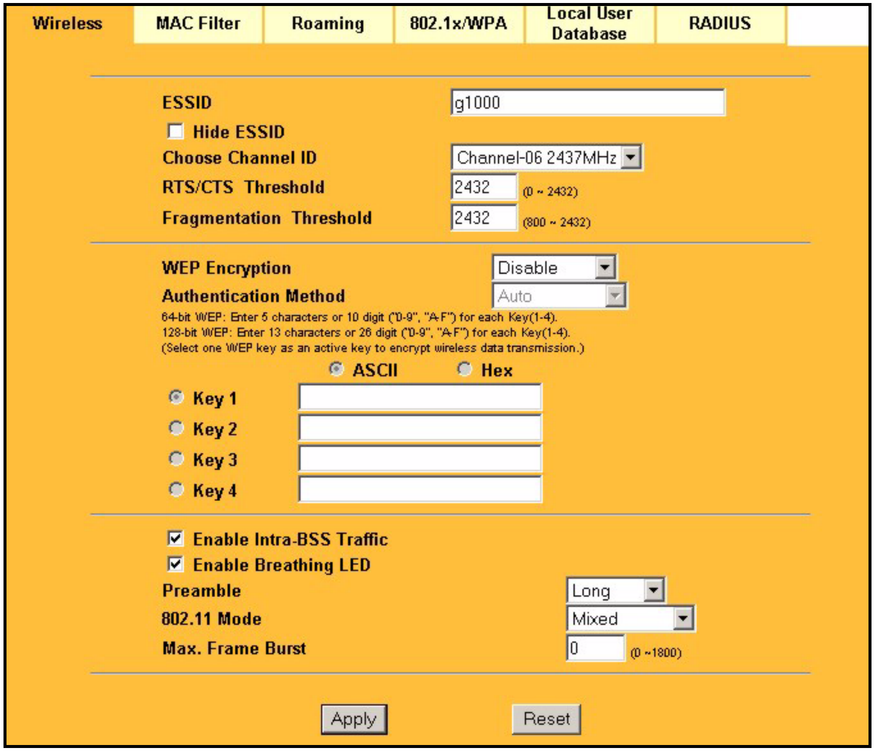
## 6.3.1 WEP Encryption

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

Your G-1000 allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

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

**Figure 14   Wireless**



ESSID: g1000

□ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

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

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Intra-BSS Traffic

☑ Enable Breathing LED

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 0 (0 ~1800)

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

**Table 13**   Wireless

| LABEL | DESCRIPTION |
|---|---|
| ESSID | The ESSID (Extended Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>**Note:** If you are configuring the G-1000 from a computer connected to the wireless LAN and you change the G-1000’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 G-1000’s new settings. |
| Hide ESSID | Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through scanning using a site survey tool. |
| Choose Channel ID | Set the operating frequency/channel depending on your particular region.<br>To manually set the G-1000 to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.<br>Refer to the Wizard Setup chapter for more information on channels. |
| 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**. |

**Table 13** Wireless

| LABEL | DESCRIPTION |
|---|---|
| Fragmentation Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **800** and **2432**. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.<br>Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Authentication Method | Select **Auto**, **Open System** or **Shared Key** from the drop-down list box. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 13 hexadecimal characters ("0-9", "A-F"). The hexadecimal characters should be preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.<br>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. |
| Enable Intra-BSS Traffic | Intra-BSS traffic is traffic between wireless stations in the same BSS. Select this check box to enable Intra-BSS traffic. |
| Enable Breathing LED | Select this check box to enable the Breathing LED, also known as the G-1000 LED.<br>The blue G-1000 LED is on when the G-1000 is on and blinks (or breaths) when data is being transmitted to/from its wireless stations.<br>Clear the check box to turn this LED off even when the G-1000 is on and data is being transmitted/received. |
| Preamble | Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**.<br>See the section on preamble for more information. |
| 802.11 Mode | Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-1000.<br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-1000.<br>Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the G-1000. The transmission rate of your G-1000 might be reduced. |
| Max. Frame Burst | Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the G-1000 transmits IEEE 802.11g wireless traffic only.<br>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.4 Configuring Roaming

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

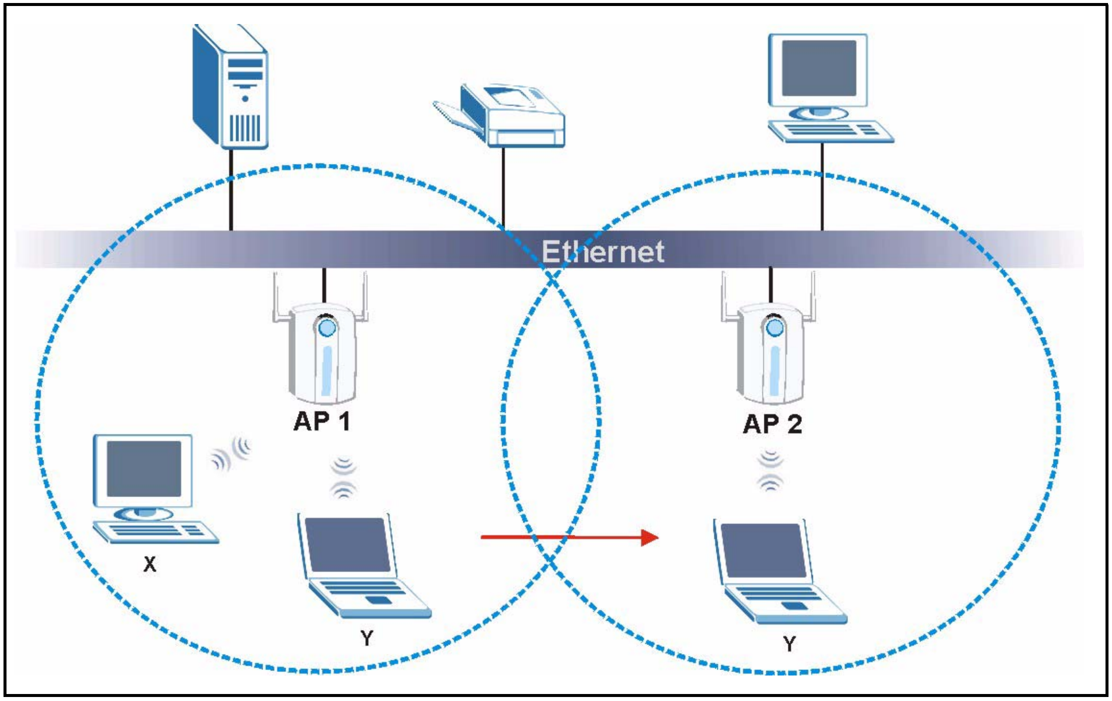
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending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

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 15.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

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

Figure 15   Roaming Example



The steps below describe the roaming process.

1 As wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point

2 **AP 2**, it scans and uses the signal of access point **AP 2**.

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

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

5 Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

## 6.4.1 Requirements for Roaming

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

1 All the access points must be on the same subnet and configured with the same ESSID.

2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

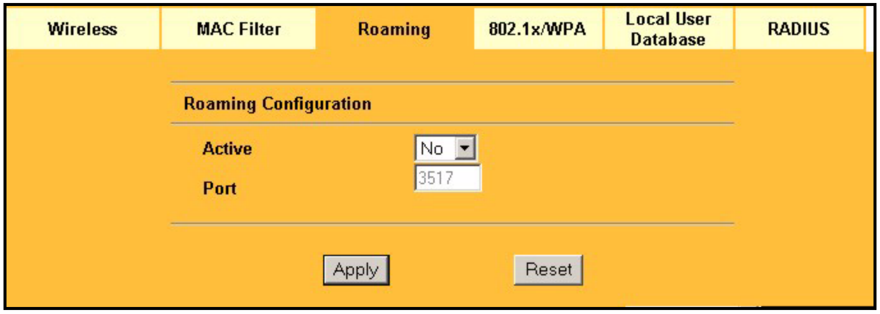
3 The adjacent access points should use different radio channels when their coverage areas overlap.

4 All access points must use the same port number to relay roaming information.

5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your G-1000, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

**Figure 16 Roaming**



Roaming Configuration

Active: No

Port: 3517

The following table describes the labels in this screen.

**Table 14** Roaming

| LABEL | DESCRIPTION |
|---|---|
| Active | Select **Yes** from the drop-down list box to enable roaming on the G-1000 if you have two or more G-1000s on the same subnet.<br>**Note:** 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 3517. Make sure this port is not used by other services. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

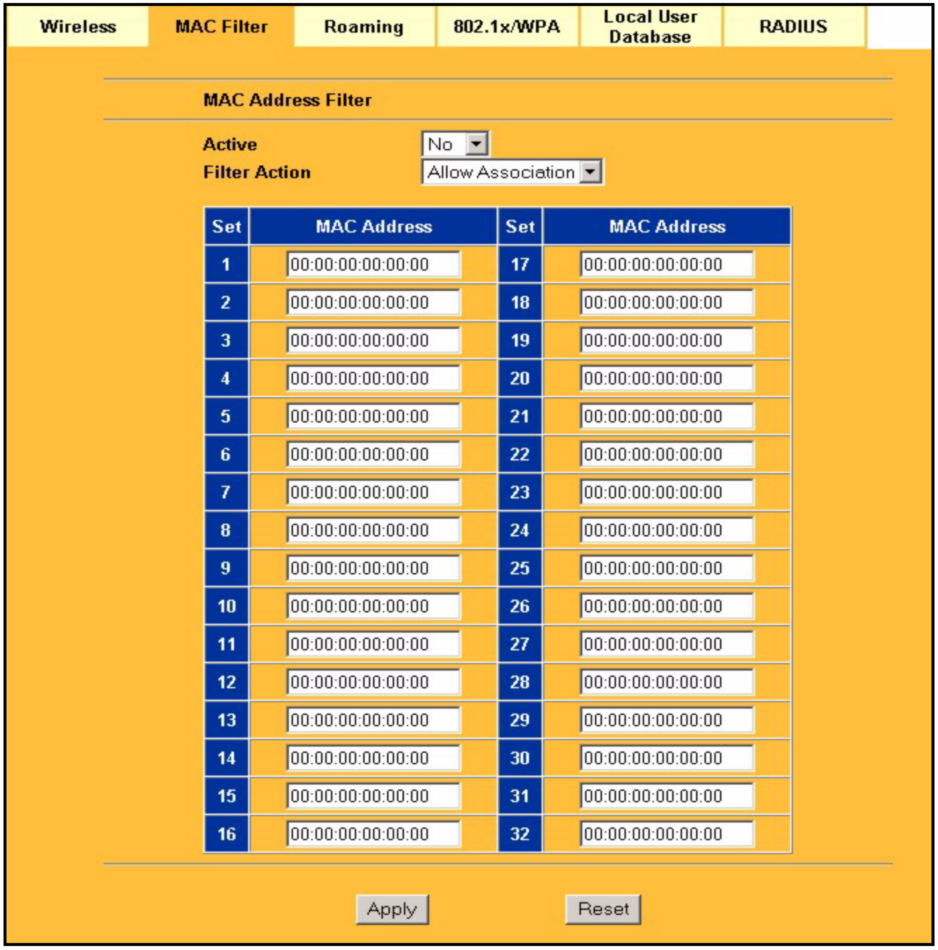
## 6.5 MAC Filter

The MAC filter screen allows you to configure the G-1000 to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the G-1000 (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.

The **WLAN Adapter** drop down list box is only available when you have an external wireless card inserted in the G-1000. No matter whether you select **Built-in** or **Removable**, the configuration screens are the same for each interface.

To change your G-1000's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

**Figure 17 MAC Address Filter**



MAC Address Filter

Active: No

Filter Action: Allow Association

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

The following table describes the labels in this screen.

**Table 15** MAC Address Filter

| LABEL | DESCRIPTION |
|---|---|
| Active | Select Yes from the drop down list box to enable MAC address filtering. |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router.<br>Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router. |
| MAC Address | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the G-1000 in these address fields. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 6.6 Introduction to WPA

Wi-Fi Protected Access (WPA and WPA2) applies IEEE 801.2x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using and external RADIUS database. WPA has better user authentication and improved data encryption than WEP, and WPA2 provides even better data encryption and user authentication than WPA. See the appendix for more information on WPA(2) user authentication and WPA encryption.

If the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key). WPA2-PSK only requires a single (identical) password entered into each WLAN member. As long as the passwords match, a client will be granted access to a WLAN.

If the wireless clients do not support WPA2, use WPA or WPA-PSK, depending on whether or not you have an additional RADIUS server. Use WEP only if the wireless clients do not support WPA(2).

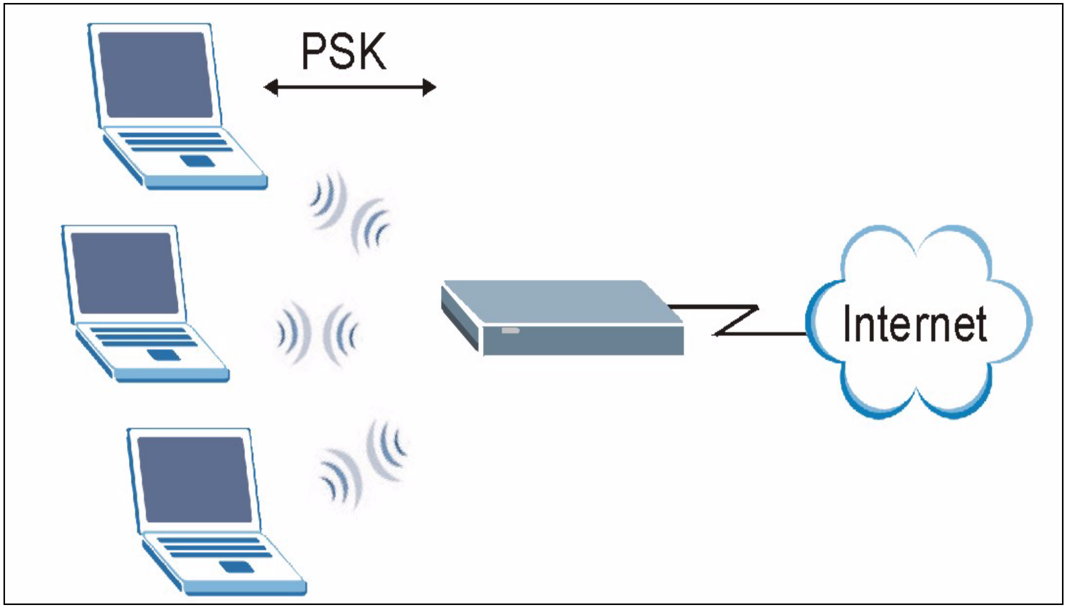
**Note:** You can't use the Local User Database for authentication when you select WPA(2).

## 6.6.1 WPA(2)-PSK Application Example

A WPA-PSK (or WPA2-PSK) application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).
2. The AP checks each client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 18** WPA(2) - PSK Authentication

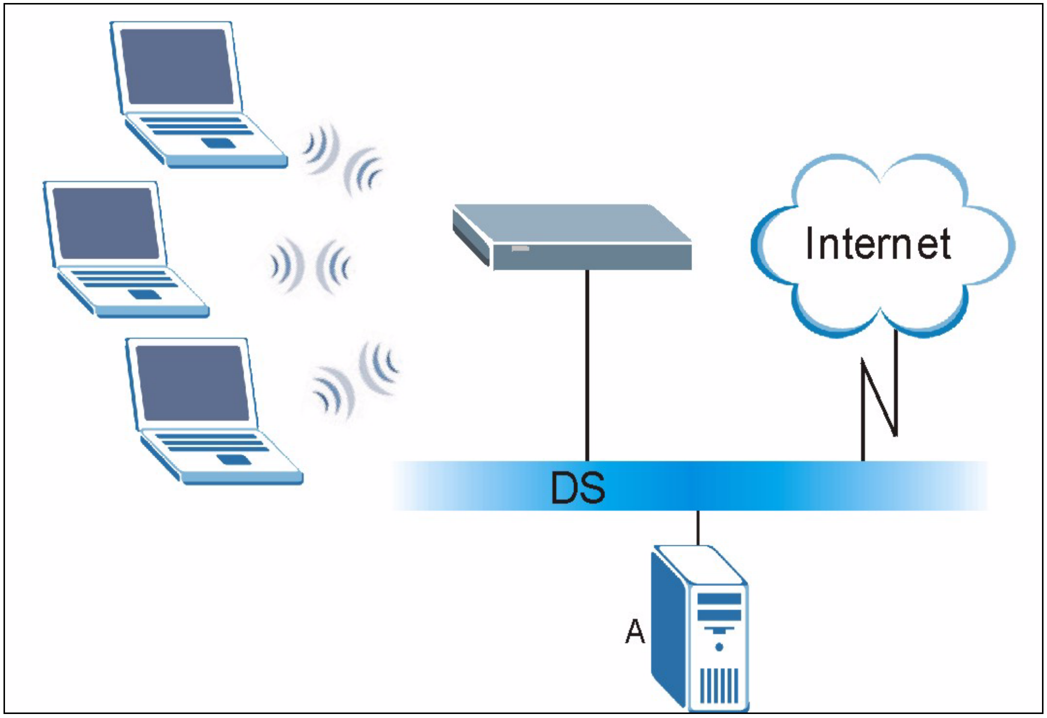


## 6.6.2 WPA(2) with RADIUS Application Example

You need the IP address, port number (default is 1812) and shared secret of a RADIUS server. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system (wired link to the LAN).

1. The AP passes the wireless client’s authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly transmitted between the AP and the wireless clients

**Figure 19** WPA with RADIUS Application Example2



## 6.6.3 Wireless Client WPA Supplicants

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

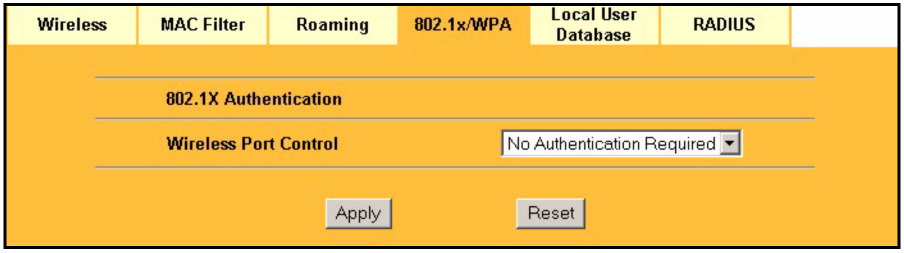
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

# 6.7 Configuring IEEE 802.1x and WPA

To change your G-1000’s authentication settings, click the **WIRELESS** link under **ADVANCED** and then the **802.1x/WPA** tab. The screen varies by the key management protocol you select.

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

**Figure 20** Wireless LAN: 802.1x/WPA



802.1X Authentication

Wireless Port Control: No Authentication Required

The following table describes the labels in this screen.

**Table 16** Wireless LAN: 802.1x/WPA

| LABEL | DESCRIPTION |
|---|---|
| Wireless Port Control | To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Access Allowed**, **No Authentication Required** and **Authentication Required**.<br>**No Access Allowed** blocks all wireless stations access to the wired network.<br>**No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.<br>**Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>Select **Authentication Required** to configure **Key Management Protocol** and other related fields. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

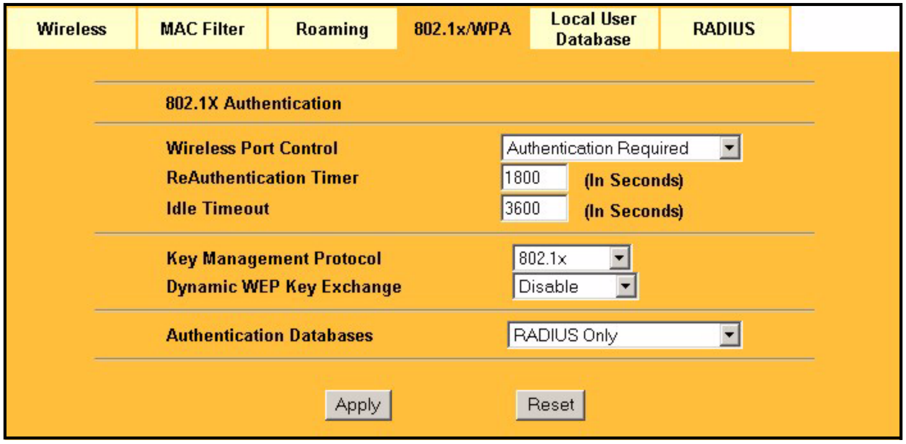
## 6.7.1 Authentication Required: 802.1x

You need the following for IEEE 802.1x authentication.

- A computer with an IEEE 802.11 b/g wireless LAN adapter and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see their documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.
- An optional network RADIUS server for remote user authentication and accounting.

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

**Figure 21** Wireless LAN: 802.1x/WPA for 802.1x Protocol



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

Authentication Databases: RADIUS Only

The following table describes the labels in this screen.

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

| LABEL | DESCRIPTION |
|---|---|
| Wireless Port Control | To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**.<br>**No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.<br>**Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>**No Access Allowed** blocks all wireless stations access to the wired network.<br>The following fields are only available when you select **Authentication Required**. |
| ReAuthentication Timer (In Seconds) | Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field.<br>Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes).<br>**Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (In Seconds) | The G-1000 automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour). |
| Key Management Protocol | Choose **802.1x** from the drop-down list. |

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

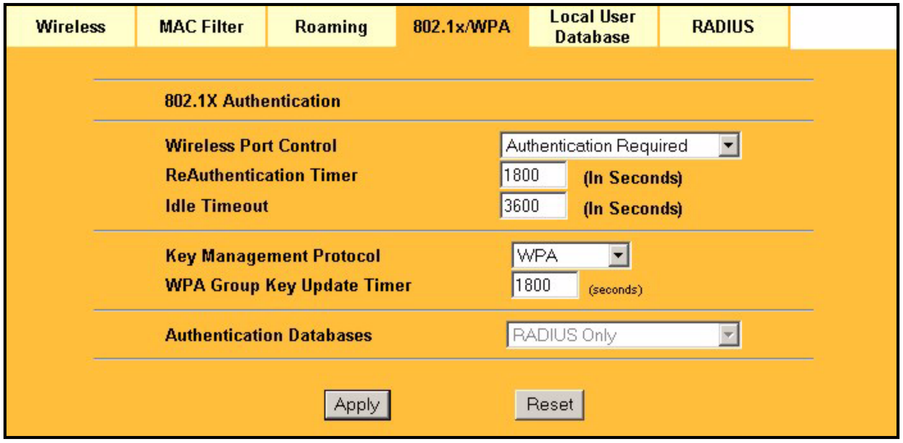
| LABEL | DESCRIPTION |
|---|---|
| Dynamic WEP Key Exchange | This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Key Management Protocol** field to **802.1x**.<br>Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption.<br>Up to 32 stations can access the G-1000 when you configure dynamic WEP key exchange.<br>This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**. |
| Authentication Databases | The authentication database contains wireless station login information. The local user database is the built-in database on the G-1000G-1000. The RADIUS is an external server. Use this drop-down list box to select which database the G-1000 should use (first) to authenticate a wireless station.<br>Before you specify the priority, make sure you have set up the corresponding database correctly first.<br>Select **Local User Database Only** to have the G-1000 just check the built-in user database on the G-1000 for a wireless station's username and password.<br>Select **RADIUS Only** to have the G-1000 just check the user database on the specified RADIUS server for a wireless station's username and password.<br>Select **Local first, then RADIUS** to have the G-1000 first check the user database on the G-1000 for a wireless station's username and password. If the user name is not found, the G-1000 then checks the user database on the specified RADIUS server.<br>Select **RADIUS first, then Local** to have the G-1000 first check the user database on the specified RADIUS server for a wireless station's username and password. If the G-1000 cannot reach the RADIUS server, the G-1000 then checks the local user database on the G-1000. When the user name is not found or password does not match in the RADIUS server, the G-1000 will not check the local user database and the authentication fails. |

**Note:** Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the G-1000 for authentication.

## 6.7.2 Authentication Required: WPA

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

**Figure 22** Wireless LAN: 802.1x/WPA for WPA Protocol



802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA
WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases: RADIUS Only

The following table describes the labels not previously discussed

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

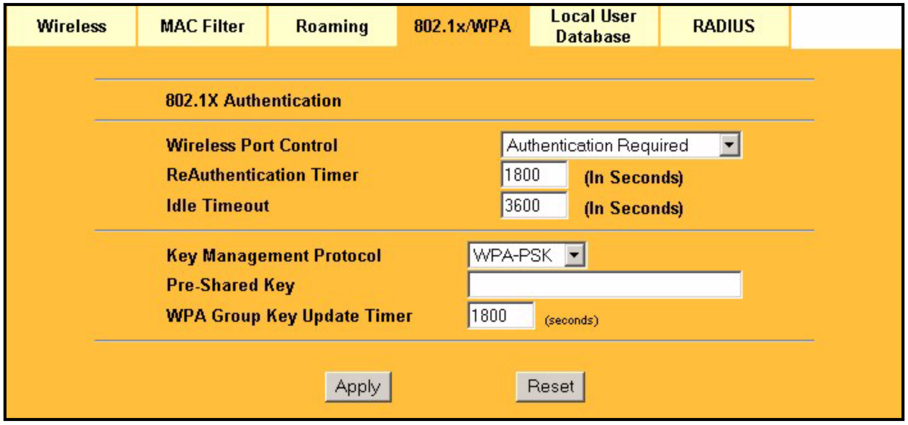
| LABEL | DESCRIPTIONS |
|---|---|
| Key Management Protocol | Choose **WPA** in this field. |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The G-1000 default is 1800 seconds (30 minutes). |
| Authentication Databases | This field is disabled. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

Please see Table 17 for information on the additional fields shown in this screen.

