Reference Manual for the NETGEAR WG102 ProSafe 802.11g Wireless Access Point

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

October 2004

October 2004

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to http://www.NETGEAR.com. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at:
http://www.NETGEAR.com/ through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

© 2004 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR is a registered trademark of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

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.

Modifications made to the product, unless expressly approved by Netgear, could void the user's authority to operate the equipment. NETGEAR does not assume any liability that may occur due to such condition.

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 2 antennas, 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*
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.

*** 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 WG102 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

CE 0681 (!)

This device is a 2.4/5.0 GHz dual band low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN 300 328, EN 301 489-17, EN 60950-1 Safety of Information Technology Equipment, Including Electrical Business Equipment EN 300 328 V1.4.1 (2003-04) Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission system; data transmission equipment operating in the 2.4 Ghz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions; Part 2; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

EN 301 489-1, Aug. 2002; EN 301 489-17, Aug. 2002 - Electromagnetic compatibility and radio spectrum matters (ERM); electromagnetic compatibility (EMC); standard for radio equipment and services: Part 1: Common technical requirements; Part 17: Specific conditions for Wideband Data and Hiperlan equipment.

EN 55 022 Declaration of Conformance

This is to certify that the NETGEAR WG102 ProSafe 802.11g Wireless Access Point is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Requirements For Operation in the European Community

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

Note: The user must use the web-based configuration GUI provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device requires that the user or installer properly **enter the current country of operation** in the Wireless Settings page as described in the user guide, **before operating this devic**e.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/ outdoor restrictions and license requirements for each European Community country as described in this document.
- This device may be operated **indoors or outdoors** in all countries of the European Community using the 2.4GHz band: Channels 1 - 13, except where noted below.
    - In **Italy** the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
    - In **France** outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Declaration of Conformity in Languages of the European Community

English	Hereby, NETGEAR Inc. declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	*Valmistaja* NETGEAR Inc. vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart NETGEAR Inc. dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze NETGEAR Inc. dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente NETGEAR Inc. déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Swedish	Härmed intygar NETGEAR Inc. att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede NETGEAR Inc. erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklärt NETGEAR Inc. dass sich *dieser/diese/dieses* Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)
	Hiermit erklärt NETGEAR Inc. die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* NETGEAR Inc. *ΔΗΛΩΝΕΙ ΟΤΙ* Radio LAN device *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*
Italian	Con la presente NETGEAR Inc. dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente NETGEAR Inc. declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	NETGEAR Inc. declara que este Radio LAN device está conforme com os requisitos essenciais e o disposições da Directiva 1999/5/CE.

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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Contents

Chapter 1
About This Manual

Audience, Versions, Conventions 1-1
How to Use this Manual 1-2
How to Print this Manual 1-3

Chapter 2
Introduction

About the NETGEAR WG102 ProSafe 802.11g Wireless Access Point 2-1
Key Features 2-2
802.11g Standards-based Wireless Networking 2-3
Autosensing Ethernet Connections with Auto Uplink 2-3
Compatible and Related NETGEAR Products 2-4
System Requirements 2-4
What's In the Box? 2-5
Hardware Description 2-6

Chapter 3
Basic Installation and Configuration

Observing Placement and Range Guidelines 3-1
Cabling Requirements 3-2
Default Factory Settings 3-3
Understanding WG102 Wireless Security Options 3-4
Installing the WG102 Access Point 3-5
How to Log In to the WG102 Using Its Default IP Address 3-11
Understanding Basic Wireless Settings 3-12
Understanding WEP/WPA Security Options 3-14
Before You Change the SSID and WEP Settings 3-17
How to Set Up and Test Basic Wireless Connectivity 3-18
How to Restrict Wireless Access by MAC Address 3-19
How to Configure WEP 3-20
How to Configure WPA 3-21
How to Configure WPA-PSK 3-23

Using the Basic IP Settings Options 3-24

Chapter 4
Management

Using Syslog and Activity Log Information 4-1
Viewing General, Log, Station, and Statistical Information 4-2
Statistics 4-4
Viewing a List of Attached Devices 4-5
Upgrading the Wireless Access Point Software 4-5
Configuration File Management 4-6
Saving and Retrieving the Configuration 4-7
Restoring the WG102 to the Factory Default Settings 4-7
Using the Reset Button to Restore Factory Default Settings 4-7
Changing the Administrator Password 4-8
Using SNMP Remote Management 4-9

Chapter 5
Advanced Configuration

Hotspot Settings 5-1
Configuring Advanced Wireless Settings 5-2
AP Settings: Enabling Wireless Bridging and Repeating 5-3
How to Configure a WG102 as a Point-to-Point Bridge 5-4
How to Configure Multi-Point Wireless Bridging 5-5
How to Configure Wireless Repeating 5-6

Chapter 6
Troubleshooting

No lights are lit on the access point. 6-1
The Wireless LAN activity light does not light up. 6-2
The LAN light is not lit. 6-2
I cannot access the Internet or the LAN with a wireless capable computer. 6-2
I cannot connect to the WG102 to configure it. 6-3
When I enter a URL or IP address I get a timeout error. 6-3
Using the Reset Button to Restore Factory Default Settings 6-3

Appendix A
Specifications

Specifications for the WG102 ..... A-1

Appendix B
Wireless Networking Basics

Wireless Networking Overview B-1
Infrastructure Mode B-1
Ad Hoc Mode (Peer-to-Peer Workgroup) B-2
Network Name: Extended Service Set Identification (ESSID) B-2
Authentication and WEP Data Encryption B-2
802.11 Authentication B-3
Open System Authentication B-3
Shared Key Authentication B-4
Overview of WEP Parameters B-5
Key Size B-6
WEP Configuration Options B-7
Wireless Channels B-7
WPA Wireless Security B-8
How Does WPA Compare to WEP? B-9
How Does WPA Compare to IEEE 802.11i? B-10
What are the Key Features of WPA Security? B-10
WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS B-12
WPA Data Encryption Key Management B-14
Is WPA Perfect? B-16
Product Support for WPA B-16
Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged B-16
Changes to Wireless Access Points B-17
Changes to Wireless Network Adapters B-17
Changes to Wireless Client Programs B-18

Glossary

Index

Chapter 1
About This Manual

Congratulations on your purchase of the NETGEAR WG102 ProSafe 802.11g Wireless Access Point. The WG102 provides connection for multiple personal computers to the Internet through an external broadband access device (such as a cable modem or DSL modem).

Audience, Versions, Conventions

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, tutorial information is provided in the Appendices and on the NETGEAR Web site.

This guide uses the following formats to highlight special messages:

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

This manual is written for the WG102 Access Point according to these versions.:

Table 1-1. Product, Firmware Version, Manual Version, and Publication Date

Product	NETGEAR WG102 ProSafe 802.11g Wireless Access Point
Manual Part Number	
Manual Publication Date	October 2004

	Note: Product updates are available on the NETGEAR Web site at *www.netgear.com/support/main.asp*.

How to Use this Manual

The HTML version of this manual includes a variety of navigation features as well as links to PDF versions of the full manual and individual chapters.

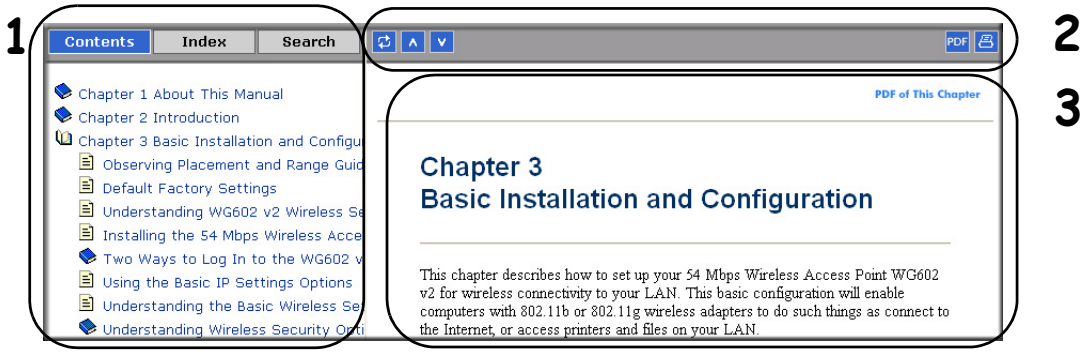


Figure 1-1: HTML version of this manual

1. **Left Pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 4 or later browser with JavaScript enabled.

2. **Toolbar Buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   The Show in Contents button locates the current topic in the Contents tab.

   Previous/Next buttons display the previous or next topic.

   The PDF button links to a PDF version of the full manual.

   The Print button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer–you do not have to worry about specifying the correct range of pages.

3. **Right Pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a PDF of This Chapter link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

To print this manual, choose one of the following options.

