NETGEAR ProSafe 802.11g Wireless Access Point WG102 Reference Manual

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10144-02
July 2008

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT and Vista are registered trademarks of Microsoft Corporation.Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

FCC Statement.

Declaration of Conformity

We Netgear,
4500 Great America Parkway
Santa Clara, CA 95054, USA
Tel: +1 408 907 8000
declare under our sole responsibility that the product(s)
WG102 *(Model Designation)*
802.11g ProSafe Wireless Access Point *(Product Name)*
complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

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

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or locate the receiving antenna.
- Increase the separation between the equipment and 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.

Placement and Range Guidelines

Indoors, computers can connect over 802.11 wireless networks at a maximum range of several hundred feet for 802.11b/g devices. However, the operating distance or range of your wireless connection can vary significantly, based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and 2.4 GHz cordless phones.
- In an elevated location such as a high shelf that is near the center of the wireless coverage area for all mobile devices.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

RF Exposure Warning for North America, and Australia

Warning! To meet FCC and other national safety guidelines for RF exposure, the antennas for this device (see below) must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be colocated with other antenna or radio transmitter.

Antenna Statement for North America and Australia

In addition to its own antenna, the WG102 device has been approved for use with the following detachable antennas and antenna cables.

.

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Antenna Cable Length	Maximum Transmitted Power[1]
NETGEAR ANT24D18	18 dBi, directional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 18 dBi ant.
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 9 dBi ant.
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 5 dBi ant.

[1] WG102 maximum radiated power in North America and Australia: 19 dBm – cable loss + antenna gain

Please go to *www.netgear.com/go/wg102_fcc* for an updated list of wireless accessories approved to be used with the WAG302 in North America and Australia.

Industry Canada Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference Causing Equipment Regulations ICES 003.

Cet appareil numerique de classe B respecte les exigences du reglement du Canada sur le materiel brouilleur NMB-003.

The device is certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

Europe - EU Declaration of Conformity

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WG102 product package.

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento NETGEAR WG102 ProSafe 802.11g Wireless Access Point je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr NETGEAR WG102 ProSafe 802.11g Wireless Access Point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät NETGEAR WG102 ProSafe 802.11g Wireless Access Point in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme NETGEAR WG102 ProSafe 802.11g Wireless Access Point vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this NETGEAR WG102 ProSafe 802.11g Wireless Access Point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el NETGEAR WG102 ProSafe 802.11g Wireless Access Point cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NETGEAR WG102 ProSafe 802.11g Wireless Access Point ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil NETGEAR WG102 ProSafe 802.11g Wireless Access Point est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo NETGEAR WG102 ProSafe 802.11g Wireless Access Point è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka NETGEAR WG102 ProSafe 802.11g Wireless Access Point atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis NETGEAR WG102 ProSafe 802.11g Wireless Access Point atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel NETGEAR WG102 ProSafe 802.11g Wireless Access Point in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan NETGEAR WG102 ProSafe 802.11g Wireless Access Point jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a NETGEAR WG102 ProSafe 802.11g Wireless Access Point megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e NETGEAR WG102 ProSafe 802.11g Wireless Access Point jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este NETGEAR WG102 ProSafe 802.11g Wireless Access Point está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta NETGEAR WG102 ProSafe 802.11g Wireless Access Point v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že NETGEAR WG102 ProSafe 802.11g Wireless Access Point spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että NETGEAR WG102 ProSafe 802.11g Wireless Access Point tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Antenna Statement for the European Community

Please note that the 100mW EIRP limit and regulations could vary in Europe from country to country. Please check the regulations in your country.

The antenna cable type and length must comply with European regulations. Refer to the table below for approved antenna and cable accessories.

In addition to its own antenna, the WG102 device has been approved for use with the following detachable antennas and antenna cables:

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Minimum Antenna Cable Length	Minimum Antenna Cable Attenuation	Maximum Transmitted Power[1]
NETGEAR ANT24D18	18 dBi, directional outdoor/indoor	NETGEAR ACC-10314-05	30 m	18 dB	-3 dBm + 18 dBi = 15 dBm EIRP
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-04 or ACC-10314-05	10 m	6.1 dB	8.9 dBm + 9 dBi = 17.9 dBm EIRP
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m	1.1 dB	14 dBm + 5 dBi = 19 dBm EIRP

[1] WG102 maximum radiated power in the European Community: 15 dBm – cable loss + antenna gain

Please go to *http://www.netgear.com* and use the search feature to find an updated list of wireless accessories approved to be used with the WG102 in the European Community.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das NETGEAR WG102 ProSafe 802.11g Wireless Access Point gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the NETGEAR WG102 ProSafe 802.11g Wireless Access Point has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Product and Publication Details

Model Number:	WG102
Publication Date:	July 2008
Product Family:	Wireless Access Point
Product Name:	NETGEAR WG102 ProSafe 802.11g Wireless Access Point
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10144-02

Contents

About This Manual

Chapter 1
Basic Installation and Configuration

Chapter 2
Configuring Security

Chapter 3
Management

Chapter 4
Advanced Configuration

Chapter 5
Troubleshooting

Appendix A
Factory Default Settings and Specifications

About This Manual

The *NETGEAR® WG102 ProSafe 802.11g Wireless Access Point Reference Manual* describes how to install, configure and troubleshoot the NETGEAR WG102 ProSafe 802.11g Wireless Access Point. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions::

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

➡	**Note:** This format is used to highlight information of importance or special interest.

💡	**Tip:** This format is used to highlight a procedure that will save time or resources.

⚠	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

- **Scope**. This manual is written for the WG102 Access Point according to these specifications:

Product Version	NETGEAR WG102 ProSafe 802.11g Wireless Access Point
Manual Publication Date	July 2008

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents."

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forward or backward through the manual one page at a time.
- A ☰ button that displays the table of contents and a button that displays an index. Double-click a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print This Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - **Printing a PDF chapter.** Use the **PDF of This Chapter** link at the top left corner of any page.

    - Click the **PDF of This Chapter** link at the top left corner of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
- **Printing a PDF version of the complete manual**. Use the **Complete PDF Manual** link at the top left corner of any page.
    - Click the **Complete PDF Manual** link at the top left corner of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left corner of your browser window.

> **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10144-02	1.0	July 2008	New firmware
202-10144-01	1.0	July 2006	Original Publication

Chapter 1
Basic Installation and Configuration

This chapter describes how to set up your NETGEAR WG102 ProSafe 802.11g Wireless Access Point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b or 802.11g wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.

System Requirements

Before installing the WG102, make sure your system meets these requirements:

- A 10/100 Mbps Local Area Network device such as a hub or switch.
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 HZ AC power source.
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.
- At least one computer with the TCP/IP protocol installed.
- 802.11g or 802.11b-compliant devices, such as the NETGEAR WG511 Wireless Adapter.

What Is In the Box?

The product package should contain the following items:

- NETGEAR WG102 ProSafe 802.11g Wireless Access Point.
- Power adapter and cord.
- Straight through Category 5 Ethernet cable.
- 802.11g ProSafe Wireless Access Point Installation Guide WG102.
- *Resource CD.*
- Installation Guide for the NETGEAR WG102 ProSafe 802.11g Wireless Access Point.

- Support Registration card.

Contact your reseller or customer support in your area if there are any missing or damaged parts. See the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WG102 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.NETGEAR.com*.

Hardware Description

The NETGEAR WG102 ProSafe 802.11g Wireless Access Point front and rear hardware functions are described below.

Front Panel

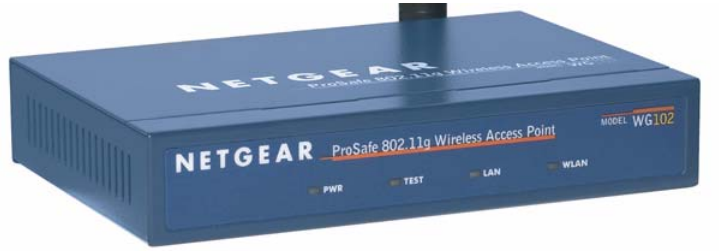


Figure 1-1

Viewed from left to right, the WG102 has these four status LEDs: PWR, TEST, LAN, and WLAN.

LED	Description	
PWR	Power Indicator	
	Off	No power. If this LED does not come on with the power adapter and cord correctly installed, see Chapter 5, “Troubleshooting.
	On	Power is on.
TEST	Self Test Indicator	
	Blink	Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off.

LED	Description	
LAN	Ethernet link indicator	
	Off	No connection detected on the Ethernet link
	Amber On	10 Mbps Ethernet link detected
	Amber Flashing	Data is being transmitted or received on the 10 Mbps Ethernet link
	Green On	100 Mbps Fast Ethernet link detected.
	Green Flashing	Data is being transmitted or received on the 100 Mbps Ethernet link
WLAN	Wireless LAN Link Activity Indicator	
	Off	No wireless link activity.
	Green Blink	Wireless link activity.

Rear Panel

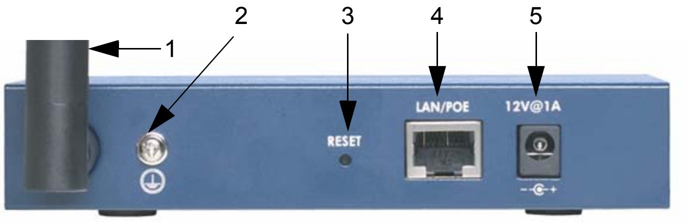


Figure 1-2

Viewed from left to right, the back of the WG102 provides the following:

1. Detachable antenna.
2. Ground.
3. Reset button. This restores the default factory settings.
4. RJ-45 Ethernet LAN/POE Port. Use the WG102 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or Power Over Ethernet (POE) switch.
5. Power socket. This connects to the WG102 power adapter.

Cabling Requirements

The WG102 Access Point connects to your LAN via twisted-pair Category 5 Ethernet cable with RJ-45 connectors.

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WG102. For complete performance specifications, see Appendix A, "Factory Default Settings and Specifications".

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate. In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones, large metal surfaces, or water.
- Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is five Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings, and placement.

Installing the WG102 Access Point

Before installing the WG102 Access Point, make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network. Then computers with 802.11b or 802.11g wireless adapters will be able to communicate with the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown in "System Requirements" on page 1-1.

1. Set up the WG102 Access Point.

> **Tip:** Before mounting the WG102 Access Point in a high location, first set up and test the WG102 Access Point to verify wireless network connectivity.

a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

b. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.

c. Connect an Ethernet cable from the WG102 Access Point to the computer.

d. Turn on your computer, connect the power adapter to the WG102 and verify the following:

   – The PWR power light goes on.

