ZyXEL G-1000 v2

Wireless-11g Access Point

User's Guide

Version 3.60
Edition 1
3/2006

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.

Interference Statements and Certifications

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 residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation

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.

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Caution

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

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

ZyXEL Communications Corporation declared that G-1000 v2 is limited in CH1~11 from 2400 to 2483.5 MHz by specified firmware controlled in USA.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Certifications

1 Go to www.zyxel.com

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

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

Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- 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.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- 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.

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

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

[1] "+" 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 v2 IEEE 802.11g wireless access point.

Your G-1000 v2 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 ZyXEL device 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 v2. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains 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.

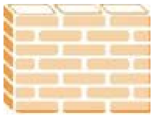
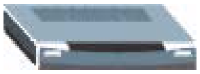
User Guide Feedback

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 predefined choice.
- Mouse action sequences are denoted using a right angle bracket (>). For example, “In Windows, click **Start > Settings > Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The ZyXEL G-1000 v2 may be referred to as the “G-1000 v2” in this User’s Guide.

Graphics Icons Key

ZyXEL device	Computer	Notebook computer
Server	DSLAM	Firewall 
Modem 	Switch	Router
Wireless Signal		

CHAPTER 1
Getting to Know Your Device

This chapter introduces the main features and applications of the G-1000 v2.

1.1 Introducing the ZyXEL G-1000 v2

The ZyXEL G-2000 Plus v2 is a wireless access point. The G-1000 v2 offers highly secured wireless connectivity to your wired network with IEEE 802.1X, WEP data encryption, WPA(2) (Wi-Fi Protected Access) and MAC address filtering.

The G-1000 v2 is easy to install and configure. The embedded web-based configurator and SNMP network management enables remote configuration and management of your G-1000 v2.

1.2 Features

The following sections describe the features of the G-1000 v2.

Note: See the product specifications in the appendix for detailed features and standards support.

1.2.1 Physical Features

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

This auto-negotiating feature allows the G-1000 v2 to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

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

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

Reset Button

The G-1000 v2 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 and subnet mask to 255.255.255.0.

ZyAIR LED

The blue **ZyAIR LED** (also known as the breathing light) is on when the G-1000 v2 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 light off even when the G-1000 v2 is on and data is being transmitted/received.

1.2.2 Firmware Features

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (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.

IEEE 802.11b Wireless LAN Standard

The G-1000 v2 complies with the IEEE 802.11b wireless standards.

The IEEE 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 Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

IEEE 802.11g Wireless LAN Standard

The G-1000 v2, complies with the IEEE 802.11g wireless standard and is also fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g device (and vice versa) at 11 Mbps or lower depending on range.The 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 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 v2 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.

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.

Limit the number of Client Connections

You may set a maximum number of wireless stations that may connect to the G-1000 v2. 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.

SSL Passthrough

SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http". The G-1000 v2 allows SSL connections to take place through the G-1000 v2.

Brute-Force Password Guessing Protection

The G-1000 v2 has a special protection mechanism to discourage brute-force password guessing attacks on the G-1000 v2'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.

Wireless LAN MAC Address Filtering

Your G-1000 v2 checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

WEP Encryption

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

IEEE 802.1X Network Security

The G-1000 v2 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.

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 v2 supports SNMP agent functionality, which allows a manager station to manage and monitor the G-1000 v2 through the network. The G-1000 v2 supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the G-1000 v2's management settings. Most functions of the G-1000 v2 are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

Logging and Tracing

- Built-in message logging.
- Unix syslog facility support.

Diagnostics Capabilities

The G-1000 v2 can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- DRAM
- LAN port
- Wireless port

Embedded FTP and TFTP Servers

The G-1000 v2's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the G-1000 v2 to access your wired network.

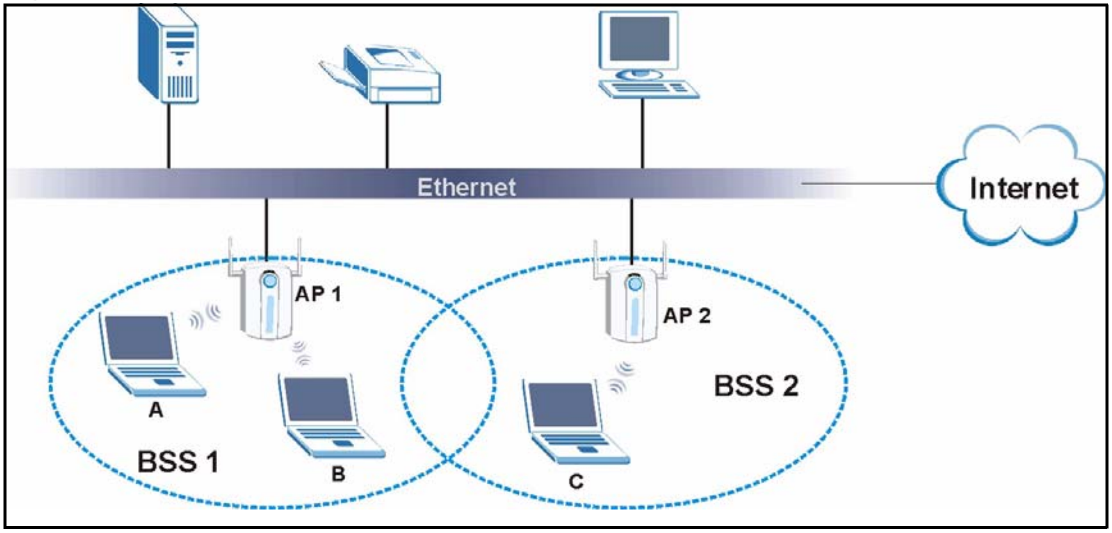
1.3 Applications for the G-1000 v2

Here are application examples of what you can do with your G-1000 v2.

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

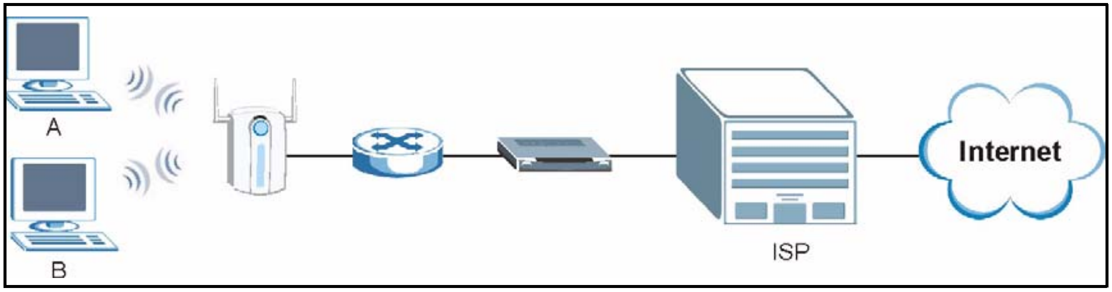


1.3.2 Corporation Network Application

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.

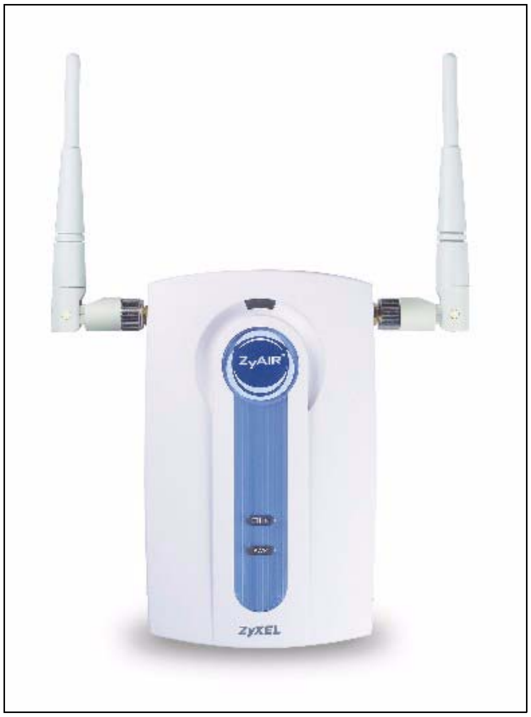
Figure 2 Corporation Network Application



1.4 Front Panel of the G-1000

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

Figure 3 G-1000 v2 Front Panel



The following table describes the lights.

Table 3 Front Panel Light Description

LIGHT	COLOR	STATUS	DESCRIPTION
SYS	Green	On	The wireless card on the G-1000 v2 is working properly.
		Off	The wireless card on the G-1000 v2 is not ready or has a malfunction.
	Red	Blinking	The G-1000 v2 is not ready or rebooting.
ZyAIR	Blue	Breathing	The G-1000 v2 is sending or receiving data.
		On (dim)	The G-1000 v2 is ready, but is not sending or receiving data.
ETHN	Green	On	The G-1000 v2 has a successful 10Mb Ethernet connection.
		Blinking	The G-1000 v2 is sending/receiving data.
		Off	The G-1000 v2 does not have 10Mb Ethernet connection.
	Orange	On	The G-1000 v2 has a successful 100Mb Ethernet connection.
		Blinking	The G-1000 v2 is sending or receiving data.
		Off	The G-1000 v2 does not have 100Mb Ethernet connection.
PWR	Green	On	The G-1000 v2 is receiving power.
		Off	The G-1000 v2 is not receiving power.

CHAPTER 2 Introducing the Web Configurator

This chapter describes how to access the G-1000 v2 web configurator and provides an overview of its screens. The default IP address of the G-1000 v2 is 192.168.1.2.

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the G-1000 v2 from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels.

2.2 Accessing the G-1000 v2 Web Configurator

1 Make sure your G-1000 v2 hardware is properly connected and prepare your computer/ computer network to connect to the G-1000 v2 (refer to the Quick Start Guide).

2 Launch your web browser.

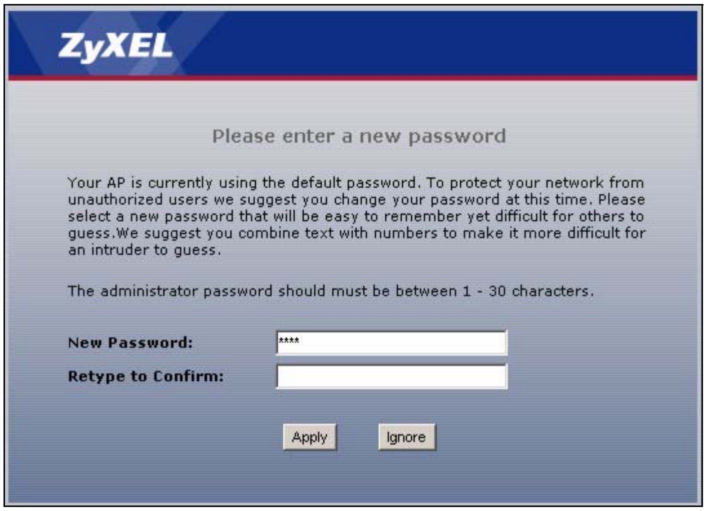
3 Type "192.168.1.2" as the URL.

4 Type "1234" (default) as the password and click **Login**.

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 4 Change Password Screen



Please enter a new password

Your AP is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.

The administrator password should must be between 1 - 30 characters.

New Password: ****

Retype to Confirm:

6 On this screen you can access the wizard setup or the advanced setup.

Click **Go to Advanced setup** to access the status screen of the web configurator.

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 v2 if this happens to you.

2.3 Resetting the G-1000 v2

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 top panel of the G-1000 v2. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to 1234.

2.3.1 .Procedure To Use The Reset Button

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

1 Press the **RESET** button for ten seconds or until the **SYS** light starts to blink, and then release it. If the **SYS** light begins to blink, the defaults have been restored and the G-1000 v2 restarts. Otherwise, go to step 2.

2 Turn the G-1000 v2 off.

3 While pressing the **RESET** button, turn the G-1000 v2 on.

4 Continue to hold the **RESET** button. The **SYS** light will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the G-1000 v2 is now restarting.

5 Release the **RESET** button and wait for the G-1000 v2 to finish restarting.

Note: You can also restore defaults via the web configurator.(refer to the Maintenance chapter).

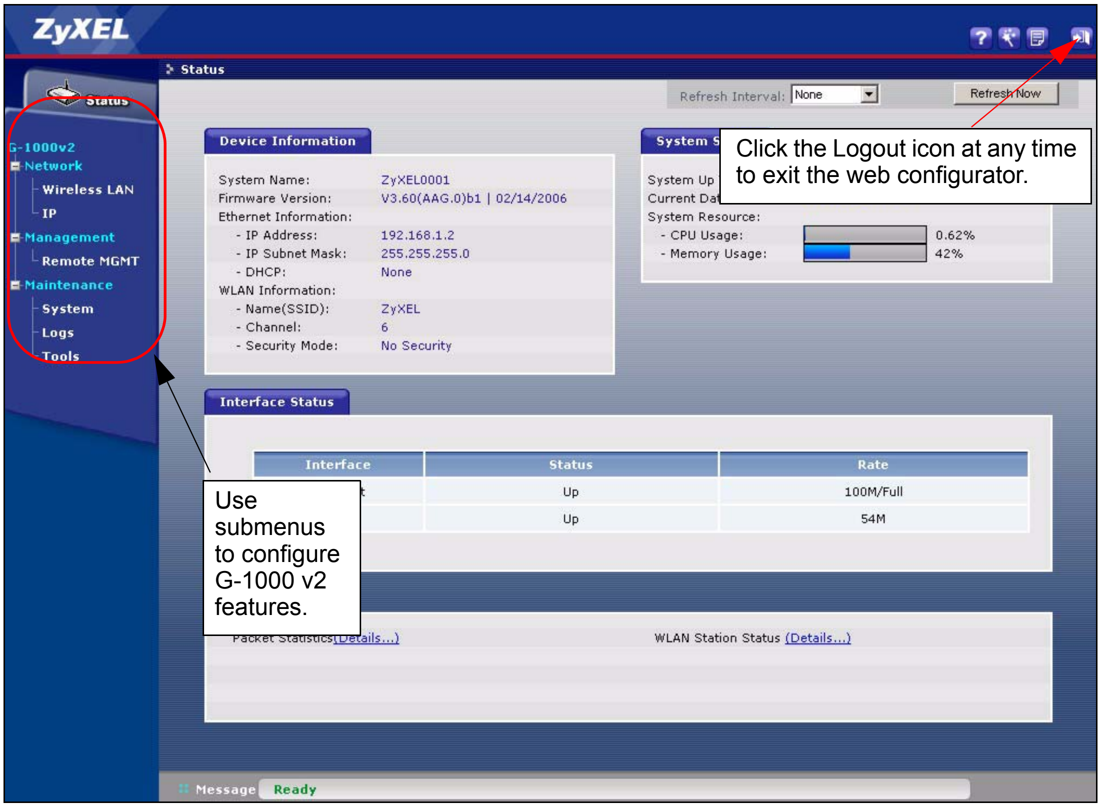
2.4 Navigating the Web Configurator

We use the P-662HW-D1 web screens in this guide as an example. Screens vary slightly for different G-1000 v2 models.

2.4.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure G-1000 v2 features. The following table describes the sub-menus.

Figure 5 Web Configurator: Main Screen



Refresh Interval: None

System Name: ZyXEL0001
Firmware Version: V3.60(AAG.0)b1 | 02/14/2006
Ethernet Information:
- IP Address: 192.168.1.2
- IP Subnet Mask: 255.255.255.0
- DHCP: None
WLAN Information:
- Name(SSID): ZyXEL
- Channel: 6
- Security Mode: No Security

System Up
Current Dat
System Resource:
- CPU Usage: 0.62%
- Memory Usage: 42%

Interface	Status	Rate
t	Up	100M/Full
	Up	54M

Packet Statistics(Details...)
WLAN Station Status (Details...)

Message Ready

Click the Logout icon at any time to exit the web configurator.

Use submenus to configure G-1000 v2 features.

Note: Click the ? icon (located in the top right corner of most screens) to view embedded help.

Table 4 Web Configurator Screens Summary

LINK/ICON	SUB-LINK	FUNCTION
Wizard		Use these screens for initial configuration including general setup, wireless security and IP address assignment.
Logout		Click this icon to exit the web configurator.

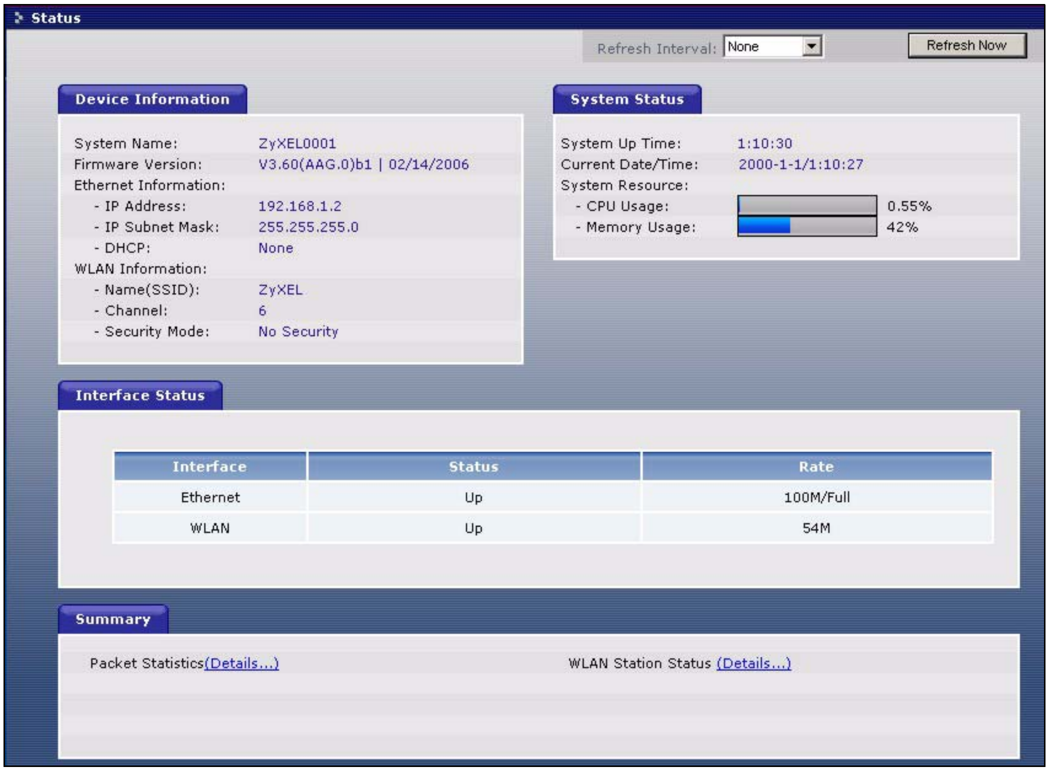
Table 4 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
About		Click this icon to see general information about G-1000 v2.
Status		This screen shows the G-1000 v2’s general device, system and interface status information. Use this screen to access the summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Filter	Use this screen to configure the G-1000 v2 to block access to devices or block the devices from accessing the G-1000 v2.
	Advanced	Use this screen to enable roaming and setup advanced wireless features.
IP	Internet Connection	Use this screen to configure IP address assignment.
	Advanced	Use this screen to configure your DNS server settings.
Management		
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the G-1000 v2.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the G-1000 v2.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the G-1000 v2.
	SNMP	Use this screen to configure your G-1000 v2’s settings for Simple Network Management Protocol management.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Time Setting	Use this screen to change your G-1000 v2’s time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your G-1000 v2’s log settings.
Tools	Firmware	Use this screen to upload firmware to your G-1000 v2.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your G-1000 v2.
	Restart	This screen allows you to reboot the G-1000 v2 without turning the power off.

2.4.2 Status Screen

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

Figure 6 Status Screen



Refresh Interval: None

System Name: ZyXEL0001
Firmware Version: V3.60(AAG.0)b1 | 02/14/2006
Ethernet Information:
- IP Address: 192.168.1.2
- IP Subnet Mask: 255.255.255.0
- DHCP: None

WLAN Information:
- Name(SSID): ZyXEL
- Channel: 6
- Security Mode: No Security

System Up Time: 1:10:30
Current Date/Time: 2000-1-1/1:10:27
System Resource:
- CPU Usage: 0.55%
- Memory Usage: 42%

Interface	Status	Rate
Ethernet	Up	100M/Full
WLAN	Up	54M

Packet Statistics(Details...)   WLAN Station Status (Details...)

The following table describes the labels shown in the **Status** screen.

Table 5 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance**, **System**, **General** screen. It is for identification purposes.
Firmware Version	This is the Firmware version and the date created.
Ethernet Information	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Relay** or **None**.
WLAN Information	
SSID	This is the descriptive name used to identify the G-1000 v2 in the wireless LAN.
Channel	This is the channel number used by the G-1000 v2 now.
Security Mode	This displays the security mode you are using.
System Status	

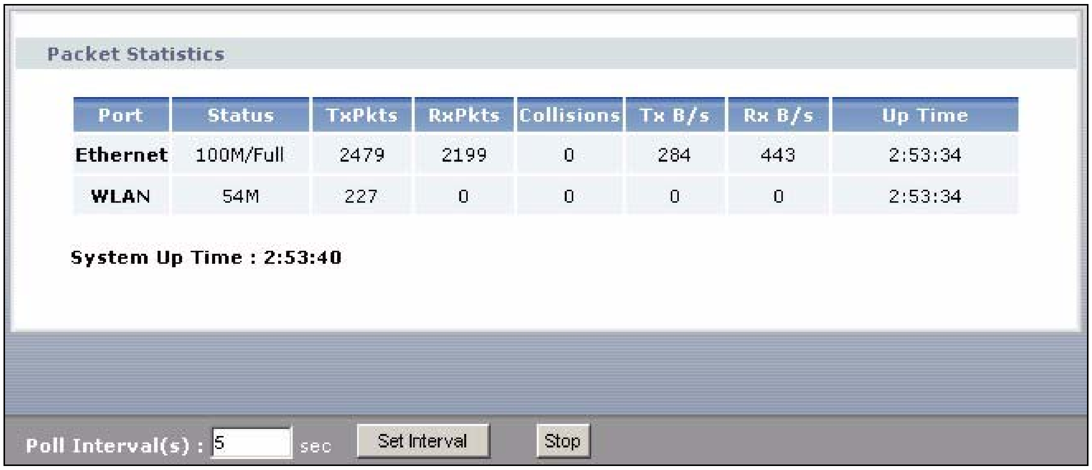
Table 5 Status Screen

LABEL	DESCRIPTION
System Uptime	This is the total time the G-1000 v2 has been on.
Current Date/Time	This field displays your G-1000 v2's present date and time.
System Resource	
CPU Usage	This number shows how many kilobytes of the heap memory the G-1000 v2 is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System). The bar displays what percent of the G-1000 v2's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Memory Usage	This number shows the G-1000 v2's total heap memory (in kilobytes). The bar displays what percent of the G-1000 v2's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Interface Status	
Interface	This displays the G-1000 v2 port types. The port types are **Ethernet** and **WLAN**.
Status	This field displays **Down** (line is down), **Up** (line is up or connected.
Rate	For the **Ethernet** port, this displays the port speed and duplex setting. For the **WAN** port, it displays the downstream and upstream transmission rate.
Summary	
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the G-1000 v2.

2.4.3 Status: Packet Statistics

To view packet statistics, click on Packet Statistics**(Details...)** link in the status screen under the **Summary** heading.

Figure 7 Status: Packet Statistics



Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
Ethernet	100M/Full	2479	2199	0	284	443	2:53:34
WLAN	54M	227	0	0	0	0	2:53:34

System Up Time : 2:53:40

Poll Interval(s) : 5 sec

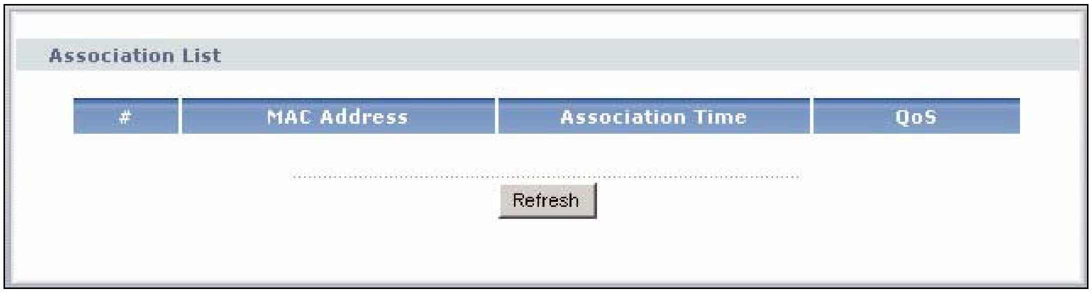
The following table describes the labels in this screen.

Table 6 Status: Packet 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. 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.

2.4.4 Status: WLAN Association List

To view packet statistics, click on Packet Statistics**(Details...)** link in the status screen under the **Summary** heading.



#	MAC Address	Association Time	QoS

The following table describes the labels in this screen.

Table 7 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 v2.

Table 7 Association List

LABEL	DESCRIPTION
QoS	This field displays the priority level of a wireless device associated with the G-1000 v2
Refresh	Click **Refresh** to reload the screen.

CHAPTER 3 Wizard Setup

The web configurator's setup wizard helps you set up a wireless LAN and configure security settings on your G-1000 v2.

3.1 Wizard Setup Overview

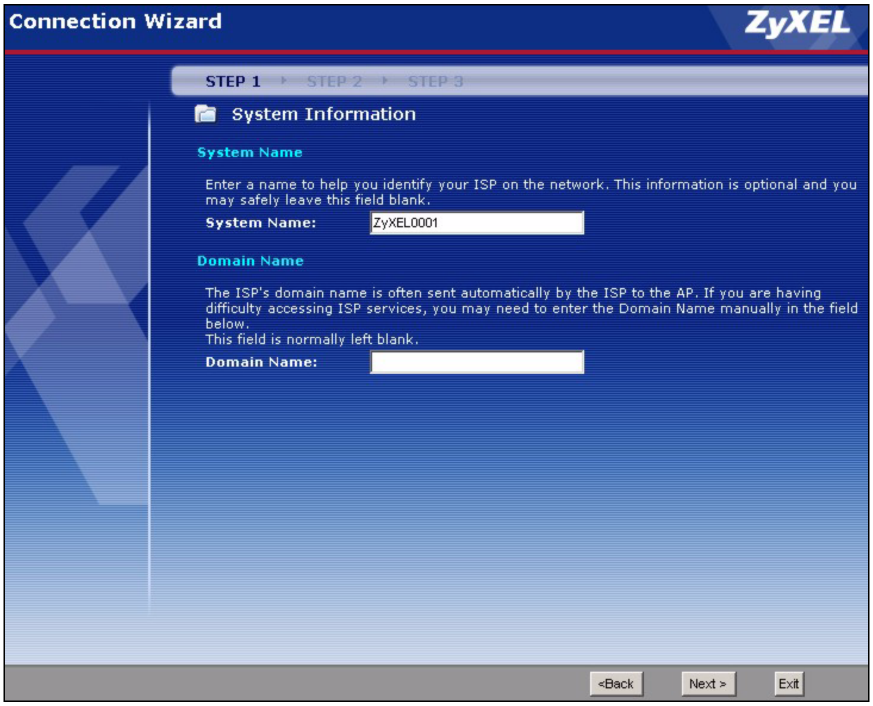
The wizard will guide you through several steps. You will need to enter some information for identification purposes, you will then setup your wireless LAN and security. The wizard will then guide you through configuring your Internet settings.

