ZyXEL G-560

802.11g Wireless Access Point

User's Guide

Version 1.0

November 2004

ZyXEL

Unleash Networking Power

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Caution

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

Notice 1

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

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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.

FC Tested To Comply With FCC Standards
FOR HOME OR OFFICE USE

ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

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

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

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

Customer Support

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

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

METHOD	SUPPORT E-MAIL	TELEPHONE[1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX[1]	FTP SITE	
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	
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	
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		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
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		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
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		

[1] "+" is the (prefix) number you enter to make an international telephone call.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase from the ZyXEL G-560 802.11g Wireless Access Point.

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

This User's Guide is designed to guide you through the configuration of your ZyXEL G-560 using the web configurator.

Use the web configurator to configure your ZyXEL G-560. Not all features can be configured through all interfaces.

Don't forget to register your product online for free future product updates and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  Our Quick Start Guide is designed to help you get up and running right away. It contains information on the configuration of key features and hardware connections and installation.

- ZyXEL Web Site

  The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- "Enter" means for you to type one or more characters (and press the carriage return). "Select" or "Choose" means for you to use one predefined choices.
- Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.

- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The ZyXEL G-560 802.11g Wireless Access Point may be referred to simply as the G-560 in the user’s guide.

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.

Graphics Icons Key

 G-560	 Computer	 Notebook computer
 Server	 Modem	 Wireless Signal
 Telephone	 Switch	 Router

Part I:

OVERVIEW

This part introduces the main features and applications of G-560 and shows how to access the web configurator and use the Wizard to set up the G-560.

Chapter 1
Getting to Know Your G-560

This chapter introduces the main features and applications of the G-560.

1.1 Introducing the G-560 Wireless Access Point

The G-560 is an access point (AP) through which wireless stations can communicate and/or access a wired network. The G-560 adds a wireless LAN to your existing network. It uses IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access) and MAC address filtering to give mobile users highly secured wireless connectivity. Both IEEE802.11b and IEEE802.11g compliant wireless devices can associate with the G-560.

The G-560 is easy to install and configure.

1.2 G-560 Features

The following sections describe the features of the G-560.

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

This auto-negotiating feature allows the G-560 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-560 reset button is built into the rear panel. Use this button to restore the factory default password.

802.11g Wireless LAN Standard

G-560 products containing the letter "G" in the model name, such as G-560 and G-162, comply with the IEEE 802.11g wireless standard.

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

SSL Passthrough

The G-560 allows SSL connections to go through the G-560. 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".

Wireless LAN MAC Address Filtering

Your G-560 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-560 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.

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the G-560's management settings.

Logging and Tracing

- Built-in message logging and packet tracing.

Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the G-560 to access your wired network.

1.3 The LED Display

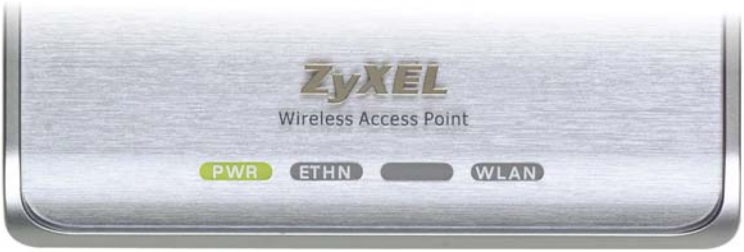


Figure 1 Front Panel

The following table describes the LEDs on the G-560.

Table 1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	Blinking	The ZyXEL G-560 is not ready or rebooting.
		On	The ZyXEL G-560 has a successful reboot and is receiving power.
		Off	The ZyXEL G-560 is not receiving power.
ETHN		Off	The ZyXEL G-560 does not have an Ethernet connection.
	Green	On	The ZyXEL G-560 has a successful 10Mbps Ethernet connection.
		Blinking	The ZyXEL G-560 is sending/receiving data.
	Amber	On	The ZyXEL G-560 has a successful 100Mbps Ethernet connection.
		Blinking	The ZyXEL G-560 is sending/receiving data.
WLAN	Green	Blinking	The ZyXEL G-560 is sending or receiving data through the wireless LAN.
		On	The ZyXEL G-560 is ready, but is not sending/receiving data.

1.4 Applications for the G-560

Here are some application examples of what you can do with your G-560.

1.4.1 Internet Access Application

The G-560 is an ideal access solution for wireless Internet connection. A typical Internet access application for your G-560 is shown as follows.

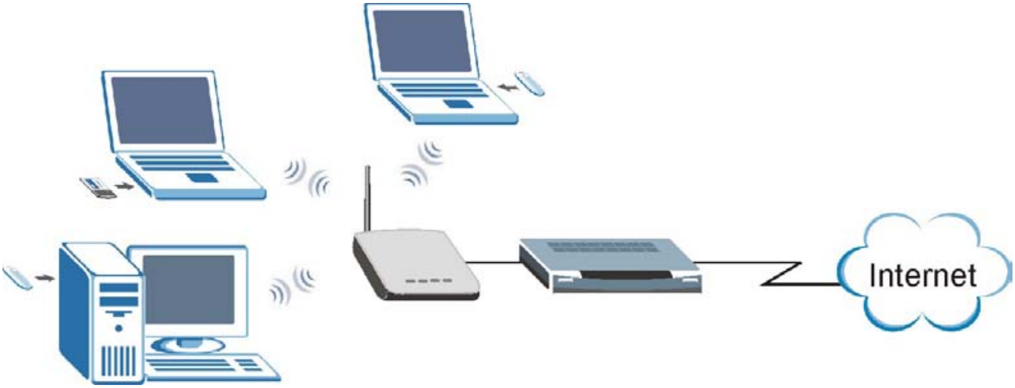


Figure 1-2 Internet Access Application

1.4.2 Corporation Network Application

In situations where users need to access corporate network resources and the Internet, the G-560 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-560 in an enterprise environment. The three computers with wireless adapters are allowed to access the network resource through the G-560 after account validation by the network authentication server.

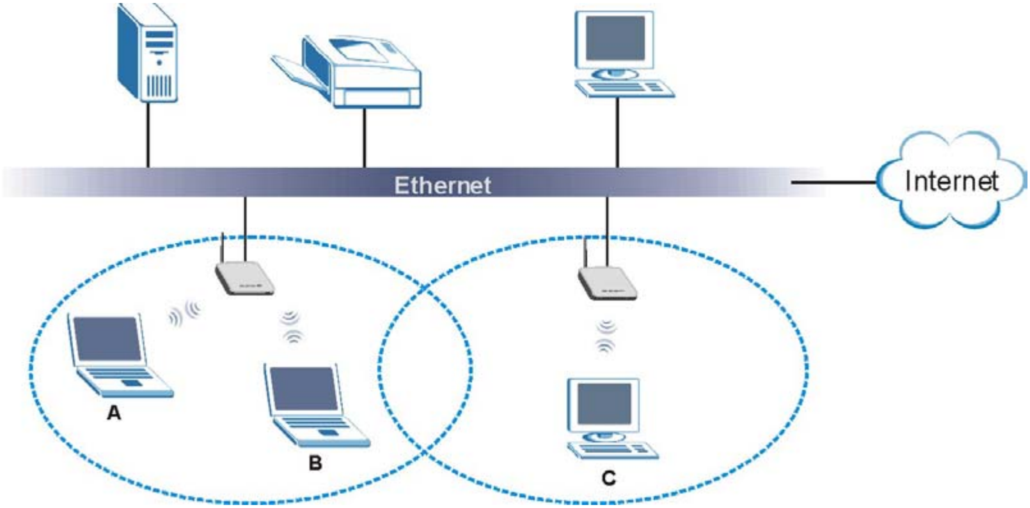


Figure 1-3 Corporation Network Application

Chapter 2
Management Computer Setup

This chapter describes how to prepare your computer to access the G-560 web configurator.

2.1 Introduction

You can connect a computer to the G-560 for management purposes either using an Ethernet connection (recommended for a first time management session) or wirelessly.

2.2 Wired Connection

You must prepare your computer/computer network to connect to the G-560 if you are using a wired connection. Your computer's IP address and subnet mask must be on the same subnet as the G-560. This can be done by setting up your computer's IP address.

The following figure shows you an example of accessing your G-560 via a wired connection with an Ethernet cable.

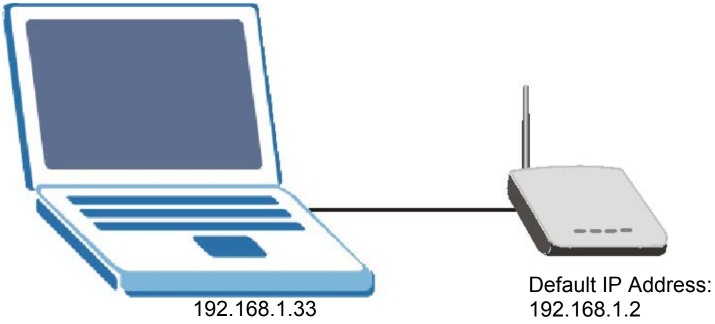


Figure 2-1 Wired Connection

2.2.1 Setting Up Your Computer’s IP Address

Skip this section if your computer’s IP address is already between 192.168.1.3 and 192.168.1.254 with subnet mask 255.255.255.0.

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

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1. Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

2. In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

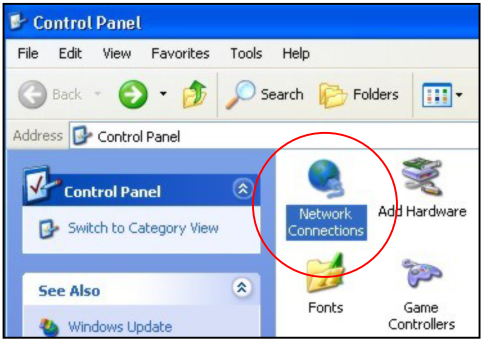


Figure 2-2 Control Panel

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

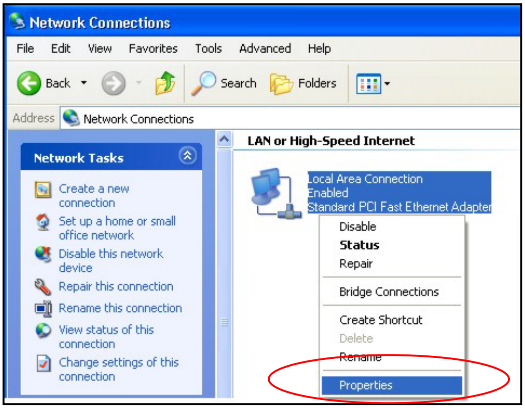
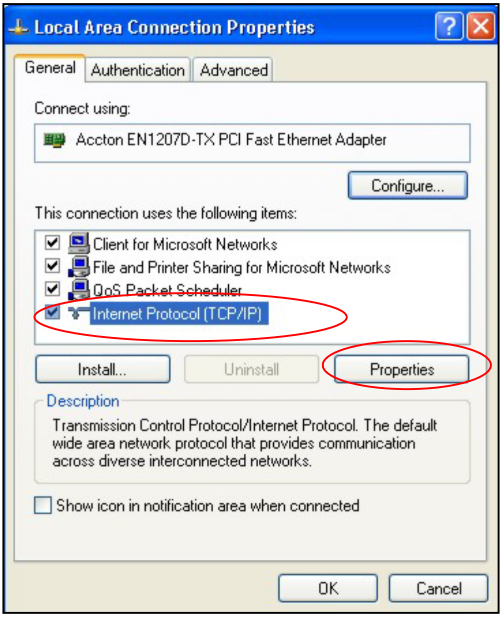


Figure 2-3 Network Connection

4. Select **Internet Protocol (TCP/IP)** and then click **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)

Description

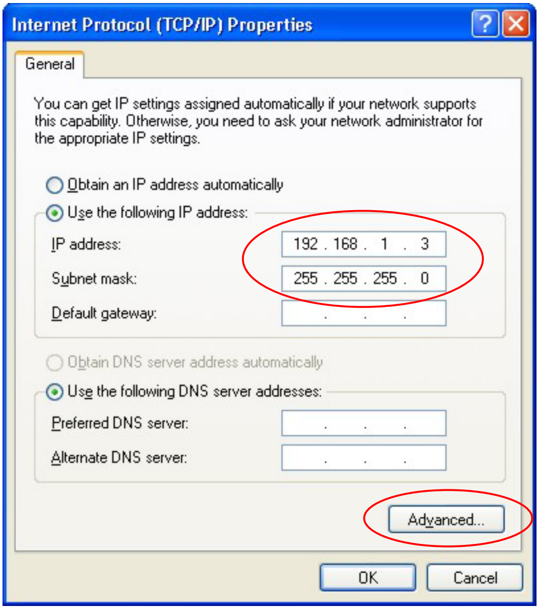
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

Figure 2-4 Local Area Connection Properties

5. Select **Use the following IP Address** and fill in an **IP address** (between 192.168.1.3 and 192.168.1.254).

- Type 255.255.255.0 as the **Subnet mask**.
- Click **Advanced**.[1]



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: 192 . 168 . 1 . 3

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

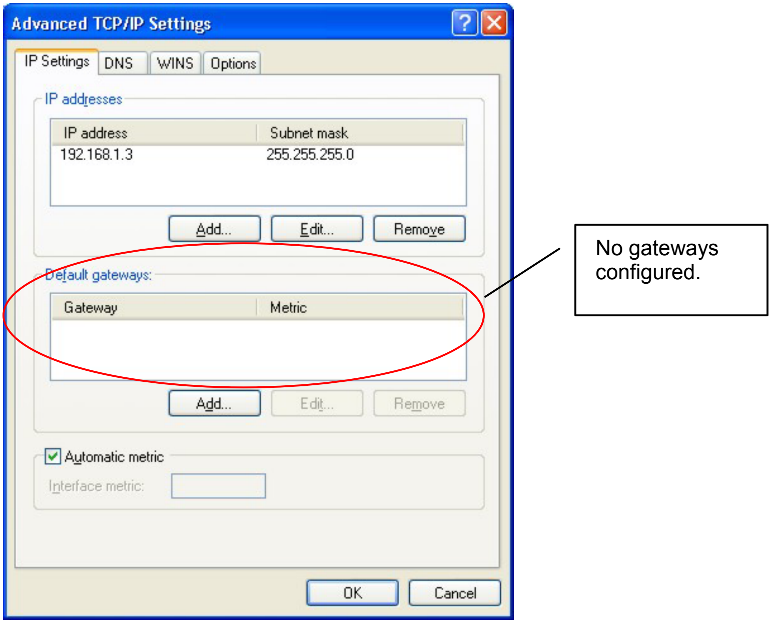
Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 2-5 Internet Protocol Properties

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

[1] See the appendices for information on configuring DNS server addresses.



IP address	Subnet mask
192.168.1.3	255.255.255.0

☑ Automatic metric

Interface metric:

No gateways configured.

Figure 2-6 Advanced TCP/IP Settings

7. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
8. Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
9. Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

2.3 Wireless Connection

Ensure that the wireless station have a compatible wireless card/adapter with the same wireless settings as the G-560. The following figure shows how you can access your G-560 wirelessly.

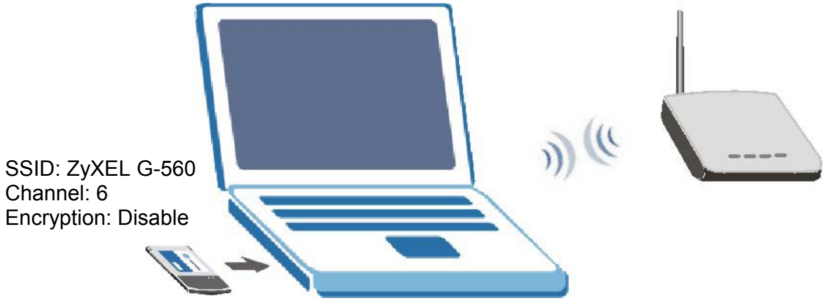


Figure 2-7 Wireless Connection

The wireless stations and G-560 must use the same SSID, channel and wireless security settings for wireless communication.

If you do not enable any wireless security on your G-560, your network traffic is visible to any wireless networking device that is within range.

2.4 Resetting the G-560

If you forget the G-560's IP address or your password, to access the G-560, you will need to reload the factory-default using the **RESET** button. Resetting the G-560 replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The following parameters will be reset to the default values.

Table 2-1 Factory Defaults

PARAMETER	DEFAULT VALUE
IP Address	192.168.1.2
Password	1234
Wireless Security	Disabled
SSID	ZyXEL G-560

2.4.1 Method of Restoring Factory-Defaults

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

1. Use the **RESET** button on the G-560 to upload the default configuration file (hold this button in for about 10 seconds or release the button when the **PWR** LED starts blinking).
2. Use the web configurator to restore defaults. Click **SYSTEM**, **Management**, and then the **Configuration File** tab. From here you can restore the G-560 to factory defaults.

Chapter 3
Introducing the web configurator

This chapter describes how to configure the G-560 using the Wizard.

3.1 Web Configurator Overview

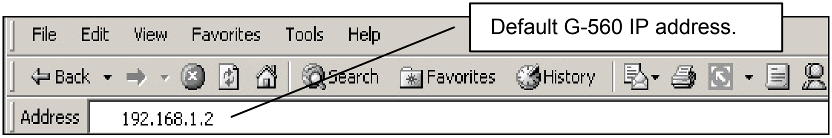
Follow the steps below to access the web configurator, select a language, change your login password and choose a configuration method from the status screen.

Step 1. Make sure your G-560 hardware is properly connected (*refer to the Quick Start Guide*).

Step 2. Prepare your computer/computer network to connect to the G-560 (refer to *section 2.2.1* for instructions on how to do this).

Step 3. Launch your web browser.