## 6.7.3 Authentication Required: WPA-PSK

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

**Figure 23** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol



802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA-PSK
Pre-Shared Key:
WPA Group Key Update Timer: 1800 (seconds)

The following table describes the labels not previously discussed

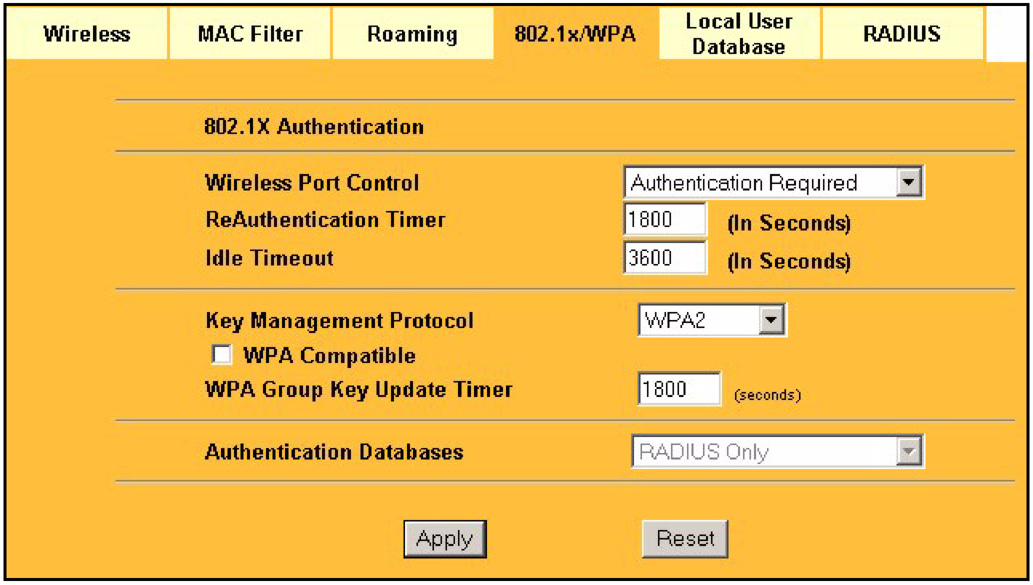
**Table 19** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

| LABEL | DESCRIPTION |
|---|---|
| Key Management Protocol | Choose **WPA-PSK** in this field. |
| Pre-Shared Key | The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The G-1000 default is 1800 seconds (30 minutes). |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.7.4 Authentication Required: WPA2

Select **Authentication Required** in the **Wireless Port Control** field and **WPA2** in the **Key Management Protocol** field to display the next screen.

**Figure 24** Wireless LAN: 802.1x/WPA for WPA2 Protocol



802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA2
□ WPA Compatible
WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases: RADIUS Only

The following table describes the labels not previously discussed

**Table 20** Wireless LAN: 802.1x/WPA2 for WPA Protocol

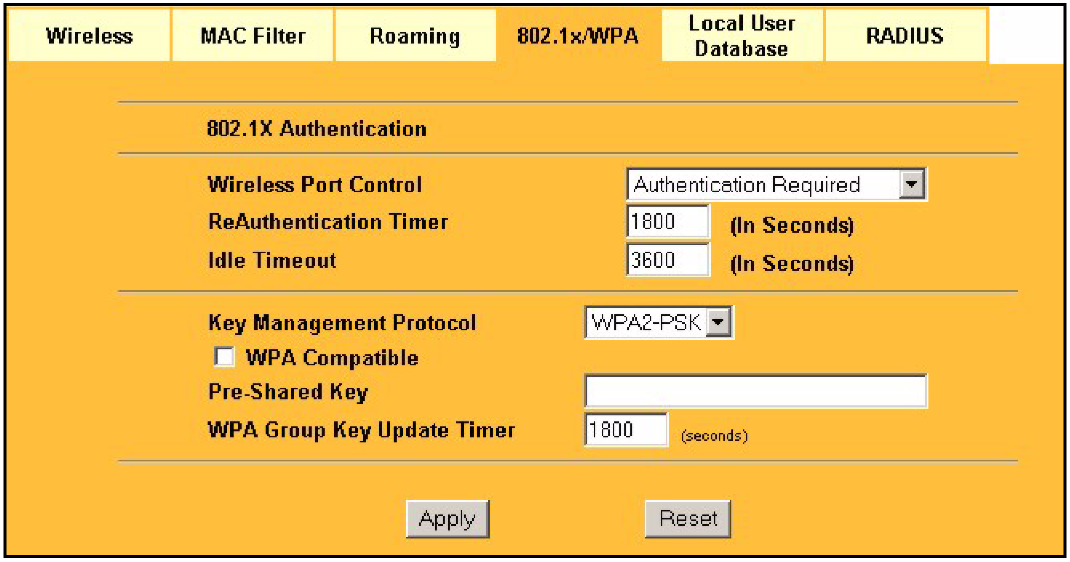
| LABEL | DESCRIPTIONS |
|---|---|
| Key Management Protocol | Choose **WPA2** in this field. |
| WPA Compatible | Check this box if you want your G-1000 to support WPA2 and WPA at the same time. This might reduce the performance of the device, however. |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA2-PSK** key management) or RADIUS server (if using **WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA2-PSK mode. The G-1000 default is 1800 seconds (30 minutes). |
| Authentication Databases | This field is disabled. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

Please see Table 17 for information on the additional fields shown in this screen.

## 6.7.5 Authentication Required: WPA2-PSK

Select **Authentication Required** in the **Wireless Port Control** field and **WPA2-PSK** in the **Key Management Protocol** field to display the next screen.

**Figure 25** Wireless LAN: 802.1x/WPA for WPA2-PSK Protocol



802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA2-PSK
□ WPA Compatible
Pre-Shared Key:
WPA Group Key Update Timer: 1800 (seconds)

The following table describes the labels not previously discussed

**Table 21** Wireless LAN: 802.1x/WPA for WPA2-PSK Protocol

| LABEL | DESCRIPTION |
|---|---|
| Key Management Protocol | Choose **WPA2-PSK** in this field. |
| WPA Compatible | Check this box if you want your G-1000 to support WPA2-PSK and WPA-PSK at the same time. This might reduce the performance of the device, however. |
| Pre-Shared Key | The encryption mechanisms used for **WPA2** and **WPA2-PSK** are the same. The only difference between the two is that **WPA2-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA2-PSK** key management) or RADIUS server (if using **WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA2-PSK mode. The G-1000 default is 1800 seconds (30 minutes). |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

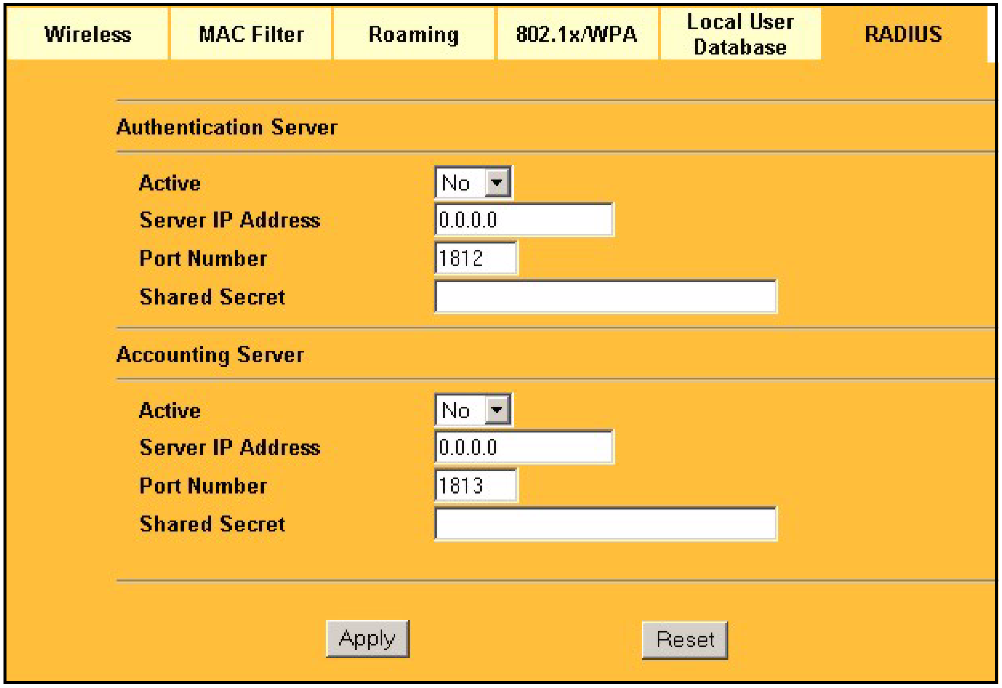
## 6.8 Configuring RADIUS

A RADIUS (Remote Authentication Dial In user Service) server enables user authentication, authorization and accounting. Use RADIUS if you want to authenticate users using an external server.

The **RADIUS** screen allows you to specify the authentication and accounting servers and to enable and disable them.

To access this screen, click the **WIRELESS** link under **ADVANCED** and then the **RADIUS** tab. The screen appears as shown.

**Figure 26** RADIUS Screen



Authentication Server

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

Accounting Server

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

The following table describes the labels in this screen.

**Table 22** RADIUS Screen

| LABEL | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Select whether or not the external RADIUS authentication server is active. |
| Server IP Address | Enter the IP address of the external RADIUS authentication server. |
| Port Number | Enter the port number used by the external RADIUS authentication server. |
| Shared Secret | Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the G-1000. This key is not sent over the network. This key must be the same on the external RADIUS server and the G-1000. |
| Accounting Server | |
| Active | Select whether or not the external RADIUS accounting server is active. |
| Server IP Address | Enter the IP address of the external RADIUS accounting server. |
| Port Number | Enter the port number used by the external RADIUS accounting server. |
| Shared Secret | Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the G-1000. This key is not sent over the network. This key must be the same on the external RADIUS server and the G-1000. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to set the RADIUS server settings again. |

# CHAPTER 7 IP Screen

This chapter discusses how to configure IP on the G-1000

## 7.1 TCP/IP Parameters

### 7.1.1 IP Address and Subnet Mask

See the IP Address and Subnet Mask section in the Wizard Setup chapter for this information. The Ethernet parameters of the G-1000 are preset in the factory with the following values:

- IP address of 192.168.1.2
- Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

### 7.1.2 WAN IP Address Assignment

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

**Table 23** Private IP Address Ranges

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

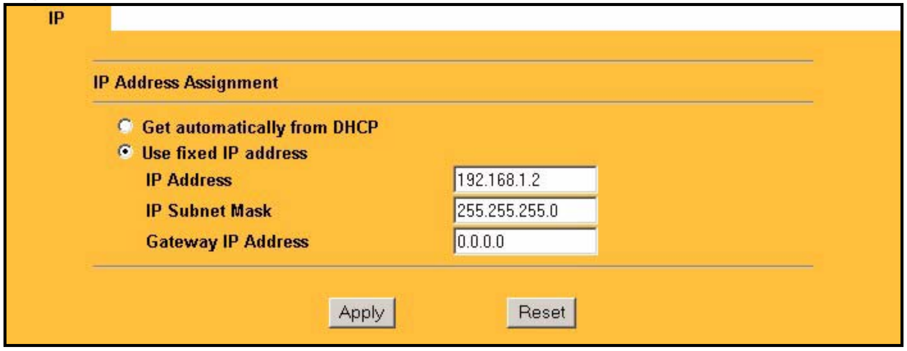
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much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

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

## 7.2 Configuring IP

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

**Figure 27** IP Setup



IP Address Assignment

○ Get automatically from DHCP
● Use fixed IP address

IP Address: 192.168.1.2
IP Subnet Mask: 255.255.255.0
Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

**Table 24** IP Setup

| LABEL | DESCRIPTION |
|---|---|
| IP Address Assignment | |
| Get automatically from DHCP | Select this option if your G-1000 is using a dynamically assigned IP address from a DHCP server each time.<br>**Note:** You must know the IP address assigned to the G-1000 (by the DHCP server) to access the G-1000 again. |
| Use fixed IP address | Select this option if your G-1000 is using a static IP address. When you select this option, fill in the fields below. |
| IP Address | Enter the IP address of your G-1000 in dotted decimal notation.<br>**Note:** If you change the G-1000's IP address, you must use the new IP address if you want to access the web configurator again. |
| IP Subnet Mask | Type the subnet mask. |
| Gateway IP Address | Type the IP address of the gateway. The gateway is an immediate neighbor of your G-1000 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your G-1000; over the WAN, the gateway must be the IP address of one of the remote node. |
| Apply | Click **Apply** to save your changes back to the G-1000. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 8 Remote Management Screens

This chapter provides information on the Remote Management screens.

## 8.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which G-1000 interface (if any) from which computers.

You may manage your G-1000 from a remote location via:

- WLAN only
- LAN only
- ALL (LAN and WLAN)
- Neither (Disable).

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

You may only have one remote management session running at a time. The G-1000 automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

### 8.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the G-1000 will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

### 8.1.2 Remote Management and NAT

When NAT is enabled:

- Use the G-1000’s WLAN IP address when configuring from the WLAN.
- Use the G-1000’s LAN IP address when configuring from the LAN.

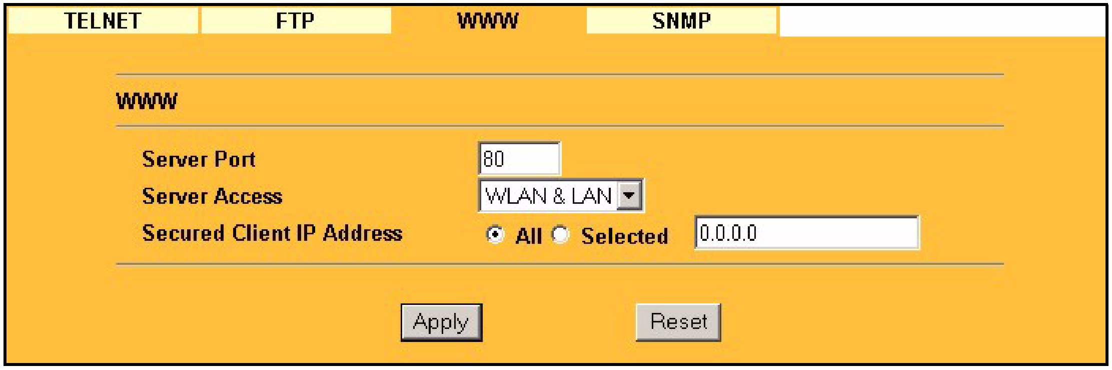
### 8.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The G-1000 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

## 8.2 Configuring WWW

To change your G-1000’s World Wide Web settings, click **REMOTE MGMT** to display the **WWW** screen.

**Figure 28** Remote Management: WWW



Server Port 80

Server Access WLAN & LAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

**Table 25** Remote Management: WWW

| LABEL | DESCRIPTION |
|---|---|
| WWW | |
| Server Port | You may change the server port number for a service, if needed; however, you must use the same port number in order to use this service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the G-1000 using this service. |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the G-1000 using this service.<br>Select **All** to allow any computer to access the G-1000 using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 using this service. |

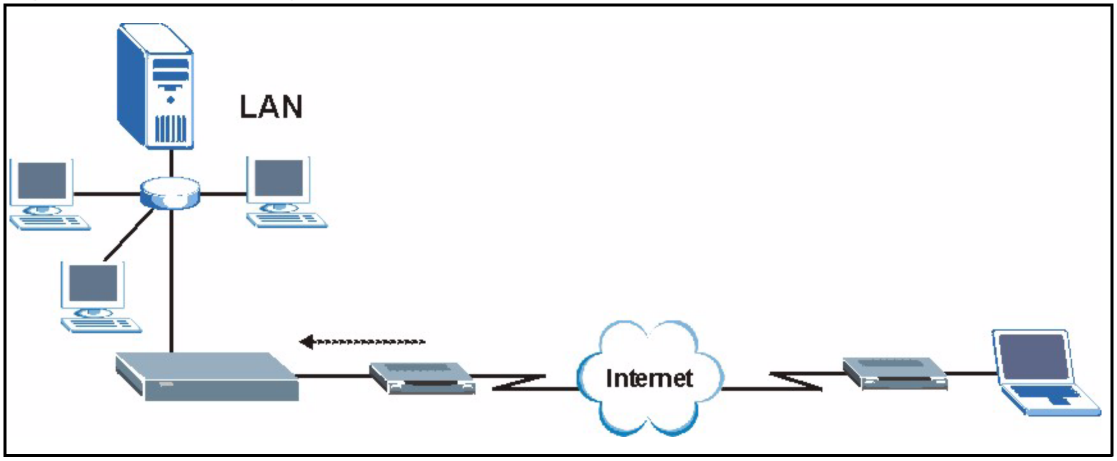
**Table 25** Remote Management: WWW

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.3 Configuring Telnet

You can configure your G-1000 for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the G-1000.

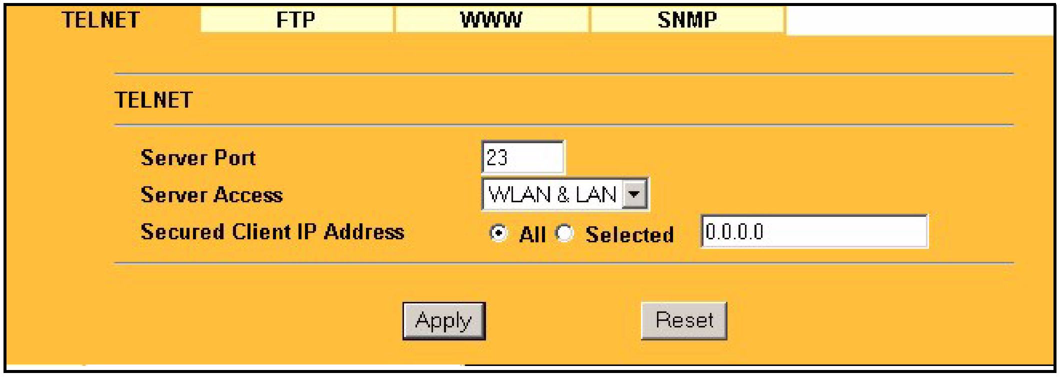
**Figure 29** Telnet Configuration on a TCP/IP Network



## 8.4 Configuring TELNET

Click **REMOTE MGMT** and the **TELNET** tab to display the screen as shown.

**Figure 30** Remote Management: Telnet



TELNET

Server Port: 23

Server Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

**Table 26** Remote Management: Telnet

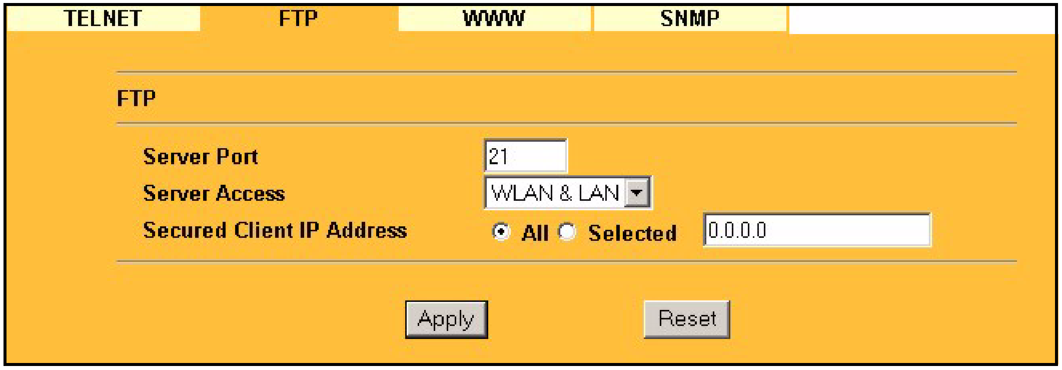
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service, if needed; however, you must use the same port number in order to use this service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the G-1000 using this service. |
| Secured Client IP Address | A secured client is a "trusted" computer that is allowed to communicate with the G-1000 using this service.<br>Select **All** to allow any computer to access the G-1000 using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.5 Configuring FTP

You can upload and download the G-1000's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your G-1000's FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

**Figure 31** Remote Management: FTP



FTP

Server Port: 21

Server Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

**Table 27** Remote Management: FTP

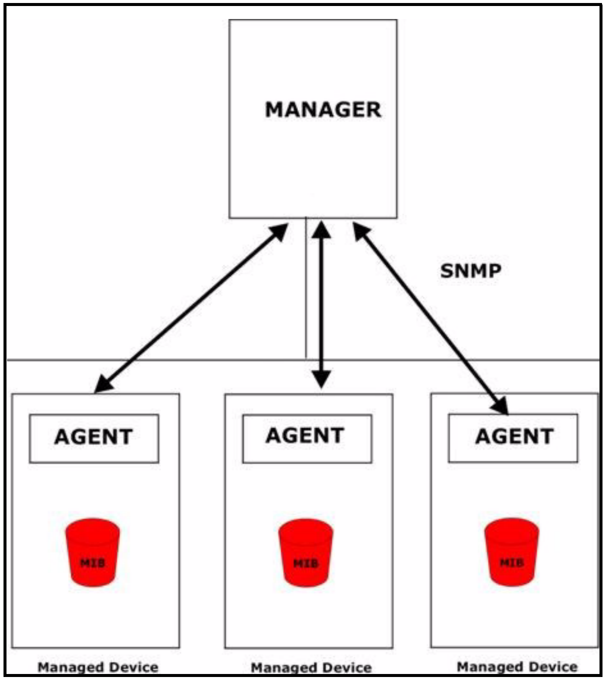
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service, if needed; however, you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the G-1000 using this service. |
| Secured Client IP Address | A secured client is a "trusted" computer that is allowed to communicate with the G-1000 using this service.<br>Select **All** to allow any computer to access the G-1000 using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 8.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your G-1000 supports SNMP agent functionality, which allows a manager station to manage and monitor the G-1000 through the network. The G-1000 supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

**Note:** SNMP is only available if TCP/IP is configured.

**Figure 32** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the G-1000). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

### 8.6.1 Supported MIBs

The G-1000 supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 8.6.2 SNMP Traps

The G-1000 can send the following traps to the SNMP manager.

**Table 28** SNMP Traps

| TRAP NAME | OBJECT IDENTIFIER # (OID) | DESCRIPTION |
|---|---|---|
| Generic Traps | | |
| coldStart | 1.3.6.1.6.3.1.1.5.1 | This trap is sent after booting (power on). This trap is defined in RFC-1215. |
| warmStart | 1.3.6.1.6.3.1.1.5.2 | This trap is sent after booting (software reboot). This trap is defined in RFC-1215. |
| linkDown | 1.3.6.1.6.3.1.1.5.3 | This trap is sent when the Ethernet link is down. |
| linkUp | 1.3.6.1.6.3.1.1.5.4 | This trap is sent when the Ethernet link is up. |
| authenticationFailure (defined in *RFC-1215*) | 1.3.6.1.6.3.1.1.5.5 | The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password).<br>Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps. |
| Traps defined in the ZyXEL Private MIB. | | |
| whyReboot | 1.3.6.1.4.1.890.1.5.13.0.1 | This trap is sent with the reason for restarting before the system reboots (warm start).<br>"System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot").<br>If the system reboots because of fatal errors, a code for the error is listed. |

## 8.6.3 SNMP Interface Index

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the G-1000's physical ports.