3.2 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 relayed via the G-1000 v2 from the DHCP server.

Figure 8 Enter System and Domain Names.



System Information

System Name

Enter a name to help you identify your ISP on the network. This information is optional and you may safely leave this field blank.

System Name: ZyXEL0001

Domain Name

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

Domain Name:

The following table describes the labels in this screen.

Table 8 Enter System and Domain Names

LABEL	DESCRIPTION
System Name	Enter a name to help you identify your ISP on the network. This is not a required field and you can safely leave this field blank.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to quit the wizard without saving the changes.

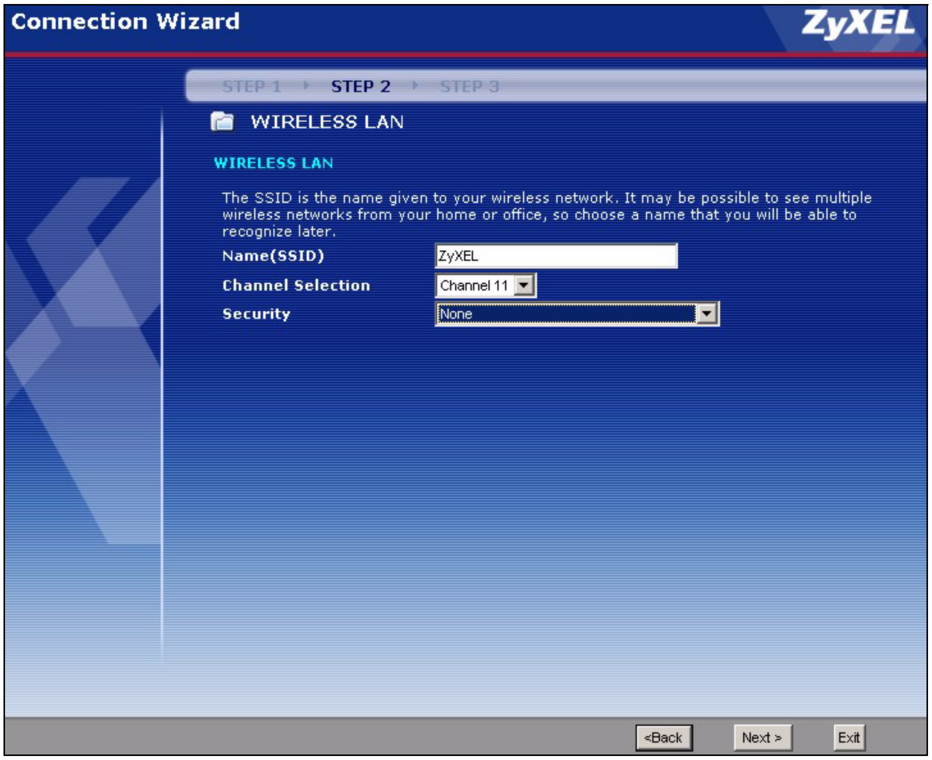
3.3 Wizard Setup Wireless LAN

This wizard helps you configure your wireless network and security.

3.3.1 Name (SSID), Channel ID and Security

This screen allows you to setup a unique name for your G-1000 v2 on the wireless network. You also decide on the channel for your wireless transmission and what kind of security you would like to use.

Figure 9 Enter Name and Select Security



WIRELESS LAN

The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.

Name(SSID): ZyXEL

Channel Selection: Channel 11

Security: None

The following table describes the labels in this screen.

Table 9 Enter Name and Select Security

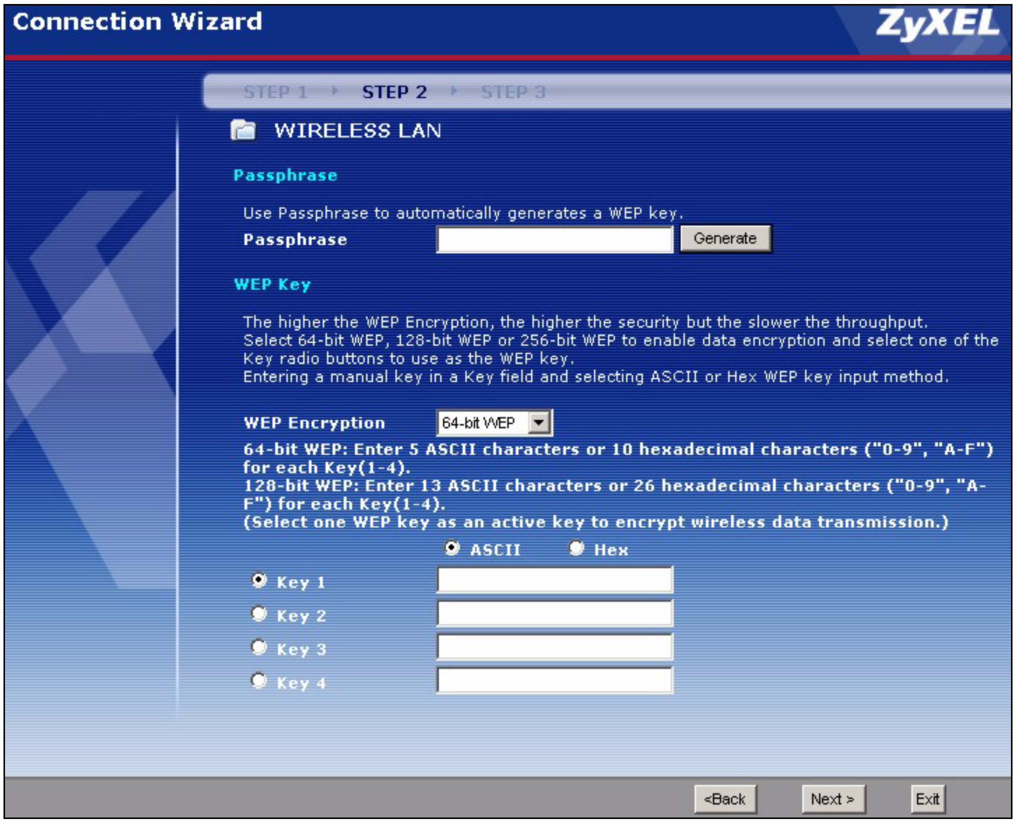
LABEL	DESCRIPTION
Wireless LAN Setup	
Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the G-1000 v2, make sure all wireless stations use the same SSID in order to access the network.
Choose Channel ID	To manually set the G-1000 v2 to use a specific channel, select a channel from the drop-down list box.
Security	The level of **Security** can be selected as none, basic or extended. Choose **None** security to have no wireless LAN security configured and proceed to the "Apply Settings" on page 47 section. Choose **Basic (WEP)** security if you want to configure **WEP Encryption** parameters. Choose **Extend (WPA-PSK with customized key)** or **Extend (WPA2-PSK with customized key)** security to configure a **Pre-Shared Key**. The next screen varies depending on which security level you select.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to quit the wizard without saving the changes.

Note: The wireless stations and G-1000 v2 must use the same SSID, channel ID and WEP encryption key (if WEP is enabled) or WPA-PSK (if WPA-PSK is enabled) for wireless communication.

3.3.2 Configuring WEP or WPA(2) PSK Security

Choose **Basic (WEP)** security to setup WEP Encryption parameters.

Figure 10 Wireless LAN Basic Security



Passphrase

Use Passphrase to automatically generates a WEP key.

Passphrase

WEP Key

The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP, 128-bit WEP or 256-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key.
Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.

WEP Encryption: 64-bit WEP

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

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

The following table describes the labels in this screen.

Table 10 Wireless LAN Basic Security

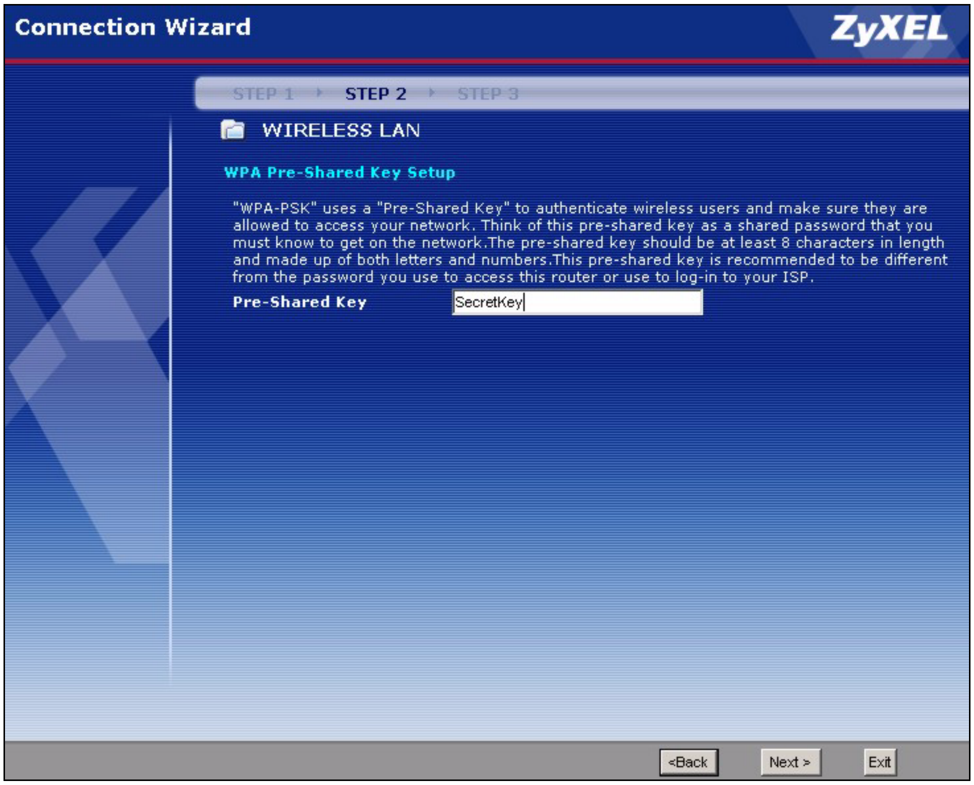
LABEL	DESCRIPTION
Passphrase	You can generate or manually enter a WEP key by either: Entering a **Passphrase** (up to 32 printable characters) and clicking **Generate**. The G-1000 v2 automatically generates a WEP key. Or Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the G-1000 v2 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

Table 10 Wireless LAN Basic Security

LABEL	DESCRIPTION
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to quit the wizard without saving the changes.

Choose **Extend(WPA-PSK with customized key)** or **Extend(WPA2-PSK with customized key)** security in the Wireless LAN Setup screen to set up a **Pre-Shared Key**.

Figure 11 Wireless LAN Extend Security



"WPA-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network.The pre-shared key should be at least 8 characters in length and made up of both letters and numbers.This pre-shared key is recommended to be different from the password you use to access this router or use to log-in to your ISP.

Pre-Shared Key: SecretKey

The following table describes the labels in this screen.

Table 11 Wireless LAN Extend Security

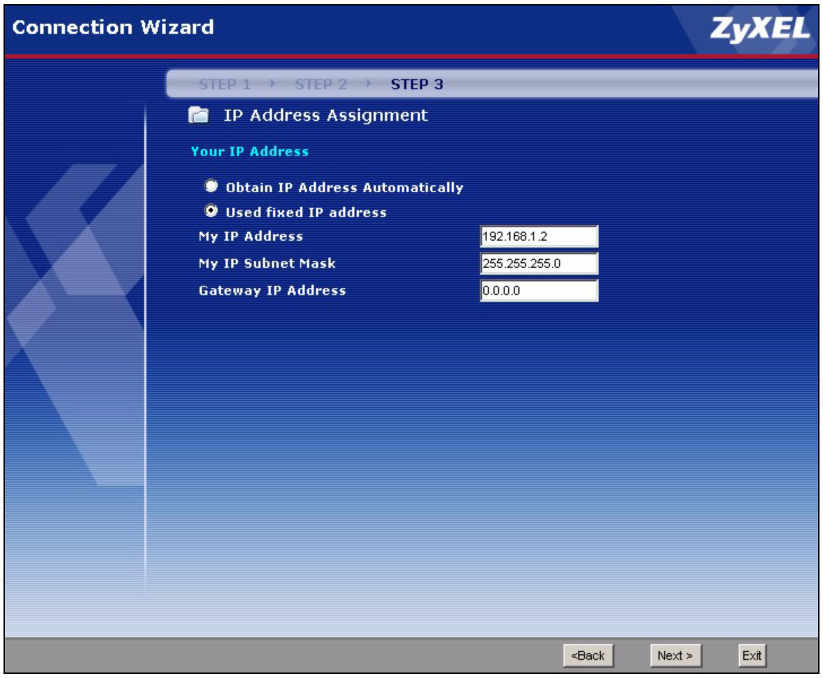
LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the advanced wireless screen. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to quit the wizard without saving the changes.

Refer to the chapter on wireless LAN for more information.

3.3.3 IP Address Assignment

Your G-1000 v2 needs an IP address to communicate with your wired network.

Figure 12 IP Address Assignment



IP Address Assignment

Your IP Address

○ Obtain IP Address Automatically

● Used fixed IP address

My IP Address: 192.168.1.2

My IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

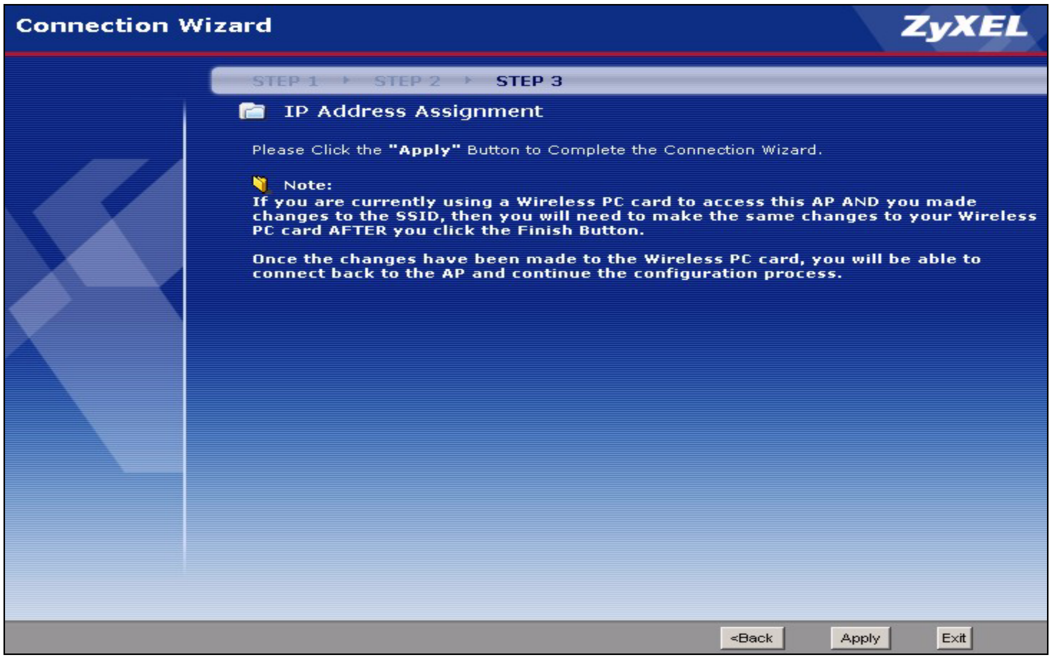
Table 12 IP Address Assignment

LABEL	DESCRIPTION
Obtain IP Address Automatically	Select this choice if your G-1000 v2 is using a dynamically assigned IP address from a DHCP server.
Use fixed IP address	Select this choice if your G-1000 v2 is using a static IP address.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to quit the wizard without saving the changes.

Note: If you change the IP address assigned to the G-1000 v2 or if a DHCP server assigns a new one to it, you must know it to access the G-1000 again.

3.3.4 Apply Settings

If you changed the SSID on your device or implemented any security, then you will have to make the corresponding changes on your wireless station to reconnect to the G-1000 v2.



Please Click the **"Apply"** Button to Complete the Connection Wizard.

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

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

The following table describes the labels in this screen.

Table 13 Apply Settings

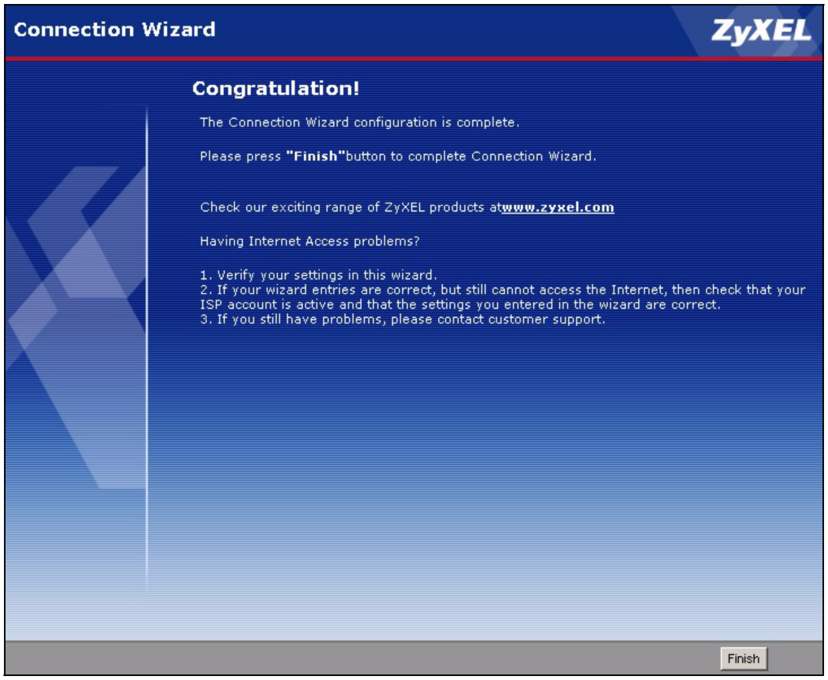
LABEL	DESCRIPTION
Back	Click **Back** to display the previous screen.
Apply	Click **Apply** to save your configuration settings.
Exit	Click **Exit** to quit the wizard without saving the changes.

Note: If you changed the SSID on your device or implemented any security, then you will have to make the corresponding changes on your wireless stations to reconnect to the AP.

If you changed the IP address of your G-1000 v2 or if an IP address is assigned to the G-1000 v2 automatically, you can access the device by using the new IP address or typing "**http://zyxelXXXX**" (where XXXX are the last four digits of your devices MAC address) in your browser. The MAC address can be found on the back label of your G-1000 v2.

Congratulations, you have completed your configuration wizard. Click **Finish** to exit the wizard.

Figure 13   Wizard Completed



Congratulation!

The Connection Wizard configuration is complete.

Please press **"Finish"**button to complete Connection Wizard.

Check our exciting range of ZyXEL products at**www.zyxel.com**

Having Internet Access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

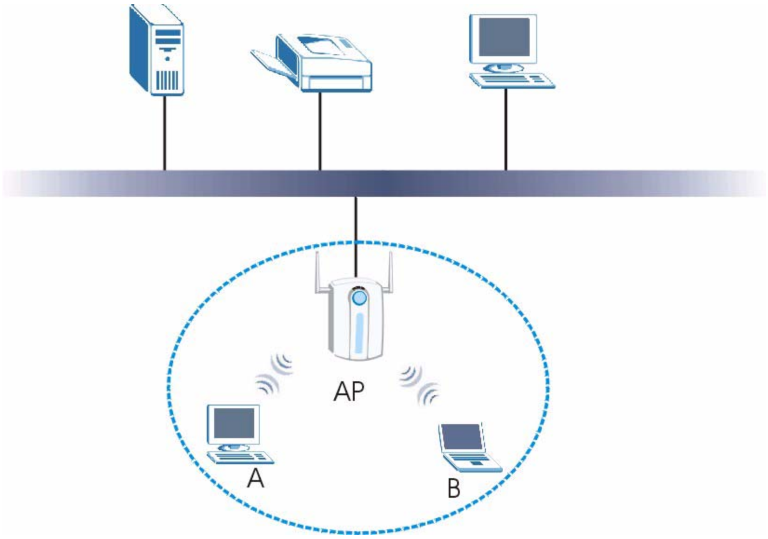
CHAPTER 4 Wireless LAN

This chapter discusses how to configure the wireless network settings in your G-1000 v2. See the appendices for more detailed information about wireless networks.

4.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 14 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your G-1000 v2 is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

4.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

4.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

4.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

4.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

4.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 4.2.3 on page 50 for information about this.)

Table 14 Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
Weakest	None	**IEEE 802.1x**
↕	**Static WEP**	**IEEE 802.1x + Static WEP**
	WPA-PSK	**WPA**
Strongest	**WPA2-PSK**	**WPA2**

For example, if the wireless network has a RADIUS server, you can choose **IEEE 802.1x**, **IEEE 802.1x + Static WEP**, **IEEE 802.1x + Dynamic WEP**, **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the G-1000 v2. The G-1000 v2 does not have a local user database, and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your G-1000 v2, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the G-1000 v2.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

4.3 Additional Wireless Terms

The following table describes wireless network terms and acronyms used in the G-1000 v2.

Table 15 Additional Wireless Terms

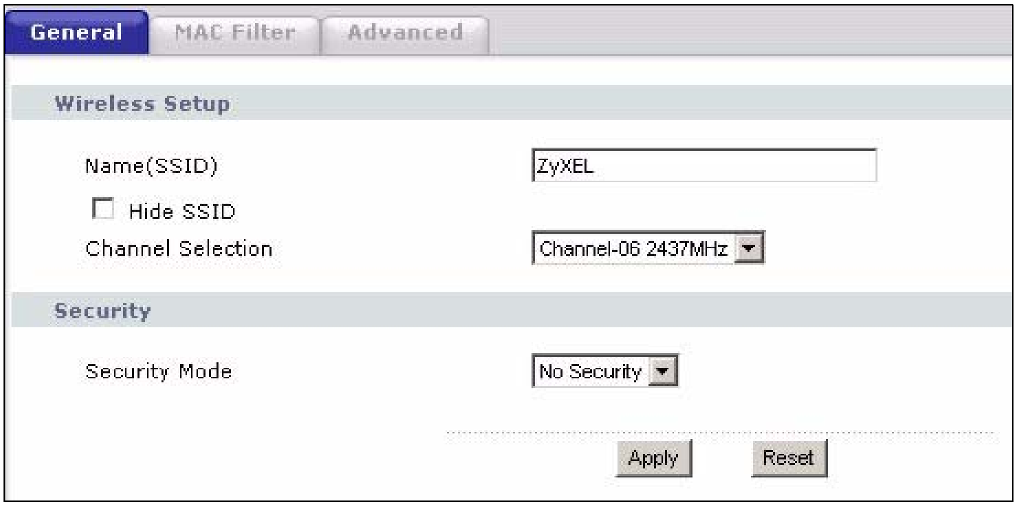
TERM	DESCRIPTION
Intra-BSS Traffic	This describes communication (through the AP) between two wireless clients within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	In a wireless network which covers a large area, wireless clients are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless clients must sometimes get permission to send information to the AP. The lower the value, the more often the wireless clients must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless clients never have to get permission to send information to the AP.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. Most wireless clients can detect the AP's preamble automatically. However, if a wireless client tries to use a different preamble mode than the AP does, it cannot communicate with the AP.
Max. Frame Burst	Enable this to improve the performance of pure IEEE 802.11g and mixed IEEE 802.11b/g networks. In pure IEEE 802.11g networks, set this to the maximum value. In mixed networks, the higher the value, the higher the priority of IEEE 802.11g traffic.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
Roaming	If you have two or more APs on your wireless network, you can enable this option so that wireless clients can change locations without having to log in again. This is useful for wireless clients, such as notebooks, that move around a lot.

4.4 Wireless LAN Screen

Note: If you are configuring the G-1000 v2 from a computer connected to the wireless LAN and you change the G-1000 v2's SSID 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 v2's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 15 Wireless LAN: General



Name(SSID) ZyXEL

□ Hide SSID

Channel Selection Channel-06 2437MHz

Security Mode No Security

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

Table 16 Wireless LAN: General

LABEL	DESCRIPTION
Wireless Setup	
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the G-1000 v2 from a computer connected to the wireless LAN and you change the G-1000 v2's SSID 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 v2's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security	See the rest of this chapter for information on the other labels in this screen.

Table 16 Wireless LAN: General

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

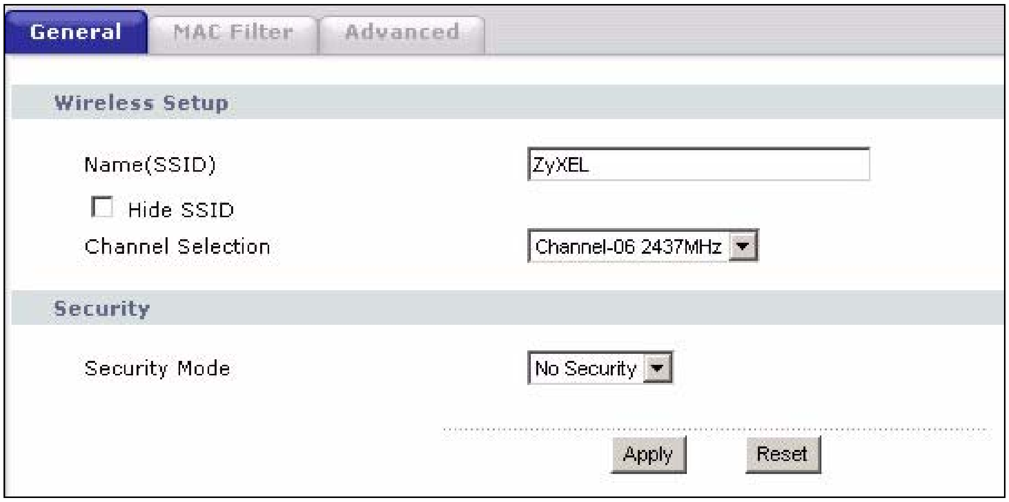
See the rest of this chapter for information on the other labels in this screen.

4.4.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your G-1000 v2, your network is accessible to any wireless networking device that is within range.

Figure 16 Wireless: No Security



Wireless Setup

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: No Security

The following table describes the labels in this screen.

