

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

NETGEAR

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

202-10144-01
November 2005

November 2005

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.

© 2005 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 antenna, the WG102 device has been approved for use with the following detachable antennas and antenna cables:

| Approved Antennas | Antenna Gain and type | Approved Antenna Cable | Antenna Cable Length | Maximum Transmitted Power* |
|--------------------------|---------------------------------------|-------------------------------|-----------------------------|-----------------------------------|
| 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 WAG302 in North America and Australia.

Industry Canada Compliance Statement

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

Cet appareil numérique de classe B respecte les exigences du règlement du Canada sur le matériel brouilleur NMB-003.

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

Europe - EU Declaration of Conformity

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

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

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

Antenna Statement for the European Community

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

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

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

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

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

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

Bestätigung des Herstellers/Importeurs

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

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

Certificate of the Manufacturer/Importer

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

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

Product and Publication Details

| | |
|----------------------------------|---|
| Model Number: | WG102 |
| Publication Date: | November 2005 |
| Product Family: | wireless access point |
| Product Name: | NETGEAR WG102 ProSafe 802.11g Wireless Access Point |
| Home or Business Product: | Business |
| Language: | English |
| Publication Part Number: | 202-10144-01 |

Contents

Chapter 1

About This Manual

| | |
|---|-----|
| Audience, Scope, Conventions, and Formats | 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 | 2-4 |
| Wireless Multimedia (WMM) Support | 2-4 |
| Compatible and Related NETGEAR Products | 2-4 |
| System Requirements | 2-5 |
| What's In the Box? | 2-5 |
| Hardware Description | 2-6 |
| Front Panel | 2-6 |
| Rear Panel | 2-7 |

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 |
| Using the Basic IP Settings Options | 3-12 |
| Understanding Wireless Settings | 3-13 |
| Understanding Security Profiles | 3-15 |
| Understanding WEP/WPA Security Options | 3-16 |
| Before You Change the SSID and WEP Settings | 3-19 |

| | |
|--|------|
| How to Set Up and Test Basic Wireless Connectivity | 3-20 |
| How to Configure WEP | 3-20 |
| How to Configure WPA with Radius | 3-22 |
| How to Configure WPA-PSK | 3-24 |
| How to Configure WPA2 with Radius | 3-25 |
| How to Configure WPA2-PSK | 3-28 |
| How to Configure WPA and WPA2 | 3-29 |
| How to Configure WPA2-PSK and WPA2-PSK | 3-32 |
| How to Restrict Wireless Access by MAC Address | 3-33 |

**Chapter 4
Management**

| | |
|--|------|
| Using Syslog and Activity Log Information | 4-1 |
| Viewing General and Statistical Information | 4-2 |
| Statistics | 4-4 |
| Viewing a List of Attached Devices | 4-5 |
| Upgrading the Wireless Access Point Software | 4-6 |
| 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 | 4-8 |
| Changing the Administrator Password | 4-8 |
| Using SNMP Remote Management | 4-9 |
| Using AutoCell Rogue Device Detection | 4-10 |
| Using Rogue AP Detection | 4-10 |
| Using Rogue Station Detection | 4-11 |

**Chapter 5
Advanced Configuration**

| | |
|--|-----|
| Hotspot Settings | 5-1 |
| Understanding Advanced Wireless Settings | 5-1 |
| AutoCell Overview | 5-2 |
| AutoCell AP/Client Interaction | 5-2 |
| Additional AutoCell View Management Options | 5-3 |
| Understanding AutoCell Configuration Options | 5-4 |
| Auto RF Management | 5-4 |
| Enhanced RF Security | 5-5 |

| | |
|---|------|
| Rogue Device Detection | 5-5 |
| Configuring Advanced Wireless LAN Settings | 5-6 |
| AP Settings: Enabling Wireless Bridging and Repeating | 5-8 |
| How to Configure a WG102 as a Point-to-Point Bridge | 5-10 |
| How to Configure Multi-Point Wireless Bridging | 5-11 |
| How to Configure Wireless Repeating | 5-13 |

Chapter 6

Troubleshooting

| | |
|--|-----|
| No lights are lit on the access point. | 6-1 |
| The Wireless LAN activity light does not light up. | 6-1 |
| 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. | 6-2 |
| 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 |
|------------------------------------|-----|