- **Printing a "How To" Sequence of Steps in the HTML View**. Use the *Print* button on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer–you do not have to worry about specifying the correct range of pages.
- **Printing a Chapter**. Use the PDF of This Chapter link at the top right of any page.
  - Click "PDF of This Chapter" link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

    Note: 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*.
  - Click the print icon in the upper left of the 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.
- **Printing the Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click the PDF button on the upper right of the toolbar. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of the 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.

Chapter 2
Introduction

This chapter introduces the NETGEAR NETGEAR WG102 ProSafe 802.11g Wireless Access Point. Minimal prerequisites for installation are presented in "System Requirements" on page 2-4.

About the NETGEAR WG102 ProSafe 802.11g Wireless Access Point

The NETGEAR WG102 ProSafe 802.11g Wireless Access Point is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The WG102 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area with about a 300 foot radius. The NETGEAR WG102 ProSafe 802.11g Wireless Access Point can support a small group of users in a range of several hundred feet. Most access points are rated between 30-50 users simultaneously.

The NETGEAR WG102 ProSafe 802.11g Wireless Access Point acts as a bridge between the wired LAN and wireless clients. Connecting multiple WG102 Access Points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network.

The auto-sensing capability of the NETGEAR WG102 ProSafe 802.11g Wireless Access Point allows packet transmission at up to 108 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features

The WG102 Access Point is easy-to-use and provides solid wireless and networking support.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliant.** The Wireless Access Point complies with the IEEE 802.11g for Wireless LANs.
- **WEP support.** Support for WEP is included. 64-bit, 128-bit, and 152-bit keys are supported.
- **Full WPA support.** WPA enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WG102 can act as a client and obtain information from your DHPC server.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.

Key Features

The NETGEAR WG102 provides solid functionality, including these features:

- **Multiple Operating Modes**
  - **Wireless Access Point.** Operates as a standard 802.11g.
  - **Point-to-Point Bridge.** In this mode, the WG102 only communicates with another bridge-mode wireless station. You must enter the MAC address (physical address) of the other bridge-mode wireless station in the field provided. WEP should be used to protect this communication.
  - **Point-to-Multi-Point Bridge.** Select this only if this WG102 is the “Master” for a group of bridge-mode wireless stations. The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using this WG102's MAC address. They then send all traffic to this “Master”, rather than communicate directly with each other. WEP should be used to protect this traffic.
  - **Wireless Repeater.** In this half-duplex mode, the WG102 only communicates with another repeater-mode wireless station. You must enter the MAC address of both adjacent repeater-mode wireless stations in the fields provided. WEP should be used to protect this communication.

- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WG102 to gain access to your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they are easy to change.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Power over Ethernet.** Power can be supplied to the WG102 over the Ethernet port from any 802.3af compliant mid-span or end-span source such as the NETGEAR FSM7326P Managed Power over Ethernet Layer 3 managed switch.
- **Autosensing Ethernet Connection with Auto Uplink Interface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power, test, LAN speed, LAN activity, and wireless activity are easily identified.

802.11g Standards-based Wireless Networking

The NETGEAR WG102 ProSafe 802.11g Wireless Access Point provides a bridge between Ethernet wired LANs and 802.11g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the WG102 supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Short or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The WG102 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The wireless access point incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a computer or an 'uplink' connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Compatible and Related NETGEAR Products

For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA, see *http://www.wi-fi.net*).

The following NETGEAR products work with the WG102 Access Point:

- WAG511 a/b/g 108 Mbps Dual Band Wireless PC Card Adapter
- WAG311 802.11a/g 54 Mbps Wireless PCI Card
- WG311T 802.11g 108 Mbps Wireless PCI Card
- WG311 802.11g 54 Mbps Wireless PCI Card
- WG511T 802.11g 108 Mbps Wireless CardBus Adapter
- WG511 802.11g 54 Mbps Wireless CardBus Adapter
- WG111 801.11g 54 Mbps Wireless Bridge

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's In the Box?

The product package should contain the following items:

- NETGEAR WG102 ProSafe 802.11g Wireless Access Point
- Power adapter and cord (12 V dc, 1.2 A)
- Straight through Category 5 Ethernet cable
- WG102 802.11g ProSafe Wireless Access Point Installation Guide
- *Resource CD for the NETGEAR WG102 ProSafe 802.11g Wireless Access Point*

  This Reference Manual 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. You can refer to 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.
The WG102 Access Point provides four status LEDs.

NEED PRODUCT PHOTO OR ILLUSTRATION

Figure 2-1: WG102 front panel

The following table explains the LED indicators:

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 4, 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.
LAN	Ethernet link indicator
Off	No connection detected on the Ethernet link
Amber On	Indicates 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	Indicates no wireless link activity.
Green Blink	Wireless link activity.

NEED PRODUCT PHOTO OR ILLUSTRATION

Figure 2-2: WG102 rear panel

- **Detachable Antenna**

  The WG102 provides one detachable antenna.

- **Restore to Factory Defaults Button**

  The restore to default button located between the Ethernet RJ-45 connector and the power socket restores the WG102 to the factory default settings.

- **RJ-45 Ethernet Port**

  Use the WG102 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or POE switch.

- **Power Socket**

  This socket connects to the WG102 12V 1.2A power adapter.

Chapter 3
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.

	Note: Indoors, computers can connect over 802.11g wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WG102 Access Point provides highly effective security features which are covered in detail in Chapter 3, "Configuring Your Wireless Network. Deploy the security features appropriate to your needs.

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the WG102 that conforms to the Observing Placement and Range Guidelines below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b or 802.11g wireless adapters.

Observing Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement 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, “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 if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- 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 5 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. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Cabling Requirements

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

Default Factory Settings

When you first receive your WG102, the default factory settings will be set as shown below. You can restore these defaults with the Factory Default Restore switch on the rear panel — see "WG102 front panel" on page 2-6.

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 enabled, however reverts to default IP address when no DHCP server detected**
IP Configuration (if DHCP server is unavailable)	**IP Address: 192.168.0.229** **Subnet Mask: 255.255.255.0** **Gateway: 0.0.0.0**
Network Name (SSID)	**NETGEAR**
Broadcast Network Name (SSID	**Enabled**
802.11g Radio Frequency Channel	**11**
WEP/WPA	**Disabled**
Restricting connectivity based on MAC Access Control List	**Disabled**
Time Zone	**GMT**
Time Zone Adjust for Daylight Saving TIme	**Disabled**
SNMP	**Enabled but Trap forwarding is disabled**

Understanding WG102 Wireless 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.

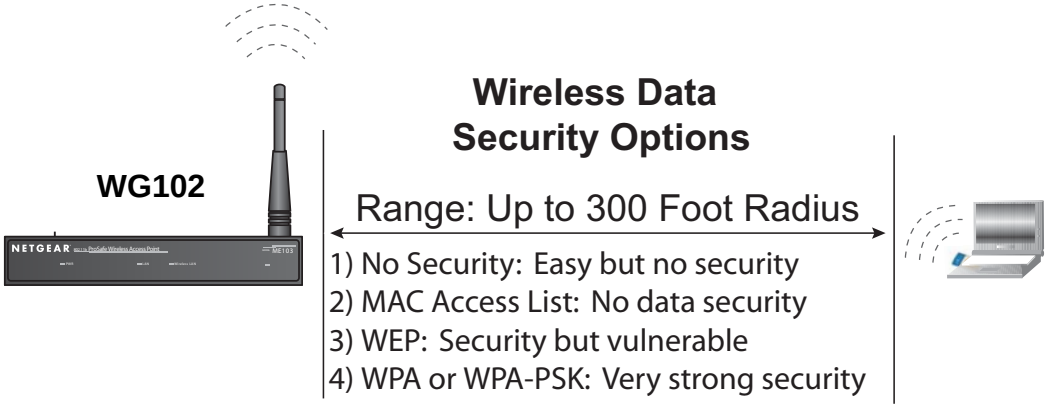


Figure 3-1: WG102 wireless data security options

There are several ways you can enhance the security of your wireless 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.
- **Use 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.

- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) 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.

Installing the WG102 Access Point

Before installing the NETGEAR WG102 ProSafe 802.11g Wireless Access Point, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b or 802.11g wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on page 2-4.

1 Set up the WG102 Access Point

Tip: Before mounting the WG102 in a high location, first set up and test the WG102 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 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. Configure the WG102 Ethernet port for LAN access.

- Connect to the WG102 by opening your browser and entering *http://192.168.0.229* in the address field. A login window like the one shown below opens:

NEED PRODUCT PHOTO OR ILLUSTRATION

Figure 3-2: Login window

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

- The Web browser will then display the WG102 settings page.