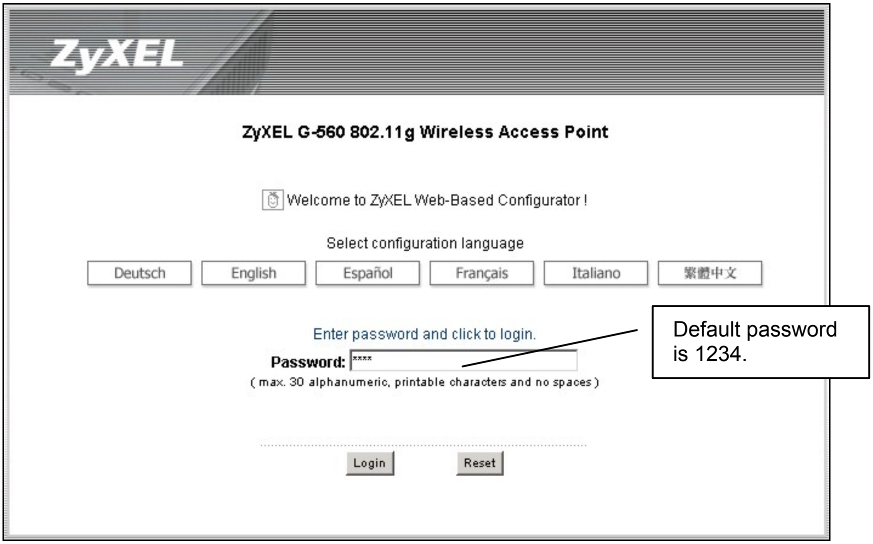
Step 4. Type "192.168.1.2" (default) as the URL. Press **Enter**.



192.168.1.2

Default G-560 IP address.

Step 5. Select your language. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.



ZyXEL G-560 802.11g Wireless Access Point

Welcome to ZyXEL Web-Based Configurator !

Select configuration language

Enter password and click to login.

Password: ****

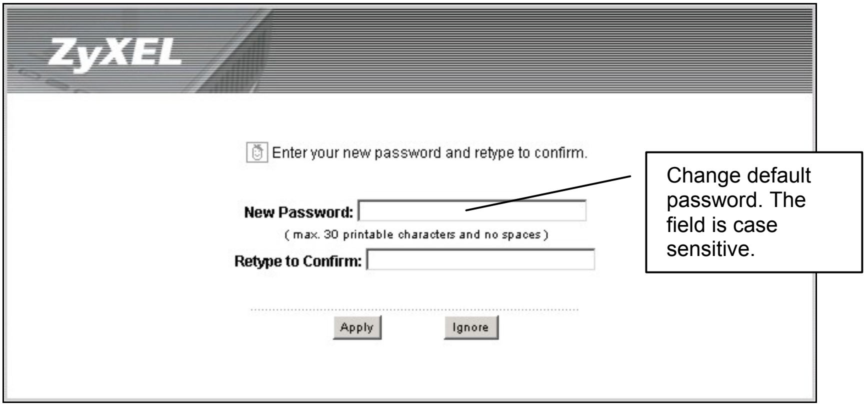
(max. 30 alphanumeric, printable characters and no spaces)

Default password is 1234.

Figure 3-1 Welcome Screen

Step 6. 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** to allow access without password change.

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



Enter your new password and retype to confirm.

New Password:

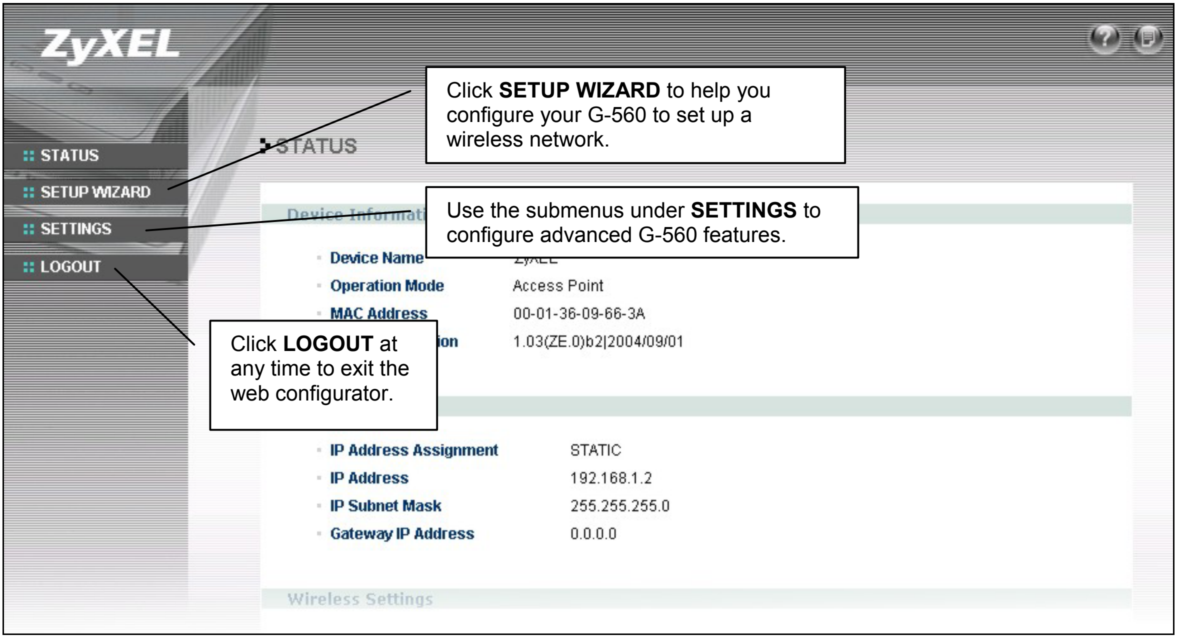
(max. 30 printable characters and no spaces)

Retype to Confirm:

Change default password. The field is case sensitive.

Figure 3-2 Change Password Screen

Step 7. You should now see the **STATUS** screen.



STATUS

Device Informati

- Device Name ZyXEL
- Operation Mode Access Point
- MAC Address 00-01-36-09-66-3A
- ion 1.03(ZE.0)b2|2004/09/01

- IP Address Assignment STATIC
- IP Address 192.168.1.2
- IP Subnet Mask 255.255.255.0
- Gateway IP Address 0.0.0.0

Wireless Settings

Click **SETUP WIZARD** to help you configure your G-560 to set up a wireless network.

Use the submenus under **SETTINGS** to configure advanced G-560 features.

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

Figure 3-3 Status Screen

See the rest of this *User’s Guide* for configuration details and background information on all G-560 features using the web configurator.

3.2 Configuring the G-560 Using the Wizard

The wizard consists of a series of screens to help you configure your G-560 for wireless stations to access your wired LAN.

Use the following buttons to navigate the Wizard:

Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue to the next screen.

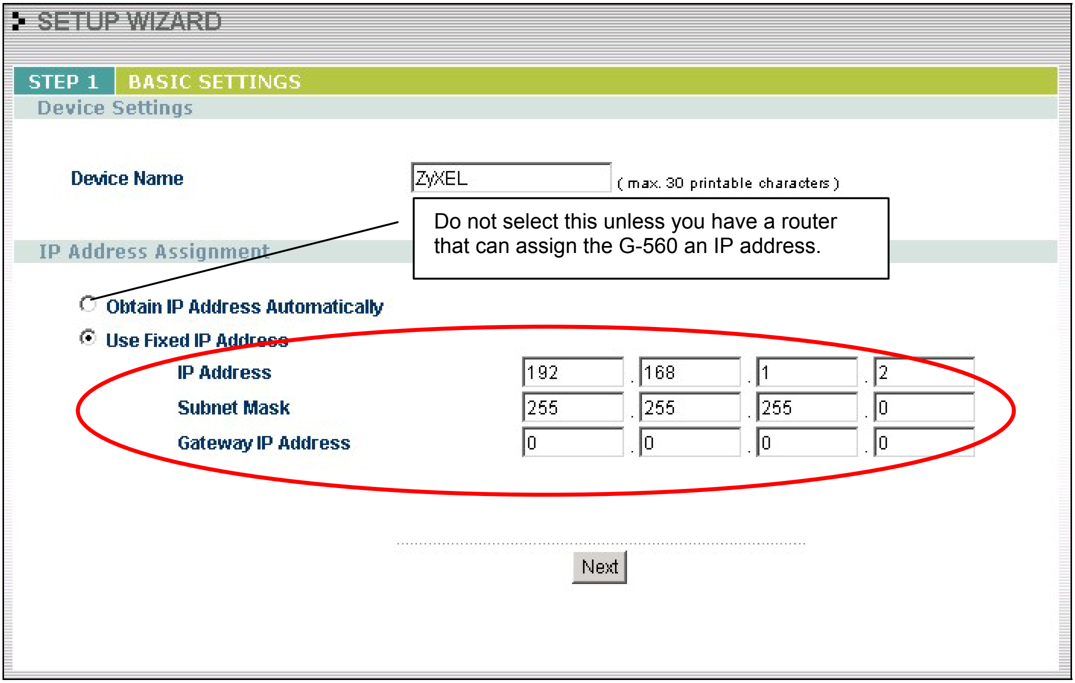
No configuration changes will be saved to the G-560 until you click **Finish**.

3.2.1 Basic Settings

Click **SETUP WIZARD** to display the first wizard screen shown next. Refer to the *System Screens* chapter for more background information.

1. Enter a descriptive name to identify the G-560 in the Ethernet network.
2. Select **Obtain IP Address automatically** if you want to put the G-560 behind a router that assigns an IP address. If you select this by mistake, use the **Reset** button to restore the factory default IP address.
3. Select **Use fixed IP address** to give the G-560 a static IP address. The IP address you configure here is used for management of the G-560 (accessing the web configurator).

   Enter a **Subnet Mask** appropriate to your network and the **Gateway IP Address** of the neighboring device, if you know it. If you do not, leave the **Gateway IP Address** field as **0.0.0.0**.



SETUP WIZARD

STEP 1 BASIC SETTINGS

Device Settings

Device Name: ZyXEL (max. 30 printable characters)

IP Address Assignment

○ Obtain IP Address Automatically

● Use Fixed IP Address

IP Address	192	168	1	2
Subnet Mask	255	255	255	0
Gateway IP Address	0	0	0	0

Do not select this unless you have a router that can assign the G-560 an IP address.

Figure 3-4 Wizard 1: Basic Settings

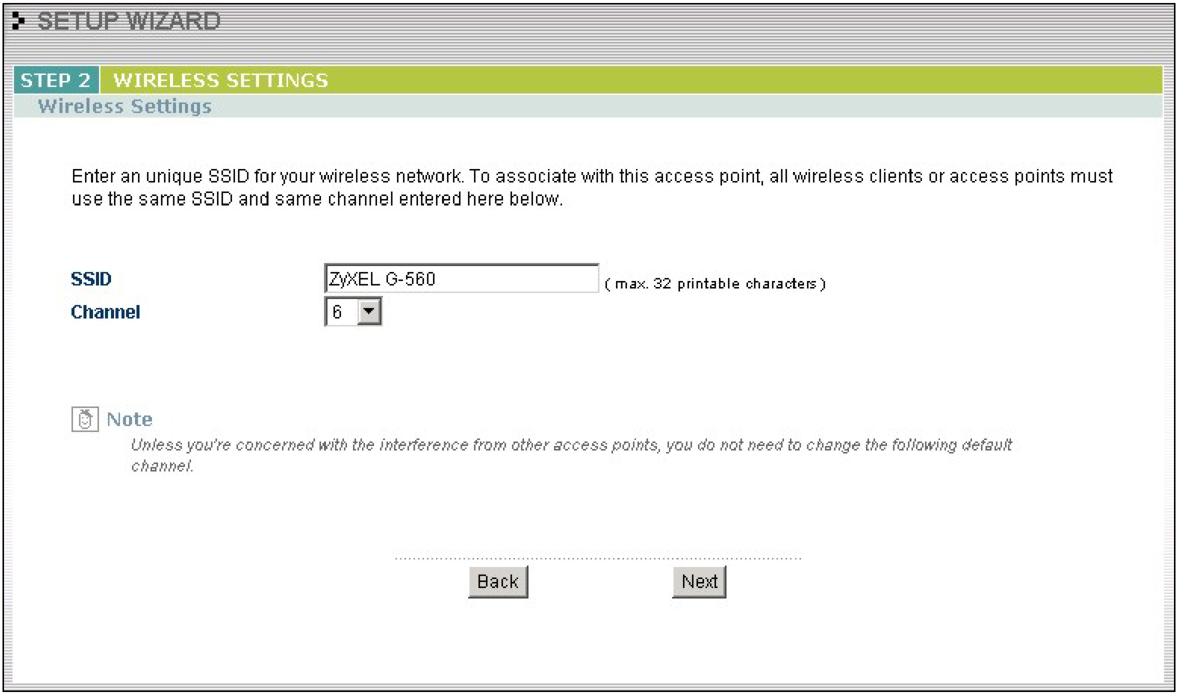
If you change the ZyXEL G-560's IP address, you must use the *new* IP address if you want to access the web configurator again.

3.2.2 Wireless Settings

Use the second wizard screen to set up the wireless LAN. See the *Wireless Screens* chapter for background information.

1. The SSID is a unique name to identify the G-560 in a wireless network. Enter up to 32 printable characters. Spaces are allowed. If you change this field on the G-560, make sure all wireless stations use the same SSID in order to access the network.
2. A wireless device uses a channel to communicate in a wireless network. Select a channel that is not already in use by a neighboring wireless device.

The wireless stations and G-560 must use the same SSID, channel and wireless security settings for wireless communication.



SETUP WIZARD

STEP 2 WIRELESS SETTINGS

Wireless Settings

Enter an unique SSID for your wireless network. To associate with this access point, all wireless clients or access points must use the same SSID and same channel entered here below.

SSID: ZyXEL G-560 (max. 32 printable characters)

Channel: 6

Note

Unless you're concerned with the interference from other access points, you do not need to change the following default channel.

Figure 3-5 Wizard 2: Wireless Settings

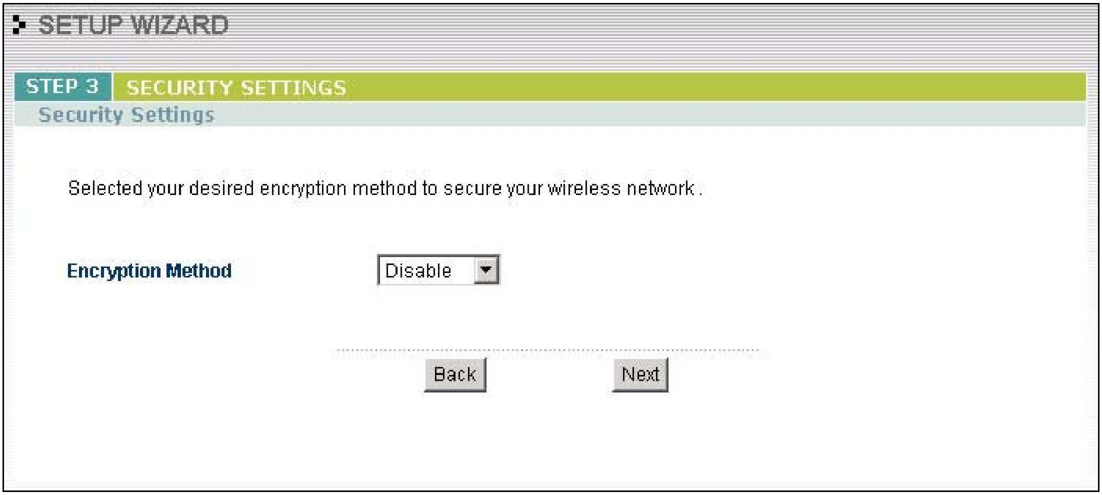
3.2.3 Security Settings

Fill in the fields in the third wizard configuration screen. The screen varies depending on what you select in the **Encryption Method** field. Select **Disable** to have no wireless security configured, select **WEP**, or select **WPA-PSK** if your wireless clients support WPA-PSK. Go to **SETTINGS**, **WIRELESS** and **Security** if you want WPA or 802.1x. See the *Wireless Screens* chapter for background information.

Disable

Select **Disable** to have no wireless LAN security configured. If you do not enable any wireless security on your G-560, your network is accessible to any wireless networking device that is within range.

With no wireless security a neighbor can access and see traffic in your network.


SETUP WIZARD

STEP 3 SECURITY SETTINGS

Security Settings

Selected your desired encryption method to secure your wireless network .

Encryption Method: Disable

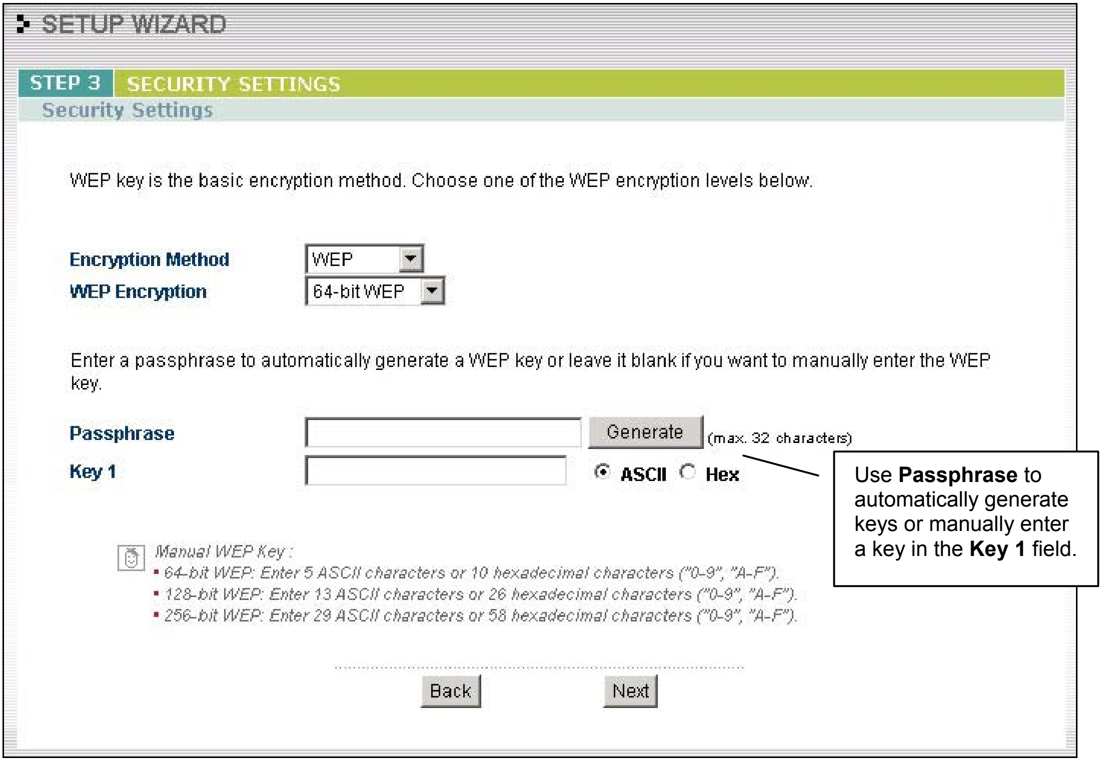
Figure 3-6 Setup Wizard 3: Disable

WEP

1. WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **64-bit**, **128-bit** or **256-bit** from the **WEP Encryption** drop-down list box and then follow the on-screen instructions to set up the WEP keys.
2. Choose an encryption level from the drop-down list. The higher the WEP Encryption, the higher the security but the slower the throughput.
3. You can generate or manually enter a WEP key by either
   - Entering a **Passphrase** (up to 32 printable characters) and clicking **Generate**. The G-560 automatically generates a WEP key.

or

- Selecting **ASCII** or **Hex** WEP key input method and entering a manual key in the **Key 1** field.