   – The LAN light of the wireless access point is lit when connected to a powered on computer.

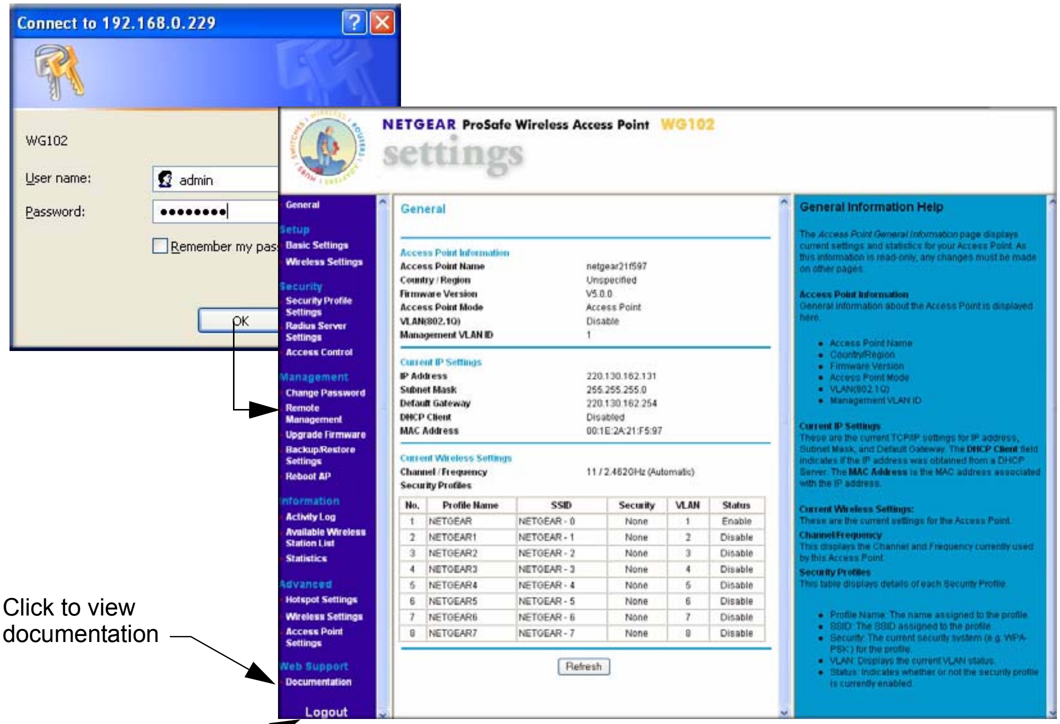
2. Configure LAN and wireless access.

a. Use your Web browser to connect to the WG102 Access Point.

– Enter **192.168.0.229** in the address field of your browser.

– When prompted, enter **admin** for the user name, and **password** for the password, both in lower case letters.

The Web browser displays the WG102 Access Point main menu and General screen, as shown below.



Connect to 192.168.0.229

WG102

User name: admin

Password: ••••••••

☐ Remember my pas

OK

NETGEAR ProSafe Wireless Access Point WG102

settings

General

Access Point Information

Access Point Name netgear21f597
Country / Region Unspecified
Firmware Version V5.0.0
Access Point Mode Access Point
VLAN(802.1Q) Disable
Management VLAN ID 1

Current IP Settings

IP Address 220.130.162.131
Subnet Mask 255.255.255.0
Default Gateway 220.130.162.254
DHCP Client Disabled
MAC Address 00:1E:2A:21:F5:97

Current Wireless Settings

Channel / Frequency 11 / 2.462GHz (Automatic)
Security Profiles

No.	Profile Name	SSID	Security	VLAN	Status
1	NETGEAR	NETGEAR - 0	None	1	Enable
2	NETGEAR1	NETGEAR - 1	None	2	Disable
3	NETGEAR2	NETGEAR - 2	None	3	Disable
4	NETGEAR3	NETGEAR - 3	None	4	Disable
5	NETGEAR4	NETGEAR - 4	None	5	Disable
6	NETGEAR5	NETGEAR - 5	None	6	Disable
7	NETGEAR6	NETGEAR - 6	None	7	Disable
8	NETGEAR7	NETGEAR - 7	None	8	Disable

Refresh

General Information Help

The *Access Point General Information* page displays current settings and statistics for your Access Point. As this information is read-only, any changes must be made on other pages.

Access Point Information
General information about the Access Point is displayed here.

- Access Point Name
- Country/Region
- Firmware Version
- Access Point Mode
- VLAN(802.1Q)
- Management VLAN ID

Current IP Settings
These are the current TCP/IP settings for IP address, Subnet Mask, and Default Gateway. The **DHCP Client** field indicates if the IP address was obtained from a DHCP Server. The **MAC Address** is the MAC address associated with the IP address.

Current Wireless Settings:
These are the current settings for the Access Point.

Channel/Frequency
This displays the Channel and Frequency currently used by this Access Point.

Security Profiles
This table displays details of each Security Profile.

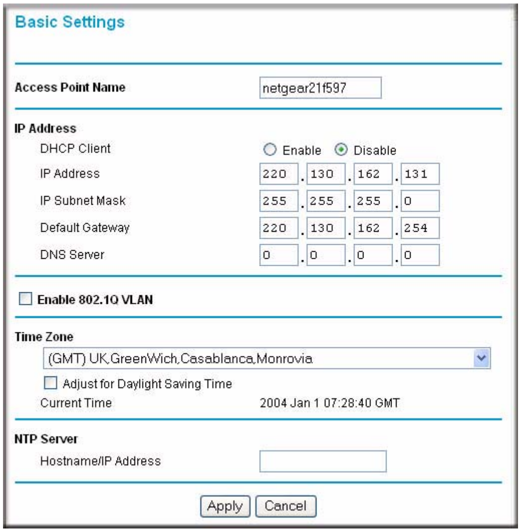
- Profile Name: The name assigned to the profile.
- SSID: The SSID assigned to the profile.
- Security: The current security system (e.g. WPA-PSK) for the profile.
- VLAN: Displays the current VLAN status.
- Status: Indicates whether or not the security profile is currently enabled.

Click to view documentation

Click to log out.
After 5 minutes with no activity,
you are logged out automatically.

Figure 1-3

b. On the main menu, select Basic Settings to view the Basic Settings screen.



Basic Settings

Access Point Name: netgear21f597

IP Address
- DHCP Client: ○ Enable ● Disable
- IP Address: 220 . 130 . 162 . 131
- IP Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 220 . 130 . 162 . 254
- DNS Server: 0 . 0 . 0 . 0

□ Enable 802.1Q VLAN

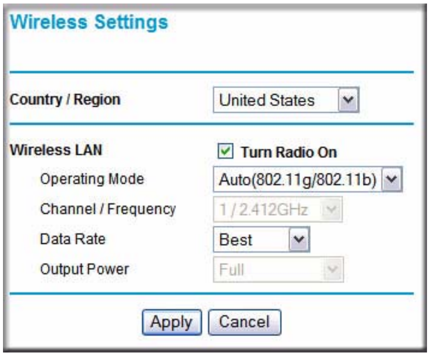
Time Zone
- (GMT) UK,GreenWich,Casablanca,Monrovia
- □ Adjust for Daylight Saving Time
- Current Time: 2004 Jan 1 07:28:40 GMT

NTP Server
- Hostname/IP Address:

Figure 1-4

Configure the settings for your network and click **Apply.**

c. Select Wireless Settings in the Setup section of the main menu to view the Wireless Settings screen.



Wireless Settings

Country / Region: United States

Wireless LAN: ☑ Turn Radio On
- Operating Mode: Auto(802.11g/802.11b)
- Channel / Frequency: 1 / 2.412GHz
- Data Rate: Best
- Output Power: Full

Figure 1-5

d. Enter the wireless settings. See the online help or "Wireless Settings" on page 1-12 for full instructions.

Note: In the US, the Country/Region is preset according to regulatory requirements. In other areas, you can and must set the Country/Region. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.

Now that you have finished the setup, you are ready to deploy the WG102 Access Point in your network. If needed, you can now reconfigure the computer you used in for this process back to its original TCP/IP settings.

3. Deploy the WG102 Access Point

a. Disconnect the WG102 Access Point and put it where you will deploy it. The best location is elevated, such as wall mounted, or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.

b. Lift the antenna on either side to be vertical.

Note: Consult the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter of this manual.

c. Connect an Ethernet cable from your WG102 Access Point to a LAN port on your router, switch, or hub.

Note: By default, the WG102 Access Point is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting..

d. Connect the power adapter to the wireless access point, and plug the power adapter in to a power outlet. The PWR, LAN, and WLAN lights should light up.

4. Verify wireless connectivity

Using a computer with an 802.11b or 802.11g wireless adapter with the correct wireless settings needed to connect to the WG102 Access Point (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Netscape or Internet Explorer to browse the Internet, or check for file and printer access on your network.

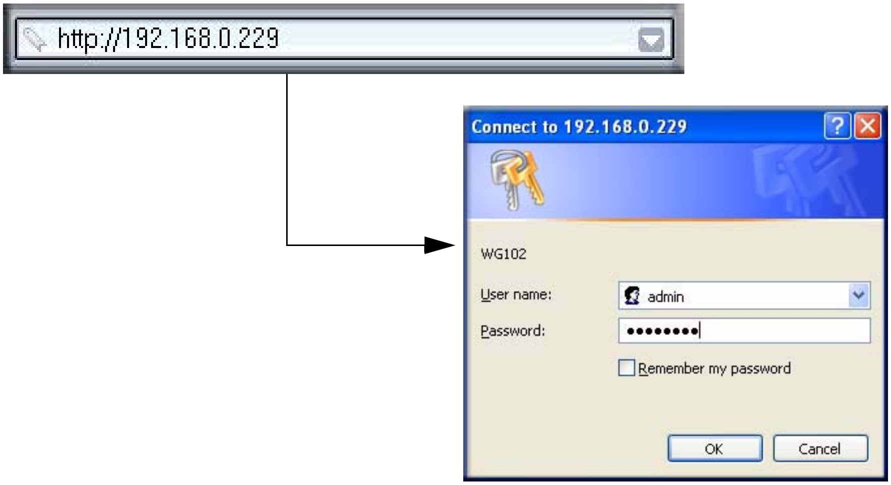
> **Note:** If you are unable to connect, see Chapter 5, "Troubleshooting

Logging in to the Wireless Access Point

The default IP address of your access point is 192.168.0.229. The WG102 Access Point is set, by default, for the DHCP client to be disabled.