Glossary

Chapter 1

About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

| | |
|----------------|--|
| <i>italics</i> | Emphasis, books, CDs, URL names |
| bold | User input |
| fixed | Screen text, file and server names, extensions, commands, IP addresses |

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 specifications:

Table 1-2. Manual Scope

| | |
|-------------------------|---|
| Product Version | NETGEAR WG102 ProSafe 802.11g Wireless Access Point |
| Manual Publication Date | November 2005 |

| | |
|---|---|
|  | Note: Product updates are available on the NETGEAR, Inc. Web site at http://kbserver.netgear.com/products/WG102.asp . |
|---|---|

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

- **Printing a Page in the HTML View.**

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter.**

Use the *PDF of This Chapter* link at the top left of any page.

- Click the *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 *Complete PDF Manual* link at the top left of any page.

- Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
- Click the print icon in the upper left 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 WG102 ProSafe 802.11g Wireless Access Point. Minimal prerequisites for installation are presented in [“System Requirements” on page 2-5](#).

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 and WPA2 support.** WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-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 DHCP server.
- **Multiple BSSID.** Support for multiple BSSIDs. When one AP is connected to a wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a 32-character unique identifier attached to the header of packets sent over a WLAN that differentiated one WLAN from another when a mobile device tries to connect to the network.
- **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.
- **AutoCell RF Management.** AutoCell provides advanced automated RF management that improves performance and enhances security.
- **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.
- **Security Profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, MAC filtering, etc.) for each BSSID.
- **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.
- **VLAN Support.** Short for virtual LAN, a network of computers that behave as if they are connected to the same network even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation and resource optimization.

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.

Wireless Multimedia (WMM) Support

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.

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 ProSafe 108 Mbps Dual Band PC Card
- WAG311 ProSafe 108 Mbps Dual Band PCI Card
- WG311T 802.11g 108 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 ([12V DC, 1 A](#))
- Straight through Category 5 Ethernet cable
- 802.11g ProSafe Wireless Access Point Installation Guide WG102
- *Resource CD for the NETGEAR WG102 ProSafe 802.11g Wireless Access Point*

This Reference Manual for the NETGEAR ProSafe 802.11g Wireless Access Point WG102 (202-10144-01).

- 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.

Front Panel



Figure 2-1: WG102 front panel

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

| LED | DESCRIPTION |
|----------------|--|
| PWR | Power Indicator |
| Off | No power. If this LED does not come on with the power adapter and cord correctly installed, see Chapter 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. |

Rear Panel



Figure 2-2: WG102 rear panel

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

- **Detachable Antenna**

The WG102 provides one detachable antenna.

- **Ground**

The WG102 provides a connector of grounding the unit.

- **Restore to Factory Defaults RESET 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 LAN/POE Port**

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

- **Power Socket**

This socket connects to the WG102 [12V DC, 1 A](#) 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 [Appendix , “Understanding Security Profiles”](#). 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.

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 disabled, it uses the default IP address |
| IP Configuration | IP Address: 192.168.0.229 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0 |
| Network Name (SSID) | NETGEAR-0 |
| Broadcast Network Name (SSID) | Enabled |
| 802.11g Radio Frequency Channel | Managed automatically by AutoCell (default), if AutoCell is disabled, channel 11 is the default |
| Super-G Mode | Disabled |
| WEP/WPA | Disabled |
| MAC Access Control | Disabled |
| AutoCell RF Management | Enabled |
| AutoCell Enhanced RF Security | Disabled |
| AutoCell Rogue Device Detection | Disabled |
| Restricting connectivity based on MAC Access Control List | Disabled |
| Time Zone | GMT |
| Time Zone Adjust for Daylight Saving Time | Disabled |
| SNMP | Disabled |
| VLAN (802.1Q) | Disabled |
| WMM Support | Disabled |

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.

