ZyXEL G-560

802.11g Wireless Access Point

User's Guide

Version 3.0
9/2005

ZyXEL

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Caution

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

Notice 1

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

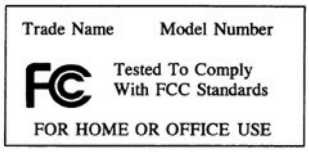
This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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

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

Certifications

1. Go to www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.



Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal 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.

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 / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (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		
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		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[A] FAX	WEB SITE FTP SITE	REGULAR MAIL
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

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

Table of Contents

List of Figures

List of Tables

Preface

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

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

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.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

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

- ZyXEL Glossary and Web Site

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

User Guide Feedback

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

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- Mouse action sequences are denoted using a right arrow bracket key (>). For example, "In Windows, click **Start** > **Settings** > **Control Panel**" means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

- The ZyXEL G-560 802.11g Wireless Access Point may be referred to simply as the G-560 in the user's guide.

Graphics Icons Key

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

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. It can also work as a bridge to extend your wireless network. The G-560 uses IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access), WPA2 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.

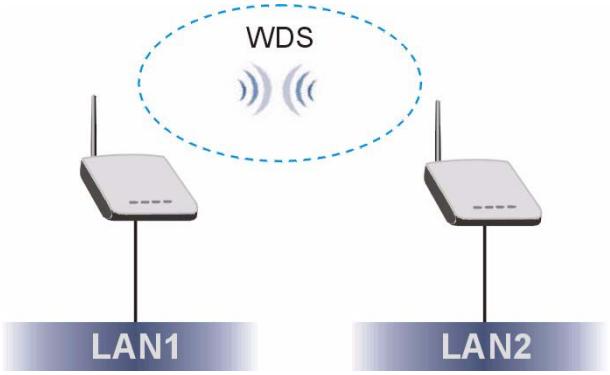
Bridge

The G-560 can act as a bridge, establishing up to four wireless links with other APs.

WDS Functionality

A Distribution System (DS) is a wired connection between two or more APs, while a Wireless Distribution System (WDS) is a wireless connection. Your G-560 supports WDS, providing a cost-effective solution for wireless network expansion.

Figure 1 WDS Functionality Example



OTIST (One-Touch Intelligent Security Technology)

OTIST allows your G-560 to assign its SSID and security settings (WEP or WPA-PSK) to the ZyXEL wireless adapters that support OTIST and are within transmission range. The ZyXEL wireless adapters must also have OTIST enabled.

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

The ZyXEL wireless 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 standard. Key differences between WPA and WEP are user authentication and improved data encryption.

WPA2

WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

WMM (Wi-Fi MultiMedia) QoS (Quality of Service)

WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of the individual and applications.

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.

Output Power Management

Output Power Management is the ability to set the level of output power.

There may be interference or difficulty with channel assignment when there is a high density of APs within a coverage area. In this case you can lower the output power of each access point, thus enabling you to place access points closer together.

Limit the Number of Client Connections

You may set a maximum number of wireless stations that may connect to the G-560. This may be necessary if for example, there is interference or difficulty with channel assignment due to a high density of APs within a coverage area.

1.3 Applications for the G-560

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

1.3.1 Access Point

1.3.1.1 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.

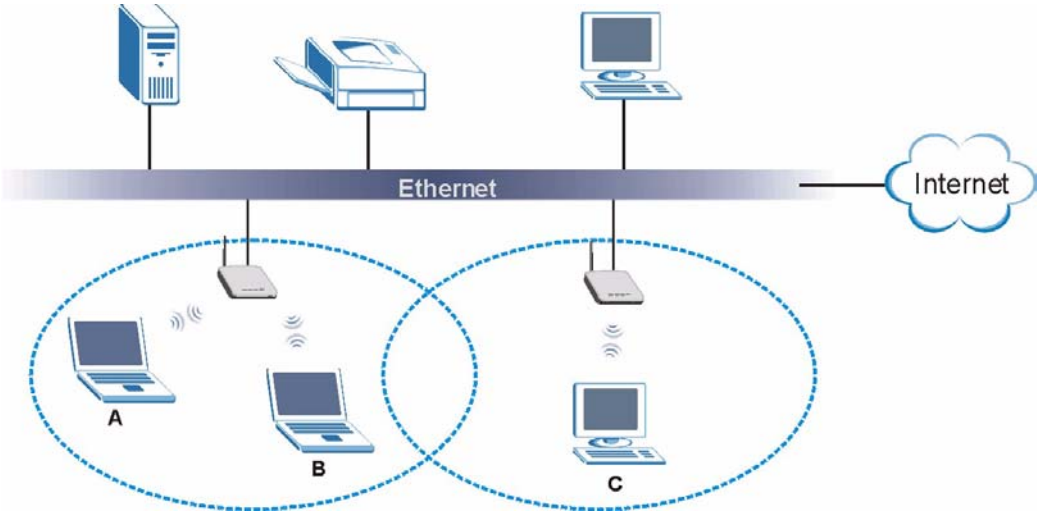
Figure 2 Internet Access Application

1.3.1.2 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. Stations **A**, **B** and **C** can access the wired network through the G-560s.

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 3 Corporation Network Application



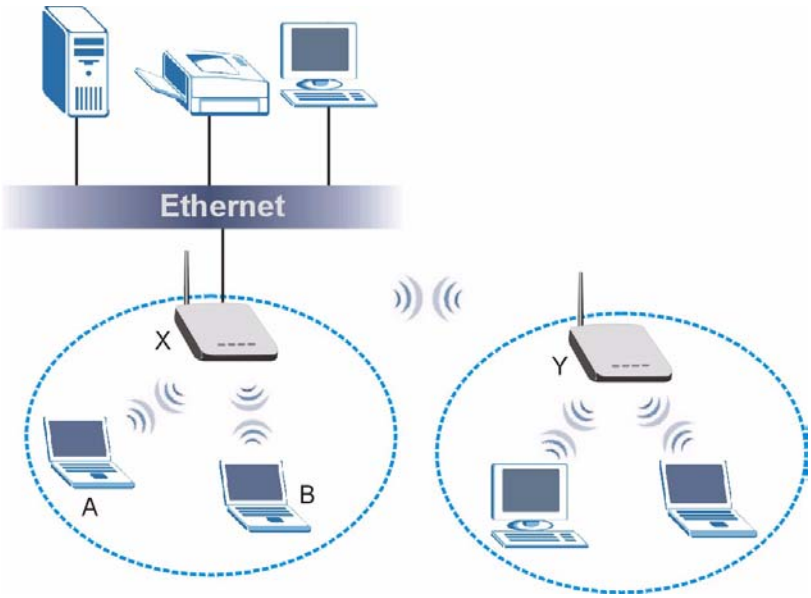
1.3.2 Access Point + Bridge

In **Access Point + Bridge** mode, the G-560 supports both AP (**A** and **B** can connect to the wired network through **X**) and bridge (**X** can communicate with **Y**) connection at the same time.

The G-560 can act as a wireless network bridge and establish wireless links with other APs. In order to prevent bridge loops when the G-560 is in the bridge mode, you should ensure that your G-560 is not connected to both wired and wireless segments of the same LAN. Also make sure that you do not have three or more G-560s (in bridge mode and on different wired LANs) wirelessly connect to each other.

When the G-560 is in **Access Point + Bridge** mode, the traffic between G-560s (the WDS) is not encrypted. The security settings on the G-560 refer to the traffic between the wireless station and the G-560.

Figure 4 AP+Bridge Application



1.4 The LED Display

Figure 5 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 G-560 is not ready or rebooting.
		On	The G-560 has a successful reboot and is receiving power.
		Off	The G-560 is not receiving power.
ETHN	Green	Blinking	The G-560 is sending/receiving data.
		On	The G-560 has a successful 10Mbps Ethernet connection.
	Amber	Blinking	The G-560 is sending/receiving data.
		On	The G-560 has a successful 100Mbps Ethernet connection.
		Off	The G-560 does not have an Ethernet connection.

Table 1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
OTIST	Green	Blinking	The OTIST automatic wireless configuration is in progress.
		On	The OTIST feature is activated on the G-560.
		Off	The OTIST feature is not activated or activated but the wireless settings are changed again.
WLAN	Green	Blinking	The G-560 is sending or receiving data through the wireless LAN.
		On	The G-560 is ready, but is not sending/receiving data.

CHAPTER 2
Management Computer Setup

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

2.1 Introduction

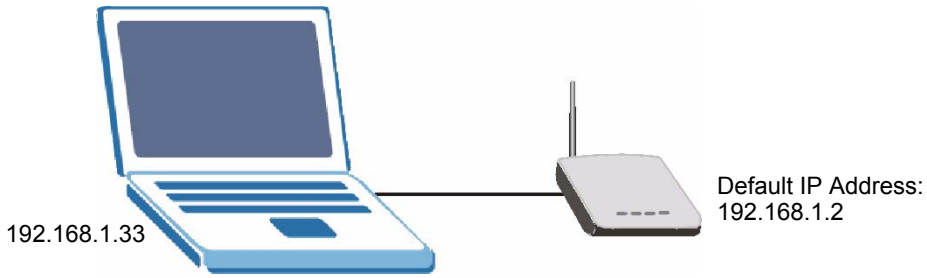
You can connect a computer to the G-560 for management purposes either using an Ethernet connection (recommended for a first time management session) or wirelessly.

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 6 Wired Connection



2.2.1 Setting Up Your Computer's IP Address

Note: 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 appendix about setting up your computer's IP address for other operating systems.

2.2.1.1 Windows 2000/NT/XP

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

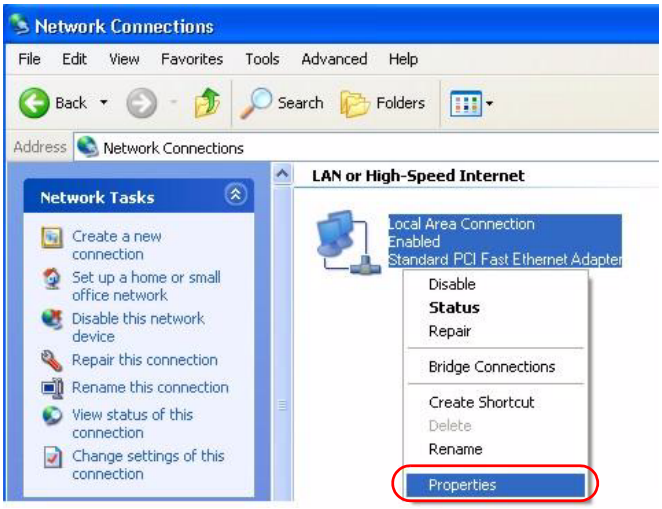
1 Click **start** (**Start** in Windows 2000/NT) **> Settings** > **Control Panel**.

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

Figure 7 Control Panel

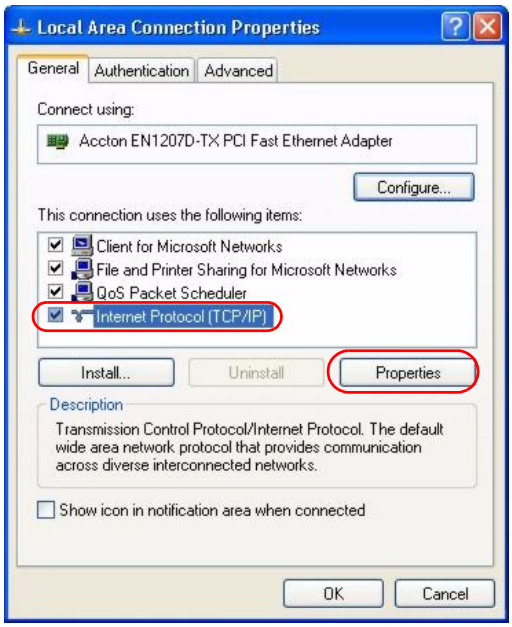
3 Right-click **Local Area Connection** and then **Properties**.

Figure 8 Network Connection



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

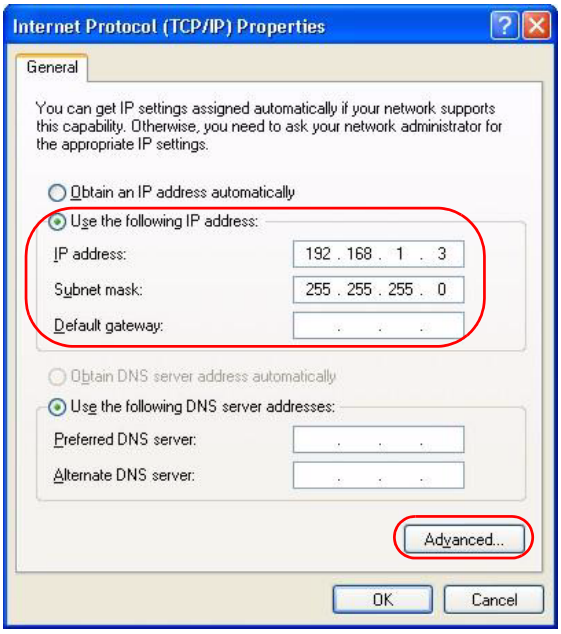
Figure 9 Local Area Connection Properties



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].

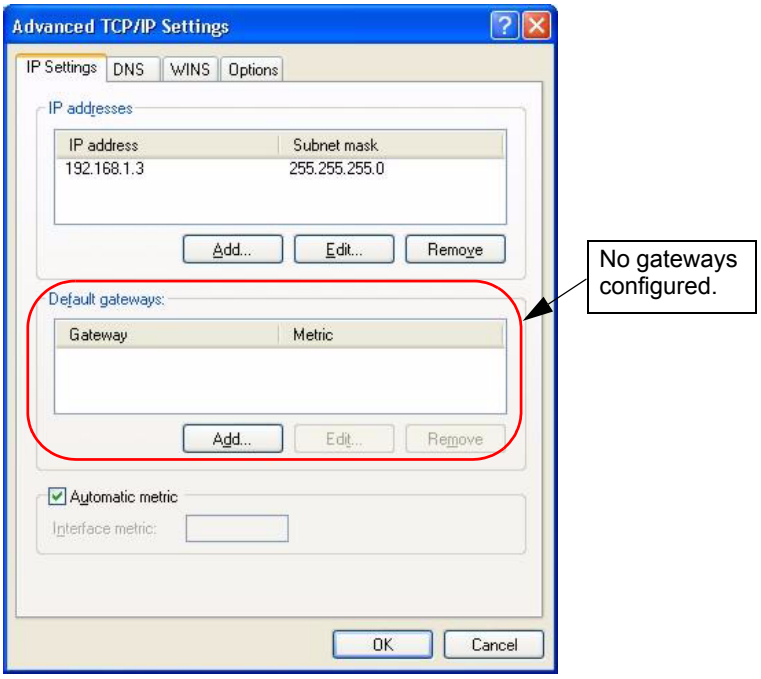
Figure 10 Internet Protocol Properties



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.

Figure 11 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 stations 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 12 Wireless Connection

Note: 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 Factory Defaults

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

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 > Configuration File**. 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

The web configurator is an HTML-based management interface that allows easy G-560 setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

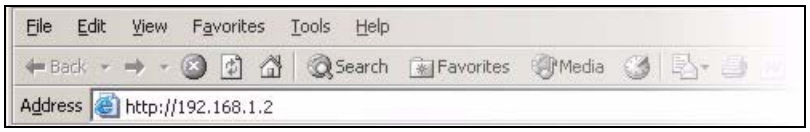
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the **Troubleshooting** chapter if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

3.2 Accessing the G-560 Web Configurator

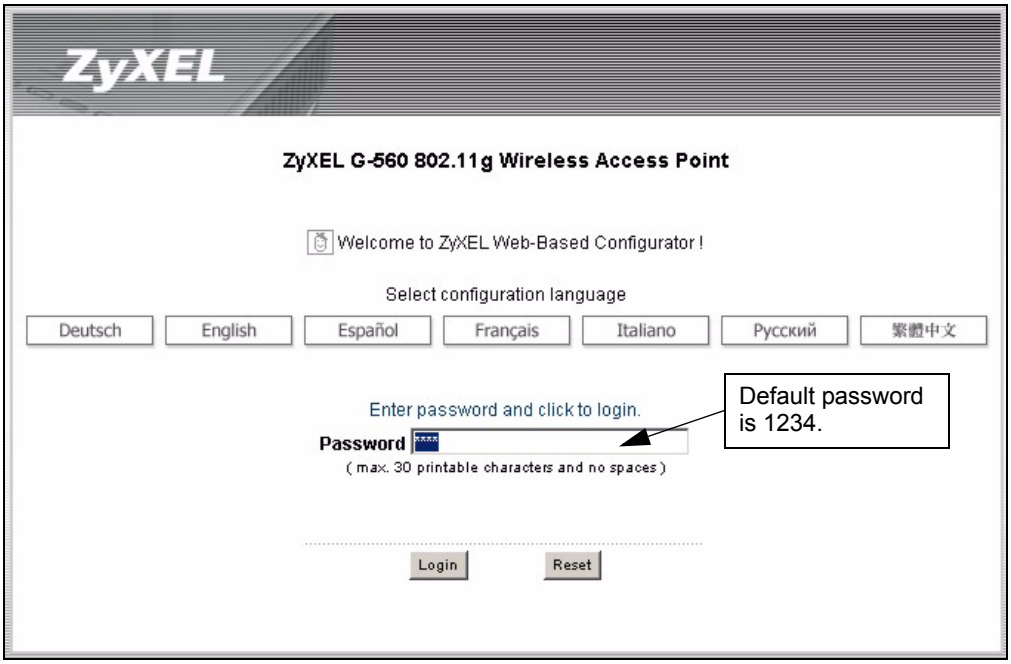
Follow the steps below to access the web configurator, select a language, change your login password and choose a configuration method from the status screen.

1. Make sure your G-560 hardware is properly connected (refer to the Quick Start Guide).
2. Prepare your computer/computer network to connect to the G-560 (refer to Section 2.2.1 on page 31 for instructions on how to do this).
3. Launch your web browser.
4. Type "192.168.1.2" (default) as the URL. Press **Enter**.



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**.

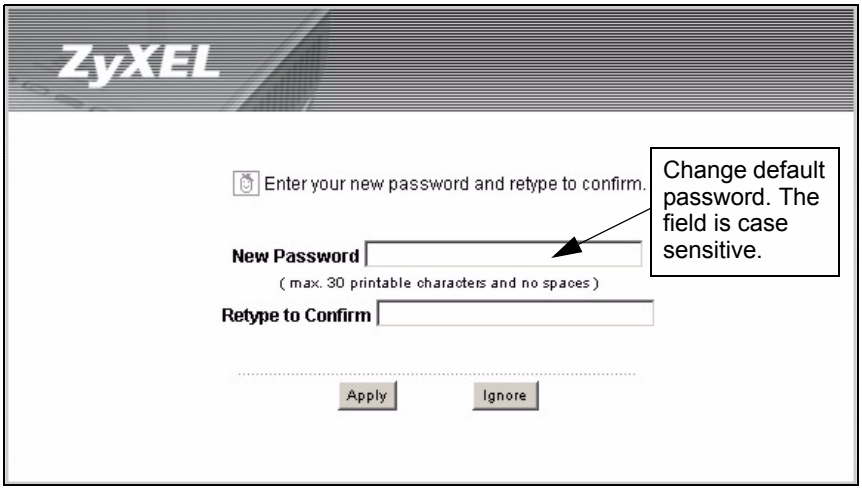
Figure 13 Welcome Screen



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.