Table 17 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

4.4.2 WEP Encryption

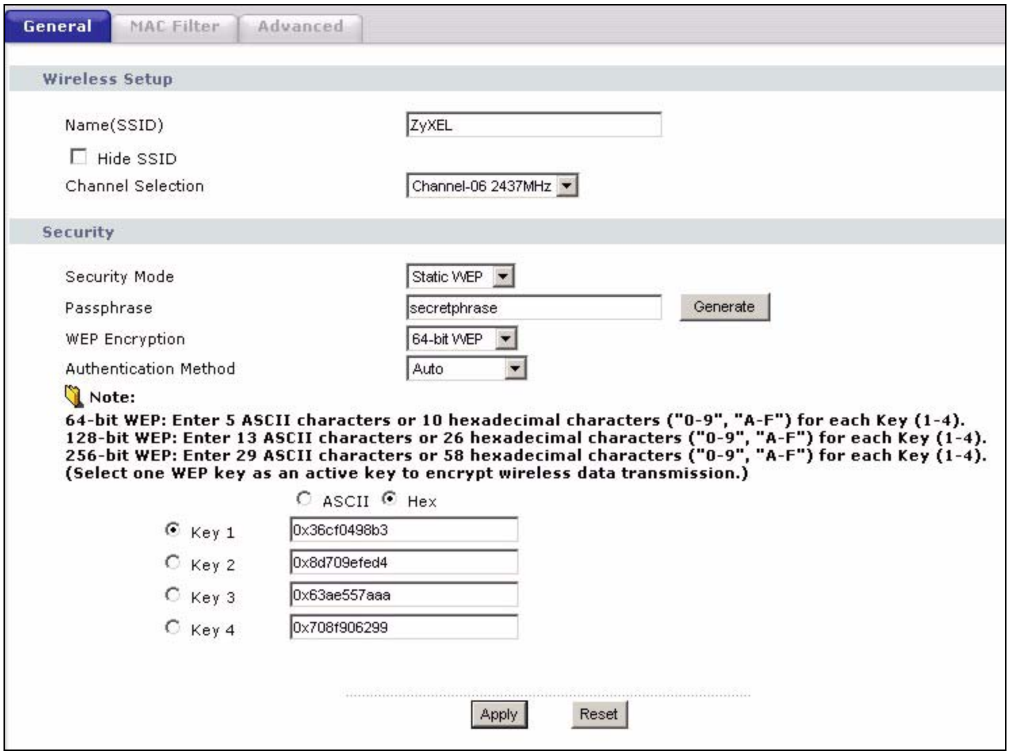
WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your G-1000 v2 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

4.4.3 WEP Encryption Screen

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 17 Wireless: Static WEP Encryption



Wireless Setup

Name(SSID): ZyXEL

☐ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: Static WEP

Passphrase: secretphrase

WEP Encryption: 64-bit WEP

Authentication Method: Auto

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
256-bit WEP: Enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● Hex

● Key 1: 0x36cf0498b3
○ Key 2: 0x8d709efed4
○ Key 3: 0x63ae557aaa
○ Key 4: 0x708f906299

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

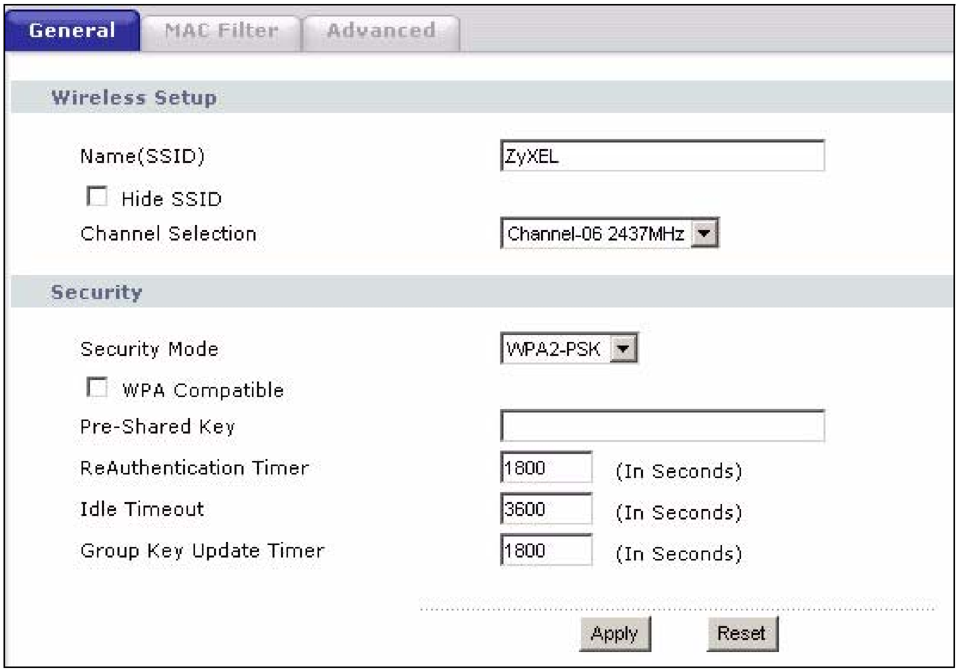
Table 18 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** from the drop-down list box.
Passphrase	You can generate or manually enter a WEP key by either: Entering a **Passphrase** (up to 32 printable characters) and clicking **Generate**. The G-1000 v2 automatically generates a WEP key. Or Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to allow data encryption.
Authentication Method	Select **Auto**, **Open System** or **Shared Key.**
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the G-1000 v2 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **256-bit WEP**, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
WEP Encryption	
WEP Key	The WEP keys are used to encrypt data. Both the G-1000 v2 and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.4 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 18 Wireless: WPA(2)-PSK



Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Security Mode: WPA2-PSK

□ WPA Compatible

Pre-Shared Key:

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

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

Table 19 Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the G-1000 v2 even when the G-1000 v2 is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (In Seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **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 v2 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. The default time interval is 3600 seconds (or 1 hour).

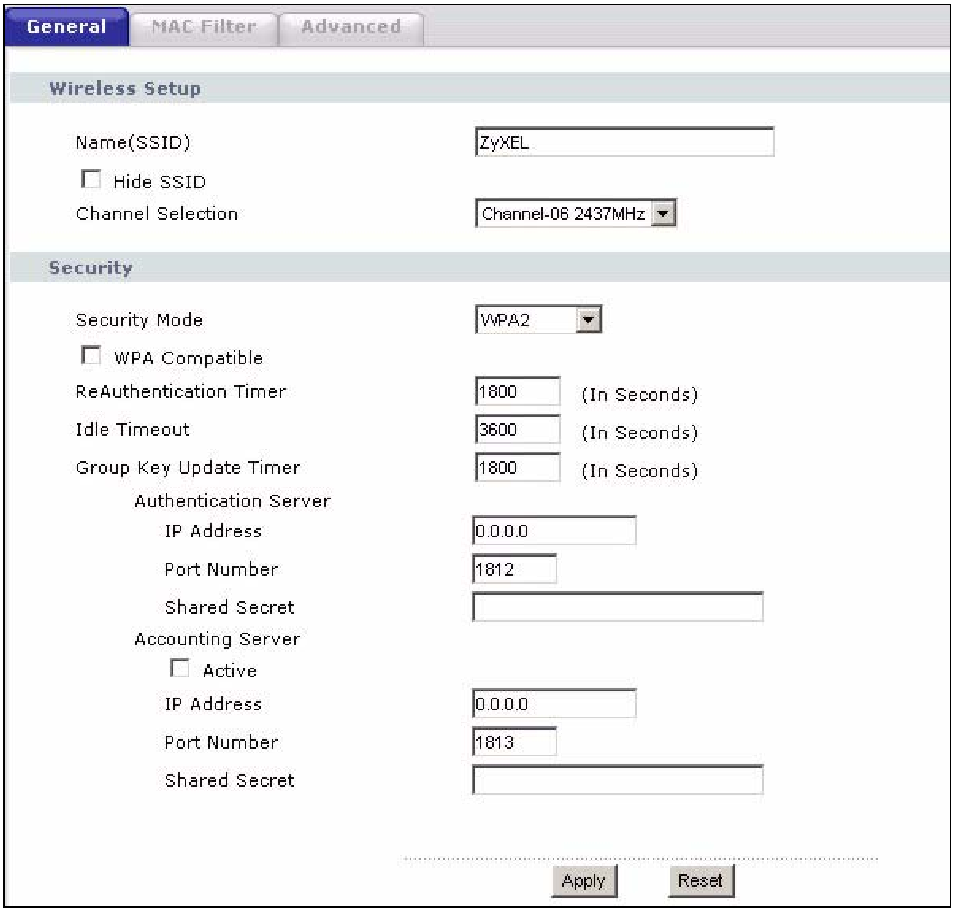
Table 19 Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Group Key Update Timer (In Seconds)	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The G-1000 v2 default is **1800** seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.5 WPA(2) Authentication Screen

In order to configure and enable WPA(2) Authentication; click the **Wireless LAN** link under **Network** to display the **Wireless** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 19 Wireless: WPA(2)



Wireless Setup

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: WPA2

□ WPA Compatible

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server

□ Active

IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

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

Table 20 Wireless: WPA(2)

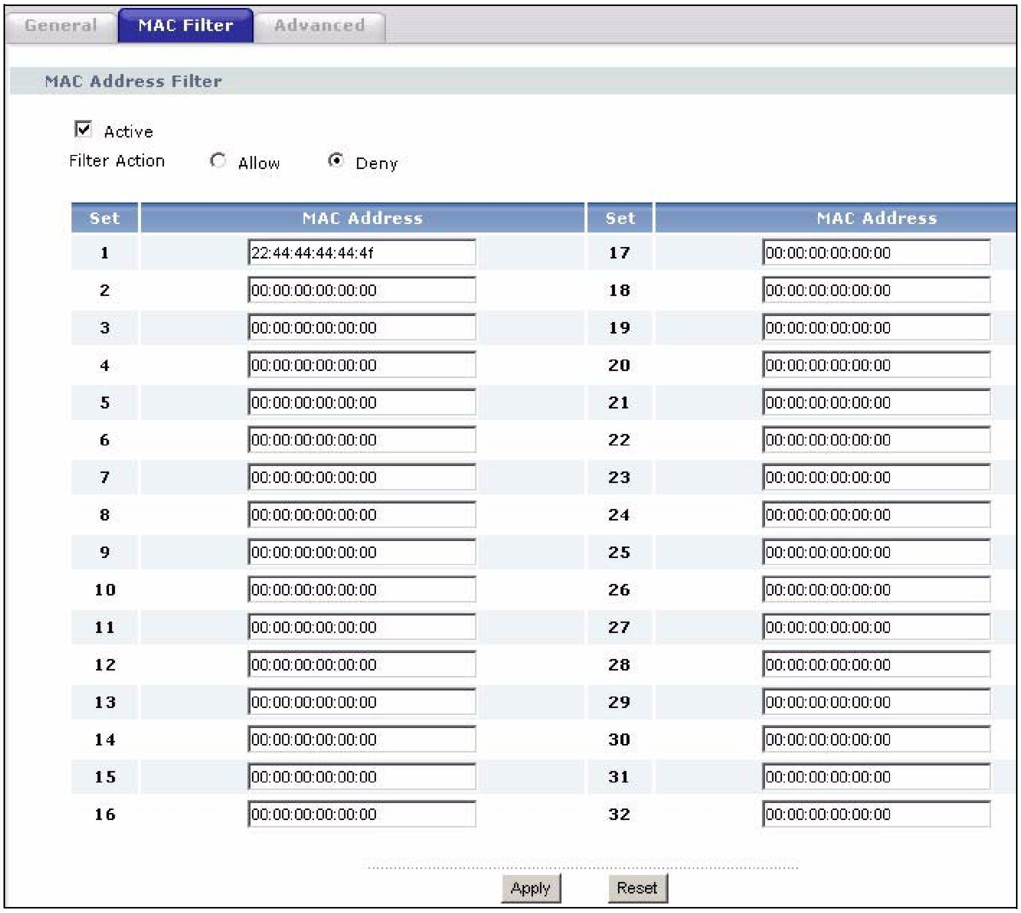
LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the G-1000 v2 even when the G-1000 v2 is using WPA2-PSK or WPA2.
ReAuthentication Timer (In Seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). **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 v2 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. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer (In Seconds)	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The G-1000 v2 default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the G-1000 v2. The key must be the same on the external authentication server and your G-1000 v2. The key is not sent over the network.
Accounting Server (optional)	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the G-1000 v2. The key must be the same on the external accounting server and your G-1000 v2. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.5 MAC Filter

The MAC filter screen allows you to configure the G-1000 v2 to give exclusive access to up to 32 devices (**Allow**) or exclude up to 32 devices from accessing the G-1000 v2 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your G-1000 v2’s MAC filter settings, click **Network > Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 20 MAC Address Filter



MAC Address Filter

☑ Active

Filter Action ○ Allow ● Deny

Set	MAC Address	Set	MAC Address
1	22:44:44:44:44:4f	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 menu.

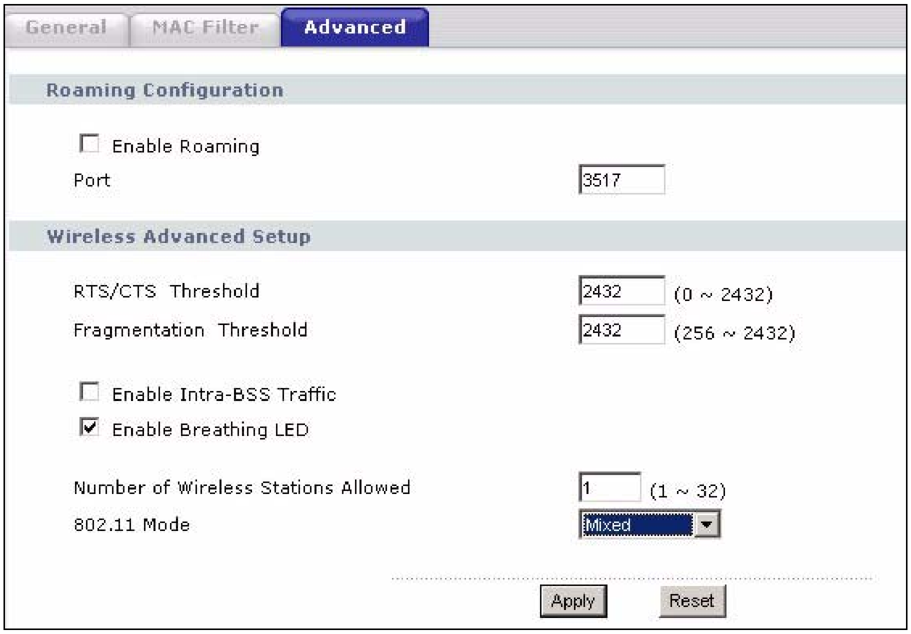
Table 21 MAC Address Filter

LABEL	DESCRIPTION
Active	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the G-1000 v2, MAC addresses not listed will be allowed to access the G-1000 v2 Select **Allow** to permit access to the G-1000 v2, MAC addresses not listed will be denied access to the G-1000 v2.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the G-1000 v2 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.6 Wireless LAN Advanced Setup

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced**. The screen appears as shown.

Figure 21 Wireless LAN: Advanced



Roaming Configuration

□ Enable Roaming

Port: 3517

Wireless Advanced Setup

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

□ Enable Intra-BSS Traffic

☑ Enable Breathing LED

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

802.11 Mode: Mixed

The following table describes the labels in this screen.

Table 22 Wireless LAN: Advanced

LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	Select this checkbox to enable roaming on the G-1000 v2 if you have two or more G-1000 v2s on the same subnet. **Note:** All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Port	Enter the port number to communicate roaming information between APs. The port number must be the same on all APs. The default is 3517. Make sure this port is not used by other services.
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the **Enable 802.11g+ mode** checkbox, this field is grayed out and the G-1000 v2 uses 4096 automatically.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the **Enable 802.11g+ mode** checkbox, this field is grayed out and the G-1000 v2 uses 4096 automatically.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the BSS (Basic Service Set). Select this check box to enable Intra-BSS Traffic.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the G-1000 v2 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 v2 is on and data is being transmitted/received.
Number of Wireless Stations Allowed	Enter a number from 1 to 32, to limit the number of wireless devices which can communicate in your wireless network.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-1000 v2. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-1000 v2. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the G-1000 v2. The transmission rate of your G-1000 v2 might be reduced.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

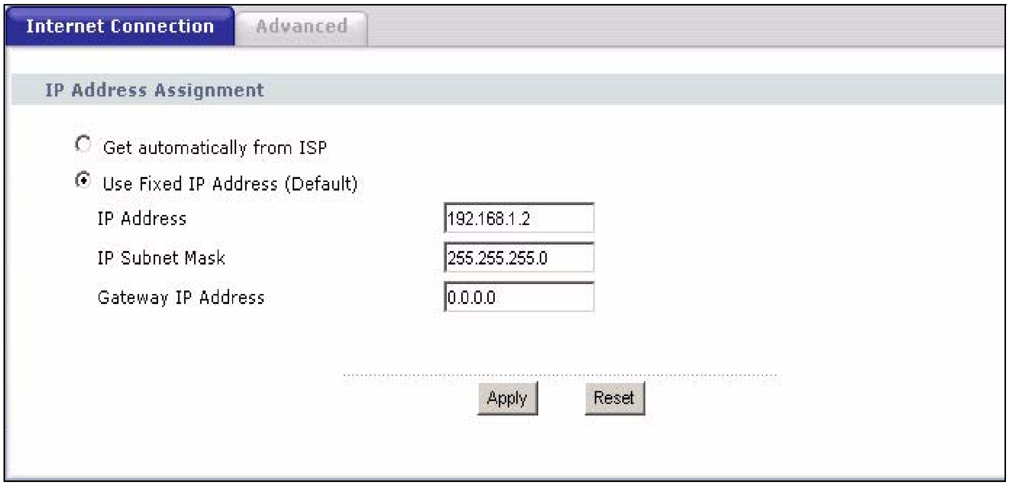
CHAPTER 5
IP and DNS Screens

This chapter describes how to configure your G-1000 v2 to interact with the wired network.

5.1 Configuring IP

To configure Internet connection, click **Network** > **IP** > **Internet Connection**. The screen appears as shown.

Figure 22 Network: Internet Connection



○ Get automatically from ISP

● Use Fixed IP Address (Default)

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 23 Network: Internet Connection

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your G-1000 v2 is using a dynamically assigned IP address from a DHCP server each time. **Note:** If you change the IP address of your G-1000 v2 or if an IP address is assigned to the G-1000 v2 automatically, you can access the device by using the new IP address or typing "**http://zyxelXXXX**" (where XXXX are the last four digits of your device's MAC address) in your browser. The MAC address can be found on the back label of your G-1000 v2.
Use fixed IP address	Select this option if your G-1000 v2 is using a static IP address. When you select this option, fill in the fields below.

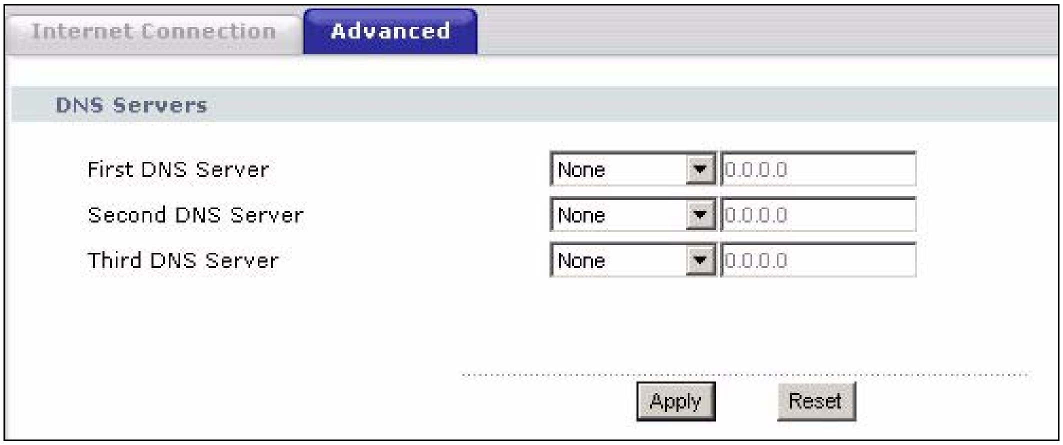
Table 23 Network: Internet Connection

LABEL	DESCRIPTION
IP Address	Enter the IP address of your G-1000 v2 in dotted decimal notation.
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 v2 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 v2; over the WAN, the gateway must be the IP address of one of the remote nodes.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.2 Configuring DNS

To configure DNS settings, click **Network > IP > Advanced**. The screen appears as shown.

Figure 23 Network: Advanced



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 24 Network: Advanced

LABEL	DESCRIPTION
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your DHCP server dynamically assigns DNS server information (and the G-1000 v2's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to None after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is **None**.

Table 24 Network: Advanced

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Reset	Click **Reset** to reload the previous configuration for this screen.

CHAPTER 6 Remote Management Configuration

This chapter provides information on configuring remote management.

6.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which G-1000 v2 interface (if any) from which computers.

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your G-1000 v2 from a remote location via:

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

Note: When you choose **WAN** only or **LAN & WAN**, you still need to configure a firewall rule to allow access.

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

You may only have one remote management session running at a time. The G-1000 v2 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

6.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- You have disabled that service in one of the remote management screens.

- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the G-1000 v2 will disconnect the session immediately.
- 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.
- There is a firewall rule that blocks it.

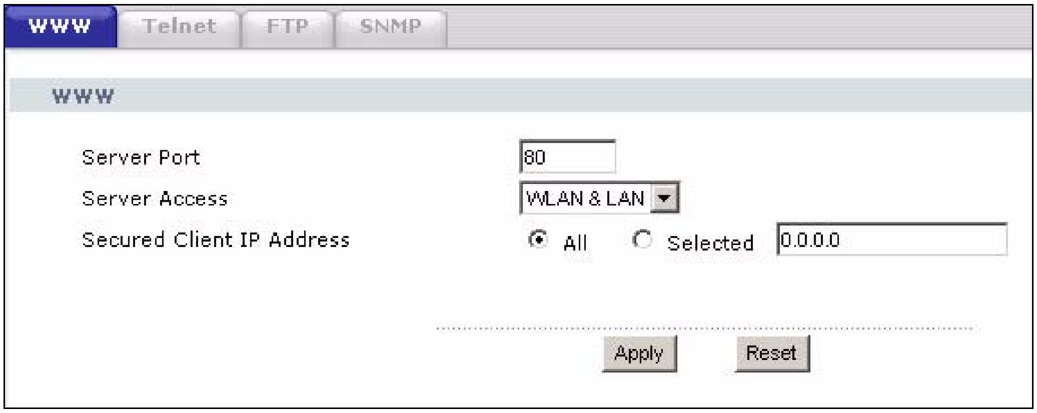
6.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The G-1000 v2 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.

6.2 WWW

To change your G-1000 v2’s World Wide Web settings, click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 24 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
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 v2 using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the G-1000 v2 using this service. Select **All** to allow any computer to access the G-1000 v2 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 v2 using this service.

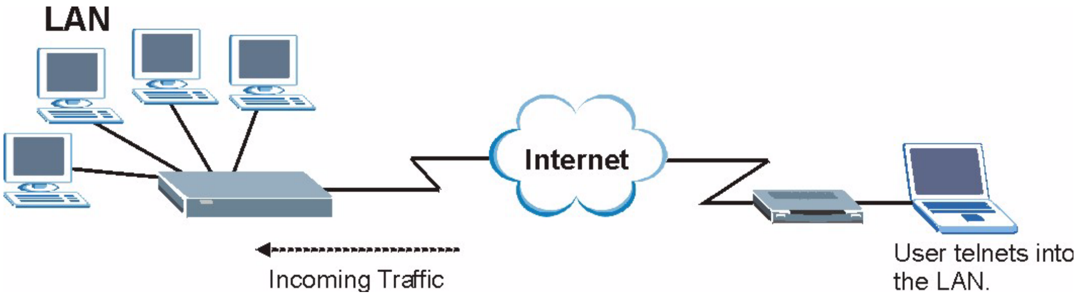
Table 25 Remote Management: WWW

LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings back to the G-1000 v2.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.3 Telnet

You can configure your G-1000 v2 for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the G-1000 v2.

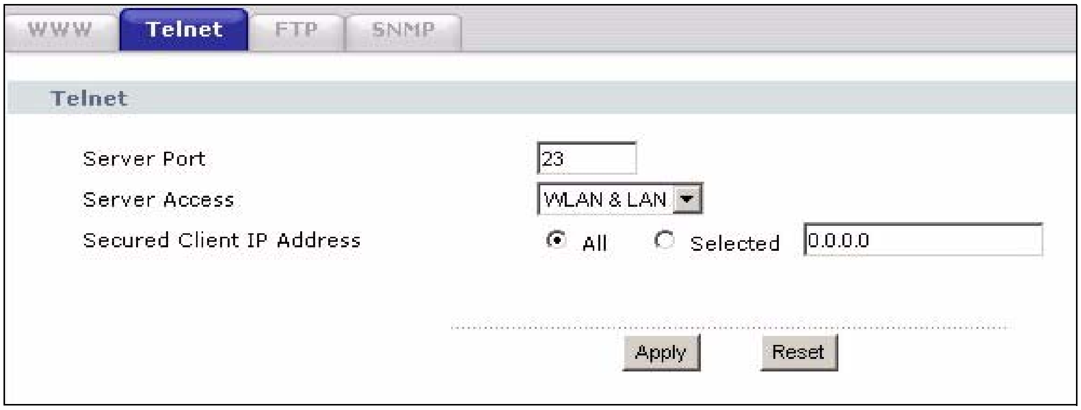
Figure 25 Telnet Configuration on a TCP/IP Network



6.4 Configuring Telnet

Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 26 Remote Management: 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

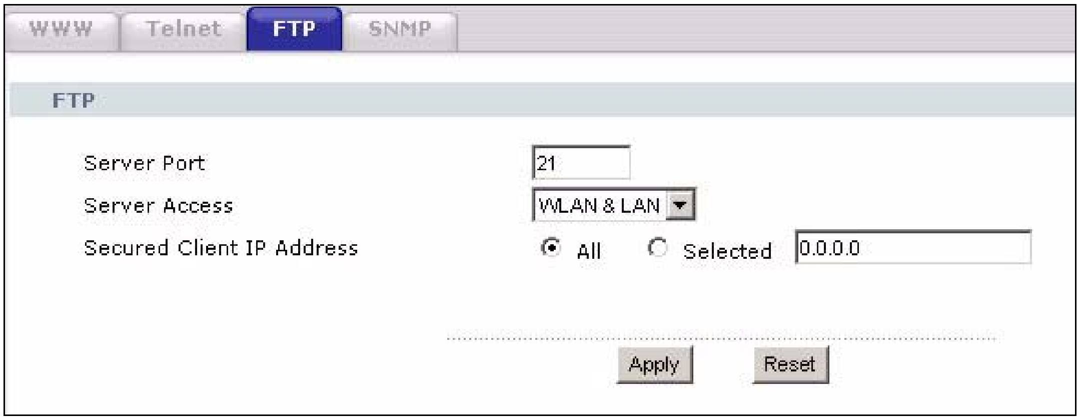
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the G-1000 v2 using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the G-1000 v2 using this service. Select **All** to allow any computer to access the G-1000 v2 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 v2 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.5 Configuring FTP

You can upload and download the G-1000 v2'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 v2's FTP settings, click **Advanced > Remote MGMT** > **FTP** tab. The screen appears as shown.

Figure 27 Remote Management: 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

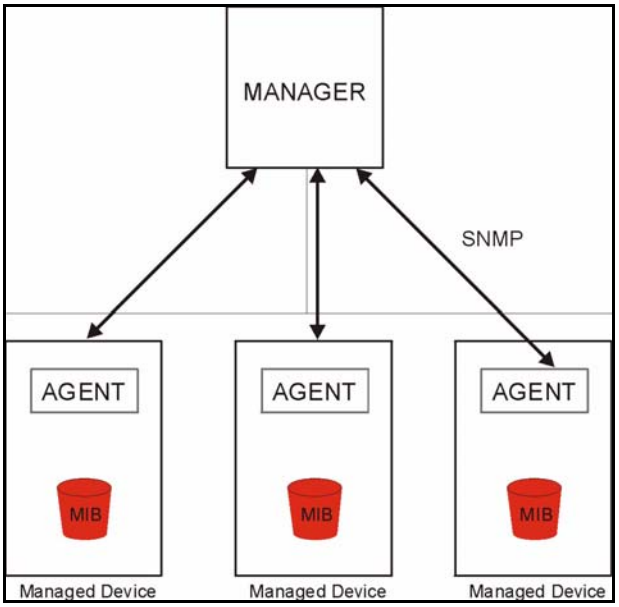
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the G-1000 v2 using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the G-1000 v2 using this service. Select **All** to allow any computer to access the G-1000 v2 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 v2 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.6 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 v2 supports SNMP agent functionality, which allows a manager station to manage and monitor the G-1000 v2 through the network. The G-1000 v2 supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

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

Figure 28 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 v2). 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.