> **Note:** The computer that you use to connect to the WG102 Access Point should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

1. Open a Web browser such as Internet Explorer or Netscape Navigator.
2. Connect to the WG102 Access Point by entering its default address of **http://192.168.0.229** into your browser.



http://192.168.0.229

Connect to 192.168.0.229

WG102

User name: admin

Password: ••••••••

□ Remember my password

Figure 1-6

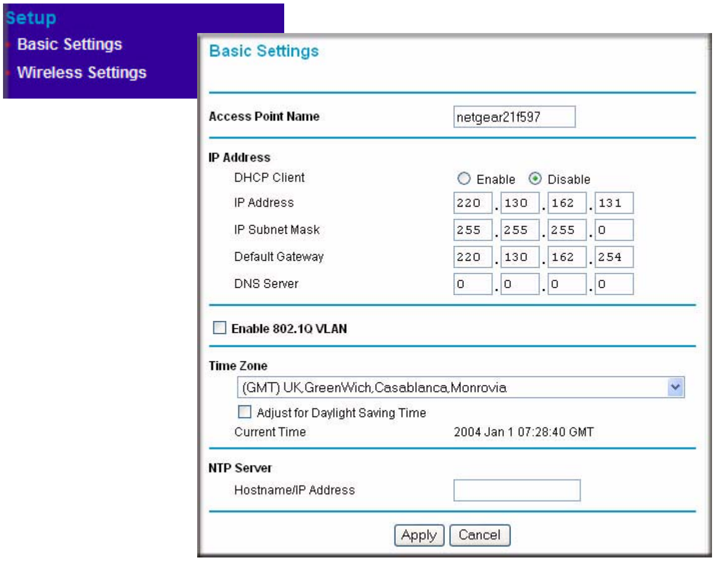
A login window opens.

3. Log in using the default user name of **admin** and default password of **password**.

   Once you have entered your access point name, the Web browser finds the WG102 Access Point and displays the main menu as shown in Figure 1-3 on page 1-6.

Basic IP Settings

To configure the basic settings of your wireless access point, select Basic Settings in the Setup section of the WG102 Access Point main menu. The Basic Settings screen displays:



Basic Settings

Access Point Name: netgear21f597

IP Address
- DHCP Client: ○ Enable ● Disable
- IP Address: 220 . 130 . 162 . 131
- IP Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 220 . 130 . 162 . 254
- DNS Server: 0 . 0 . 0 . 0

□ Enable 802.1Q VLAN

Time Zone
- (GMT) UK,GreenWich,Casablanca,Monrovia
- □ Adjust for Daylight Saving Time
- Current Time: 2004 Jan 1 07:28:40 GMT

NTP Server
- Hostname/IP Address:

Figure 1-7

The default values for Basic Settings work for most users and situations. They are described below:

- **Access Point Name.** This unique name is the access point NetBIOS name. The default Access Point Name is on the bottom label of the WG102. You can modify the default name with a unique name up to 15 characters long. The default is netgearxxxxxx, where xxxxxxx represents the last six digits of the WG102 MAC address.

- **DHCP Client:** By default, Dynamic Host Configuration Protocol (DHCP) client is disabled. After installation (), you can enable DHCP to let the wireless access point get its TCP/IP configuration from the DHCP server on your network. The wireless access point gets the IP address, subnet mask and the default gateway settings automatically from the DHCP server if DHCP is enabled.
- **IP Address.** The default IP address is 192.168.0.229. If you want to change it, enter an unused IP address from the address range used on your LAN (factory default: 192.168.0.229); or enable DHCP.
- **IP Subnet Mask.** Enter the subnet mask value used on your LAN (factory default: 255.255.255.0).
- **Default Gateway.** Enter the IP address of the Gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected (factory default: 0.0.0.0).
- **DNS Server.** Enter the IP address of the DNS (Domain Name Server) you wish to use (factory default: 0.0.0.0.
- **Enable 802.1Q VLAN.** Check the box Enable 802.1Q VLAN to enable the WG102 to process VLAN membership information.
- **Time Zone.** Select the Time Zone to match your location. If your location uses daylight saving, check the box Adjust for Daylight Saving Time.

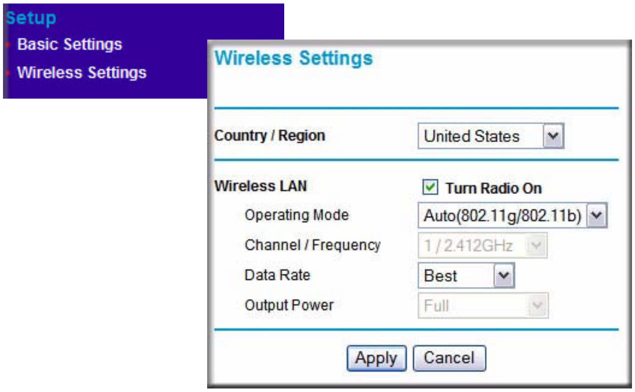
  The Current Time, as used on the wireless access point, is displayed.

  Note: You must have an Internet connection to get the current time.

- **NTP Server.** Provide the URL for the time server the WG102 Access Point will use to keep its time correct.

Wireless Settings

To configure the wireless settings, click Wireless Settings in the Setup section of the WG102 Access Point main screen. The Wireless Settings screen appears, as shown below.



Setup
- Basic Settings
- Wireless Settings

Wireless Settings

Country / Region: United States

Wireless LAN: ☑ Turn Radio On

Operating Mode: Auto(802.11g/802.11b)

Channel / Frequency: 1 / 2.412GHz

Data Rate: Best

Output Power: Full

Figure 1-8

The Wireless Settings screen options are discussed below.

- **Country/Region.** This is the region where the WG102 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. For products sold in the United States, the default country domain is preset. Also, the channel is set to 11. For products sold outside the United States, unless a country domain is selected, the channel cannot be changed.
- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Operating Mode.** Select the desired wireless operating mode. The options are:
  - Auto (802.11g/802.11b): Both 802.11g and 802.11b wireless stations can be used. This is the default.
  - 802.11g Only: Only 802.11g wireless stations can be used.
  - 802.11b Only: All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- **Channel.** This sets which operating frequency is used. You should not need to change the channel unless you notice interference problems, or are setting up the WG102 near another access point.

  - Access points use a fixed channel. You can select the channel used. This lets you choose a channel that provides the least interference and best performance. In the USA and Canada, 11 channels are available.
  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use channels 1 and 6, or 6 and 11).
  - In "Infrastructure" mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the access points use the same SSID.

  See the link to the online document "Wireless Communications" in Appendix B for more information about wireless channels.

- **Data Rate.** Shows the available transmit data rate of the wireless network. The default is Best.
- **Output Power.** Set the transmit signal strength of the access point (AP). The options are full, half, quarter, eighth, and min. Decrease the transmit power if two or more APs are close together and using the same channel frequency. The default is Full.

Setting up and Testing Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. After this is done, then you can set up wireless security settings appropriate to your needs.

1. Connect to the WG102 Access Point.

   In address field of your Web browser, enter the default LAN address of **http://192.168.0.229**. Log in with the user name of **admin** and default password of **password**, or using the LAN address and password that you set up.

2. On the main menu, below the Setup heading, select Wireless Settings.

   The default SSID is NETGEAR-0-0.

   > **Note:** The SSID of any wireless access adapters must match the SSID you configure in the NETGEAR WG102 ProSafe 802.11g Wireless Access Point. If they do not match, you will not get a wireless connection to the WG102.

3. Select the Country/Region in which the wireless interface will operate.
4. For now, do not make other changes

5. Click **Apply** to save your changes.

> **Note:** If you are configuring the WG102 Access Point from a wireless computer and you change the SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

6. Configure and test your PCs for wireless connectivity.

   Set up the wireless adapters of your PCs so that they all have the same SSID and channel that you configured in the WG102 Access Point. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WG102 Access Point.

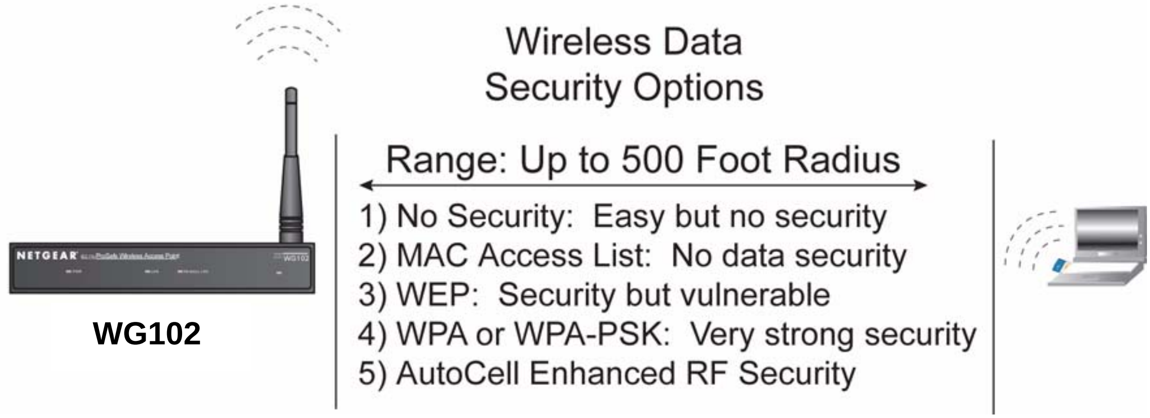
Now that your PCs can connect to the WG102 Access Point, you can configure the wireless security. See Chapter 2, "Configuring Security."

Chapter 2
Configuring Security

This chapter describes how to set up security features and advanced features of your NETGEAR WG102 ProSafe 802.11g Wireless Access Point.

Wireless Data Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WG102 Access Point provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.



Wireless Data Security Options

Range: Up to 500 Foot Radius

1) No Security: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but vulnerable
4) WPA or WPA-PSK: Very strong security
5) AutoCell Enhanced RF Security

Figure 2-1

There are several ways you can enhance the security of your wireless network:

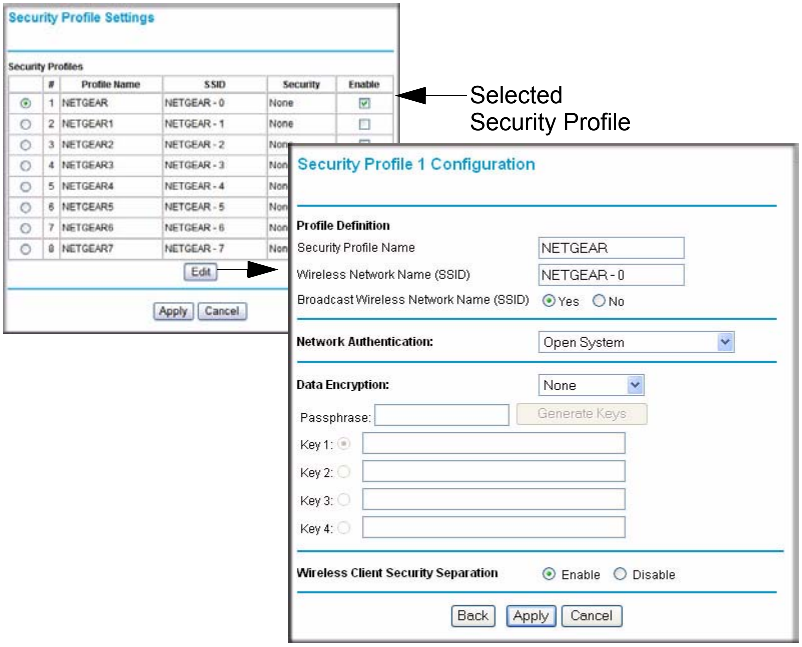
- **Use Multiple BSSIDs combined with VLANs.** You can configure combinations of VLANS and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network.