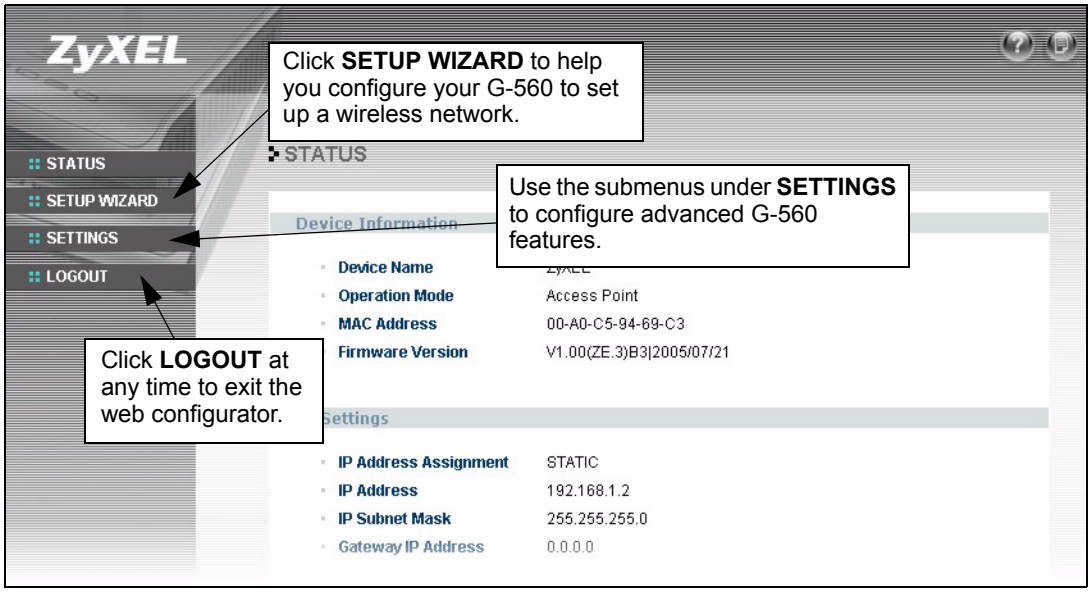
Note: If you do not change the password, the following screen appears every time you login.

Figure 14 Change Password Screen



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

Figure 15 Status Screen



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

3.3 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**.

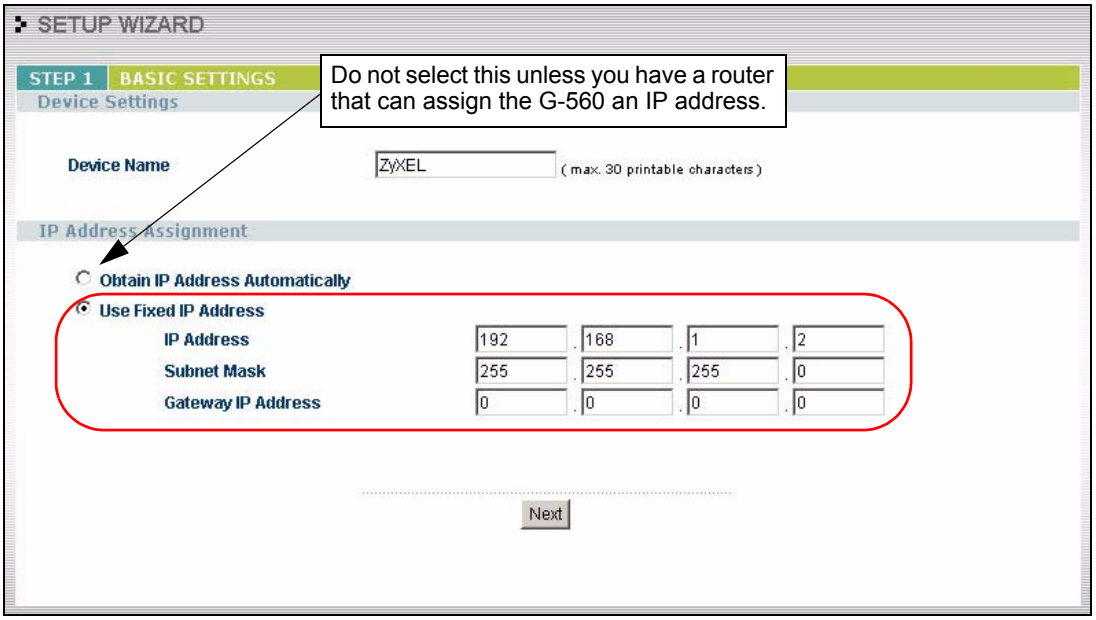
3.3.1 Basic Settings

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**.

Figure 16 Wizard 1: Basic Settings



Note: 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.

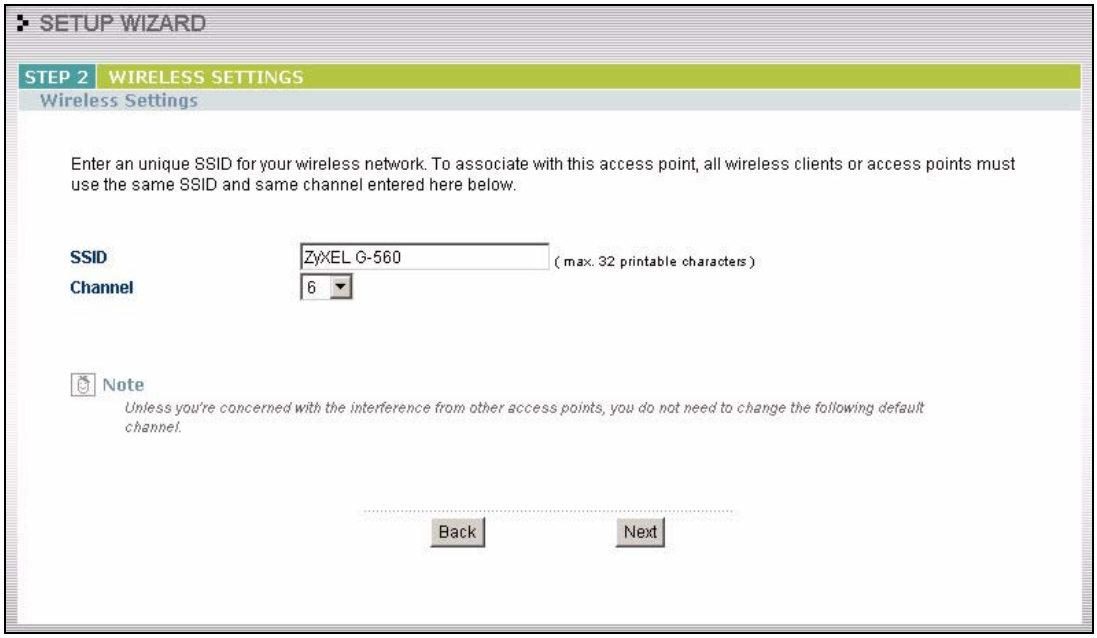
3.3.2 Wireless Settings

Use the second wizard screen to set up the wireless LAN. See the chapter on the wireless screens 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.

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

Figure 17 Wizard 2: Wireless Settings



3.3.3 Security Settings

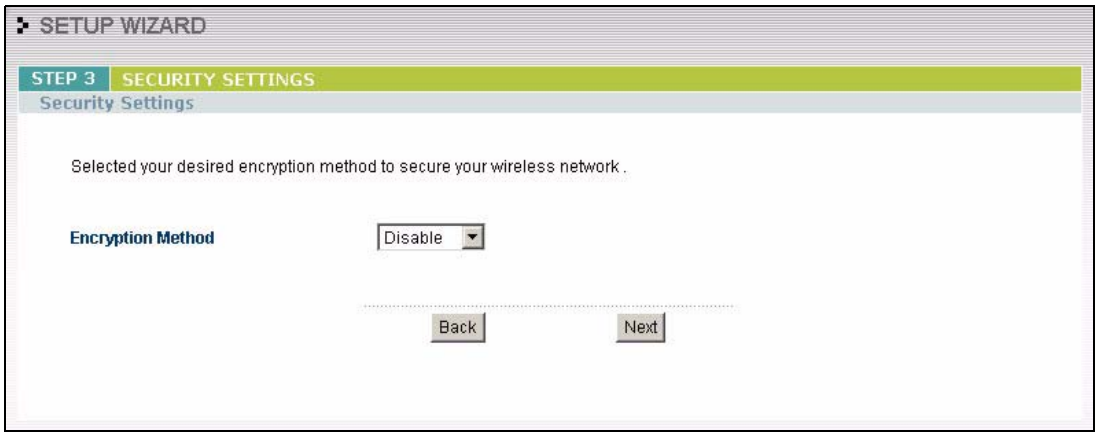
Fill in the fields in the third wizard configuration screen. The screen varies depending on what you select in the **Encryption Method** field. Select **Disable** to have no wireless security configured, select **WEP**, or select **WPA-PSK** if your wireless clients support WPA-PSK. Go to **SETTINGS** > **WIRELESS** > **Security** if you want WPA2, WPA or 802.1x. See Chapter 6 on page 53 for background information.

3.3.3.1 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.

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

Figure 18 Setup Wizard 3: Disable



3.3.3.2 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.

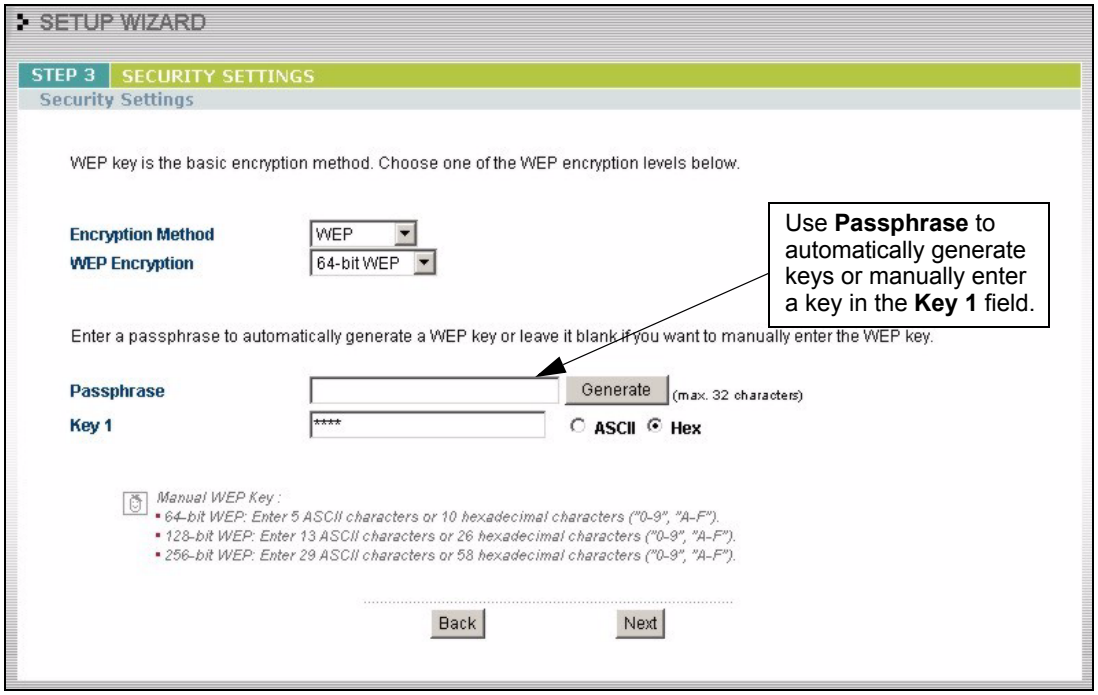
3 You can generate or manually enter a WEP key by either

- 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.

Figure 19 Wizard 3: WEP

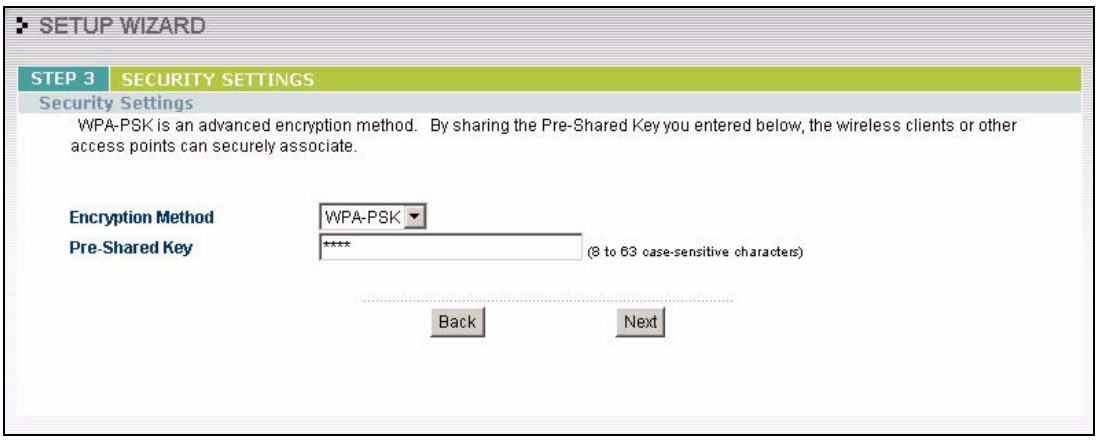


3.3.3.3 WPA-PSK

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.

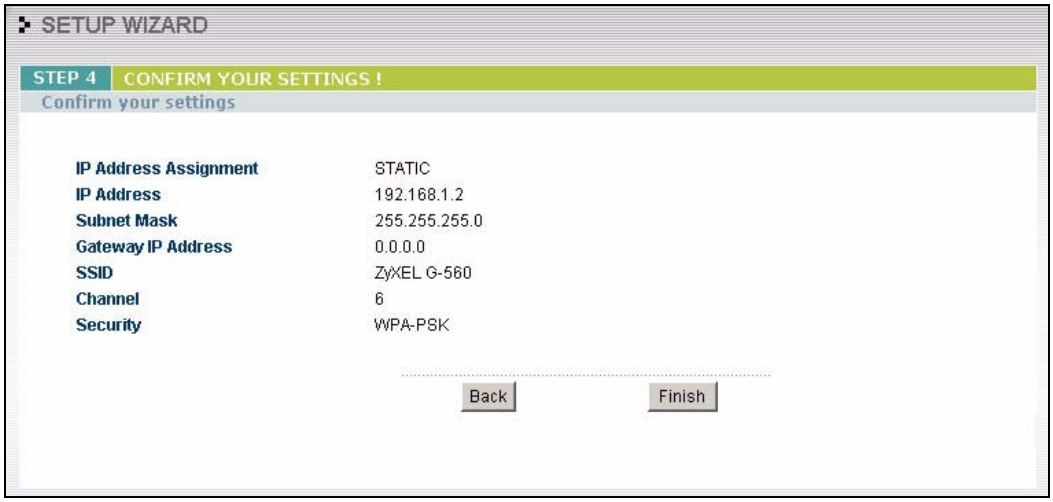
Figure 20 Wizard 3: WPA-PSK



3.3.4 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.

Figure 21 Wizard 4: Confirm Your Settings



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

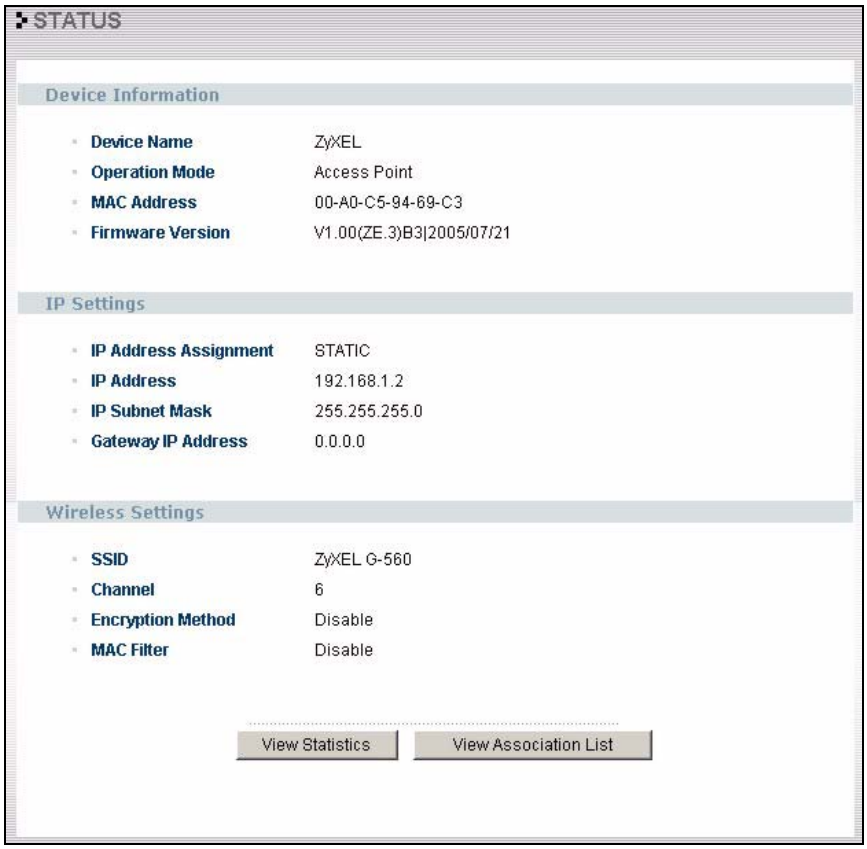
CHAPTER 4
Status Screens

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.

Figure 22 Status



The following table describes the labels in this screen.

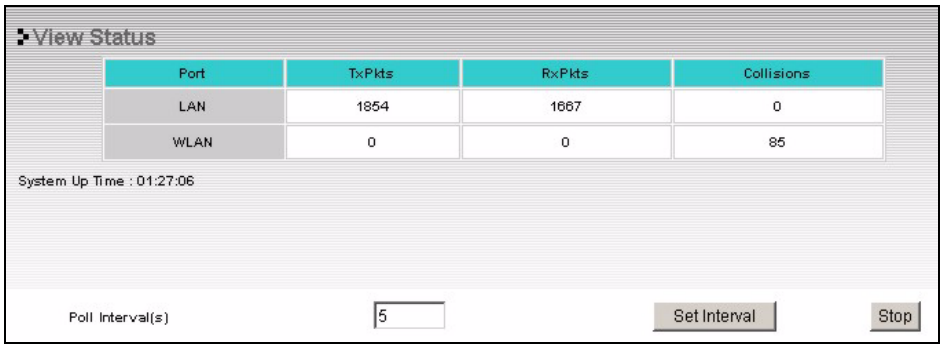
Table 3 Status

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 or an access point and bridge simultaneously.
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**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK Mixed**, **WPA**, **WPA2**, **WPA/WPA2 Mixed** 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.