6.6.1 Supported MIBs

The G-1000 v2 supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

6.6.2 SNMP Traps

The G-1000 v2 will send traps to the SNMP manager when any one of the following events occurs:

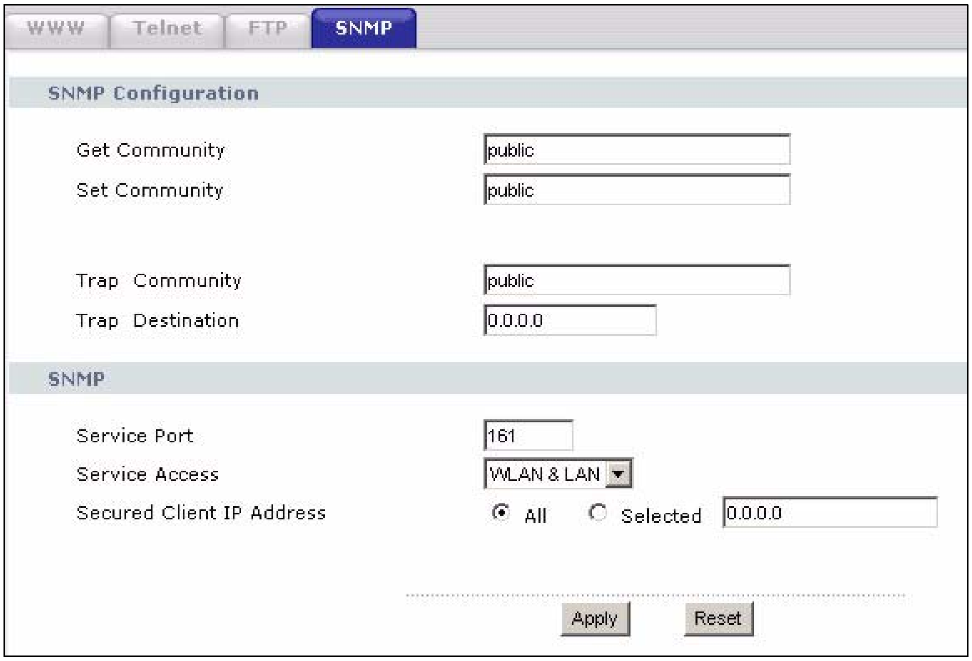
Table 28 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

6.6.3 Configuring SNMP

To change your G-1000 v2's SNMP settings, click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Figure 29 Remote Management: SNMP



Get Community: public

Set Community: public

Trap Community: public

Trap Destination: 0.0.0.0

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 29 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.
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.
Trap 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.
Server Access	Select the interface(s) through which a computer may access the G-1000 v2 using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the G-1000 v2 using this service. Select **All** to allow any computer to access the G-1000 v2 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the G-1000 v2 using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 7
System

Use this screen to configure the G-1000 v2's time and date settings.

7.1 General Setup

7.1.1 General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

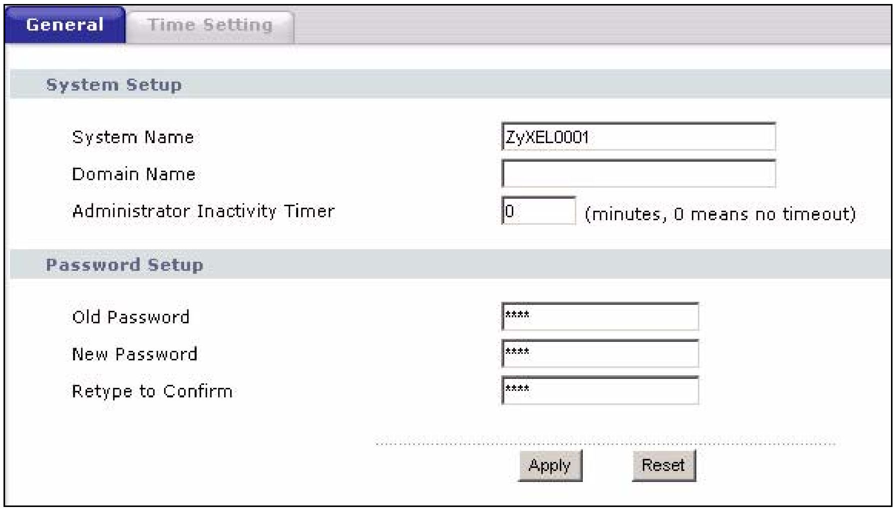
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the G-1000 v2 **System Name**.

7.1.2 General Setup

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), the domain name can be assigned from the G-1000 v2 via DHCP.

Click **Maintenance > System** to open the **General** screen.

Figure 30 System General Setup



System Setup

System Name: ZyXEL0001

Domain Name:

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

Password Setup

Old Password: ****

New Password: ****

Retype to Confirm: ****

The following table describes the labels in this screen.

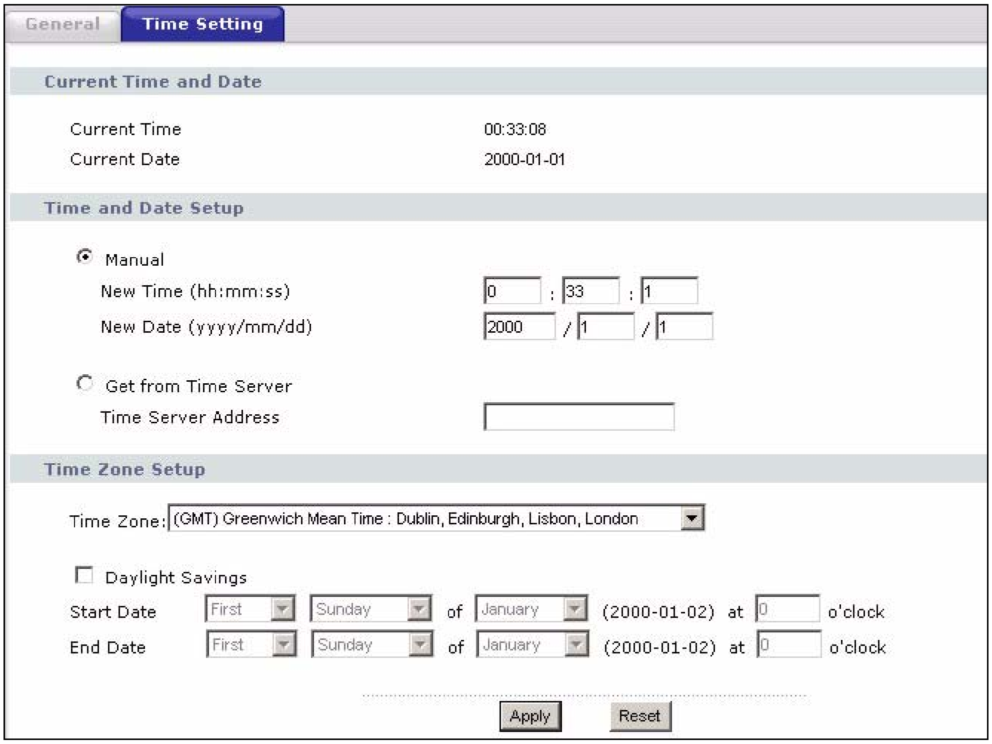
Table 30 System General Setup

LABEL	DESCRIPTION
System Setup	
System Name	Enter a name to help you identify your ISP on the network. This is not a required field and you can safely leave this field blank.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or CLI (Command Line Interpreter)) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	
User Password	Type your current password. The default password is **1234**.
New Password	Type your new password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the G-1000 v2.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.2 Time Setting

To change your G-1000 v2’s time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the G-1000 v2’s time based on your local time zone.

Figure 31 System Time Setting



Current Time and Date

Current Time 00:33:08

Current Date 2000-01-01

Time and Date Setup

● Manual

New Time (hh:mm:ss) 0 : 33 : 1

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

○ Get from Time Server

Time Server Address

Time Zone Setup

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

□ Daylight Savings

Start Date First Sunday of January (2000-01-02) at 0 o'clock

End Date First Sunday of January (2000-01-02) at 0 o'clock

The following table describes the fields in this screen.

Table 31 System Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your G-1000 v2. Each time you reload this page, the G-1000 v2 synchronizes the time with the time server.
Current Date	This field displays the date of your G-1000 v2. Each time you reload this page, the G-1000 v2 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.

Table 31 System Time Setting (continued)

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the G-1000 v2 get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Savings	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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 31 System Time Setting (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the G-1000 v2.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 8
Logs

This chapter contains information about configuring general log settings and viewing the G-1000 v2's logs. Refer to the appendix for example log message explanations.

8.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the G-1000 v2 log and then display the logs or have the G-1000 v2 send them to an administrator (as e-mail) or to a syslog server.

8.1.1 Alerts and Logs

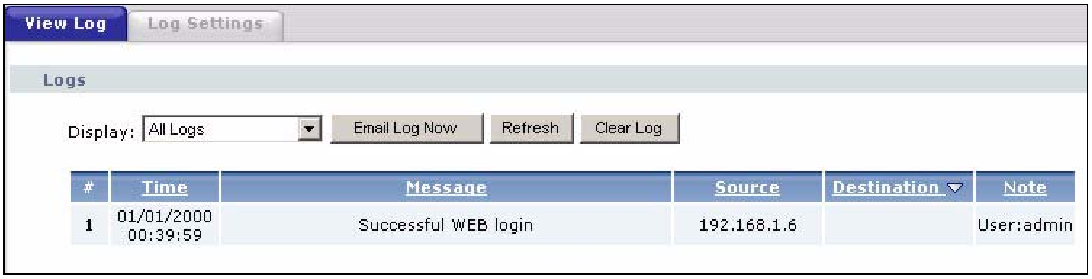
An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen.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

8.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see "Configuring Log Settings" on page 82).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 32 View Log



Display: All Logs

#	Time	Message	Source	Destination ▽	Note
1	01/01/2000 00:39:59	Successful WEB login	192.168.1.6		User:admin

The following table describes the fields in this screen.

Table 32 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

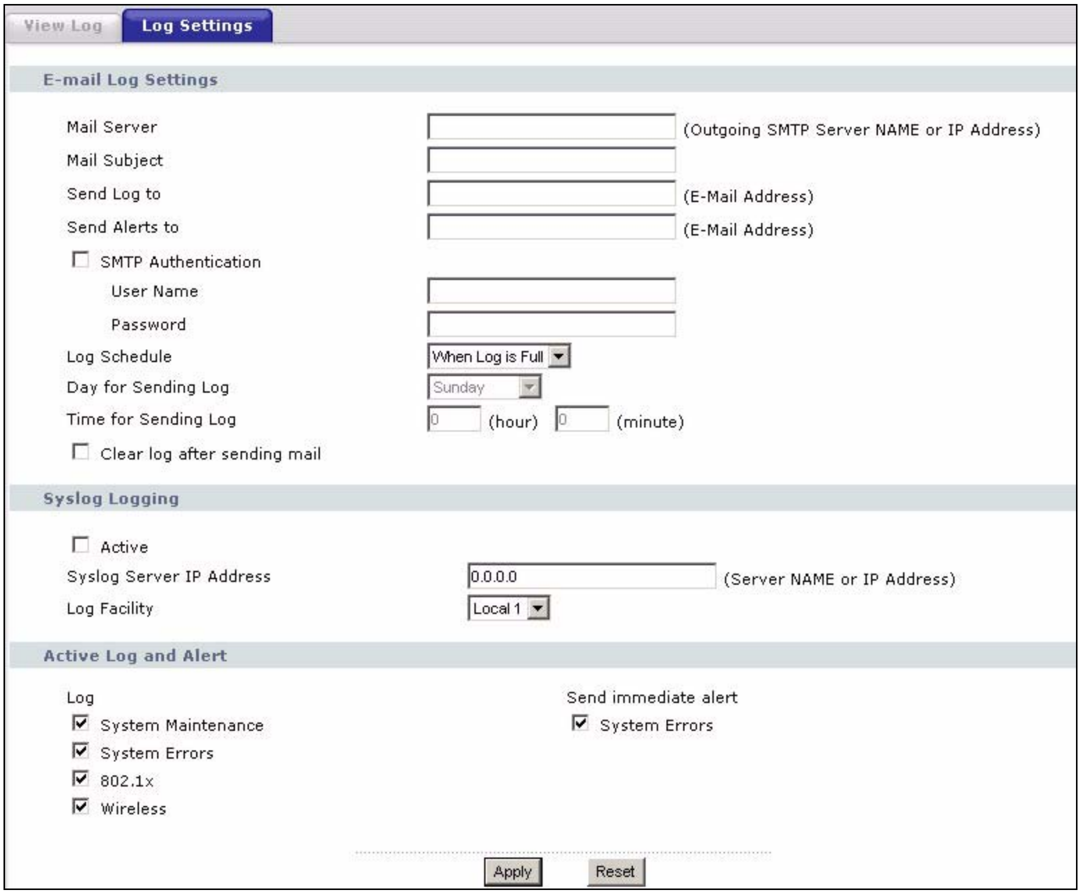
8.3 Configuring Log Settings

Use the **Log Settings** screen to configure to where the G-1000 v2 is to send logs; the schedule for when the G-1000 v2 is to send the logs and which logs and/or immediate alerts the G-1000 v2 is to record. See "Logs Overview" on page 81 for more information.

To change your G-1000 v2's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 33 Log Settings



E-mail Log Settings

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

Log Schedule: When Log is Full

Day for Sending Log: Sunday

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

□ Clear log after sending mail

Syslog Logging

□ Active

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

Log Facility: Local 1

Active Log and Alert

Log	Send immediate alert
☑ System Maintenance	☑ System Errors
☑ System Errors	
☑ 802.1x	
☑ Wireless	

The following table describes the fields in this screen.

Table 33 Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
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 v2 sends. Not all G-1000 v2 models have this field.
Send Log To	The G-1000 v2 sends logs to the e-mail address specified in this field. If this field is left blank, the G-1000 v2 does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).

Table 33 Log Settings

LABEL	DESCRIPTION
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None**. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	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 checkbox to delete all the logs after the G-1000 v2 sends an E-mail of the logs.
Syslog Logging	The G-1000 v2 sends a log to an external syslog server.
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 syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the G-1000 v2 to send E-mail alerts immediately.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

8.4 SMTP Error Messages

The following table lists common SMTP errors.

Table 34 SMTP Error Messages

-1 means G-1000 v2 out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail

Table 34 SMTP Error Messages

-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

CHAPTER 9 Tools

This chapter describes how to upload new firmware, manage configuration and restart your G-1000 v2.

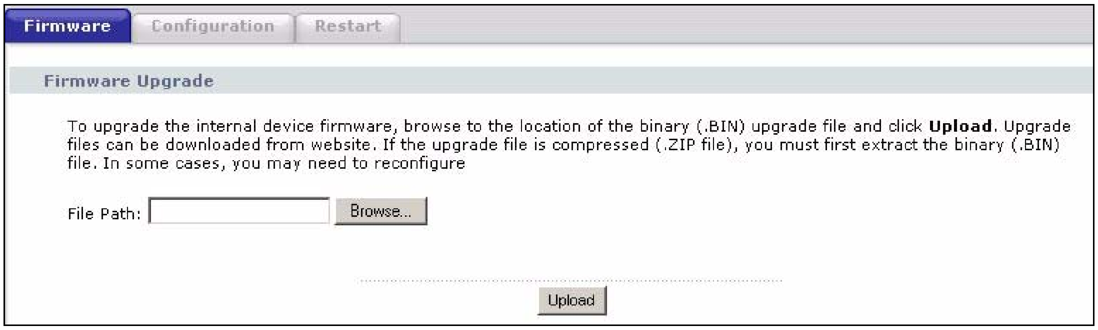
9.1 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a.bin extension, for example, "G-1000 v2.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

Click **Maintenance** > **Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your G-1000 v2.

Figure 34 Firmware Upgrade



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.

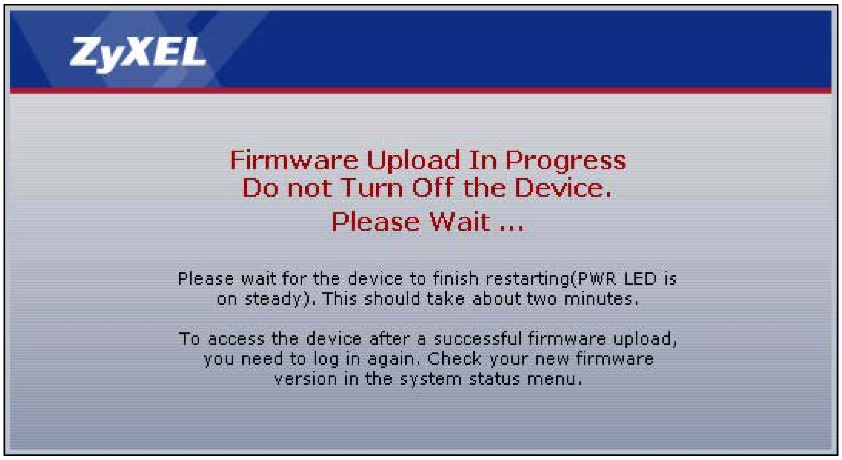
Table 35 Firmware Upgrade

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 v2 while firmware upload is in progress!

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the G-1000 v2 again.

Figure 35 Firmware Upload In Progress



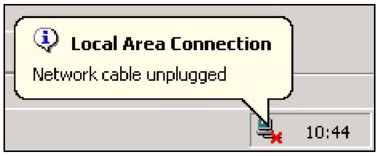
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...

Please wait for the device to finish restarting(PWR 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 your new firmware version in the system status menu.

The G-1000 v2 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 36 Network Temporarily Disconnected

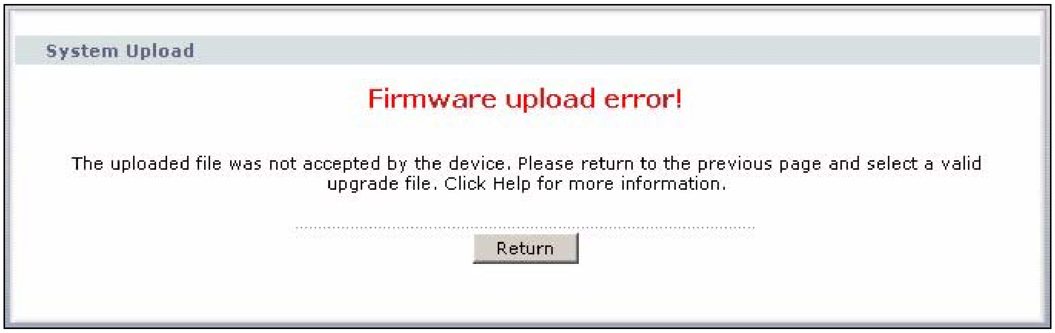


Local Area Connection
Network cable unplugged

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

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

Figure 37 Error Message



System Upload

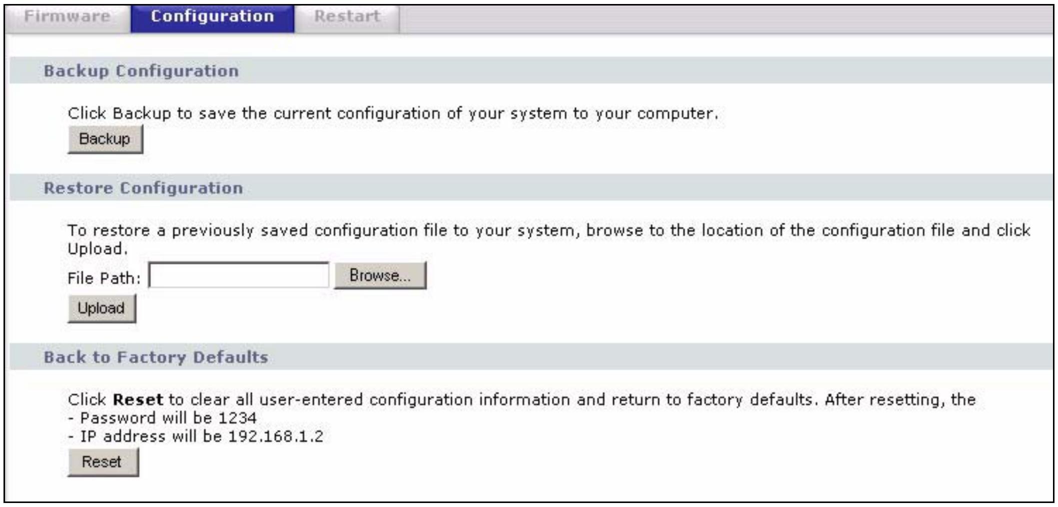
Firmware upload error!

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.

9.2 Configuration Screen

Click **Maintenance > Tools** > **Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 38 Configuration



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

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

File Path:

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

9.2.1 Backup Configuration

Backup configuration allows you to back up (save) the G-1000 v2's current configuration to a file on your computer. Once your G-1000 v2 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 v2's current configuration to your computer

9.2.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your G-1000 v2.

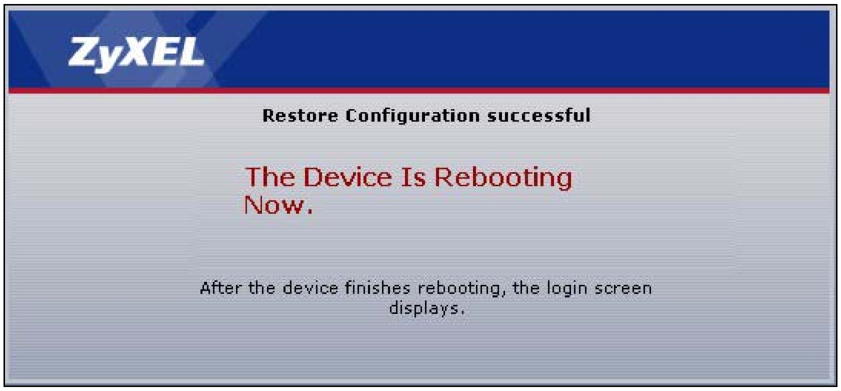
Table 36 Maintenance Restore Configuration

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 v2 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 v2 again.

Figure 39 Configuration Restore Successful



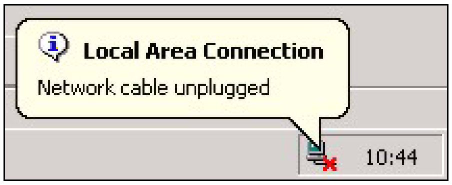
Restore Configuration successful

The Device Is Rebooting Now.

After the device finishes rebooting, the login screen displays.

The G-1000 v2 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 40 Temporarily Disconnected



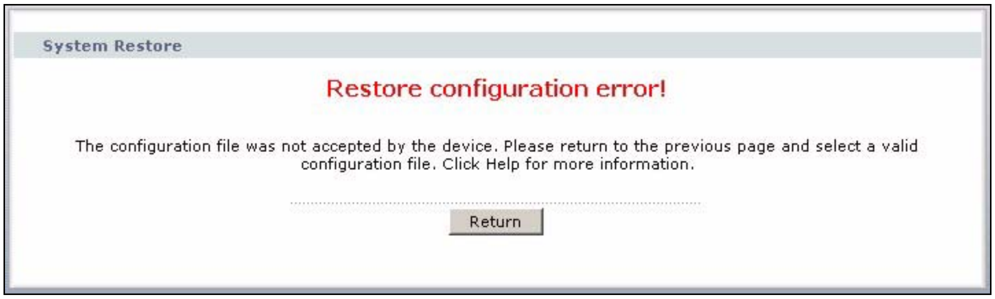
Local Area Connection

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 v2 IP address (192.168.1.2). See the appendix for details on how to set up your computer's IP address.

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

Figure 41 Configuration Restore Error



System Restore

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.

9.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the G-1000 v2 to its factory defaults.

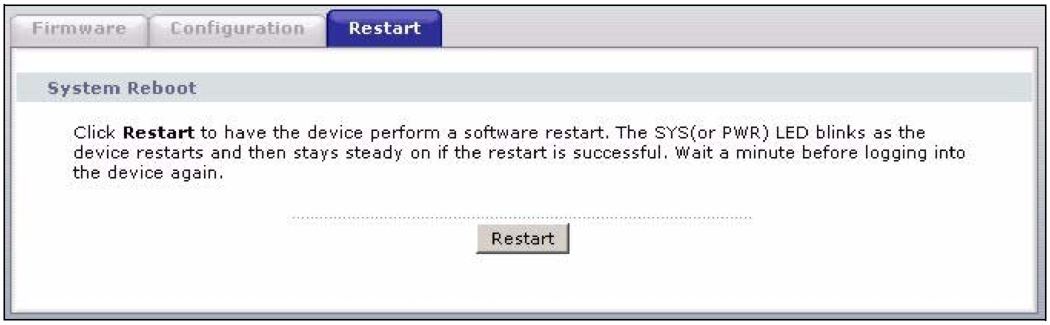
You can also press the **RESET** button on the rear panel to reset the factory defaults of your G-1000 v2. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

9.3 Restart

System restart allows you to reboot the G-1000 v2 without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the G-1000 v2 reboot. This does not affect the G-1000 v2's configuration.

Figure 42 Restart Screen



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 10 Introducing the SMT

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

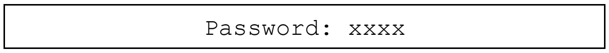
10.1 Connect to your G-1000 v2 Using Telnet

The following procedure details how to telnet into your G-1000 v2.

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 43 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 v2 will automatically log you out. You will then have to telnet into the G-1000 v2 again. You can use the web configurator or the CI commands to change the inactivity time out period.

10.2 Changing the System Password

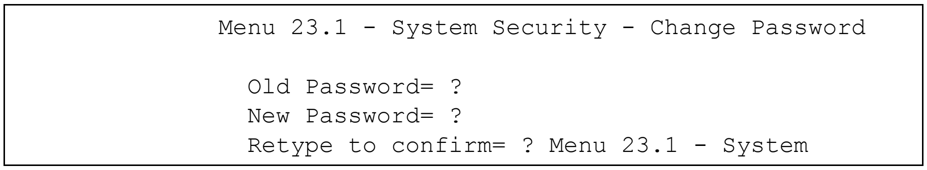
Change the G-1000 v2 default password by following the steps shown next.

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 44 Menu 23.1 System Security: Change Password



```
              Menu 23.1 - System Security - Change Password

                Old Password= ?
                New Password= ?
                Retype to confirm= ? Menu 23.1 - System
```

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.

10.3 G-1000 v2 SMT Menus Overview

The following table gives you an overview of your G-1000 v2's various SMT menus.