SETUP WIZARD

STEP 3 SECURITY SETTINGS

Security Settings

WEP key is the basic encryption method. Choose one of the WEP encryption levels below.

Encryption Method	WEP
WEP Encryption	64-bit WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

Passphrase (max. 32 characters)

Key 1 ● ASCII ○ Hex

Manual WEP Key :

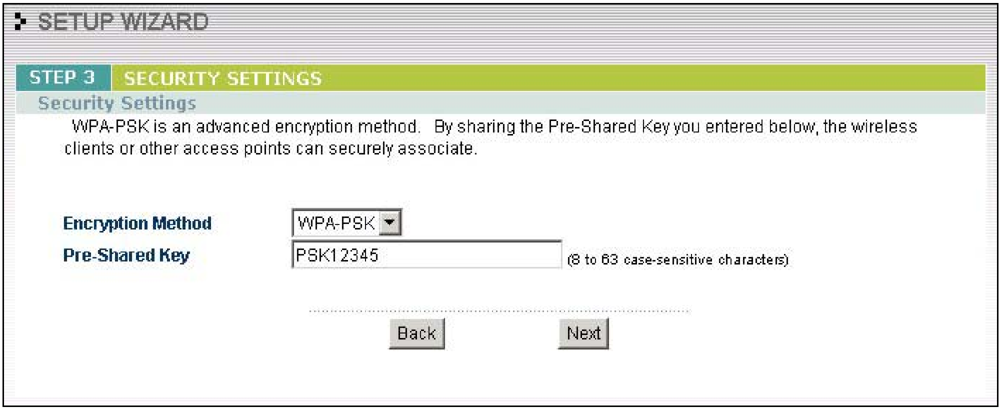
- *64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").*
- *128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").*
- *256-bit WEP: Enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F").*

Use **Passphrase** to automatically generate keys or manually enter a key in the **Key 1** field.

Figure 3-7 Wizard 3: WEP

WPA-PSK

1. Type a pre-shared key to have a more secure wireless connection. Choose this option only if your wireless clients support it.
2. Type from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.



SETUP WIZARD

STEP 3 SECURITY SETTINGS

Security Settings

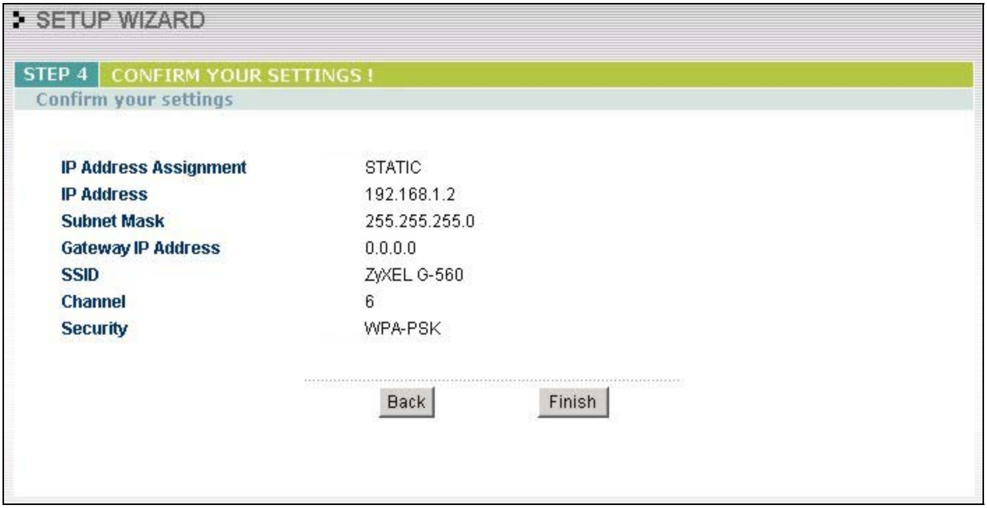
WPA-PSK is an advanced encryption method. By sharing the Pre-Shared Key you entered below, the wireless clients or other access points can securely associate.

Encryption Method	WPA-PSK
Pre-Shared Key	PSK12345 (8 to 63 case-sensitive characters)

Figure 3-8 Wizard 3: WPA-PSK

3.2.4 Confirm Your Settings

The following read-only screen shows the status of the current settings. Use the summary table to check whether what you have configured is correct. Click **Finish** to complete the wizard configuration and save your settings.



SETUP WIZARD

STEP 4 CONFIRM YOUR SETTINGS !

Confirm your settings

IP Address Assignment	STATIC
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
SSID	ZyXEL G-560
Channel	6
Security	WPA-PSK

Figure 3-9 Wizard 4: Confirm Your Settings

For more detailed background information, see the rest of this *User's Guide*.

Part II:

STATUS AND SETTINGS

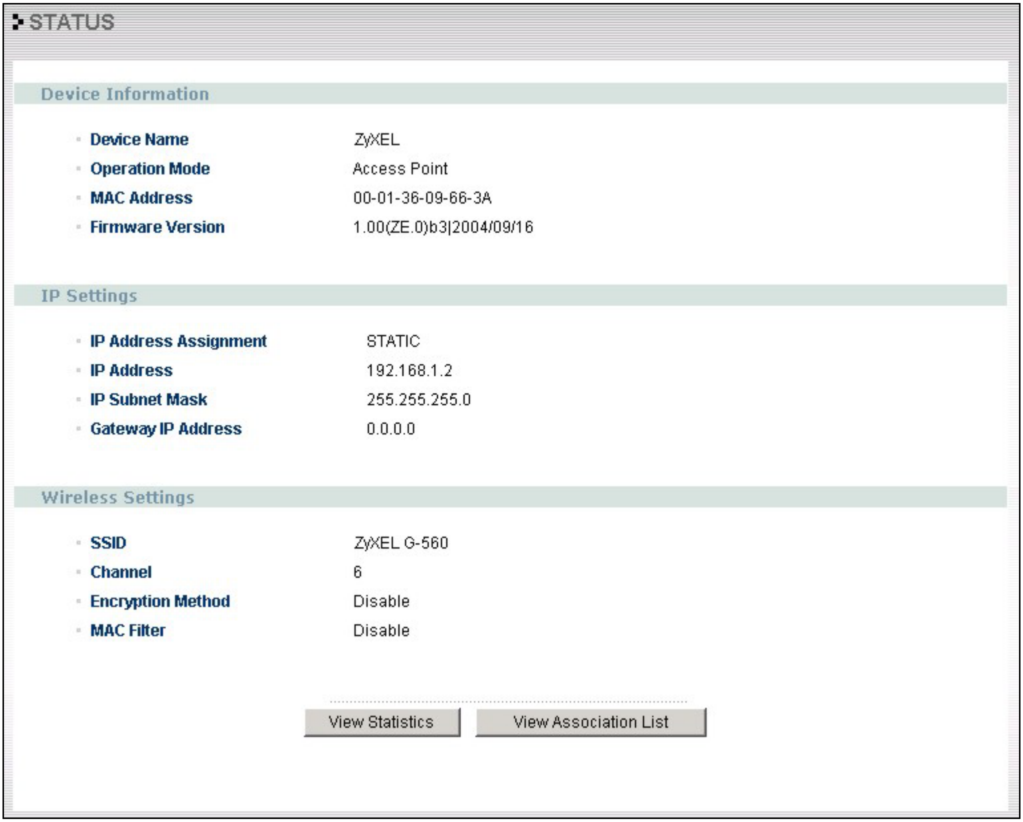
This part covers the information and web configurator screens of Status and Settings.

Chapter 4
Status Screens

This chapter describes the Status screens.

4.1 System Status

Click **STATUS** to display a snapshot of your G-560 settings. You can also view network statistics and a list of wireless stations currently associated with the G-560. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.



STATUS

Device Information

Device Name	ZyXEL
Operation Mode	Access Point
MAC Address	00-01-36-09-66-3A
Firmware Version	1.00(ZE.0)b3|2004/09/16

IP Settings

IP Address Assignment	STATIC
IP Address	192.168.1.2
IP Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0

Wireless Settings

SSID	ZyXEL G-560
Channel	6
Encryption Method	Disable
MAC Filter	Disable

Figure 4-1 Status

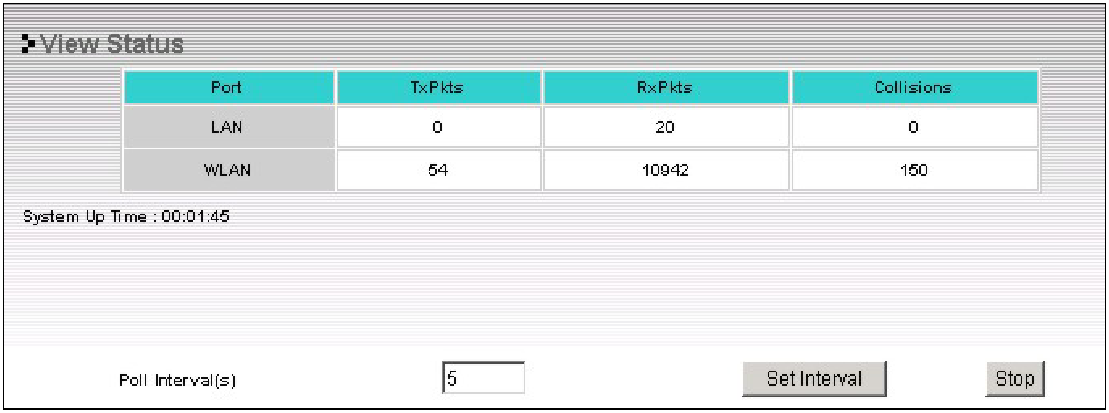
The following table describes the labels in this screen.

Table 4-1 Status

LABEL	DESCRIPTION
Device Information	
Device Name	This is the same as **Device Name** you entered in the first wizard screen if you entered one there. It is for identification purposes.
Operation Mode	This field shows whether the G-560 is functioning as an access point.
MAC Address	This field displays the MAC address of the G-560. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer. A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Firmware Version	This is the firmware version and the date the firmware was created.
IP Settings	
IP Address Assignment	This field displays whether the G-560 is set to obtain an IP address from a DHCP server or use a manually entered static IP address.
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.
Gateway IP Address	This is the IP address of a gateway. Leave this field as **0.0.0.0** if you do not know it.
Wireless Settings	
SSID	This is the descriptive name used to identify the G-560 in a wireless network.
Channel	This field displays the radio channel the G-560 is currently using.
Encryption Method	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA** or **802.1X**) or inactive (**Disable**).
MAC Filter	This field shows whether MAC filter is enabled or not. With MAC filtering, you can allow or deny access to the G-560 based on the MAC addresses of the wireless stations.
View Statistics	Click **View Statistics** to see performance statistics such as number of packets sent and number of packets received.
View Association List	Click **View Association List** to show the wireless stations that are currently associated to the G-560.

4.1.1 Statistics

Click **View Statistics** in the **STATUS** screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.



View Status

Port	TxPkts	RxPkts	Collisions
LAN	0	20	0
WLAN	54	10942	150

System Up Time : 00:01:45

Poll Interval(s) 5

Figure 4-2 Status: View Statistics

The following table describes the labels in this screen.

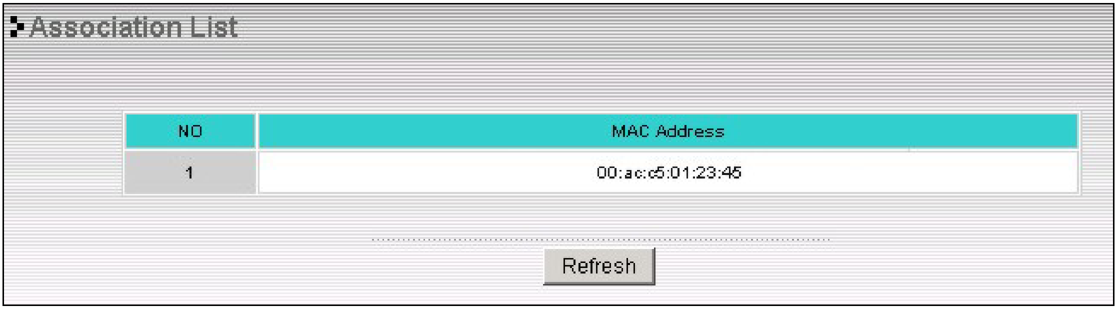
Table 4-2 Status: View Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet or 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.
System Up Time	This is the total time the G-560 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.

4.1.2 Association List

Click **View Association List** in the **STATUS** screen. View the wireless stations that are currently associated to the G-560 in the **Association List** screen.

Click **STATUS** and then the **View Association List** button to display the screen as shown next.



Association List

NO	MAC Address
1	00:ac:c5:01:23:45

Figure 4-3 Status: View Association List

The following table describes the labels in this screen.

Table 4-3 Status: View Association List

LABEL	DESCRIPTION
No.	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Refresh	Click **Refresh** to reload the screen.

Chapter 5 System Screens

This chapter provides information on the System screens.

5.1 Factory Ethernet Defaults

The Ethernet parameters of the G-560 are preset in the factory with the following values:

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

These parameters should work for the majority of installations.

5.2 TCP/IP Parameters

5.2.1 IP Address Assignment

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

Table 5-1 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

5.2.2 IP Address and Subnet Mask

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

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

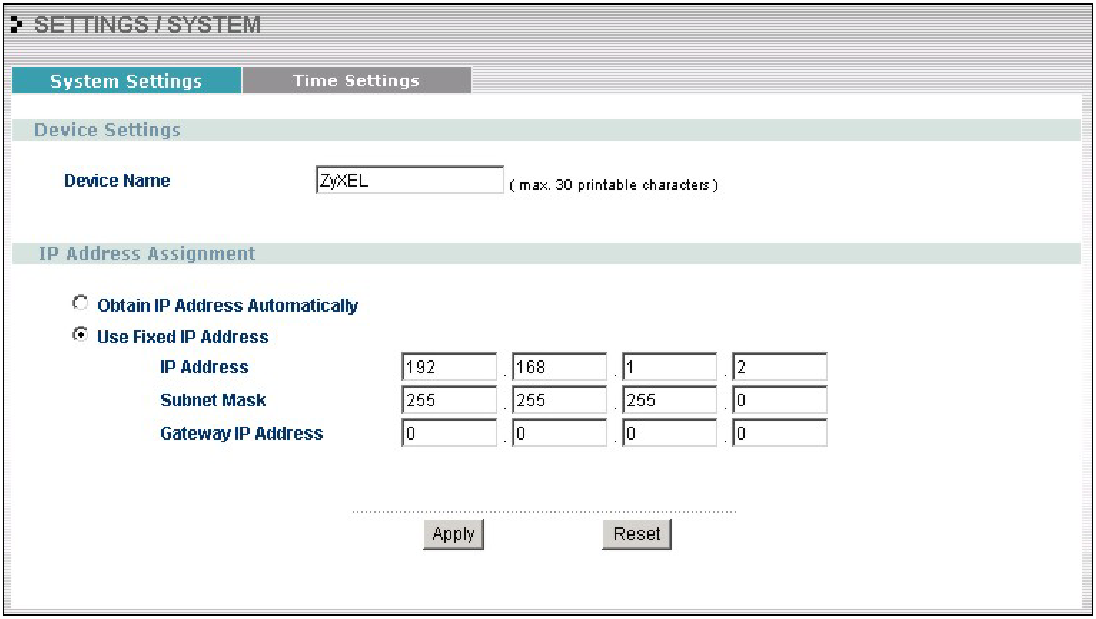
If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use;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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your G-560, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your G-560 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the G-560 unless you are instructed to do otherwise.

5.3 Configuring System Settings

Click **SETTINGS**, then **SYSTEM** to open the **System Settings** screen.



SETTINGS / SYSTEM

System Settings | Time Settings

Device Settings

Device Name: ZyXEL (max. 30 printable characters)

IP Address Assignment

○ Obtain IP Address Automatically

● Use Fixed IP Address

IP Address: 192 . 168 . 1 . 2

Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Figure 5-1 System Settings

The following table describes the labels in this screen.