Figure 23 Status: View Statistics



The following table describes the labels in this screen.

Table 4 Status: View Statistics

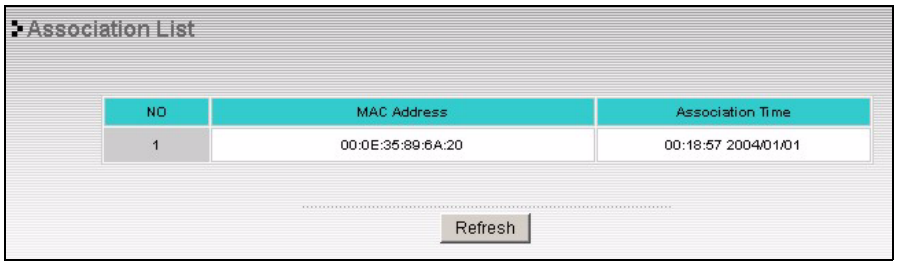
LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
System Up Time	This is the total time the G-560 has been on.
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

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.

Figure 24 Status: View Association List



The following table describes the labels in this screen.

Table 5 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.
Association Time	This field displays the time a wireless station first associated with the G-560.
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 6 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

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.

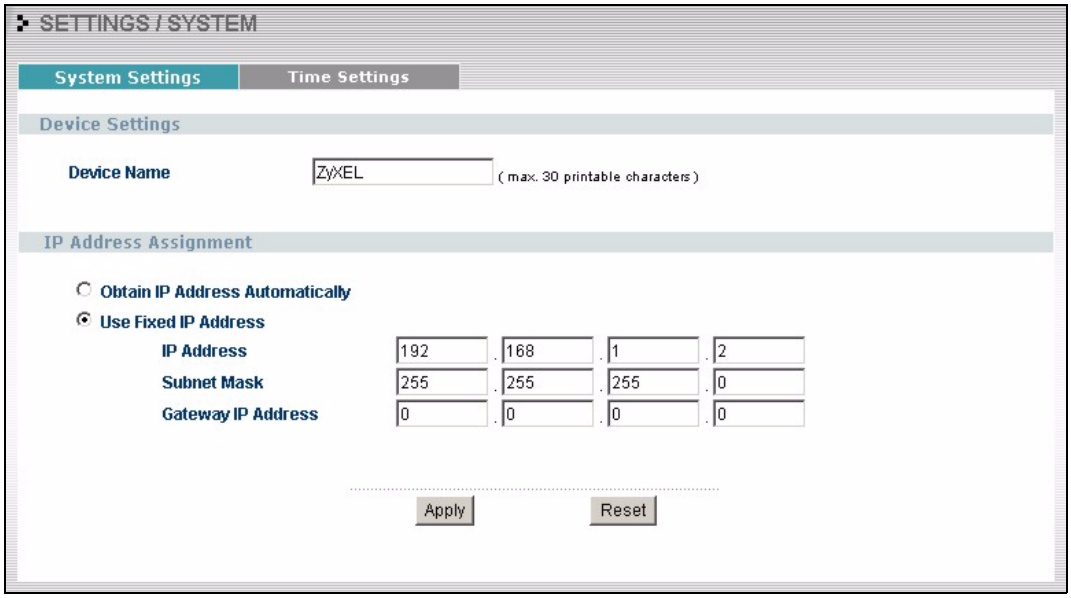
Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your G-560, but make sure that no other device on your network is using that IP address.

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 > SYSTEM** to open the **System Settings** screen.

Figure 25 System Settings



The following table describes the labels in this screen.

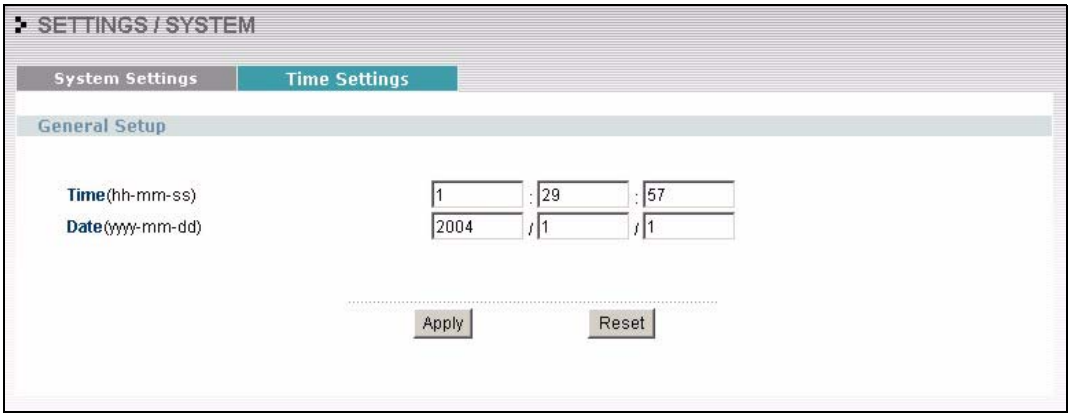
Table 7 System Settings

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. **Note:** 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.
IP Address	Enter the IP address of your G-560 in dotted decimal notation. **Note:** 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 > Time Settings**. 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.

Figure 26 Time Settings



The following table describes the labels in this screen.

Table 8 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.

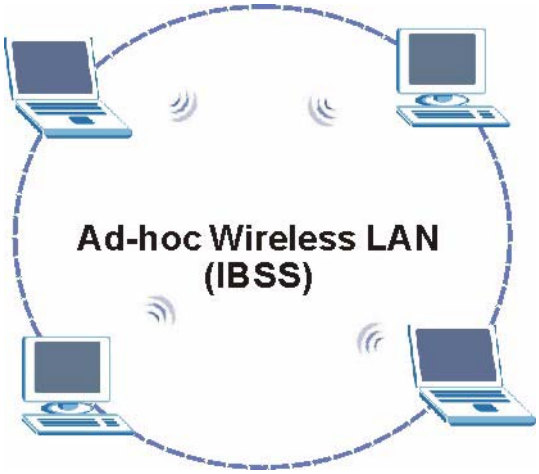
6.1 Wireless LAN Overview

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 27 IBSS (Ad-hoc) Wireless LAN

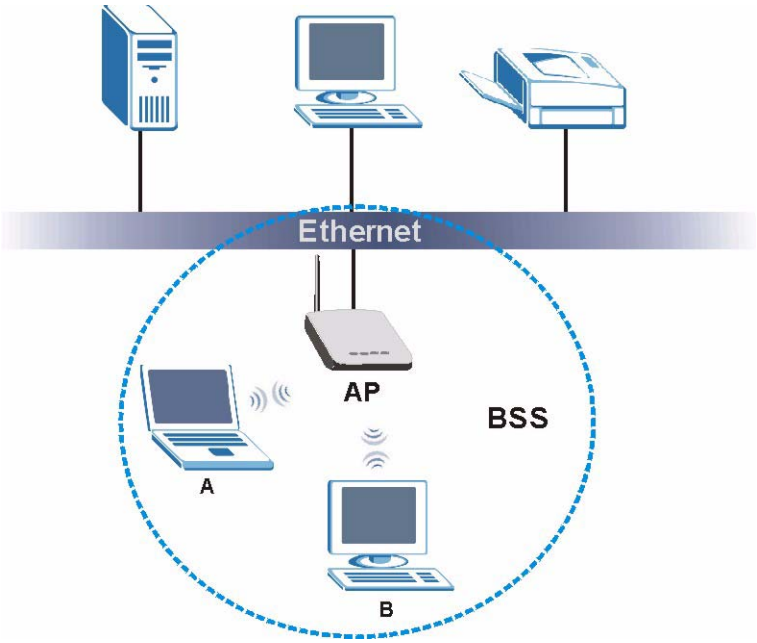


6.1.2 BSS

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.

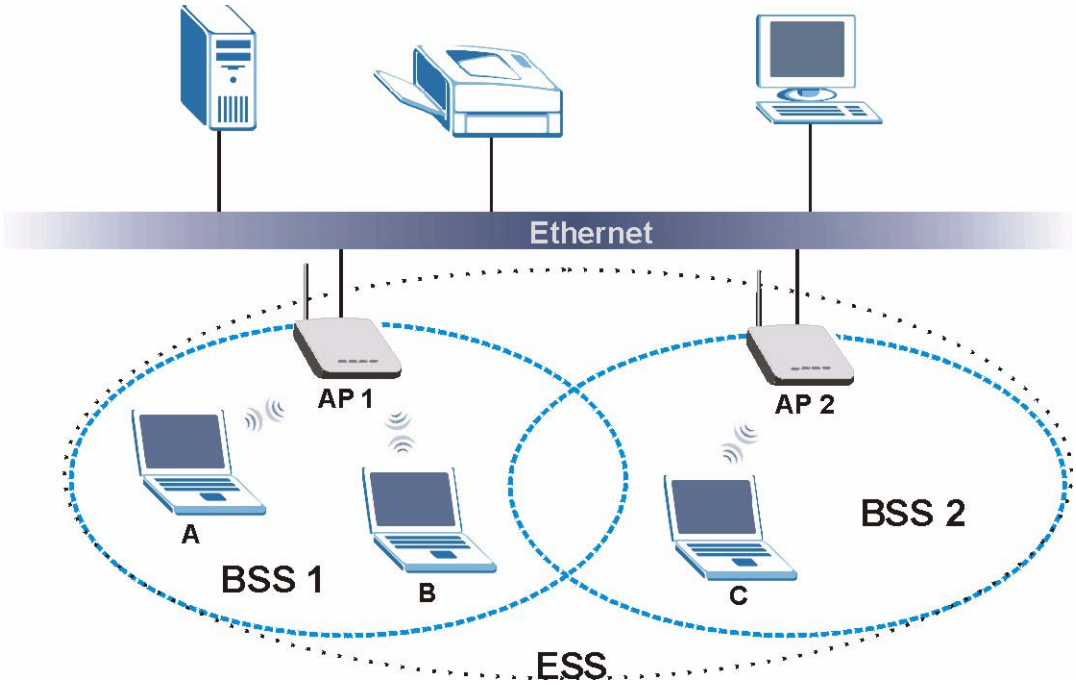
Figure 28 Basic Service set



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 29 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.

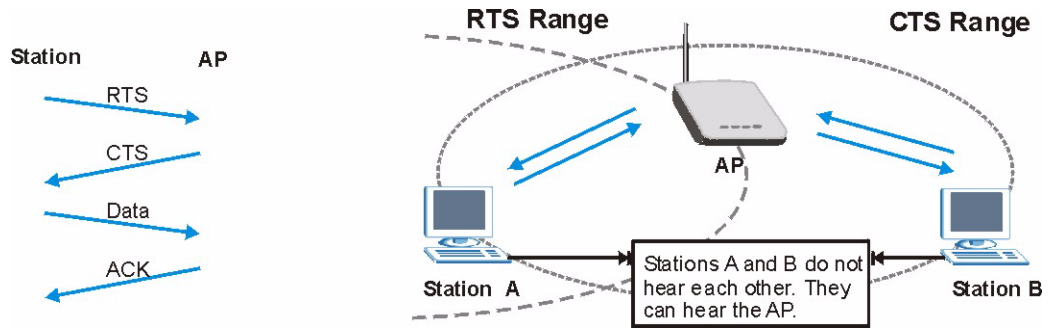
6.2.2 SSID

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.

Figure 30 RTS/CTS



When station A sends data to the G-560, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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

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

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

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

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

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

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 WMM QoS

WMM (Wi-Fi MultiMedia) is a part of the IEEE 802.11e QoS (Quality of Service) enhancement to the Wi-Fi standard that ensures quality of service for multimedia applications in wireless networks.

WMM allows you to prioritize wireless traffic according to the delivery requirements of the individual and applications.

6.3.1 WMM QoS Example

When WMM QoS is not enabled, all traffic streams are given the same access throughput to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

When WMM QoS is enabled, the streams are prioritized according to the needs of the application. You can assign different priorities to different applications. This prevents reductions in data transmission for applications that are sensitive.

6.3.2 WMM QoS Priorities

The following table describes the priorities that you can apply to traffic that the G-560 sends to the wireless network.

Table 9 WMM QoS Priorities

PRIORITY LEVELS:	
Highest	Typically used for voice traffic or video that is especially sensitive to jitter (variations in delay). Use the highest priority to reduce latency for improved voice quality.
High	Typically used for video traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.

Table 9 WMM QoS Priorities

PRIORITY LEVELS:	
Mid	Typically used for traffic from applications or devices that lack QoS capabilities. Use mid priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
Low	This is typically used for non-critical "background" traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use low priority for applications that do not have strict latency and throughput requirements.

6.3.3 ToS (Type of Service) and WMM QoS

ToS defines the DS(Differentiated Service) field in the IP packet header. The ToS value of outgoing packets is between 0 and 255. 0 is the lowest priority.

WMM QoS checks the ToS in the header of transmitted data packets. It gives the application a priority according to this number. If the ToS is not specified, then transmitted data is treated as normal or best-effort traffic.

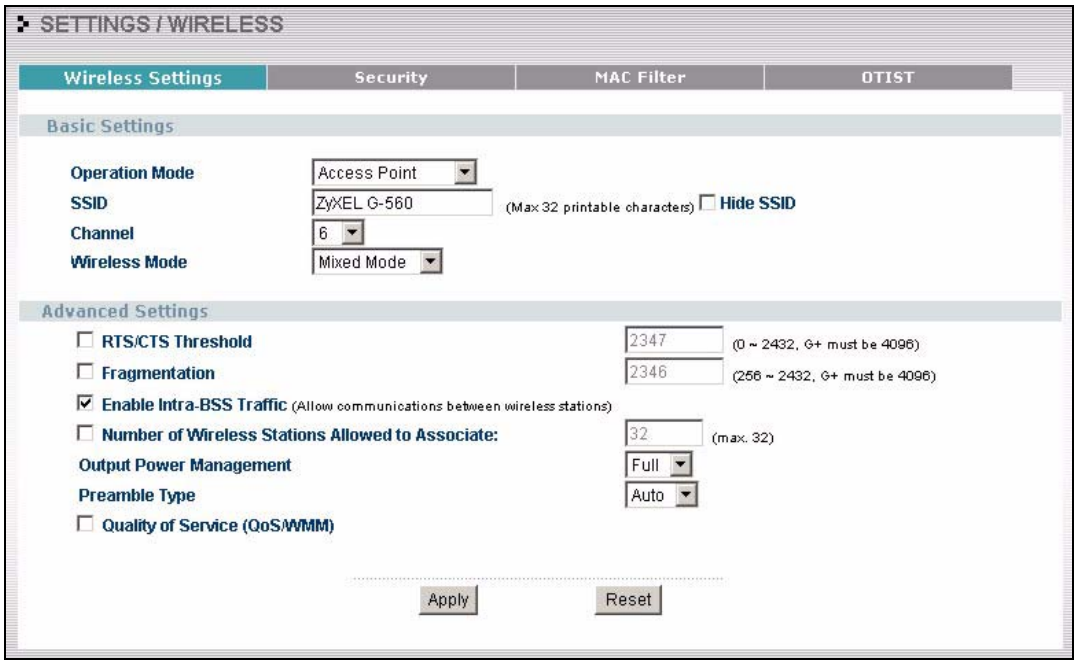
6.4 Configuring Wireless

Click **SETTINGS > WIRELESS** to display the **Wireless Settings** screen.The screen varies depending upon the operation mode you select.

6.4.1 Access Point Mode

Select **Access Point Operation Mode** to display the screen as shown next.

Figure 31 Wireless Settings: Access Point



The following table describes the labels in this screen.

Table 10 Wireless Settings: Access Point

Operation Mode	Select the operation mode from the drop-down list. The options are **Access Point** and **Access Point + Bridge**.
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. **Note:** 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.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
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.

Table 10 Wireless Settings: Access Point (continued)

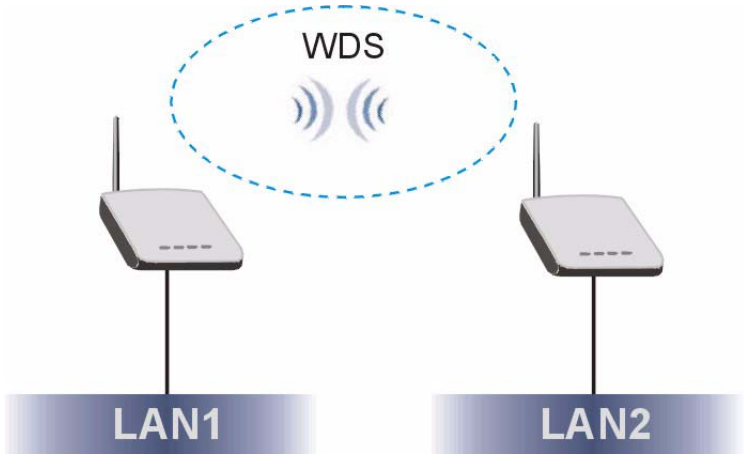
Wireless Mode	Select **Pure B Mode** to allow only IEEE 802.11b compliant WLAN devices to associate with the G-560. Select **Pure G Mode** to allow only IEEE 802.11g compliant WLAN devices to associate with the G-560. Select **Mixed Mode** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices 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	Select the check box and 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	Select the check box and 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.
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. Select **Auto** to have the G-560 automatically use short preamble when all wireless clients support it, otherwise the G-560 uses long preamble. **Note:** The G-560 and the wireless stations MUST use the same preamble mode in order to communicate.
Quality of Service (QoS/WMM)	Select the check box to enable WMM QoS. WMM QoS prioritizes wireless traffic to ensure quality of service in wireless networks. See Table 9 on page 57 for traffic priority.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4.2 Access Point + Bridge Mode

The G-560 can act as a wireless network bridge and establish up to four wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

In the example below, when both G-560s are in **Access Point + Bridge** mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

Figure 32 Bridging Example

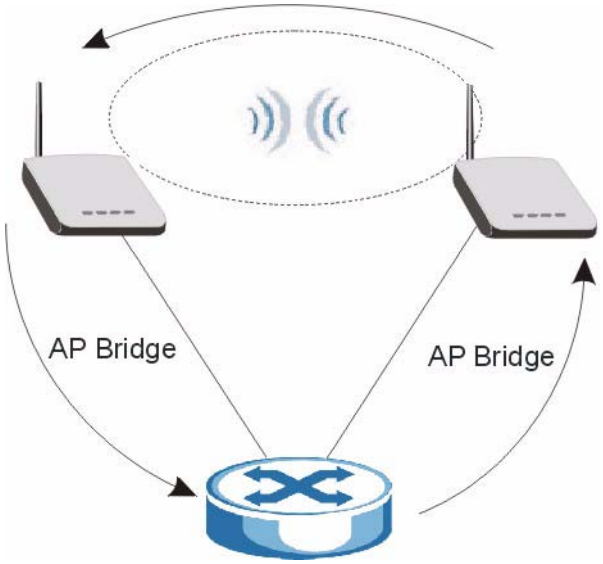


6.4.2.1 Bridge Loop

Be careful to avoid bridge loops when you enable bridging in the G-560. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show network topologies that can lead to this problem:

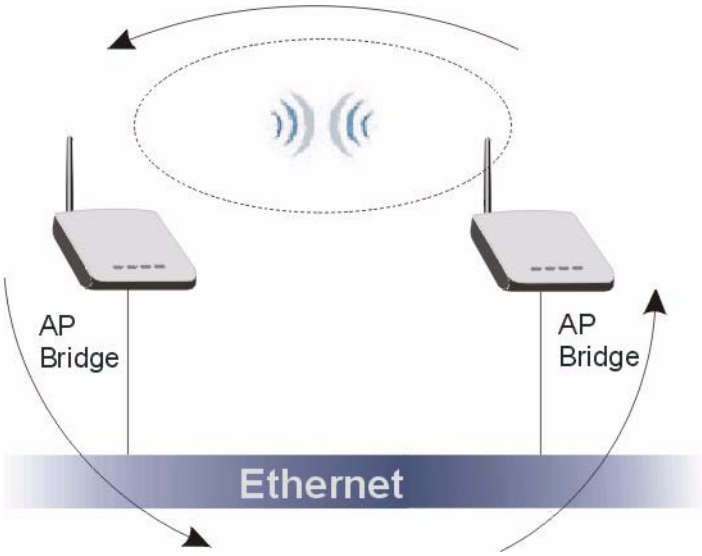
If two or more G-560s (in bridge mode) are connected to the same hub as shown next.