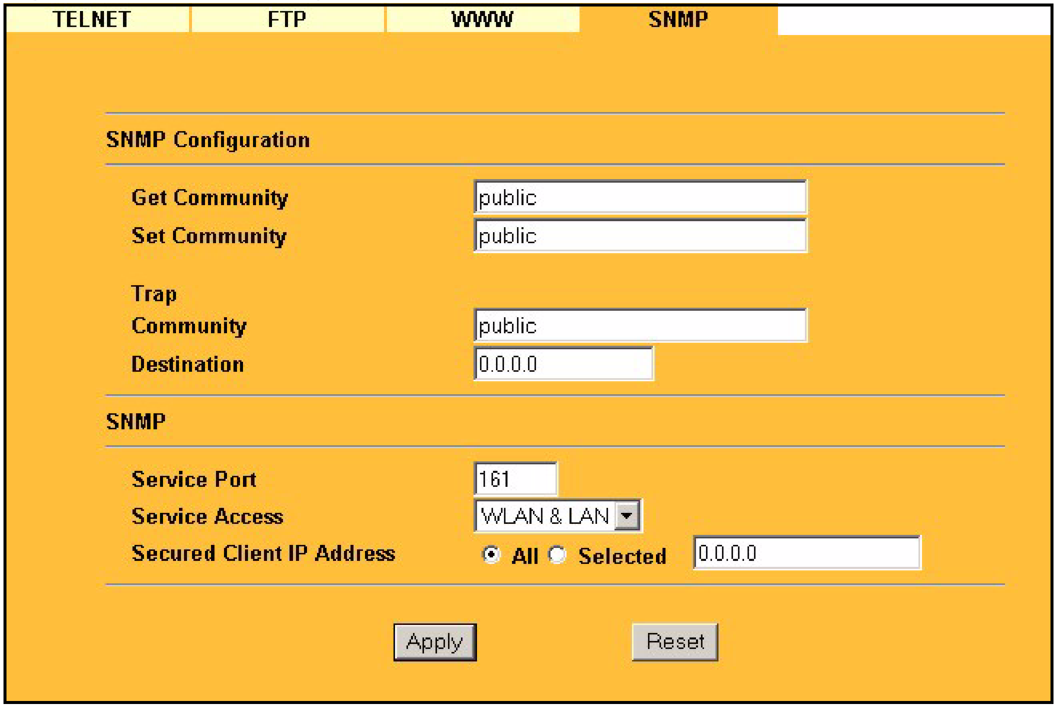
**Table 29** SNMP Interface Index to Physical Port Mapping

| INTERFACE TYPE | PHYSICAL PORT |
|---|---|
| enet0 | WLAN |
| enet1 | Ethernet port |

## 8.6.4 Configuring SNMP

To change your G-1000's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

**Figure 33** Remote Management: SNMP



SNMP Configuration

Get Community: public

Set Community: public

Trap

Community: public

Destination: 0.0.0.0

SNMP

Service Port: 161

Service Access: WLAN & LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

**Table 30** Remote Management: SNMP

| LABEL | DESCRIPTION |
|---|---|
| SNMP Configuration | |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |

**Table 30** Remote Management: SNMP

| LABEL | DESCRIPTION |
|---|---|
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests. |
| Trap | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| SNMP | |
| Service Port | You may change the server port number for a service, if needed; however, you must use the same port number in order to use that service for remote management. |
| Service Access | Select the interface(s) through which a computer may access the G-1000 using this service. |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the G-1000 using this service.<br>Select **All** to allow any computer to access the G-1000 using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# CHAPTER 9 Log Screens

This chapter contains information about configuring general log settings and viewing the G-1000's logs. Refer to the appendix for example log message explanations.

## 9.1 Configuring View Log

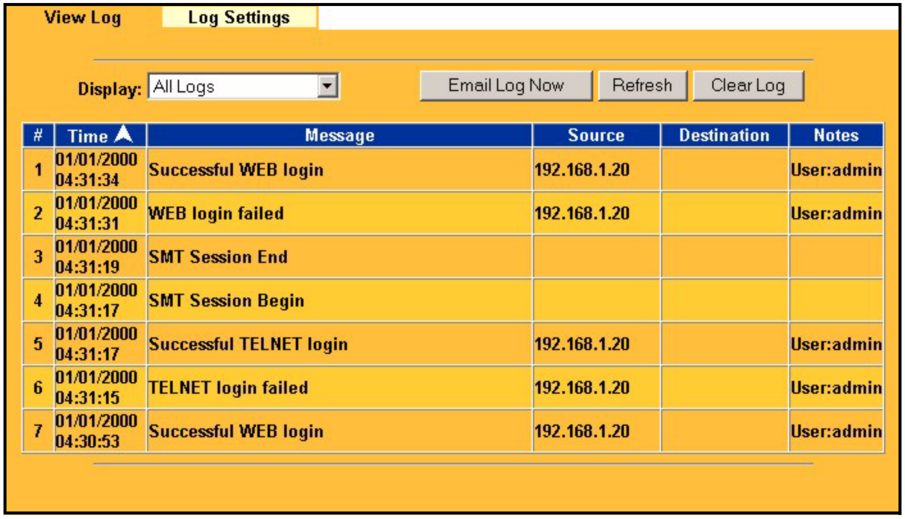
The web configurator allows you to look at all of the G-1000's logs in one location.

Click the **LOGS** links under **ADVANCED** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 35). Options include logs about system maintenance, system errors and access control.

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

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

**Figure 34   View Log**



| # | Time | Message | Source | Destination | Notes |
|---|---|---|---|---|---|
| 1 | 01/01/2000 04:31:34 | Successful WEB login | 192.168.1.20 | | User:admin |
| 2 | 01/01/2000 04:31:31 | WEB login failed | 192.168.1.20 | | User:admin |
| 3 | 01/01/2000 04:31:19 | SMT Session End | | | |
| 4 | 01/01/2000 04:31:17 | SMT Session Begin | | | |
| 5 | 01/01/2000 04:31:17 | Successful TELNET login | 192.168.1.20 | | User:admin |
| 6 | 01/01/2000 04:31:15 | TELNET login failed | 192.168.1.20 | | User:admin |
| 7 | 01/01/2000 04:30:53 | Successful WEB login | 192.168.1.20 | | User:admin |

The following table describes the labels in this screen.

**Table 31**   View Log

| LABEL | DESCRIPTION |
|---|---|
| Display | Select a log category from the drop down list box to display logs within the selected category. To view all logs, select **All Logs**.<br>The number of categories shown in the drop down list box depends on the selection in the **Log Settings** page. |
| Email Log Now | Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page. |
| Refresh | Click **Refresh** to renew the log screen. |
| Clear Log | Click **Clear Log** to clear all the logs. |
| Time | This field displays the time the log was recorded. |
| Message | This field states the reason for the log. |
| Source | This field lists the source IP address and the port number of the incoming packet. |
| Destination | This field lists the destination IP address and the port number of the incoming packet. |
| Notes | This field displays additional information about the log entry. |

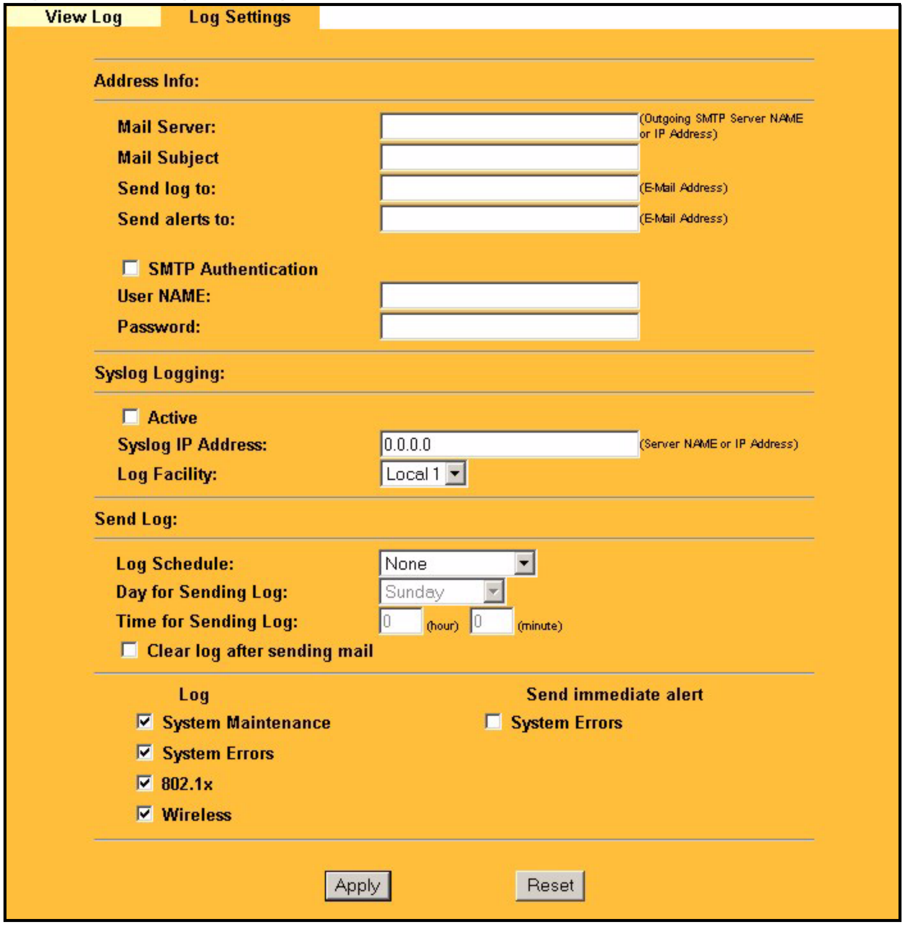
## 9.2 Configuring Log Settings

To change your G-1000’s log settings, click the **LOGS** links under **ADVANCED** and then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the G-1000 is to send the logs; the schedule for when the G-1000 is to send the logs and which logs and/or immediate alerts the G-1000 is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

**Figure 35 Log Settings**



Address Info:

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

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

□ SMTP Authentication

User NAME:

Password:

Syslog Logging:

□ Active

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

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

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

□ Clear log after sending mail

| Log | Send immediate alert |
|---|---|
| ☑ System Maintenance | □ System Errors |
| ☑ System Errors | |
| ☑ 802.1x | |
| ☑ Wireless | |

The following table describes the labels in this screen.

**Table 32** Log Settings

| LABEL | DESCRIPTION |
|---|---|
| Address Info | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the G-1000 sends. |
| Send log to | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |
| Send alerts to | Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail. |
| SMTP Authentication | Check this box if e-mail requires a user name and password to be delivered through the specified mail server. |

**Table 32** Log Settings

| LABEL | DESCRIPTION |
|---|---|
| User NAME | This field is effective if **SMTP Authentication** is checked. Enter the user name of the account on the SMTP server. |
| Password | This field is effective if **SMTP Authentication** is checked. Enter the password of the account on the SMTP server. |
| Syslog Logging | Syslog logging sends a log to an external syslog server used to store logs. |
| Active | Click **Active** to enable syslog logging. |
| Syslog Server IP Address | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Send Log | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>• Daily<br>• Weekly<br>• Hourly<br>• When Log is Full<br>• None.<br>If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent. |
| Day for Sending Log | This field is only available when you select **Weekly** in the **Log Schedule** field.<br>Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| Clear log after sending mail | Select the check box to clear all logs after logs and alert messages are sent via e-mail. |
| Log | Select the categories of logs that you want to record. |
| Send Immediate Alert | Select the categories of alerts for which you want the G-1000 to immediately send e-mail alerts. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to reconfigure all the fields in this screen. |

# CHAPTER 10 Maintenance

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

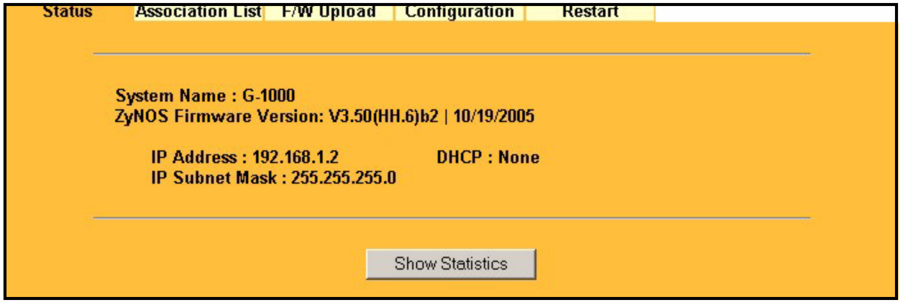
## 10.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your G-1000.

## 10.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your G-1000. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

**Figure 36** System Status



System Name : G-1000
ZyNOS Firmware Version: V3.50(HH.6)b2 | 10/19/2005

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

The following table describes the labels in this screen.

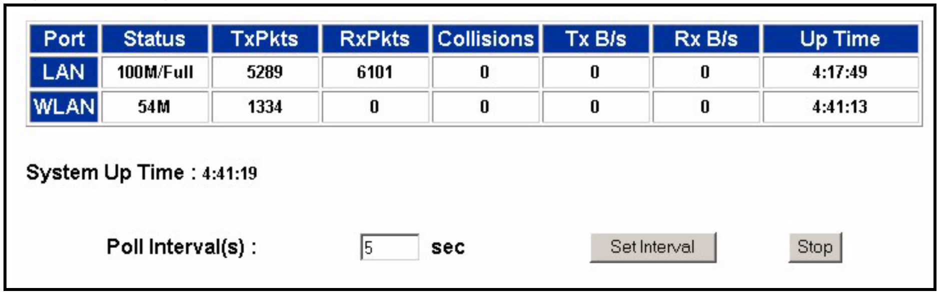
**Table 33** System Status

| LABEL | DESCRIPTION |
|---|---|
| System Name | This is the **System Name** you enter in the first Internet Access Wizard screen. It is for identification purposes |
| ZyNOS Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. |
| IP Address | This is the Ethernet port IP address. |
| IP Subnet Mask | This is the Ethernet port subnet mask. |
| DHCP | This is the Ethernet port DHCP role - **Client** or **None**. |
| Show Statistics | Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port. |

### 10.2.1 System Statistics

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

**Figure 37 System Status: Show Statistics**



| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|---|---|---|---|---|---|---|---|
| LAN | 100M/Full | 5289 | 6101 | 0 | 0 | 0 | 4:17:49 |
| WLAN | 54M | 1334 | 0 | 0 | 0 | 0 | 4:41:13 |

System Up Time : 4:41:19

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

**Table 34** System Status: Show Statistics

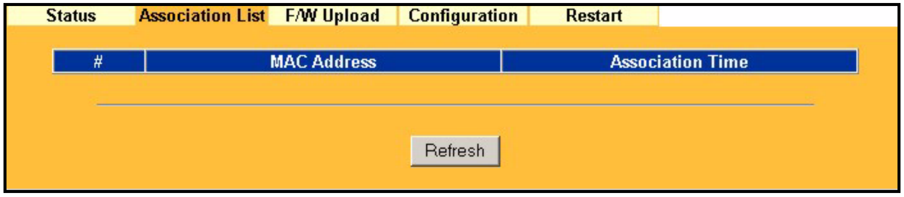
| LABEL | DESCRIPTION |
|---|---|
| Port | This is the Ethernet or wireless port. The wireless port may be the **WLAN – Built-in** card or the **WLAN – Removable** wireless card. |
| Status | This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port.<br>This shows the transmission speed only for wireless port. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Collisions | This is the number of collisions on this port. |
| Tx B/s | This shows the transmission speed in bytes per second on this port. |
| Rx B/s | This shows the reception speed in bytes per second on this port. |
| Up Time | This is total amount of time the line has been up. |
| System Up Time | This is the total time the G-1000 has been on. |
| Poll Interval(s) | Enter the time interval for refreshing statistics. |
| Set Interval | Click this button to apply the new poll interval you entered above. |
| Stop | Click this button to stop refreshing statistics. |

## 10.3 Association List

View the wireless stations that are currently associated to the G-1000 in the **Association List** screen.

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

**Figure 38 Association List**



| # | MAC Address | Association Time |
|---|---|---|

The following table describes the labels in this screen.

**Table 35** Association List

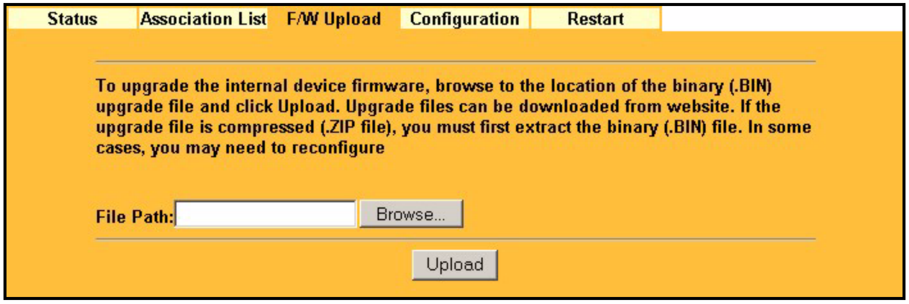
| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of an associated wireless station. |
| MAC Address | This field displays the MAC address of an associated wireless station. |
| Association Time | This field displays the time a wireless station first associated with the G-1000. |
| Refresh | Click **Refresh** to reload the screen. |

## 10.4 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "G-1000.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** and then **F/W Upload**. Follow the instructions in this screen to upload firmware to your G-1000.

**Figure 39   Firmware Upload**



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

File Path:

The following table describes the labels in this screen.

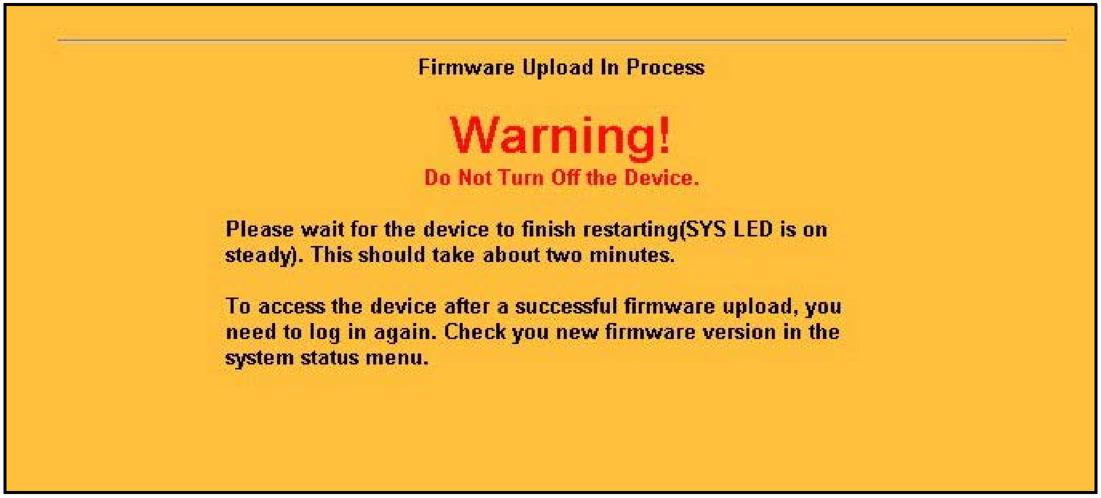
**Table 36**   Firmware Upload

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

**Note:** Do not turn off the G-1000 while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the G-1000 again.

**Figure 40   Firmware Upload In Process**



Firmware Upload In Process

Warning!

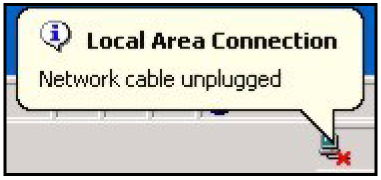
Do Not Turn Off the Device.

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

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

The G-1000 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 41 Network Temporarily Disconnected**



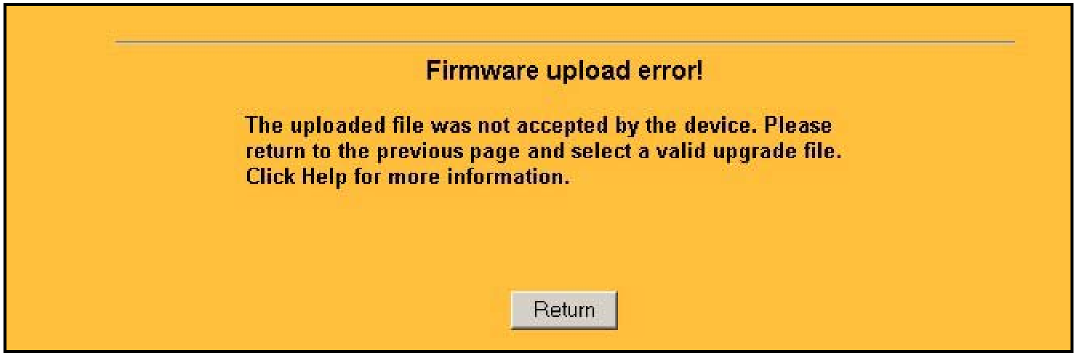
Local Area Connection

Network cable unplugged

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

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

**Figure 42 Firmware Upload Error**



Firmware upload error!

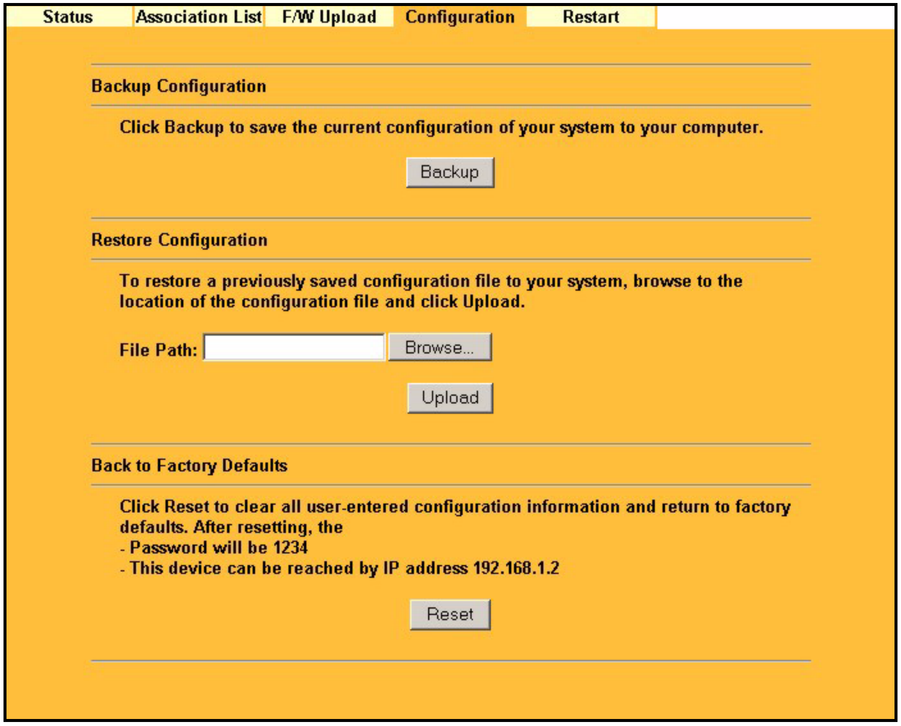
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

## 10.5 Configuration Screen

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

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

**Figure 43 Configuration**



Backup Configuration

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

Restore Configuration

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

File Path:

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- This device can be reached by IP address 192.168.1.2

## 10.5.1 Backup Configuration

Backup configuration allows you to back up (save) the G-1000's current configuration to a file on your computer. Once your G-1000 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the G-1000's current configuration to your computer.

## 10.5.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your G-1000.

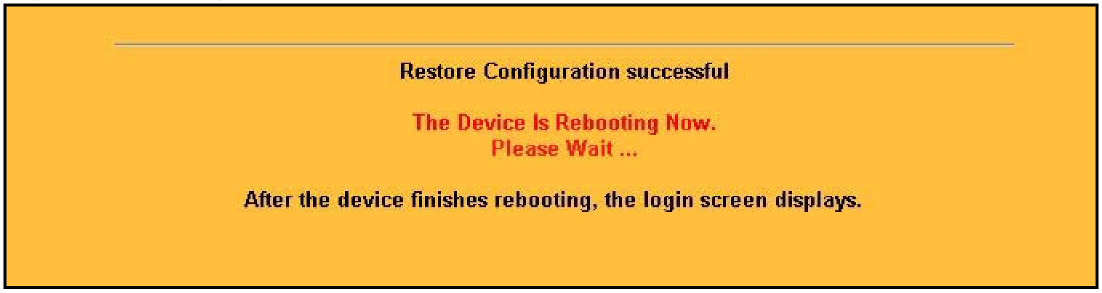
**Table 37** Restore Configuration

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

**Note:** Do not turn off the G-1000 while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the G-1000 again.

**Figure 44 Configuration Upload Successful**



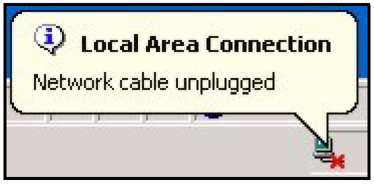
Restore Configuration successful

The Device Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The G-1000 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 45 Network Temporarily Disconnected**

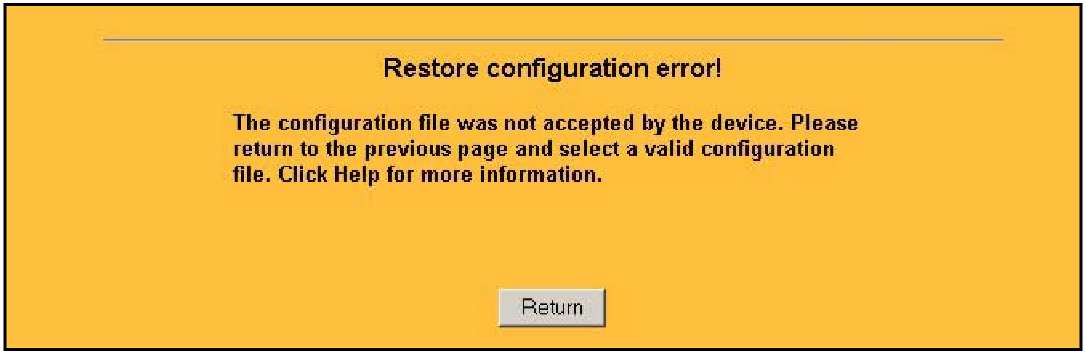


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default G-1000 IP address (192.168.1.2). See your *Quick Installation Guide* for details on how to set up your computer's IP address.