Table 5-2 System Settings

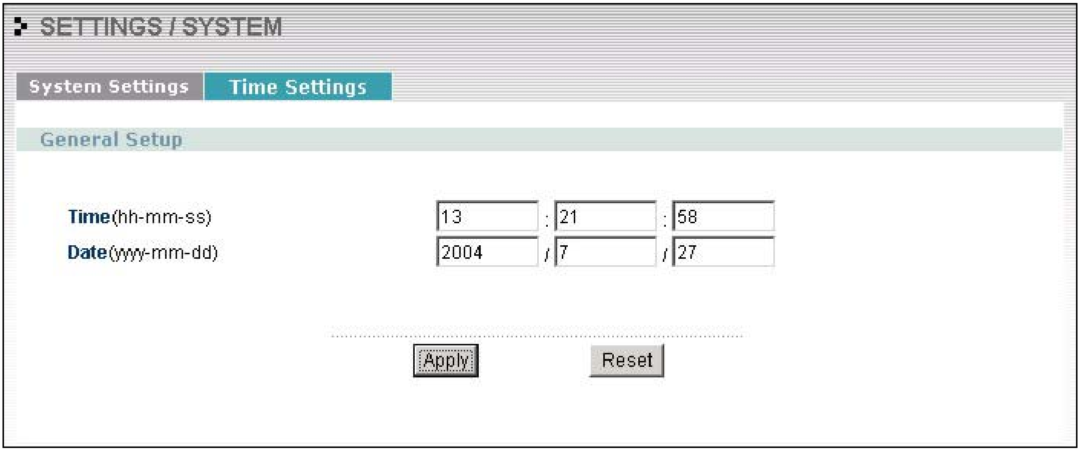
LABEL	DESCRIPTION
Device Name	This name can be up to 30 printable characters long. Spaces are allowed.
IP Address Assignment	
Obtain IP Address Automatically	Select this option to have your G-560 use a dynamically assigned IP address from a router each time. **You must know the IP address assigned to the G-560 (by the router) to access the G-560 again.**
Use fixed IP address	Select this option to have your G-560 use a static IP address. When you select this option, fill in the fields below.

Table 5-2 System Settings

LABEL	DESCRIPTION
IP Address	Enter the IP address of your G-560 in dotted decimal notation. **If you change the G-560's IP address, you must use the new IP address if you want to access the web configurator again.**
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the G-560. The gateway helps forward packets to their destinations. Leave this field as **0.0.0.0** if you do not know it.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.4 Time Settings

To change your G-560's time and date, click **SETTINGS**, **SYSTEM** and then the **Time Settings** tab. The screen appears as shown. Use this screen to manually enter a time and date. Log times and dates are based on the time and date you configure here.



SETTINGS / SYSTEM

General Setup

Time(hh-mm-ss) 13 : 21 : 58

Date(yyyy-mm-dd) 2004 / 7 / 27

Figure 5-2 Time Settings

The following table describes the labels in this screen.

Table 5-3 Time Settings

LABEL	DESCRIPTION
Time (hh-mm-ss)	This field displays the time of your G-560 in hour-minute-second format. Enter the new time in this field and then click **Apply**.
Date (yyyy-mm-dd)	This field displays the date of your G-560 in year-month-day format. Enter the new date in this field and then click **Apply**.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to reload the previous configuration for this screen.

Chapter 6 Wireless Screens

This chapter discusses how to configure wireless settings and wireless security on your G-560.

6.1 Wireless LAN Overview

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

6.1.1 IBSS

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

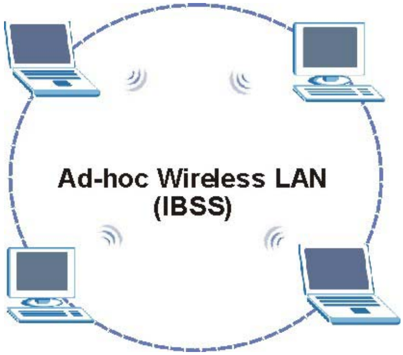


Figure 6-1 IBSS (Ad-hoc) Wireless LAN

6.1.2 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.

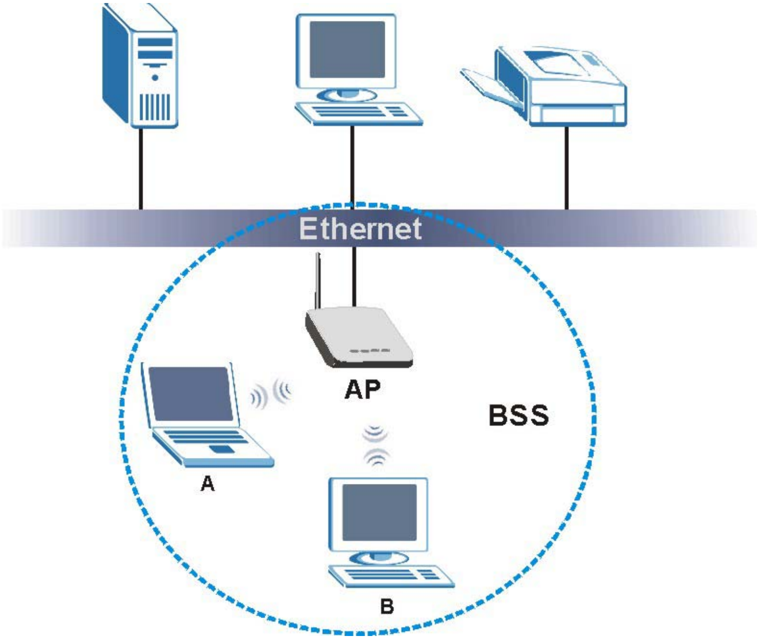


Figure 6-2 Basic Service set

6.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

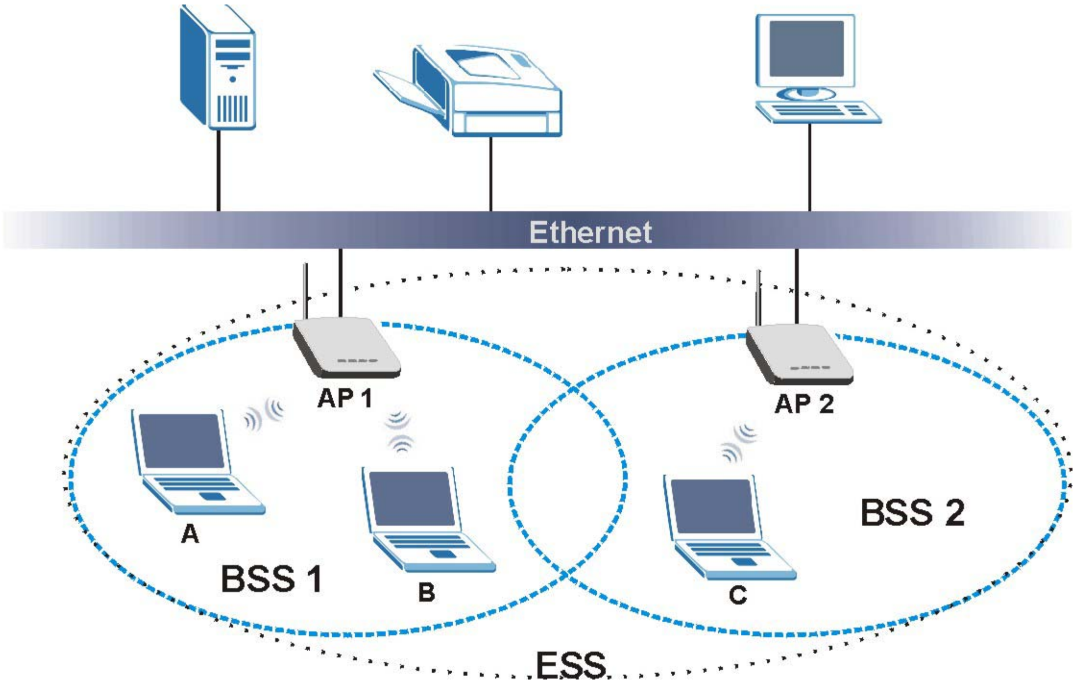


Figure 6-3 Extended Service Set

6.2 Wireless LAN Basics

This section describes the wireless LAN network terms.

6.2.1 Channel

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

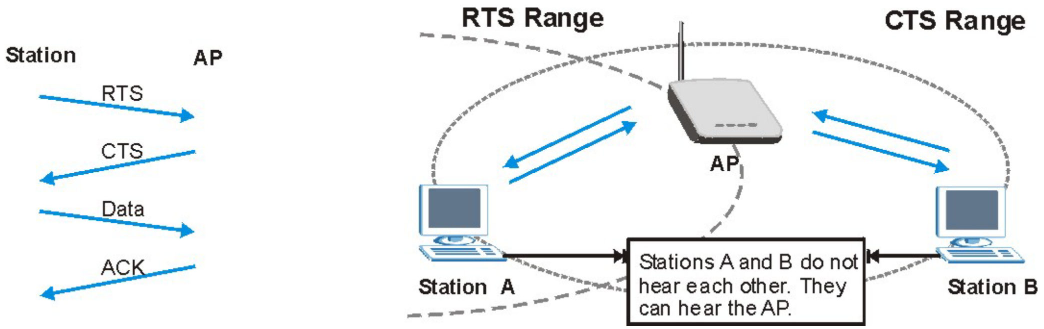
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel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

6.2.2 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

6.2.3 RTS/CTS

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



Stations A and B do not hear each other. They can hear the AP.

Figure 6-4 RTS/CTS

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

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

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

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

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

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

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

6.2.4 Fragmentation Threshold

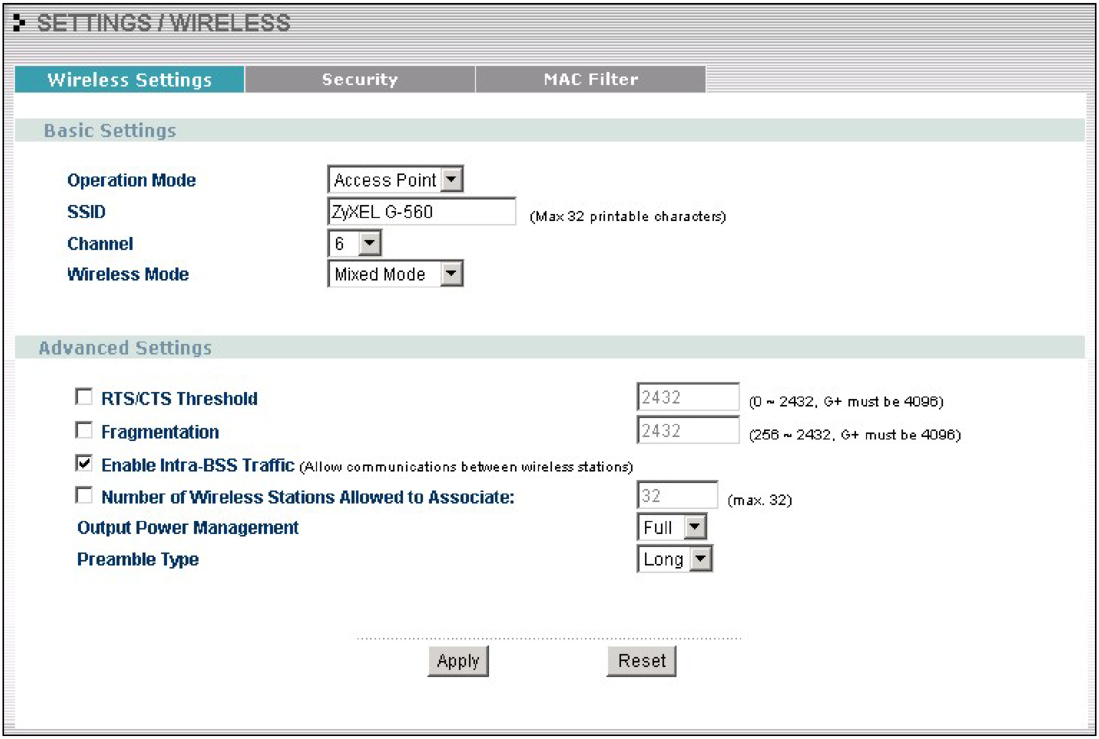
A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the G-560 will fragment the packet into smaller data frames.

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

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

6.3 Configuring Wireless

Click **SETTINGS** and **WIRELESS** to display the **Wireless Settings** screen.



Basic Settings

Operation Mode: Access Point
SSID: ZyXEL G-560 (Max 32 printable characters)
Channel: 6
Wireless Mode: Mixed Mode

Advanced Settings

□ RTS/CTS Threshold: 2432 (0 ~ 2432, G+ must be 4096)
□ Fragmentation: 2432 (256 ~ 2432, G+ must be 4096)
☑ Enable Intra-BSS Traffic (Allow communications between wireless stations)
□ Number of Wireless Stations Allowed to Associate: 32 (max. 32)
Output Power Management: Full
Preamble Type: Long

Figure 6-5 Wireless Settings

The following table describes the labels in this screen.

Table 6-1 Wireless Settings

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select **Access Point** from the drop-down list. At the time of writing, the G-560 can only work as an access point.
SSID	Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable characters) for the wireless LAN. Spaces are allowed. **If you are configuring the G-560 from a computer connected to the wireless LAN and you change the G-560's SSID, channel or security 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-560's new settings.**
Channel	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the chapter on wizard setup for more information about channels.
Wireless Mode	Select **Pure B Mode** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-560. Select **Pure G Mode** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-560. Select **Mixed Mode** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the G-560. The transmission rate of your G-560 might be reduced. Select **G+** to allow any ZyXEL WLAN devices that support this feature to associate with the G-560. This permits the G-560 to transmit at a higher speed than the pure G mode. Select **B+** to allow any ZyXEL WLAN devices that support this feature to associate with the G-560. This permits the G-560 to transmit at a higher speed than the pure B mode.
Advanced Settings	
RTS/CTS Threshold	Enter a value between 0 and 2432. The default is **2432**. You must enter 4096 if you select **G+** in the **Wireless Mode** field.
Fragmentation Threshold	Enter a value between 256 and 2432. The default is **2432**. It is the maximum data fragment size that can be sent. You must enter 4096 if you select **G+** in the **Wireless Mode** field.

Table 6-1 Wireless Settings

LABEL	DESCRIPTION
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Select this check box to enable Intra-BSS traffic.
Number of Wireless Stations Allowed to Associate:	Use this field to set a maximum number of wireless stations that may connect to the G-560. Enter the number (from 1 to 32) of wireless stations allowed.
Output Power Management	Set the output power of the G-560 in this field. If there is a high density of APs within an area, decrease the output power of the G-560 to reduce interference with other APs. The options are **Full**, **50%**, **25%** and **12%**.
Preamble Type	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble. Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications. **The G-560 and the wireless stations MUST use the same preamble mode in order to communicate.**
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4 Wireless Security Overview

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

The figure below shows the possible wireless security levels on your G-560. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

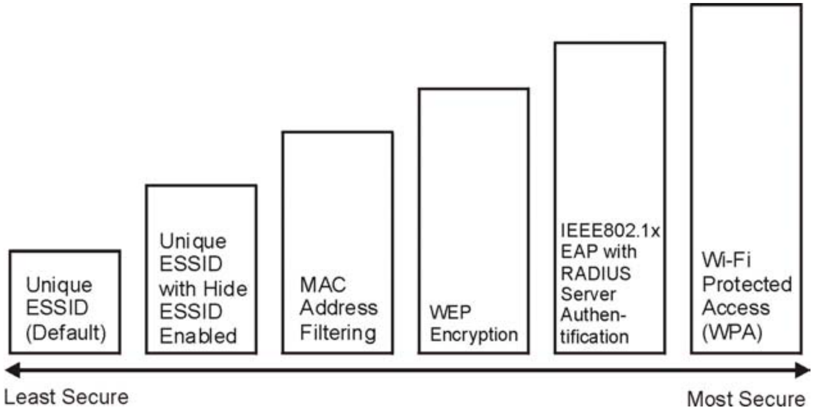


Figure 6-6 G-560 Wireless Security Levels

If you do not enable any wireless security on your G-560, your network is accessible to any wireless networking device that is within range.

6.5 WEP Overview

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

6.5.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your G-560 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys, but only one key can be used at any one time.

6.5.2 Authentication

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

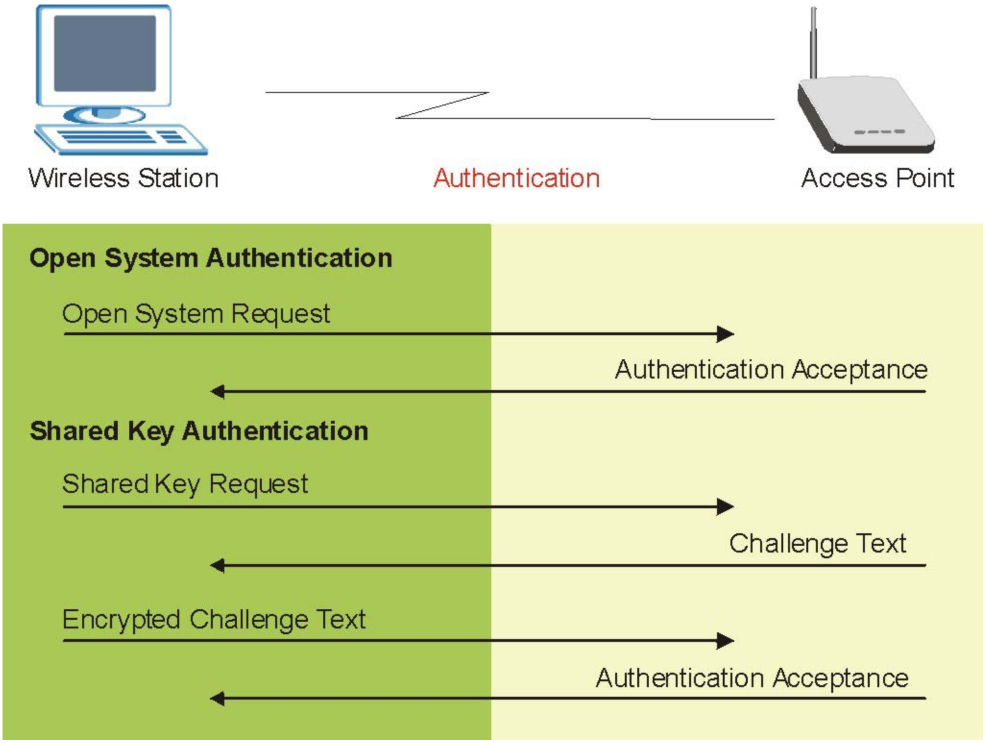


Figure 6-7 WEP Authentication Steps

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-560'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-560 will accept either type of authentication request and the G-560 will fall back to use open authentication if the shared key does not match.