Figure 33 Bridge Loop: Two Bridges Connected to Hub



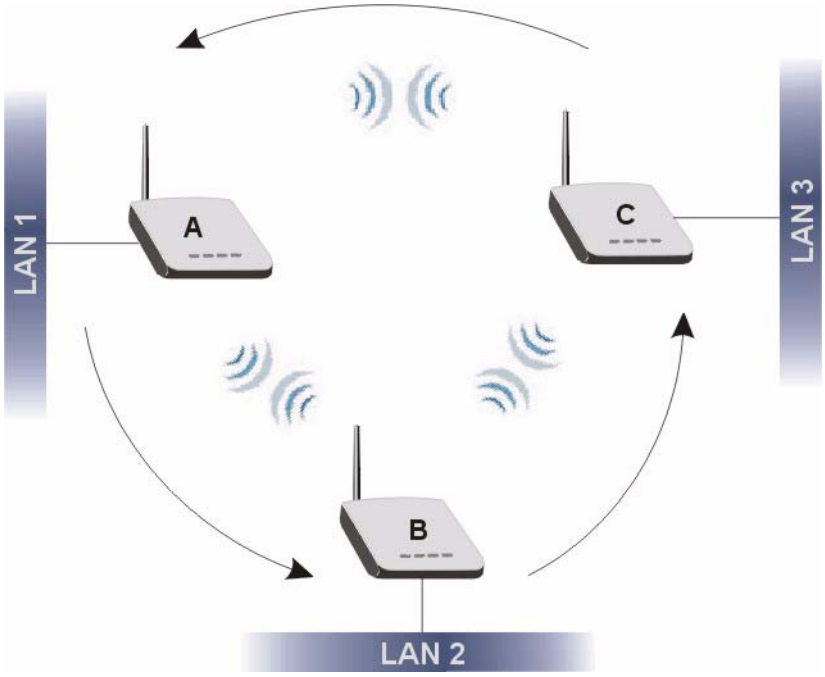
If your G-560 (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN as shown next.

Figure 34 Bridge Loop: Bridges Connected to the Same Wired LAN



If three or more G-560s (in bridge mode) are on different wired LANs but wirelessly connected to each other as shown next.

Figure 35 Bridge Loop: Bridges on Different Wired LANs

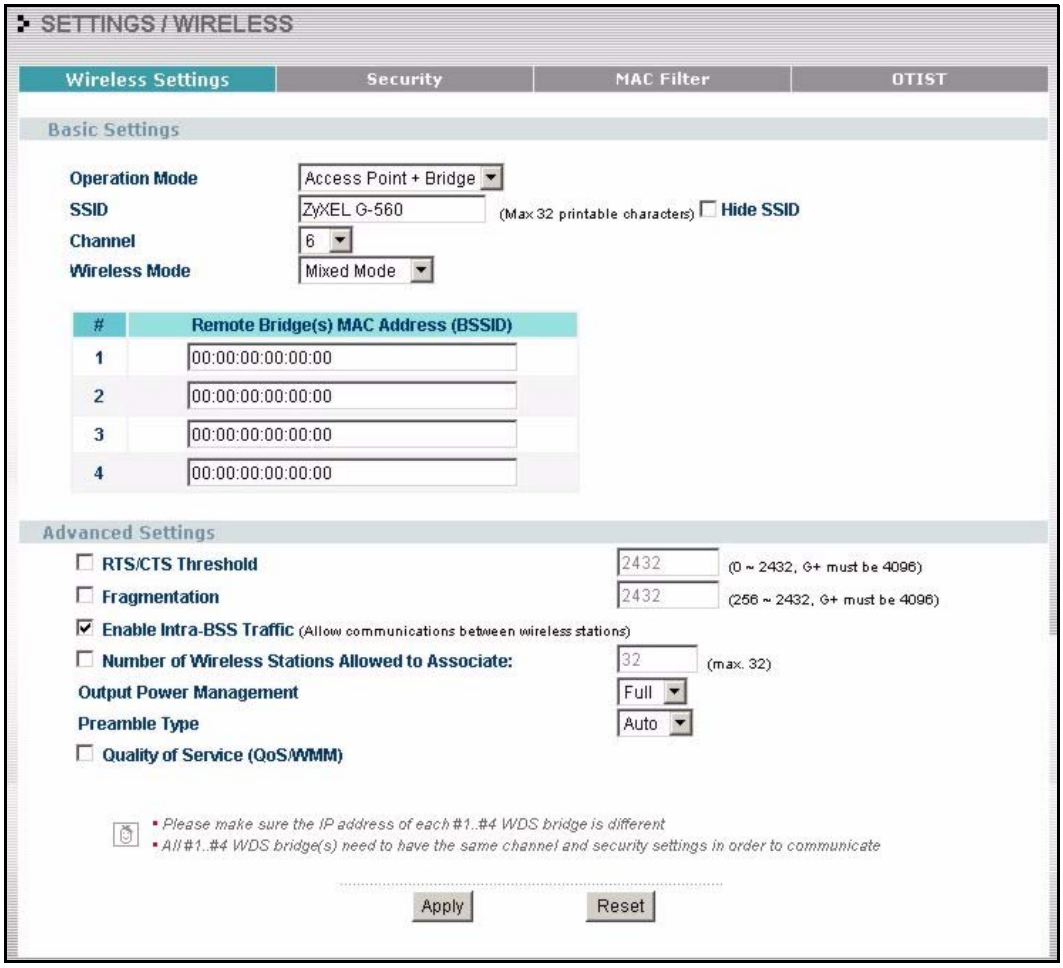


To prevent bridge loops, do not set the G-560 to bridge mode while connected to both wired and wireless segments of the same LAN. Also make sure that you do not have three or more G-560s (in bridge mode and on different wired LANs) wirelessly connect to each other.

6.4.2.2 Configuring Access Point + Bridge Mode

Select **Access Point + Bridge** in the **Operation Mode** drop-down list box to display the screen as shown next. In this screen, you can configure the G-560 to function as an AP and bridge simultaneously.

Figure 36 Wireless Settings: Access Point + Bridge



The following table describes the labels in this screen.

Table 11 Wireless Settings: Access Point + Bridge

Operation Mode	Select the operation mode from the drop-down list. The options are **Access Point** and **Access Point + Bridge**.
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. **Note:** 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.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.

Table 11 Wireless Settings: Access Point + Bridge (continued)

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 IEEE 802.11b or IEEE 802.11g 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.
#	This is the index number of the bridge connection.
Remote Bridge(s) MAC Address (BSSID)	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Advanced Settings	
RTS/CTS Threshold	Select the check box and 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	Select the check box and 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.
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%**.

Table 11 Wireless Settings: Access Point + Bridge (continued)

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. Select **Auto** to have the G-560 automatically use short preamble when all wireless clients support it, otherwise the G-560 uses long preamble. **Note:** The G-560 and the wireless stations MUST use the same preamble mode in order to communicate.
Quality of Service (QoS/WMM)	Select the check box to enable WMM QoS. WMM QoS prioritizes wireless traffic to ensure quality of service in wireless networks. See Table 9 on page 57 for traffic priority.
Apply	Click **Apply** to save your changes back to the G-560.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 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.

Table 12 Wireless Security Levels

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

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.

6.5.1 Encryption

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

6.5.2 Authentication

Use a RADIUS server with WPA or IEEE 802.1x key management protocol.

See the appendix for information on protocols used when a client authenticates with a RADIUS server via the G-560.

6.5.3 Restricted Access

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

6.5.4 Hide G-560 Identity

If you hide the ESSID, then the G-560 cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the G-560 may be inconvenience for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

6.6 WEP Overview

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

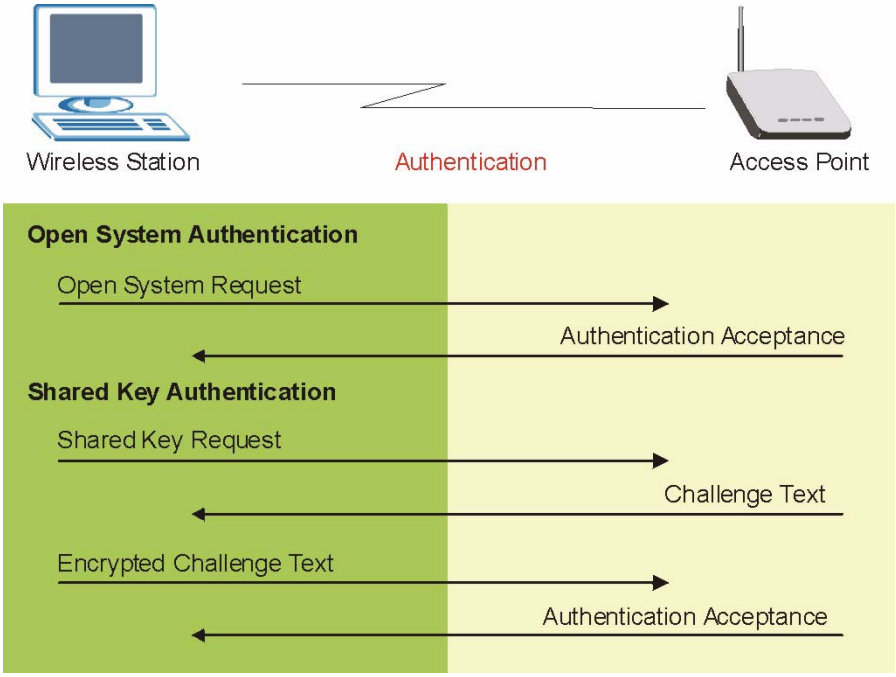
6.6.1 Data Encryption

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 enabled at any one time.

6.6.2 Authentication

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

Figure 37 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.

6.7 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the G-560 (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

6.8 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.

6.8.1 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.

6.9 EAP Authentication Overview

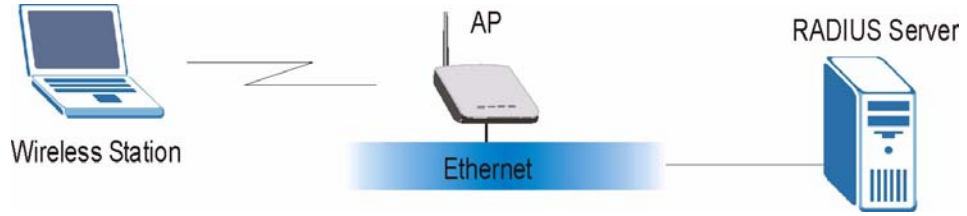
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS 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, EAP-MD5 and PEAP with RADIUS. Refer to the appendix about the types of EAP authentication for descriptions on the common types.

Your G-560 supports EAP-MD5 (Message-Digest Algorithm 5) and PEAP (Protected EAP) with the built-in RADIUS server.

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

Figure 38 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

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

6.10 Dynamic WEP Key Exchange

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

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

To use Dynamic WEP, enable and configure the RADIUS server and enable Dynamic WEP Key Exchange in the **WIRELESS Security 802.1x** screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

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

6.11 Introduction to WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

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

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

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

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

6.11.1 Encryption

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

The encryption mechanisms used for WPA(2) and WPA(2)-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(2)-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.

6.11.2 User Authentication

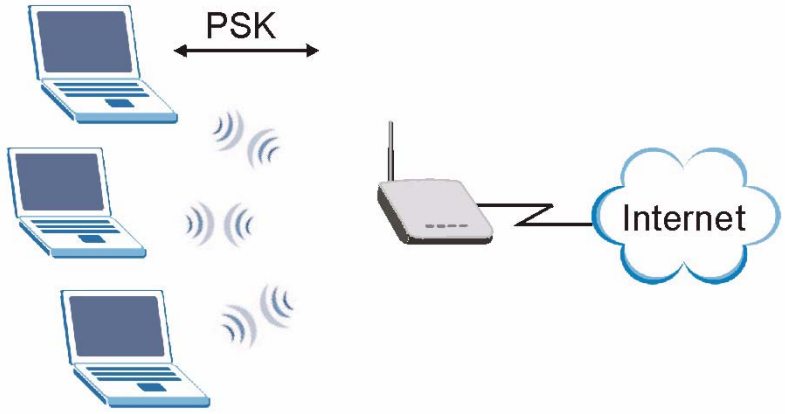
WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

6.12 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

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).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 39 WPA(2)-PSK Authentication



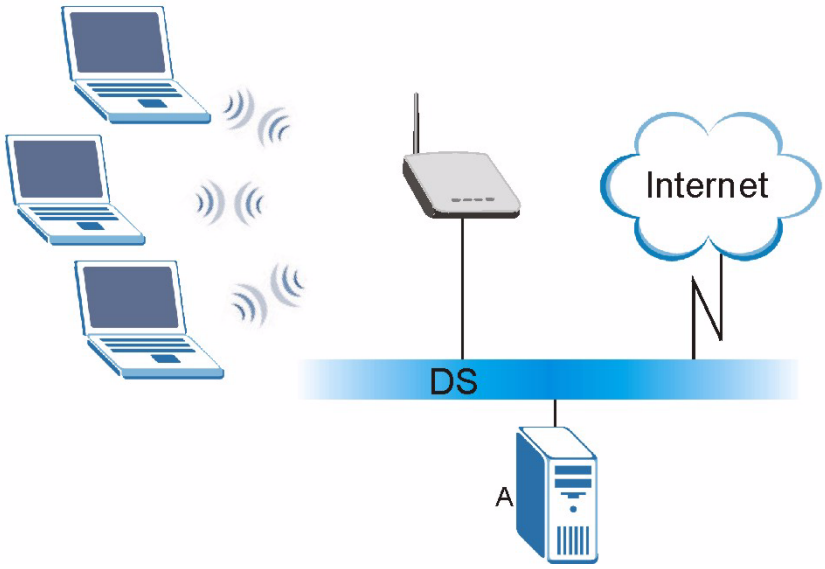
6.13 WPA(2) with RADIUS Application Example

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

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically

generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 40 WPA with RADIUS Application Example



6.14 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**, **128-bit WEP** or **256-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 13 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	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable

Table 13 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

6.15 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.

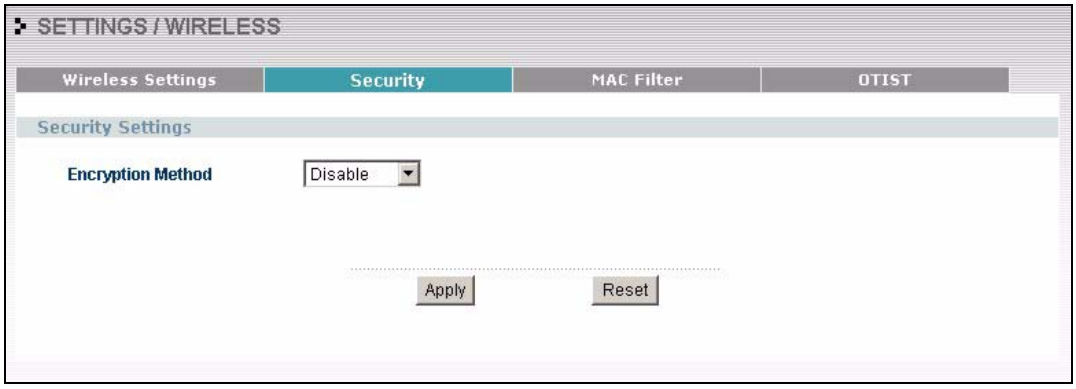
6.16 Configuring Wireless Security

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

6.16.1 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.

Figure 41 Wireless Security: Disable



The following table describes the labels in this screen.

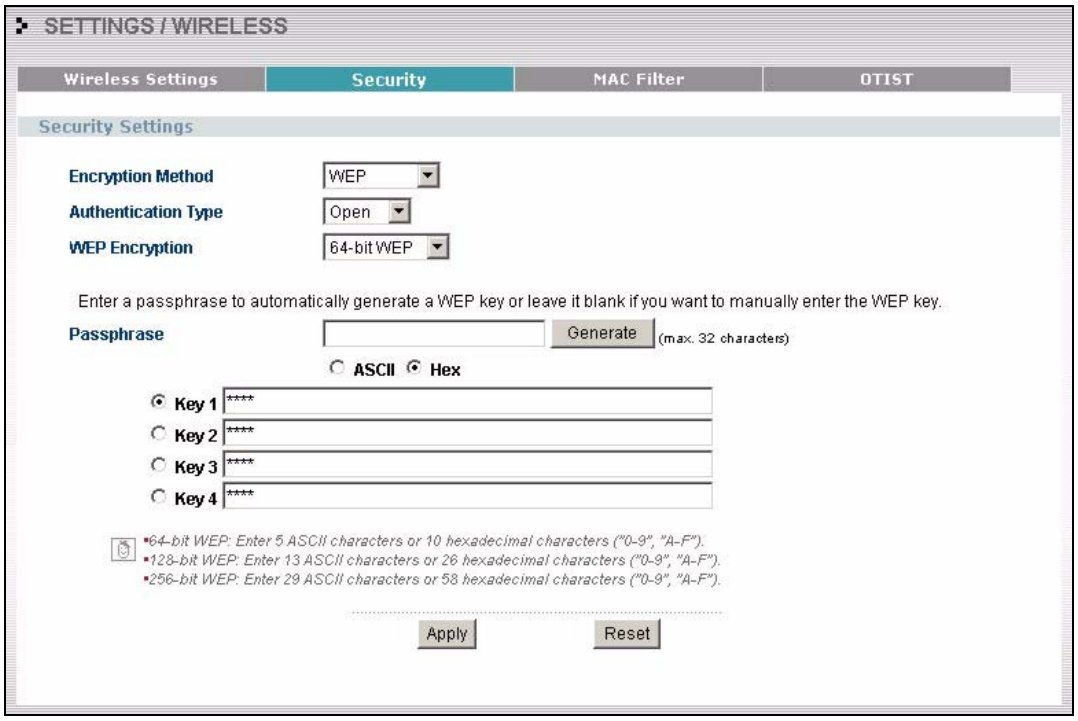
Table 14 Wireless Security: Disable

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.