Table 37 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	
22 SNMP Configuration			
23 System Security	23.1 Change Password		
	23.2 RADIUS Server		
	23.4 IEEE 802.1X		
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	24.3.2 Syslog Logging	
	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		

10.4 Navigating the SMT Interface

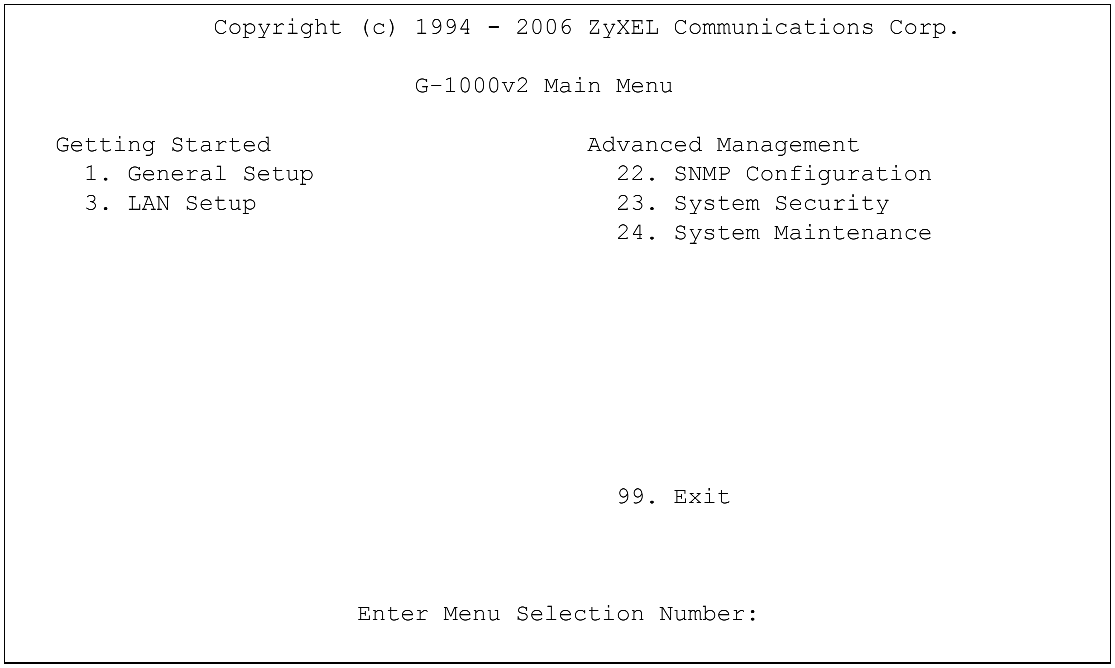
The SMT (System Management Terminal) is the interface that you use to configure your G-1000 v2. Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 38 Main Menu Commands

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

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

Figure 45   G-1000 v2 SMT Main Menu



```
              Copyright (c) 1994 - 2006 ZyXEL Communications Corp.

                           G-1000v2 Main Menu

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









                                          99. Exit




                       Enter Menu Selection Number:
```

This menu is summarized below.

Table 39   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.
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 11
General Setup

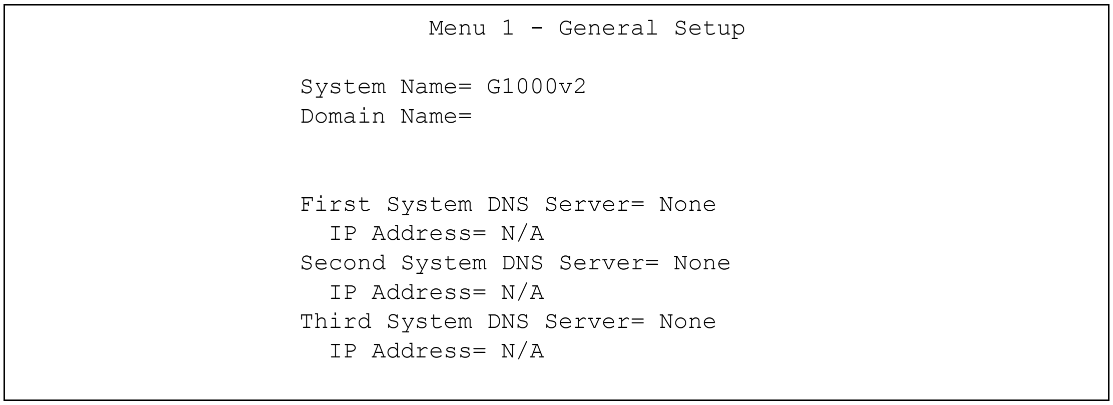
The chapter shows you the information on general setup.

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 v2 via DHCP.

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

Figure 46 Menu 1 General Setup



```
                            Menu 1 - General Setup

                   System Name= G1000v2
                   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 40 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]. These fields are not available on all models.

Table 40 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.	

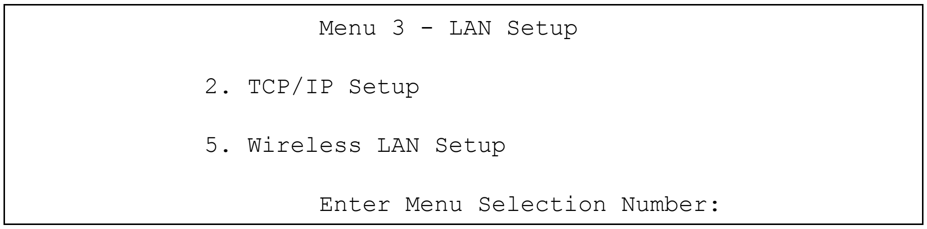
CHAPTER 12 LAN Setup

This chapter shows you how to configure the LAN on your G-1000 v2.

12.1 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 47 Menu 3 LAN Setup



```
                      Menu 3 - LAN Setup

              2. TCP/IP Setup

              5. Wireless LAN Setup

                      Enter Menu Selection Number:
```

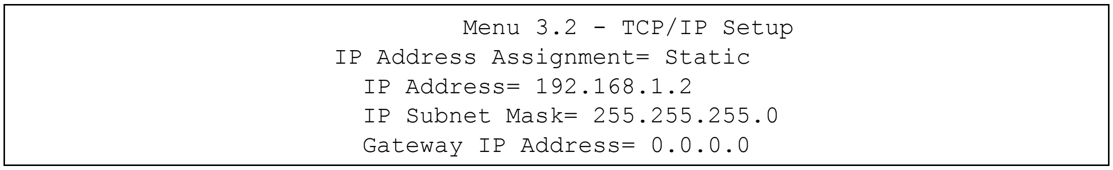
Detailed explanation about the LAN Setup menu is given in the next chapter.

12.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your G-1000 v2 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 48 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.

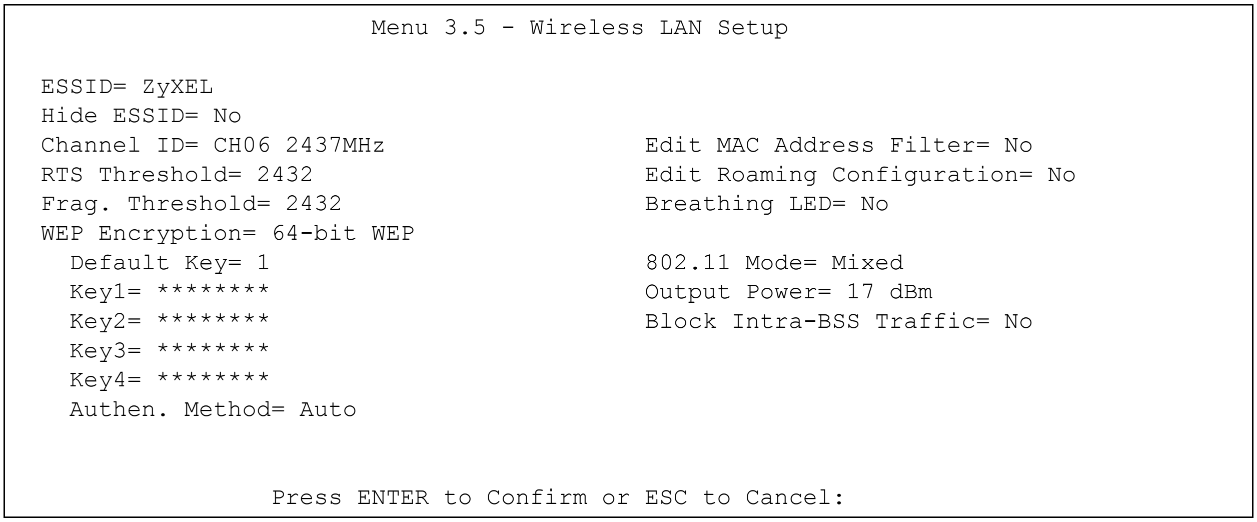
Table 41 Menu 3.2 TCP/IP Setup

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** to have the G-1000 v2 obtain an IP address from a DHCP server. You must know the IP address assigned to the G-1000 v2 (by the DHCP server) to access the G-1000 v2 again. Select **Static** to give the G-1000 v2 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 v2 in dotted decimal notation
IP Subnet Mask	Your G-1000 v2 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 v2.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your G-1000 v2 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 v2.
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.	

12.3 Wireless LAN Setup

Use menu 3.5 to set up your G-1000 v2 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 49 Menu 3.5 Wireless LAN Setup



```
                         Menu 3.5 - Wireless LAN Setup

  ESSID= ZyXEL
  Hide ESSID= No
  Channel ID= CH06 2437MHz                  Edit MAC Address Filter= No
  RTS Threshold= 2432                       Edit Roaming Configuration= No
  Frag. Threshold= 2432                     Breathing LED= No
  WEP Encryption= 64-bit WEP
    Default Key= 1                          802.11 Mode= Mixed
    Key1= ********                          Output Power= 17 dBm
    Key2= ********                          Block Intra-BSS Traffic= No
    Key3= ********
    Key4= ********
    Authen. Method= Auto


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

Note: In the SMT, the ESSID is referred to as SSID. Both of them refer to the same ID for the G-1000 v2.

The following table describes the fields in this menu.

Table 42 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters. This field is only available when you select **Access Point** or **AP + Bridge** in the **Operating Mode** field.
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide ESSID in the outgoing data frame so an intruder cannot obtain the ESSID 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. 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 v2 and the wireless stations to communicate.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the G-1000 v2 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). **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]. This field is **N/A** if WEP is not activated. 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**.
Breathing LED	Select Yes to enable the Breathing LED, also known as the G-1000 v2 LED. The blue G-1000 v2 LED is on when the G-1000 v2 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 v2 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**. The default setting is **Long**. See the section on preamble for more information.

Table 42 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
802.11 Mode	Select **B Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-1000 v2. Select **G Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-1000 v2. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the G-1000 v2. The transmission rate of your G-1000 v2 might be reduced.
Output Power	Press [SPACE BAR] to select **11dBm**, **14dBm** or **17dBm** and press [ENTER].
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.
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.	

12.3.1 Configuring MAC Address Filter

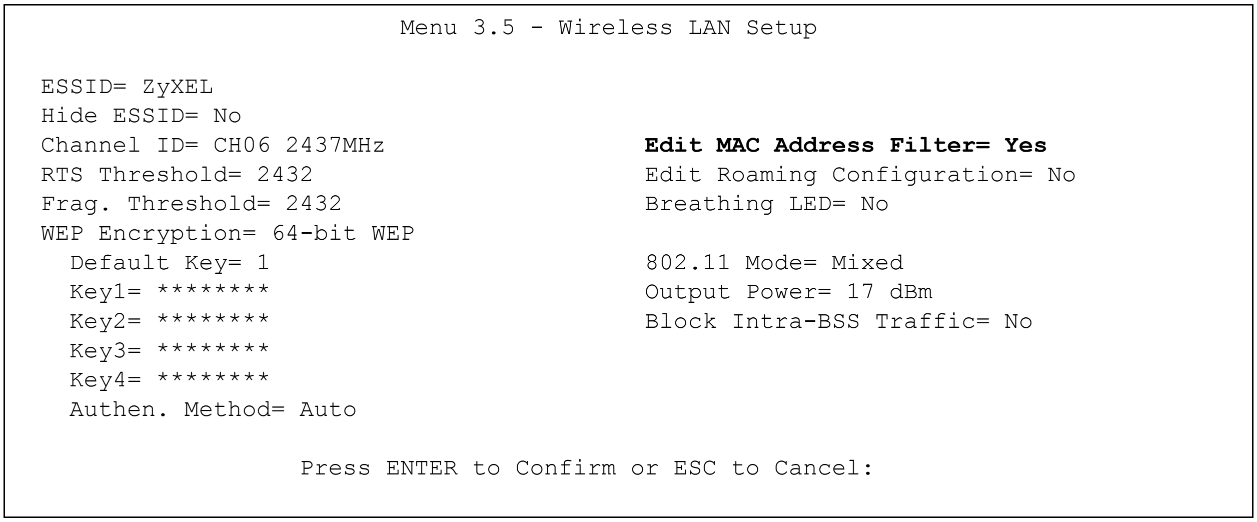
Your G-1000 v2 checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your G-1000 v2.

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

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

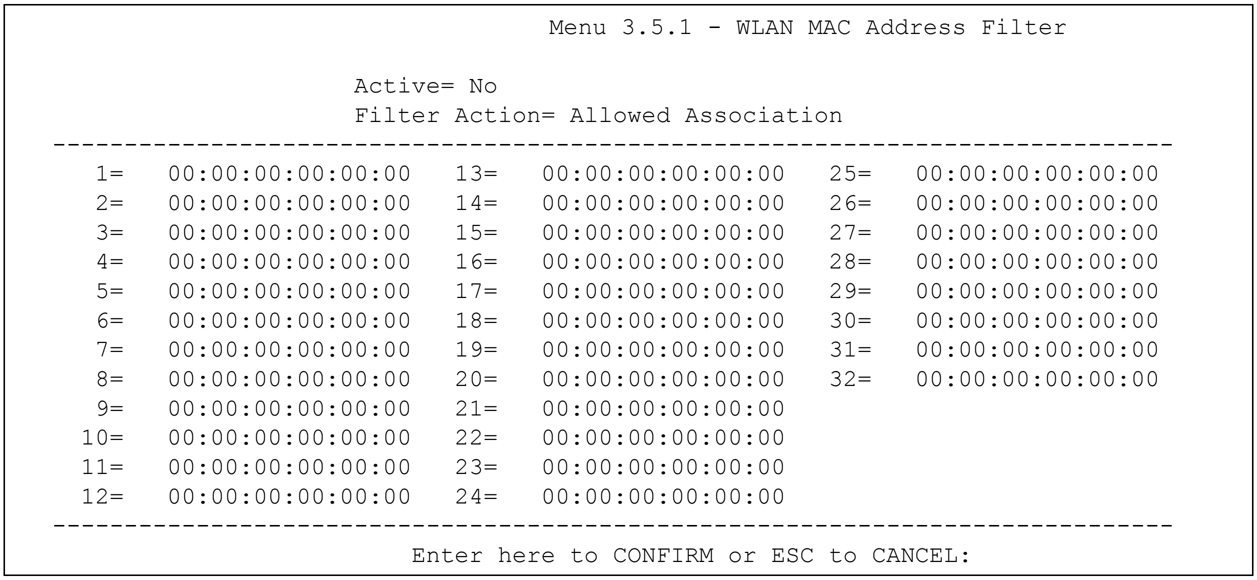
Figure 50 Menu 3.5 Wireless LAN Setup



```
                         Menu 3.5 - Wireless LAN Setup

  ESSID= ZyXEL
  Hide ESSID= No
  Channel ID= CH06 2437MHz                  Edit MAC Address Filter= Yes
  RTS Threshold= 2432                       Edit Roaming Configuration= No
  Frag. Threshold= 2432                     Breathing LED= No
  WEP Encryption= 64-bit WEP
    Default Key= 1                          802.11 Mode= Mixed
    Key1= ********                          Output Power= 17 dBm
    Key2= ********                          Block Intra-BSS Traffic= No
    Key3= ********
    Key4= ********
    Authen. Method= Auto

                  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 51   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 43   Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the G-1000 v2, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the G-1000 v2. 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 v2 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.	

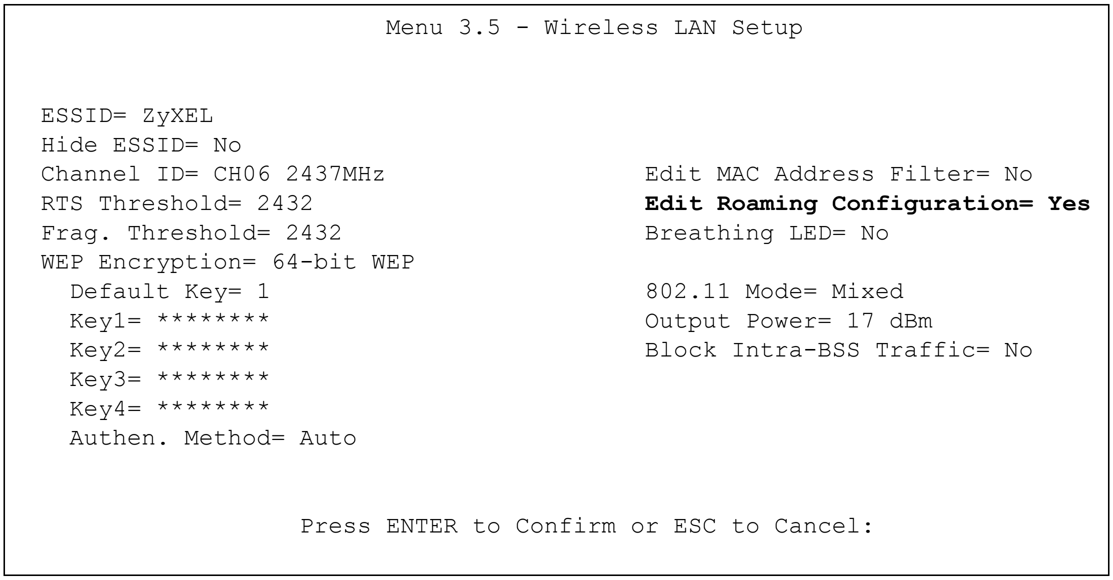
12.3.2 Configuring Roaming

Enable the roaming feature if you have two or more G-1000 v2s on the same subnet. Follow the steps below to allow roaming on your G-1000 v2.

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

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

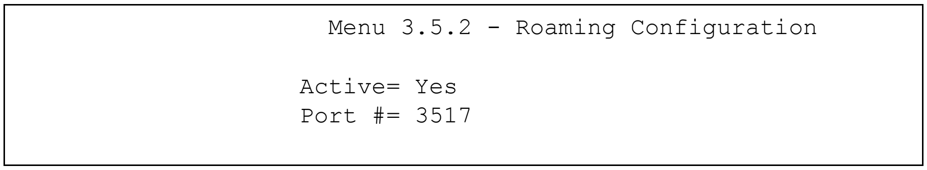
Figure 52   Menu 3.5 Wireless LAN Setup



```
                          Menu 3.5 - Wireless LAN Setup


  ESSID= ZyXEL
  Hide ESSID= No
  Channel ID= CH06 2437MHz                  Edit MAC Address Filter= No
  RTS Threshold= 2432                       Edit Roaming Configuration= Yes
  Frag. Threshold= 2432                     Breathing LED= No
  WEP Encryption= 64-bit WEP
    Default Key= 1                          802.11 Mode= Mixed
    Key1= ********                          Output Power= 17 dBm
    Key2= ********                          Block Intra-BSS Traffic= No
    Key3= ********
    Key4= ********
    Authen. Method= Auto


                    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 53   WLAN Roaming Configuration



```
                      Menu 3.5.2 - Roaming Configuration

                    Active= Yes
                    Port #= 3517
```

The following table describes the fields in this menu.

Table 44   Menu 3.5.4 Bridge Link Configuration

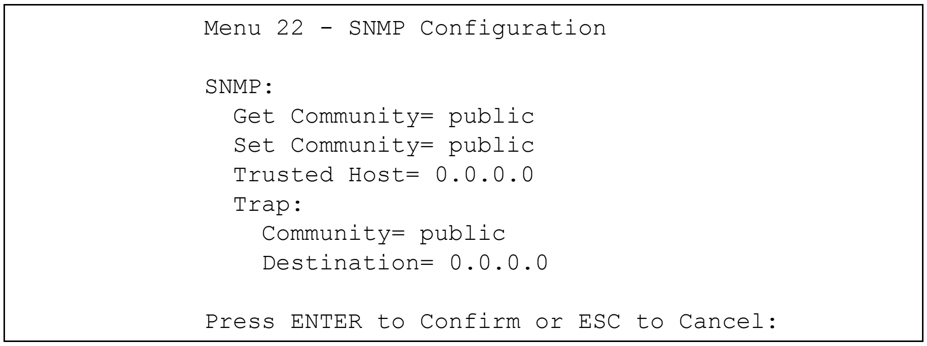
FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select Yes to enable roaming on the G-1000 v2 if you have two or more G-1000 v2s on the same subnet.
Port #	Type the port number to communicate roaming information between access points. The port number must be the same on all access points. 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 13 SNMP Configuration

This chapter shows you how to use SMT to configure SNMP on the G-1000 v2.

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 54   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 45   Menu 22 SNMP Configuration

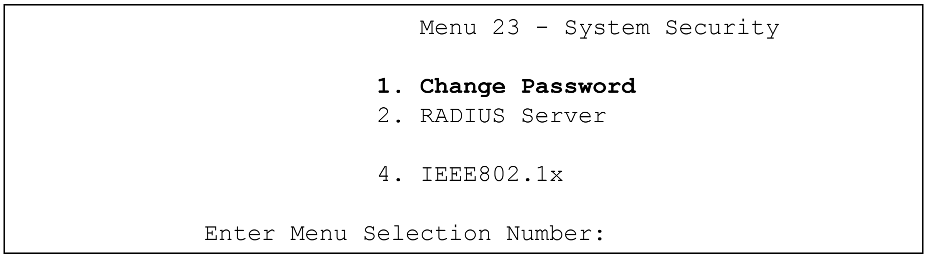
FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set Community**, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your G-1000 v2 will only respond to SNMP messages from this address. A blank (default) field means your G-1000 v2 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 14 System Security

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

14.1 System Password

Figure 55 Menu 23 System Security



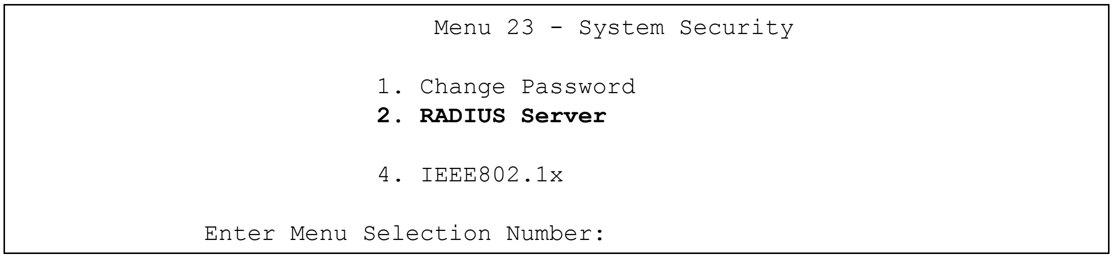
```
                              Menu 23 - System Security

                           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 v2 in the *Introducing the Web Configurator* chapter.

14.2 Configuring External RADIUS Server

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

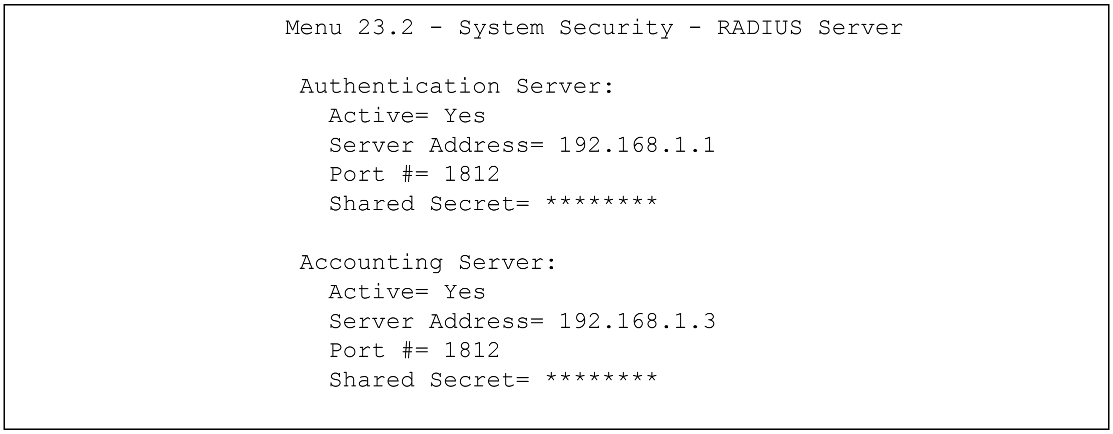
Figure 56 Menu 23 System Security



```
                               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 57 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 46 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**. 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. The key is not sent over the network. This key must be the same on the external authentication server and G-1000 v2.
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**. 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. The key is not sent over the network. This key must be the same on the external accounting server and G-1000 v2.
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.	

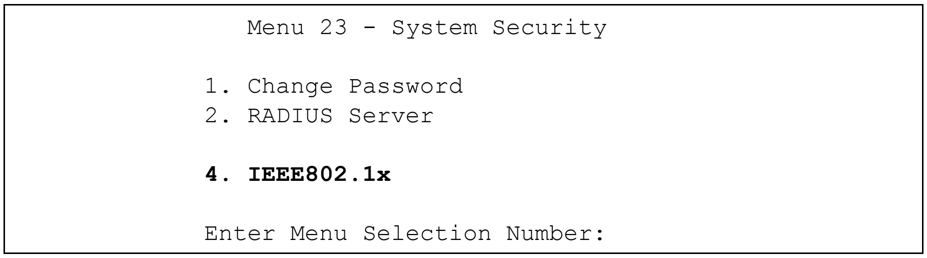
14.3 802.1x

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 v2.