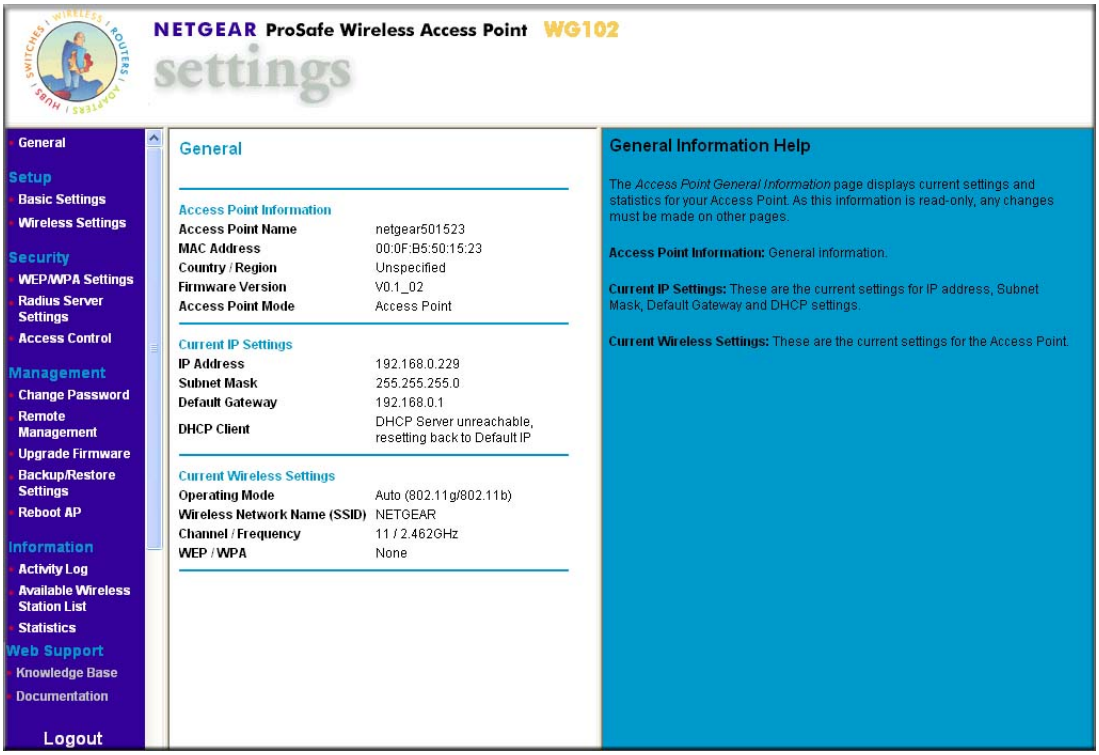


Figure 3-3: Login result: WG102 home page

  - When the wireless access point is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless access point.
  - If you do not click Logout, the wireless access point will wait 5 minutes after there is no activity before it automatically logs you out.

- Click the Basic Settings link to view the Basic Settings menu.

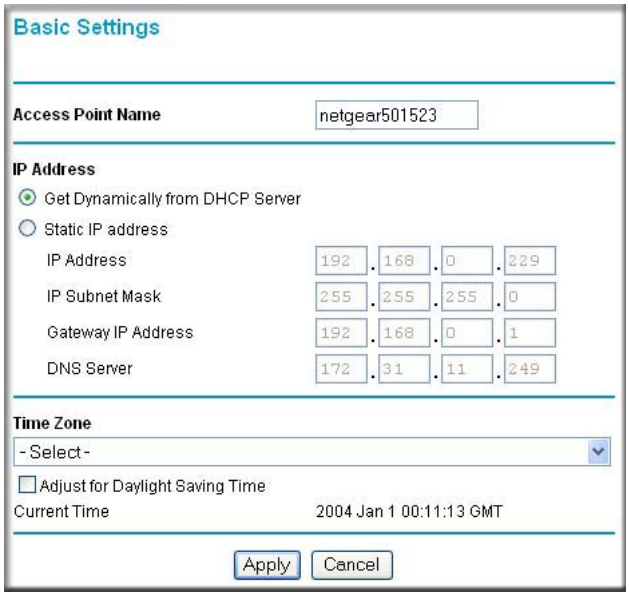


Figure 3-4: Basic Settings menu

- Configure the settings appropriate for your network.

b. Click the Wireless Settings link in the Setup section of the main menu to view the Wireless Settings menu.

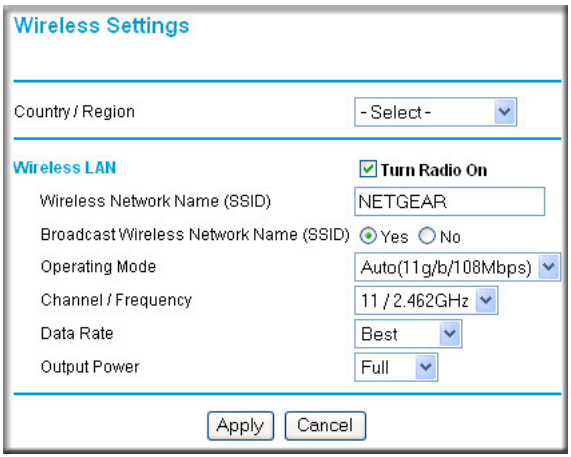


Figure 3-5: Basic Wireless Settings menu

c. Configure the wireless interface for wireless access. See the online help or the Understanding Basic Wireless Settings topic of this Reference Manual for full instructions.

Note: You 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 steps, you are ready to deploy the WG102 in your network. If needed, you can now reconfigure the computer you used in step 1 back to its original TCP/IP settings.

3 Deploy the WG102 Access Point

a. Disconnect the WG102 and position 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 so that they are vertical.

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

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

Note: By default, WG102 is set to with the DHCP client disabled. If your network uses dynamic IP addresses, you will need to 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 (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 6, “Troubleshooting.”

How to Log In to the WG102 Using Its Default IP Address

1. 192.168.0.229 is the default IP address of your access point. The WG102 is set, by default, the DHCP client to be disabled.

   Note: The computer you are using to connect to the WG102 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

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

4. A login window like the one shown below opens:

Figure 3-6: Login window

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

Once you have entered your access point name, your Web browser should automatically find the WG102 Access Point and display the home page, as shown in "Login result: WG102 home page" on page 3-7.

Understanding Basic Wireless Settings

To configure the wireless settings of your wireless access point, click the Wireless Settings link in the Basic section of the main menu of the browser interface. The Basic Wireless Settings menu will appear, as shown below.

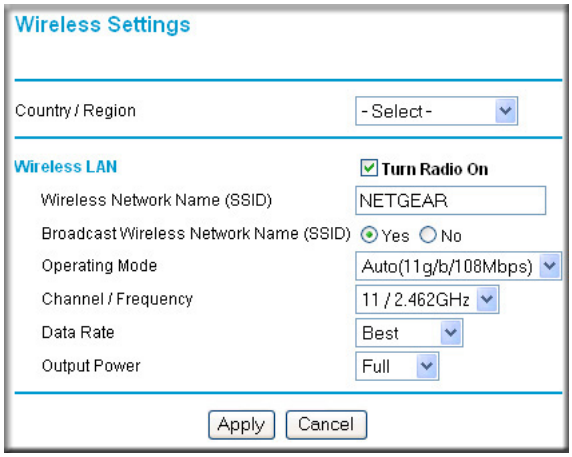


Figure 3-7: Basic Wireless Settings menu

The Basic Wireless Settings menu options are discussed below:

- **Country/Region.** This field identifies 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. There is no default country domain, and the channel is set to 11. 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.
- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use the SSID. The WG102 default SSID is: **NETGEAR**.
  - A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).

- Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).
- A group of wireless stations and multiple access points, all using the same ID (ESSID), form an Extended Service Set (ESS).
- Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points *should* use different channels.
- As wireless stations physically move through the area covered by an ESS, they will automatically change to the access point which has the least interference or best performance. This capability is called roaming.

  Note: The AutoCell feature enhances the roaming, interference, and channel selection of an extended wireless network.

- **Broadcast Wireless Network Name (SSID).** This field lets you turn off the SSID broadcast. If you turn off the SSID broadcast, only stations that know the SSID will connect. Disabling SSID broadcast somewhat hampers the wireless network ‘discovery’ feature of some products. The default is to enable SSID broadcast.
- **Operating Mode**. Select the desired wireless operating mode. The options are:
  - Auto (11g/b) – Both 802.11g and 802.11b wireless stations can be used. This is the default.
  - 11g Only - Only 802.11g wireless stations can be used. This is required for 108 Mbps data rate operation.
  - 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 field identifies which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems or setting up the WG102 near another access point. See “Wireless Channels” on page B-7 for more information on wireless channels.
  - Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available.

    Note: Channel 6 is required for 108 Mbps data rate.
  - 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 5 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 various access points are using the same SSID.