6.16.2 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.

Figure 42 Wireless Security: WEP



The following table describes the labels in this screen.

Table 15 Wireless 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.

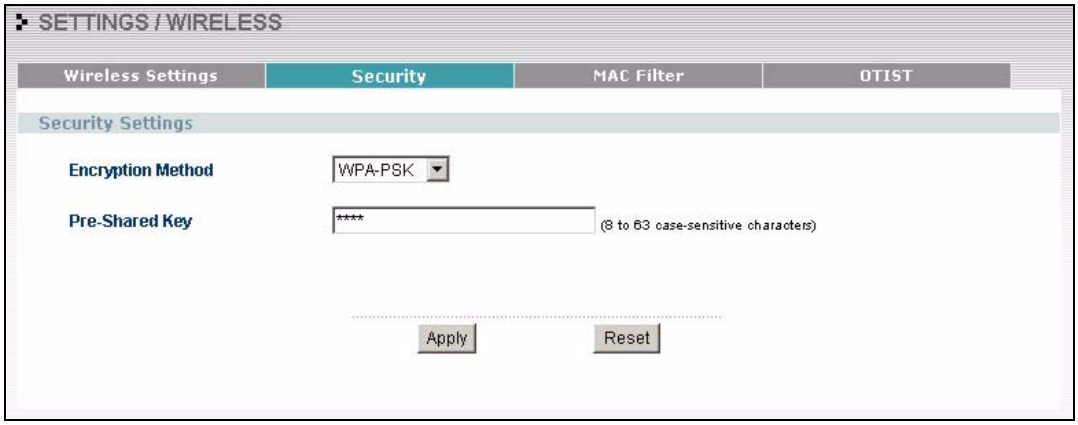
Table 15 Wireless Security: WEP

LABEL	DESCRIPTION
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.
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, select **ASCII** or **Hex** WEP key input method and 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.

6.16.3 WPA-PSK/WPA2-PSK/Mixed

Select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK/WPA2-PSK/Mixed** in the **Encryption Method** drop down list-box to display the screen displays as next.

Figure 43 Wireless Security: WPA-PSK



The following table describes the labels in this screen.

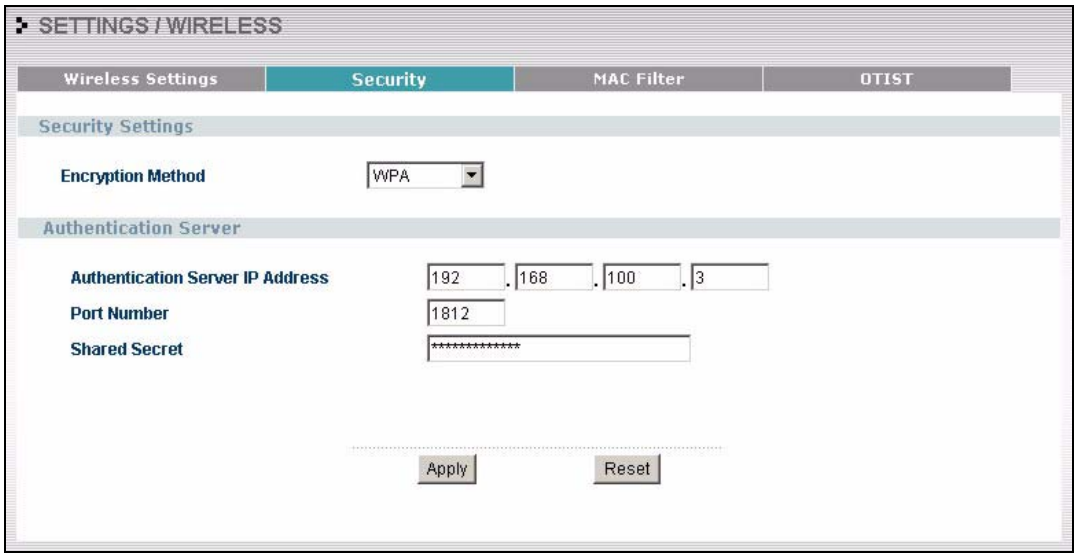
Table 16 Wireless Security: WPA-PSK

LABEL	DESCRIPTION
Encryption Method	Select **WPA-PSK** if you want to configure a pre-shared key but your wireless clients don't support WPA2. Select **WPA2-PSK** if you want to configure a pre-shared key and your wireless clients support WPA2. Select **WPA-PSK/WPA2-PSK Mixed** if you want to configure a pre-shared key and your wireless clients support either WPA or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 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.

6.16.4 WPA/WPA2/Mixed

WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are user authentication and improved data encryption.

Figure 44 Wireless Security: WPA



The following table describes the labels in this screen.

Table 17 Wireless Security: WPA

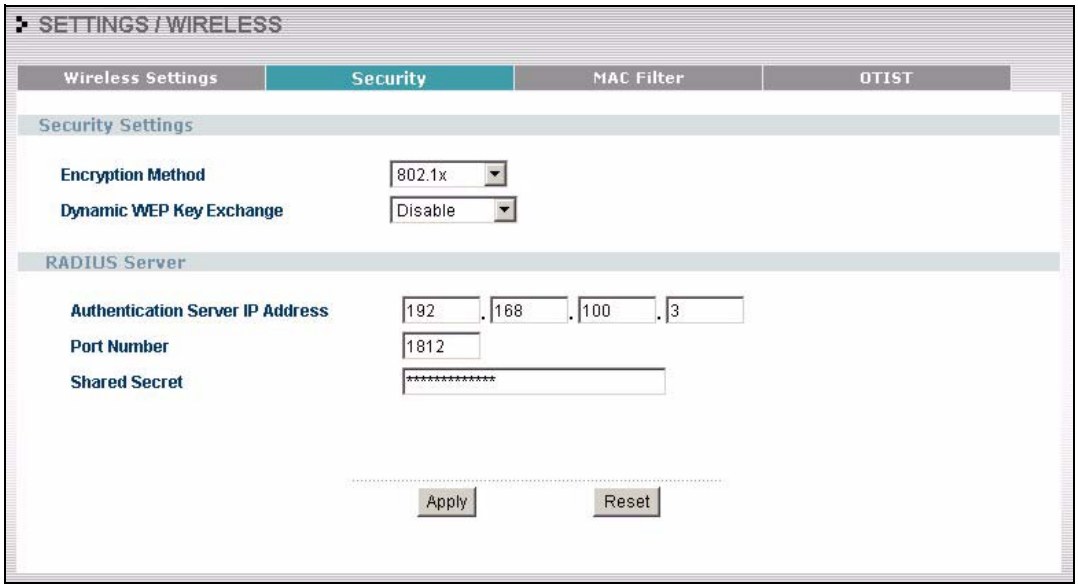
	DESCRIPTION
Encryption Method	Select **WPA** to configure user authentication and improved data encryption if your wireless clients don't support WPA2. Select **WPA2** to configure user authentication and improved data encryption when your wireless clients support WPA2. Select **WPA/WPA2 Mixed** to configure user authentication and improved data encryption if your wireless clients support either WPA or WPA2.
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.

6.16.5 IEEE 802.1x

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

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

Figure 45 Wireless Security: 802.1x



The following table describes the labels in this screen.

Table 18 Wireless 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.
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.

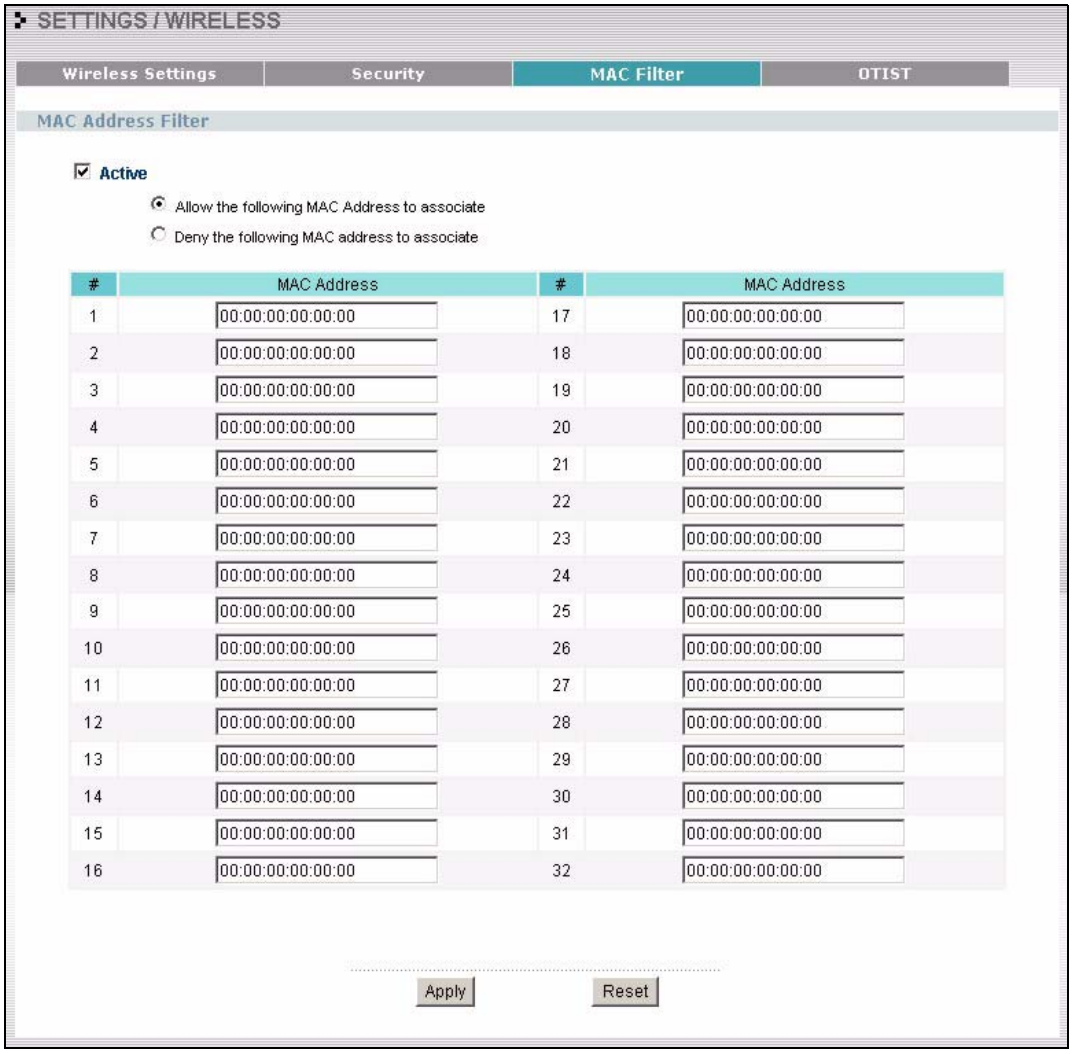
6.17 MAC Filter

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 **WIRELESS > SETTINGS > MAC Filter**. The screen appears as shown.

Note: 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.

Figure 46 MAC Filter



The following table describes the labels in this screen.

Table 19 MAC 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.

6.18 Introduction to OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as "AP" here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

Note: OTIST replaces the pre-configured wireless settings on the wireless clients.

6.18.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

Note: The AP and wireless client(s) MUST use the same **Setup key**.

6.18.1.1 AP

You can enable OTIST using the Reset button or the web configurator.

6.18.1.1.1 Reset button

If you use the **Reset** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

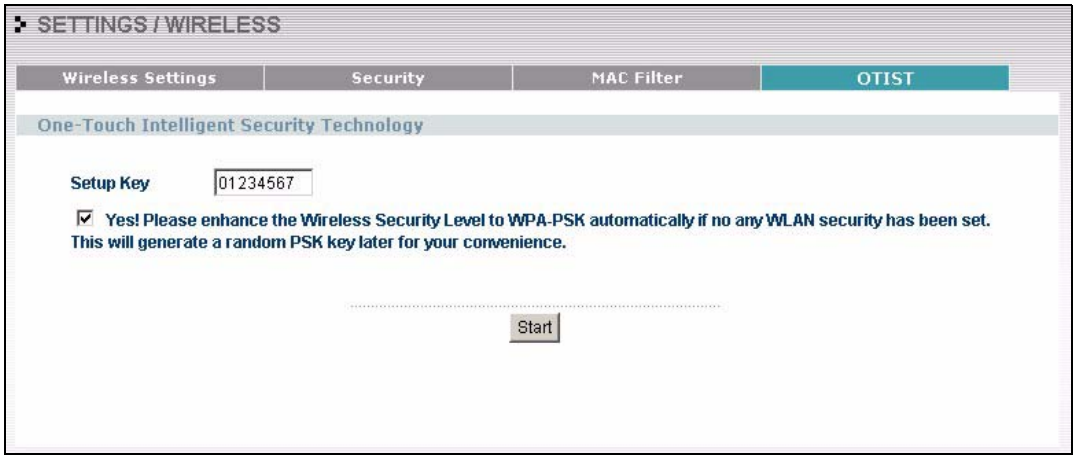
Hold in the **Reset** button for one or two seconds.

Note: If you hold in the **Reset** button too long, the device will reset to the factory defaults!

6.18.1.1.2 Web Configurator

Click **WIRELESS > SETTINGS > OTIST** to configure and enable OTIST. The screen appears as shown.

Figure 47 OTIST



The following table describes the labels in this screen.

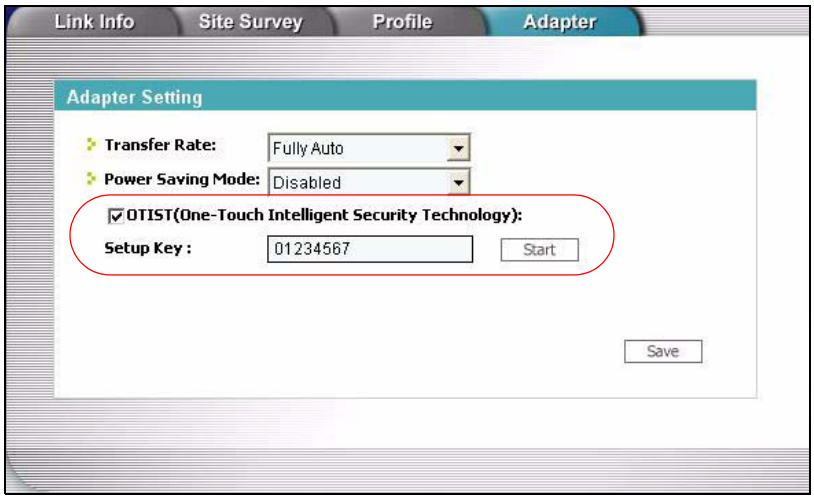
Table 20 OTIST

LABEL	DESCRIPTION
One-Touch Intelligent Security Technology	
Setup Key	Enter the setup key of up to eight printable characters. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key here, you must also make the same change on the wireless client(s).
Yes!	To have OTIST automatically generate a WPA-PSK key, select this check box. If you manually configured a WEP key or a WPA-PSK key and you also select this check box, then the key you manually configured is used.
Start	Click **Start** to encrypt the wireless security data using the setup key and have the G-560 set the wireless client to use the same wireless settings as the G-560. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.

6.18.1.2 Wireless Client

Start the ZyXEL utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP's and click **Save**.

Figure 48 Example Wireless Client OTIST Screen

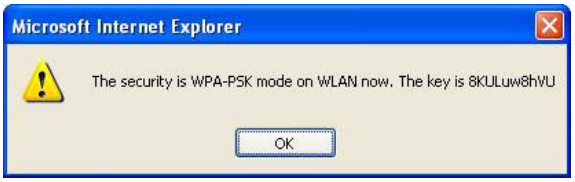


6.18.2 Starting OTIST

Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.

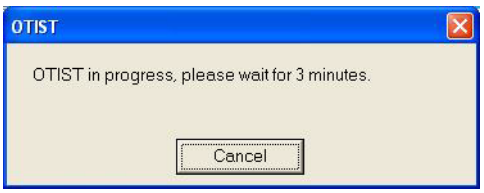
Figure 49 Security Key



2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

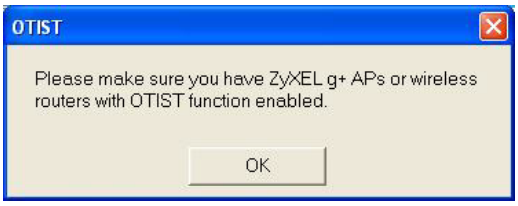
Figure 50 OTIST in Progress (AP)

Figure 51 OTIST in Progress (Client)



- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.

Figure 52 No AP with OTIST Found

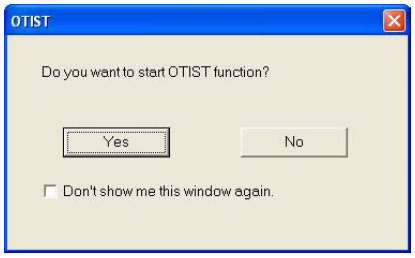


- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

6.18.3 Notes on OTIST

1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.

Figure 53 Start OTIST?



2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **Reset** button (for one or two seconds) for the AP to transfer settings.

4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).

5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

CHAPTER 7
Management Screens

This chapter describes the Maintenance screens.

7.1 Maintenance Overview

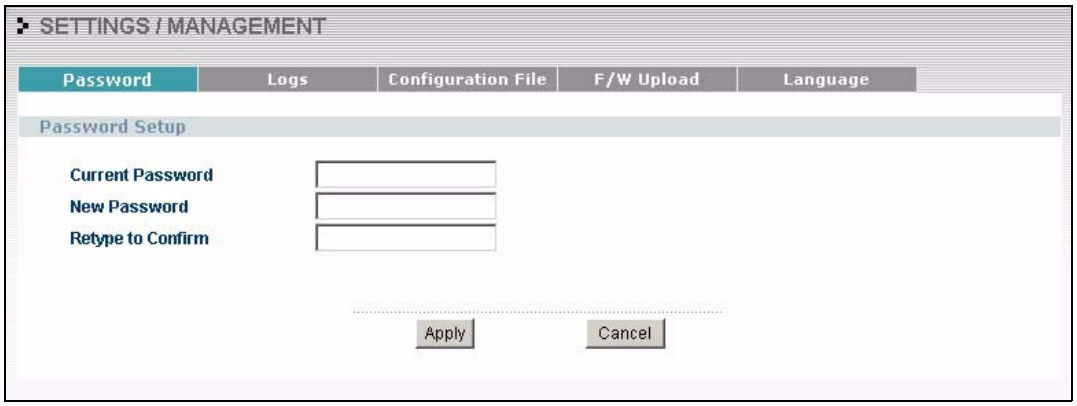
Use these maintenance screens to change the password, view logs, back up or restore the G-560 configuration and change the web configurator language.