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

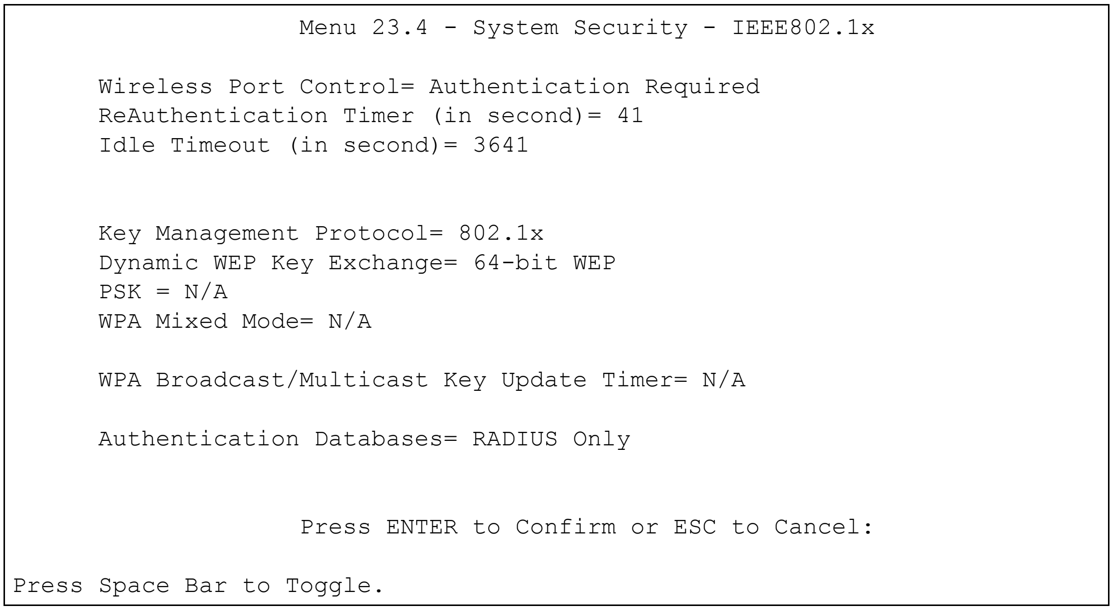
Figure 58 Menu 23 System Security



```
                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 59 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 47 Menu 23.4 System Security: IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **No Access Allowed** to block all wireless stations access to the wired network. The following fields are not available when you select **No Authentication Required** or **No Access Allowed**.
ReAuthentication Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the wired network. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout (in second)	The G-1000 v2 automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER].
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the G-1000 v2 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.

Table 47 Menu 23.4 System Security: IEEE802.1x

FIELD	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the G-1000 v2. The RADIUS is an external server. Use this field to decide which database the G-1000 v2 should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**. Select **Local User Database Only** to have the G-1000 v2 just check the built-in user database on the G-1000 v2 for a wireless station's username and password. Select **RADIUS Only** to have the G-1000 v2 just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the G-1000 v2 first check the user database on the G-1000 v2 for a wireless station's username and password. If the user name is not found, the G-1000 v2 then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the G-1000 v2 first check the user database on the specified RADIUS server for a wireless station's username and password. If the G-1000 v2 cannot reach the RADIUS server, the G-1000 v2 then checks the local user database on the G-1000 v2. When the user name is not found or password does not match in the RADIUS server, the G-1000 v2 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 v2 for authentication

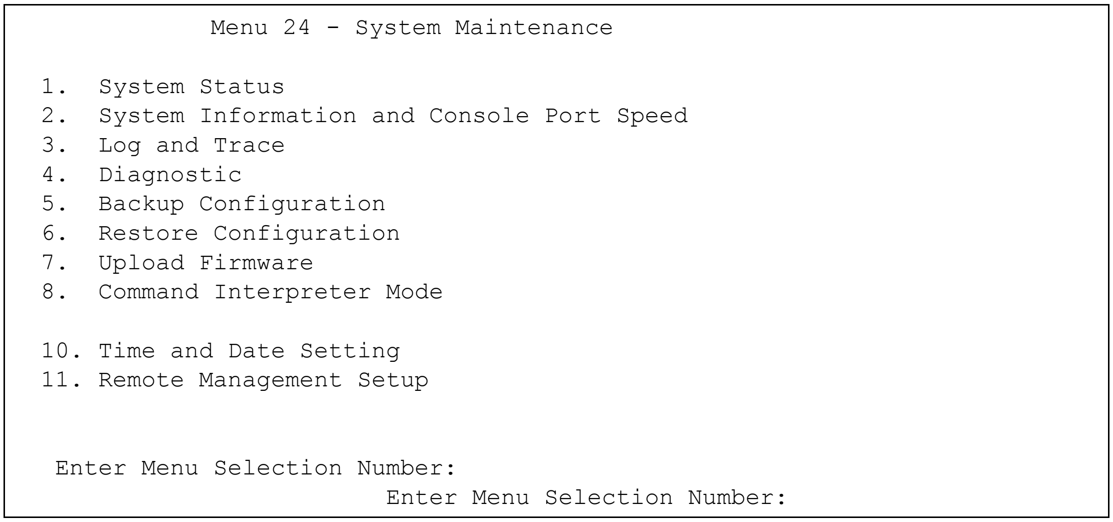
CHAPTER 15 System Information and Diagnosis

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 60 Menu 24 System Maintenance



```
              Menu 24 - System Maintenance

  1.  System Status
  2.  System Information and Console Port Speed
  3.  Log and Trace
  4.  Diagnostic
  5.  Backup Configuration
  6.  Restore Configuration
  7.  Upload Firmware
  8.  Command Interpreter Mode

  10. Time and Date Setting
  11. Remote Management Setup


   Enter Menu Selection Number:
                          Enter Menu Selection Number:
```

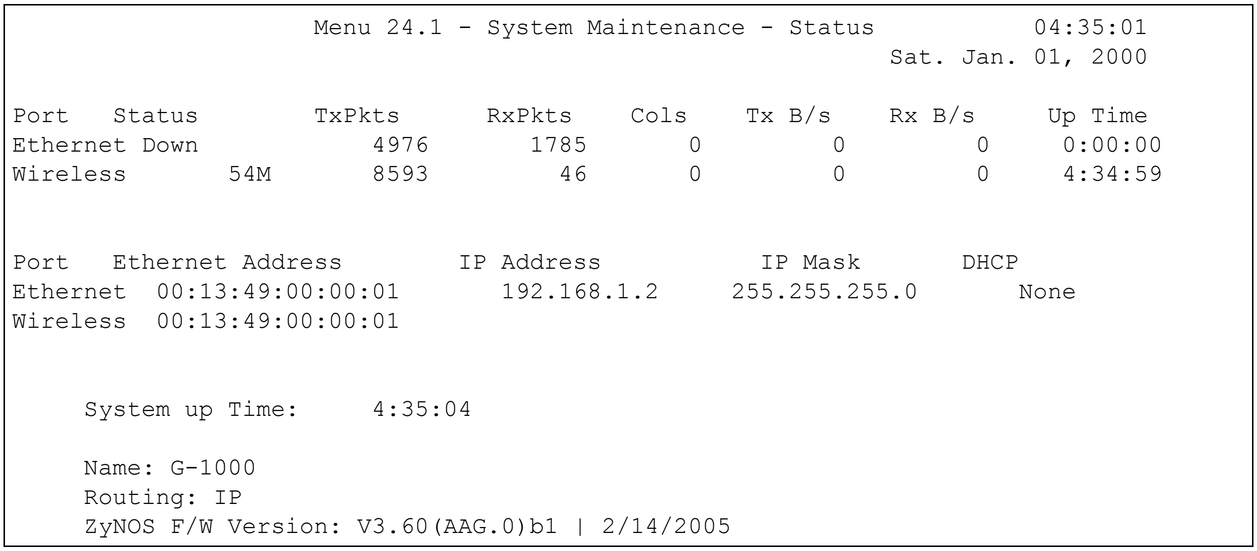
15.1 System Status

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 v2. 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 61 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
     Routing: IP
     ZyNOS F/W Version: V3.60(AAG.0)b1 | 2/14/2005
```

The following table describes the fields present in this menu.

Table 48 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 v2 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.

15.2 System Information

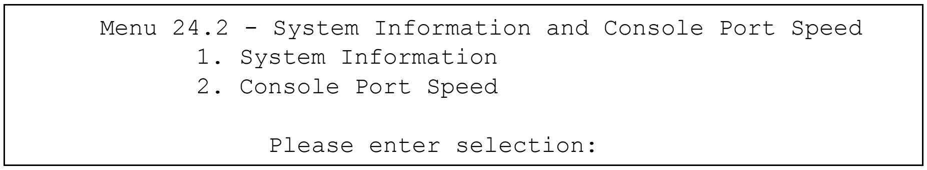
To get to the System Information:

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 62 Menu 24.2 System Information and Console Port Speed



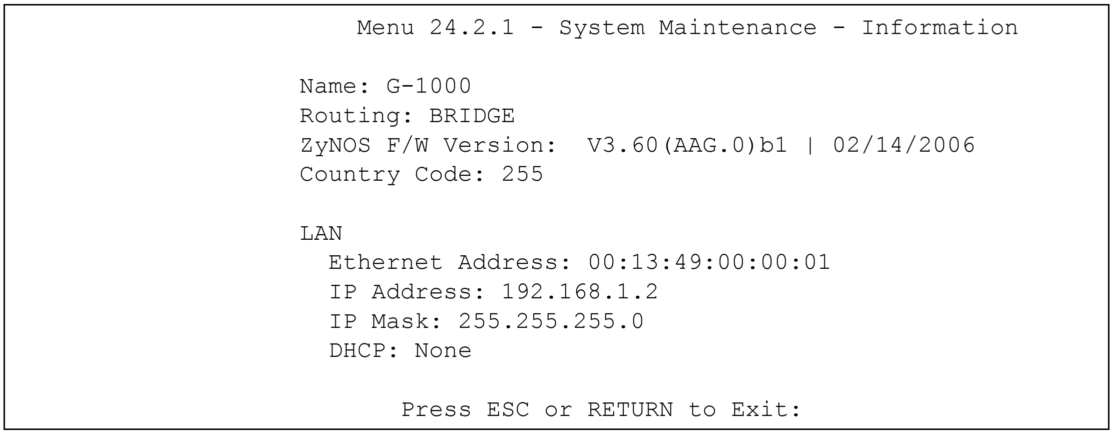
```
      Menu 24.2 - System Information and Console Port Speed
             1. System Information
             2. Console Port Speed

                  Please enter selection:
```

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

15.2.1 System Information

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

Figure 63 Menu 24.2.1 System Information: Information



```
                        Menu 24.2.1 - System Maintenance - Information

                    Name: G-1000
                    Routing: BRIDGE
                    ZyNOS F/W Version:  V3.60(AAG.0)b1 | 02/14/2006
                    Country Code: 255

                    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 49 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your G-1000 v2. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.

Table 49 Menu 24.2.1 System Maintenance: Information

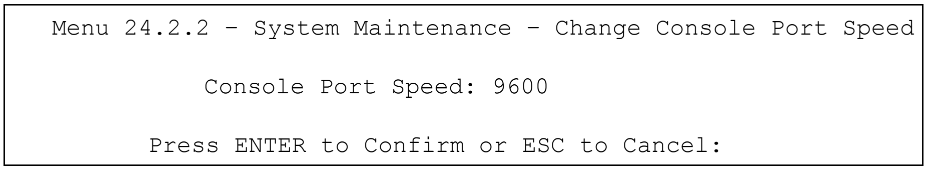
FIELD	DESCRIPTION
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your G-1000 v2.
IP Address	This is the IP address of the G-1000 v2 in dotted decimal notation.
IP Mask	This shows the subnet mask of the G-1000 v2.
DHCP	This field shows the DHCP setting of the G-1000 v2.
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.	

15.2.2 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 v2 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 64 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 v2, you must also make the same change to the console port speed parameter of your communication software.

15.3 Log and Trace

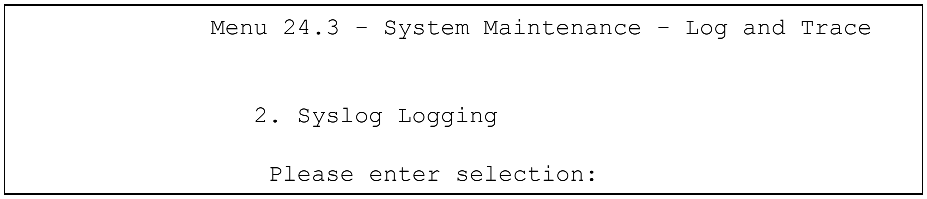
To get to the log and trace information:

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

2 Enter 3 to display **Menu 24.3 – Log and Trace**.

3 From this menu you have one choice as shown in the next figure:

Figure 65 Menu 24.3 Log and Trace



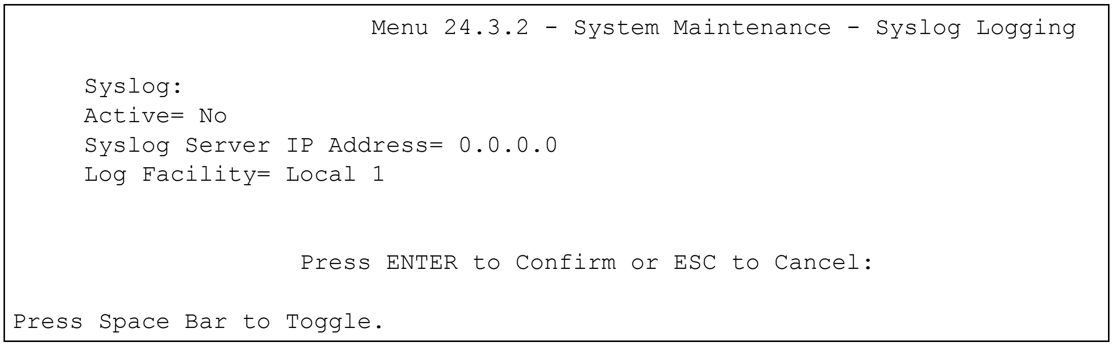
```
              Menu 24.3 - System Maintenance - Log and Trace


                 2. Syslog Logging

                  Please enter selection:
```

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

15.3.1 Syslog Logging

Enter 2 in menu 24.2 to display the screen shown next.

Figure 66 Menu 24.3.2 System Maintenance - Syslog Logging



```
                         Menu 24.3.2 - System Maintenance - Syslog Logging

     Syslog:
     Active= No
     Syslog Server IP Address= 0.0.0.0
     Log Facility= Local 1


                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

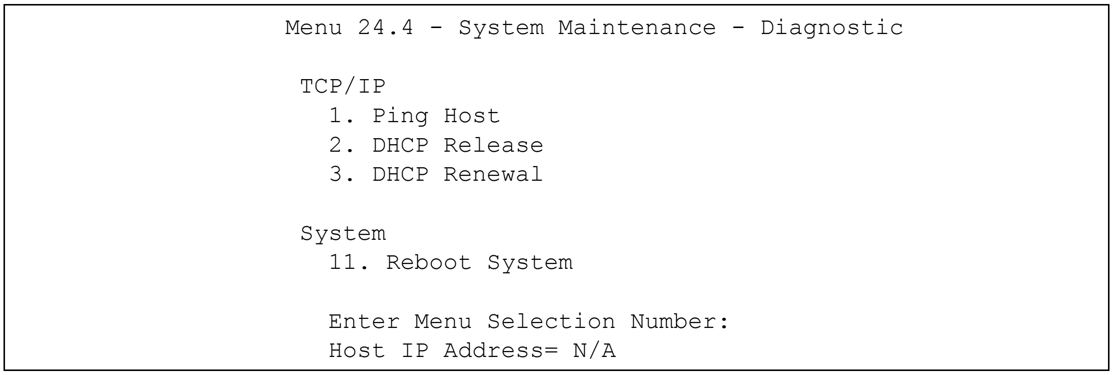
Table 50 Menu 24.3.2 System Maintenance - Syslog Logging

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable logging.
Syslog Server IP Address	Enter the IP Address of a server where you want to store the log information.
Log Facility	Press [SPACE BAR] to toggle log facilities.

15.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your G-1000 v2 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 67   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 v2 and the connections.

Table 51   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 v2.
Host IP Address	If you typed 1 to Ping Host, now type the address of the computer you want to ping.

CHAPTER 16 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.

16.1 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 v2'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 v2.

```
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 v2 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 v2 and the external filename refers to the filename not on the G-1000 v2, 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 52 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the G-1000 v2. Uploading the rom-0 file replaces the entire ROM file system, including your G-1000 v2 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 v2.

16.2 Backup Configuration

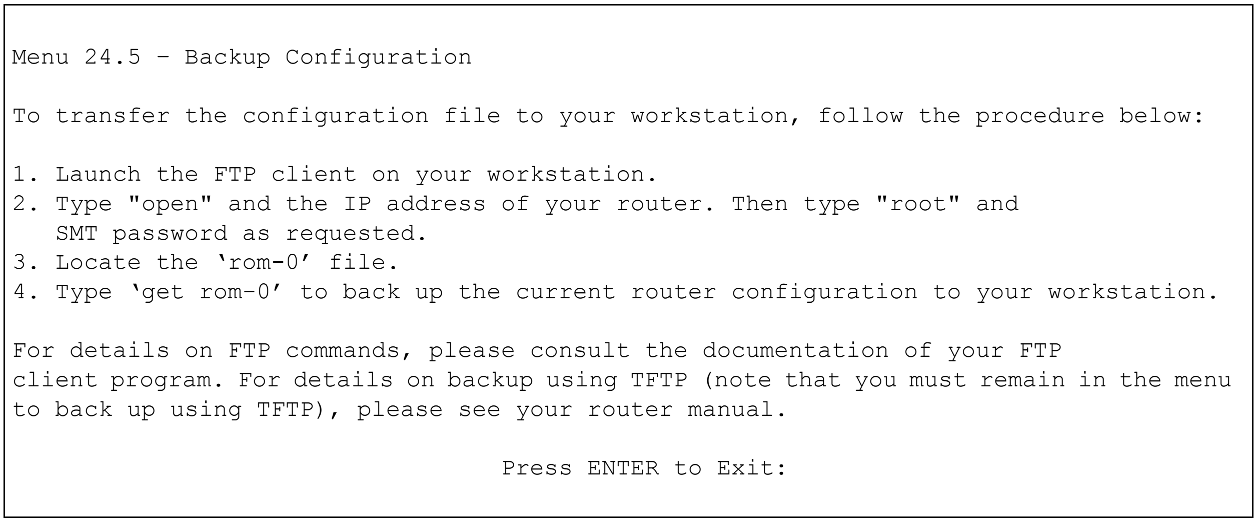
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current G-1000 v2 configuration to your computer. Backup is highly recommended once your G-1000 v2 is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms "download" and "upload" are relative to the computer. Download means to transfer from the G-1000 v2 to the computer, while upload means from your computer to the G-1000 v2.

16.2.1 Backup Configuration Using FTP

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

Figure 68   Menu 24.5 Backup Configuration

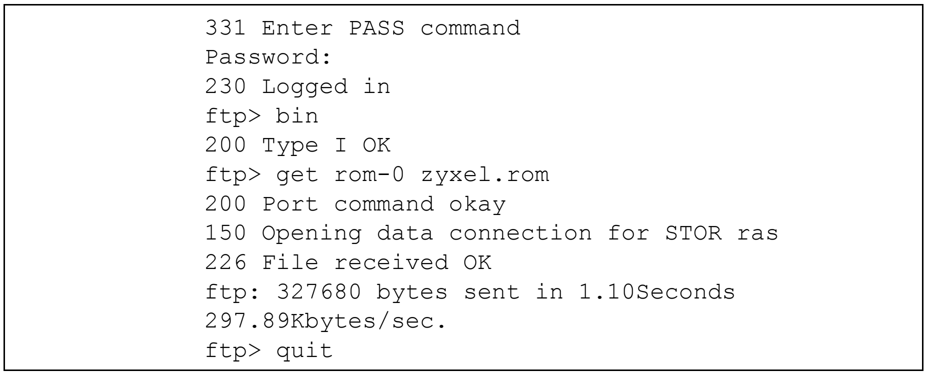


```
Menu 24.5 - Backup Configuration

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:
```

16.2.2 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 v2.
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 v2 to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the G-1000 v2 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 69   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 53 General Commands for Third Party FTP Clients

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

16.2.3 Backup Configuration Using TFTP

The G-1000 v2 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 v2 and log in. Because TFTP does not have any security checks, the G-1000 v2 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 v2. 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 v2 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 v2 to the computer and "binary" to set binary transfer mode.

16.2.4 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 v2 IP address, "get" transfers the file source on the G-1000 v2 (rom-0 name of the configuration file on the G-1000 v2) 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 54 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the G-1000 v2. 192.168.1.2 is the G-1000 v2's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the G-1000 v2 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 v2. 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.

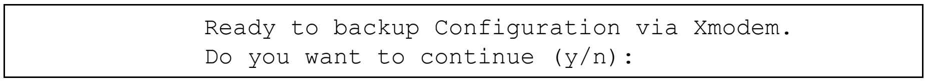
16.2.5 Backup Via Console Port

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.

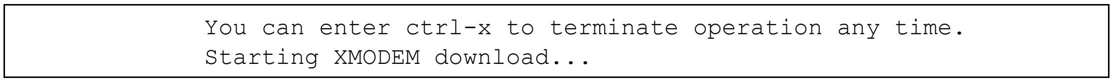
Figure 70 System Maintenance: Backup Configuration



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

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

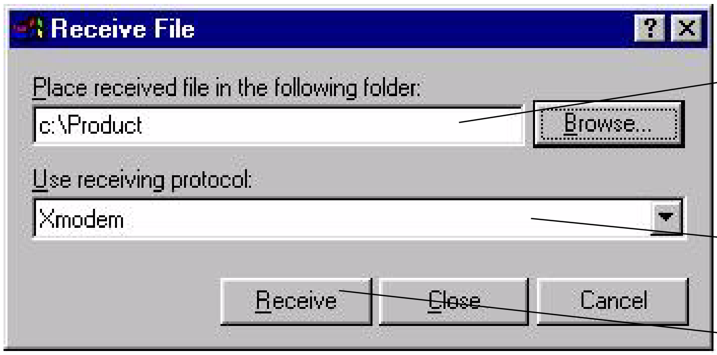
Figure 71 System Maintenance: Starting Xmodem Download Screen



```
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 72 Backup Configuration Example



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 73 Successful Backup Confirmation Screen

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

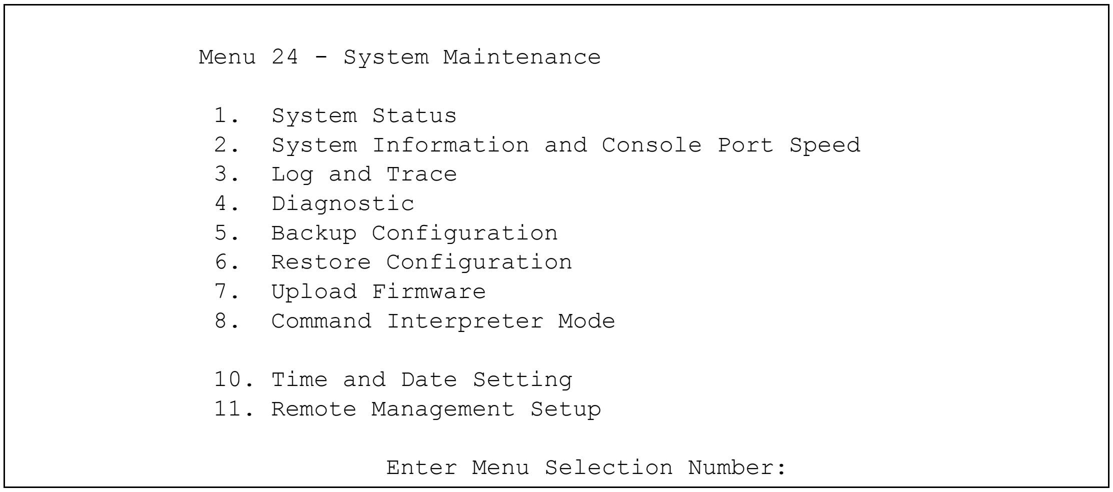
CHAPTER 17
System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

17.1 Command Interpreter Mode

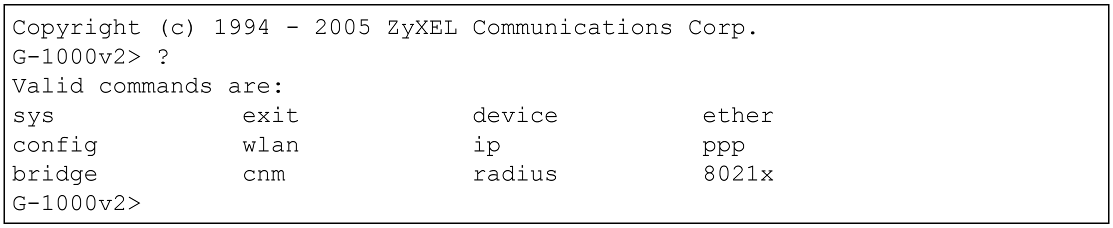
The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed 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 74 Menu 24 System Maintenance



```
             Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode

              10. Time and Date Setting
              11. Remote Management Setup

                          Enter Menu Selection Number:
```

Figure 75 Valid CI Commands



```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
G-1000v2> ?
Valid commands are:
sys             exit            device          ether
config          wlan            ip              ppp
bridge          cnm             radius          8021x
G-1000v2>
```

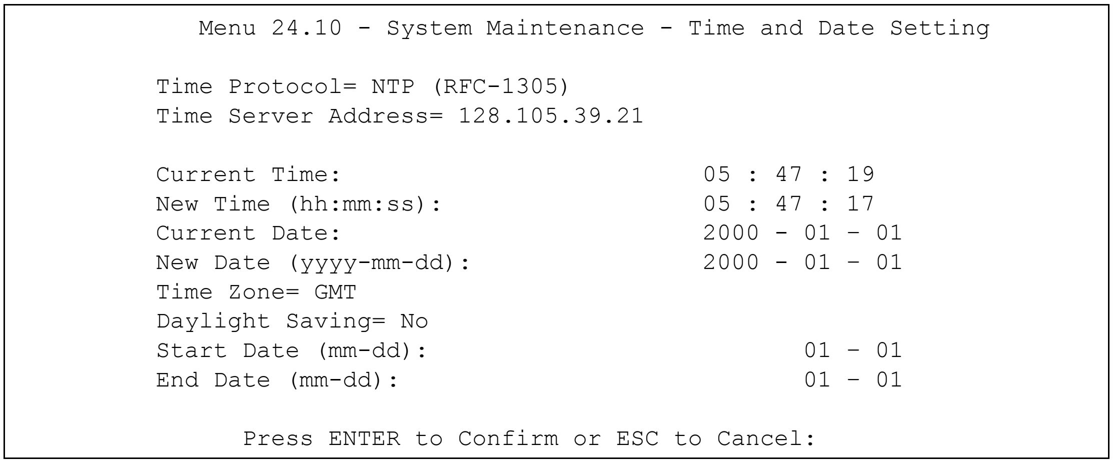
17.2 Time and Date Setting

The G-1000 v2 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 v2. Menu 24.10 allows you to update the time and date settings of your G-1000 v2. The real time is then displayed in the G-1000 v2 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 v2 as shown in the following screen.

Figure 76 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 55 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 v2. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	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.

Table 55 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
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 v2 resets the time in three instances:

1 On leaving menu 24.10 after making changes.

2 When the G-1000 v2 starts up, if there is a timeserver configured in menu 24.10.

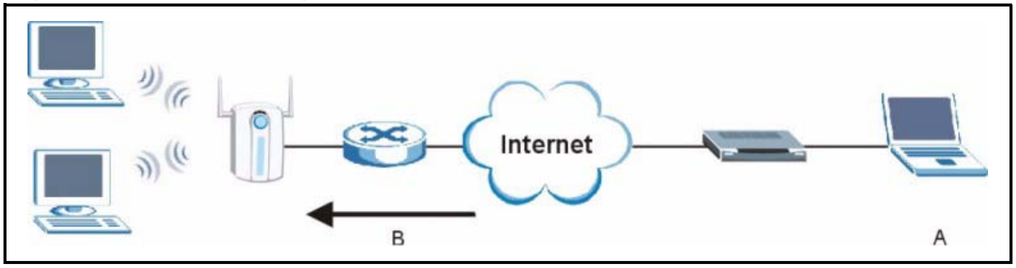
3 24-hour intervals after starting.

17.3 Remote Management Setup

17.3.1 Telnet

You can configure your G-1000 v2 for remote Telnet access as shown next.

Figure 77 Telnet Configuration on a TCP/IP Network



17.3.2 FTP

You can upload and download G-1000 v2 firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

17.3.3 Web

You can use the G-1000 v2's embedded web configurator for configuration and file management. See the *online help* for details.