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WG102. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **WPA, WPA-PSK, WPA2, or WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.
- **WPA with Radius, WPA2 with Radius, or WPA and WPA2 with Radius.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Security Profiles

Security profiles let you configure unique security settings for each SSID. The WG102 Access Point supports up to eight SSIDs. The Security Profile Settings screen is shown in the following figure. To edit a security profile, select it from the list, and click **Edit**.

The Security Profile Configuration screen opens for that profile.



Selected
Security Profile

Security Profile Settings

Security Profiles

	#	Profile Name	SSID	Security	Enable
●	1	NETGEAR	NETGEAR - 0	None	☑
○	2	NETGEAR1	NETGEAR - 1	None	□
○	3	NETGEAR2	NETGEAR - 2	Non	
○	4	NETGEAR3	NETGEAR - 3	Non	
○	5	NETGEAR4	NETGEAR - 4	Non	
○	6	NETGEAR5	NETGEAR - 5	Non	
○	7	NETGEAR6	NETGEAR - 6	Non	
○	8	NETGEAR7	NETGEAR - 7	Non	

Security Profile 1 Configuration

Profile Definition

Security Profile Name: NETGEAR

Wireless Network Name (SSID): NETGEAR - 0

Broadcast Wireless Network Name (SSID): ● Yes ○ No

Network Authentication: Open System

Data Encryption: None

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Wireless Client Security Separation ● Enable ○ Disable

Figure 2-2

Profile Definition

- **Security Profile Name.** Use a name that makes it easy to recognize the profile, and to tell profiles apart.
- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. The SSID separates network traffic from different wireless networks. To connect any wireless device to a wireless network, you need to use the SSID. The default SSID is: NETGEAR-0-0 for the first profile, NETGEAR-0-1 for the second, and so on. You can enter a value of up to 32 alphanumeric characters. Some concepts regarding the SSID are explained below:
  - Using the same SSID is essential. Devices with different SSIDs cannot communicate with each other. However, some access points allow connections from wireless stations that have their SSID set to “any” or whose SSID is blank (null).
  - A Basic Service Set (BSS) is a group of wireless stations and a single access point, all using the same SSID.
  - An Extended Service Set (ESS) is a group of wireless stations and multiple access points, all using the same ID (ESSID).

  - Different access points within an ESS can use different channels. To reduce interference, adjacent access points *should* use different channels.
  - Roaming is the ability of wireless stations to connect wirelessly when they physically move from one ESS to another. The wireless station automatically changes to the access point with the least interference or best performance.

- **Broadcast Wireless Network Name (SSID).** This field lets you turn off the SSID broadcast. If you do so, then only stations that know the SSID can connect. Disabling the SSID broadcast somewhat hampers the wireless network 'discovery' feature of some products. The default is to enable SSID broadcast.

Network Authentication

The WG102 Access Point is set by default as an open system with no authentication. When setting up Network Authentication, bear in mind the following:

- If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options may be unavailable.
- Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

You can configure the WG102 Access Point to use authentication types shown in the table below.

Network Authentication Types	
Open System	Can be used with WEP encryption, or no encryption.
Shared Key	WEP must be used. At least one shared key must be entered.
Legacy 802.1x:	You must configure the Radius Server Settings to use this option.
WPA-PSK	You must use TKIP encryption, and enter the WPA passphrase (Network key).
WPA with Radius	You must configure the Radius Server Settings to use this option.
WPA2-PSK	WPA2 is a newer version of WPA. Select this only if all clients support WPA2. With WPA2, you must use AES encryption, and enter the WPA passphrase (Network key).
WPA-PSK and WPA2-PSK	Clients can use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES. The WPA passphrase (Network key) must also be entered.
WPA2 with Radius	WPA2 is a later version of WPA. Only select this if all clients support WPA2. You must use AES encryption, and configure the Radius Server Settings screen.
WPA and WPA2 with Radius	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES, and you must also configure the Radius Server Settings screen

Data Encryption

Select the data encryption that you want to use. The available options depend on the Network Authentication setting above (otherwise, the default is None). The Data Encryption settings are explained in the table below:

Data Encryption Settings	
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that only works with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA.
AES	This is the standard encryption method for WPA2. Some clients may support AES with WPA, but this is not supported by this Access Point.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

The Passphrases and Keys are explained below:

- **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
- **Key 1, Key 2, Key 3, Key 4.** If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
- **WPA Passphrase (Network Key).** If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.

Wireless Client Security Separation

If enabled, the associated wireless clients will not be able to communicate with each other. This feature is used for hotspots and other public access situations. The default is Disabled.

Before You Change the SSID and WEP Settings

For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the person who set up or is responsible for the network can provide this information. Be sure to set the Regulatory Domain correctly as the first step. Store this information in a safe place.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. You may customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: ____________________________________

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:
- **Authentication**
  Circle one: Open System or Shared Key. Choose "Shared Key" for more security.

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key and have the same keys in the same positions as those in the WG102.
- **WEP Encryption Keys**
  For all four 802.11b keys, choose the Key Size. Circle one: 64, 128, or 152 bits

  Key 1: ____________________________________

  Key 2: ____________________________________

  Key 3: ____________________________________

  Key 4: ____________________________________
- **WPA-PSK (Pre-Shared Key)WPA2-PSK (Pre-Shared Key)**
  Record the WPA-PSK key:Record the WPA2-PSK key:

  Key: _______________________________ Key: _______________________________
- **WPA RADIUS Settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _________________ Secondary __________________

  Port: ____________________________________

  Shared Secret: ____________________________________
- **WPA2 RADIUS Settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _________________ Secondary __________________

  Port: ____________________________________

  Shared Secret: ____________________________________

Use the procedures described in the following sections to configure the WG102.

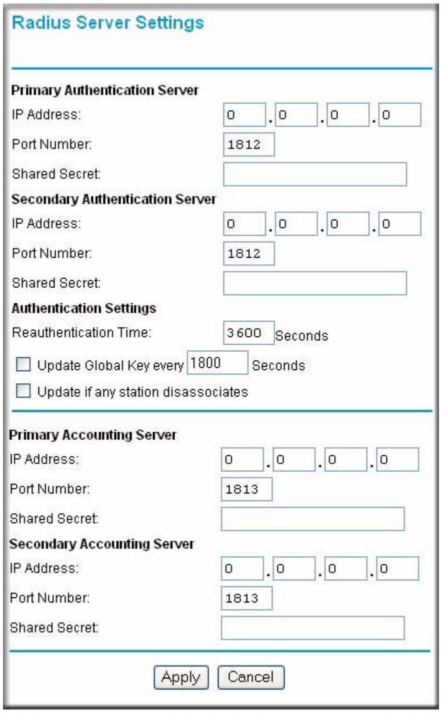
Configuring the Radius Server Settings

You can view or change the Radius Server Settings from the Security menu. Follow the steps below:

1. Connect to the WG102 Access Point.

In address field of your Web browser, enter the default LAN address of **http://192.168.0.229**. Log in with the user name of **admin** and default password of **password**, or using the LAN address and password that you set up.

2. In the Security menu, click Radius Server Settings.



Radius Server Settings

Primary Authentication Server

IP Address:	0 . 0 . 0 . 0
Port Number:	1812
Shared Secret:	

Secondary Authentication Server

IP Address:	0 . 0 . 0 . 0
Port Number:	1812
Shared Secret:	

Authentication Settings

Reauthentication Time: 3600 Seconds

□ Update Global Key every 1800 Seconds

□ Update if any station disassociates

Primary Accounting Server

IP Address:	0 . 0 . 0 . 0
Port Number:	1813
Shared Secret:	

Secondary Accounting Server

IP Address:	0 . 0 . 0 . 0
Port Number:	1813
Shared Secret:	

Figure 2-3

3. Enter the settings, and click **Apply**.

The Radius Server Settings are explained below:

- **Authentication/Access Control Radius Server Configuration.** This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
- **IP Address.** The IP address of the Radius Server. The default is 0.0.0.0.
- **Port Number.** Port number of the Radius Server. The default is 1812.
- **Shared Secret.** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
- **Re-authentication Time.** The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.
- **Global-key Re-Key Time.** Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
- **Update if any station disassociates.** Check on this option to refresh global key when any stations disassociated with wireless Access Point.
- **Accounting Radius Server Configuration.** This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
- **IP Address.** The IP address of the Radius Server. The default is 0.0.0.0.
- **Port Number.** Port number of the Radius Server. The default is 1813.
- **Shared Secret.** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

Configuring Network Authentication

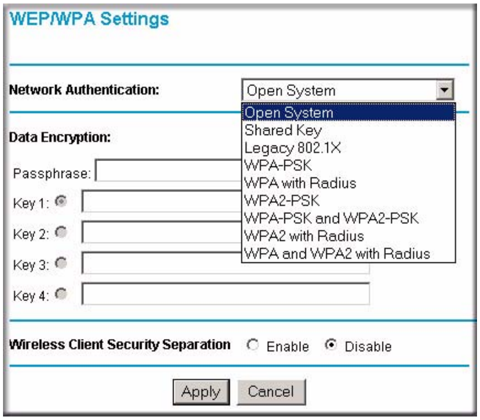
Follow the steps below:

1. Connect to the WG102 Access Point.

Log in at the default LAN address of **http://192.168.0.229** with the user name of **admin** and default password of **password**, or using the LAN address and password that you set up.

2. If you are using Radius Server Settings, set them up first, as described in "Configuring the Radius Server Settings" on page 2-7.

3. Set the Network Authentication that you want to use.



WEP/WPA Settings

Network Authentication: Open System

Data Encryption:

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Wireless Client Security Separation ○ Enable ● Disable

Figure 2-4

a. On the Security menu, click Security Profiles Settings.

b. Select the profile that you want.

c. Click Edit to view the Security Profiles Configuration menu.

d. Choose the type of Network Authentication that you want from the list.