- **Data Rate**. Shows the available transmit data rate of the wireless network. 108 Mbps is only available when the operating mode is 802.11g only and the channel is 6. The default is Best.
- **Output Power**. Set the transmit signal strength of the access point. The options are full, half, quarter, eighth, and min. Decrease the transmit power if more than one AP is colocated using the same channel frequency. The default is Full.

Understanding WEP/WPA Security Options

The table below identifies the various WEP/WPA security options. A full explanation of these standards is available in Appendix B, “Wireless Networking Basics”.

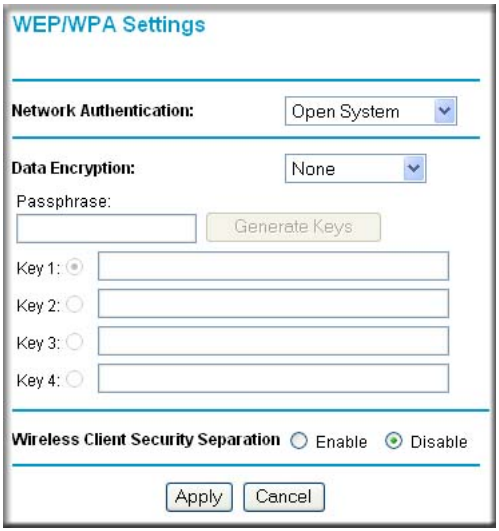


Figure 3-8: Wireless Security Settings

- Enable Wireless Client Security Separator

  The associated wireless clients will not be able to communicate with each other if this feature is enabled. The default setting is disabled.

The Wireless LAN options are explained in the following table.

Table 3-1. Basic Wireless Security Options

Field	Description
Network Authentication	You can select the following network authentication options: • Open System: the WG102 does not perform any authentication. However, if the 802.1x option is configured, authentication of connections can be performed by a RADIUS server. • Shared: this is for shared key authentication. The SSID and data are encrypted.
Encryption Strength	You can select the following data encryption options: • Disabled • 64- 128- or 152-bit WEP With Open System Authentication and 64- 128- or 152-bit WEP Data Encryption, the WG102 *does* perform data encryption but *does not* perform any authentication.
Security Encryption (WEP) Keys	If WEP is enabled, 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 (key 1 must be the same for all, key 2 must be the same for all, etc.) There are two methods for creating WEP encryption keys: • Passphrase. These characters *are* case sensitive. Enter a word or group of printable characters in the Passphrase box and click the Generate button. **Note**: Not all wireless adapters support passphrase key generation. • Manual. These values *are not* case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). 152-bit WEP: enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F).
Enable Wireless Security Separator	The associated wireless clients will not be able to communicate with each other if this feature is enabled. The default setting is Disable.

Table 3-1. Basic Wireless Security Options

Field	Description
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. For a full explanation of WPA, see "WPA Wireless Security" on page B-8. **Note**: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.
WPA with RADIUS	User authentication is implemented using RADIUS servers. For a full explanation of WPA, see "WPA Wireless Security" on page B-8. **Authentication/Access Control Radius Server Login Requirements** You will also have to fill in the following Radius server settings: • Primary Radius Server Name/IP Address This field is required. Enter the name or IP address of the Radius Server on your LAN. • Secondary Radius Server Name/IP Address This field is optional. Enter the name or IP address of the Secondary Radius Server on your LAN. • Radius Port Enter the port number used for connections to the Radius Server. • Radius Shared Key Enter the desired value for the Radius shared key. This key enables the WG102 to log in to the Radius server and must match the value used on the Radius server. **Radius Accounting Option** The Radius Accounting option can be enabled so that you can track various information like who connected to the network, when they connected, how long they were connected, how much network traffic they generated, and so on.

Before You Change the SSID and WEP Settings

Take the following steps:

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. **Wireless** is the default WG102 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  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 as well 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 or 128 bits

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____
- **WPA-PSK (Pre-Shared Key)**

  Record the WPA-PSK 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: _____

Use the procedures described in the following sections to configure the WG102. Store this information in a safe place.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the WG102 using its default address of *http://192.168.0.229* or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever password you set up.
2. Click the Wireless Settings link in the main menu of the WG102.
3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

   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.
4. Select the Country/Region in which the wireless interface will operate.
5. Set the Channel. It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point. For more information on the wireless channel frequencies see "Wireless Channels" on page B-7.
6. For initial configuration and testing, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."
7. Click Apply to save your changes.

	Note: If you are configuring the WG102 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.

8. Configure and test your PCs for wireless connectivity.

   Program the wireless adapter of your PCs to have the same SSID and channel that you configured in the WG102. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WG102.

Once your PCs have basic wireless connectivity to the WG102, you can configure the advanced wireless security functions.

How to Restrict Wireless Access by MAC Address

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

1. Log in to the WG102 using its default address of *http://192.168.0.229* or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.

	Note: When configuring the WG102 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. From the Security menu, click the Access Control link to display the Access Control List menu shown below.

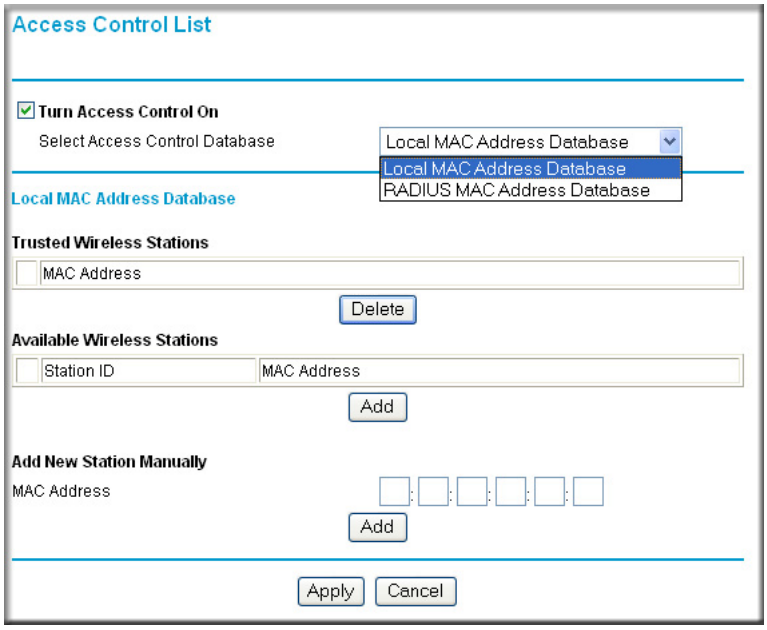


Figure 3-9: Access Control List menu

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.

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the WG102 using its default address of *http://192.168.0.229* or at whatever IP address the unit is currently configured Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Click the WEP/WPA Settings link in the main menu of the WG102.

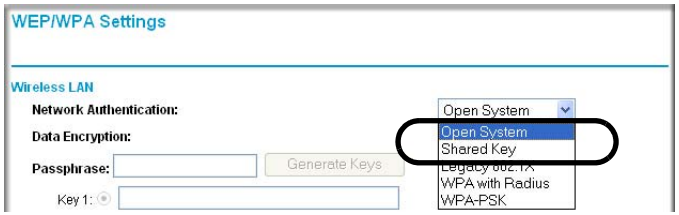


Figure 3-10: Wireless Settings menu

3. Choose Open System or Shared Key authentication.
4. Select encryption strength.
5. 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 box and click the Generate button. The four key boxes 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 "Overview of WEP Parameters" on page B-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

6. 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.

How to Configure WPA

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Radius Server Settings** in the Security menu.

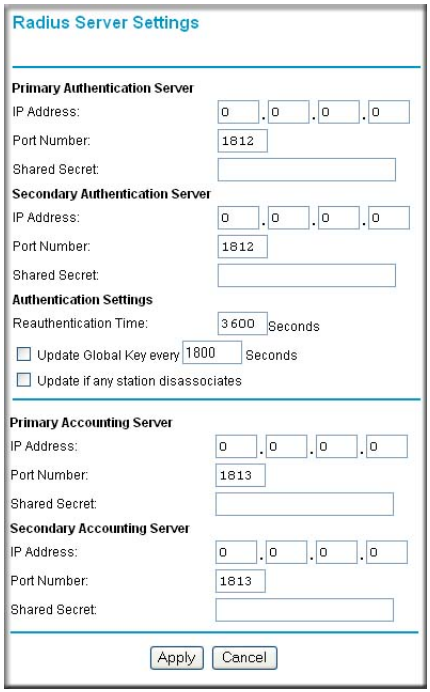


Figure 3-11: Wireless Settings menu

3. Enter the Radius settings.
4. Click **Apply** to save your settings.
5. Click **WEP/WPA Settings** in the Security menu.