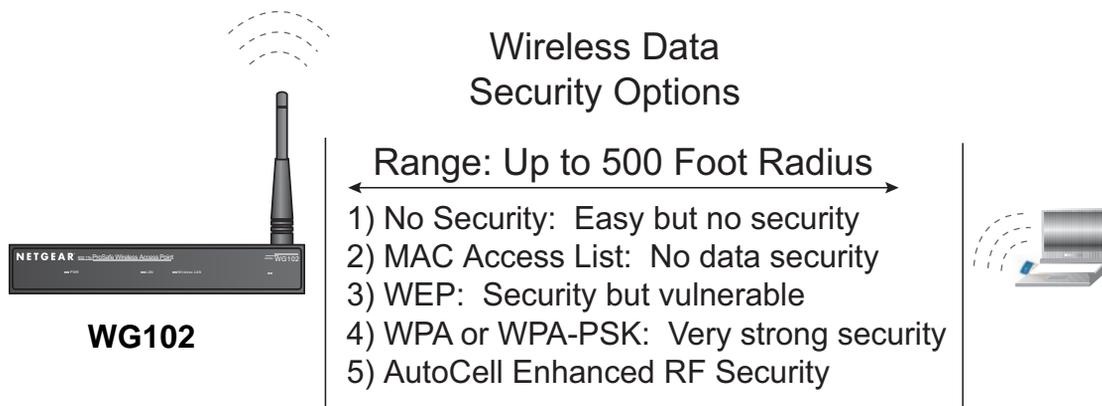


Figure 3-1: WG102 wireless data security options

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

- **Use Multiple BSSIDs combined with VLANs.** You can configure combinations of VLANs and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network.
- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WG102. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

- **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, WPA-PSK, WPA2, or WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.
- **Use AutoCell Enhanced RF Security.** In addition to standard encryption and security mechanisms such as WEP and WPA, the WG102 AutoCell feature provides self-organizing micro cells for an additional level of privacy for enterprises. In this mode, AutoCell shrinks the size of coverage to the minimum to reach clients but also shrinks the size of the beacons that access points use to announce their presence. This mode makes an enterprise wireless LAN nearly invisible to users outside an office building. AutoCell clients such as the NETGEAR WAG511 are highly-recommended for Enhanced RF Security. Furthermore, the AutoCell Rogue Device Detection feature lets you identify and block wireless devices in your that should never be given access to the wireless network.

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 2-5](#).

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



Figure 3-2: Login window

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

NETGEAR ProSafe Wireless Access Point WG102 settings

General

Access Point Information

| | |
|--------------------|---------------|
| Access Point Name | netgearffa19e |
| Country / Region | United States |
| Firmware Version | V4.0.4 |
| Access Point Mode | Access Point |
| VLAN(802.1Q) | Disable |
| Management VLAN ID | 1 |

Current IP Settings

| | |
|-----------------|-------------------|
| IP Address | 192.168.0.229 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |
| DHCP Client | Disabled |
| MAC Address | 00:C0:02:FF:A1:9E |

Current Wireless Settings

| | |
|---------------------|--------------------------|
| Channel / Frequency | 1 / 2.412GHz (Automatic) |
|---------------------|--------------------------|

Security Profiles

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

General Information Help

The Access Point General Information is read-only, any changes...

Access Point Information
General information about the Access Point

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

Current IP Settings
These are the current TCP/IP settings for the Access Point. If the IP address was obtained from a DHCP server, the IP address is read-only.

Current Wireless Settings:
These are the current settings for the Access Point's wireless interface.

Channel/Frequency
This displays the Channel and Frequency for the Access Point's wireless interface.

Security Profiles
This table displays details of each Security Profile.

- Profile Name: The name assigned to the Security Profile.
- SSID: The SSID assigned to the Security Profile.
- Security: The current security type for the Security Profile.
- VLAN: Displays the current VLAN for the Security Profile.
- Status: Indicates whether or not the Security Profile is enabled.

Figure 3-3: Login result: WG102 home page

- When the wireless access point is connected to the Internet, click the Documentation link under the Web Support menu to view 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.

The screenshot shows the 'Basic Settings' configuration page. At the top, the 'Access Point Name' is set to 'netgearffa19e'. Under the 'IP Address' section, the 'DHCP Client' option is set to 'Disable'. The IP Address is 192.168.0.229, the IP Subnet Mask is 255.255.255.0, the Default Gateway is 0.0.0.0, and the DNS Server is 0.0.0.0. There is an unchecked checkbox for 'Enable 802.1Q VLAN'. The 'Time Zone' is set to '(GMT) UK,GreenWich,Casablanca,Monrovia', and the 'Adjust for Daylight Saving Time' checkbox is unchecked. The current time is displayed as '2004 Jan 1 03:44:41 GMT'. At the bottom, there are 'Apply' and 'Cancel' buttons.