Note: WEP can be used with Open System or Shared Key. Choose the encryption strength, and then enter the Keys as explained in "Entering WEP Data Encryption Keys" on page 2-10

e. Click **Apply** to save your settings.

Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

Entering WEP Data Encryption Keys

You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

- **Automatic**. Enter a word or group of printable characters in the Passphrase field, and click the Generate button. The four key fields will be automatically populated with key values.
- **Manual**. Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F).
  Select which of the four keys will be the default.

See the link to the online document "Wireless Data Security Options" in Appendix 2 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

Restricting Wireless Access by MAC Address

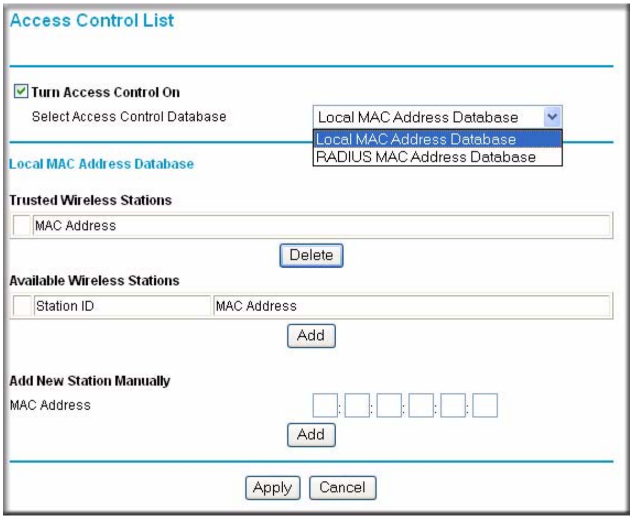
To restrict access based on MAC addresses, follow these steps:

1. Connect to the WG102 Access Point.

Log in at the default LAN address of **http://192.168.0.229** with the user name of **admin** and default password of **password**, or using the LAN address and password that you set up.

> **Note:** When configuring the WG102 Access Point from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

2. Below the Security heading, select Access Control to display the Access Control List screen shown below.



Access Control List

☑ Turn Access Control On

Select Access Control Database: Local MAC Address Database

Local MAC Address Database
RADIUS MAC Address Database
Local MAC Address Database
Trusted Wireless Stations
MAC Address
Delete
Available Wireless Stations
Station ID
MAC Address
Add
Add New Station Manually
MAC Address
Add
Apply
Cancel

Figure 2-5

3. Select the **Turn Access Control On** check box.

4. Choose to use the local MAC address database stored on the access point, or use the RADIUS MAC address database stored on a RADIUS server.

   - If you choose the RADIUS MAC Address Database, you must configure the RADIUS Server Settings first.
   - If you choose Local MAC Address Database, either select from the list of available wireless cards the WG102 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter. Click Add to add the wireless device to the access list. Repeat these steps for each additional device you want to add to the list.

5. Be sure to click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WG102 Access Point.

Chapter 3
Management

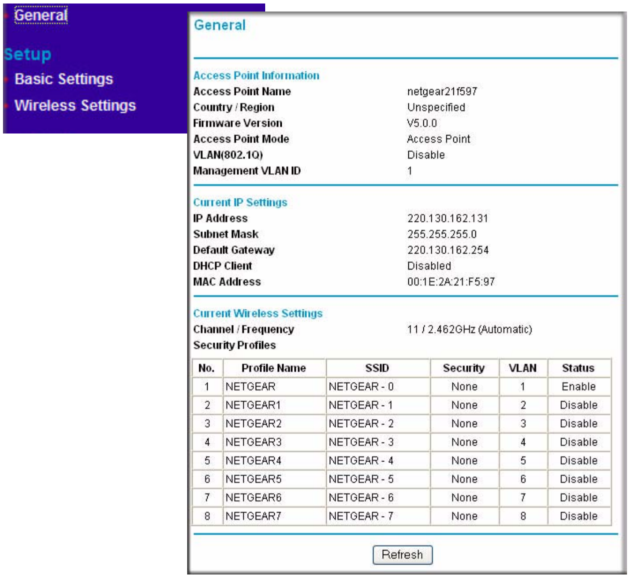
This chapter describes how to view information about your NETGEAR WG102 ProSafe 802.11g Wireless Access Point and to use the management features. To get to these features, connect to the WG102 Access Point as described in "Logging in to the Wireless Access Point" on page 1-9.

Viewing Information

You can view General Information, the Activity Log, Statistics, and the Available Wireless Stations list.

General Information

The General information is a summary of the WG102 Access Point configuration settings. From the top of the WG102 main menu, select General to view the screen shown below.



General

Access Point Information

Access Point Name	netgear21f597
Country / Region	Unspecified
Firmware Version	V5.0.0
Access Point Mode	Access Point
VLAN(802.1Q)	Disable
Management VLAN ID	1

Current IP Settings

IP Address	220.130.162.131
Subnet Mask	255.255.255.0
Default Gateway	220.130.162.254
DHCP Client	Disabled
MAC Address	00:1E:2A:21:F5:97

Current Wireless Settings

Channel / Frequency	11 / 2.462GHz (Automatic)
Security Profiles	

No.	Profile Name	SSID	Security	VLAN	Status
1	NETGEAR	NETGEAR - 0	None	1	Enable
2	NETGEAR1	NETGEAR - 1	None	2	Disable
3	NETGEAR2	NETGEAR - 2	None	3	Disable
4	NETGEAR3	NETGEAR - 3	None	4	Disable
5	NETGEAR4	NETGEAR - 4	None	5	Disable
6	NETGEAR5	NETGEAR - 5	None	6	Disable
7	NETGEAR6	NETGEAR - 6	None	7	Disable
8	NETGEAR7	NETGEAR - 7	None	8	Disable

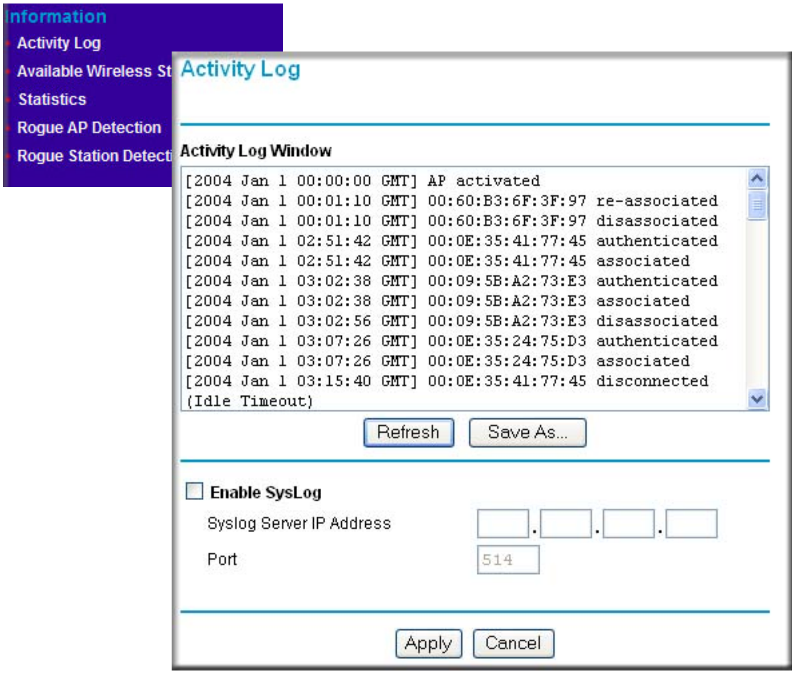
Figure 3-6

Table 3-1. General Information Fields

Field	Description
Access Point Information	
Access Point Name (NetBIOS name)	The default name may be changed if desired.
Country/Region	The domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Access Point Mode	The operating mode of the WG102: Access Point, Point-to-point bridge, Multi-point bridge or Repeater.
VLAN (802.1Q)	Indicates if VLAN support is enabled. The default is disabled.
Management VLAN ID	Displays the VLAN ID.
Current IP Settings	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	If this is enabled, the current IP address was obtained from a DHCP server on your network. Disabled indicates a static IP configuration.
MAC Address	The Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Current Wireless Settings	
Channel/Frequency	The channel the wireless port uses. The default channel setting is automatic channel selection. For the frequencies used on each channel, see the link to the online document "Wireless Communications" in Appendix B."
Security Profiles	For each Security Profile, the following are displayed: Profile name, SSID, security option, VLAN ID, and enabled/disabled.

Activity Log

From the WG102 Access Point main menu, under the Information heading, select Activity Log.



```
[2004 Jan 1 00:00:00 GMT] AP activated
[2004 Jan 1 00:01:10 GMT] 00:60:B3:6F:3F:97 re-associated
[2004 Jan 1 00:01:10 GMT] 00:60:B3:6F:3F:97 disassociated
[2004 Jan 1 02:51:42 GMT] 00:0E:35:41:77:45 authenticated
[2004 Jan 1 02:51:42 GMT] 00:0E:35:41:77:45 associated
[2004 Jan 1 03:02:38 GMT] 00:09:5B:A2:73:E3 authenticated
[2004 Jan 1 03:02:38 GMT] 00:09:5B:A2:73:E3 associated
[2004 Jan 1 03:02:56 GMT] 00:09:5B:A2:73:E3 disassociated
[2004 Jan 1 03:07:26 GMT] 00:0E:35:24:75:D3 authenticated
[2004 Jan 1 03:07:26 GMT] 00:0E:35:24:75:D3 associated
[2004 Jan 1 03:15:40 GMT] 00:0E:35:41:77:45 disconnected
(Idle Timeout)
```

☐ Enable SysLog

Syslog Server IP Address ___ . ___ . ___ . ___

Port 514

Figure 3-7

You can use a SysLog server to view the Activity Log. If you have a SysLog server on your LAN, then enable the SysLog. If enabled, you must enter the IP address of your SysLog server and the port number that your SysLog server uses.