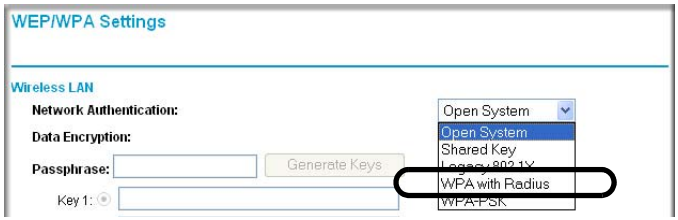


Figure 3-12: Wireless Settings menu

6. Choose **WPA with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA-PSK

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **WEP/WPA Settings** in the Security menu of the WG102.

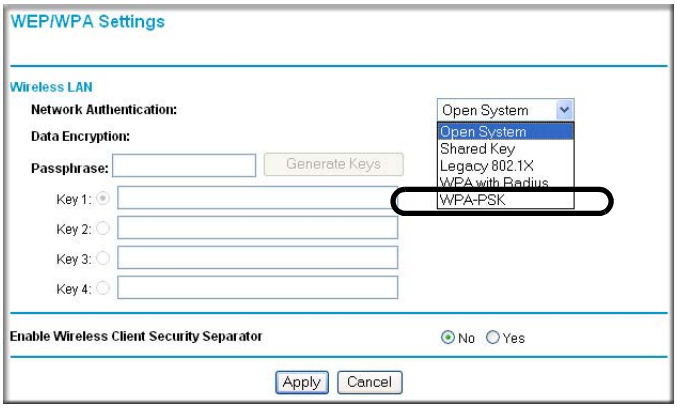


Figure 3-13: Wireless Settings menu

3. Choose **WPA-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.

Using the Basic IP Settings Options

The Basic IP Settings menu is under the Basic heading of the main menu. Use this menu to configure DHCP, static IP, and access point access point name settings.

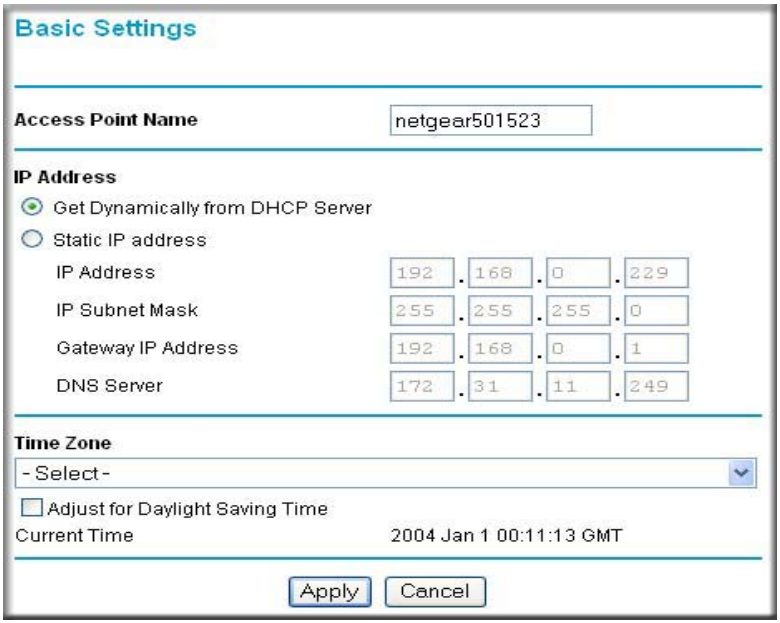


Figure 3-14: IP Settings menu

- **Access Point Name (NetBIOS)**

  Enter a new name for the wireless access point and click Apply to save your changes.

- **The IP Address**

  The wireless access point is shipped preconfigured with its DHCP client disabled and with the following private static IP addresses:

  – IP Address — 192.168.0.229
  – IP Subnet Mask — 255.255.255.0
  – Gateway — 0.0.0.0
  – Primary and Secondary DNS Servers — 0.0.0.0

If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu. These settings are only required if the “Use this IP address” radio button is chosen. Remember to click Apply to save your changes.

- **Time Zone**

  Select the time zone setting for your location.

Chapter 4
Management

This chapter describes how to use the management features of your NETGEAR WG102 ProSafe 802.11g Wireless Access Point. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Using Syslog and Activity Log Information

The Information contains the activity log link you can use for setting up a syslog server and viewing activity log information. From the main menu of the browser interface, under the Information heading, click the Station List link to view the list, shown below.

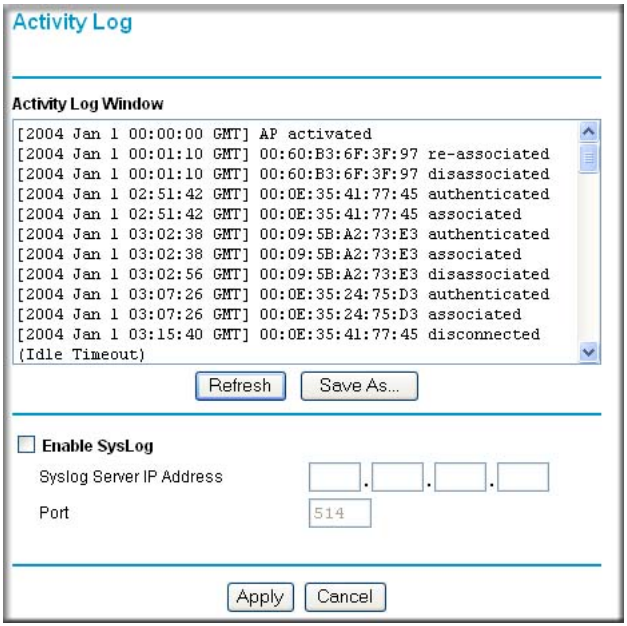


Figure 4-1: Syslog and Activity Log information

Enable the SysLog option if you have a SysLog server on your LAN. If enabled, you must enter the IP address of your SysLog server and the port number your SysLog server is configured to use.

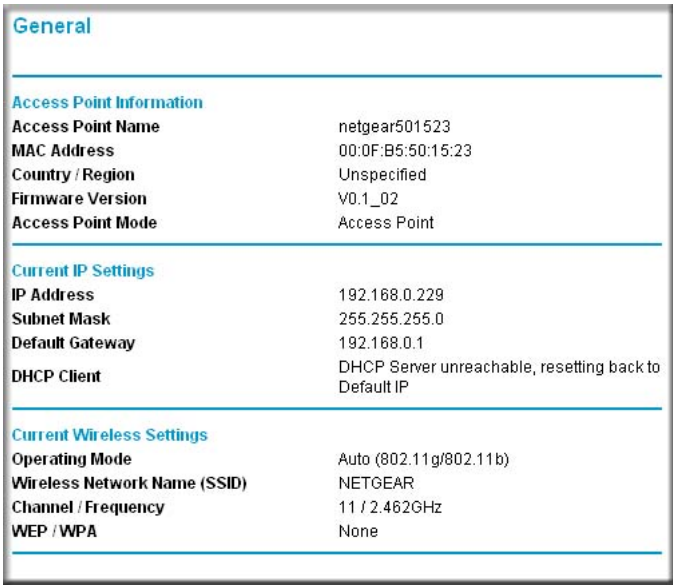
- SysLog Server IP address: The access point will send all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0
- Port: The port number configured in the SysLog server on your LAN. Default: 514

The Activity Log Window displays the Access Point system activity.

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

Viewing General, Log, Station, and Statistical Information

The General information screen provides a summary of the current WG102 configuration settings. From the main Menu of the browser interface, click General to view the System Status screen, shown below.



General

Access Point Information	
Access Point Name	netgear501523
MAC Address	00:0F:B5:50:15:23
Country / Region	Unspecified
Firmware Version	V0.1_02
Access Point Mode	Access Point
Current IP Settings	
IP Address	192.168.0.229
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DHCP Client	DHCP Server unreachable, resetting back to Default IP
Current Wireless Settings	
Operating Mode	Auto (802.11g/802.11b)
Wireless Network Name (SSID)	NETGEAR
Channel / Frequency	11 / 2.462GHz
WEP / WPA	None

Figure 4-2: Wireless Access Point Status screen

This screen shows the following parameters:

Table 4-1. General Information Fields

Field	Description
Access Point Information	
Access Point Name (NetBIOS name)	The default name may be changed if desired.
MAC Address	Displays the Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Country/Region	Displays 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	Identifies the operating mode of the WG102: Access Point, Point-to-point bridge, Multi-point bridge or Repeater.
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	Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicates a static IP configuration.
Current Wireless Settings	
Operating Mode	Identifies the 802.11 operating mode of the WG102.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR.
Channel/Frequency	Identifies the channel the wireless port is using. 11 is the default channel setting. See "Wireless Channels" on page B-7 for the frequencies used on each channel.
WEP/WPA	WEP/WPA setting.

Statistics

The Information - Statistics screen provides various LAN and WLAN statistics.