6.6 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server for an unlimited number of users.

6.7 Introduction to RADIUS

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

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your G-560 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 wired network from unauthorized access.

6.7.1 EAP Authentication Overview

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

The type of authentication you use depends on the RADIUS server or the AP. The G-560 supports EAP-TLS, EAP-TTLS and PEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the common types.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

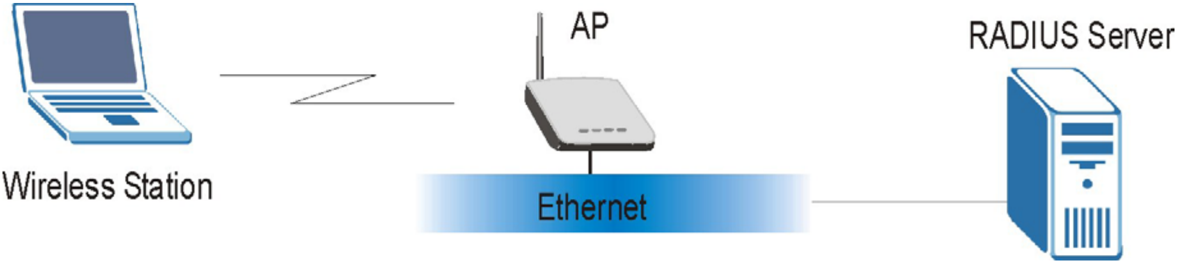


Figure 6-8 EAP Authentication

The details below provide a general description of how IEEE 802.1x EAP authentication works.

- The wireless station sends a "start" message to the G-560.
- The G-560 sends a "request identity" message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

6.8 Dynamic WEP Key Exchange

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

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

To use Dynamic WEP, enable and configure Dynamic WEP Key Exchange in the **Wireless Security 802.1x** screen (see *section 6.14.5*). Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

6.9 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

6.9.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the G-560's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA -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 client will be granted access to a WLAN.

6.9.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

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

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

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

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

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

6.10 WPA-PSK Application Example

A WPA-PSK application looks as follows.

Step 1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

Step 2. The AP checks each client's password and (only) allows it to join the network if it matches its password.

Step 3. The AP derives and distributes keys to the wireless clients.

Step 4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

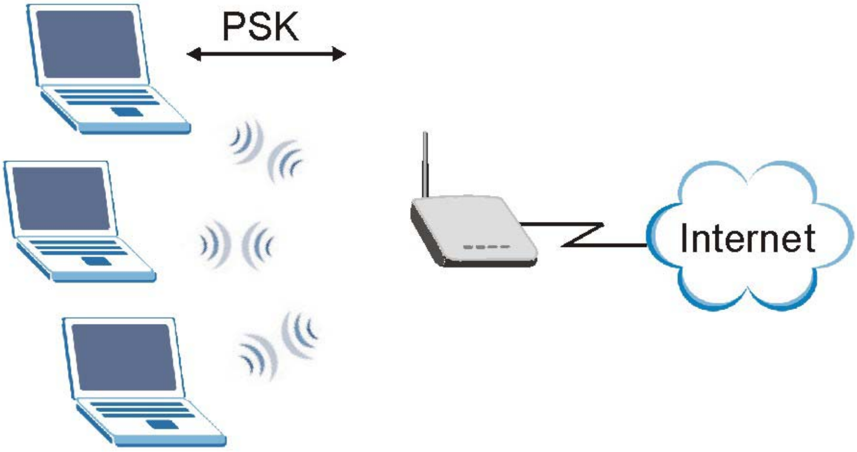


Figure 6-9 WPA-PSK Authentication

6.11 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.

Step 1. The AP passes the wireless client's authentication request to the RADIUS server.

Step 2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

Step 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.

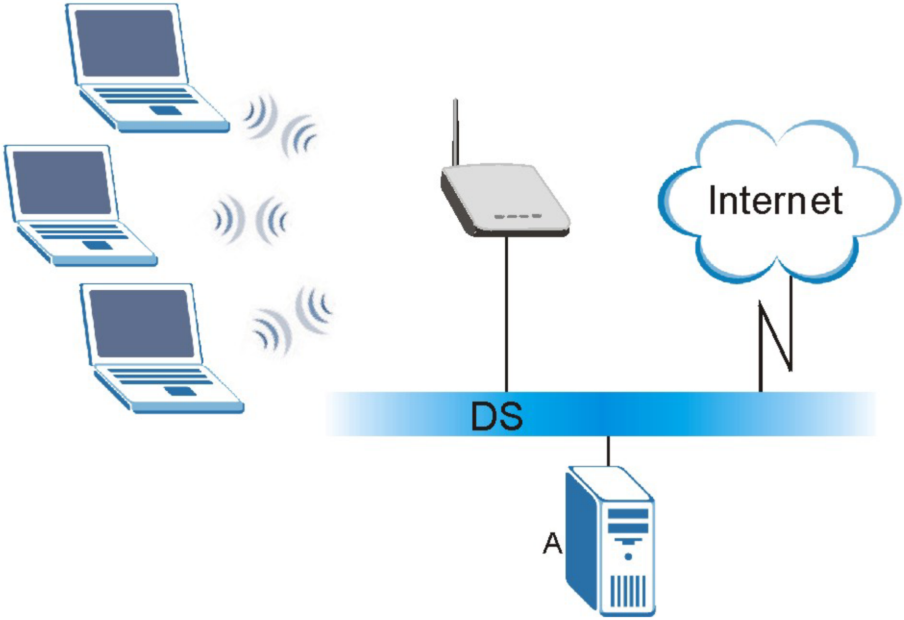


Figure 6-10 WPA with RADIUS Application Example

6.12 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 6-2 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
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	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

6.13 Wireless Client WPA Supplicants

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

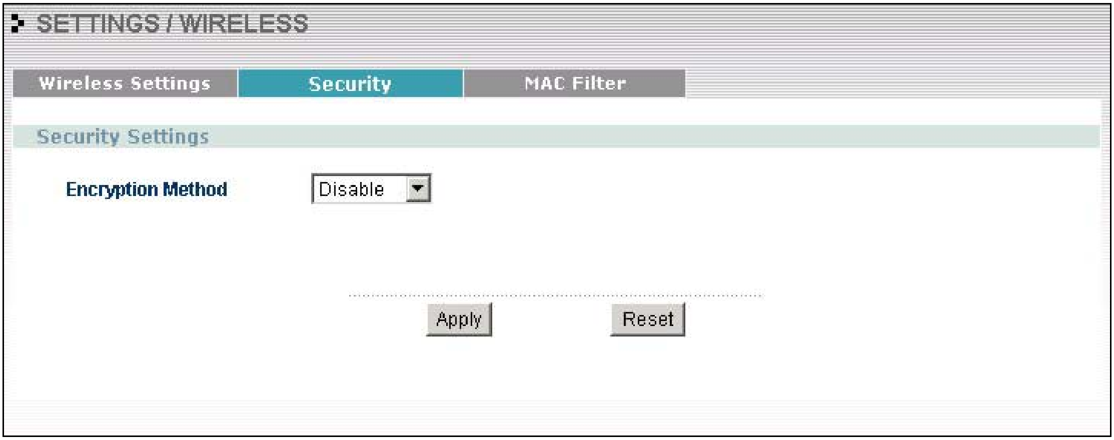
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

6.14 Configuring Wireless Security

In order to configure and enable wireless security; click the **SETTINGS**, **WIRELESS** and the **Security** tab to display the **Security** screen. This screen varies according to the encryption method you select.

6.14.1 Disable

If you do not enable any wireless security on your G-560, your network is accessible to any wireless networking device that is within range.



Encryption Method: Disable

Figure 6-11 Security: Disable

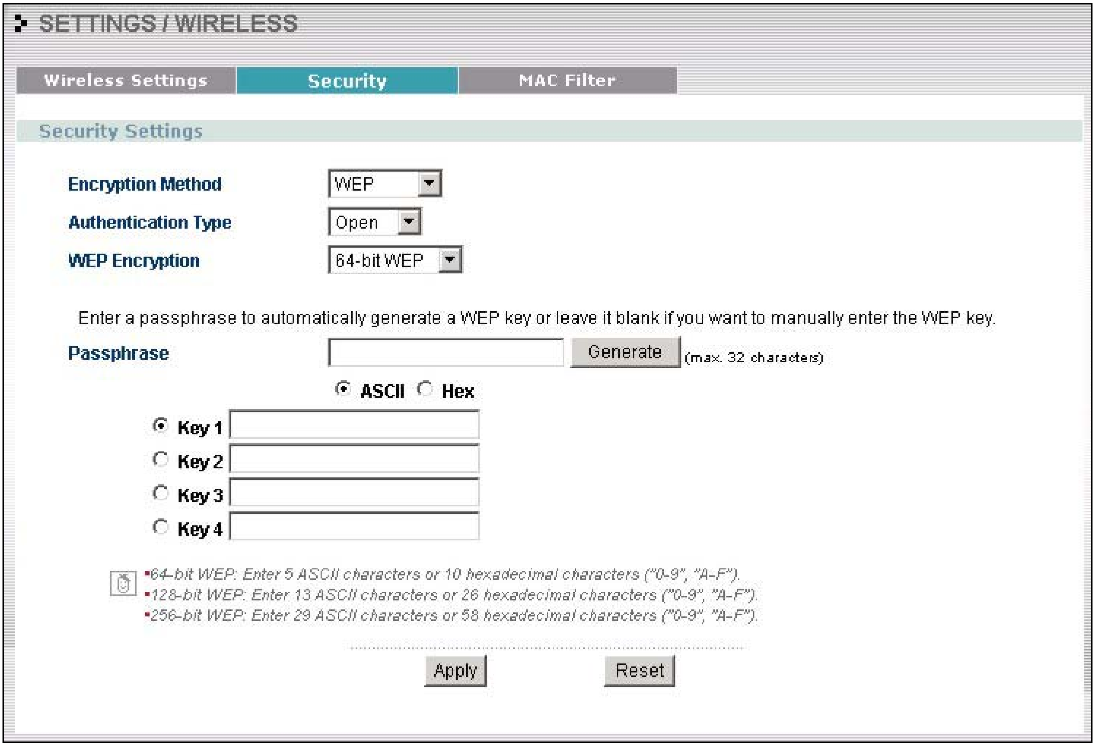
The following table describes the labels in this screen.

Table 6-3 Security: Disable

LABEL	DESCRIPTION
Encryption Method	Select **Disable** to have no wireless LAN security configured.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.14.2 WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your G-560 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys, but only one key can be used at any one time.



Security Settings

Encryption Method: WEP

Authentication Type: Open

WEP Encryption: 64-bit WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

Passphrase: Generate (max. 32 characters)

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

- 64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").
- 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
- 256-bit WEP: Enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F").

Apply Reset

Figure 6-12 Security: WEP

The following table describes the labels in this screen.

Table 6-4 Security: WEP

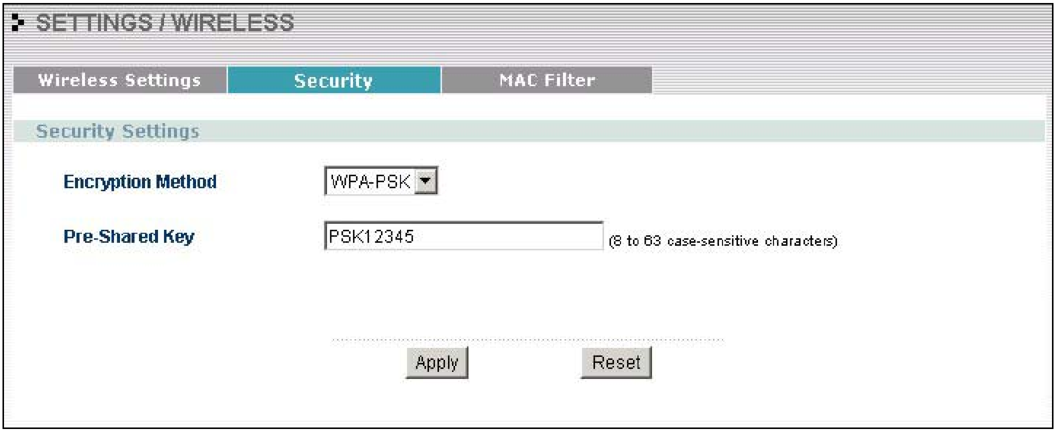
LABEL	DESCRIPTION
Encryption Method	Select **WEP** if you want to configure WEP encryption parameters.
Authentication Type	Select **Auto**, **Open** or **Shared** from the drop-down list box.
WEP Encryption	Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to enable data encryption.
Passphrase	Enter a “passphrase” (password phrase) of up to 32 case-sensitive printable characters and click **Generate** to have the G-560 create four different WEP keys.

Table 6-4 Security: WEP

LABEL	DESCRIPTION
Generate	After you enter the passphrase, click **Generate** to have the G-560 generates four different WEP keys automatically.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys.
Key 1 to Key 4	If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the G-560 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").
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.14.3 WPA-PSK

Select **WPA-PSK** in the **Encryption Method** drop down list-box to display the screen displays as next.



SETTINGS / WIRELESS

Security Settings

Encryption Method: WPA-PSK

Pre-Shared Key: PSK12345 (8 to 63 case-sensitive characters)

Figure 6-13 Security: WPA-PSK

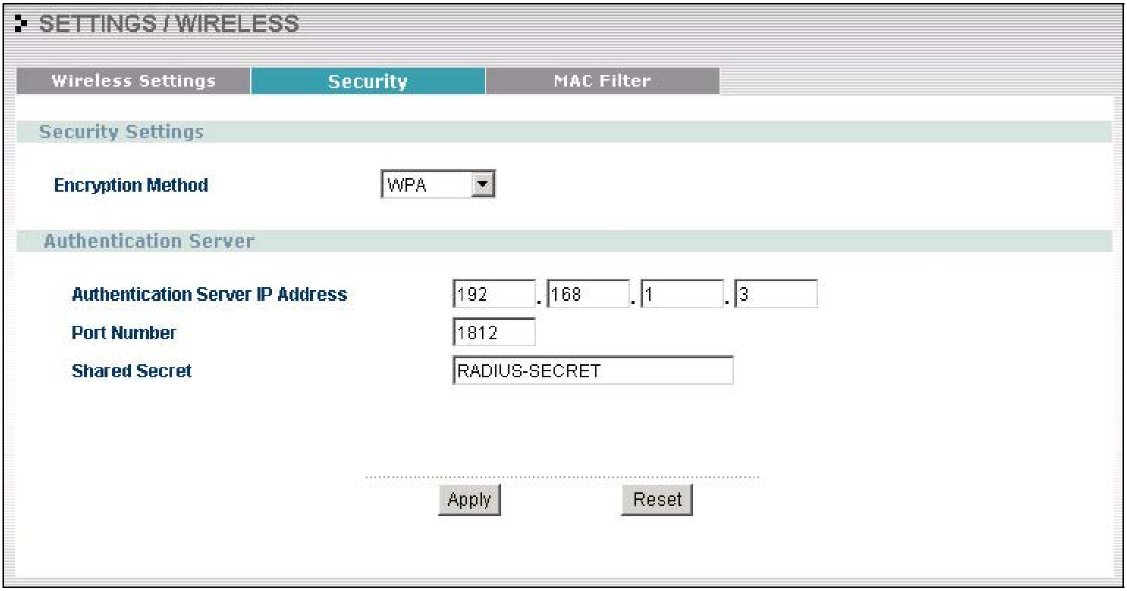
The following table describes the labels in this screen.

Table 6-5 Security: WPA-PSK

LABEL	DESCRIPTION
Encryption Method	Select **WPA-PSK** if you want to configure a pre-shared key. Choose this option only if your wireless clients support it.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.14.4 WPA

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.



Encryption Method: WPA

Authentication Server IP Address: 192 . 168 . 1 . 3

Port Number: 1812

Shared Secret: RADIUS-SECRET

Figure 6-14 Security: WPA

The following table describes the labels in this screen.

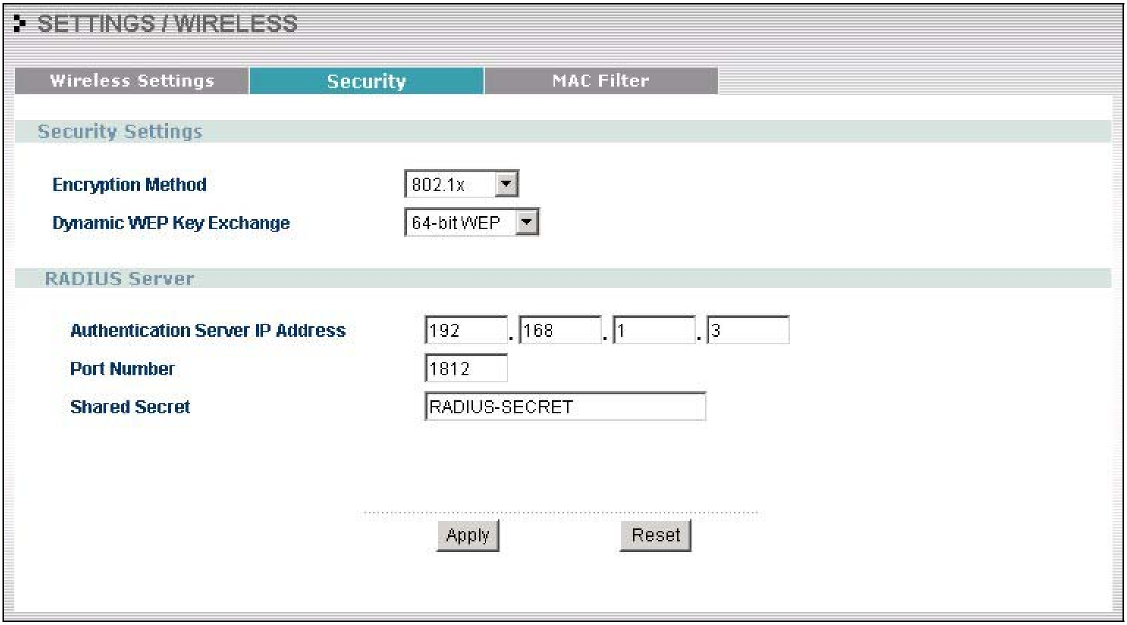
Table 6-6 Security: WPA

LABEL	DESCRIPTION
Encryption Method	Select **WPA** to configure user authentication and improved data encryption.
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 63 printable characters) as the key to be shared between the external authentication server and the G-560. The key must be the same on the external authentication server and your G-560. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.14.5 802.1x

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

Once you enable user authentication, you need to specify an external RADIUS server on the G-560 for authentication.