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

Figure 46   Configuration Upload Error



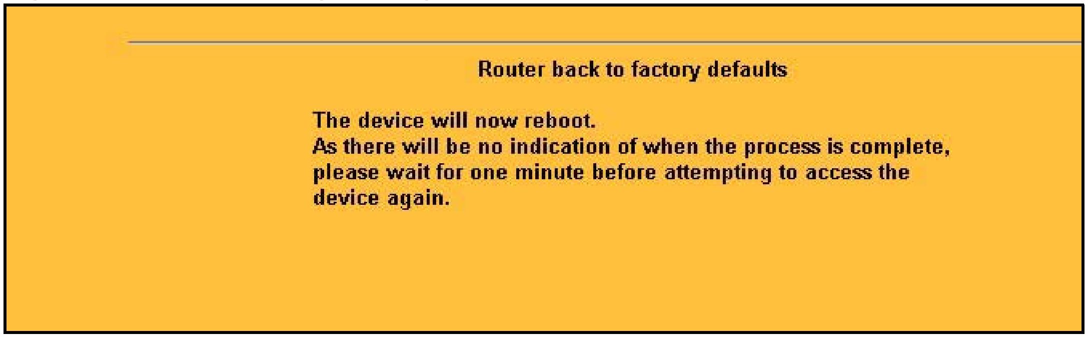
Restore configuration error!

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

### 10.5.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the G-1000 to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 47   Reset Warning Message



Router back to factory defaults

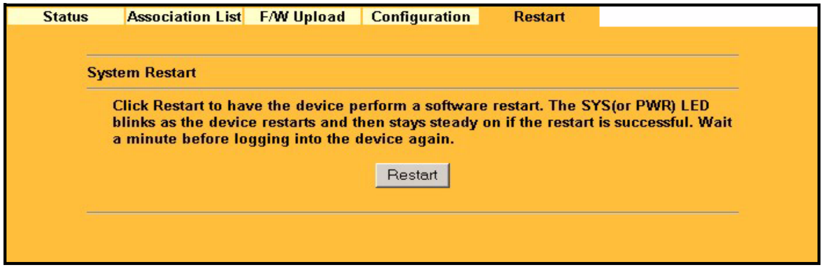
The device will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

You can also press the **RESET** button on the side panel to reset the factory defaults of your G-1000. Refer to the section on resetting the G-1000 for more information on the **RESET** button.

## 10.6 Restart Screen

System restart allows you to reboot the G-1000 without turning the power off. Click **MAINTENANCE**, and then click **Restart** to have the G-1000 reboot. This does not affect the G-1000's configuration.

Figure 48   Restart Screen



System Restart

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

# Chapter 11
# Introducing the SMT

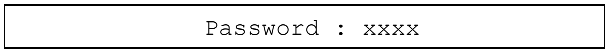
This chapter describes how to access the SMT and provides an overview of its menus.

## 11.1 Connect to your G-1000 Using Telnet

The following procedure details how to telnet into your G-1000.

1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.2" (the default IP address) and click **OK**.
2. For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "*" for each character you type.

**Figure 49** Login Screen



```
Password : xxxx
```

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

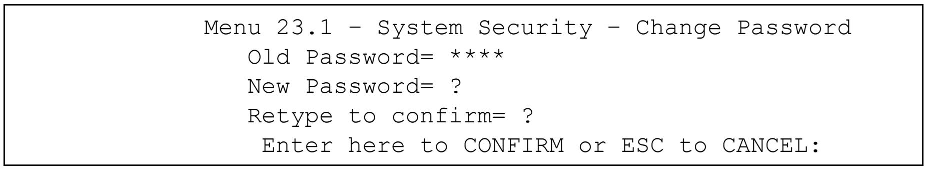
Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your G-1000 will automatically log you out. You will then have to telnet into the G-1000 again. You can use the web configurator or the CI commands to change the inactivity time out period.

## 11.2 Changing the System Password

Change the G-1000 default password by following the steps shown next.

1. From the main menu, enter 23 to display **Menu 23 – System Security**.
2. Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.
3. Type your existing system password in the **Old Password** field, and press [ENTER].

**Figure 50   Menu 23.1 System Security: Change Password**



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

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

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

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

## 11.3 G-1000 SMT Menus Overview

The following table gives you an overview of your G-1000's various SMT menus.

**Table 38**   SMT Menus Overview

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 1 General Setup | 1.1 Configure Dynamic DNS | | |
| 3 LAN Setup | 3.2 TCP/IP Setup | | |
| | 3.5 Wireless LAN Setup | 3.5.1 WLAN MAC Address Filter | |
| | | 3.5.2 Roaming Configuration | |
| 14 Dial-in User Setup | 14.1 Edit Dial-in User | | |
| 22 SNMP Configuration | | | |
| 23 System Security | 23.1 Change Password | | |
| | 23.2 RADIUS Server | | |
| | 23.4 IEEE 802.1X | | |

**Table 38** SMT Menus Overview (continued)

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 24 System Maintenance | 24.1 Status | | |
| | 24.2 System Information and Console Port Speed | 24.2.1 Information | |
| | | 24.2.2 Change Console Port Speed | |
| | 24.3 Log and Trace | 24.3.1 View Error Log | |
| | 24.4 Diagnostic | | |
| | 24.5 Backup Configuration | | |
| | 24.6 Restore Configuration | | |
| | 24.7 Upload Firmware | 24.7.1 Upload System Firmware | |
| | | 24.7.2 Upload System Configuration File | |
| | 24.8 Command Interpreter Mode | | |
| | 24.10 Time and Date Setting | | |
| | 24.11 Remote Management Control | | |

## 11.4 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your G-1000. Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 39** Main Menu Commands

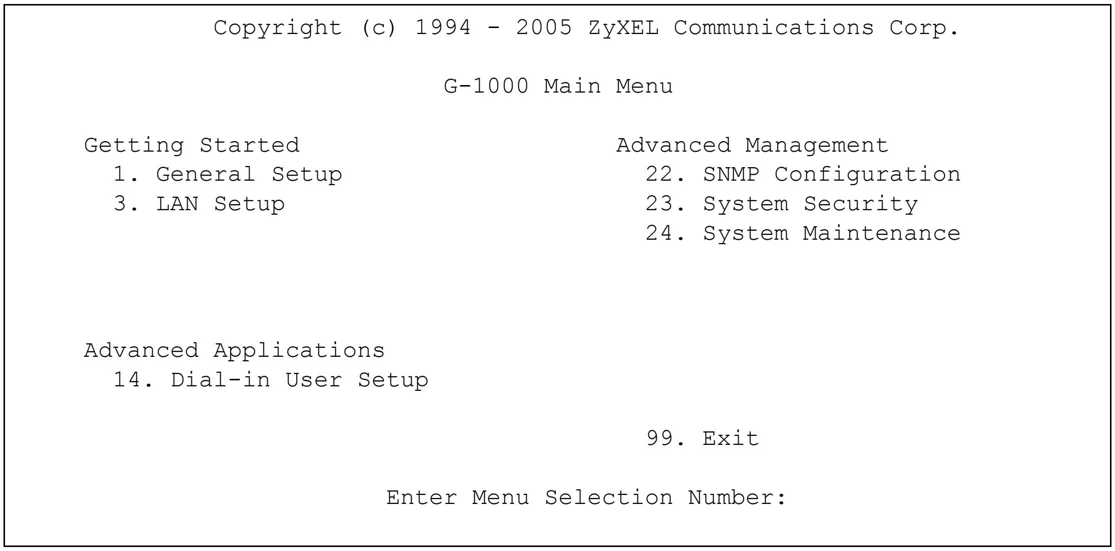
| OPERATION | KEYSTROKE | DESCRIPTION |
|---|---|---|
| Move down to another menu | [ENTER] | To move forward to a submenu, type in the number of the desired submenu and press [ENTER]. |
| Move up to a previous menu | [ESC] | Press [ESC] to move back to the previous menu. |
| Move to a "hidden" menu | Press [SPACE BAR] to change **No** to **Yes** then press [ENTER]. | Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu. |
| Move the cursor | [ENTER] or [UP]/[DOWN] arrow keys. | Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively. |
| Entering information | Type in or press [SPACE BAR], then press [ENTER]. | You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR]. |
| Required fields | <?> or **ChangeMe** | All fields with the symbol <?> must be filled in order to be able to save the new configuration.<br>All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration. |

**Table 39** Main Menu Commands

| OPERATION | KEYSTROKE | DESCRIPTION |
|---|---|---|
| N/A fields | <N/A> | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable. |
| Save your configuration | [ENTER] | Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu. |
| Exit the SMT | Type 99, then press [ENTER]. | Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface. |

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

**Figure 51 G-1000 SMT Main Menu**



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

                              G-1000 Main Menu

     Getting Started                     Advanced Management
       1. General Setup                    22. SNMP Configuration
       3. LAN Setup                        23. System Security
                                           24. System Maintenance



     Advanced Applications
       14. Dial-in User Setup

                                           99. Exit

                          Enter Menu Selection Number:
```

This menu is summarized below.

**Table 40** Main Menu Summary

| # | MENU TITLE | DESCRIPTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up your general information. |
| 3 | LAN Setup | Use this menu to set up your LAN and WLAN connection. |
| 14 | Dial-in User Setup | Use this menu to set up local user profiles on the G-1000. |
| 22 | SNMP Configuration | Use this menu to set up SNMP related parameters. |
| 23 | System Security | Use this menu to change your password and enable network user authentication. |
| 24 | System Maintenance | This menu provides system status, diagnostics, software upload, etc. |
| 99 | Exit | Use this to exit from SMT and return to a blank screen. |

# CHAPTER 12
# General Setup

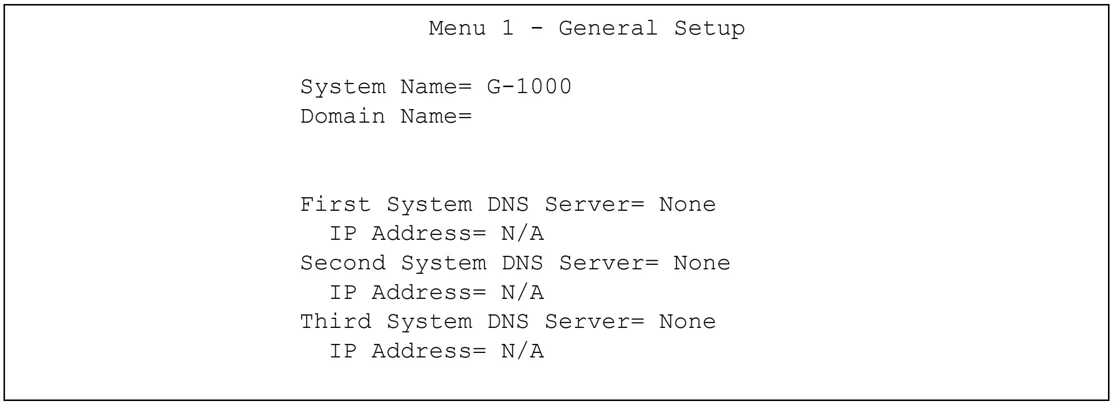
The chapter shows you the information on general setup.

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

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the G-1000 via DHCP.

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

**Figure 52** Menu 1 General Setup



```
                          Menu 1 - General Setup

                 System Name= G-1000
                 Domain Name=


                 First System DNS Server= None
                   IP Address= N/A
                 Second System DNS Server= None
                   IP Address= N/A
                 Third System DNS Server= None
                   IP Address= N/A
```

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

**Table 41** Menu 1 General Setup

| FIELD | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores "_" are accepted. |
| Domain Name | This is not a required field. Leave this field blank or enter the domain name here if you know it. |
| First/Second/Third System DNS Server | Press [SPACE BAR] to select **From DHCP**, **User Defined** or **None** and press [ENTER].<br>These fields are not available on all models. |

**Table 41** Menu 1 General Setup

| FIELD | DESCRIPTION |
|---|---|
| IP Address | Enter the IP addresses of the DNS servers. This field is available when you select **User-Defined** in the field above. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

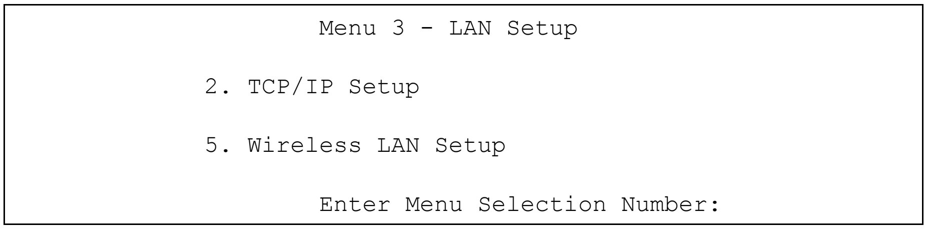
# CHAPTER 13 LAN Setup

This chapter shows you how to configure the LAN on your G-1000.

## 13.1 LAN Setup

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

**Figure 53   Menu 3 LAN Setup**



```
                      Menu 3 - LAN Setup

              2. TCP/IP Setup

              5. Wireless LAN Setup

                      Enter Menu Selection Number:
```

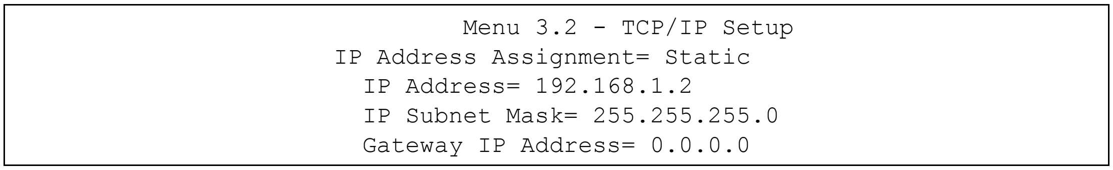
Detailed explanation about the LAN Setup menu is given in the next chapter.

## 13.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your G-1000 for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3-LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP Setup**, as shown next:

**Figure 54   Menu 3.2 TCP/IP Setup**



```
                                 Menu 3.2 - TCP/IP Setup
                        IP Address Assignment= Static
                          IP Address= 192.168.1.2
                          IP Subnet Mask= 255.255.255.0
                          Gateway IP Address= 0.0.0.0
```

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

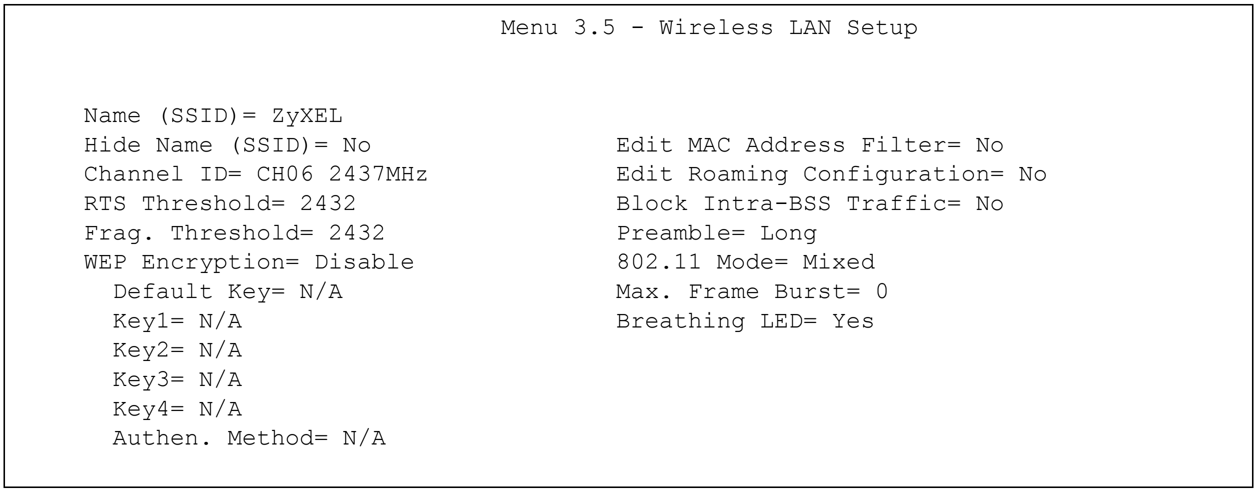
**Table 42**   Menu 3.2 TCP/IP Setup

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | Press [SPACE BAR] and then [ENTER] to select **Dynamic** to have the G-1000 obtain an IP address from a DHCP server. You must know the IP address assigned to the G-1000 (by the DHCP server) to access the G-1000 again.<br>Select **Static** to give the G-1000 a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable. |
| IP Address | Enter the (LAN) IP address of your G-1000 in dotted decimal notation |
| IP Subnet Mask | Your G-1000 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the G-1000. |
| Gateway IP Address | Type the IP address of the gateway. The gateway is an immediate neighbor of your G-1000 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your G-1000. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 13.3  Wireless LAN Setup

Use menu 3.5 to set up your G-1000 as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

**Figure 55** Menu 3.5 Wireless LAN Setup



```
                              Menu 3.5 - Wireless LAN Setup


     Name (SSID)= ZyXEL
     Hide Name (SSID)= No                 Edit MAC Address Filter= No
     Channel ID= CH06 2437MHz             Edit Roaming Configuration= No
     RTS Threshold= 2432                  Block Intra-BSS Traffic= No
     Frag. Threshold= 2432                Preamble= Long
     WEP Encryption= Disable              802.11 Mode= Mixed
       Default Key= N/A                   Max. Frame Burst= 0
       Key1= N/A                          Breathing LED= Yes
       Key2= N/A
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A
```

**Note:** In the SMT, the ESSID is referred to as SSID. Both of them refer to the same ID for the G-1000.

The following table describes the fields in this menu.

**Table 43** Menu 3.5 Wireless LAN Setup

| FIELD | DESCRIPTION |
|---|---|
| Name (SSID) | The SSID (Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same SSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.<br>This field is only available when you select **Access Point** or **AP + Bridge** in the **Operating Mode** field. |
| Hide Name (SSID) | Press [SPACE BAR] and select **Yes** to hide the SSID in the outgoing data frame so an intruder cannot obtain the SSID through passive scanning. |
| Channel ID | Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/ channel depending on your particular region. |
| RTS Threshold | Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432. |
| Frag. Threshold | This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. |
| WEP Encryption | Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Default Key | Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the G-1000 and the wireless stations to communicate. |

**Table 43** Menu 3.5 Wireless LAN Setup

| FIELD | DESCRIPTION |
|---|---|
| Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the G-1000 and the wireless stations must use the same WEP key for data transmission.<br>If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>**Note:** Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key. |
| Authen. Method | Press [SPACE BAR] to select **Auto**, **Open System Only** or **Shared Key Only** and press [ENTER].<br>This field is **N/A** if WEP is not activated.<br>If WEP encryption is activated, the default setting is **Auto**. |
| Edit MAC Address Filter | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.1 - WLAN MAC Address Filter**. |
| Edit Roaming Configuration | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.2 - Roaming Configuration**. |
| Block Intra-BSS Traffic | Intra-BSS traffic is traffic between wireless stations in the same BSS. Select **No** to allow Intra-BSS traffic, select **Yes** to block all Intra-BSS traffic. |
| Preamble | Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** and **Dynamic**. The default setting is **Long**.<br>See the section on preamble for more information. |
| 802.11 Mode | Select **B Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-1000.<br>Select **G Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-1000.<br>Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the G-1000. The transmission rate of your G-1000 might be reduced. |
| Max. Frame Burst | Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the G-1000 transmits IEEE 802.11g wireless traffic only.<br>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. |
| Breathing LED | Select Yes to enable the Breathing LED, also known as the G-1000 LED.<br>The blue G-1000 LED is on when the G-1000 is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the G-1000 is on and data is being transmitted/received. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

## 13.3.1 Configuring MAC Address Filter

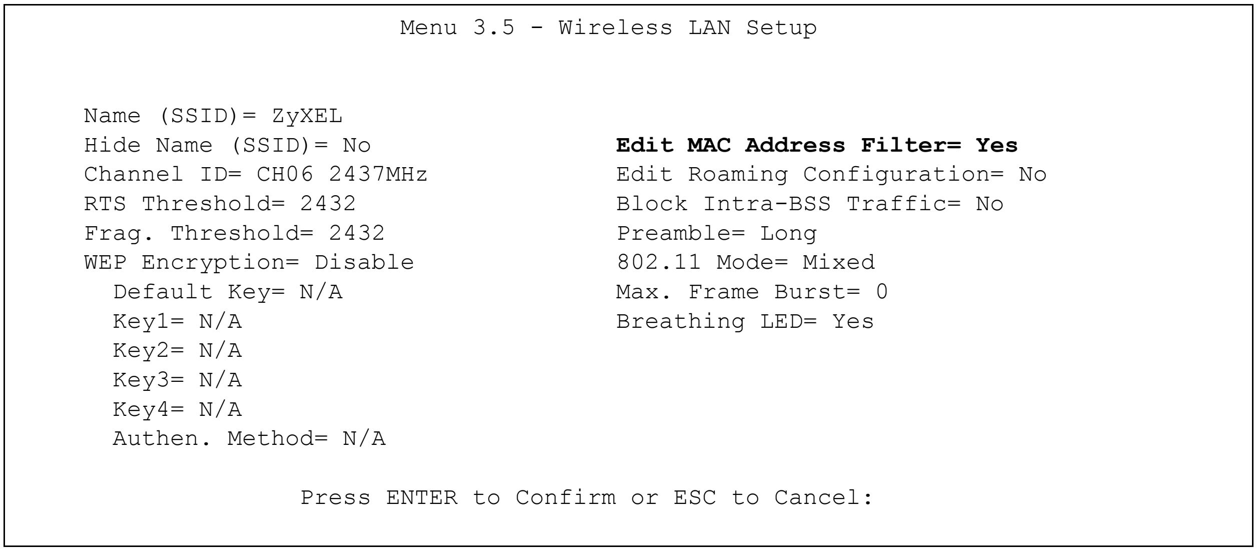
Your G-1000 checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your G-1000.

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

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

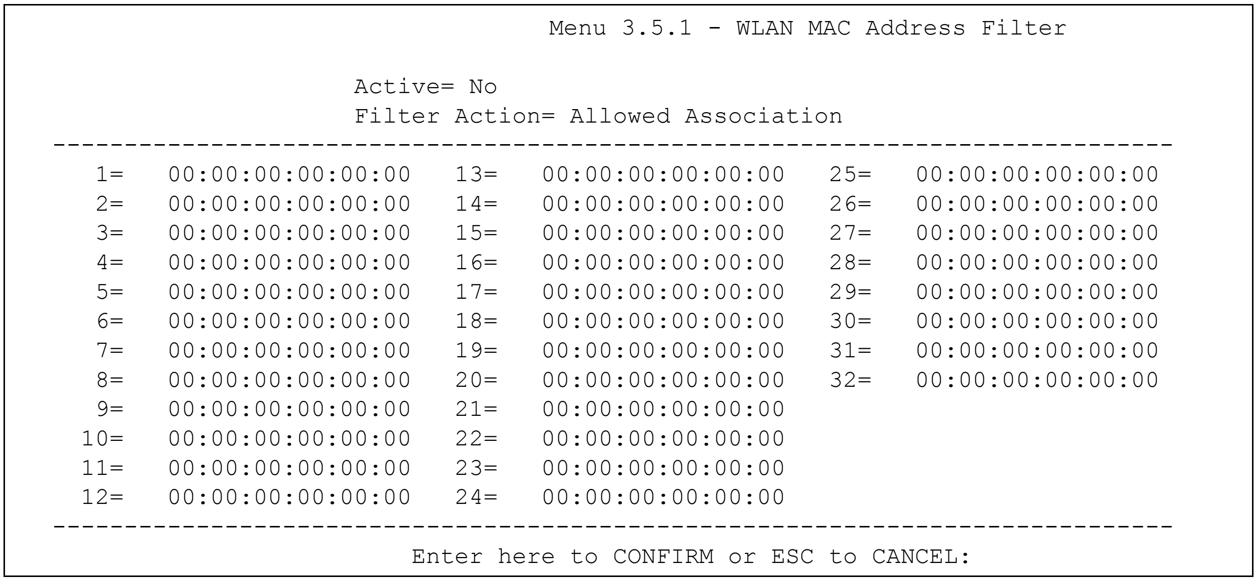
**Figure 56 Menu 3.5 Wireless LAN Setup**