17.3.4 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 v2 from a remote location via:

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

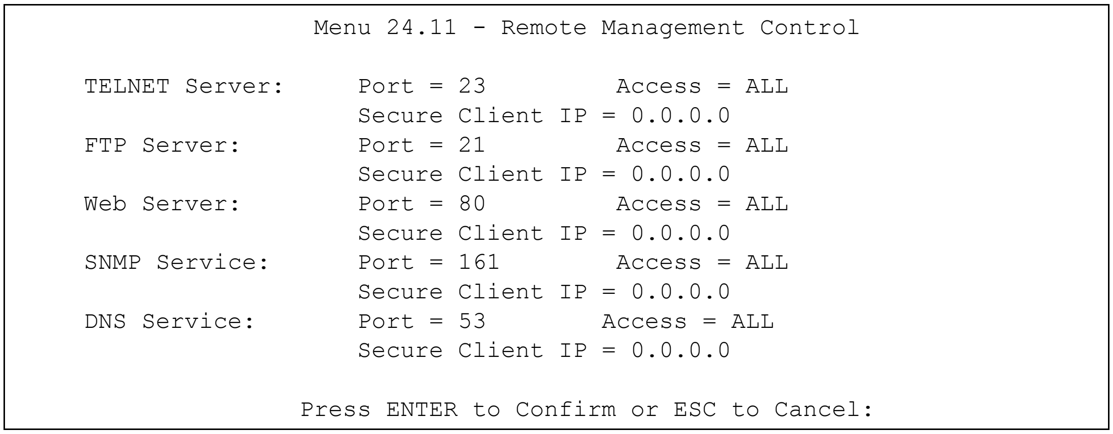
Table 56 Remote Management Port Control

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 78 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 57 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
TELNET Server: FTP Server: Web Server: SNMP Service: DNS Service:	Each of these read-only labels denotes a server or service that you may use to remotely manage the G-1000 v2.
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 v2. 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.	

17.3.5 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 v2 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.

17.4 Remote Management and NAT

When NAT is enabled:

- Use the G-1000 v2's WAN IP address when configuring from the WAN.
- Use the G-1000 v2's LAN IP address when configuring from the LAN.

17.5 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your G-1000 v2 will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

CHAPTER 18 Troubleshooting

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

Problems Starting Up the G-1000 v2

Table 58 Troubleshooting the Start-Up of Your G-1000 v2

PROBLEM	CORRECTIVE ACTION
None of the lights 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. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The G-1000 v2 reboots automatically sometimes.	The supplied power to the G-1000 v2 is too low. Check that the G-1000 v2 is receiving enough power. Make sure the power source is working properly.

Problems with the Ethernet Interface

Table 59 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the G-1000 v2 from the LAN.	If the **ETHN** light on the front panel is off, check the Ethernet cable connection between your G-1000 v2 and the Ethernet device connected to the **ETHERNET** port. Check for faulty Ethernet cables. Make sure your computer's Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the G-1000 v2, the Ethernet device and your computer are on the same subnet. If you changed the IP address of your G-1000 v2 or if an IP address is assigned to the G-1000 v2 automatically, you can access the device by using the new IP address or typing "**http://zyxelXXXX**" (where XXXX are the last four digits of your device's MAC address) in your browser. The MAC address can be found on the back label of your G-1000 v2.
I cannot ping any computer on the LAN.	If the **ETHN** light on the front panel is off, check the Ethernet cable connections between your G-1000 v2 and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make sure the LAN computer's Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of the G-1000 v2, the Ethernet device and the LAN computers are on the same subnet.

Problems with the Password

Table 60 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the G-1000 v2.	The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the **RESET** button on the top panel of the G-1000 v2 to restore the factory default configuration file (hold this button in for about 10 seconds or until the link light turns red). This will restore all of the factory defaults including the password.

Problems with the WLAN Interface

Table 61 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the G-1000 v2 from the WLAN.	Make sure the link light on the ZyXEL device is on. Check that both the G-1000 v2 and your wireless station are using the same security settings. Refer to Chapter 4, "Wireless LAN," on page 49 to confirm your settings.
I cannot ping any computer on the WLAN.	Make sure the link light on the ZyXEL device is on. Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the G-1000 v2 and wireless station(s) are using the same Name(SSID), channel and WEP keys (if WEP encryption is activated).

APPENDIX A
Product Specifications

See also the Introduction chapter for a general overview of the key features.

Specification Tables

Table 62 Hardware

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions	(152 W) x (92 D) x (45 H) mm
Weight	300g
Power Specification	12V DC 1A Max
Ethernet Interface	One auto-negotiating MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Wireless LAN Interface	One IEEE 802.11g standard based 54Mbp Mini-PCI card
Detachable Antennas	2 detachable dipole antenna with diversity (Reverse SMA Connectors)
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º ~ 60º C
Operation Humidity	20% ~ 95% RH
Storage Humidity	10% ~ 90% RH

Table 63 Firmware

Applications	DNS Proxy DHCP Client VPN pass through - IPSec, PPTP and L2TP pass through support
Standard Compliance	IEEE 802.3 and 802.3u 10Base-T and 100Base-TX physical layer specification IEEE 802.11g specification compliance for wireless LAN IEEE 802.11b specification compliance for wireless LAN IEEE 802.1x security standard support (WPA/WPA2) Roaming between Access Points Wi-Fi WPA/WPA2certificate Wi-Fi WMM certificate

Table 63 Firmware (continued)

Management	Embedded Web Configurator CLI (Command Line Interpreter) Remote Management via Telnet or Web SMT (System Management Terminal) SNMP Management Embedded FTP/TFTP server for firmware downloading, configuration backup and restoration with large rom file support Syslog Built-in Diagnostic Tools for FLASH memory, DRAM, LAN ports and wireless ports
Wireless Network Standard	IEEE 802.11bCompliance IEEE 802.11g Compliance
Operating Frequency	RF Frequency Range: 2.412-2.462 GHZ: North America 2.412-2.472 GHZ: Japan 2.412-2.472 GHZ: Europe
Receiver Sensitivity	72 dBm @ 54M (OFDM, 10% PER) 85 dBm @ 11M (CCK, 8% PER)
Wireless Coverage	Indoor : 9.5M@54Mbps , 25M@24Mbps , 55M@6Mbps , 37M@11Mbps Outdoor : 60M@54Mbps, 70M@48Mbps, 80M@36Mbps, 120M@24, 18, 12/ 9/6Mbps, 80M@11Mbps, 120M@5.5Mbps, 200M@2Mbps, 300M@1Mbps
RF Output Power	15dBm (54 Mbps, OFDM, typical) 18 dBm (11Mbps, CCK, QPSK, BPSK, typical)
Security	WPA and WPA2 WPA-PSK and WPA2-PSK IEEE 802.1x security (TLS/TTLS/PEAP/SIM) Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit Up to 32 MAC Address filters Block intra BSS traffic
Logs	Sys log Error log Trace log Packet log

APPENDIX B
Brute-Force Password Guessing Protection

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

Table 64 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 C
Setting up Your Computer’s IP Address

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

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

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

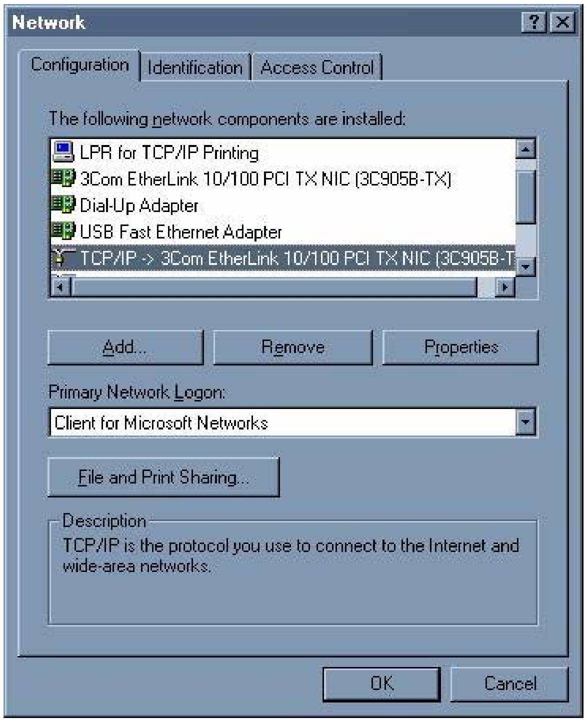
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the G-1000 v2’s LAN port.

Windows 95/98/Me

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

Figure 79 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.

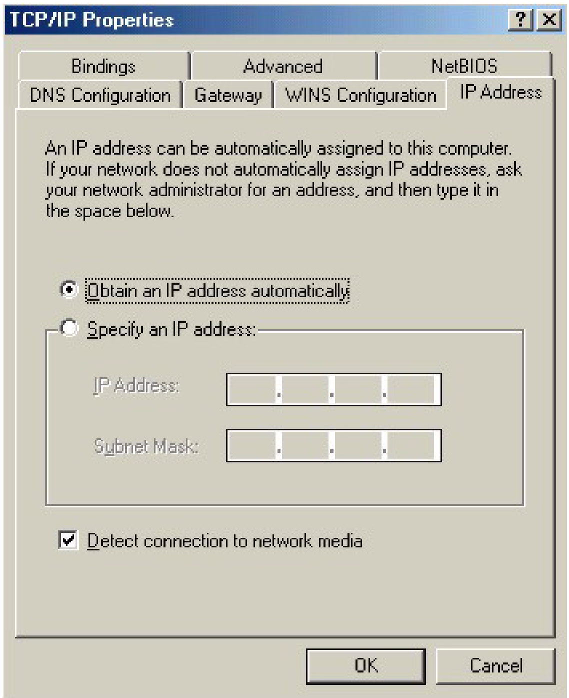
Configuring

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 80 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:

IP Address: . . .

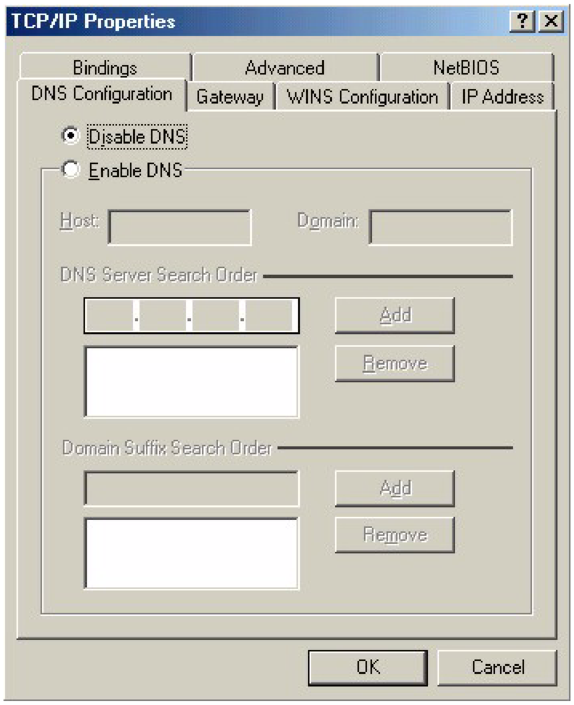
Subnet Mask: . . .

☑ 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 81 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



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 v2 and restart your computer when prompted.

Verifying Settings

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

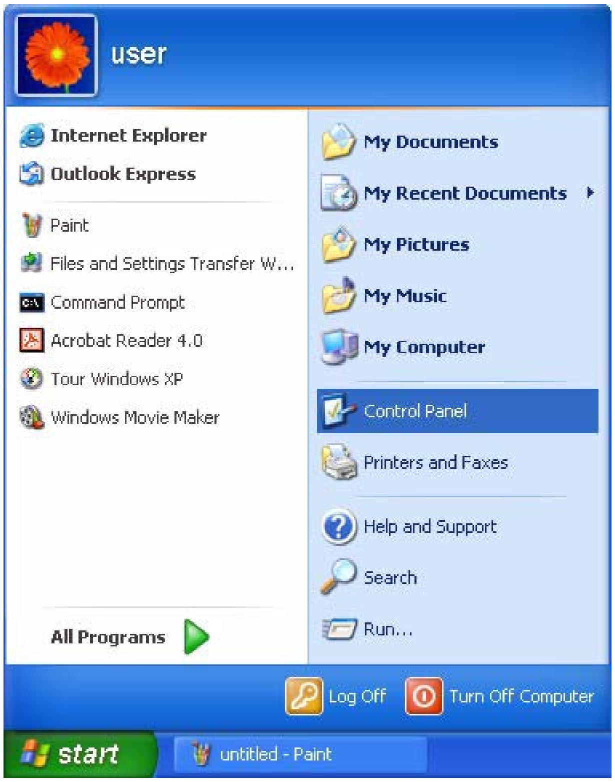
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

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

Windows 2000/NT/XP

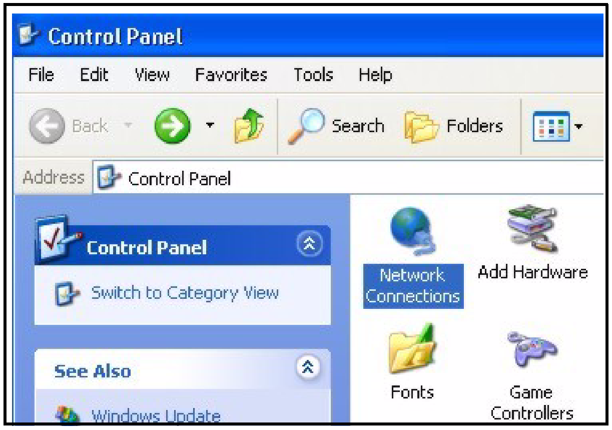
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 82 Windows XP: Start Menu



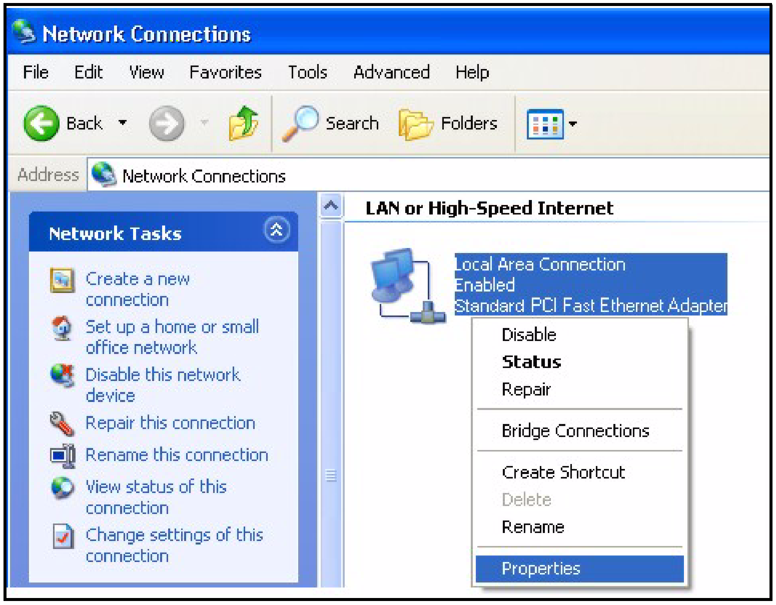
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 83 Windows XP: Control Panel



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

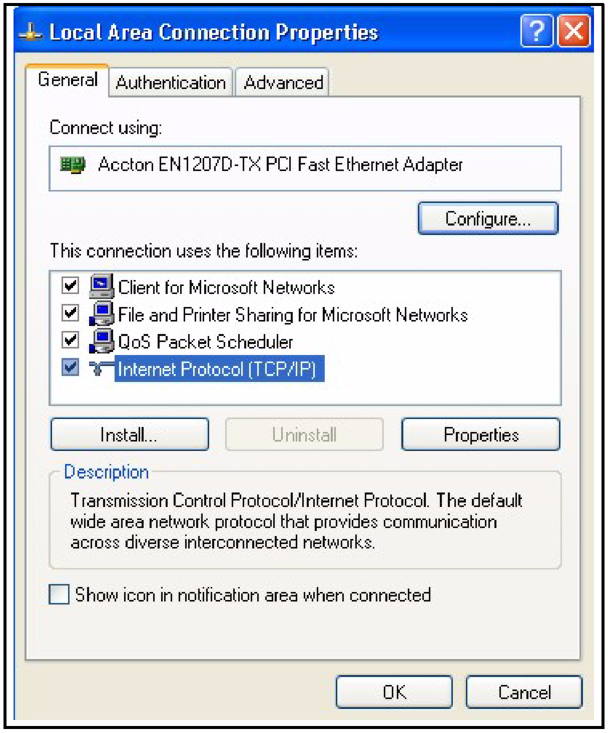
Figure 84 Windows XP: Control Panel: Network Connections: Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

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

Figure 85 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.

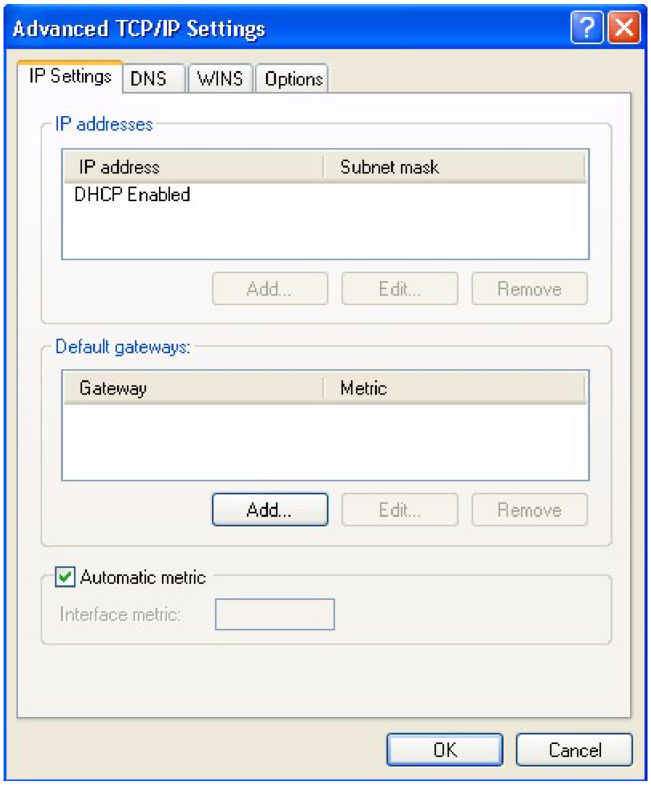
□ Show icon in notification area when connected

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 86 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 Setting**s tab and click **OK**.

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

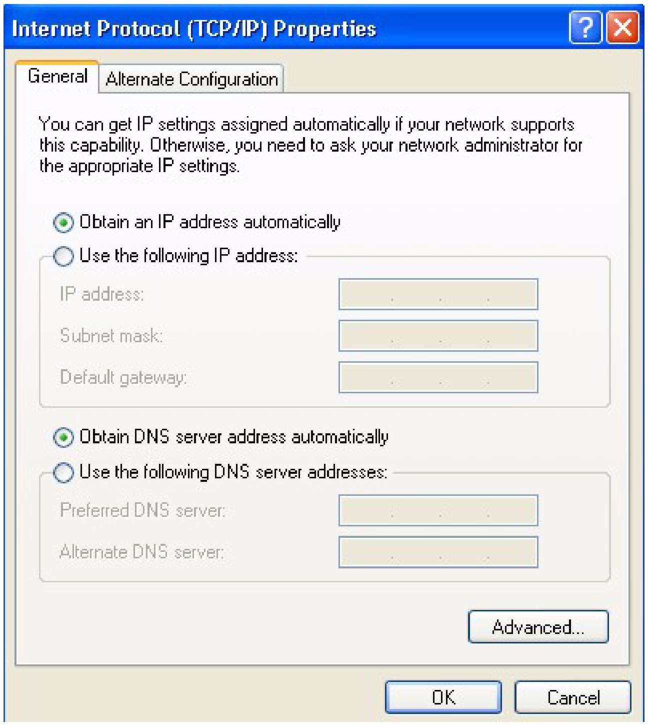
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

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

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

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

Figure 87 Windows XP: Internet Protocol (TCP/IP) Properties



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.

10Turn on your G-1000 v2 and restart your computer (if prompted).

Verifying Settings

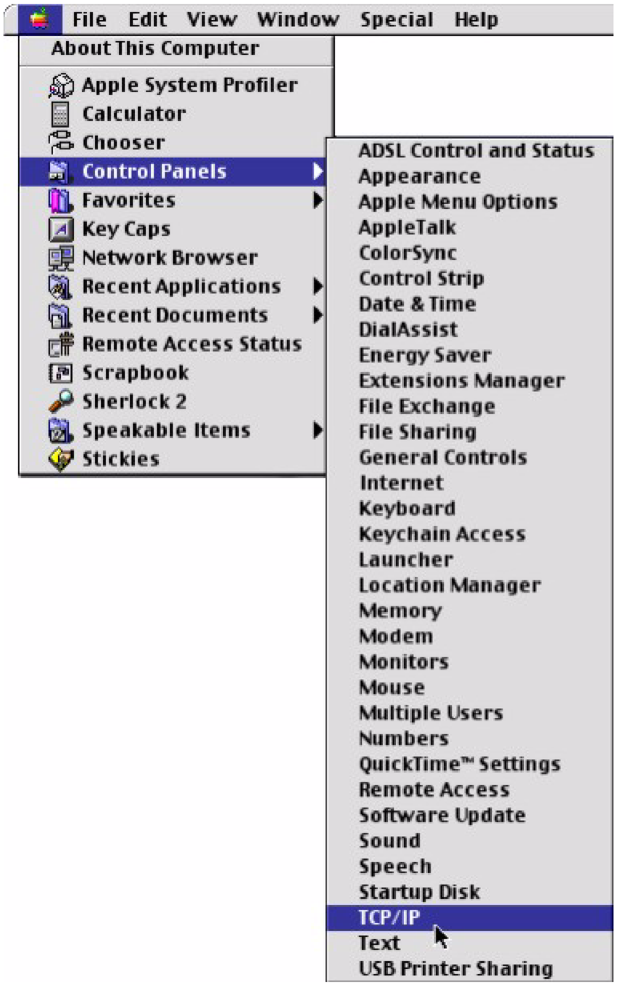
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

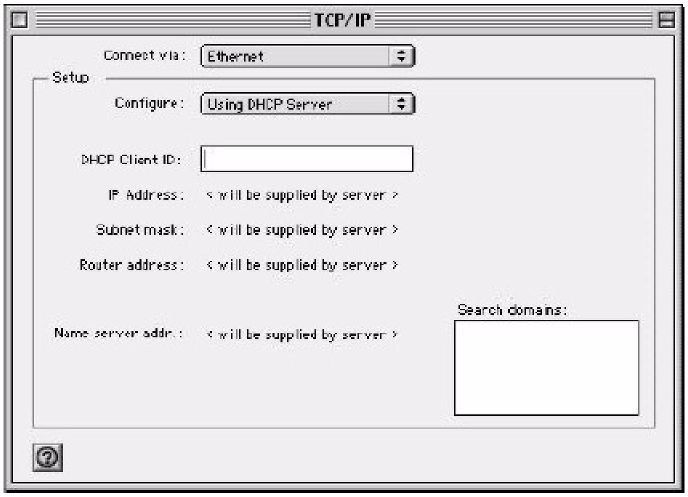
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 88 Macintosh OS 8/9: Apple Menu



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

Figure 89 Macintosh OS 8/9: TCP/IP



Connect via: Ethernet

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 >

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 v2 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 v2 and restart your computer (if prompted).

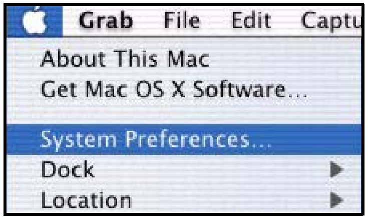
Verifying Settings

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 90 Macintosh OS X: Apple Menu

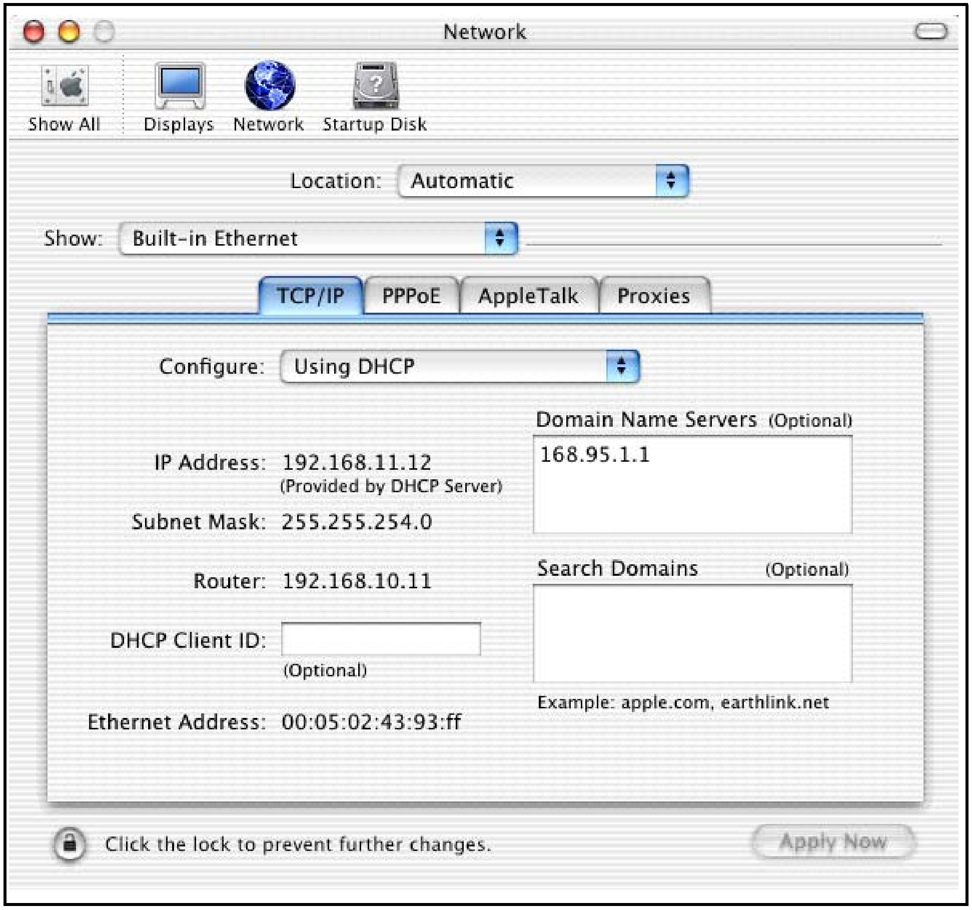


2 Click **Network** in the icon bar.

- 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 91 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

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 v2 in the **Router address** box.