7.2 Configuring Password

To change your G-560's password (recommended), click **SETTINGS > 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 54 Management: Password



The following table describes the labels in this screen.

Table 21 Management: 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.

Table 21 Management: Password (continued)

LABEL	DESCRIPTION
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes back to the G-560.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

7.3 Logs

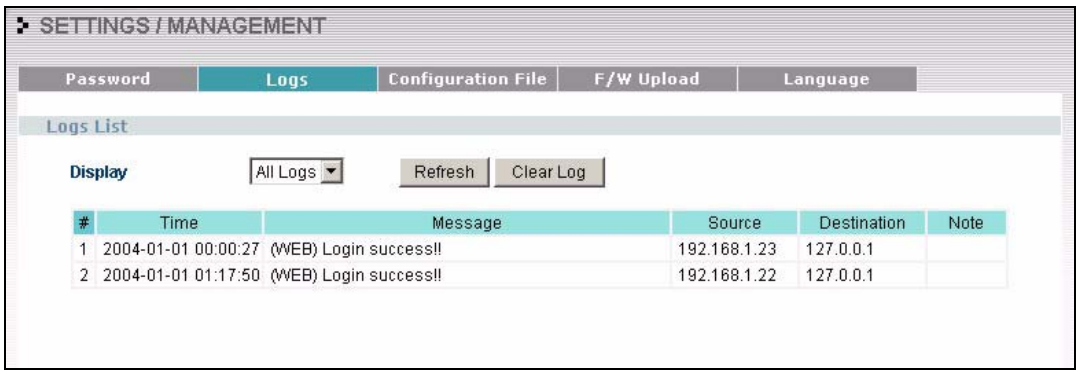
The web configurator allows you to look at all of the G-560's logs in one location.

Click **SETTINGS > MANAGEMENT > Logs** 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.

Figure 55 Management: Logs



The following table describes the labels in this screen.

Table 22 Management: Logs

LABEL	DESCRIPTION
Display	Select a category of logs to view.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.
#	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.

Table 22 Management: Logs (continued)

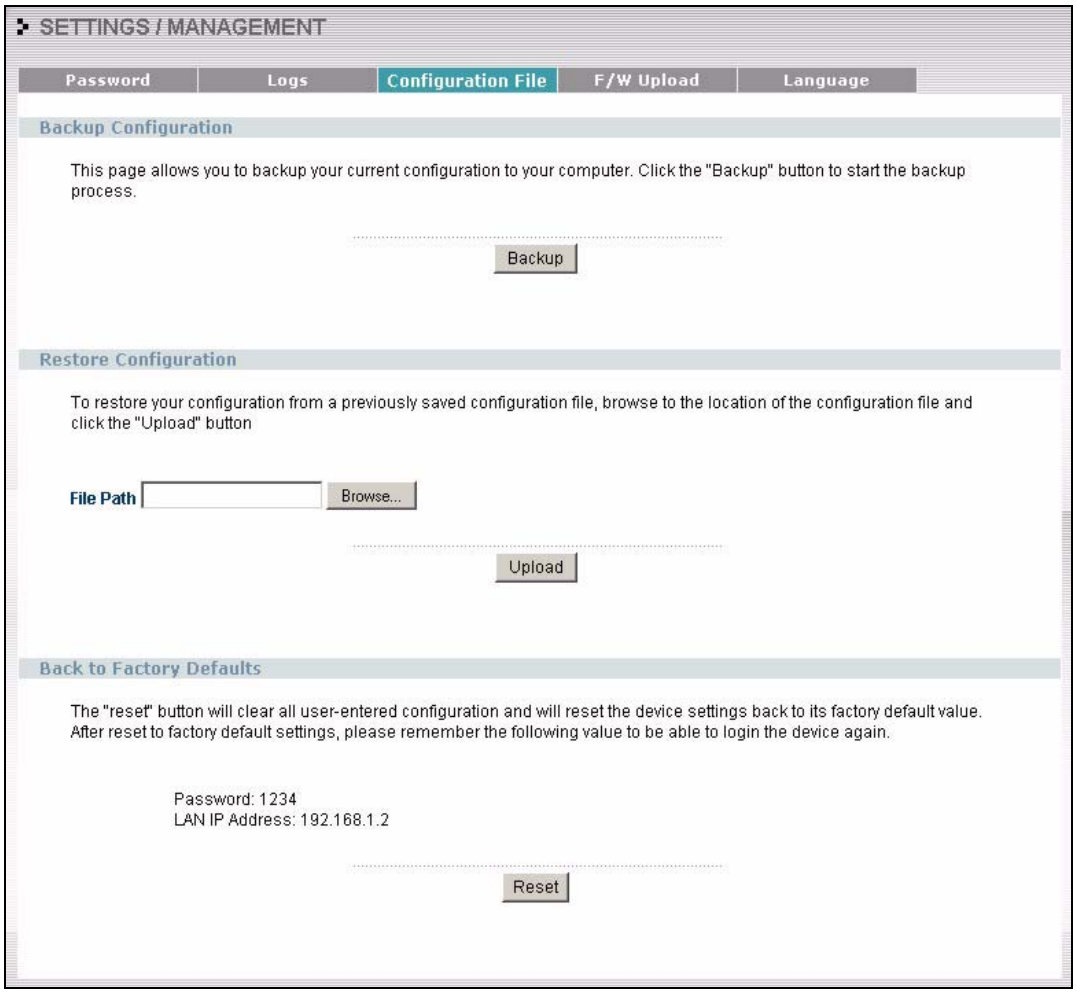
LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the outgoing packet that caused the log.
Note	This field displays additional information about the log entry.

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

Figure 56 Management: 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.

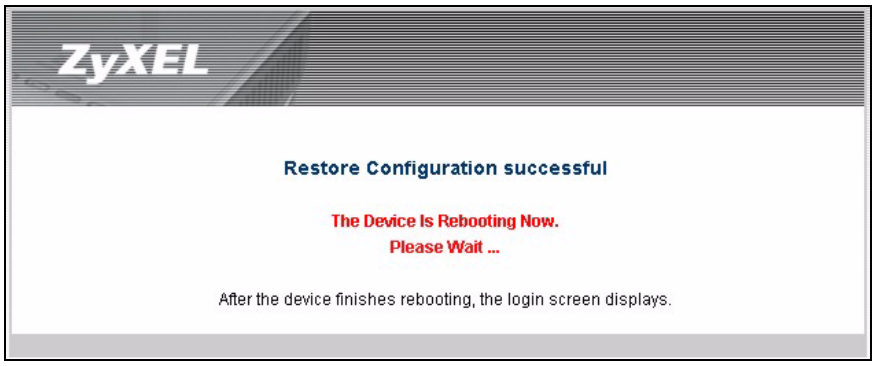
Table 23 Management: Configuration File: Restore Configuration

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

Note: Do not turn off the G-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.

Figure 57 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.

Figure 58 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).

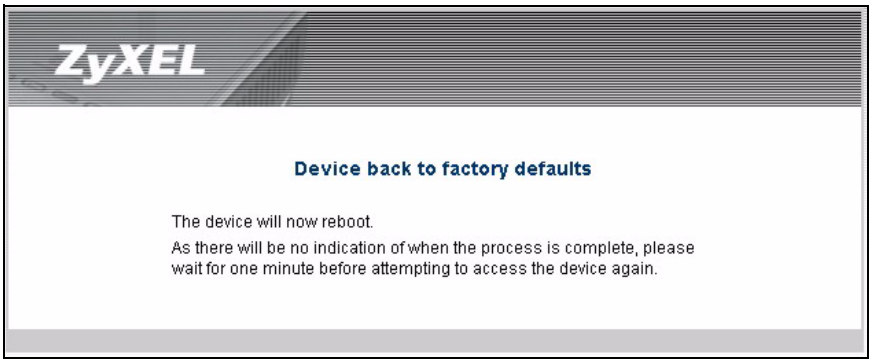
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration File** screen.

Figure 59 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.

Figure 60 Reset Warning Message



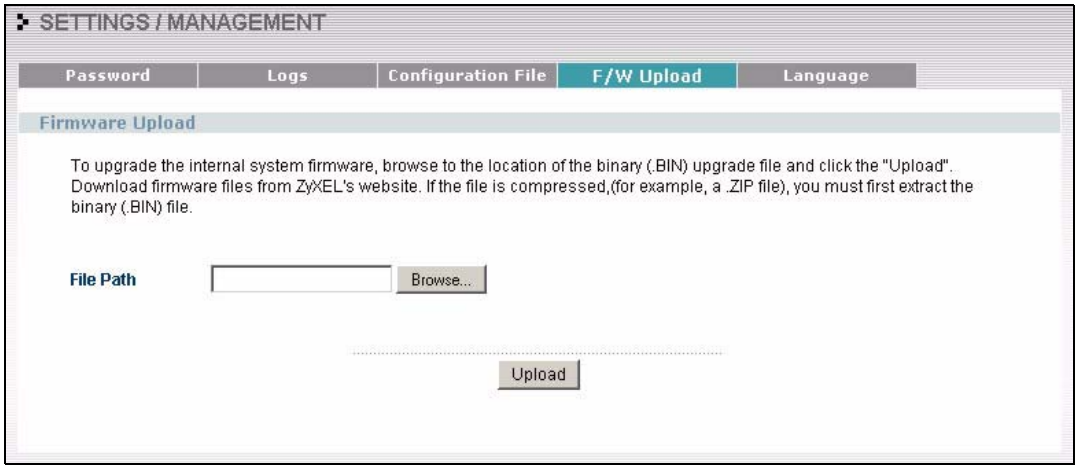
You can also press the **RESET** button on the rear panel to reset the factory defaults of your G-560. Refer to the section on resetting the G-560 for more information on the **RESET** button.

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 > F/W Upload** to display the screen as shown. Follow the instructions in this screen to upload firmware to your G-560.

Figure 61 Management: F/W Upload



The following table describes the labels in this screen.

Table 24 Management: F/W Upload

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

Note: Do not turn off the G-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.

Figure 62 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.

Figure 63 Network Temporarily Disconnected

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

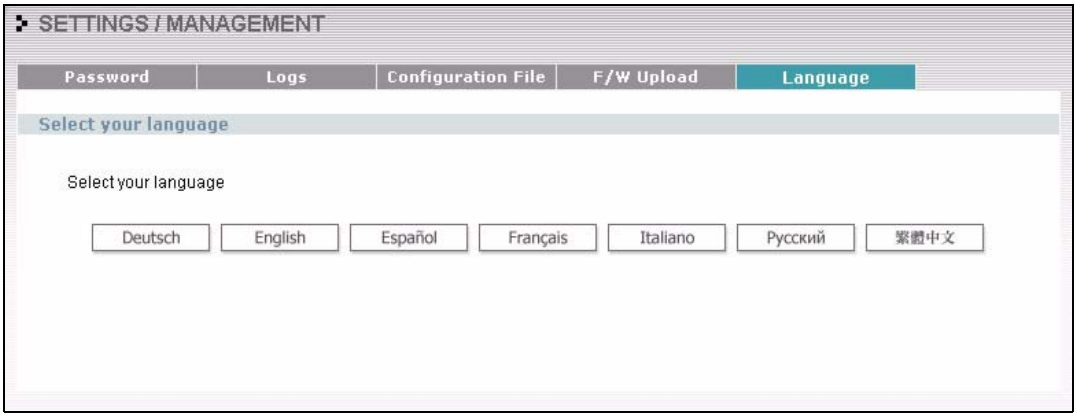
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 64 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 > Language**. Click the language you need.

Figure 65 Management: Language



CHAPTER 8
Troubleshooting

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

8.1 Problems Starting Up the G-560

Table 25 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.

8.2 Problems with the Password

Table 26 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.

8.3 Problems with the WLAN Interface

Table 27 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.

8.4 Problems with the Ethernet Interface

Table 28 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I 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.
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.

Table 28 Troubleshooting the Ethernet Interface (continued)

PROBLEM	CORRECTIVE ACTION
Cannot access the web configurator.	Your computer's and the G-560's IP addresses must be on the same subnet for LAN access. If you changed the G-560's IP address, then enter the new one as the URL. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

8.4.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

8.4.1.1 Internet Explorer Pop-up Blockers

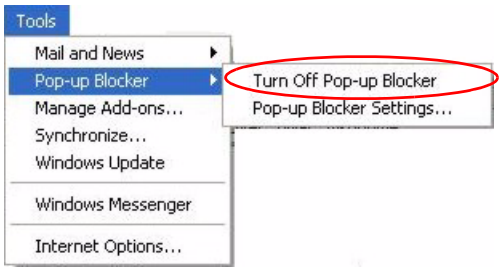
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

8.4.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 66 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 67 Internet Options

3 Click **Apply** to save this setting.

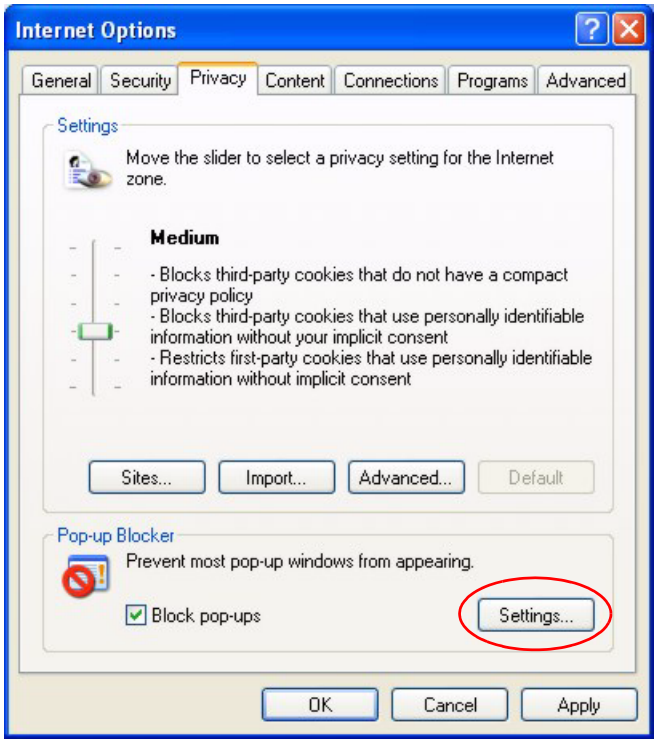
8.4.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 68 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 69 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

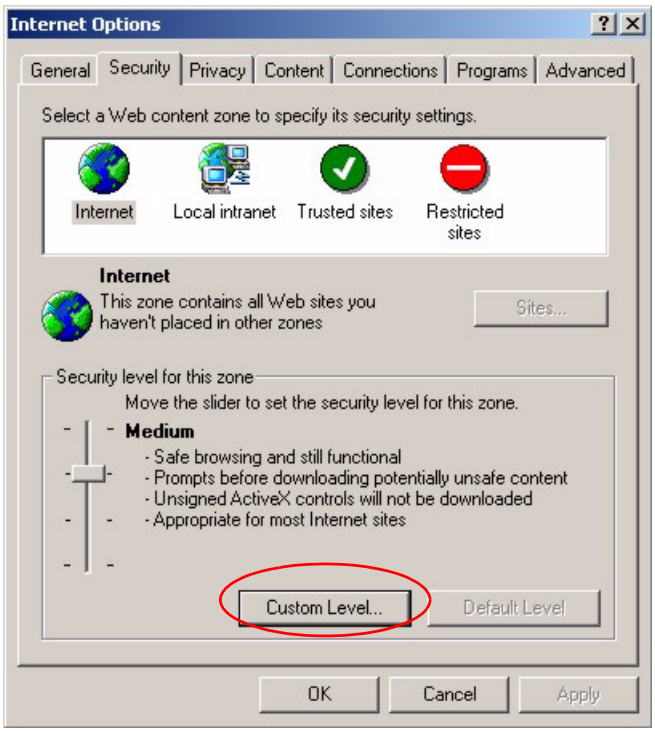
6 Click **Apply** to save this setting.

8.4.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 70 Internet Options



2 Click the **Custom Level...** button.

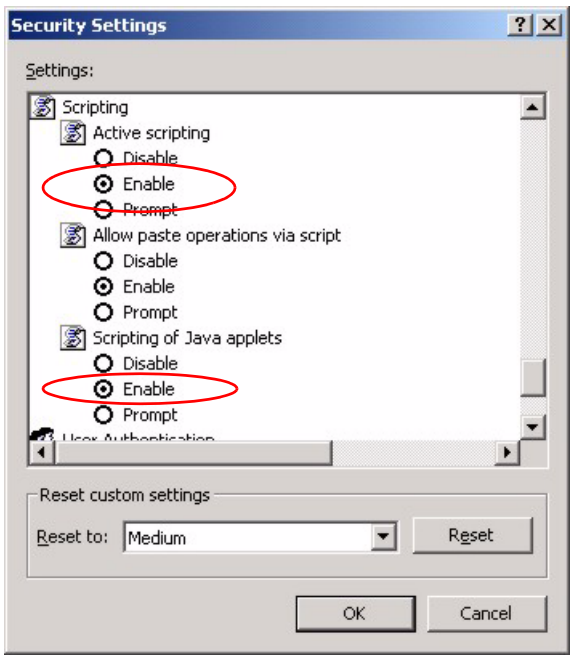
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 71 Security Settings - Java Scripting



8.4.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

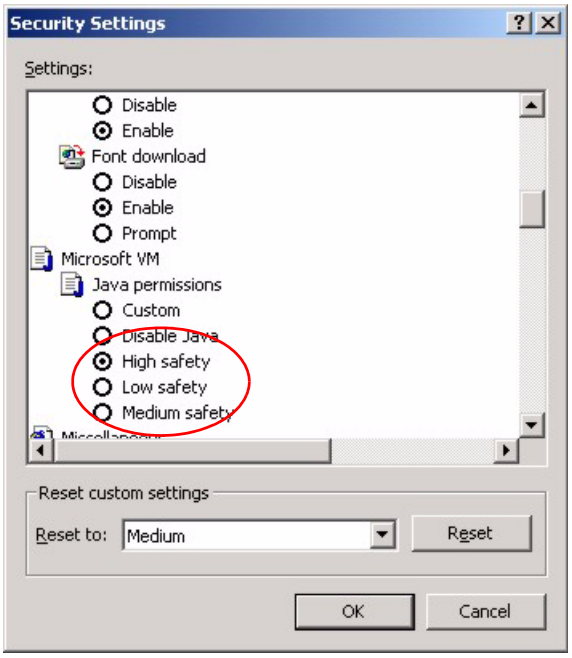
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

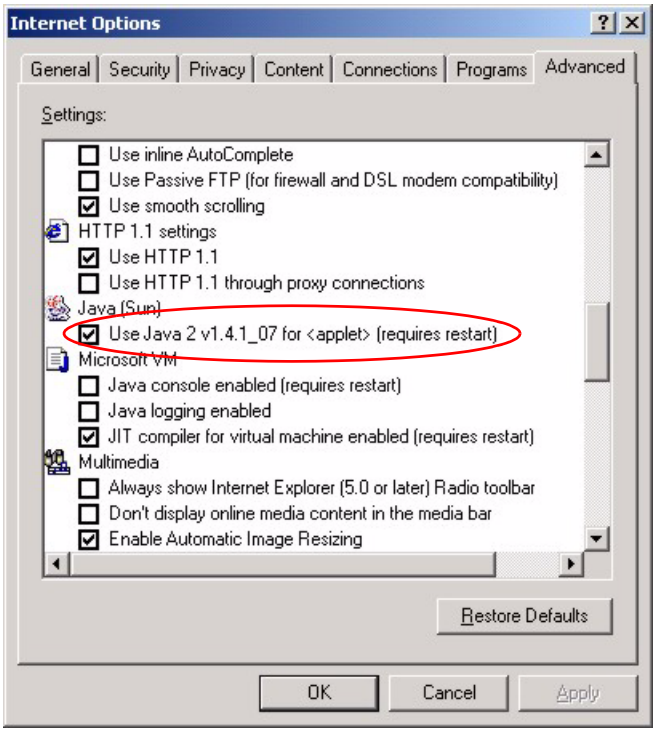
Figure 72 Security Settings - Java



8.4.1.3.1 JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 73 Java (Sun)



8.5 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.