```
                        Menu 3.5 - Wireless LAN Setup


  Name (SSID)= ZyXEL
  Hide Name (SSID)= No                 Edit MAC Address Filter= Yes
  Channel ID= CH06 2437MHz             Edit Roaming Configuration= No
  RTS Threshold= 2432                  Block Intra-BSS Traffic= No
  Frag. Threshold= 2432                Preamble= Long
  WEP Encryption= Disable              802.11 Mode= Mixed
    Default Key= N/A                   Max. Frame Burst= 0
    Key1= N/A                          Breathing LED= Yes
    Key2= N/A
    Key3= N/A
    Key4= N/A
    Authen. Method= N/A

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

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

**Figure 57 Menu 3.5.1 WLAN MAC Address Filter**



```
                                   Menu 3.5.1 - WLAN MAC Address Filter

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

The following table describes the fields in this menu.

**Table 44** Menu 3.5.1 WLAN MAC Address Filter

| FIELD | DESCRIPTION |
|---|---|
| Active | To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER]. |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>To deny access to the G-1000, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router.<br>The default action, **Allowed Association**, permits association with the G-1000. MAC addresses not listed will be denied access to the router. |
| MAC Address Filter | |
| 1..32 | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the G-1000 in these address fields. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

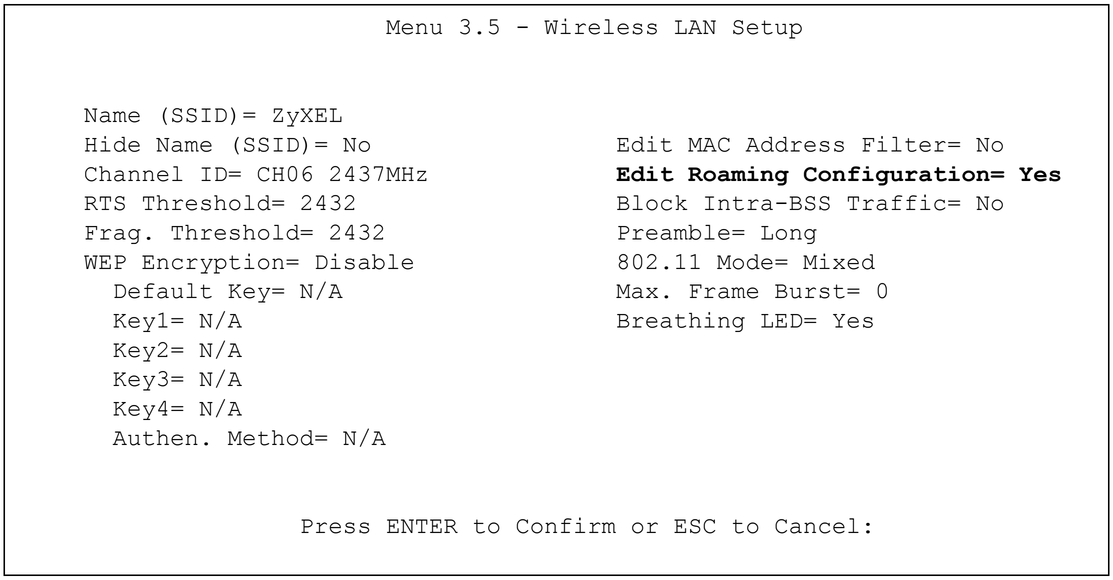
## 13.3.2 Configuring Roaming

Enable the roaming feature if you have two or more G-1000s on the same subnet. Follow the steps below to allow roaming on your G-1000.

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

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

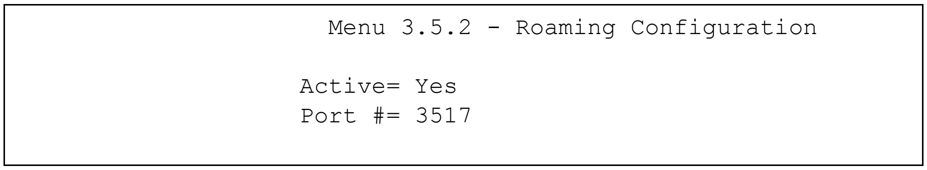
**Figure 58 Menu 3.5 Wireless LAN Setup**



```
                         Menu 3.5 - Wireless LAN Setup


    Name (SSID)= ZyXEL
    Hide Name (SSID)= No                 Edit MAC Address Filter= No
    Channel ID= CH06 2437MHz             Edit Roaming Configuration= Yes
    RTS Threshold= 2432                  Block Intra-BSS Traffic= No
    Frag. Threshold= 2432                Preamble= Long
    WEP Encryption= Disable              802.11 Mode= Mixed
      Default Key= N/A                   Max. Frame Burst= 0
      Key1= N/A                          Breathing LED= Yes
      Key2= N/A
      Key3= N/A
      Key4= N/A
      Authen. Method= N/A


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

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

**Figure 59** WLAN Roaming Configuration



```
                        Menu 3.5.2 - Roaming Configuration

                      Active= Yes
                      Port #= 3517
```

The following table describes the fields in this menu.

**Table 45** Menu 3.5.4 Bridge Link Configuration

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select Yes to enable roaming on the G-1000 if you have two or more G-1000s on the same subnet. |
| Port # | Type the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

# CHAPTER 14
# Dial-in User Setup

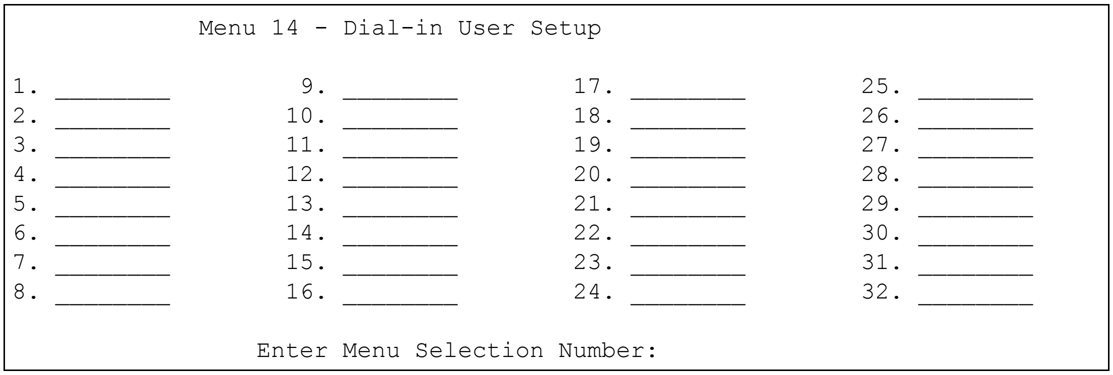
This chapter shows you how to create user accounts on the G-1000.

By storing user profiles locally, your G-1000 is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your G-1000.

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

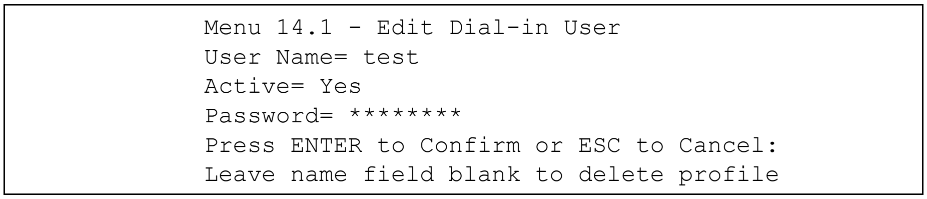
**Figure 60   Menu 14- Dial-in User Setup**



```
                Menu 14 - Dial-in User Setup

1. _________          9. _________          17. _________          25. _________
2. _________         10. _________          18. _________          26. _________
3. _________         11. _________          19. _________          27. _________
4. _________         12. _________          20. _________          28. _________
5. _________         13. _________          21. _________          29. _________
6. _________         14. _________          22. _________          30. _________
7. _________         15. _________          23. _________          31. _________
8. _________         16. _________          24. _________          32. _________

                     Enter Menu Selection Number:
```

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

**Figure 61 Menu 14.1- Edit Dial-in User**



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

The following table describes the fields in this screen.

**Table 46** Menu 14.1- Edit Dial-in User

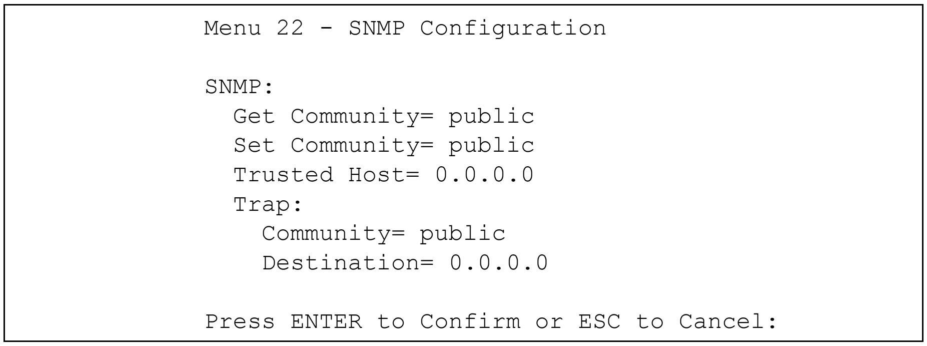
| FIELD | DESCRIPTION |
|---|---|
| User Name | Enter a username up to 31 alphanumeric characters long for this user profile.<br>This field is case sensitive. |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

# CHAPTER 15
# SNMP Configuration

This chapter shows you how to use SMT to configure SNMP on the G-1000.

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

**Figure 62   Menu 22 SNMP Configuration**



```
              Menu 22 - SNMP Configuration

              SNMP:
                Get Community= public
                Set Community= public
                Trusted Host= 0.0.0.0
                Trap:
                  Community= public
                  Destination= 0.0.0.0

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

The following table describes the SNMP configuration parameters.

**Table 47**   Menu 22 SNMP Configuration

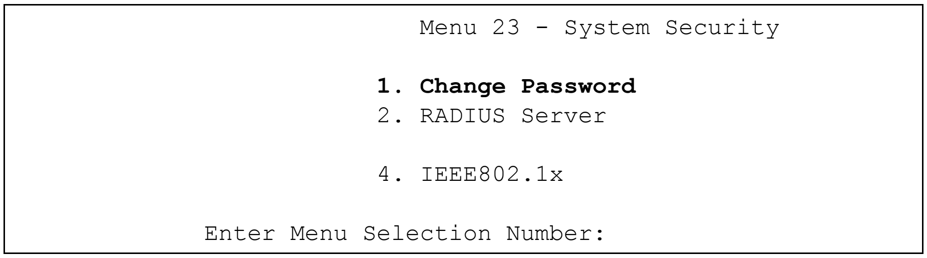
| FIELD | DESCRIPTION |
|---|---|
| SNMP: | |
| Get Community | Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station. |
| Set Community | Type the **Set Community**, which is the password for incoming Set requests from the management station. |
| Trusted Host | If you enter a trusted host, your G-1000 will only respond to SNMP messages from this address. A blank (default) field means your G-1000 will respond to all SNMP messages it receives, regardless of source. |
| Trap: | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

# CHAPTER 16
# System Security

This chapter describes how to configure the system password, an external RADIUS server and 802.1x in SMT.

## 16.1 System Password

**Figure 63 Menu 23 System Security**



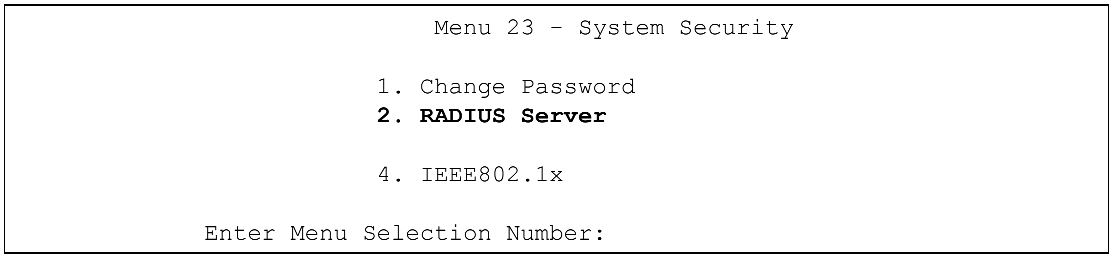
```
                            Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x

              Enter Menu Selection Number:
```

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the G-1000 in the *Introducing the Web Configurator* chapter.

## 16.2 Configuring External RADIUS Server

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

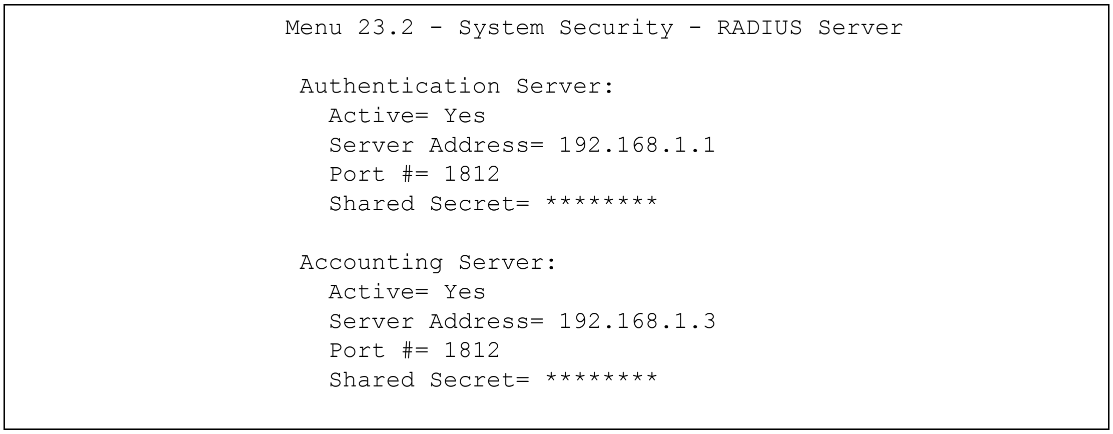
**Figure 64 Menu 23 System Security**



```
                             Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x

              Enter Menu Selection Number:
```

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

**Figure 65** Menu 23.2 System Security: RADIUS Server



```
                    Menu 23.2 - System Security - RADIUS Server

                     Authentication Server:
                       Active= Yes
                       Server Address= 192.168.1.1
                       Port #= 1812
                       Shared Secret= ********

                     Accounting Server:
                       Active= Yes
                       Server Address= 192.168.1.3
                       Port #= 1812
                       Shared Secret= ********
```

The following table describes the fields in this menu.

**Table 48** Menu 23.2 System Security: RADIUS Server

| FIELD | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server. |
| Server Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points.<br>The key is not sent over the network. This key must be the same on the external authentication server and G-1000. |
| Accounting Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server. |
| Server Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points.<br>The key is not sent over the network. This key must be the same on the external accounting server and G-1000. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

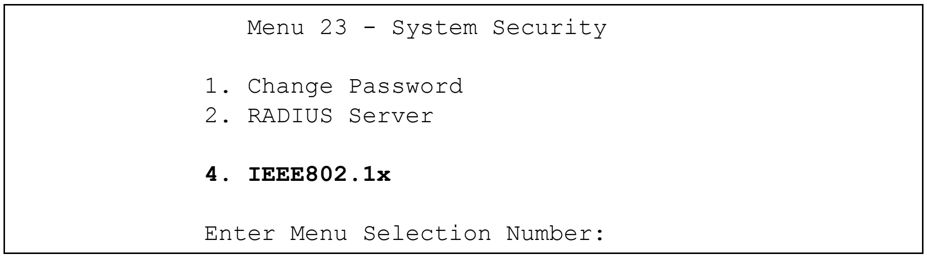
## 16.3 802.1x

The IEEE 802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your G-1000.

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

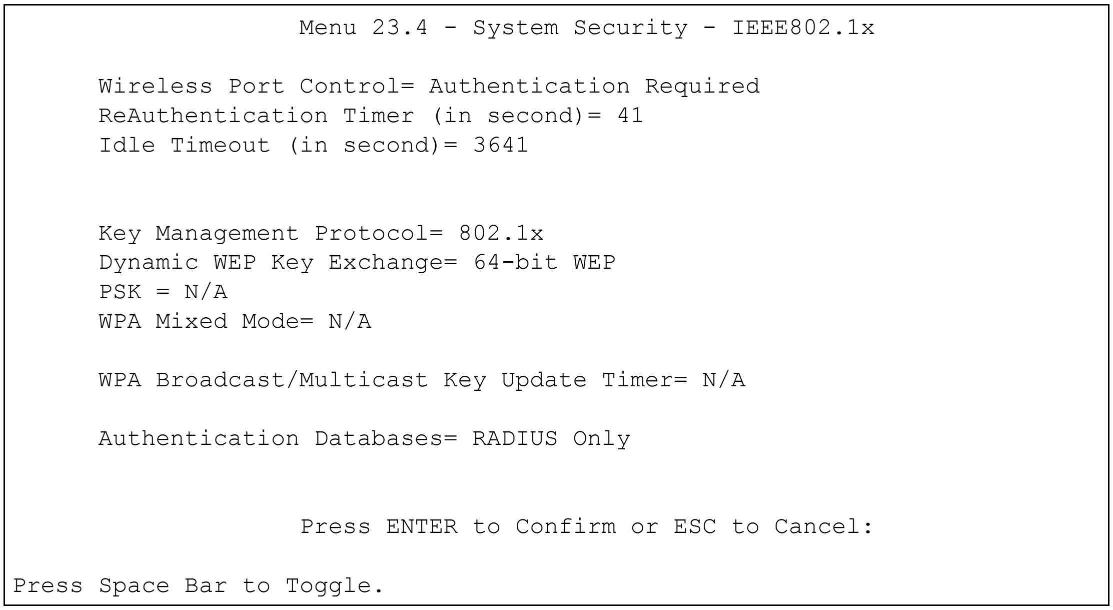
**Figure 66 Menu 23 System Security**



```
                 Menu 23 - System Security

              1. Change Password
              2. RADIUS Server

              4. IEEE802.1x

              Enter Menu Selection Number:
```

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

**Figure 67** Menu 23.4 System Security: IEEE802.1x



```
                    Menu 23.4 - System Security - IEEE802.1x

      Wireless Port Control= Authentication Required
      ReAuthentication Timer (in second)= 41
      Idle Timeout (in second)= 3641


      Key Management Protocol= 802.1x
      Dynamic WEP Key Exchange= 64-bit WEP
      PSK = N/A
      WPA Mixed Mode= N/A

      WPA Broadcast/Multicast Key Update Timer= N/A

      Authentication Databases= RADIUS Only


                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

**Table 49** Menu 23.4 System Security: IEEE802.1x

| FIELD | DESCRIPTION |
|---|---|
| Wireless Port Control | Press [SPACE BAR] and select a security mode for the wireless LAN access.<br>Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.<br>Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>Select **No Access Allowed** to block all wireless stations access to the wired network.<br>The following fields are not available when you select **No Authentication Required** or **No Access Allowed**. |
| ReAuthentication Timer (in second) | Specify how often a client has to re-enter username and password to stay connected to the wired network.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes). |
| Idle Timeout (in second) | The G-1000 automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour). |
| Key Management Protocol | Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER]. |

**Table 49** Menu 23.4 System Security: IEEE802.1x

| FIELD | DESCRIPTION |
|---|---|
| Dynamic WEP Key Exchange | This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used.<br>Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption.<br>Up to 32 stations can access the G-1000 when you configure dynamic WEP key exchange. |
| PSK | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field. |
| WPA Mixed Mode | Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Data Privacy for Broadcast/Multicast packets** field. |
| WPA Broadcast/ Multicast Key Update Timer | The **WPA Broadcast/Multicast Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Broadcast/ Multicast Key Update Timer** is also supported in WPA-PSK mode. The G-1000 default is 1800 seconds (30 minutes). |
| Authentication Databases | The authentication database contains wireless station login information. The local user database is the built-in database on the G-1000. The RADIUS is an external server. Use this field to decide which database the G-1000 should use (first) to authenticate a wireless station.<br>Before you specify the priority, make sure you have set up the corresponding database correctly first.<br>When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**.<br>Select **Local User Database Only** to have the G-1000 just check the built-in user database on the G-1000 for a wireless station's username and password.<br>Select **RADIUS Only** to have the G-1000 just check the user database on the specified RADIUS server for a wireless station's username and password.<br>Select **Local first, then RADIUS** to have the G-1000 first check the user database on the G-1000 for a wireless station's username and password. If the user name is not found, the G-1000 then checks the user database on the specified RADIUS server.<br>Select **RADIUS first, then Local** to have the G-1000 first check the user database on the specified RADIUS server for a wireless station's username and password. If the G-1000 cannot reach the RADIUS server, the G-1000 then checks the local user database on the G-1000. When the user name is not found or password does not match in the RADIUS server, the G-1000 will not check the local user database and the authentication fails. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the G-1000 for authentication

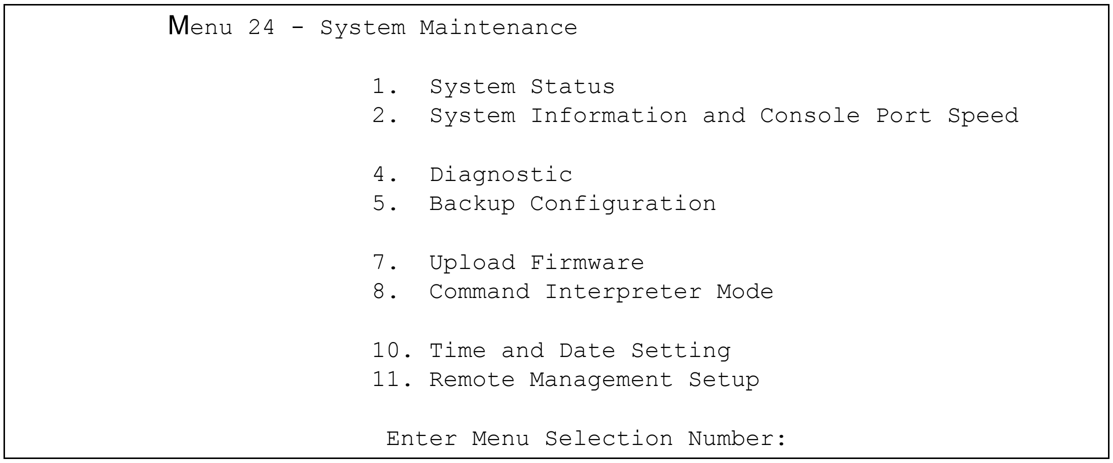
# CHAPTER 17 System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

**Figure 68 Menu 24 System Maintenance**



```
           Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed

                         4.  Diagnostic
                         5.  Backup Configuration

                         7.  Upload Firmware
                         8.  Command Interpreter Mode

                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

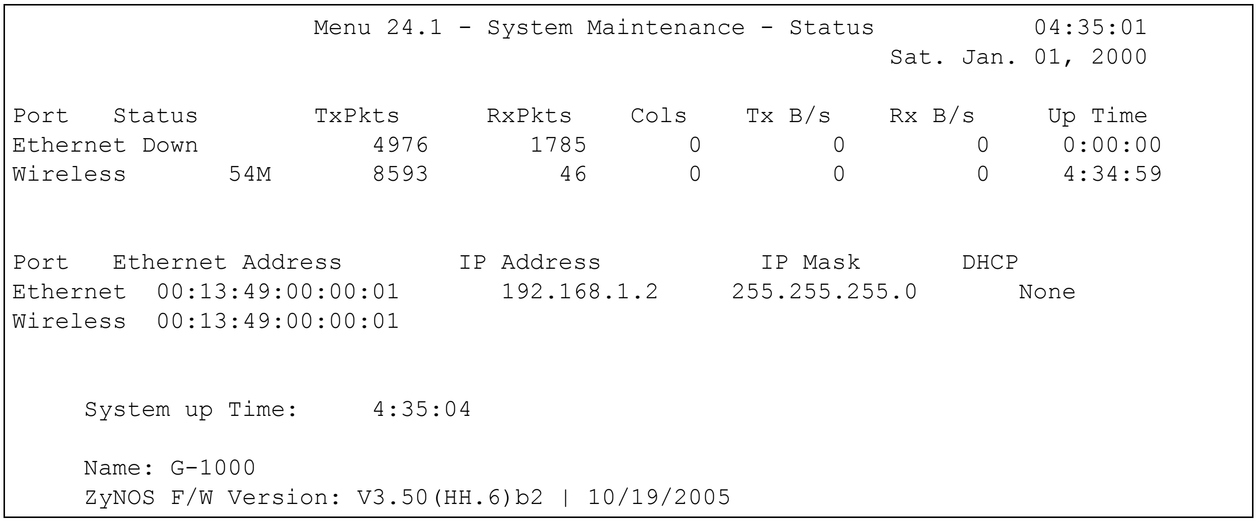
## 17.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your G-1000. Specifically, it gives you information on your Ethernet and Wireless LAN status, number of packets sent and received.

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

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

**Figure 69   Menu 24.1 System Maintenance: Status**