SETTINGS / WIRELESS

Security Settings

Encryption Method: 802.1x

Dynamic WEP Key Exchange: 64-bit WEP

RADIUS Server

Authentication Server IP Address: 192 . 168 . 1 . 3

Port Number: 1812

Shared Secret: RADIUS-SECRET

Figure 6-15 Security: 802.1x

The following table describes the labels in this screen.

Table 6-7 Security: 802.1x

LABEL	DESCRIPTION
Encryption Method	Select **802.1x** to configure authentication of wireless stations and encryption key management.
Dynamic WEP Key Exchange	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-560 when you configure dynamic WEP key exchange.
Authentication Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation

Table 6-7 Security: 802.1x

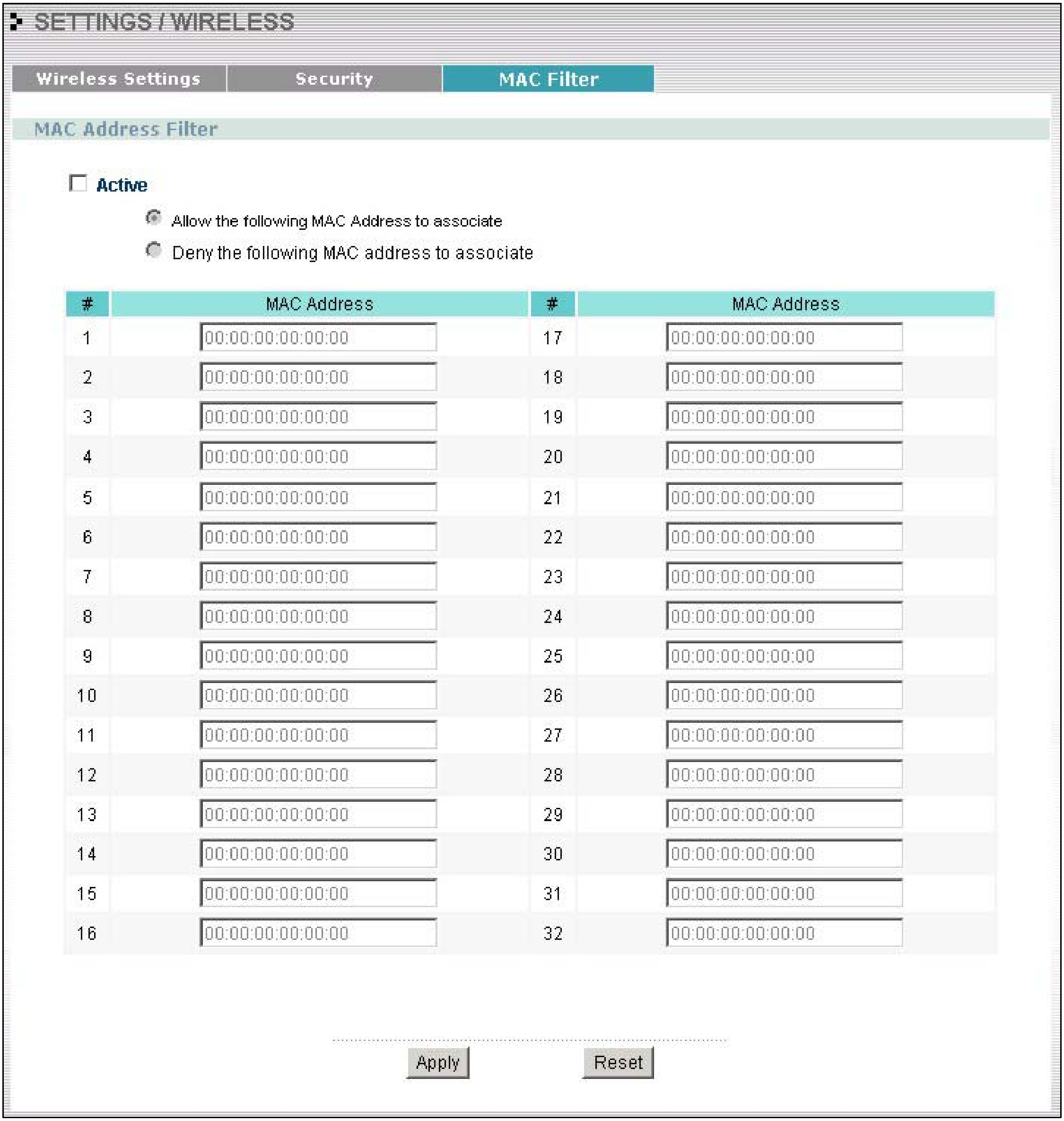
LABEL	DESCRIPTION
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 63 printable characters) as the key to be shared between the external authentication server and the G-560. The key must be the same on the external authentication server and your G-560. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15 MAC Filter

The MAC filter screen allows you to configure the G-560 to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the G-560 (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your G-560's MAC Filter settings, click the **WIRELESS** link under **SETTINGS** and then the **MAC Filter** tab. The screen appears as shown.

Be careful not to list your computer's MAC address and select Deny the following MAC address to associate **when managing the G-560 via a wireless connection. This would lock you out.**



SETTINGS / WIRELESS

MAC Address Filter

□ Active

● Allow the following MAC Address to associate

○ Deny the following MAC address to associate

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

Figure 6-16 MAC Address Filter

The following table describes the labels in this screen.

Table 6-8 MAC Address Filter

LABEL	DESCRIPTION
Active	Select the check box to enable MAC address filtering and define the filter action for the list of MAC addresses in the MAC address filter table. Select **Allow the following MAC address to associate** to permit access to the G-560, MAC addresses not listed will be denied access to the G-560. Select **Deny the following MAC address to associate** to block access to the G-560, MAC addresses not listed will be allowed to access the G-560.
#	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the G-560 in these address fields.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

Chapter 7 Management Screens

This chapter describes the Maintenance screens.

7.1 Maintenance Overview

Use these maintenance screens to change the password, view logs, back up or restore the G-560 configuration and change the web configurator language.

7.2 Configuring Password

To change your G-560's password (recommended), click **SETTINGS** and then **MANAGEMENT**. The screen appears as shown. This screen allows you to change the G-560's password.

If you forget your password (or the G-560 IP address), you will need to reset the G-560. See the section on resetting the G-560 for details.

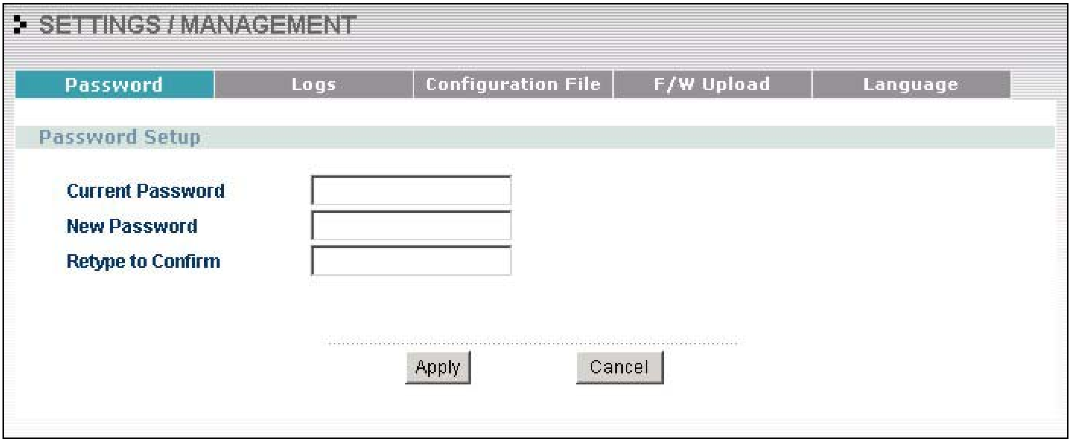


Figure 7-1 Password

The following table describes the labels in this screen.

Table 7-1 Password

LABEL	DESCRIPTION
Current Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 30 printable characters). Spaces are not allowed. Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to reload the previous configuration for this screen.

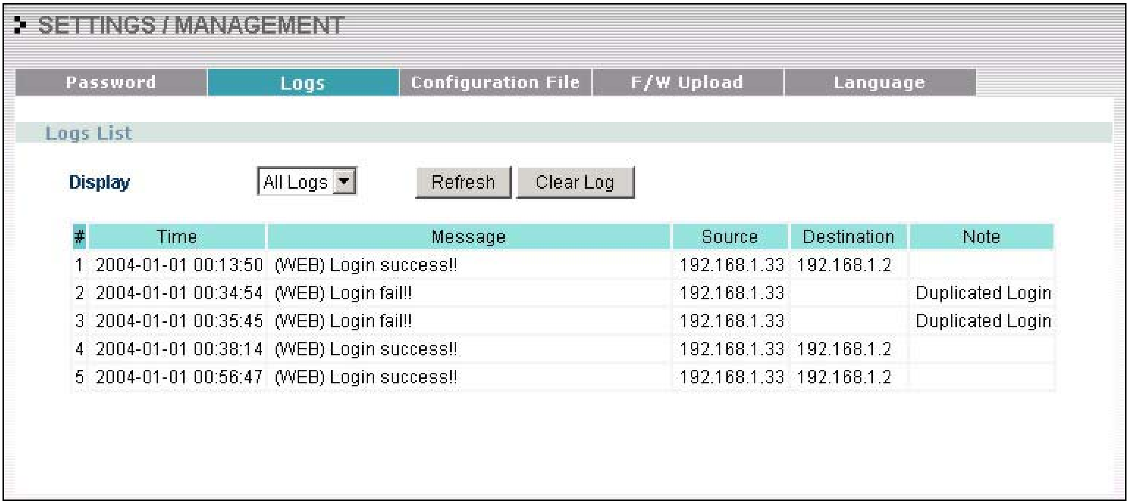
7.3 Logs

The web configurator allows you to look at all of the G-560's logs in one location.

Click **SETTINGS**, **MANAGEMENT** and then the **Logs** tab to open the **Logs** screen.

You can view logs and alert messages in this page. Once the log table is full, old logs are deleted as new logs are created.

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



#	Time	Message	Source	Destination	Note
1	2004-01-01 00:13:50	(WEB) Login success!!	192.168.1.33	192.168.1.2	
2	2004-01-01 00:34:54	(WEB) Login fail!!	192.168.1.33		Duplicated Login
3	2004-01-01 00:35:45	(WEB) Login fail!!	192.168.1.33		Duplicated Login
4	2004-01-01 00:38:14	(WEB) Login success!!	192.168.1.33	192.168.1.2	
5	2004-01-01 00:56:47	(WEB) Login success!!	192.168.1.33	192.168.1.2	

Figure 7-2 Logs

The following table describes the labels in this screen.

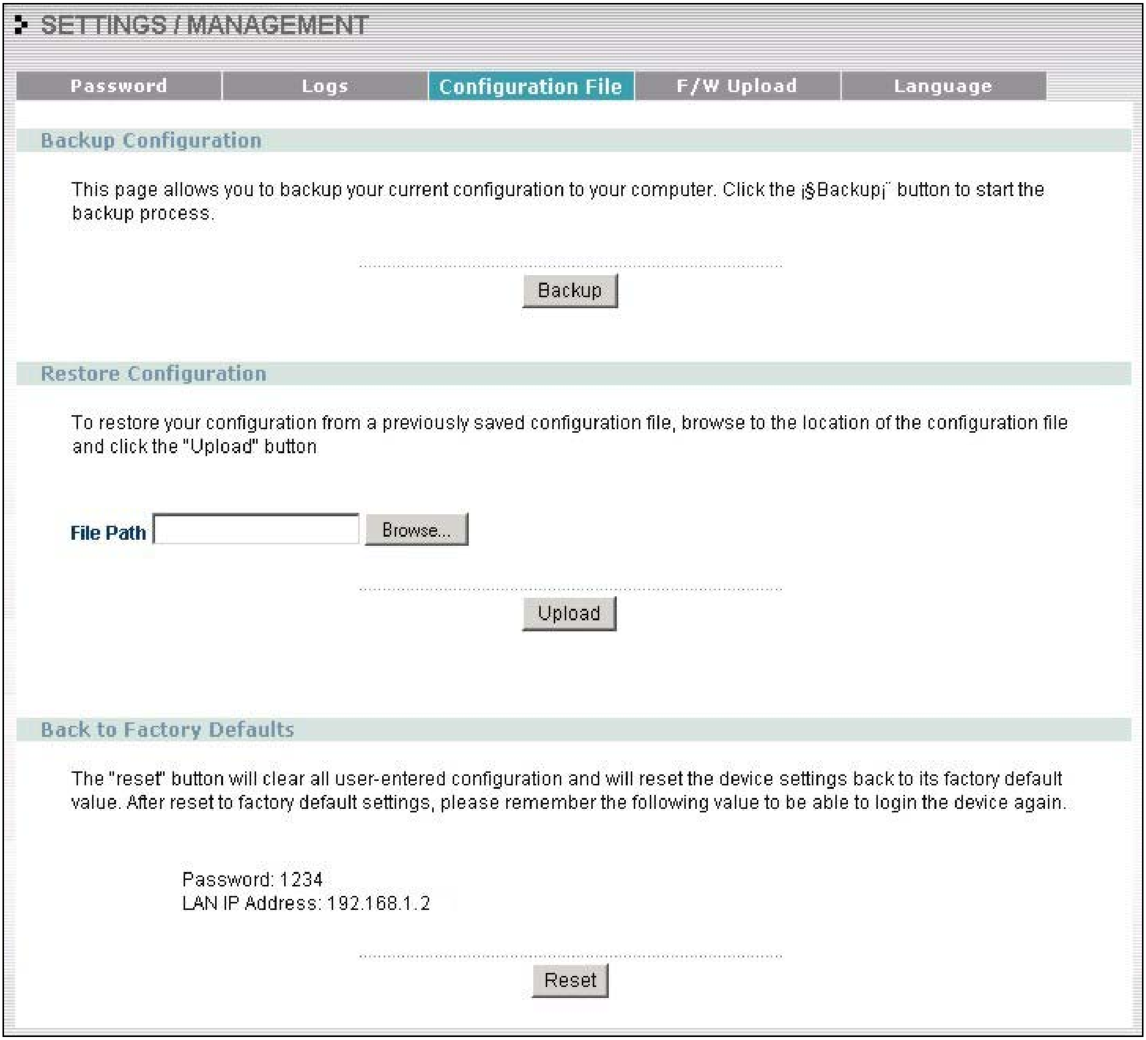
Table 7-2 Logs

LABEL	DESCRIPTION
Display	Select a category of logs to view.
#	This is the log’s index number.
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 that caused the log.
Destination	This field lists the destination IP address and the port number of the outgoing packet that caused the log.
Note	This field displays additional information about the log entry.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

7.4 Configuration Screen

The configuration file (often called the romfile or rom-0) contains the factory default settings such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a .rom filename extension. Once you have customized the G-560's settings, they can be saved back to your computer under a filename of your choosing.

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



Backup Configuration

This page allows you to backup your current configuration to your computer. Click the ¡§Backup¡¨ button to start the backup process.

Restore Configuration

To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "Upload" button

File Path

Back to Factory Defaults

The "reset" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again.

Password: 1234
LAN IP Address: 192.168.1.2

Figure 7-3 Configuration File

7.4.1 Backup Configuration

Backup configuration allows you to back up (save) the G-560's current configuration to a file on your computer. Once your G-560 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-560's current configuration to your computer.

7.4.2 Restore Configuration

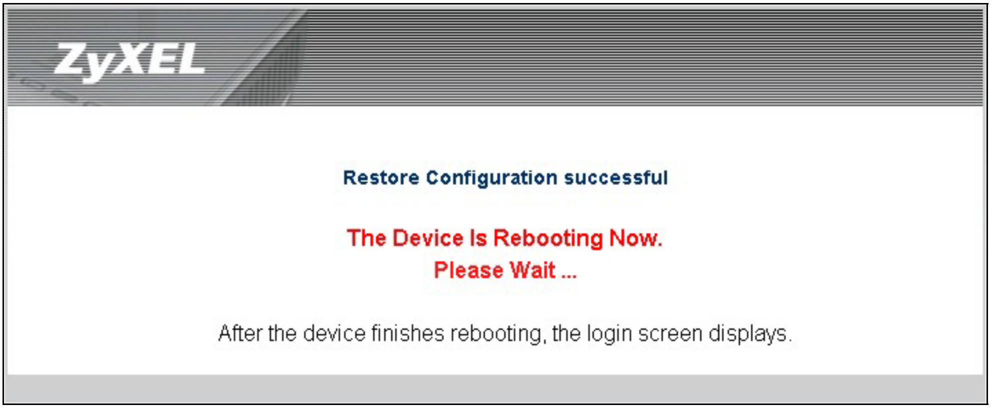
Restore configuration allows you to upload a new or previously saved configuration file from your computer to your G-560.

Table 7-3 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.

Do not turn off the G-560 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-560 again.