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

6 Turn on your G-1000 v2 and restart your computer (if prompted).

Verifying Settings

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

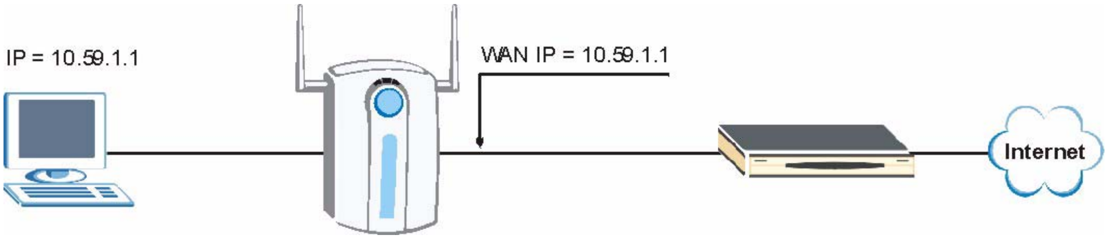
Appendix D
IP Address Assignment Conflicts

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 v2 is using the same LAN and WAN IP addresses

The following figure shows an example where the G-1000 v2 is using a WAN IP address that is the same as the IP address of a computer on the LAN.

Figure 92 IP Address Conflicts: CaseA

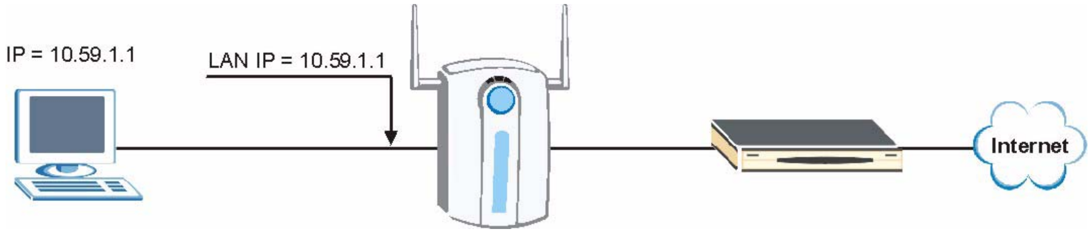


You must set the G-1000 v2 to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the G-1000 v2. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the G-1000 v2 use a public WAN IP address.

Case B: The G-1000 v2 LAN IP address conflicts with the DHCP client IP address

In the following figure, the G-1000 v2 is acting as a DHCP server. The G-1000 v2 assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 93 IP Address Conflicts: Case B

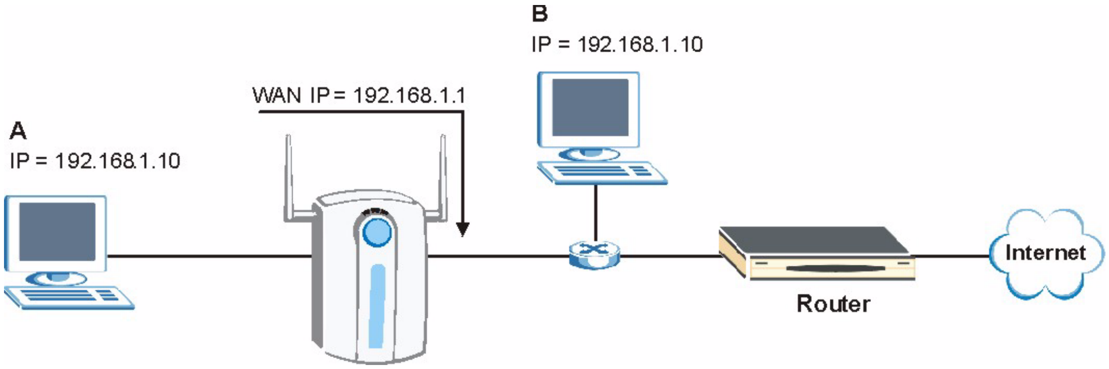


To solve this problem, make sure the G-1000 v2 LAN IP address is not in the DHCP IP address pool.

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 v2.

Figure 94 IP Address Conflicts: Case C



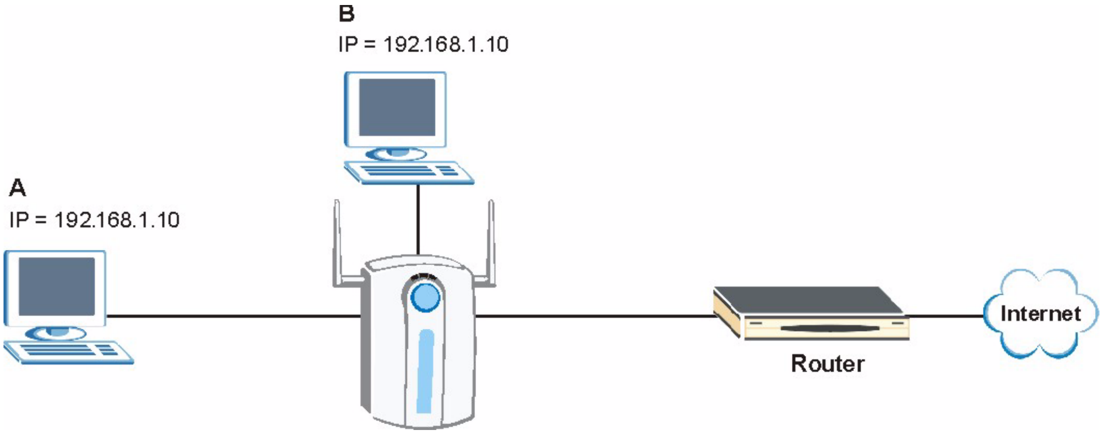
You must set the G-1000 v2 to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the G-1000 v2. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the G-1000 v2 use a public WAN IP address.

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 v2 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 v2 DHCP server assigns to another subscriber acting as a DHCP client.

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

Figure 95 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 E
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 65 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 66 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 67 "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 68 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 69 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.

Note: Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Table 70 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 71 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 72 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 73 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 74 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 75 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 76 Eight Subnets

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

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

Table 77 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 65) available for subnetting.

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

Table 78 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 F
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 G
Log Descriptions

This appendix provides descriptions of example log messages

Table 79 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

.

Table 80 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 81 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable

Table 81 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	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
	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 82 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 v2 to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the G-1000 v2 is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 83 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
8021x	0, 1
access	0, 1, 2, 3
attack	0, 1, 2, 3
error	0, 1, 2, 3
icmp	0, 1
javablocked	0, 1, 2, 3
mten	0, 1
packetfilter	0, 1
remote	0, 1
tcpreset	0, 1
upnp	0, 1
urlblocked	0, 1, 2, 3
urlforward	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 v2 (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 v2'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 v2 log category.

Use the `sys logs clear` command to erase all of the G-1000 v2's logs.

Log Command Example

This example shows how to set the G-1000 v2 to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#  .time              source             destination
notes
    message
  0|11/11/2002 15:10:12 |172.22.3.80:137
|172.22.255.255:137    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  1|11/11/2002 15:10:12 |172.21.4.17:138
|172.21.255.255:138    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  2|11/11/2002 15:10:11 |172.17.2.1         |224.0.1.60
|ACCESS BLOCK
    Firewall default policy: IGMP(set:8)
  3|11/11/2002 15:10:11 |172.22.3.80:137
|172.22.255.255:137    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  4|11/11/2002 15:10:10 |192.168.10.1:520
|192.168.10.255:520    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  5|11/11/2002 15:10:10 |172.21.4.67:137
|172.21.255.255:137    |ACCESS BLOCK
```

APPENDIX H
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

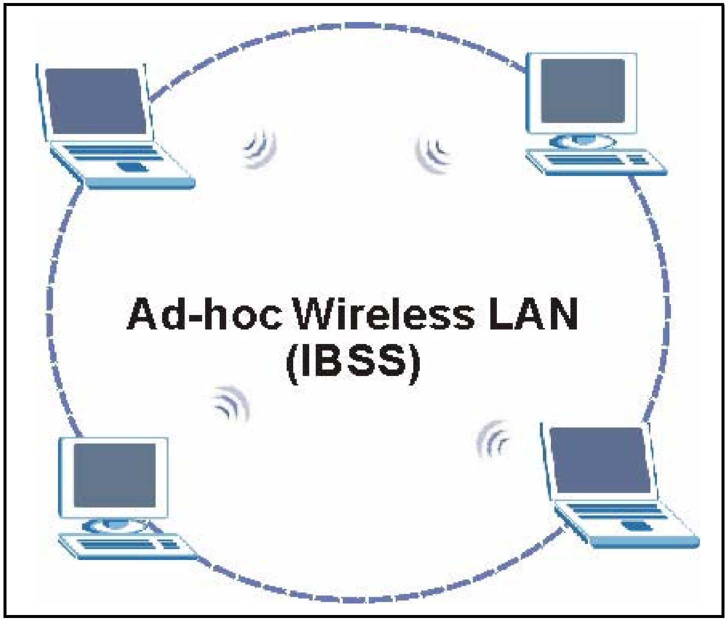
It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IBSS

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

Figure 96 IBSS (Ad-hoc) Wireless LAN

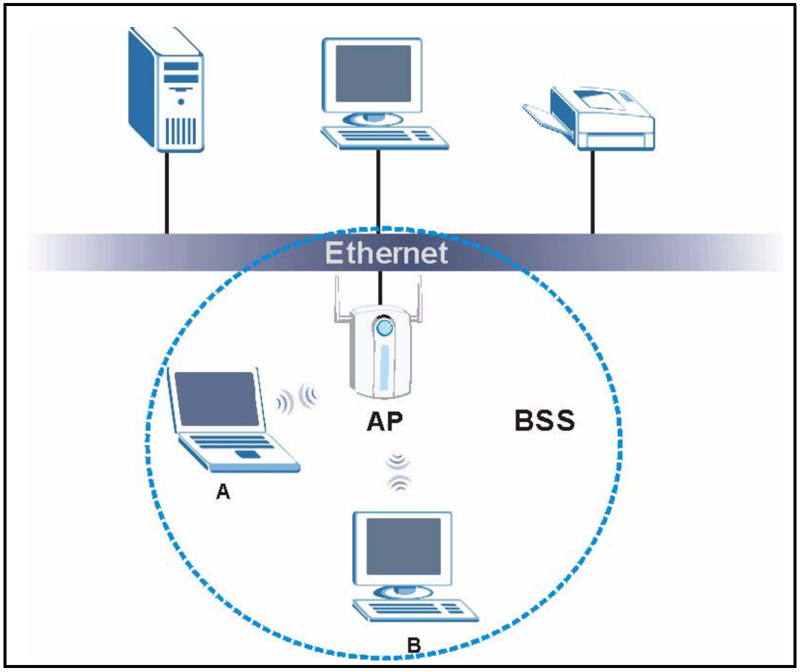


BSS

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.

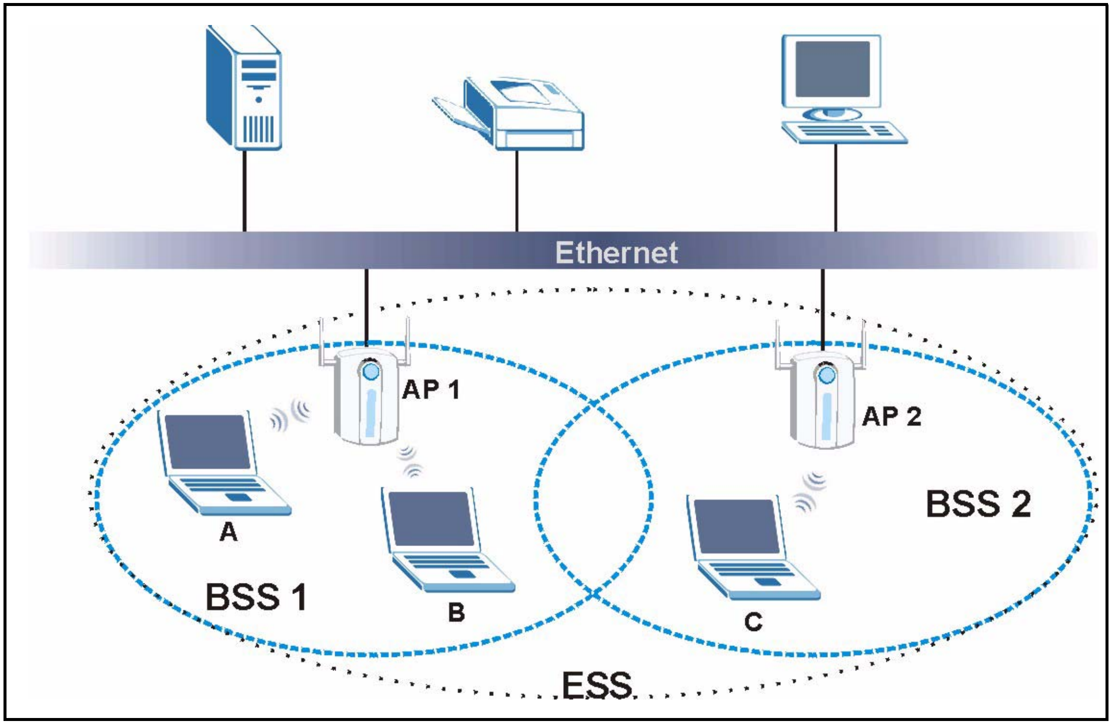
Figure 97 Basic Service Set



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). 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 98 Extended Service Set

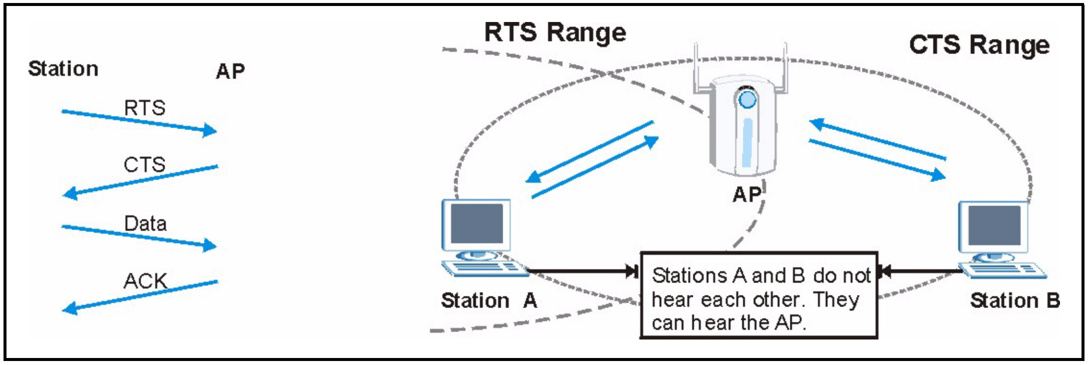


Wireless LAN Basics

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 99 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 G-1000 v2, it might not know that station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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

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

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

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

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

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 G-1000 v2 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 previous) 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.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

APPENDIX I
Wireless LAN Security

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

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 84 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.

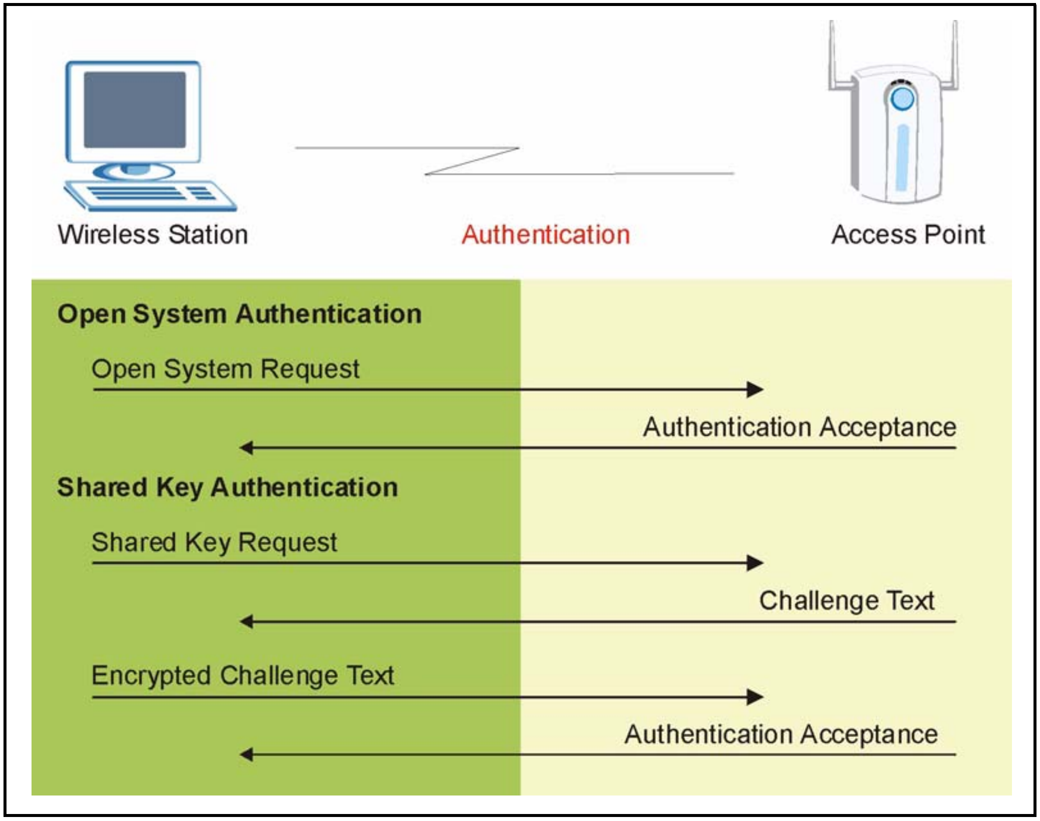
Table 85 Comparison of EAP Authentication Types

	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

WEP Authentication

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

Figure 100 WEP Authentication Steps



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

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

When your G-1000 v2's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the G-1000 v2 will accept either type of authentication request and the G-1000 v2 will fall back to use open authentication if the shared key does not match.

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (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.

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.

Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include 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.

WPA and WPA2 regularly change and rotate 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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

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

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

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a sucessful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

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 supplicant is 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.

The Funk Software's Odyssey client is bundled free (at the time of writing) with the client wireless adaptor(s).

WPA with RADIUS Application Example

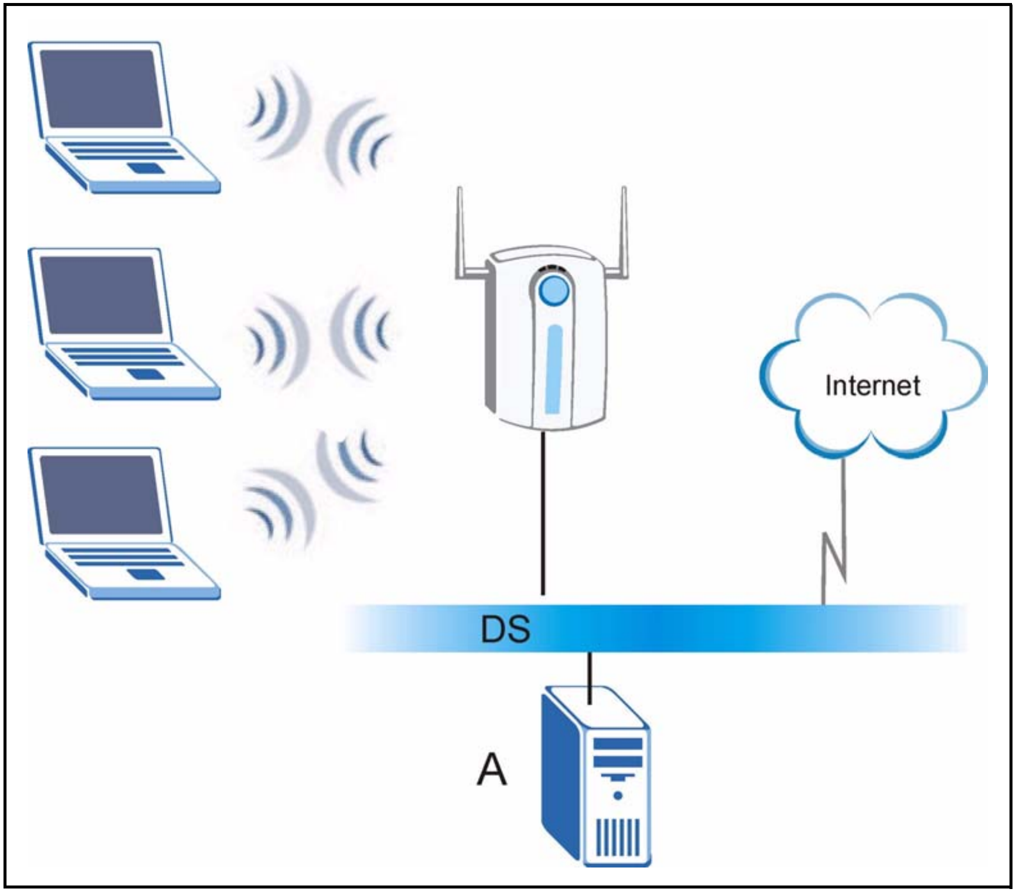
You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

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 communicated between the AP and the wireless clients.

Figure 101 WPA with RADIUS Application Example



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.

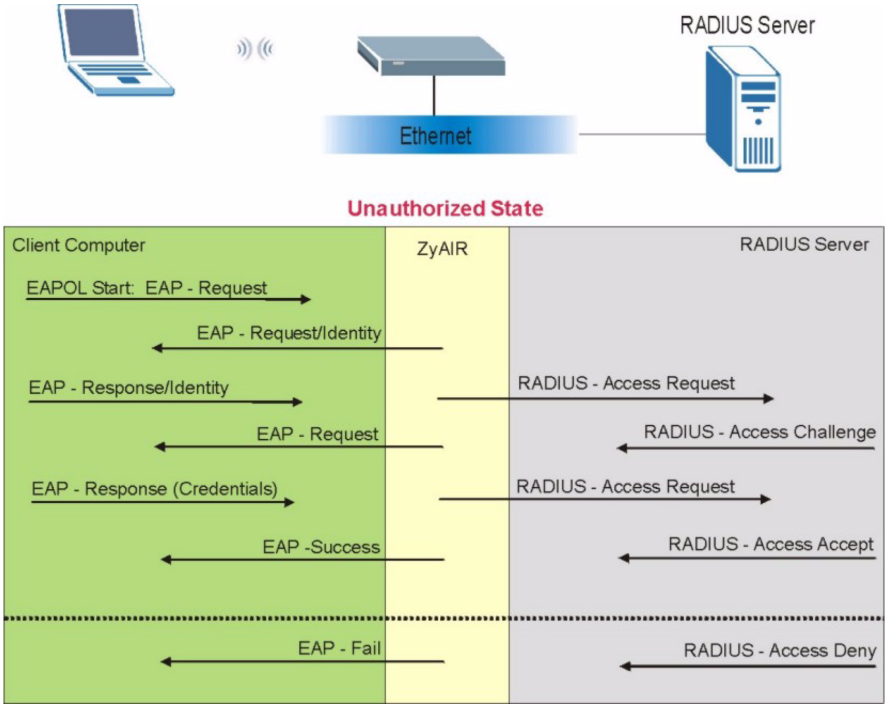
Table 86 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Disable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Disable

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 102 Sequences for EAP MD5–Challenge Authentication



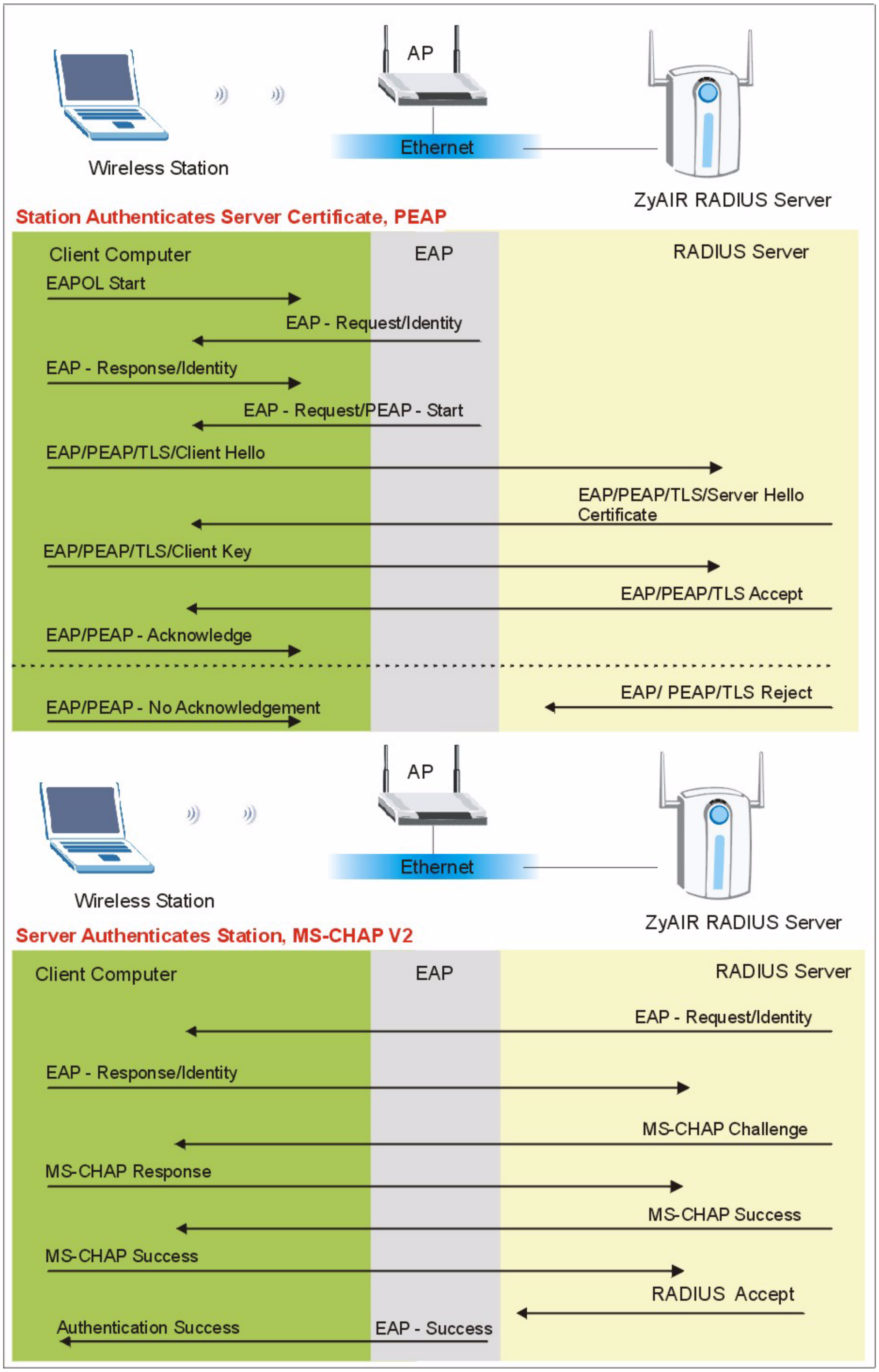
Mutual Authentication with Internal RADIUS server.

Microsofts Challenge-Handshake Authentication Protocol (MS-CHAP V2) is used to periodically verify the identity of the peer (station or other AP) using a three-way handshake.

The following figure depicts a typical wireless network with a G-1000 v2 RADIUS server for user authentication using PEAP (Protected EAP) and MS-CHAP V2.

The G-1000 v2 authenticates in two phases when it is acting as a RADIUS server:

Figure 103 Sequences for PEAP, MS–CHAP V2 Authentication



APPENDIX J
Types of EAP Authentication

This appendix discusses popular EAP authentication types.

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 IEEE802.1x.

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 the authentication types.

Table 87 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

APPENDIX K
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 v2 is equipped with a reverse polarity SMA jack, so it will work with any 2.4GHz wireless antenna with a reverse polarity SMA plug.

Index