```
                     Menu 24.1 - System Maintenance - Status           04:35:01
                                                             Sat. Jan. 01, 2000

Port   Status         TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
Ethernet Down             4976       1785       0         0         0     0:00:00
Wireless       54M       8593         46       0         0         0     4:34:59


Port   Ethernet Address        IP Address           IP Mask       DHCP
Ethernet  00:13:49:00:00:01       192.168.1.2     255.255.255.0       None
Wireless  00:13:49:00:00:01


     System up Time:     4:35:04

     Name: G-1000
     ZyNOS F/W Version: V3.50(HH.6)b2 | 10/19/2005
```

The following table describes the fields present in this menu.

**Table 50**   Menu 24.1 System Maintenance: Status

| FIELD | DESCRIPTION |
|---|---|
| Port | This is the port type. Port types are: Ethernet, WLAN1 and WLAN 2. |
| Status | This shows the status of the remote node. |
| TxPkts | This is the number of transmitted packets to this remote node. |
| RxPkts | This is the number of received packets from this remote node. |
| Cols | This is the number of collisions on this connection. |
| Tx B/s | This shows the transmission rate in bytes per second. |
| Rx B/s | This shows the receiving rate in bytes per second. |
| Up Time | This is the time this channel has been connected to the current remote node. |
| Ethernet Address | This shows the MAC address of the port. |
| IP Address | This shows the IP address of the network device connected to the port. |
| IP Mask | This shows the subnet mask of the network device connected to the port. |
| DHCP | This shows the DHCP setting (None or Client) for the port. |
| System Up Time | This is the time the G-1000 is up and running from the last reboot. |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |
| Name | This displays the device name. |

## 17.2 System Information

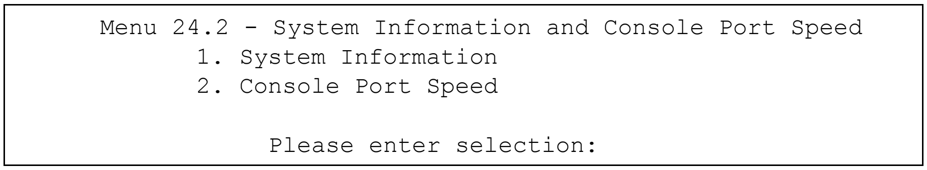
To get to the System Information:

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

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

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

**Figure 70   Menu 24.2 System Information and Console Port Speed**



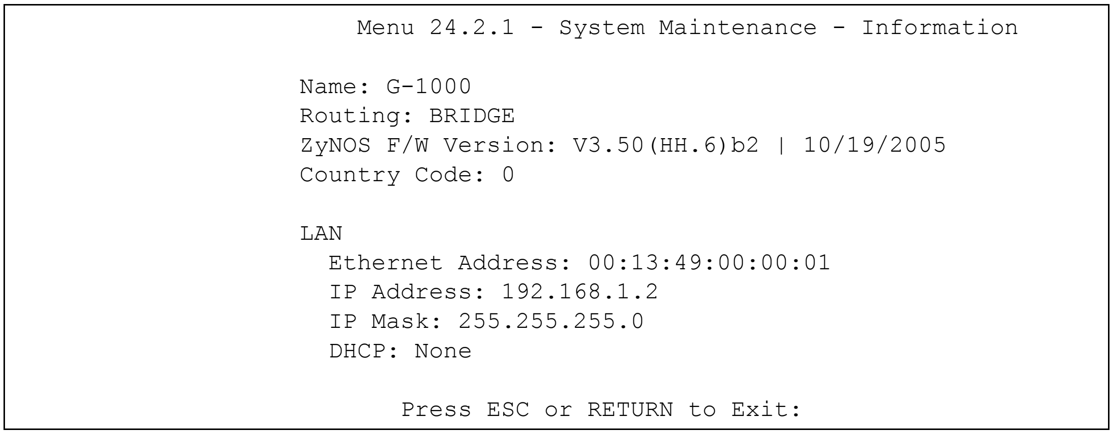
```
      Menu 24.2 - System Information and Console Port Speed
             1. System Information
             2. Console Port Speed

                  Please enter selection:
```

**Note:** The console port is internal and reserved for technician use only.

## 17.2.1  System Information

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

**Figure 71   Menu 24.2.1 System Information: Information**



```
                        Menu 24.2.1 - System Maintenance - Information

                    Name: G-1000
                    Routing: BRIDGE
                    ZyNOS F/W Version: V3.50(HH.6)b2 | 10/19/2005
                    Country Code: 0

                    LAN
                      Ethernet Address: 00:13:49:00:00:01
                      IP Address: 192.168.1.2
                      IP Mask: 255.255.255.0
                      DHCP: None

                           Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

**Table 51**   Menu 24.2.1 System Maintenance: Information

| FIELD | DESCRIPTION |
|---|---|
| Name | Displays the system name of your G-1000. This information can be changed in **Menu 1 – General Setup**. |
| Routing | Refers to the routing protocol used. |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |
| Country Code | Refers to the country code of the firmware. |
| LAN | |
| Ethernet Address | Refers to the Ethernet MAC (Media Access Control) of your G-1000. |
| IP Address | This is the IP address of the G-1000 in dotted decimal notation. |

**Table 51** Menu 24.2.1 System Maintenance: Information

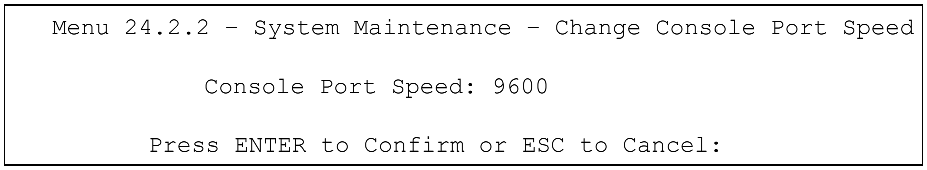
| FIELD | DESCRIPTION |
|---|---|
| IP Mask | This shows the subnet mask of the G-1000. |
| DHCP | This field shows the DHCP setting of the G-1000. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

## 17.2.2 Console Port Speed

**Note:** The console port is internal and reserved for technician use only.

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your G-1000 supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

**Figure 72 Menu 24.2.2 System Maintenance: Change Console Port Speed**



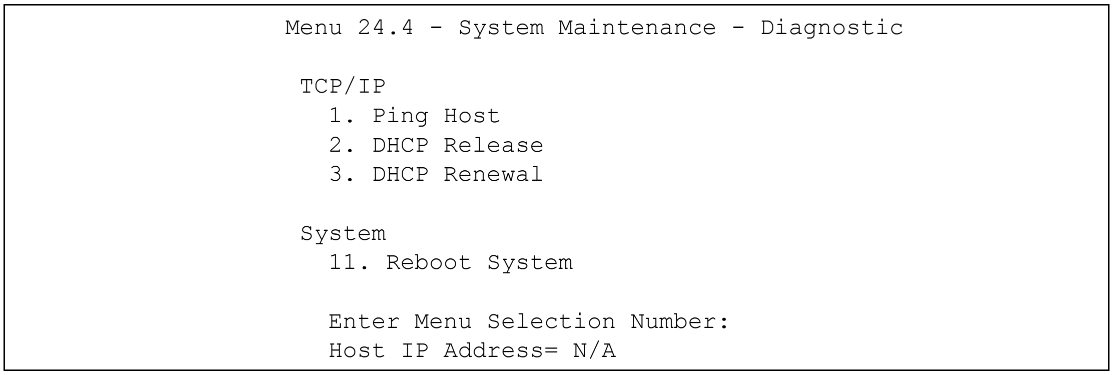
```
  Menu 24.2.2 - System Maintenance - Change Console Port Speed

             Console Port Speed: 9600

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

After you changed the console port speed on your G-1000, you must also make the same change to the console port speed parameter of your communication software.

# 17.3 Diagnostic

The diagnostic facility allows you to test the different aspects of your G-1000 to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

**Figure 73   Menu 24.4 System Maintenance: Diagnostic**



```
                   Menu 24.4 - System Maintenance - Diagnostic

                    TCP/IP
                      1. Ping Host
                      2. DHCP Release
                      3. DHCP Renewal

                    System
                      11. Reboot System

                      Enter Menu Selection Number:
                      Host IP Address= N/A
```

Follow the procedure next to get to display this menu:

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

2 From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for your G-1000 and the connections.

**Table 52**   Menu 24.4 System Maintenance Menu: Diagnostic

| FIELD | DESCRIPTION |
|---|---|
| Ping Host | Ping the host to see if the links and TCP/IP protocol on both systems are working. |
| DHCP Release | Release the IP address assigned by the DHCP server. |
| DHCP Renewal | Get a new IP address from the DHCP server. |
| Reboot System | Reboot the G-1000. |
| Host IP Address | If you typed 1 to Ping Host, now type the address of the computer you want to ping. |

# CHAPTER 18
# Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

## 18.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a rom filename extension. Once you have customized the G-1000's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the G-1000.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the G-1000 only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the G-1000 and the external filename refers to the filename not on the G-1000, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

**Table 53** Filename Conventions

| FILE TYPE | INTERNAL NAME | EXTERNAL NAME | DESCRIPTION |
|---|---|---|---|
| Configuration File | Rom-0 | *.rom | This is the configuration filename on the G-1000. Uploading the rom-0 file replaces the entire ROM file system, including your G-1000 configurations, system-related data (including the default password), the error log and the trace log. |
| Firmware | Ras | *.bin | This is the generic name for the ZyNOS firmware on the G-1000. |

## 18.2 Backup Configuration

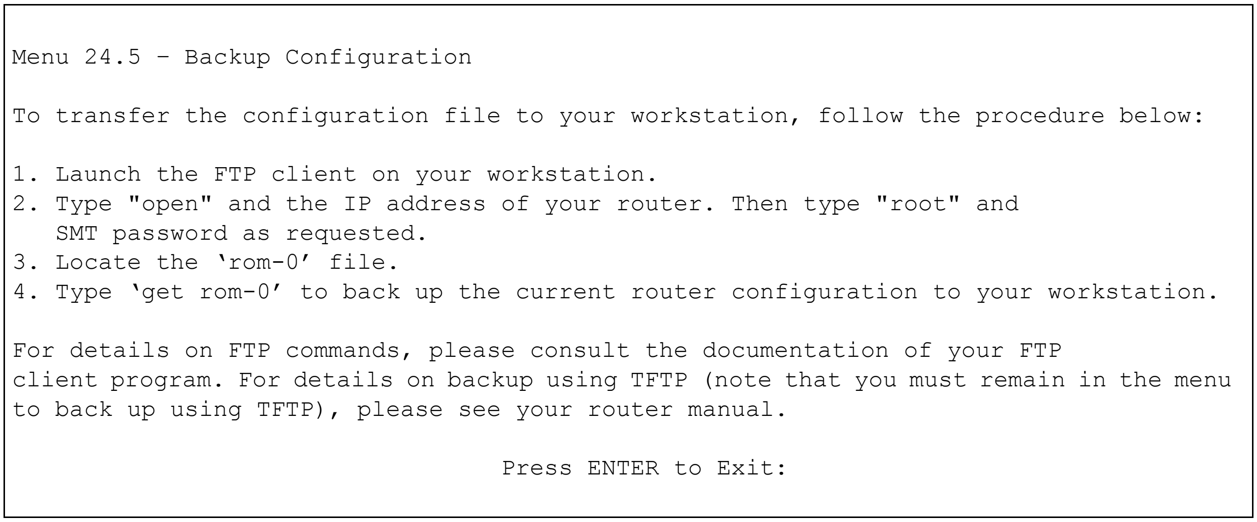
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current G-1000 configuration to your computer. Backup is highly recommended once your G-1000 is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms "download" and "upload" are relative to the computer. Download means to transfer from the G-1000 to the computer, while upload means from your computer to the G-1000.

### 18.2.1 Backup Configuration Using FTP

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

**Figure 74   Menu 24.5 Backup Configuration**



```
Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the ‘rom-0’ file.
4. Type ‘get rom-0’ to back up the current router configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain in the menu
to back up using TFTP), please see your router manual.

                                  Press ENTER to Exit:
```

## 18.2.2 Using the FTP command from the DOS Prompt

1. Launch the FTP client on your computer.
2. Enter “open” and the IP address of your G-1000.
3. Press [ENTER] when prompted for a username.
4. Enter “root” and your SMT password as requested. The default is 1234.
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer files from the G-1000 to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the G-1000 to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the FTP prompt.

**Figure 75 FTP Session Example**

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

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

**Table 54** General Commands for Third Party FTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

## 18.2.3 Backup Configuration Using TFTP

The G-1000 supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

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

**1** Use telnet from your computer to connect to the G-1000 and log in. Because TFTP does not have any security checks, the G-1000 records the IP address of the telnet client and accepts TFTP requests only from this address.

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

3 Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the G-1000. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the G-1000 and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the G-1000 to the computer and "binary" to set binary transfer mode.

### 18.2.4 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the G-1000 IP address, "get" transfers the file source on the G-1000 (rom-0 name of the configuration file on the G-1000) to the file destination on the computer and renames it config.rom.

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

**Table 55** General Commands for Third Party TFTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host | Enter the IP address of the G-1000. 192.168.1.2 is the G-1000's default IP address when shipped. |
| Send/Fetch | Use "Send" to upload the file to the G-1000 and "Fetch" to back up the file on your computer. |
| Local File | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer. |
| Remote File | This is the filename on the G-1000. The filename for the firmware is "ras" and for the configuration file, is "rom-0". |
| Binary | Transfer the file in binary mode. |
| Abort | Stop transfer of the file. |

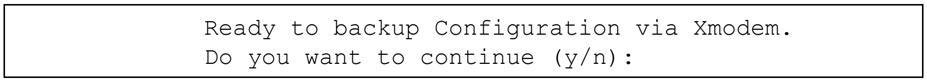
### 18.2.5 Backup Via Console Port

**Note:** The console port is internal and reserved for technician use only.

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

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

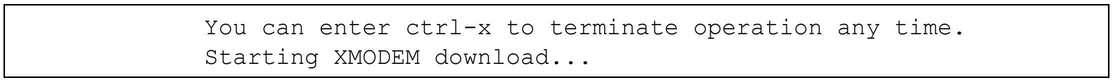
**Figure 76 System Maintenance: Backup Configuration**



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

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

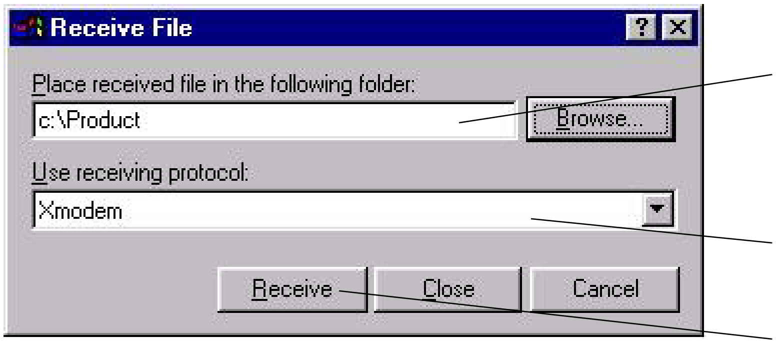
**Figure 77 System Maintenance: Starting Xmodem Download Screen**



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

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

**Figure 78 Backup Configuration Example**



Receive File

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

Use receiving protocol: Xmodem

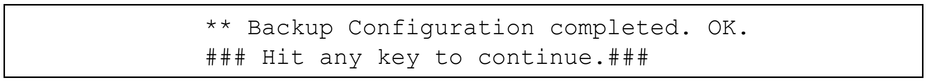
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

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

**Figure 79 Successful Backup Confirmation Screen**



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

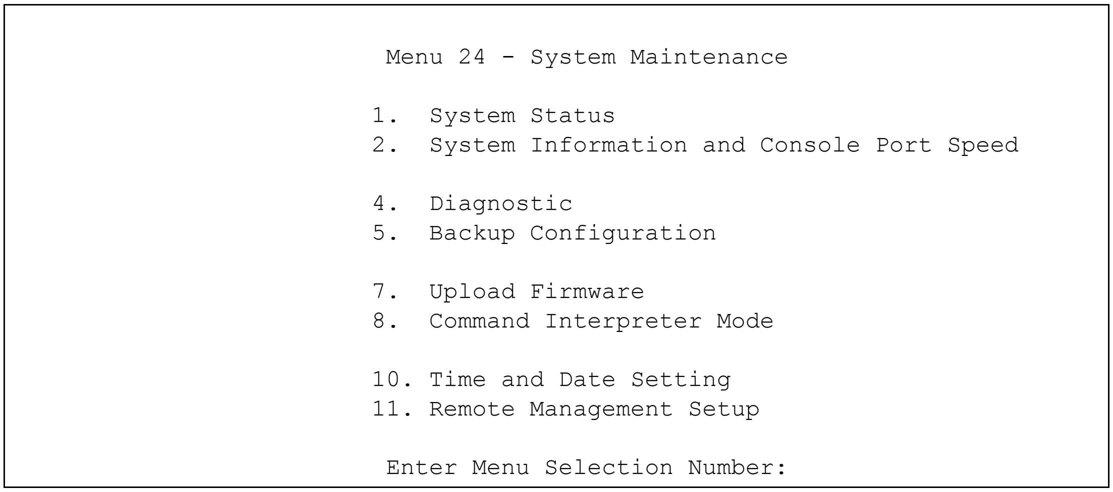
# CHAPTER 19
# System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

## 19.1 Command Interpreter Mode

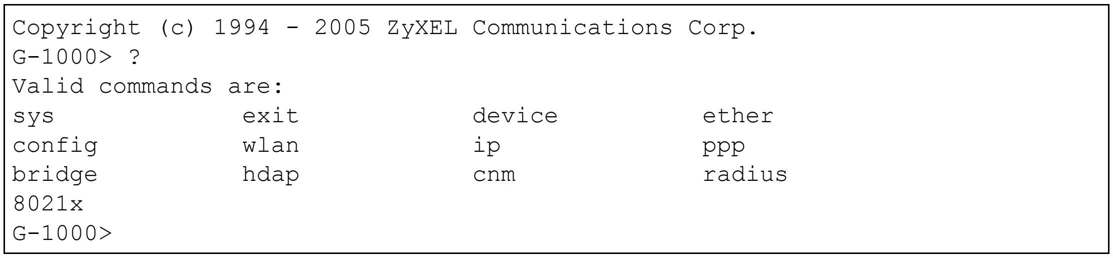
The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

**Figure 80 Menu 24 System Maintenance**



```
                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed

                         4.  Diagnostic
                         5.  Backup Configuration

                         7.  Upload Firmware
                         8.  Command Interpreter Mode

                         10. Time and Date Setting
                         11. Remote Management Setup

                          Enter Menu Selection Number:
```

**Figure 81 Valid CI Commands**



```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
G-1000> ?
Valid commands are:
sys             exit            device          ether
config          wlan            ip              ppp
bridge          hdap            cnm             radius
8021x
G-1000>
```

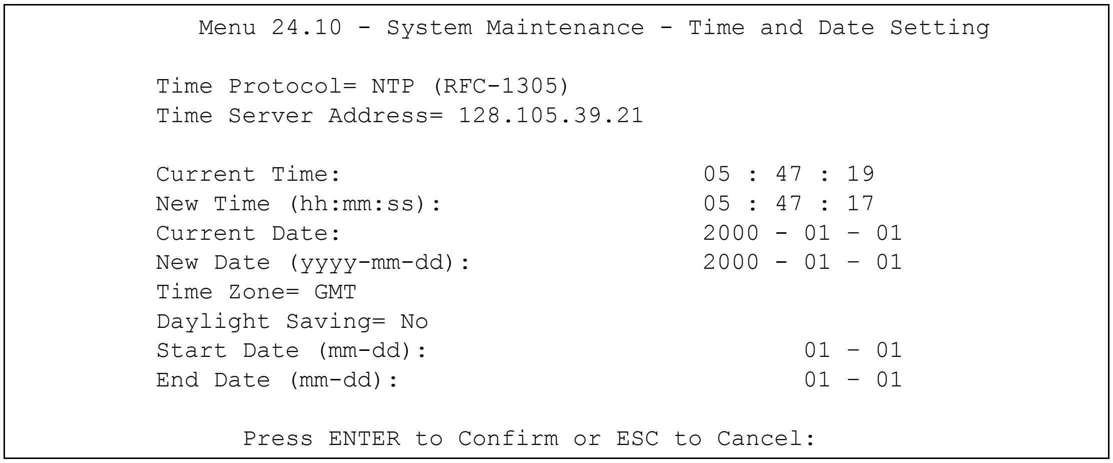
## 19.2 Time and Date Setting

The G-1000 keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your G-1000. Menu 24.10 allows you to update the time and date settings of your G-1000. The real time is then displayed in the G-1000 error logs.

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

2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your G-1000 as shown in the following screen.

**Figure 82   Menu 24.10 System Maintenance: Time and Date Setting**



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

          Time Protocol= NTP (RFC-1305)
          Time Server Address= 128.105.39.21

          Current Time:                         05 : 47 : 19
          New Time (hh:mm:ss):                  05 : 47 : 17
          Current Date:                         2000 - 01 - 01
          New Date (yyyy-mm-dd):                2000 - 01 - 01
          Time Zone= GMT
          Daylight Saving= No
          Start Date (mm-dd):                          01 - 01
          End Date (mm-dd):                            01 - 01

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

The following table describes the fields in this menu.

**Table 56**   System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Time Protocol | Enter the time service protocol that your time server sends when you turn on the G-1000. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**NTP (RFC-1305)** is similar to **Time (RFC-868)**.<br>**None**. The default, enter the time manually. |
| Time Server Address | Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Current Time | This field displays an updated time only when you reenter this menu. |
| New Time | Enter the new time in hour, minute and second format. |
| Current Date | This field displays an updated date only when you re-enter this menu. |
| New Date | Enter the new date in year, month and day format. |
| Time Zone | Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Saving | If you use daylight savings time, then choose **Yes**. |
| Start Date | If using daylight savings time, enter the month and day that it starts on. |
| End Date | If using daylight savings time, enter the month and day that it ends on |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. | |

The G-1000 resets the time in three instances:

**1** On leaving menu 24.10 after making changes.

2 When the G-1000 starts up, if there is a timeserver configured in menu 24.10.

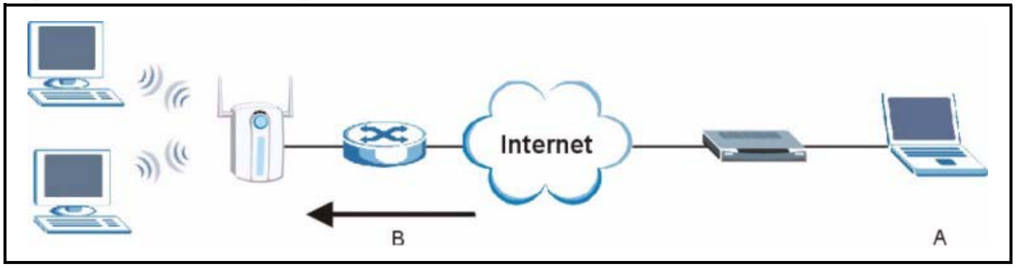
3 24-hour intervals after starting.

# 19.3 Remote Management Setup

## 19.3.1 Telnet

You can configure your G-1000 for remote Telnet access as shown next.

**Figure 83 Telnet Configuration on a TCP/IP Network**



## 19.3.2 FTP

You can upload and download G-1000 firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

## 19.3.3 Web

You can use the G-1000's embedded web configurator for configuration and file management. See the *online help* for details.

## 19.3.4 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your G-1000 from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

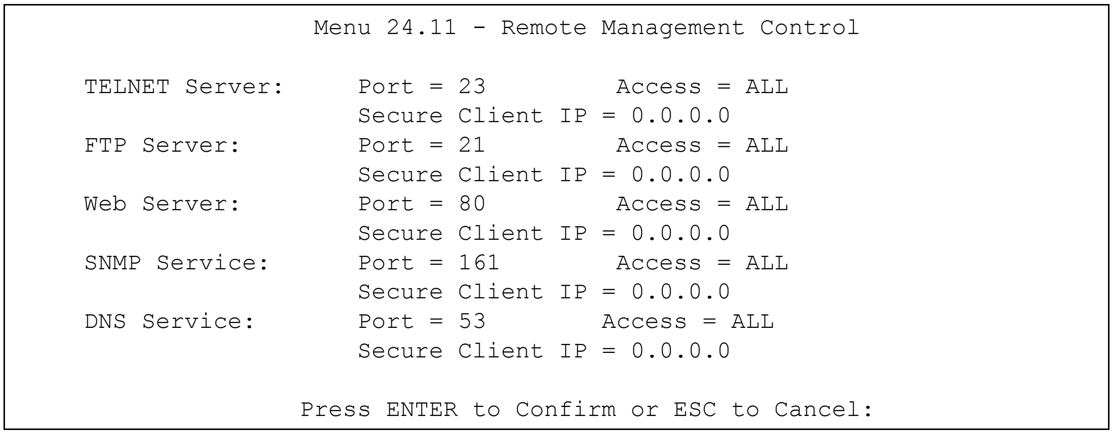
**Table 57** Remote Management Port Control

| | |
|---|---|
| WAN only (Internet) | ALL (LAN and WAN) |
| LAN only | Disable (Neither) |

**Note:** If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next)

**Figure 84   Menu 24.11 Remote Management Control**



```
                     Menu 24.11 - Remote Management Control

     TELNET Server:      Port = 23         Access = ALL
                         Secure Client IP = 0.0.0.0
     FTP Server:         Port = 21         Access = ALL
                         Secure Client IP = 0.0.0.0
     Web Server:         Port = 80         Access = ALL
                         Secure Client IP = 0.0.0.0
     SNMP Service:       Port = 161        Access = ALL
                         Secure Client IP = 0.0.0.0
     DNS Service:        Port = 53        Access = ALL
                         Secure Client IP = 0.0.0.0

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

The following table describes the fields in this menu.