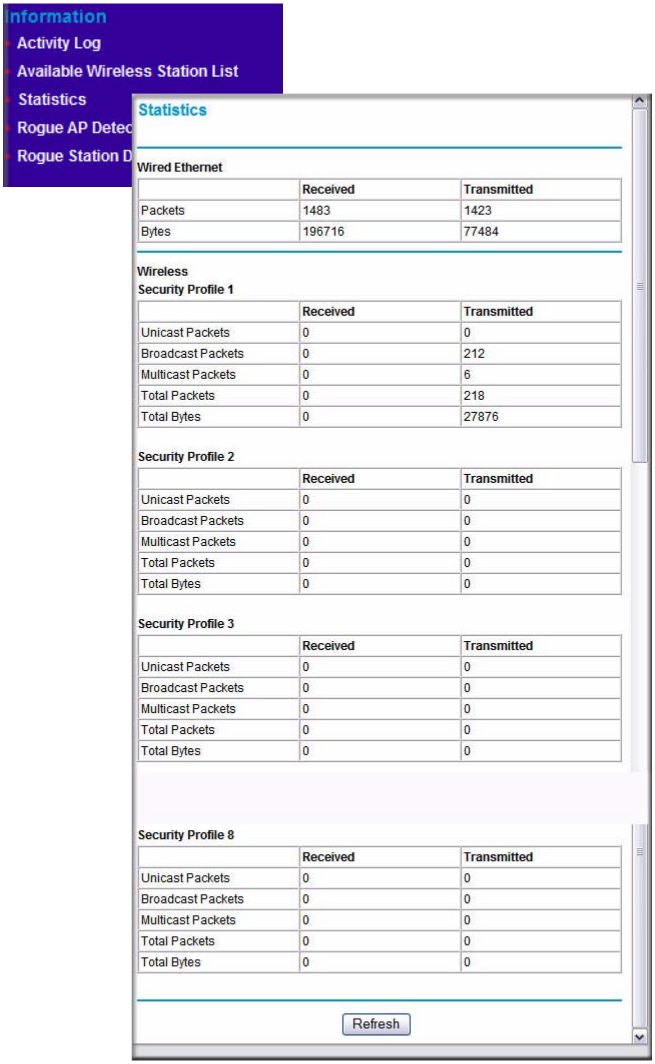
- SysLog Server IP address: The access point sends all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0
- Port: The port number configured in the SysLog server on your LAN. The default is 514

The Activity Log screen displays the Access Point system activity.

You can click Refresh to update the display. To save the log contents into a file on your PC, click Save As and save the file to a disk drive.

Statistics

The Statistics screen provides LAN and WLAN statistics. From the WG102 main menu, select Statistics under the Information heading to view the screen shown below:



Statistics

Wired Ethernet

	Received	Transmitted
Packets	1483	1423
Bytes	196716	77484

Wireless

Security Profile 1

	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	212
Multicast Packets	0	6
Total Packets	0	218
Total Bytes	0	27876

Security Profile 2

	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	0
Total Bytes	0	0

Security Profile 3

	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	0
Total Bytes	0	0

Security Profile 8

	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	0
Total Bytes	0	0

Figure 3-8

Available Wireless Station List

The Available Wireless Station List contains a table of all IP devices associated with the wireless access point for the Wired Network Name (SSID). From the WG102 main menu, under the Information heading, click Available Wireless Station List to view the list.

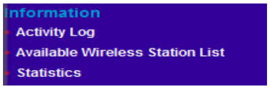


Figure 3-9

The fields in the list are explained below.

Table 3-2. Available Wireless Station List

Field	Description
Wired Ethernet	Received/Transmitted
Packets	The number of packets sent since the WG102 was restarted.
Bytes	The number of bytes sent since the WG102 was restarted.
For Each Wireless Security Profile	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WG102 was restarted.
Broadcast Packets	The Broadcast packets sent since the WG102 was restarted.
Multicast Packets	The Multicast packets sent since the WG102 was restarted.
Total Packets	The Wireless packets sent since the WG102 was restarted.
Total Bytes	The Wireless bytes sent since the WG102 was restarted.
Refresh button	Click the Refresh button to update the statistics on this screen.

For each device, the table shows the Station ID, MAC address, IP Address, and Status (whether the device is allowed to communicate with the wireless access point or not).

Note that if the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the Refresh button.

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This extends the reach of the wireless network. Users can roam from one access point to another, providing seamless network connectivity. If this is the case, only the stations associated with this access point are shown in the Available Station List.

Upgrading the Wireless Access Point Firmware

Warning: When uploading firmware to the WG102 Access Point, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the firmware, and render the WG102 Access Point completely inoperable

You cannot upgrade the firmware from a computer that is connected to the WG102 Access Point with a wireless link. You must use a computer that is connected to the WG102 Access Point with an Ethernet cable.

The WG102 Access Point firmware is stored in FLASH memory, and can be upgraded as new firmware is released by NETGEAR. You can download the upgrade files from the NETGEAR website. If the upgrade file is compressed (.ZIP file), you must first extract the image (.IMG) file before you send it to the wireless access point. The upgrade file can be sent using your browser.

Note: The Web browser used to upload new firmware into the WG102 Access Point must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

Follow the steps below to upgrade the firmware:

1. Download the file from the NETGEAR website, save it to your hard disk, and unzip it.
2. If you want to save your configuration settings, see “Backing up and Restoring the Configuration” on page 3-8.

3. From the main menu Management section, select Upgrade Firmware.

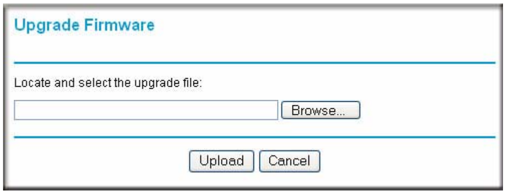


Figure 3-10

4. Click **Browse** and browse to the location of the image (.IMG) upgrade file.
5. Click **Upload**.

   When the upload completes, your wireless access point automatically restarts. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the wireless access point after upgrading.

Configuration File Management

The WG102 Access Point settings are stored in the wireless access point in a configuration file. This file can be saved (backed up) to a computer, retrieved (restored) from a computer, or cleared to factory default settings.

From the main menu, select Backup/Restore Settings to go to the screen shown below.

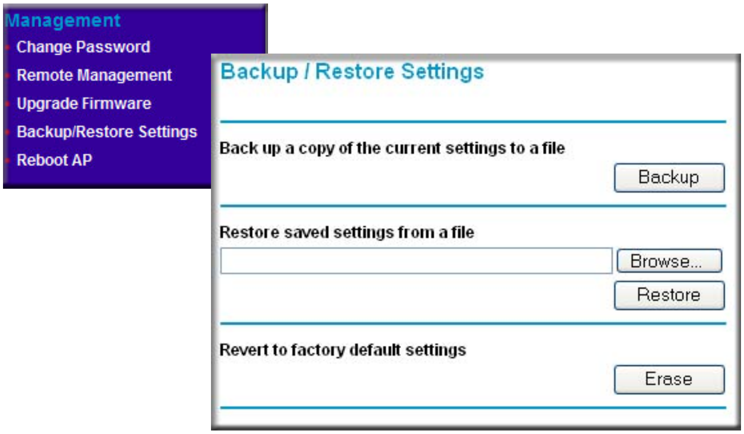

Management
Change Password
Remote Management
Upgrade Firmware
Backup/Restore Settings
Reboot AP
Backup / Restore Settings
Back up a copy of the current settings to a file
Backup
Restore saved settings from a file
Browse...
Restore
Revert to factory default settings
Erase

Figure 3-11

The options displayed are described in the following sections.

Backing up and Restoring the Configuration

To save your settings, click Backup. Your browser extracts the configuration file from the wireless access point and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as `WG102.cfg`.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click the Browse button to locate the file. When you have located it, click the Restore button to upload the file. After completing the upload, the WG102 reboots automatically.

Erasing the Configuration

You can erase the wireless access point configurations, and return to the factory default settings. After erasing, the wireless access point's password will be **password**, the SSID will be NETGEAR-0, the DHCP client will be disabled, the default LAN IP address will be 192.168.0.229, and the access point name will be netgearxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address (on the label on the bottom of the unit).

Using the Reset Button to Restore Factory Default Settings

If you do not know the login password, or IP address, you can still restore the factory default configuration settings with the Reset button. This button is on the rear panel of the wireless access point (see "Rear Panel" on page 1-3). The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point reboots (restarts).
- **Reset to Factory Defaults.** When pressed and held down, it clears all data and restores all settings to the factory default values.

To clear all data and restore the factory default values:

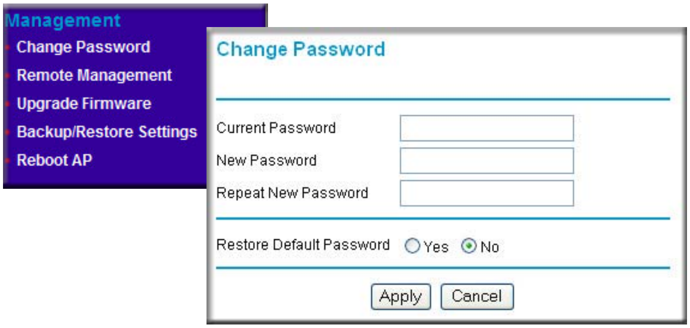
1. Hold the Reset button until the LEDs blink twice, usually more than five seconds.
2. Release the Reset button.

The factory default configuration has been restored, and the wireless access point is ready to use.

Changing the Administrator Password

The default password is **password**. Change this password to a more secure password. You cannot change the administrator login name.

From the main menu, select Change Password to go to the screen shown below.



Change Password

Current Password
New Password
Repeat New Password

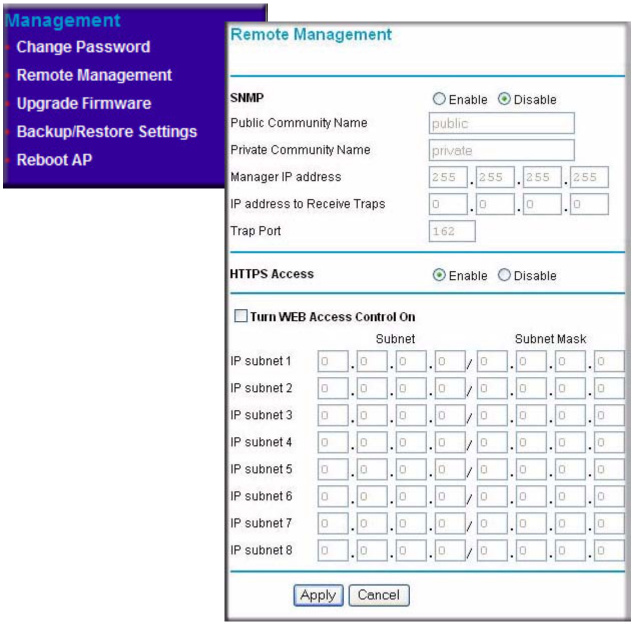
Restore Default Password ○ Yes ● No

Figure 3-12

SNMP Remote Management

Enable SNMP to allow SNMP network management software such as HP OpenView to manage the wireless access point via the SNMPv1/v2 protocol.

From the main menu Management section, select Remote Management to view this screen.