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.

The screenshot shows the 'Wireless Settings' configuration page. The 'Country / Region' is set to 'United States'. Under the 'Wireless LAN' section, the 'Turn Radio On' checkbox is checked. The 'Operating Mode' is set to 'Auto(802.11g/802.11b)', the 'Channel / Frequency' is 1 / 2.412GHz, the 'Data Rate' is 'Best', and the 'Output Power' is 'Full'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 3-5: Basic Wireless Settings menu

- c. Configure the wireless interface for wireless access. See the online help or the [“Understanding Wireless Settings” on page 3-13](#) topic of this Reference Manual for full instructions.

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

Now that you have finished the setup 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 3-8.

Using the Basic IP Settings Options

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

The screenshot shows the 'Basic Settings' configuration page. At the top, the 'Access Point Name' is set to 'netgearffa19e'. Below this, the 'IP Address' section includes a 'DHCP Client' option with 'Enable' and 'Disable' radio buttons; 'Disable' is selected. The IP address is set to 192.168.0.229, the subnet mask to 255.255.255.0, the default gateway to 0.0.0.0, and the DNS server to 0.0.0.0. There is an unchecked checkbox for 'Enable 802.1Q VLAN'. The 'Time Zone' is set to '(GMT) UK,GreenWich,Casablanca,Monrovia', and there is an unchecked checkbox for 'Adjust for Daylight Saving Time'. The 'Current Time' is displayed as '2004 Jan 1 03:44:41 GMT'. At the bottom are 'Apply' and 'Cancel' buttons.

Figure 3-7: Basic Settings menu

The Basic Settings menu options are discussed below. The default values are suitable for most users and situations.

- **Access Point Name:** This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of the WG102. You may modify the default name with a unique name up to 15 characters long. The default is netgearxxxxxx, where xxxxxxxx represents the last 6 digits of the WG102 MAC address.
- **IP Address:** By default, the Access Point has DHCP (Dynamic Host Configuration Protocol) client set to Disable. The default IP address is 192.168.0.229.

You may enable the DHCP client to let the Access Point get its TCP/IP configuration from the DHCP server on your network.

- **DHCP Client:** The Access Point will get the IP address, subnet mask and the default gateway settings automatically from the DHCP server if DHCP is enabled.

- **IP Address:** Enter an unused IP address from the address range used on your LAN (factory default: 192.168.0.229).
- **IP Subnet Mask:** Enter the subnet mask value used on your LAN (factory default: 255.255.255.0).
- **Default Gateway:** Enter the IP address of the Gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the Access Point is connected (factory default: 0.0.0.0).
- **DNS Server:** Enter the IP address of the DNS (Domain Name Server) you wish to use (factory default: 0.0.0.0).
- **Enable 802.1Q VLAN:** Check the box Enable 802.1Q VLAN to enable the WG102 to process VLAN membership information.
- **Time Zone:** Select the Time Zone to match your location. If your location uses daylight saving, check the box Adjust for Daylight Saving Time.

The Current Time, as used on the Access Point, is displayed.

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

Understanding Wireless Settings

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

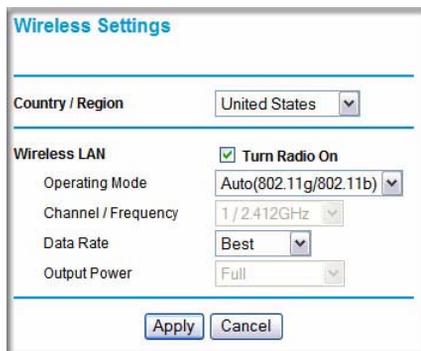


Figure 3-8: Wireless Settings menu

The Wireless Settings menu options are discussed below:



Note: Channel selection and power management is automatically adjusted by the AutoCell Auto RF Management option. The Auto RF Management option is enabled by default.