Figure 74 Pinging the G-650

```
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
```

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

APPENDIX A
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.

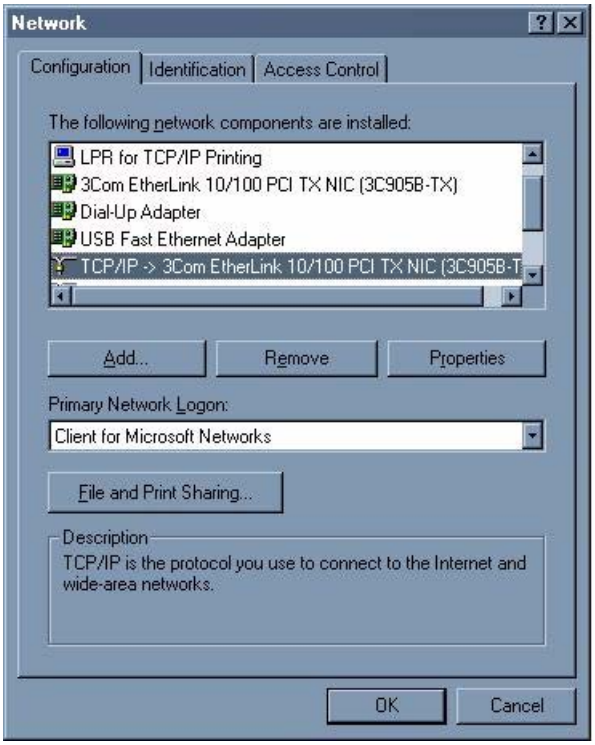
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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.

Figure 75 WIndows 95/98/Me: Network: Configuration



Installing Components

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

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

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

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

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

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

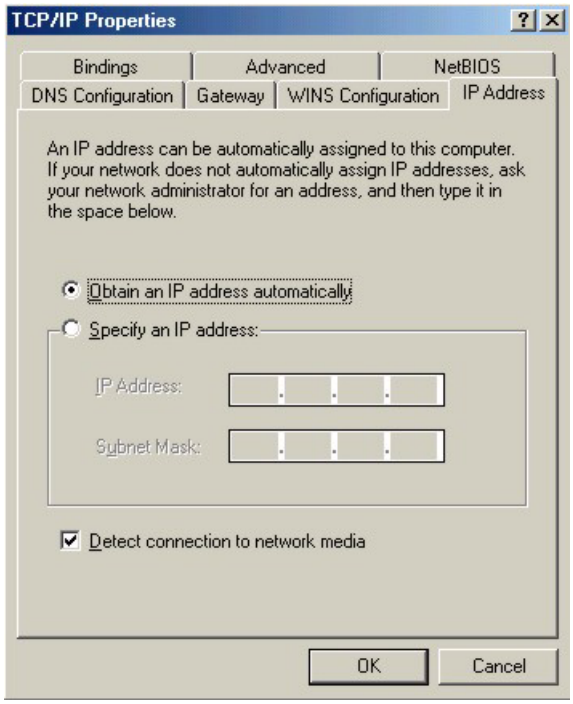
Configuring

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

2 Click the **IP Address** tab.

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

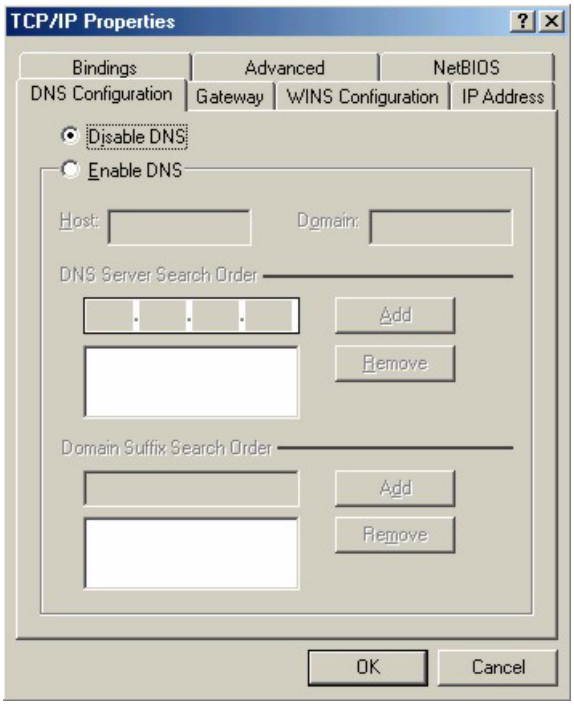
Figure 76 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

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

Figure 77 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

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

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

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

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

Verifying Settings

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

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

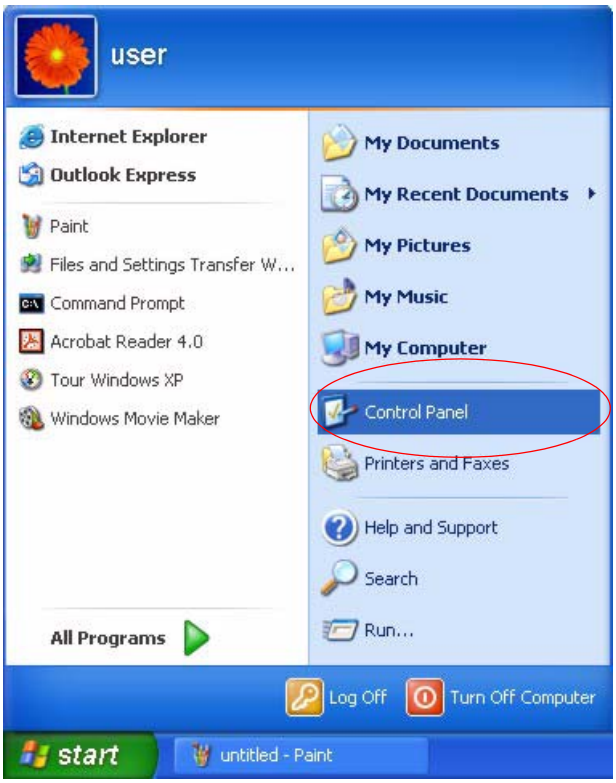
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

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

Figure 78 Windows XP: Start Menu

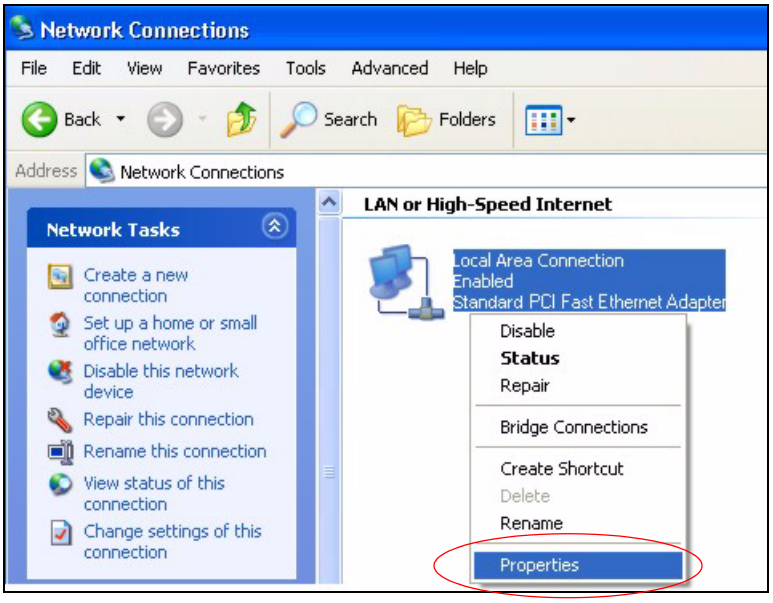


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 79 Windows XP: Control Panel

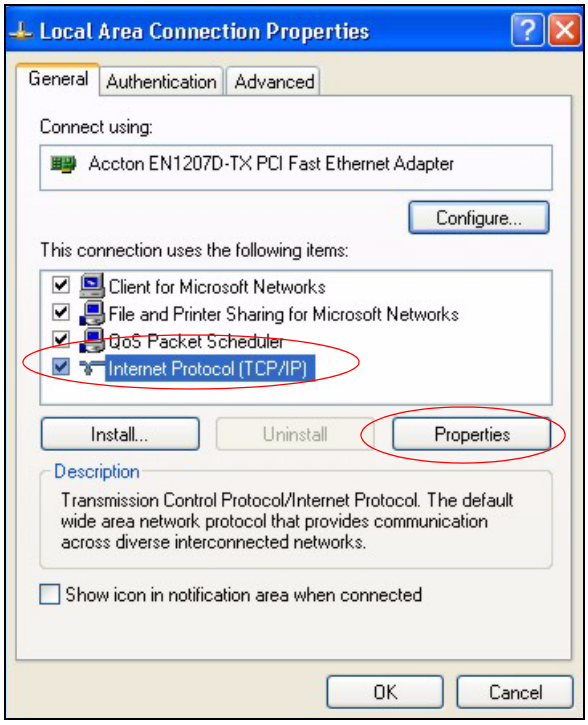
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 80 Windows XP: Control Panel: Network Connections: Properties



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

Figure 81 Windows XP: Local Area Connection Properties

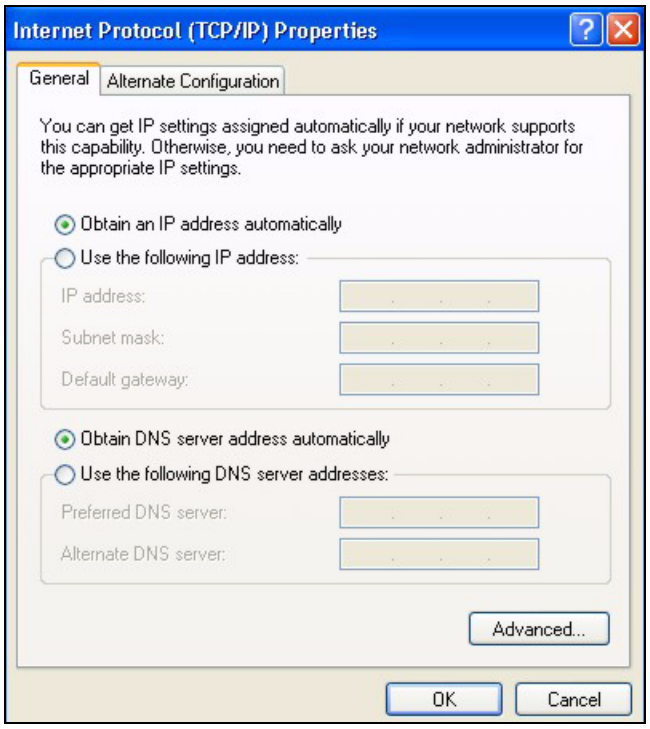


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

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

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

Figure 82 Windows XP: Internet Protocol (TCP/IP) Properties

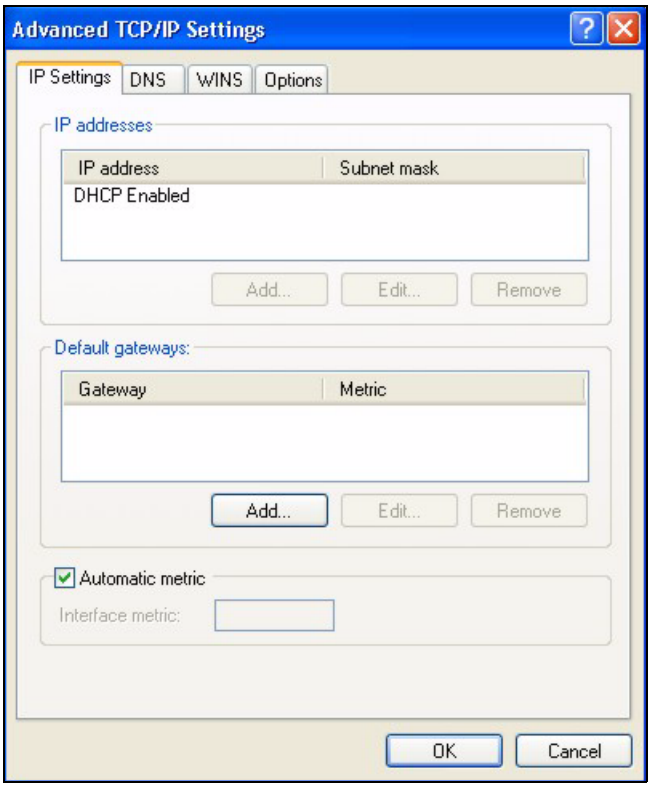


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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.

Figure 83 Windows XP: Advanced TCP/IP Properties

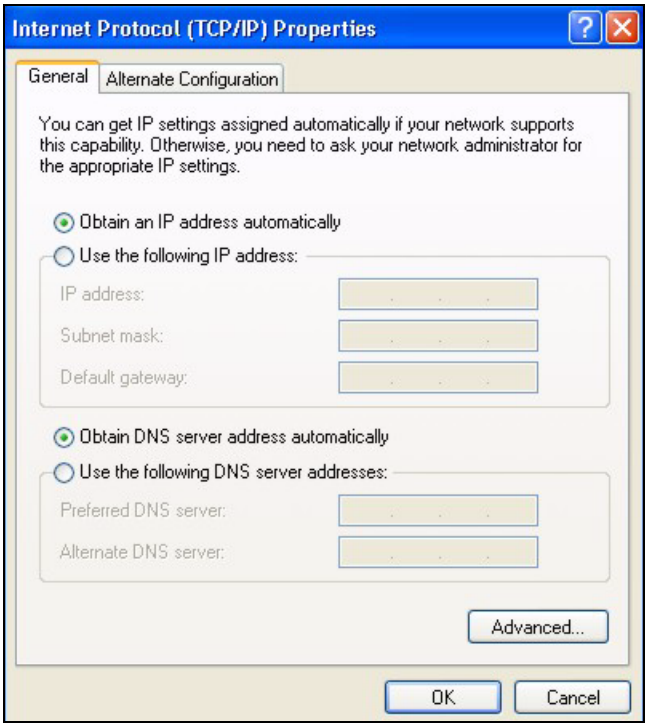


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

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

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

Figure 84 Windows XP: Internet Protocol (TCP/IP) Properties



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 Settings

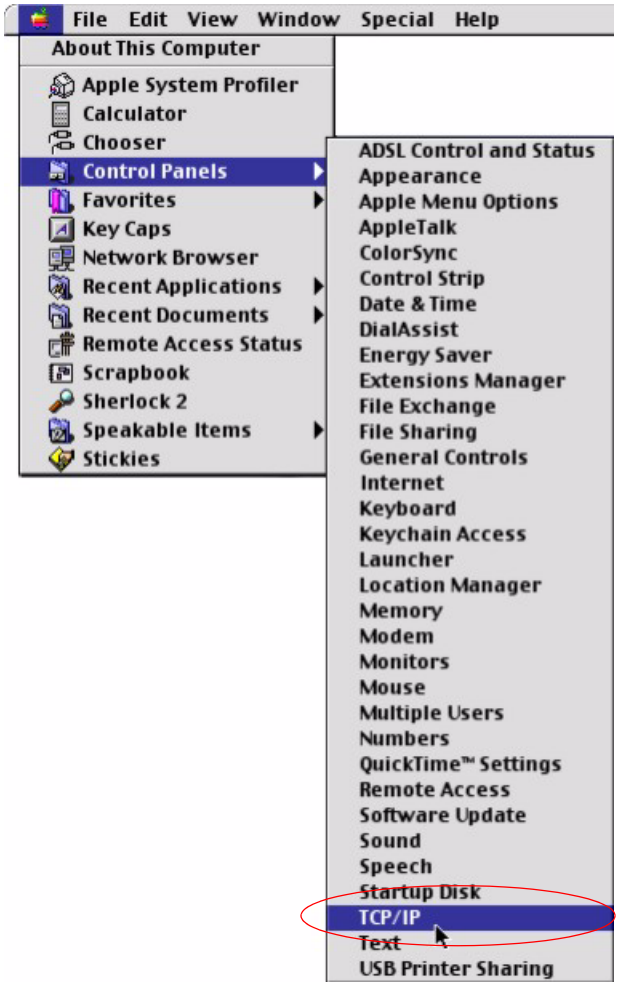
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

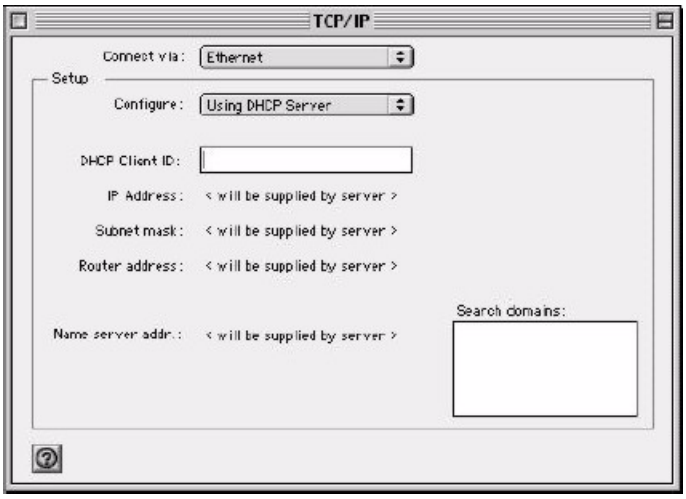
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 85 Macintosh OS 8/9: Apple Menu



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

Figure 86 Macintosh OS 8/9: TCP/IP



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).