Remote Management

SNMP ○ Enable ● Disable

Public Community Name: public

Private Community Name: private

Manager IP address: 255 . 255 . 255 . 255

IP address to Receive Traps: 0 . 0 . 0 . 0

Trap Port: 162

HTTPS Access ● Enable ○ Disable

□ Turn WEB Access Control On

	Subnet	Subnet Mask
IP subnet 1	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 2	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 3	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 4	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 5	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 6	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 7	0 . 0 . 0 . 0	0 . 0 . 0 . 0
IP subnet 8	0 . 0 . 0 . 0	0 . 0 . 0 . 0

Figure 3-13

Follow the steps below to enable Remote Management

1. Select the **Enable** radio button to use the SNMP remote management feature.
2. Fill in the fields according to the requirements of your location.
   - **Public Community Name**. (Default: public) The community string to allow the SNMP manager to read the MIB objects of the WG102.
   - **Private Community Name**. (Default: private) The community string to allow the SNMP manager to read and write the MIB objects of the WG102.
   - **Manager IP address**. Enter the IP address of the SNMP manager. If this is set to 255.255.255.255, any SNMP manager will be allowed.
   - **IP address to Receive Traps.** Enter the IP address of the SNMP manager to receive traps sent from the wireless Access Point. If you don't want Traps to be sent, leave this at the default value of 0.0.0.0
   - **Turn WEB Access Control On.** Enter the IP address of the subnets that you will allow to access this access point.
3. Be sure to click **Apply** to save your changes.

Chapter 4
Advanced Configuration

This chapter describes how to configure the advanced features of your NETGEAR WG102 ProSafe 802.11g Wireless Access Point. These features can be found under the Advanced heading in the main menu.

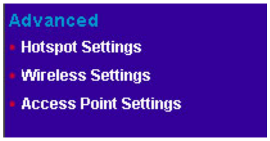


Figure 4-1

The following features are explained:

- Hotspot Settings: Redirect HTTP requests.
- Advanced Wireless Settings: Set up advanced wireless LAN parameters.
- Access Point Settings: Enable wireless bridging and repeating.

Hotspot Settings

If you want the access point to capture and redirect all HTTP (TCP, port 80) requests, use this feature. For example, a hotel might want all wireless connections to go to its server to start a billing transaction.

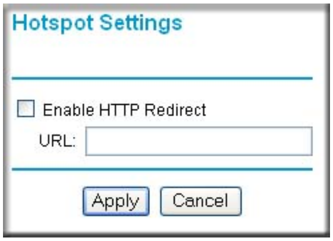
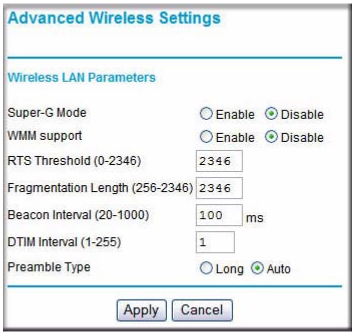


Figure 4-2

Enter the URL of the Web server where you wish to redirect HTTP requests.

Configuring Advanced Wireless Settings

You can use the Advanced Wireless Settings screen to configure the advanced wireless settings. If you want the AP to operate in Super-G mode, use this feature.



Advanced Wireless Settings

Wireless LAN Parameters

Super-G Mode ○ Enable ● Disable

WMM support ○ Enable ● Disable

RTS Threshold (0-2346) 2346

Fragmentation Length (256-2346) 2346

Beacon Interval (20-1000) 100 ms

DTIM Interval (1-255) 1

Preamble Type ○ Long ● Auto

Figure 4-3

The advanced wireless settings normally do not need to be changed.

- **Super-G Mode.** Super-G Mode is a proprietary extension to the 802.11g standard, which can double the throughput to 108Mbps. Only compatible wireless stations can use this mode. The default is Disable.
- **WMM support.** WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, have a higher priority than normal traffic. For WMM to work correctly, wireless clients must also support WMM. The default is Disable.
- **RTS Threshold.** Request to Send Threshold. The packet size that is used to determine if it should use the Carrier Sense Multiple Access with Collision Detection mechanism (CSMA/CD) or the CSMA/CA mechanism for packet transmission. With CSMA/CD, the transmitting station sends the packet as soon as it has waited for the silence period. With CSMA/CA, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a Clear to Send (CTS) packet before sending the packet data. The default is 2346.
- **Fragmentation Length.** This is the maximum packet size used for fragmentation. Packets larger than this size will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval.** The interval time (between 20ms and 1000ms) for each beacon transmission. The default is 100.

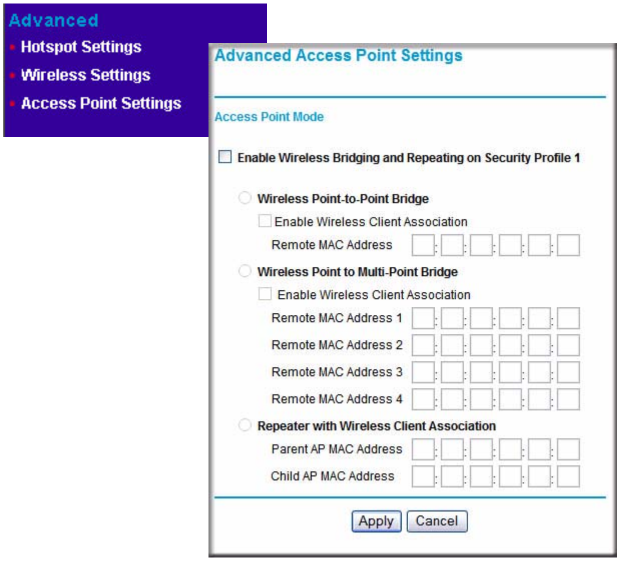
- **DTIM Interval.** The Delivery Traffic Indication Message (DTIM) specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type.** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto automatically handles both long and short preambles. The default is Auto.

Wireless Bridging and Repeating

The WG102 Access Point lets you build large bridged wireless networks. Examples of wireless bridged configurations are:

- **Point-to-Point Bridge**. The WG102 Access Point communicates with another bridge-mode wireless station. See "Point-to-Point Bridge Configuration" on page 4-4.
- **Multi-Point Bridge**. The WG102 Access Point is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this "master," rather than to other access points. See "Multi-Point Bridge Configuration" on page 4-5.
- **Repeater with Wireless Client Association**. Sends all traffic to the remote AP. See "Repeater with Wireless Client Association" on page 4-7.

These configurations can be set up from the Advanced Access Point Settings screen, shown below.



Advanced Access Point Settings

Access Point Mode

□ Enable Wireless Bridging and Repeating on Security Profile 1

○ Wireless Point-to-Point Bridge
□ Enable Wireless Client Association
Remote MAC Address □:□:□:□:□:□

○ Wireless Point to Multi-Point Bridge
□ Enable Wireless Client Association
Remote MAC Address 1 □:□:□:□:□:□
Remote MAC Address 2 □:□:□:□:□:□
Remote MAC Address 3 □:□:□:□:□:□
Remote MAC Address 4 □:□:□:□:□:□

○ Repeater with Wireless Client Association
Parent AP MAC Address □:□:□:□:□:□
Child AP MAC Address □:□:□:□:□:□

Figure 4-4

Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the WG102 Access Point communicates with another bridge-mode wireless station. In addition, you can enable client associations with this WG102 Access Point. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use WEP to protect this communication. The figure below shows an example of Point-to-Point Bridge mode.

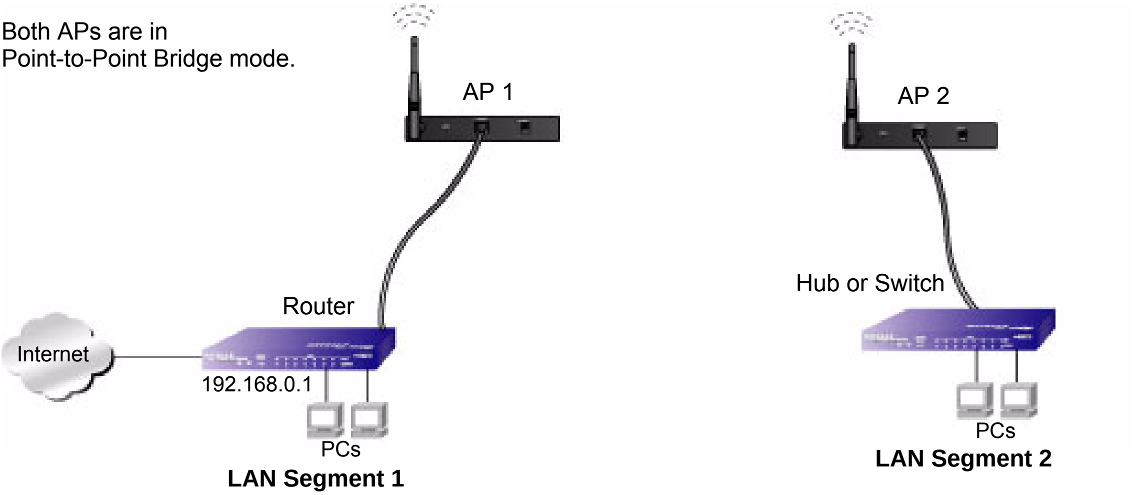


Figure 4-5

Follow the steps below to set up a Point-to-Point Bridge configuration.

1. Configure the WG102 Access Point (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the other access point (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.

   AP 1 must have AP 2’s MAC address in its Remote MAC Address field and AP 2 must have AP 1’s MAC address in its Remote MAC Address field.
3. Configure and verify the following for both access points:
   - Verify the LAN network configuration of the access points. Both must be configured to operate in the same LAN network address range as the LAN devices
   - Both APs must use the same ESSID, Channel, authentication mode, if any, and security settings if security is in use.
4. Verify connectivity across the LAN 1 and LAN 2.

A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Multi-Point Bridge Configuration

Set up a Multi-Point Bridge only if this WG102 Access Point is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this "master," rather than to the other access points. In addition, you can enable client associations with this WG102 Access Point.

- You must enter the MAC addresses of the other access points in the fields provided.
- The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using the MAC address of this WG102 Access Point as the Remote MAC Address.
- Use WEP to protect this traffic.

The figure below shows an example of a Multi-Point Bridge mode configuration.