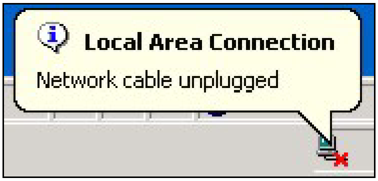
Restore Configuration successful

The Device Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

Figure 7-4 Configuration Upload Successful

The G-560 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



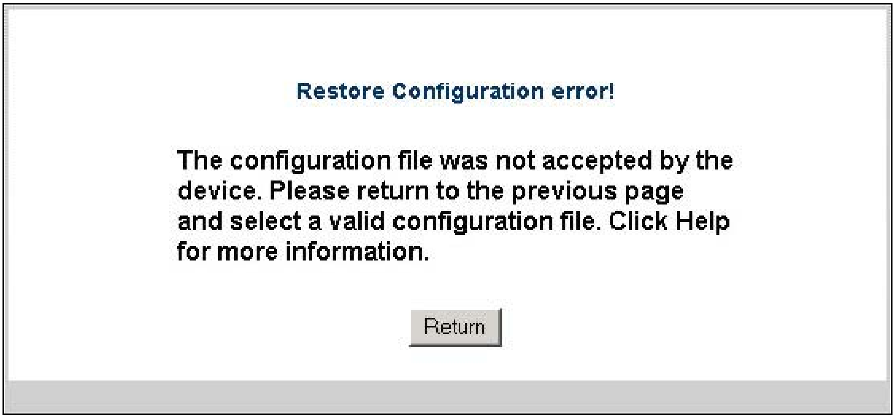
Local Area Connection

Network cable unplugged

Figure 7-5 Network Temporarily Disconnected

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-560 IP address (192.168.1.2).

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



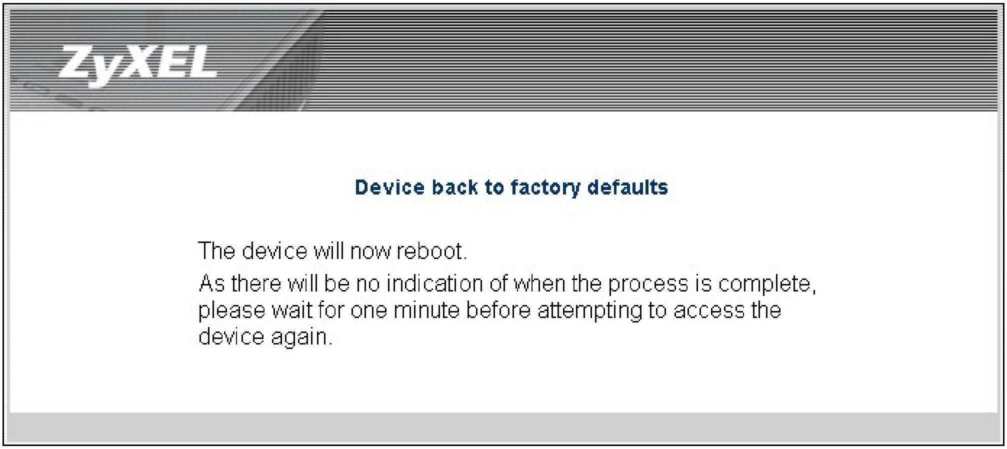
Restore Configuration error!

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.

Figure 7-6 Configuration Upload Error

7.4.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the G-560 to its factory defaults as shown on the screen. The following warning screen will appear.



Device back to factory defaults

The device will now reboot.

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

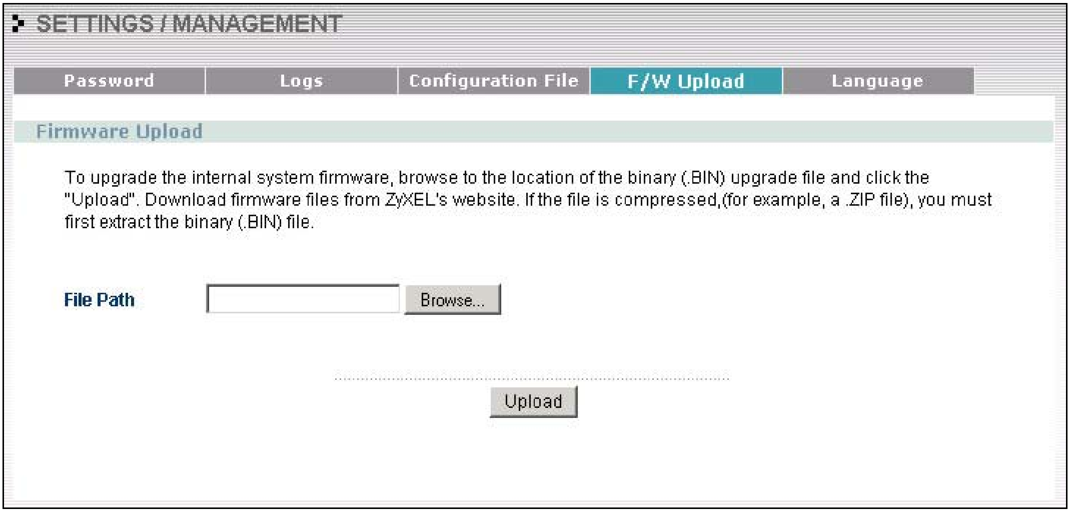
Figure 7-7 Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your G-560. Refer to the section on resetting the G-560 for more information on the **RESET** button.

7.5 F/W Upload Screen

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

Click **SETTINGS**, **MANAGEMENT** and then the **F/W Upload** tab to display the screen as shown. Follow the instructions in this screen to upload firmware to your G-560.



SETTINGS / MANAGEMENT

Firmware Upload

To upgrade the internal system firmware, browse to the location of the binary (.BIN) upgrade file and click the "Upload". Download firmware files from ZyXEL's website. If the file is compressed,(for example, a .ZIP file), you must first extract the binary (.BIN) file.

File Path

Figure 7-8 Firmware Upload

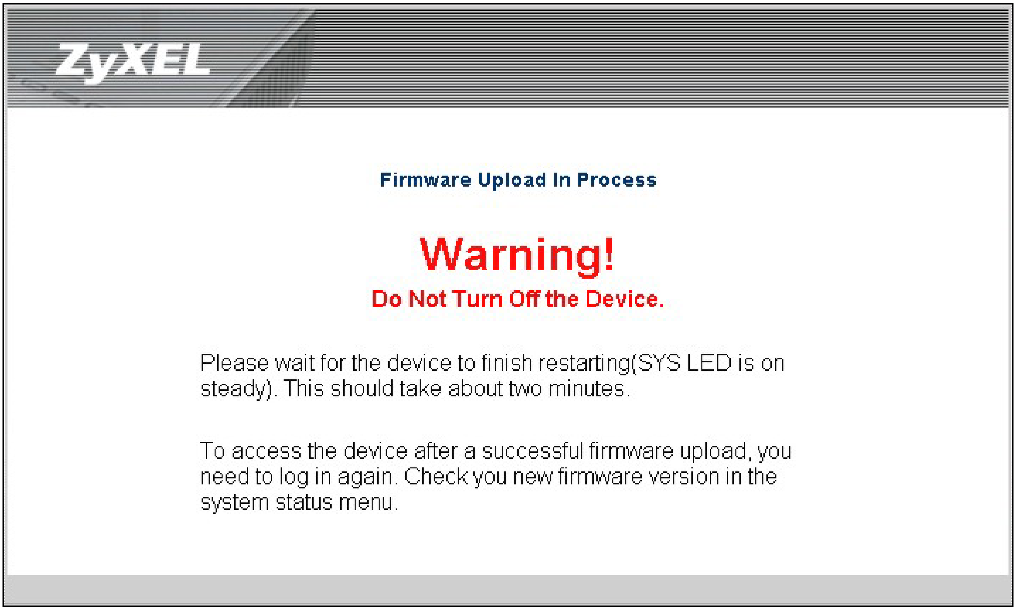
The following table describes the labels in this screen.

Table 7-4 Firmware Upload

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

Do not turn off the G-560 while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the G-560 again.



Firmware Upload In Process

Warning!

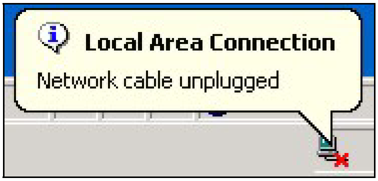
Do Not Turn Off the Device.

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

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

Figure 7-9 Firmware Upload In Process

The G-560 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



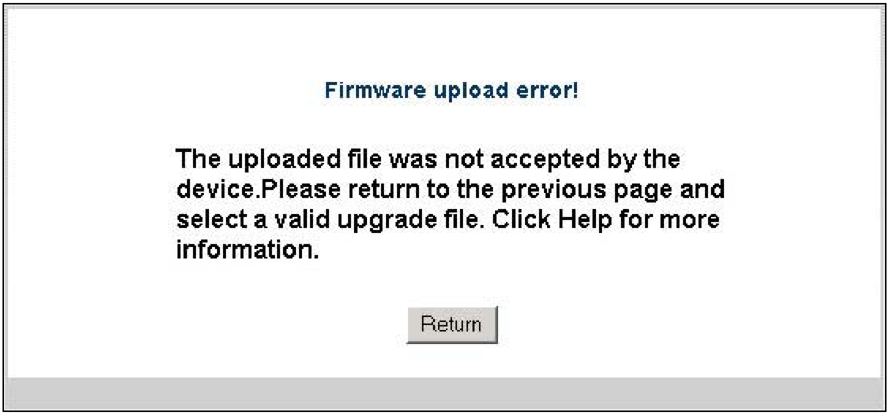
Local Area Connection

Network cable unplugged

Figure 7-10 Network Temporarily Disconnected

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

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



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.

Figure 7-11 Firmware Upload Error

7.6 Language Screen

If you want to view the web configurator and corresponding web help in another language, click **SETTINGS**, **MANAGEMENT** and then **Language**. Click the language you need.

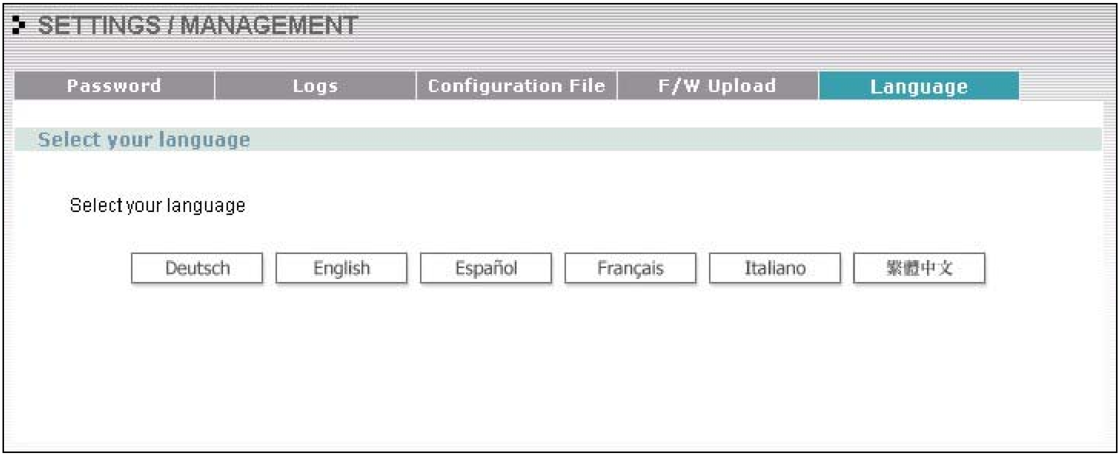


Figure 7-12 Language

Part III:

APPENDICES

This part provides troubleshooting and background information about setting up your computer's IP address, wireless LAN, 802.1x and IP subnetting. It also provides information on the command interpreter interface and logs.

Appendix A Troubleshooting

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

Problems Starting Up the G-560

Chart A-1 Troubleshooting the Start-Up of Your G-560

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The G-560 reboots automatically sometimes.	The supplied power to the G-560 is too low. Check that the G-560 is receiving enough power. Make sure the power source is working properly.

Problems with the Ethernet Interface

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the G-560 from the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connection between your G-560 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-560, the Ethernet device and your computer are on the same subnet.

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot ping any computer on the LAN.	If the **ETHN** LED on the front panel is off, check the Ethernet cable connections between your G-560 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-560, the Ethernet device and the LAN computers are on the same subnet.

Problems with the Password

Chart A-3 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the G-560.	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 rear panel of the G-560 to restore the factory default configuration file (hold this button in for about 10 seconds or release the button when the **PWR** LED starts blinking). This will restore all of the factory defaults including the password.

Problems with Telnet

Chart A-4 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the G-560 through Telnet.	Refer to the *Problems with the Ethernet Interface* section for instructions on checking your Ethernet connection.

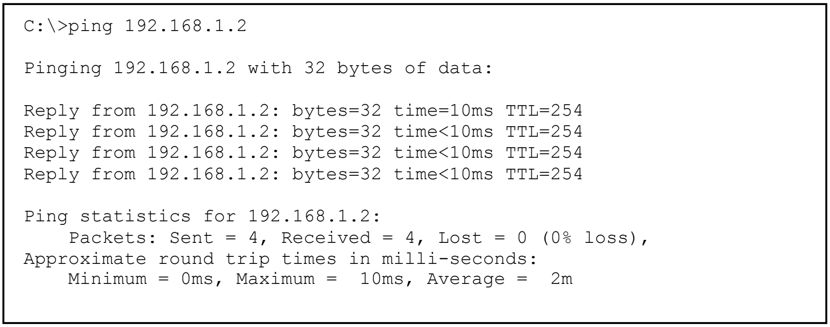
Problems with the WLAN Interface

Chart A-5 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the G-560 from the WLAN.	Make sure the wireless adapter on the wireless station is working properly. Check that both the G-560 and your wireless station are using the same ESSID, channel and security settings.
I cannot ping any computer on the WLAN.	Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the G-560 and wireless station(s) are using the same ESSID, channel and security settings.

Testing the Connection to the G-560

1. Click **Start**, (**All**) **Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ping" followed by a space and the IP address of the G-560 (192.168.1.2 is the default).
3. Press **ENTER**. The following screen displays.