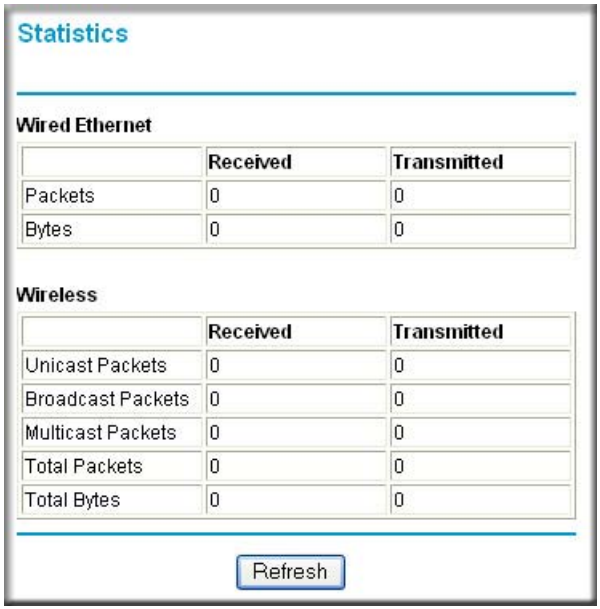


Figure 4-3: Wireless Access Point Status screen

Table 4-1. Statistics Fields

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.
Wireless	**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.

Viewing a List of Attached Devices

The Available Wireless Station List contains a table of all IP devices associated with the wireless access point in the wireless network defined by the Wireless Network Name (SSID). From the main menu of the browser interface, under the Information heading, click the Available Wireless Station List link to view the list, shown below.

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 enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point will be presented in the Available Station List.

Upgrading the Wireless Access Point Software

	Note: When uploading software to the WG102 Access Point, it is important not to 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 software, and render the WG102 completely inoperable.

You cannot perform the firmware upgrade from a workstation connected to the WG102 via a wireless link. The firmware upgrade must be performed via a workstation connected to the WG102 via the Ethernet LAN interface.

The software of the WG102 Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.IMG) file before sending 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 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file from NETGEAR, save it to your hard disk, and unzip it.
2. From the main menu Management section, click the Upgrade Firmware link to display the screen above.
3. In the Upgrade Firmware menu, click the Browse button and browse to the location of the image (.IMG) upgrade file.
4. Click Upload.

   When the upload completes, your wireless access point will automatically restart. 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 user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

From the main menu Management heading, click the Backup/Restore Settings link to bring up the menu shown below.

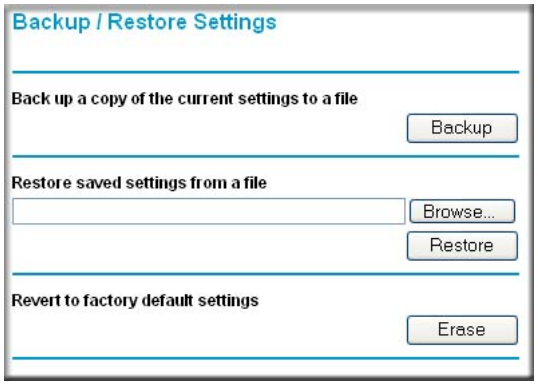


Figure 4-4: Settings Backup menu

The three options displayed are described in the following sections:

Saving and Retrieving the Configuration

The Backup/Restore Settings menu allows you to save or retrieve a file containing your wireless access point's configuration settings.

To save your settings, click the Save button. Your browser will extract 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 Retrieve button to upload the file. After completing the upload, the WG102 will reboot automatically.

Restoring the WG102 to the Factory Default Settings

It is sometimes desirable to restore the wireless access point to the factory default settings. This can be done by using the Restore function, which restores all factory settings. After a restore, the wireless access point's password will be **password**, the WG102's DHCP client is enabled, the default LAN IP address is 192.168.0.229, and the access point name is reset to the name printed on the label on the bottom of the unit.

Using the Reset Button to Restore Factory Default Settings

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless access point (see "WG102 rear panel" on page 2-7). The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point 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
2. Hold the Reset Button down while you Power On the WG102 for 5 seconds.
3. Continue holding the Reset Button until the LEDs blink twice.
4. Release the Reset Button.

The factory default configuration has now been restored, and the WG102 is ready for 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 of the browser interface, under the Management heading, click Change Password to bring up the menu shown below.

Figure 4-5: Set Password menu

To change the password, first enter the old password, and then enter the new password twice. Click Apply to save your change.

Using 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 of the browser interface, under the Management heading, click the Remote Management link to view this menu.

Figure 4-6: Remote Management settings

- **Public Community Name (Default: public)**: The community string to allow the SNMP manager to read the wireless Access Point's MIB objects.
- **Private Community Name (Default: private)**: The community string to allow the SNMP manager to read and write the wireless Access Point's MIB objects.
- **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

Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your NETGEAR WG102 ProSafe 802.11g Wireless Access Point:

- **Hotspot Settings**: Set up advanced wireless LAN parameters.
- **Wireless Settings**: Set up advanced wireless LAN parameters.
- **Access Point Settings**: Enable wireless bridging and repeating.

These features can be found under the Advanced heading in the main menu.

Hotspot Settings

If you want the AP to capture and re-direct 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.

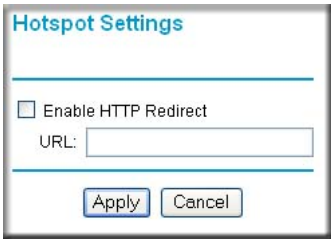


Figure 5-1: Hotspot Settings screen

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

Configuring Advanced Wireless Settings

The default advanced wireless LAN parameter settings usually work well. If you want the AP to operate in Supger-G mode, use this feature.

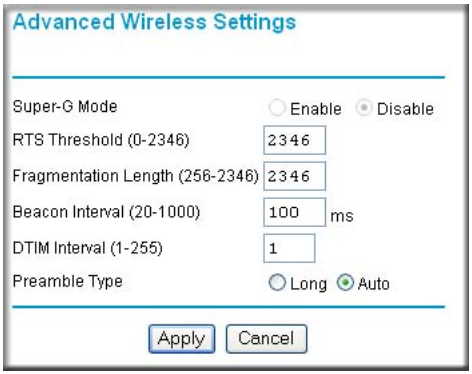


Figure 5-2: Advanced Wireless Settings screen

The table below describes the advanced wireless parameters.

Table 5-1. Advanced Wireless LAN Settings Fields

Field	Description
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. Select Enable or Disable as required.
RTS Threshold	The packet size used to determine whether it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.
Fragmentation Length	This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.
Beacon Interval	Specifies the data beacon rate between 20 and 1004.
DTIM Interval	The Delivery Traffic Indication Message specifies the data beacon rate between 1 and 255.
Preamble Type	A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Long is the default
Antenna	Select the desired antenna for transmitting and receiving. Auto is the default.

AP Settings: Enabling Wireless Bridging and Repeating

The WG102 Access Point lets you build large bridged wireless networks.

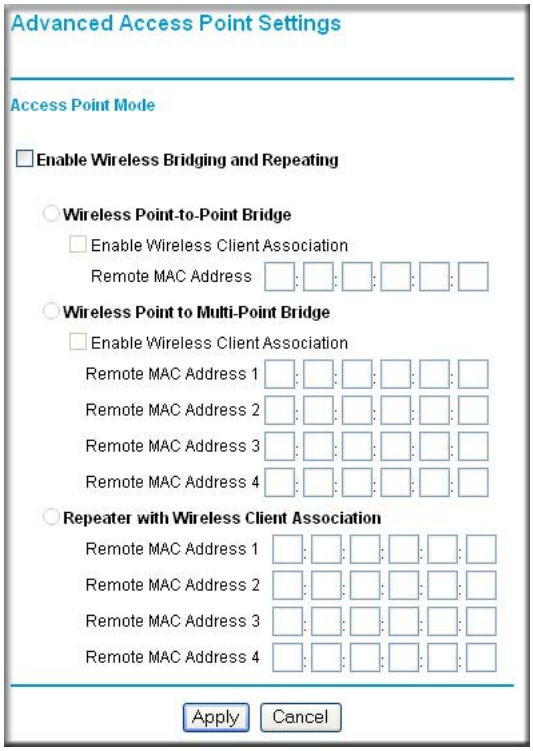


Figure 5-3: Advanced Wireless Settings Access Point Mode settings

Examples of wireless bridged configurations are:

- Client Access Point to Access Point, the default
- Point-to-Point Bridge
- Multi-Point Bridge
- Repeater with Wireless Client Association

These features are discussed below.