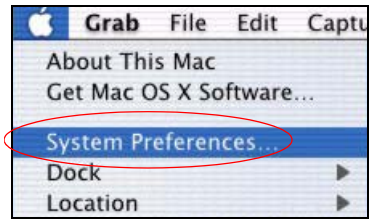
Verifying Settings

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

Macintosh OS X

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

Figure 87 Macintosh OS X: Apple Menu

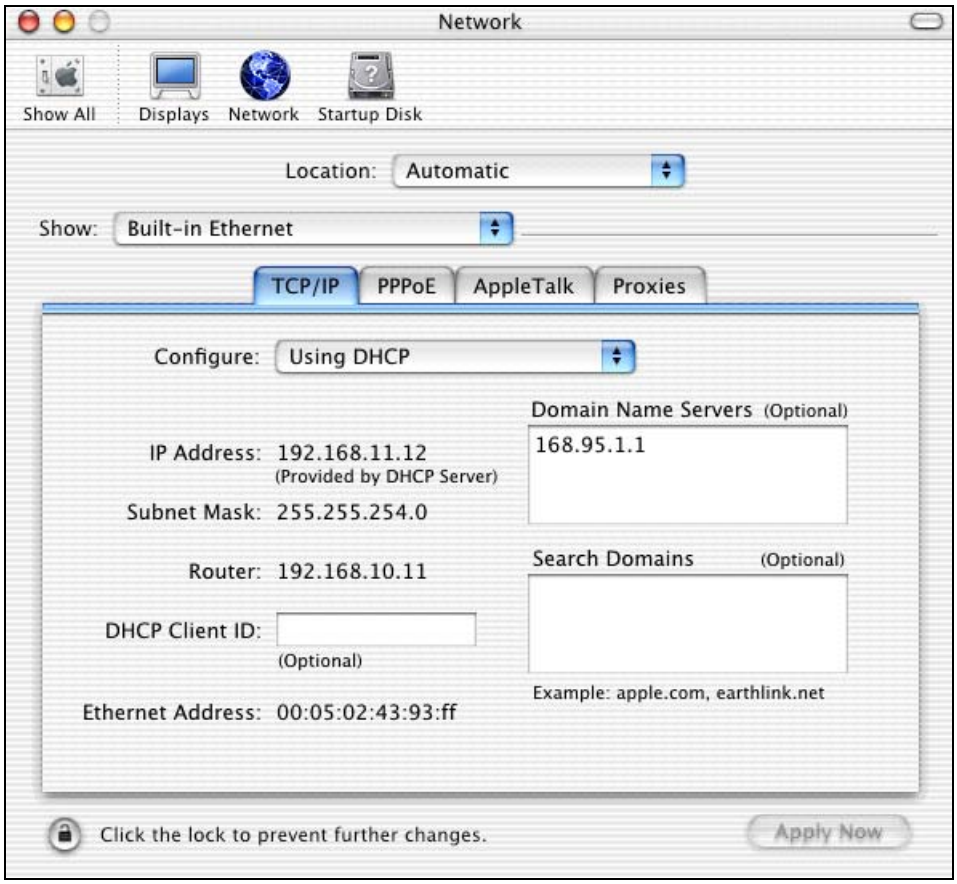


2 Click **Network** in the icon bar.

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

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

Figure 88 Macintosh OS X: Network



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 Settings

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

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

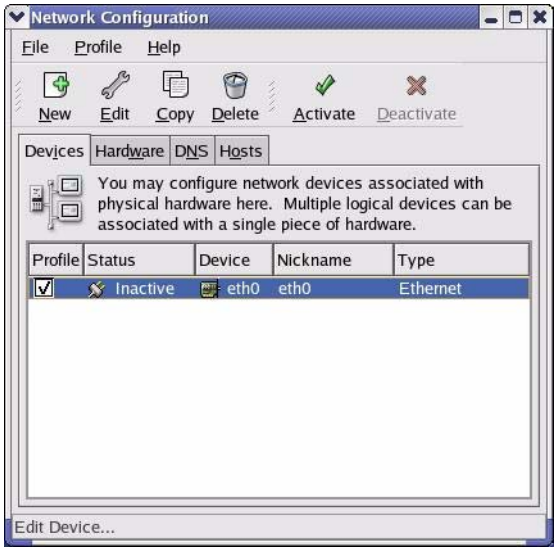
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 89 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

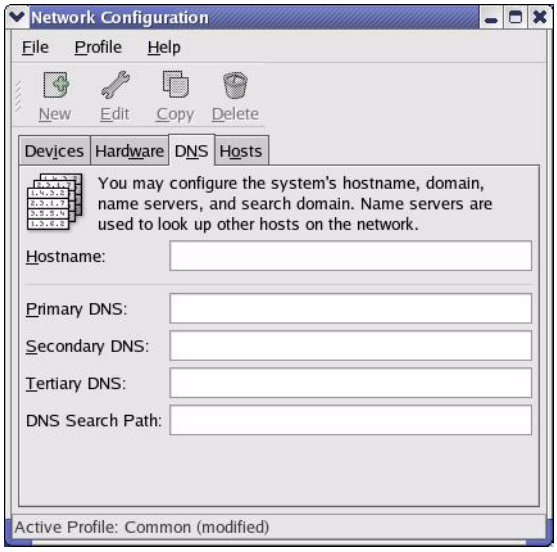
Figure 90 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 91 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 92 Red Hat 9.0: KDE: Network Configuration: Activate

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 93 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 94 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 95 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 96 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 97 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

APPENDIX B
Wireless LANs

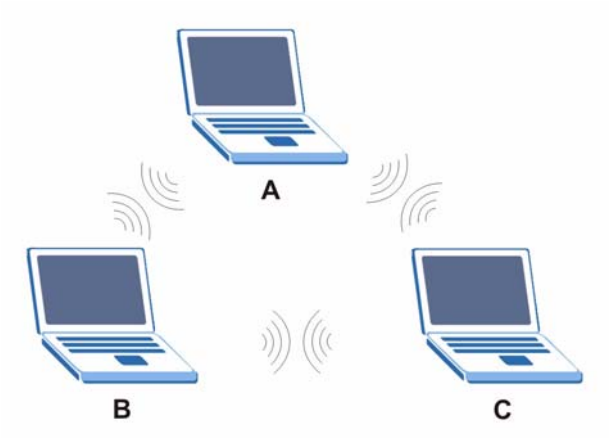
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

Figure 98 Peer-to-Peer Communication in an Ad-hoc Network

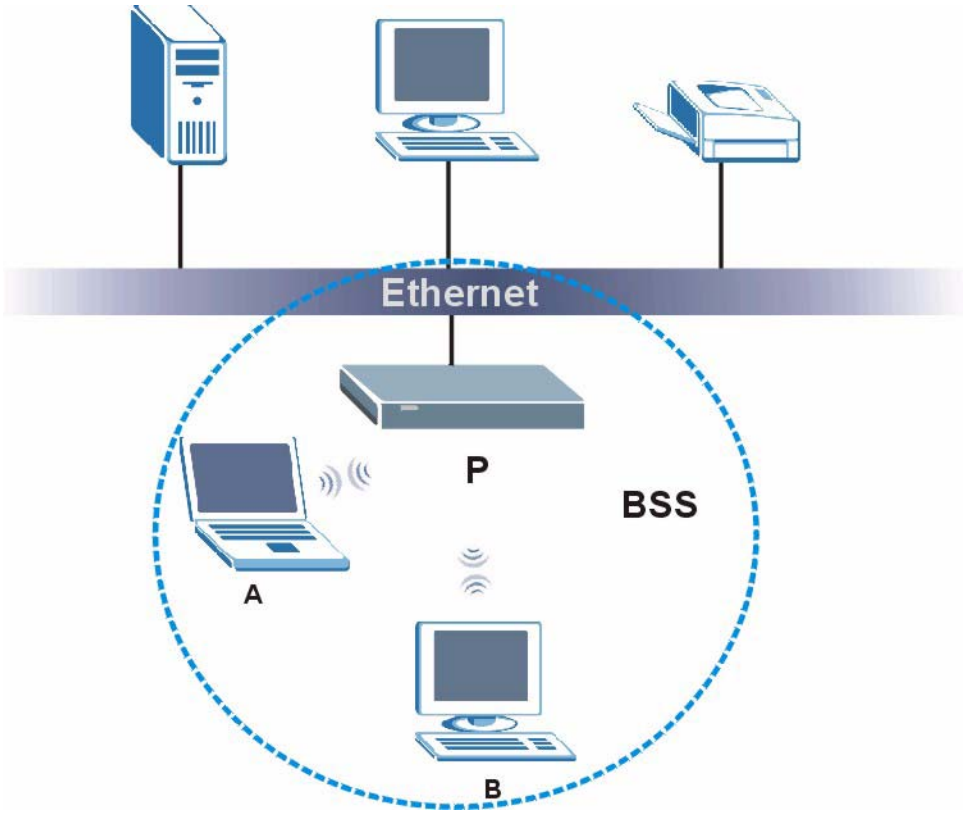


BSS

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

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

Figure 99 Basic Service Set



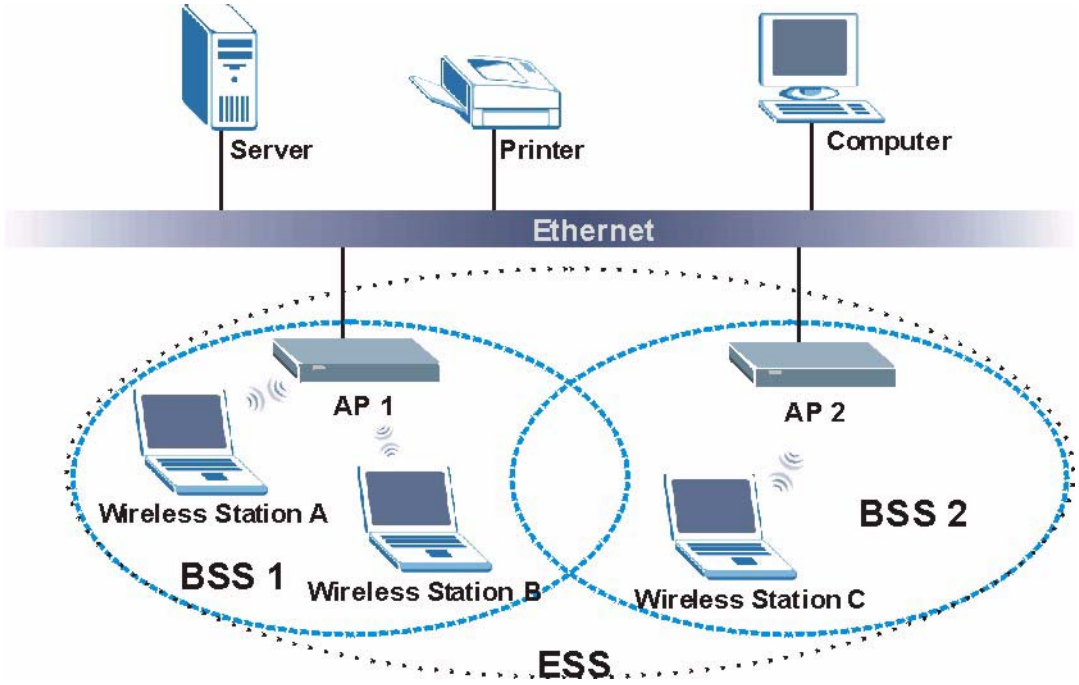
ESS

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

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

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

Figure 100 Infrastructure WLAN



Channel

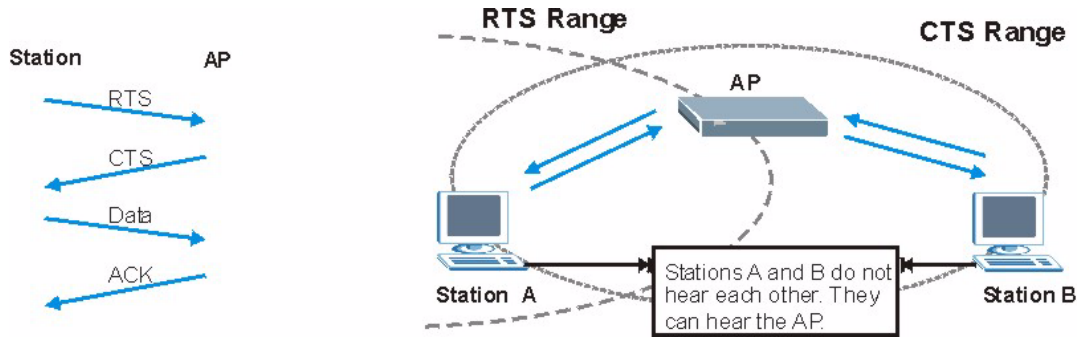
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs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

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

RTS/CTS

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

Figure 101 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.

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

Fragmentation Threshold

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

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

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

IEEE 802.11g Wireless LAN

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

Table 29 IEEE802.11g

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

IEEE 802.1x

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

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

RADIUS

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

- Authentication

  Determines the identity of the users.

- Authorization

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

- Accounting

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

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

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

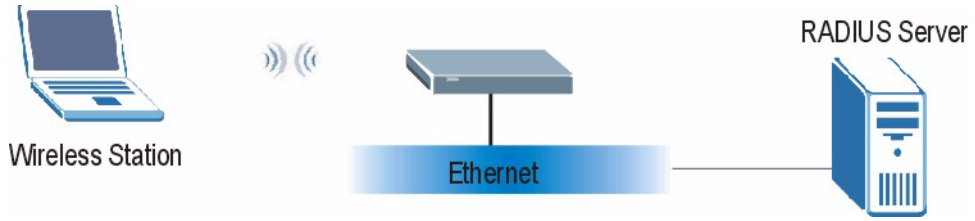
EAP Authentication

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

Figure 102 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

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

Types of Authentication

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

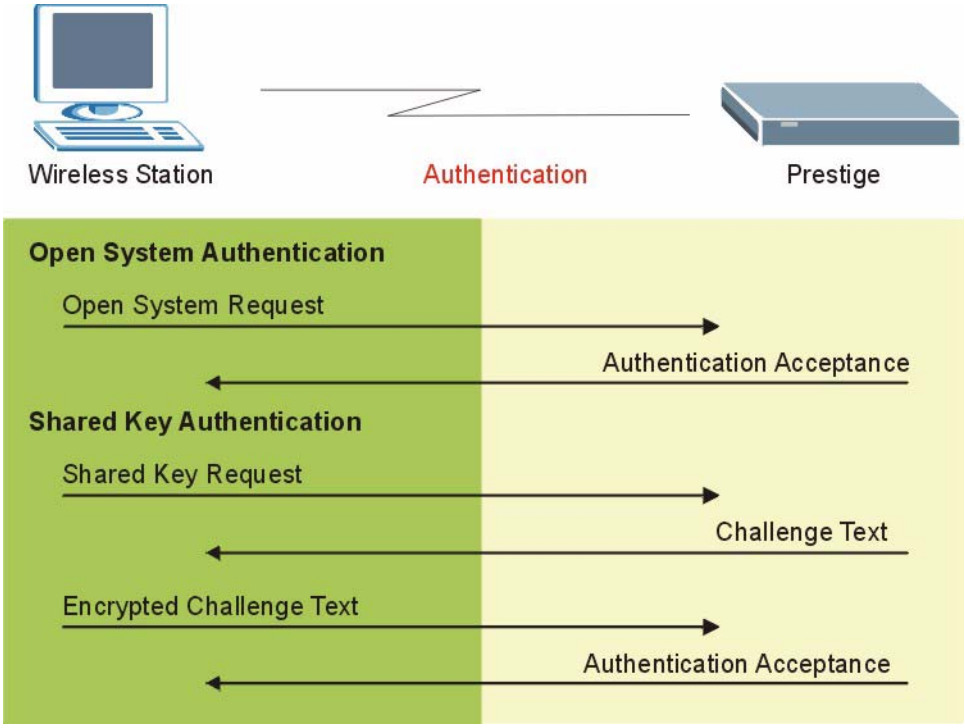
WEP Encryption

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

WEP Authentication Steps

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

Figure 103 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 device 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 device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

Dynamic WEP Key Exchange

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

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

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

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

Table 30 Comparison of EAP Authentication Types

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

WPA(2)

User Authentication

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

Encryption

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

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

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

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

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decrypt 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.

Roaming

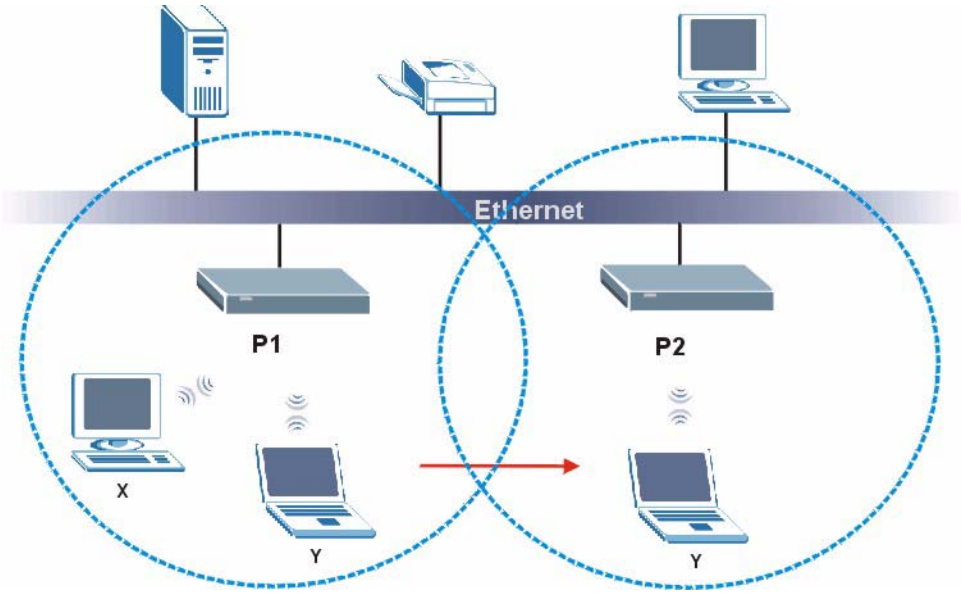
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access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

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

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 104.

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

Figure 104 Roaming Example



The steps below describe the roaming process.

1. As wireless station **Y** moves from the coverage area of access point **P1** to that of access point
2. **P2**, it scans and uses the signal of access point **P2**.
3. Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
4. Access point **P1** updates the new position of wireless station.
5. Wireless station **Y** sends a request to access point **P2** for re-authentication.

Requirements for Roaming

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

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.

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

APPENDIX C
IP Subnetting

IP Addressing

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

IP Classes

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

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

Table 31 Classes of IP Addresses

			OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

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

Therefore:

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

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

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

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

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

Table 32 Allowed IP Address Range By Class

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

Subnet Masks

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

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

Table 33 "Natural" Masks

	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

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

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

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

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

Table 34 Alternative Subnet Mask Notation

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

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

Example: Two Subnets

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

Table 35 Two Subnets Example

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

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

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

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

Table 36 Subnet 1

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

Table 37 Subnet 2

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

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

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

Example: Four Subnets

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

Table 38 Subnet 1

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

Table 39 Subnet 2

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

Table 40 Subnet 3

		LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 41 Subnet 4

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

Example Eight Subnets

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

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

Table 42 Eight Subnets

	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

Table 43 Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

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

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 31 on page 133) available for subnetting.

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

Table 44 Class B Subnet Planning

	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z