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2m
```

Diagram A-1 Pinging the G-650

Your computer can now communicate with the G-560 via the **ETHERNET** port.

Appendix B
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.

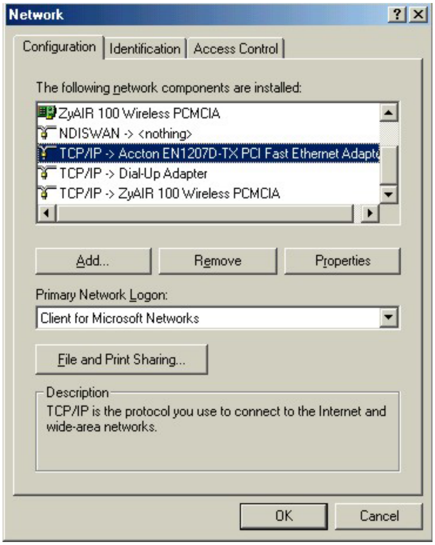
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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-560's LAN port.

Windows 95/98/Me

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



The following network components are installed:

- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

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

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

If you need the adapter:

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

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

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

If you need TCP/IP:

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

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

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

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

If you need Client for Microsoft Networks:

a. Click **Add**.

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

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

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

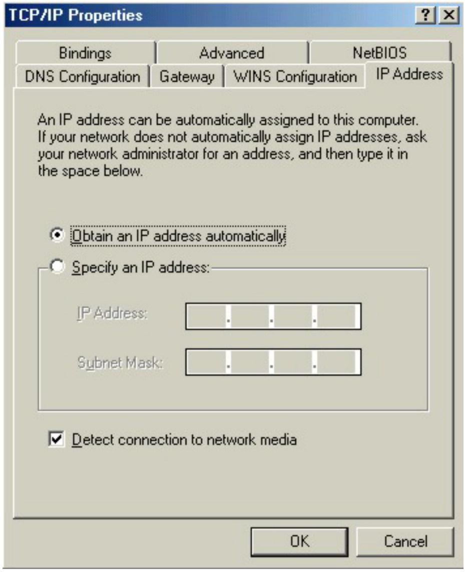
e. Restart your computer so the changes you made take effect.

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

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

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

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



TCP/IP Properties

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

● Obtain an IP address automatically

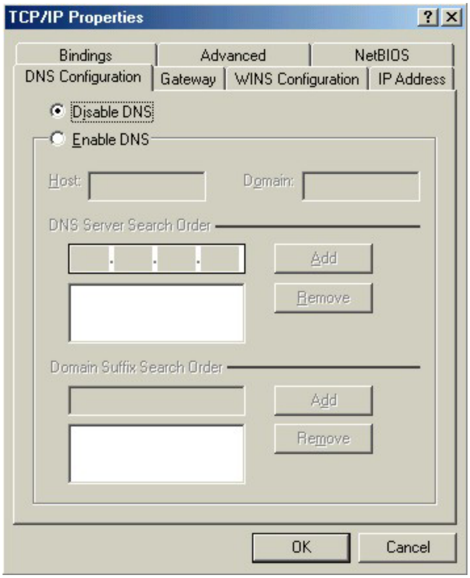
○ Specify an IP address:

☑ Detect connection to network media

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

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

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



TCP/IP Properties

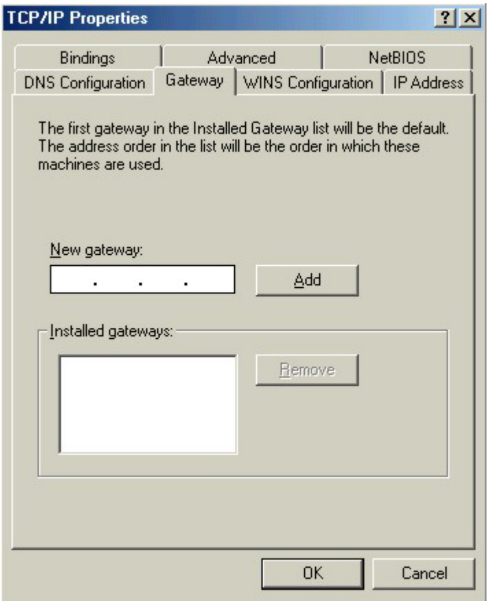
● Disable DNS

○ Enable DNS

3. Click the **Gateway** tab.

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

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



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

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

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

6. Turn on your G-560 and restart your computer when prompted.

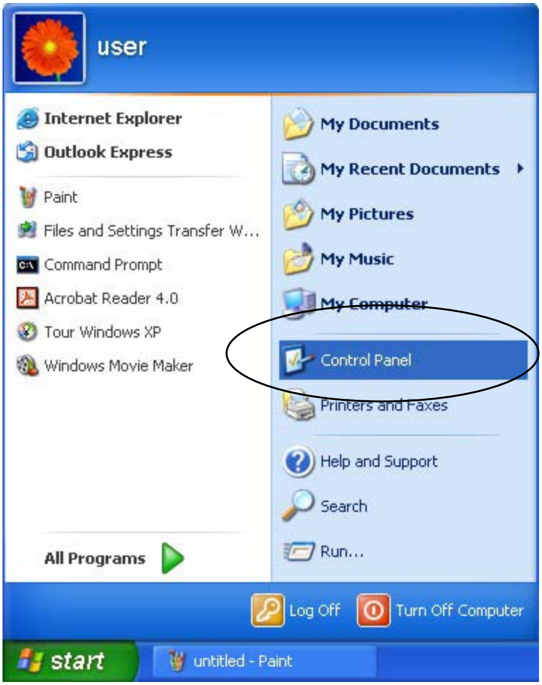
Verifying Your Computer's IP Address

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

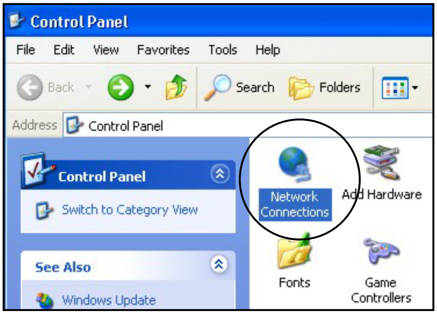
Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

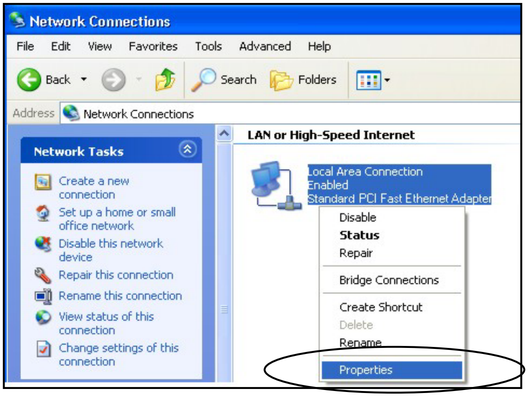
1. Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.



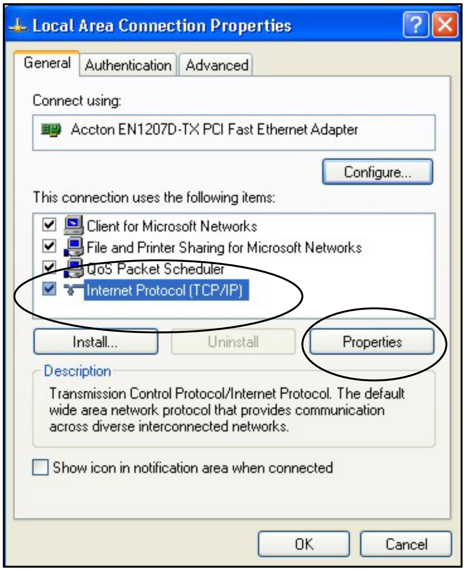
2. In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).



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



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



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

Configure...

This connection uses the following items:

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

Install... | Uninstall | Properties

Description

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

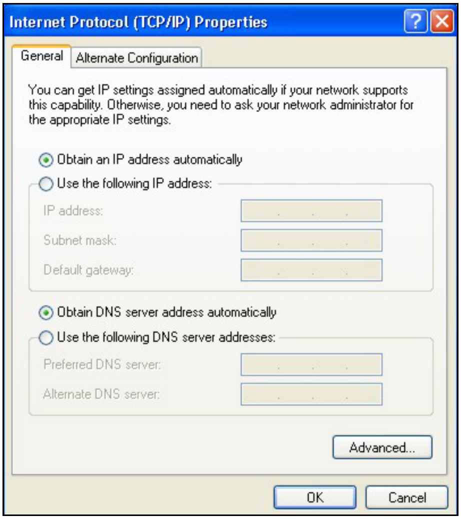
OK | Cancel

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**.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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: . . .

Advanced...

OK | Cancel

6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setti**ngs 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.

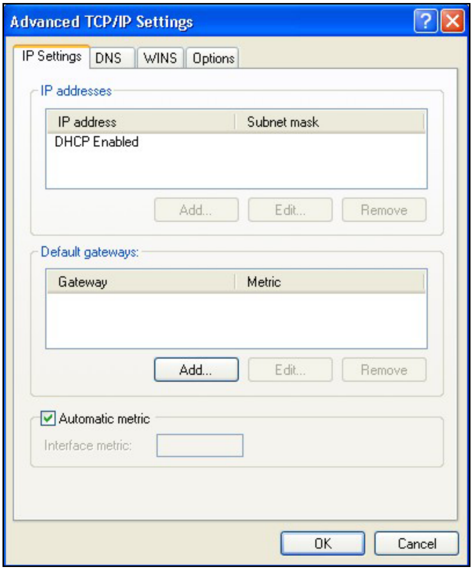
   -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

   -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.



Advanced TCP/IP Settings

IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

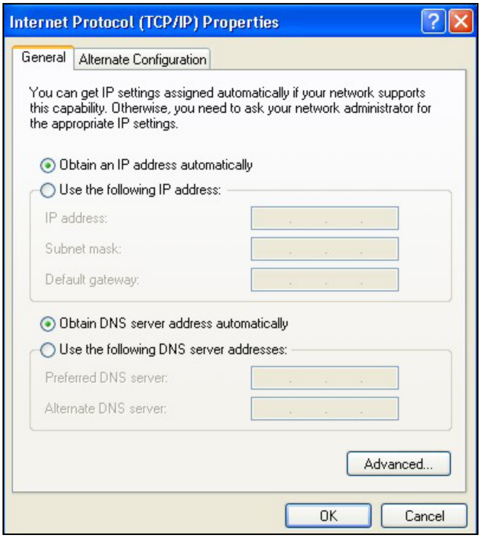
Interface metric:

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.



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 **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10. Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11. Turn on your G-560 and restart your computer (if prompted).

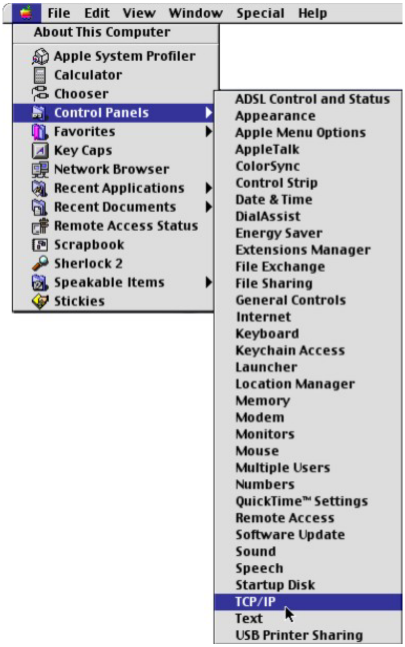
Verifying Your Computer's IP Address

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

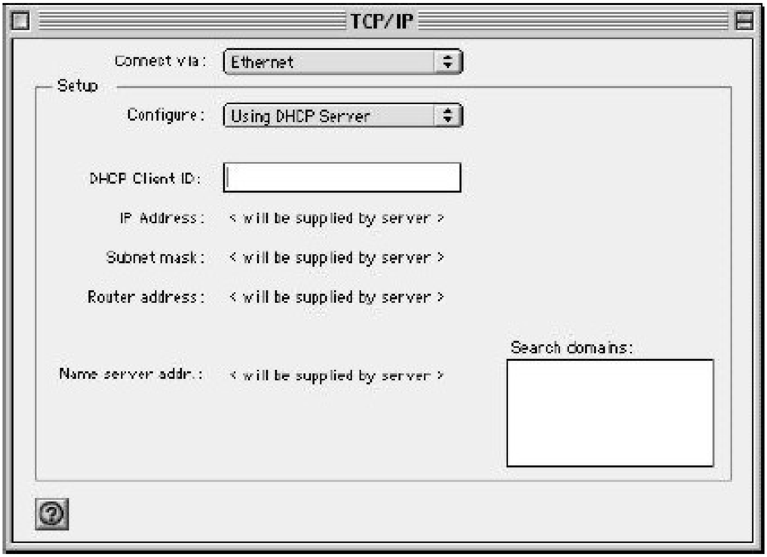
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

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-560 in the **Router address** box.

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

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

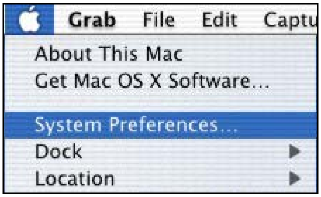
7. Turn on your G-560 and restart your computer (if prompted).

Verifying Your Computer's IP Address

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

Macintosh OS X

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

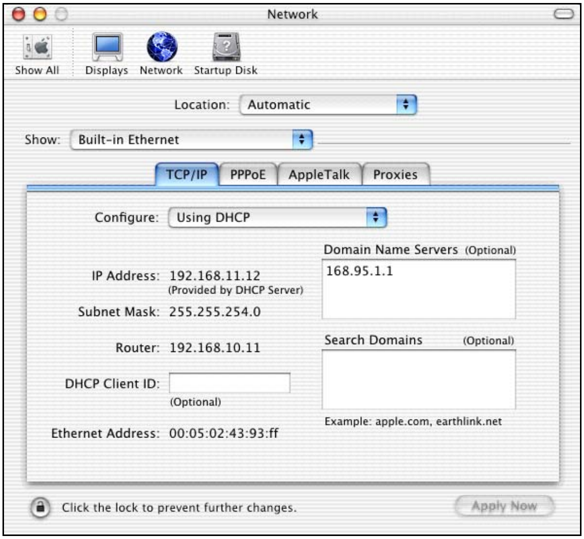


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

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

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

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

4. For statically assigned settings, do the following:

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

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

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

   -Type the IP address of your G-560 in the **Router address** box.

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

6. Turn on your G-560 and restart your computer (if prompted).

Verifying Your Computer’s IP Address

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

Appendix C
Wireless LAN and IEEE 802.11

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

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

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

IEEE 802.11

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

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

Ad-hoc Wireless LAN Configuration

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

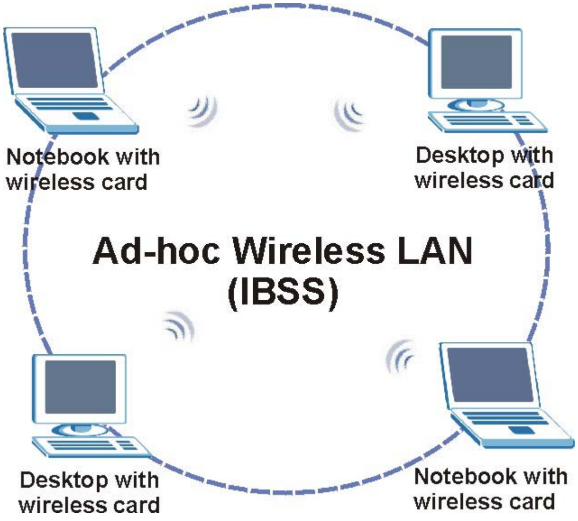

Notebook with wireless card
Desktop with wireless card
Ad-hoc Wireless LAN (IBSS)
Desktop with wireless card
Notebook with wireless card

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

Infrastructure Wireless LAN Configuration

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

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

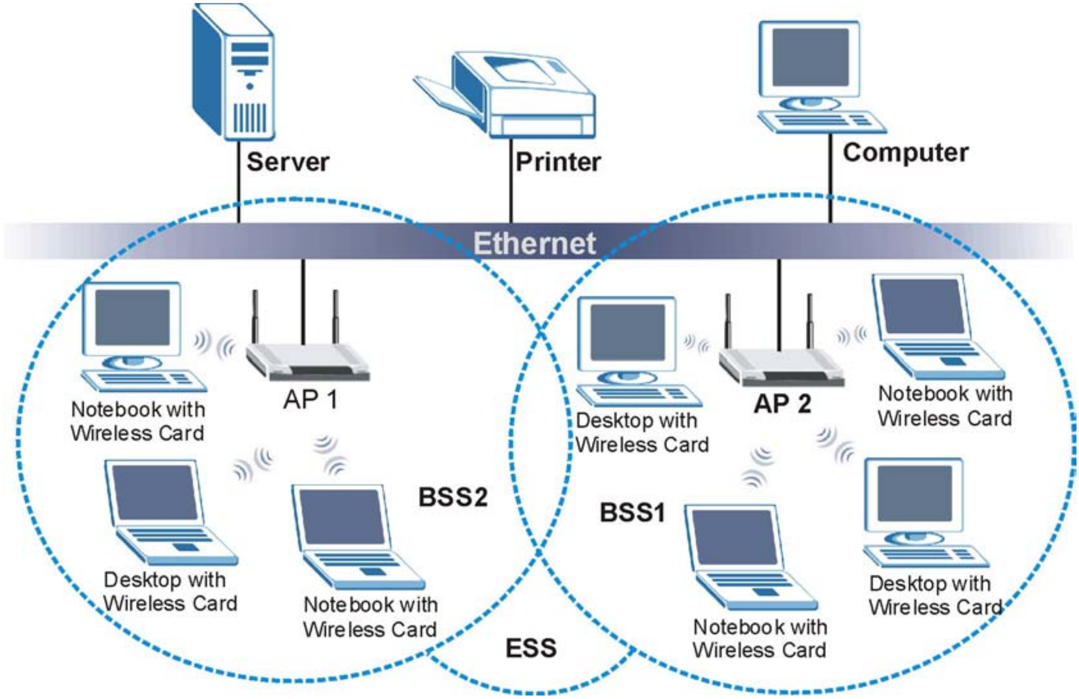

Server
Printer
Computer
Ethernet
Notebook with Wireless Card
AP 1
Desktop with Wireless Card
Notebook with Wireless Card
BSS2
Desktop with Wireless Card
AP 2
Notebook with Wireless Card
BSS1
Notebook with Wireless Card
Desktop with Wireless Card
ESS

Diagram C-2 ESS Provides Campus-Wide Coverage

Appendix D
Wireless LAN With IEEE 802.1x

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

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

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.

Advantages of the IEEE 802.1x

- 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 Server Authentication Sequence

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

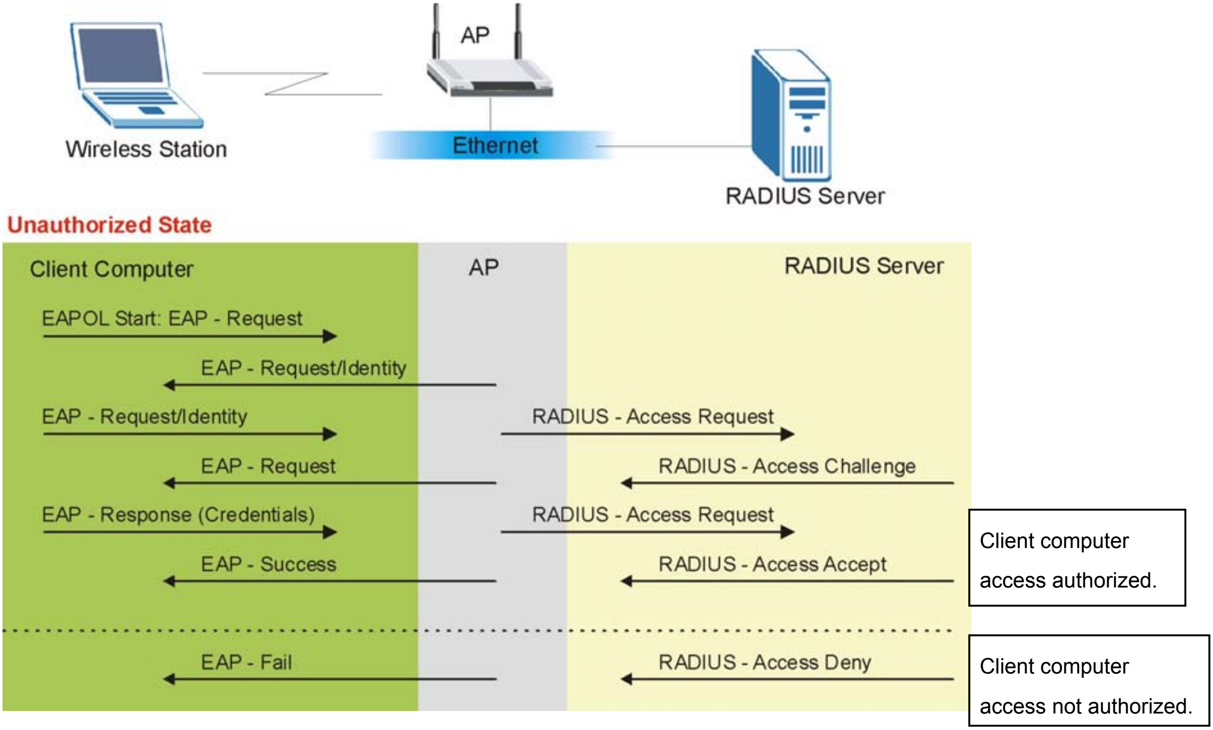


Diagram D-1 Sequences for EAP MD5–Challenge Authentication

Appendix E
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. 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 five authentication types.

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 F
IP Subnetting

IP Addressing

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

IP Classes

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

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

Chart F-1 Classes of IP Addresses

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

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

Therefore:

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

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

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

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

Chart F-2 Allowed IP Address Range By Class

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

Subnet Masks

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

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Chart F-3 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

Chart F-4 Alternative Subnet Mask Notation

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

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

Example: Two Subnets

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

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

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

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

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

Chart F-5 Subnet 1

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

Chart F-6 Subnet 2

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

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

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart F-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.63		Highest Host ID: 192.168.1.62

Chart F-8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64		Lowest Host ID: 192.168.1.65
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart F-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000

Chart F-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.191		Highest Host ID: 192.168.1.190

Chart F-10 Subnet 4

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

Example Eight Subnets

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

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

Chart F-11 Eight Subnets

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

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

Chart F-12 Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

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

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

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

Chart F-13 Class B Subnet Planning

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

Chart F-13 Class B Subnet Planning

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

Appendix G Index