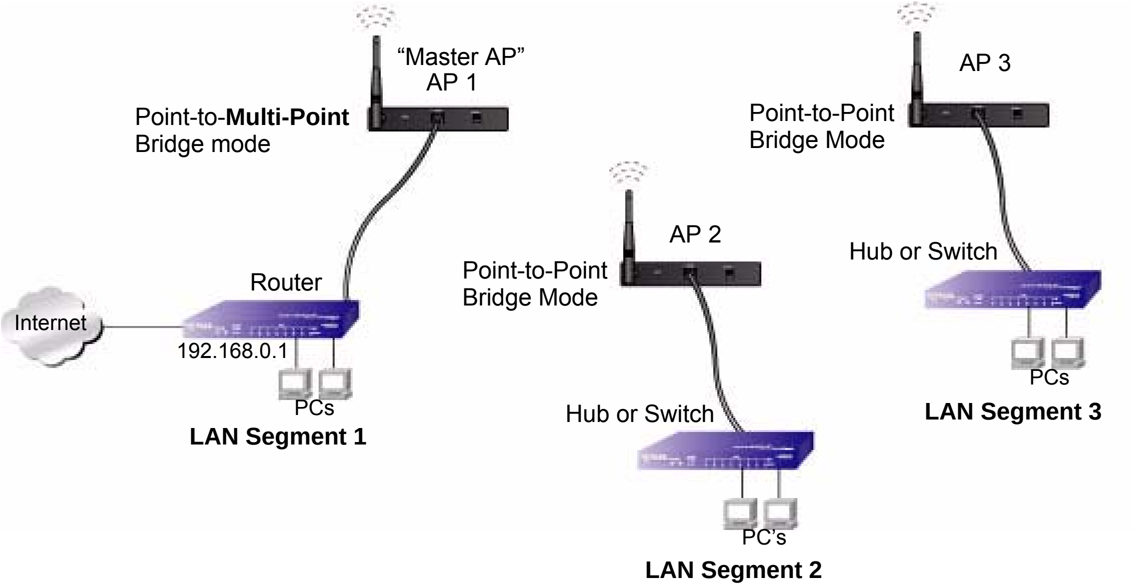


Figure 4-6

Follow the steps below to set up the Multi-Point Bridge configuration.

1. Configure the Operating Mode of the WG102 Access Points.
   - Because it is in the central location, configure WG102 Access Point (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode. The MAC addresses of AP2 and AP3 are required in AP1.

- Configure WG102 Access Point (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.
- Configure the WG102 Access Point (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.

2. Verify the following for all access points:

- The LAN network configuration of the WG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
- Only one AP is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
- All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
- If using DHCP, all WG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All WG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
- All Point-to-Point APs must have AP2’s MAC address in its Remote AP MAC address field.

3. Verify connectivity across the LANs.

- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
- Wireless stations will not be able to connect to the WG102 Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can use additional WG102 Access Points configured in Wireless Access Point mode to any LAN segment.

⇨	**Note:** You can extend this multi-point bridging by adding additional WG102 Access Points configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Repeater with Wireless Client Association

In this mode, the WG102 Access Point sends all traffic to the remote AP. For repeater mode, you must enter the MAC address of the remote "parent" access point. You can also enter the address of the "child" access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this WG102.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent/child AP pair.

The figure below shows an example of a Repeater Mode configuration.

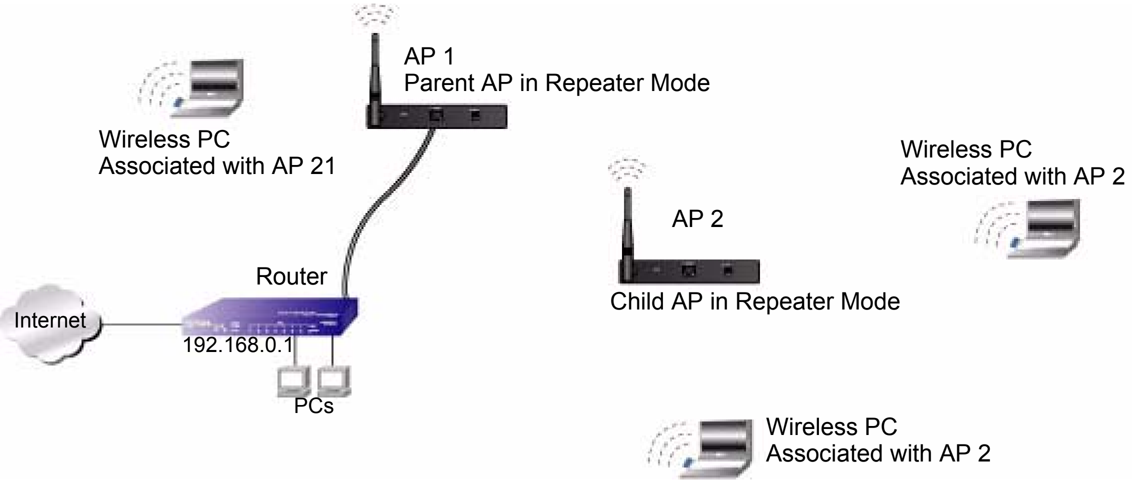


Figure 4-7

To set up a repeater with wireless client association, follow the steps below:

1. Configure the Operating Mode of the WG102 Access Points.
   - Configure AP 1 on LAN Segment 1 as the Parent in Repeater mode with the its own MAC address in the Parent AP MAC Address field, and the MAC Address of the 'downstream' AP (AP 2) in the Child AP MAC Address field.
   - Configure AP 2 in the Child Repeater mode with its MAC addresses as in the Child AP MAC Address field and the MAC address of the 'upstream' AP (AP 1) in the Parent MAC Address field.
2. Verify the following for all access points:

- The LAN network configuration of the WG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
- All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
- If using DHCP, all WG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All WG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.

3. Verify connectivity across the LANs.

A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

Note: You can extend this repeating by adding up to two more WG102 Access Points configured in repeater mode. However, since repeaters communicate in half-duplex mode, the bandwidth decreases as you add repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Chapter 5
Troubleshooting

This chapter provides information about troubleshooting your NETGEAR WG102 ProSafe 802.11g Wireless Access Point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WG102 Access Point on?
- Have I connected the wireless access point correctly?

  Go to "Installing the WG102 Access Point" on page 1-4.
- I cannot remember the wireless access point's configuration password.

  Go to "Changing the Administrator Password" on page 3-8.

If you have trouble setting up your WG102, check the tips below.

No Lights Are Lit on the Access Point

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point.

If the access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.

Wireless LAN Activity Light Is Off

The access point's antennae are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the WG102.
- Contact NETGEAR technical support if the Wireless LAN activity light remains off.

LAN Light is Off

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

Cannot Access the Internet or the LAN with a Wireless Capable Computer

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to “Obtain an IP address automatically.”
- The access point’s default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

Cannot Connect to the WG102 Access Point

Check these items:

- The WG102 Access Point is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is on (amber indicating a 10 Mbps Ethernet connection or green indicating a 100 Mbps Ethernet connection) to verify that the Ethernet connection is OK.
- The default configuration of the WG102 is for a static IP address of 192.168.0.229 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the WG102 to connect, ensure that your computer and the WG102 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to “Obtain an IP Address automatically” (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WG102. The WG102 default IP Address is 192.168.0.229 and the default Subnet Mask is 255.255.255.0.

When I Enter a URL or IP Address I Get a Timeout Error

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WG102 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WG102 Access Point is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

Using the Reset Button to Restore Factory Default Settings

The Reset button (see “Rear Panel” on page 1-3) has two functions:

- *Reboot.* When pressed and released quickly, the WG102 will reboot (restart).
- *Reset to Factory Defaults.* This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WG102 Access Point and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Release the Reset button.

The factory default configuration has now been restored (see "Factory Default Settings" in Appendix A), and the WG102 Access Point is ready for use.

Appendix A
Factory Default Settings and Specifications

Factory Default Settings

When you first receive your WG102 Access Point, the default factory settings are set as shown below. You can restore these defaults with the Reset button on the rear panel — see "Rear Panel" on page 1-3.

Feature	Factory Default Settings
User name (case sensitive)	admin
Password (case sensitive)	password
Operating mode	Access point
Access point name	netgearxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address
Built-in DHCP client	DHCP client disabled, it uses the default IP address
IP configuration	IP Address: 192.168.0.229 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
Network Name (SSID)	NETGEAR-0-0
Broadcast Network Name (SSID)	Enabled
Super-G mode	Disabled
WEP/WPA	Disabled
MAC Access Control	Disabled
Restricting connectivity based on MAC Access Control List	Disabled
Time Zone	GMT
Time Zone Adjust for Daylight Saving TIme	Disabled
SNMP	Disabled
VLAN (802.1Q)	Disabled
WMM support	Disabled

Technical Specifications

Parameter	**NETGEAR WG102 ProSafe 802.11g Wireless Access Point**
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 15 to 20 nodes.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1 A
Electromagnetic Compliance	FCC Part 15 Class B, CE, C-TICK, Medical EMC EN60601
Environmental Specifications	Operating temperature: 0 to 45° C Operating humidity: 5-95%, non-condensing
Wireless	
Data Encoding:	802.11b: 1 and 2 Mbps, Direct Sequence Spread Spectrum (DSSS) 802.11b: 5.5 and 11 Mbps, Complementary Code Keying (CCK) 802.11g: All rates, Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.
802.11b and g Radio Data Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11b and g Operating Frequencies and Channels	2.412 ~ 2.462 GHz (North America), Channels 1-11 2.412 ~ 2.472 GHz (Europe including France and Spain, and Japan), Channels 1-13
802.11b and g Typical Maximum Transmit Power	802.11b mode, 1 to 11Mbps: +19 dBm* 802.11g mode, 6 to 24 Mbps: +18 dBm* 802.11g mode, 36/48/54 Mbps: +17/16/15 dBm* *Note: Maximum transmit power varies based on country or region selection to ensure local regulatory compliance.

Parameter	**NETGEAR WG102 ProSafe 802.11g Wireless Access Point**
802.11b and g Typical Receive Sensitivity	802.11b mode at 1Mbps: -95 dBm 802.11b mode at 2 Mbps: -93 dBm 802.11b mode at 5.5 Mbps: -91dBm 802.11b mode at 11 Mbps: -89 dBm 802.11g mode at 6 Mbps: -91 dBm 802.11g mode at 9 Mbps: -90 dBm 802.11g mode at 12 Mbps: -89 dBm 802.11g mode at 18 Mbps: -87 dBm 802.11g mode at 24 Mbps: -84 dBm 802.11g mode at 36 Mbps: -81 dBm 802.11g mode at 48 Mbps: -77 dBm 802.11g mode at 54 Mbps: -75 dBm 802.11g mode at 108 Mbps: -72 dBm
Antenna:	One (1) external 5 dBi 2.4 GHz detachable antenna
802.11 Security	40-bits (also called 64-bits), 128, and 152-bits WEP data encryption; WPA and WPA2

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Windows XP and Vista Wireless Configuration Utilities	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
Internet Networking and TCP/IP Addressing	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN)	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*