**Table 58**   Menu 24.11 Remote Management Control

| FIELD | DESCRIPTION |
|---|---|
| TELNET Server:<br>FTP Server:<br>Web Server:<br>SNMP Service:<br>DNS Service: | Each of these read-only labels denotes a server or service that you may use to remotely manage the G-1000. |
| Port | This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management. |
| Access | Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**. |
| Secured Client IP | The default 0.0.0.0 allows any client to use this service to remotely manage the G-1000. Enter an IP address to restrict access to a client with a matching IP address. |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. | |

## 19.3.5 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1 A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.

2 You have disabled that service in menu 24.11.

3 The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the G-1000 will disconnect the session immediately.

4 There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.

5 There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

## 19.4 Remote Management and NAT

When NAT is enabled:

- Use the G-1000's WAN IP address when configuring from the WAN.
- Use the G-1000's LAN IP address when configuring from the LAN.

## 19.5 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your G-1000 will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

# Appendix A Troubleshooting

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

## Problems Starting Up the G-1000

**Table 59** Troubleshooting the Start-Up of Your G-1000

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| None of the LEDs turn on when I plug in the power adaptor. | Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on.<br>If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor. |
| The G-1000 reboots automatically sometimes. | The supplied power to the G-1000 is too low. Check that the G-1000 is receiving enough power.<br>Make sure the power source is working properly. |

## Problems with the Ethernet Interface

**Table 60** Troubleshooting the Ethernet Interface

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the G-1000 from the LAN. | If the **ETHN** LED on the front panel is off, check the Ethernet cable connection between your G-1000 and the Ethernet device connected to the **ETHERNET** port.<br>Check for faulty Ethernet cables.<br>Make sure your computer's Ethernet adapter is installed and working properly.<br>Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the G-1000, the Ethernet device and your computer are on the same subnet. |
| I cannot ping any computer on the LAN. | If the **ETHN** LED on the front panel is off, check the Ethernet cable connections between your G-1000 and the Ethernet device.<br>Check the Ethernet cable connections between the Ethernet device and the LAN computers.<br>Check for faulty Ethernet cables.<br>Make sure the LAN computer's Ethernet adapter is installed and working properly.<br>Verify that the IP address and the subnet mask of the G-1000, the Ethernet device and the LAN computers are on the same subnet. |

# Problems with the Password

**Table 61** Troubleshooting the Password

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| I cannot access the G-1000. | The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.<br>Use the **RESET** button on the top panel of the G-1000 to restore the factory default configuration file (hold this button in for about 10 seconds or until the link LED turns red). This will restore all of the factory defaults including the password. |

# Problems with Telnet

**Table 62** Troubleshooting Telnet

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| I cannot access the G-1000 through Telnet. | Refer to the Problems with the Ethernet Interface section for instructions on checking your Ethernet connection. |

# Problems with the WLAN Interface

**Table 63** Troubleshooting the WLAN Interface

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the G-1000 from the WLAN. | Make sure the wireless card is properly inserted in the G-1000 and the link LED is on.<br>Make sure the wireless adapter on the wireless station is working properly.<br>Check that both the G-1000 and your wireless station are using the same ESSID, channel and WEP keys (if WEP encryption is activated). |
| I cannot ping any computer on the WLAN. | Make sure the wireless card is properly inserted in the G-1000 and the link LED is on.<br>Make sure the wireless adapter on the wireless station(s) is working properly.<br>Check that both the G-1000 and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated). |

# Appendix B Specifications

## Hardware

**Table 64** Hardware

| | |
|---|---|
| Power Specification | DC 12V 1200mA |
| Operation Temperature | 5º C ~ 50º C |
| Storage Temperature | -20º C ~ 55º C |
| Operation Humidity | 10% to 90% (Non-condensing) |
| Storage Humidity | 5% to 95% (Non-condensing) |

## Firmware

**Table 65** Firmware

| | |
|---|---|
| Standards | IEEE 802.3 and 802.3u 10Base-T and 100Base-TX.<br>IEEE 802.11b specification compliance for wireless LAN.<br>IEEE 802.11g specification compliance for wireless LAN.<br>IEEE 802.1x security standard.<br>IEEE 802.3af standard. |
| Spanning Tree Protocol | IEEE 802.1d |
| DHCP Relay | Ability to act as a DHCP relay to pass the IP address from the DHCP server from WLAN port or NAT router. |
| Security | MAC address filtering through WLAN, supporting 32 accounts.<br>IEEE 802.1x security; MD5, EAP-TLS, EAP-TTLS, EAP-SIM and PEAP included.<br>64/128 bits WEP.<br>WPA support.<br>Dynamic WEP key exchange.<br>Mixed WEP & WPA mode supporting both 802.1x with Dynamic WEP and WPA clients.<br>Built-in RADIUS server, MD5 security and 32-entry local user database.<br>SSL passthrough.<br>VPN passthrough. |

**Table 65** Firmware (continued)

| | |
|---|---|
| Diagnostics Capabilities | The access point can perform self-diagnostic tests.<br>These tests check the integrity of the following circuits:<br>FLASH memory.<br>DRAM.<br>Dual Ethernet port.<br>Wireless port.<br>Syslog.<br>Errorlog.<br>Trace log.<br>Packet Log. |
| Management | Embedded Web Configurator management.<br>Command-line interface.<br>Telnet support; Password-protected telnet access to internal configuration manager.<br>FTP/TFTP/Web for firmware downloading, configuration backup and restoration.<br>Telnet remote access support.<br>Built-in Diagnostic Tool.<br>SNMP Management.<br>RADIUS client. |

# Appendix C Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix H” for information on the command structure.

**Table 66** Brute-Force Password Guessing Protection Commands

| COMMAND | DESCRIPTION |
|---|---|
| sys pwderrtm | This command displays the brute-force guessing password protection settings. |
| sys pwderrtm 0 | This command turns off the password’s protection from brute-force guessing. The brute-force password guessing protection is turned off by default. |
| sys pwderrtm N | This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered. |

## Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

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

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

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

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

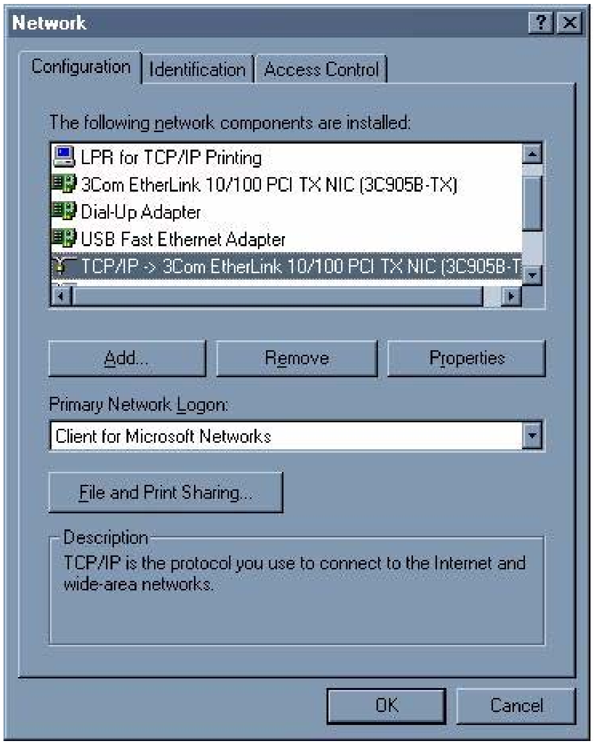
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the G-1000's LAN port.

## Windows 95/98/Me

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

**Figure 85** WIndows 95/98/Me: Network: Configuration



The following network components are installed:

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

Primary Network Logon: Client for Microsoft Networks

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

## Installing Components

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

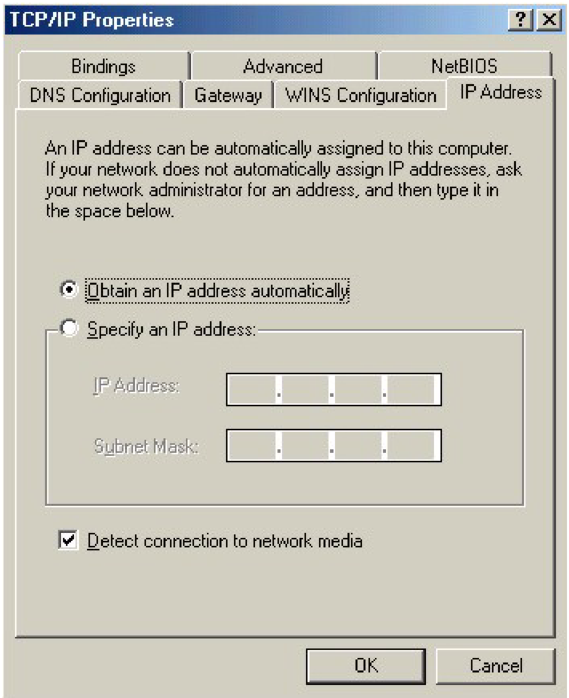
## Configuring

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

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

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

**Figure 86** Windows 95/98/Me: TCP/IP Properties: IP Address



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

● Obtain an IP address automatically

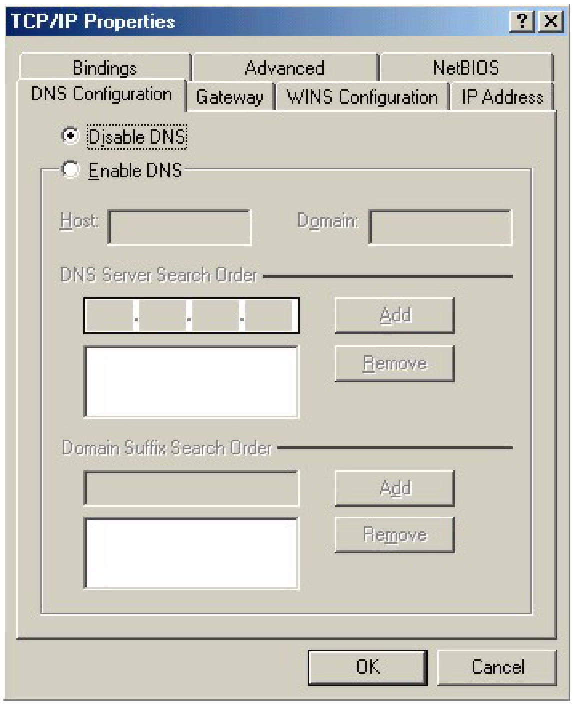
○ Specify an IP address:

☑ Detect connection to network media

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

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

**Figure 87** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS
○ Enable DNS

4 Click the **Gateway** tab.

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

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

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

7 Turn on your G-1000 and restart your computer when prompted.

## Verifying Settings

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

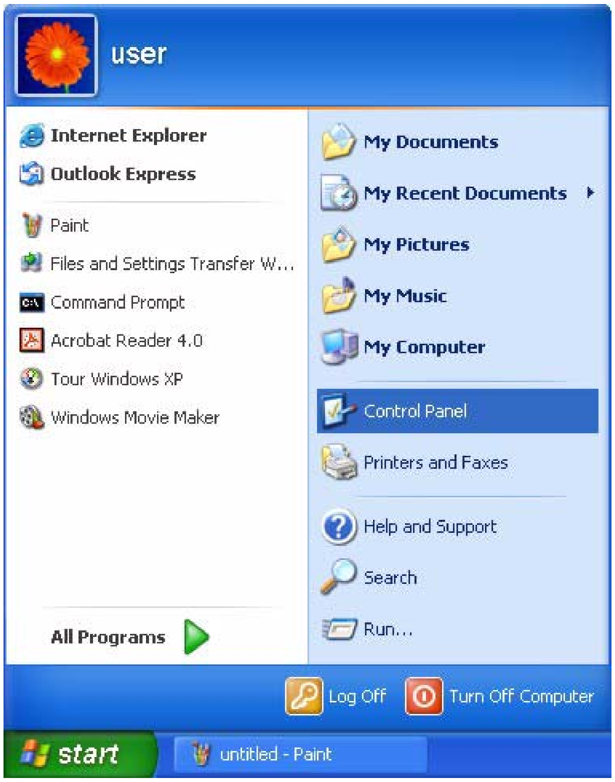
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

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

# Windows 2000/NT/XP

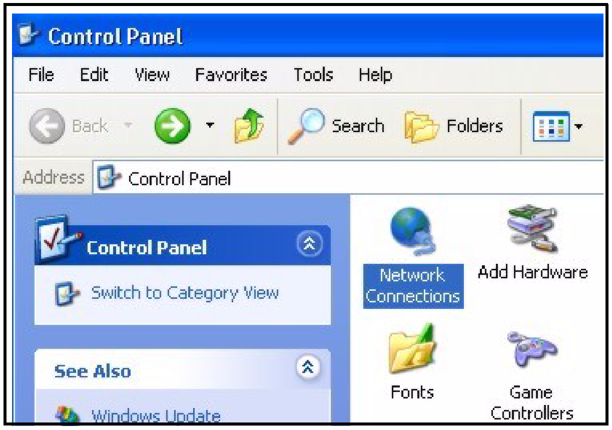
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

**Figure 88** Windows XP: Start Menu



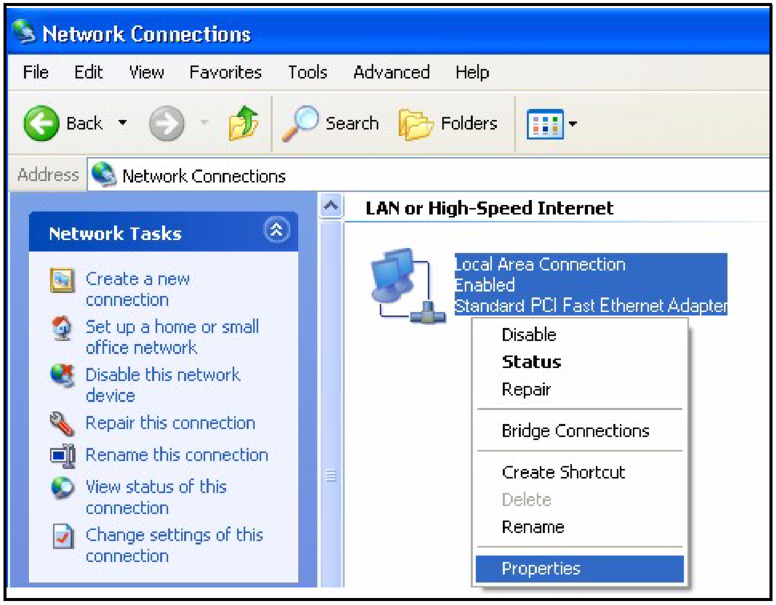
**2** For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 89** Windows XP: Control Panel



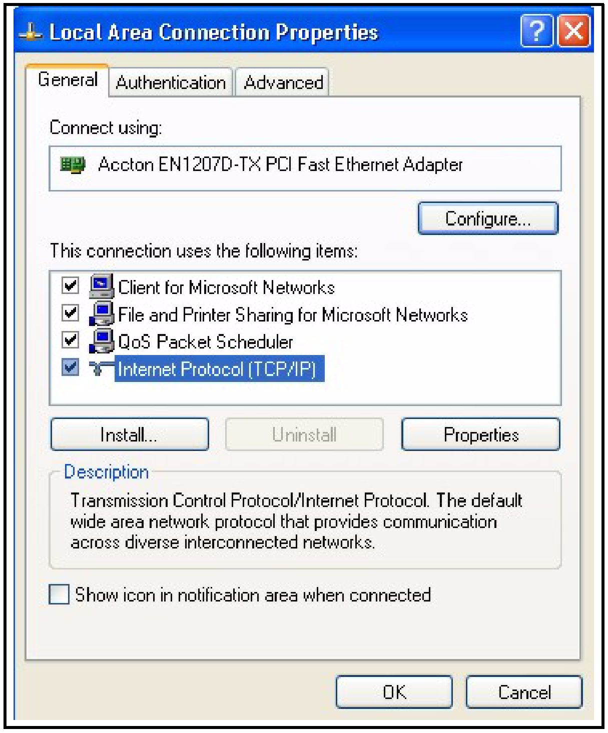
**3** Right-click **Local Area Connection** and then click **Properties**.

**Figure 90** Windows XP: Control Panel: Network Connections: Properties



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

**Figure 91** Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

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

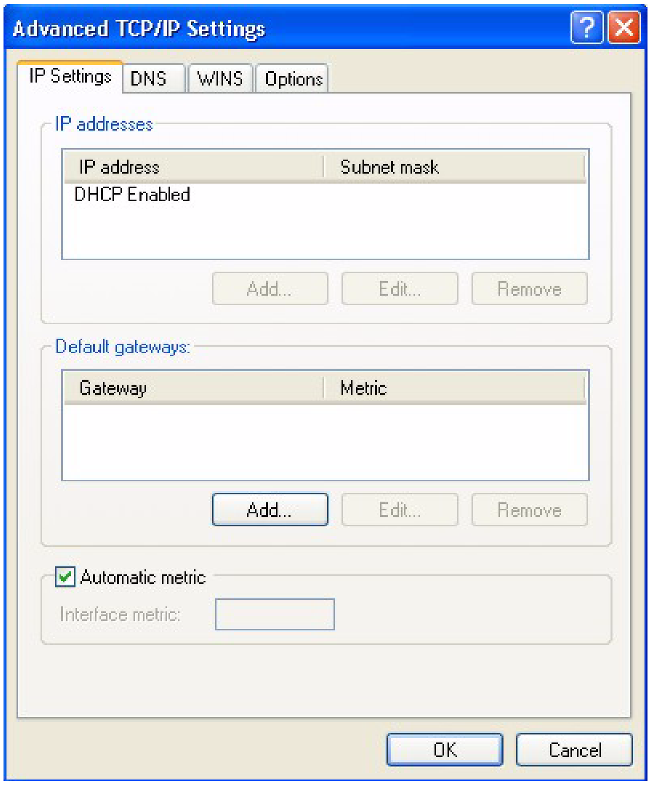
☐ Show icon in notification area when connected

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

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

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

**Figure 92** Windows XP: Advanced TCP/IP Settings



| IP address | Subnet mask |
|---|---|
| DHCP Enabled | |

| Gateway | Metric |
|---|---|

☑ Automatic metric

Interface metric:

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

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

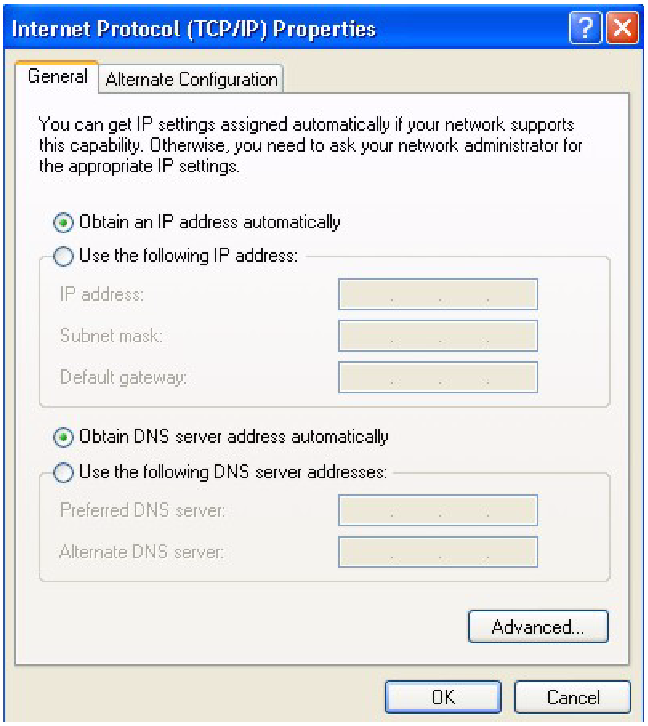
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

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

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

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

**Figure 93** Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

**9** Click **OK** to close the **Local Area Connection Properties** window.

**10**Turn on your G-1000 and restart your computer (if prompted).

## Verifying Settings

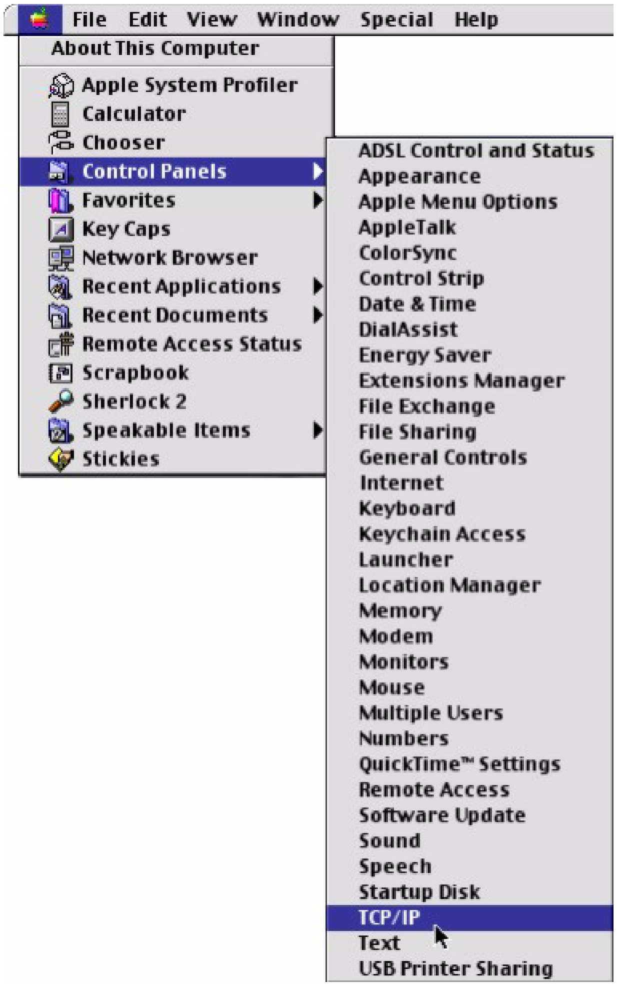
**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

# Macintosh OS 8/9

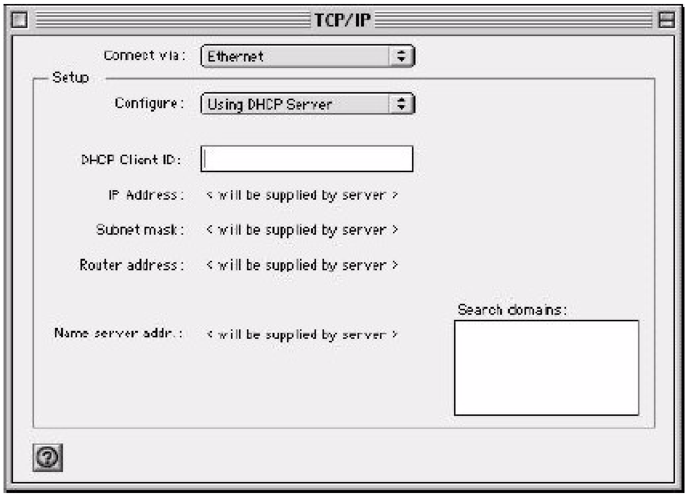
**1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 94** Macintosh OS 8/9: Apple Menu



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

**Figure 95** Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

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

Search domains:

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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your G-1000 in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your G-1000 and restart your computer (if prompted).