How to Configure a WG102 as a Point-to-Point Bridge

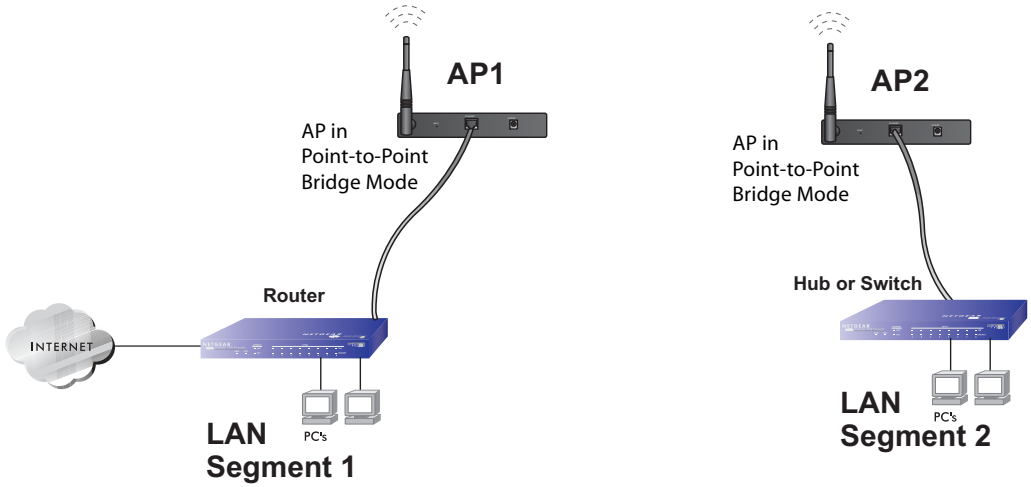


Figure 5-4: Point-to-Point Bridge

1. Configure the WG102 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the WG102 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.
   AP1 must have AP2's MAC address in its Remote MAC Address field and AP2 must have AP1's MAC address in its Remote MAC Address field.
3. Configure and verify the following parameters for both access points:
   - Verify that the LAN network configuration of the WG102 Access Points both are configured to operate in the same LAN network address range as the LAN devices
   - Both 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.

How to Configure Multi-Point Wireless Bridging

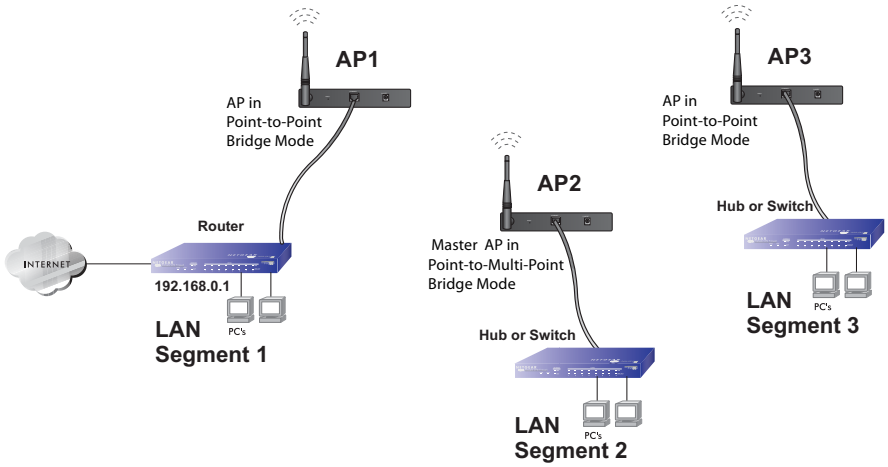


Figure 5-5: Multi-Point bridging

1. Configure the Operating Mode of the WG102 Access Points.
   - WG102 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
   - Because it is in the central location, configure WG102 (AP2) on LAN Segment 2 in Point-to-Multi-Point Bridge mode. The MAC addresses of the adjacent APs are required in AP2.
   - Configure the WG102 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
2. Verify the following parameters for all access points:
   - Verify that the LAN network configuration 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 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 WG102s 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.

How to Configure Wireless Repeating

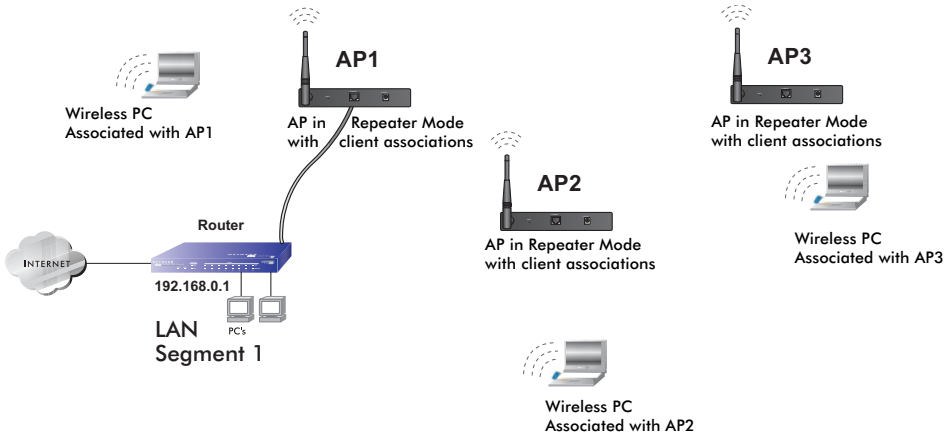


Figure 5-6: Multi-Point bridging

1. Configure the Operating Mode of the WG102 Access Points.
   - WG102 (AP1) on LAN Segment 1 in Repeater mode with the Remote MAC Address of AP2.
   - Configure WG102 (AP2) in Repeater mode with MAC addresses of AP1 and AP3.

– Configure the WG102 (AP3) in Repeater mode with the Remote MAC Address of AP2.

2. Verify the following parameters for all access points:
   - Verify that the LAN network configuration 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 2 additional WG102s configured in repeater mode. However, since Repeater configurations 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 6
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 on?
- Have I connected the wireless access point correctly?

  Go to "Installing the WG102 Access Point" on page 3-5.
- I cannot remember the wireless access point's configuration password.

  Go to "Changing the Administrator Password" on page 4-8.

	Note: For up-to-date WG102 installation details and troubleshooting guidance visit *www.NETGEAR.com*.

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.

The Wireless LAN activity light does not light up.

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.

The LAN light is not lit.

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.

I 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.

I cannot connect to the WG102 to configure it.

Check these items:

- The WG102 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green 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 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 “WG102 rear panel” on page 2-7) 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 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, and the WG102 is ready for use.

Appendix A
Specifications

This appendix provides technical specifications for the NETGEAR WG102 ProSafe 802.11g Wireless Access Point.

Specifications for the WG102

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 and Class E
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing
Wireless	
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: 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, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11g Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.412 ~ 2.484 GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI) 2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)

Parameter	NETGEAR WG102 ProSafe 802.11g Wireless Access Point
802.11b and g Typical Transmit Power Typical Receive Sensitivity	 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* 802.11b mode at 1/2/5.5/11Mbps: -95/-93/-91/-89 dBm 802.11g mode at 6/9/12/18/24/36/48/54 Mbps: -91/-90/-87/-84/-81/-77/-75 dBm Note: Maximum transmit power varies based on country or region selection to ensure local regulatory compliance.
Antenna:	One (1) external 5 dBi 2.4 GHz detachable antenna
802.11 Security	40-bits (also called 64-bits), 128-bits WEP data encryption, and WPA

Appendix B
Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The WG102 Access Point conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.11g standards for wireless LANs (WLANs). On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11b wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID **ANY.** This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

Authentication and WEP Data Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined these two types of authentication methods:

- **Open System**. With Open System authentication, a wireless computer can join any network and receive any messages that are not encrypted.

- **Shared Key**. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point, such as the one built in to the WG102:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.

2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated below.

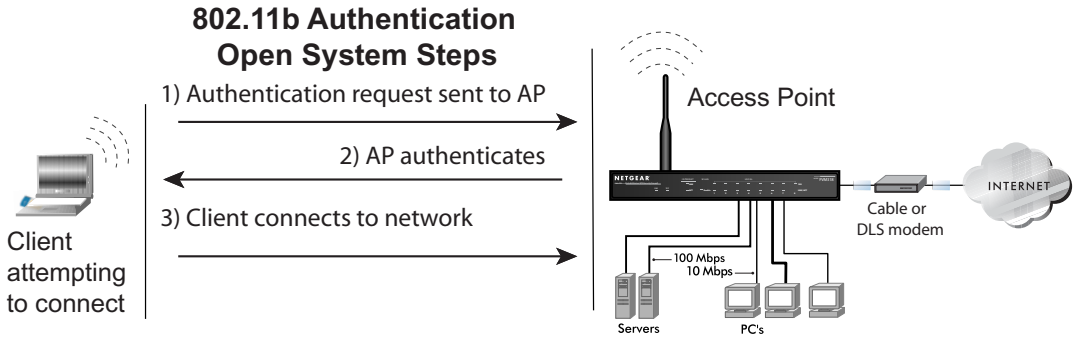


Figure B-1: Open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated below.