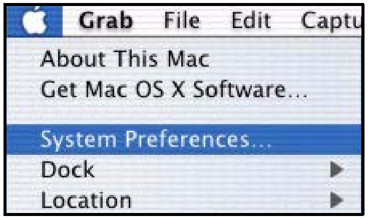
## Verifying Settings

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

# Macintosh OS X

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

**Figure 96** Macintosh OS X: Apple Menu

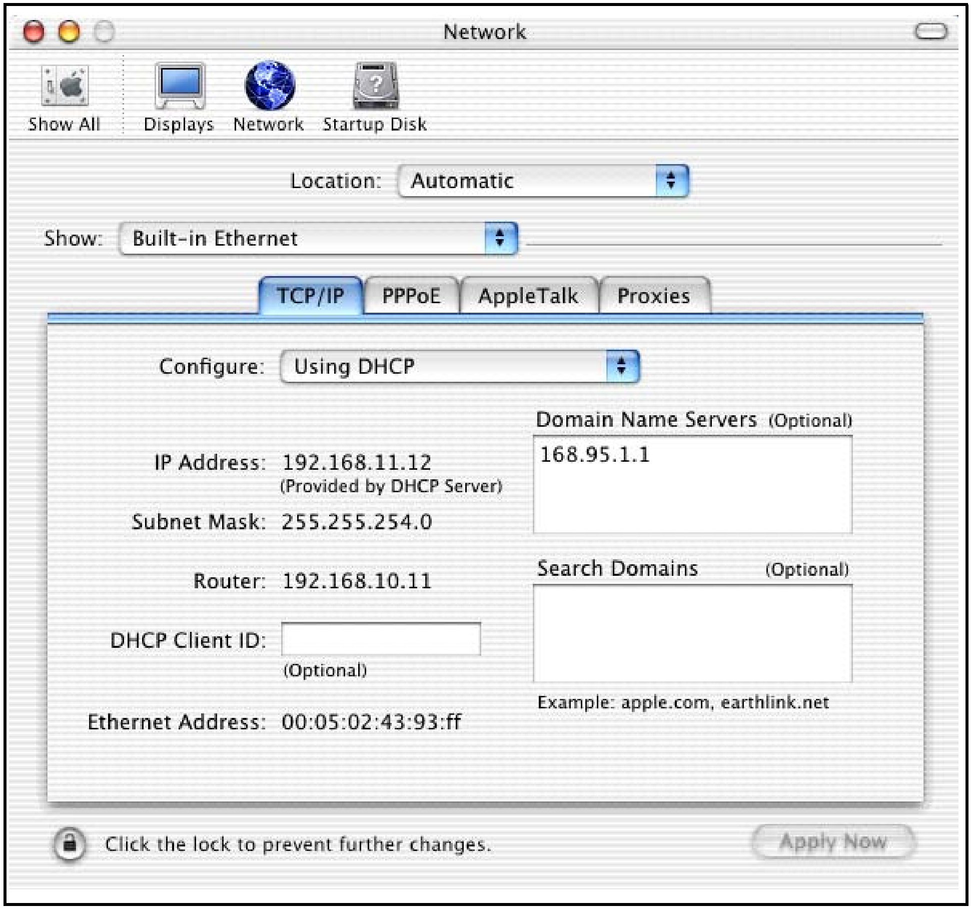


2 Click **Network** in the icon bar.

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

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

**Figure 97** Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your G-1000 in the **Router address** box.

**5** Click **Apply Now** and close the window.

**6** Turn on your G-1000 and restart your computer (if prompted).

## Verifying Settings

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

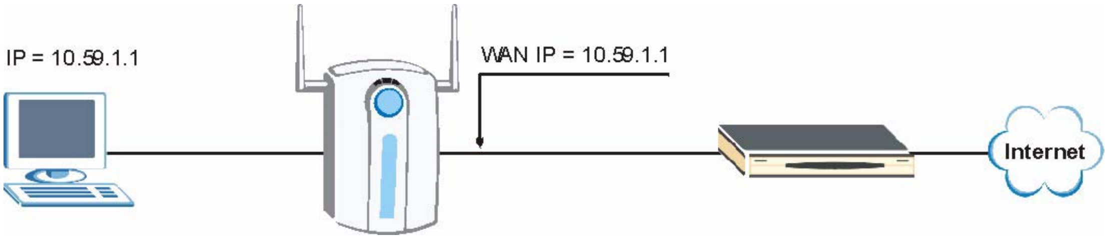
# Appendix E
# IP Address Assignment Conflicts

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

## Case A: The G-1000 is using the same LAN and WAN IP addresses

The following figure shows an example where the G-1000 is using a WAN IP address that is the same as the IP address of a computer on the LAN.

**Figure 98** IP Address Conflicts: Case A

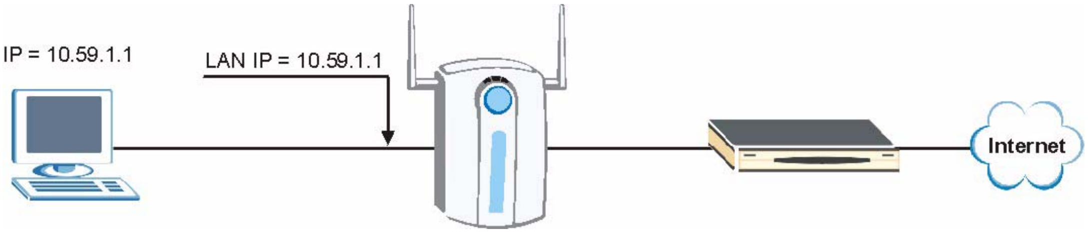


You must set the G-1000 to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the G-1000. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the G-1000 use a public WAN IP address.

## Case B: The G-1000 LAN IP address conflicts with the DHCP client IP address

In the following figure, the G-1000 is acting as a DHCP server. The G-1000 assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

**Figure 99** IP Address Conflicts: Case B

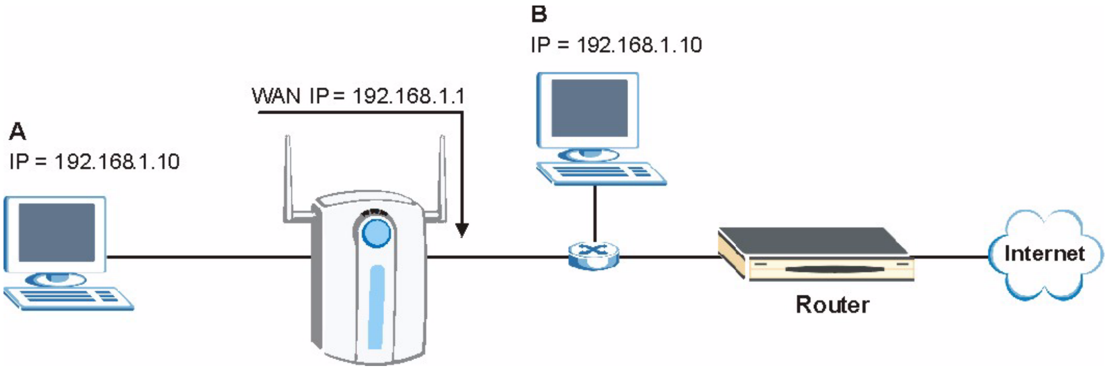


To solve this problem, make sure the G-1000 LAN IP address is not in the DHCP IP address pool.

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

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the G-1000.

**Figure 100** IP Address Conflicts: Case C



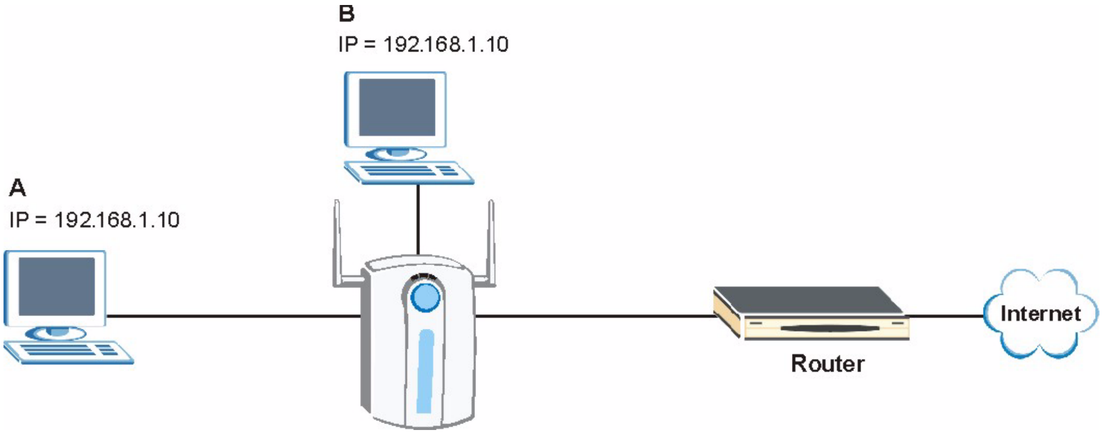
You must set the G-1000 to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the G-1000. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the G-1000 use a public WAN IP address.

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

By converting all private IP addresses to the WAN IP address, the G-1000 allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the G-1000 DHCP server assigns to another subscriber acting as a DHCP client.

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

**Figure 101** IP Address Conflicts: Case D



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

# Appendix F Wireless LANs

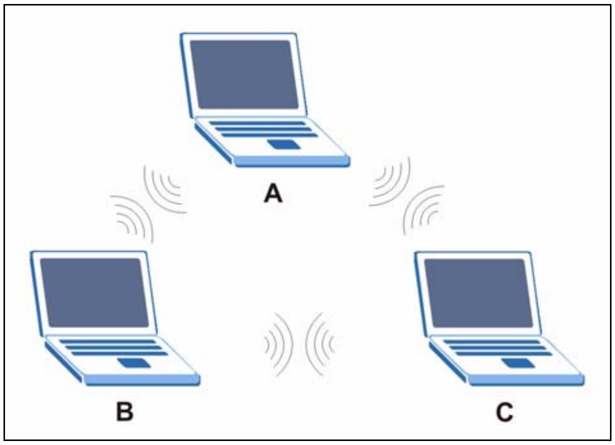
## Wireless LAN Topologies

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

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 102** Peer-to-Peer Communication in an Ad-hoc Network

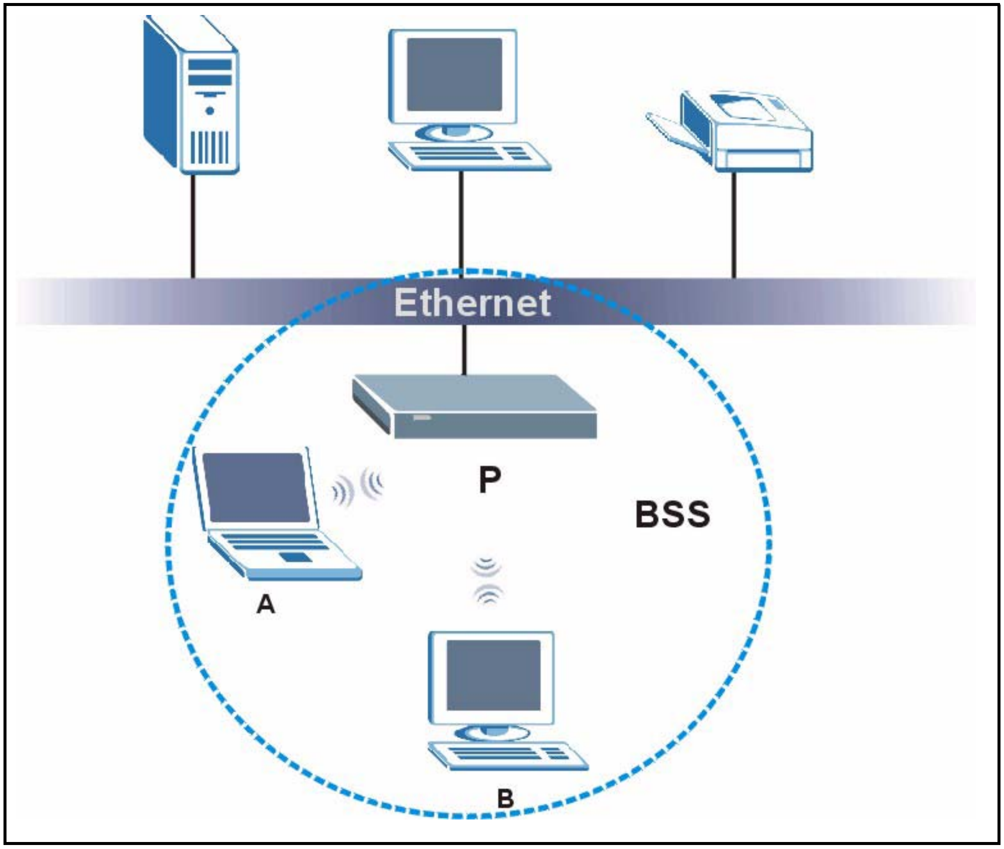


### BSS

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

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

**Figure 103** Basic Service Set



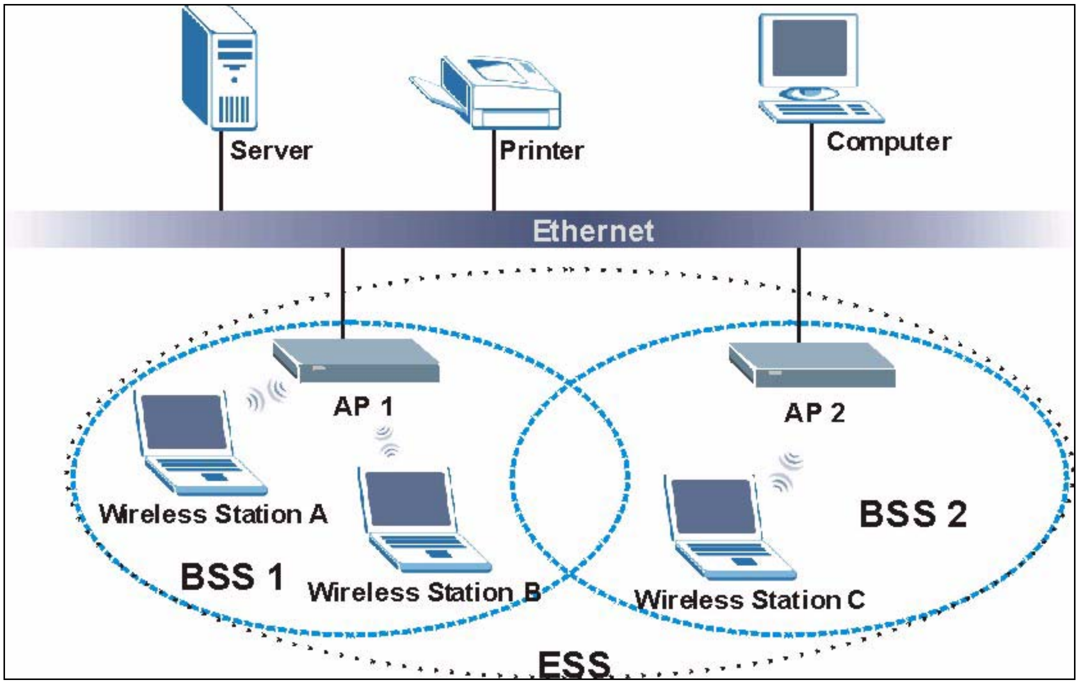
## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

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

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 104 Infrastructure WLAN



## Channel

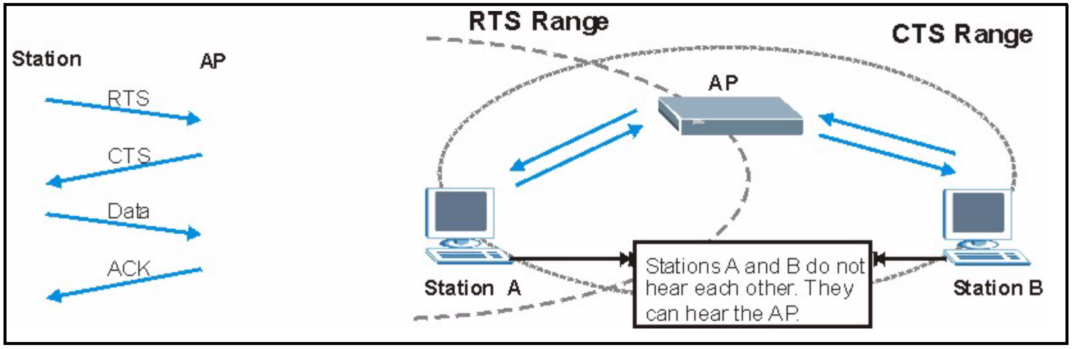
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs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

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

## RTS/CTS

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

**Figure 105** RTS/CTS


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

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

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

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

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

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

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

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

## Fragmentation Threshold

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

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

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

# Preamble Type

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

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

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

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

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

## IEEE 802.11g Wireless LAN

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

**Table 67** IEEE 802.11g

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

# IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

# RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

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

  Keeps track of the client's network activity.

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

## Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

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

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

# Types of Authentication

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

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

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

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

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

## EAP-TLS (Transport Layer Security)

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

## EAP-TTLS (Tunneled Transport Layer Service)

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

## PEAP (Protected EAP)

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

## LEAP

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

## Dynamic WEP Key Exchange

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

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

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

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

**Table 68** Comparison of EAP Authentication Types

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

# WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA 2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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

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

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

### User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Security Parameters Summary

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

**Table 69** Wireless Security Relational Matrix

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

**Table 69** Wireless Security Relational Matrix (continued)

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | ENABLE IEEE 802.1X |
|---|---|---|---|
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP | No | Enable |
| WPA-PSK | TKIP | Yes | Enable |
| WPA2 | AES | No | Enable |
| WPA2-PSK | AES | Yes | Enable |

# Appendix G IP Subnetting

## IP Addressing

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

## IP Classes

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

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

**Table 70** Classes of IP Addresses

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

**Note:** Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have $2^8$ –2 or 254 hosts.

A class "B" address (16 host bits) can have $2^{16}$ –2 or 65534 hosts.

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

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

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

**Table 71** Allowed IP Address Range By Class

| CLASS | ALLOWED RANGE OF FIRST OCTET (BINARY) | ALLOWED RANGE OF FIRST OCTET (DECIMAL) |
|---|---|---|
| Class A | **0**0000000 to **0**1111111 | 0 to 127 |
| Class B | **10**000000 to **10**111111 | 128 to 191 |
| Class C | **110**00000 to **110**11111 | 192 to 223 |
| Class D | **1110**0000 to **1110**1111 | 224 to 239 |

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32  is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

**Table 72** "Natural" Masks

| CLASS | NATURAL MASK |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

**Table 73** Alternative Subnet Mask Notation

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

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

# Example: Two Subnets

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

**Table 74** Two Subnets Example

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

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

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

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

**Table 75** Subnet 1

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

**Table 76** Subnet 2

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

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

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

# Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6$-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

**Table 77** Subnet 1

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 78** Subnet 2

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 79** Subnet 3

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 80** Subnet 4

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address:<br>192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address:<br>192.168.1.255 | Highest Host ID: 192.168.1.254 | |

# Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

**Table 81** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

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

**Table 82** Class C Subnet Planning

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

# Subnetting With Class A and Class B Networks.

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

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 70) available for subnetting.

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

**Table 83** Class B Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

# Appendix H Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

## Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  sys filter netbios config <type> <on|off>

  means that you must specify the type of netbios filter and whether to turn it on or off.

## Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

# Appendix I
# Log Descriptions

This appendix provides descriptions of example log messages.

**Table 84** System Maintenance Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Time calibration is successful` | The router has adjusted its time based on information from the time server. |
| `Time calibration failed` | The router failed to get information from the time server. |
| `DHCP client gets %s` | A DHCP client got a new IP address from the DHCP server. |
| `DHCP client IP expired` | A DHCP client's IP address has expired. |
| `DHCP server assigns %s` | The DHCP server assigned an IP address to a client. |
| `SMT Login Successfully` | Someone has logged on to the router's SMT interface. |
| `SMT Login Fail` | Someone has failed to log on to the router's SMT interface. |
| `WEB Login Successfully` | Someone has logged on to the router's web configurator interface. |
| `WEB Login Fail` | Someone has failed to log on to the router's web configurator interface. |
| `TELNET Login Successfully` | Someone has logged on to the router via telnet. |
| `TELNET Login Fail` | Someone has failed to log on to the router via telnet. |
| `FTP Login Successfully` | Someone has logged on to the router via FTP. |
| `FTP Login Fail` | Someone has failed to log on to the router via FTP. |

**Table 85** ICMP Notes

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| 0 | | Echo Reply |
| | 0 | Echo reply message |
| 3 | | Destination Unreachable |
| | 0 | Net unreachable |
| | 1 | Host unreachable |
| | 2 | Protocol unreachable |
| | 3 | Port unreachable |
| | 4 | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF) |
| | 5 | Source route failed |
| 4 | | Source Quench |
| | 0 | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5 | | Redirect |
| | 0 | Redirect datagrams for the Network |

**Table 85** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| | 1 | Redirect datagrams for the Host |
| | 2 | Redirect datagrams for the Type of Service and Network |
| | 3 | Redirect datagrams for the Type of Service and Host |
| 8 | | Echo |
| | 0 | Echo message |
| 11 | | Time Exceeded |
| | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 | | Parameter Problem |
| | 0 | Pointer indicates the error |
| 13 | | Timestamp |
| | 0 | Timestamp request message |
| 14 | | Timestamp Reply |
| | 0 | Timestamp reply message |
| 15 | | Information Request |
| | 0 | Information request message |
| 16 | | Information Reply |
| | 0 | Information reply message |

**Table 86** Sys log

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"` | This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts. |

# Log Commands

Go to the command interpreter interface (the *Command Interpreter Appendix* explains how to access and use the commands).

## Configuring What You Want the G-1000 to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the G-1000 is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Table 87** Log Categories and Available Settings

| LOG CATEGORIES | AVAILABLE PARAMETERS |
|---|---|
| error | 0, 1, 2, 3 |
| mten | 0, 1 |
| Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category. | |

Use the `sys logs save` command to store the settings in the G-1000 (you must do this in order to record logs).

## Displaying Logs

Use the `sys logs display` command to show all of the logs in the G-1000’s log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual G-1000 log category.

Use the `sys logs clear` command to erase all of the G-1000’s logs.

# Log Command Example

This example shows how to set the G-1000 to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#  .time              source              destination
notes
    message
  0|11/11/2002 15:10:12 |172.22.3.80:137
|172.22.255.255:137    |ACCESS BLOCK
```

# Appendix J
# Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

### Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to –point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# Connector Type

The G-1000 is equipped with a reverse polarity SMA jack, so it will work with any 2.4GHz wireless antenna with a reverse polarity SMA plug.

# Appendix K
# Power Adaptor Specifications

**Table 88** NORTH AMERICAN PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | AD48-1201200DUY |
| Input Power | AC120Volts/60Hz/0.25A |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | UL, CUL (UL 1950, CSA C22.2 No.234-M90) |

**Table 89** NORTH AMERICAN PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | DV-121A2-5720 |
| Input Power | AC120Volts/60Hz/27VA |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | UL, CUL (UL 1310, CSA C22.2 No.223-M91) |

**Table 90** EUROPEAN PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | AD-1201200DV |
| Input Power | AC230Volts/50Hz/0.2A |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | TUV, CE (EN 60950) |

**Table 91** UNITED KINGDOM PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | AD-1201200DK |
| Input Power | AC230Volts/50Hz/0.2A |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | TUV, CE (EN 60950, BS7002) |

**Table 92** JAPAN PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | JOD-48-1124 |
| Input Power | AC100Volts/ 50/60Hz/ 27VA |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | T-Mark (Japan Dentori) |

**Table 93** AUSTRALIA AND NEW ZEALAND PLUG STANDARDS

| | |
|---|---|
| AC Power Adaptor Model | AD-1201200DS or AD-121200DS |
| Input Power | AC240Volts/50Hz/0.2A |
| Output Power | DC12Volts/1.2A |
| Power Consumption | 10 W |
| Safety Standards | NATA (AS 3260) |

# Index