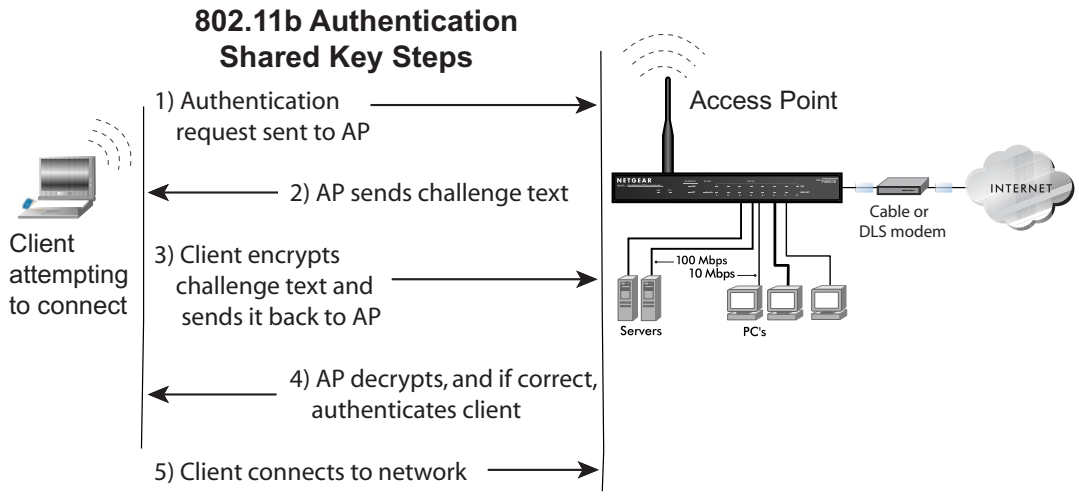


Figure B-2: Shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the wireless network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Table B-1: Encryption Key Sizes

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters’ configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, and so on.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

The wireless frequencies used by 802.11b/g networks are discussed below.

IEEE 802.11b/g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used in 802.11b/g networks are listed in Table B-2:

Table B-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz

Table B-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products will have to support WPA. NETGEAR will implement WPA on client and access point products and make this available in the second half of 2003. Existing Wi-Fi certified products will have one year to add WPA support or they will lose their Wi-Fi certification.

The 802.11i standard is currently in draft form, with ratification due at the end of 2003. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on WPA as an interoperable interim standard.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support (to be phased in)
- Support for a Mixture of WPA and WEP Wireless Clients, but mixing WEP and WPA is discouraged

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).

- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.

- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

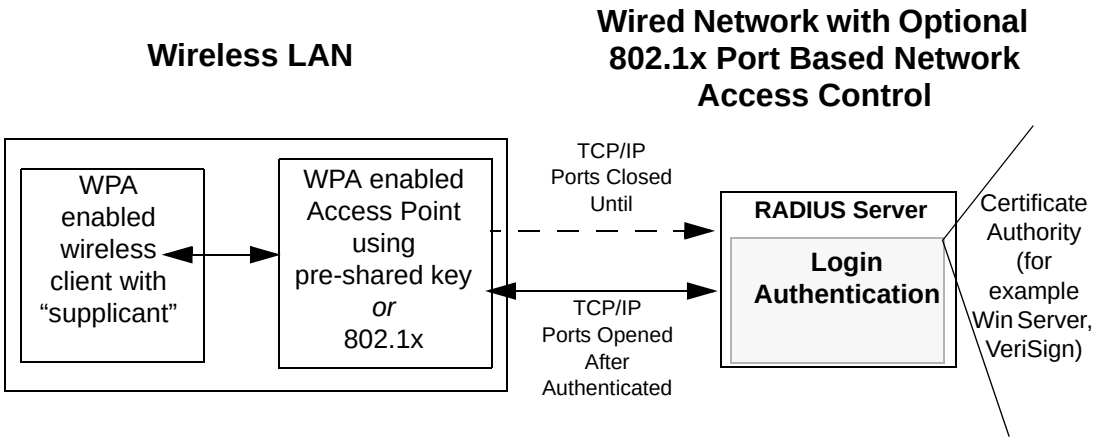


Figure B-3: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

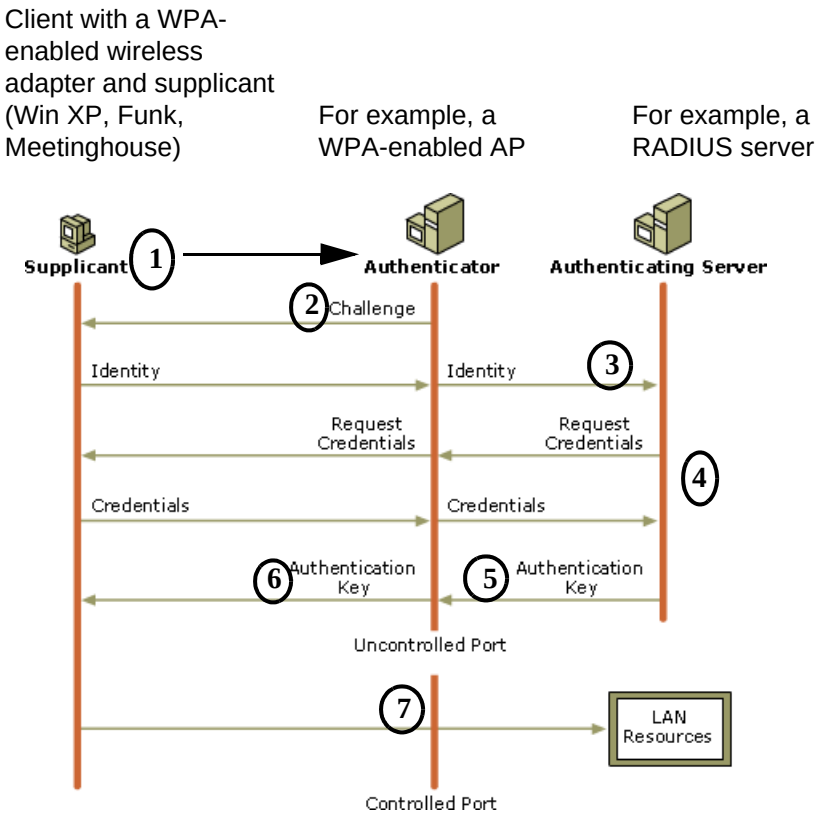


Figure B-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Optional AES Support to be Phased In

One of the encryption methods supported by WPA, besides TKIP, is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC’s hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Glossary

Use the list below to find definitions for technical terms used in this manual.

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

802.11g
A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

ARP
Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is

also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic_commerce because they guarantee that the two parties exchanging information are really who they claim to be.

DHCP

An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DMZ

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you'll willing to risk open access.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol

DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.
EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

IP

Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP
Internet service provider.

Internet Protocol
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN
A communications network serving users within a limited area, such as one floor of a building.

local area network
LAN. A communications network serving users within a limited area, such as one floor of a building.
A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

MD5
MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.
When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also Auto Uplink.

NAT
A technique by which several hosts share a single IP address for access to the Internet.

NetBIOS

Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

A technique by which several hosts share a single IP address for access to the Internet.

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

RADIUS

Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.
Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RIP

A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

SSID

A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Subnet Mask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

TLS

Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

WAN

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEP

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.

All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

wide area network

WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

Index

Numerics

802.11b B-1

A

ad-hoc mode B-2
Auto MDI/MDI-X C-2
Auto Uplink 2-4, C-2

B

Basic Wireless Connectivity 3-18
Basic Wireless Settings 3-9, 3-12, 3-14
BSSID B-2

C

Carrier Sense Multiple Access with Collision Avoidance 5-2
Carrier Sense Multiple Access with Collision Detection 5-2
Cat5 cable C-2
configuration
  erasing 4-7
  restore 4-6
Country Domain 3-12
crossover cable 2-4, C-2
CSMA/CA 5-2
CSMA/CD 5-2

E

ESSID 3-18, B-2
Ethernet 2-3

F

factory settings, restoring 4-7
features 2-2

G

General 4-3

I

infrastructure mode B-2
IP Settings 3-24

L

Log In to the ME103 3-11
Logout 3-7

M

MDI/MDI-X C-2
MDI/MDI-X wiring C-4

O

Open System authentication B-2

P

Passphrase 3-15, 3-20
Placement 3-1

R

Range 3-1
range 3-1
restore configuration 4-6
restore factory settings 4-7
Restrict Wireless Access by MAC Address 3-19
RTS Threshold 5-1, 5-2, 5-3

S

Saving the Configuration File 4-7
Shared Key authentication B-3
SNMP 2-2
SSID 3-12, 3-18, 4-3, B-2

T

troubleshooting 6-1

W

WEP B-3
Wi-Fi B-1
Wired Equivalent Privacy. *See* WEP
Wireless Ethernet B-1
Wireless Network Name 3-12, 4-3
Wireless Security 3-4