- **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. For products sold in the United States, the default country domain is preset. Also, the channel is set to 11. For products sold outside the United States, unless a country domain is selected, the channel cannot be changed.
- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Operating Mode.** Select the desired wireless operating mode. The options are:
 - Auto (802.11g/802.11b) – Both 802.11g and 802.11b wireless stations can be used. This is the default.
 - 802.11g Only - Only 802.11g wireless stations can be used.
 - 802.11b Only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- **Channel.** This 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 <http://documentation.netgear.com/reference/enu/wireless/index.htm> for more information on wireless channels.



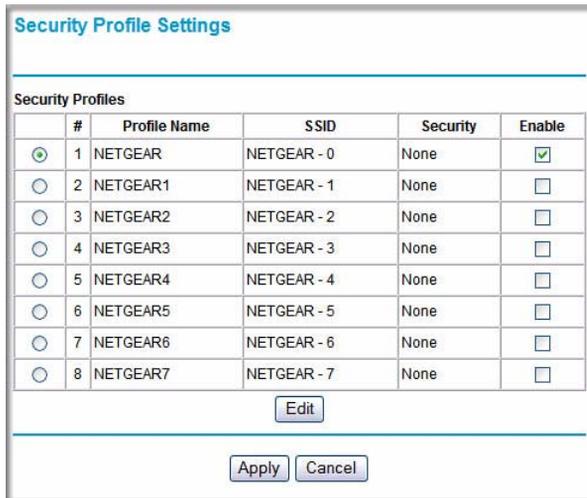
Note: Channel selection is automatically adjusted by AutoCell when the Auto RF Management option is enabled. The default setting is for the AutoCell Auto RF Management option to be enabled.

- 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.
- 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. 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 Security Profiles

Security profiles let you configure unique security settings for each SSID. The WG102 now supports up to eight SSIDs.



The screenshot shows the "Security Profile Settings" menu. It contains a table with the following data:

| Security Profiles | | | | | |
|----------------------------------|---|--------------|-------------|----------|-------------------------------------|
| | # | Profile Name | SSID | Security | Enable |
| <input checked="" type="radio"/> | 1 | NETGEAR | NETGEAR - 0 | None | <input checked="" type="checkbox"/> |
| <input type="radio"/> | 2 | NETGEAR1 | NETGEAR - 1 | None | <input type="checkbox"/> |
| <input type="radio"/> | 3 | NETGEAR2 | NETGEAR - 2 | None | <input type="checkbox"/> |
| <input type="radio"/> | 4 | NETGEAR3 | NETGEAR - 3 | None | <input type="checkbox"/> |
| <input type="radio"/> | 5 | NETGEAR4 | NETGEAR - 4 | None | <input type="checkbox"/> |
| <input type="radio"/> | 6 | NETGEAR5 | NETGEAR - 5 | None | <input type="checkbox"/> |
| <input type="radio"/> | 7 | NETGEAR6 | NETGEAR - 6 | None | <input type="checkbox"/> |
| <input type="radio"/> | 8 | NETGEAR7 | NETGEAR - 7 | None | <input type="checkbox"/> |

Below the table is an "Edit" button. At the bottom of the menu are "Apply" and "Cancel" buttons.

Figure 3-9: Security Profiles Settings menu

To edit a security profile, select it from the list, and click Edit.

Understanding WEP/WPA Security Options

The table below identifies the various WEP/WPA security options. A full explanation of these standards is available at <http://documentation.netgear.com/reference/enu/wireless/index.htm>.

Figure 3-10: Security Profiles Configuration menu

The settings are explained as follows:

- **Security Profile Name.** The Security Profile Name is a descriptive name you assign to differentiate one profile from another.
- **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-0 for the first profile, NETGEAR-1 for the second, and so on.
 - 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 Auto RF Management option 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.



Note: Broadcast Wireless Network Name (SSID) is turned off when the AutoCell Enhanced RF Security option is enabled. By default it is disabled.

- **Network Authentication:** Specifies the Authentication type used. The default is Open System. Select the desired option:
 - **Open System:** If selected, you have the option of using WEP encryption, or no encryption.
 - **Shared Key:** If selected, you must use WEP; at least one shared key must be entered.
 - **Legacy 802.1x:** If selected, you must configure the Radius Server Settings Screen.
 - **WPA-PSK:** If selected, you must use TKIP encryption, and enter the WPA passphrase (Network key).
 - **WPA with Radius:** If selected, you must configure the Radius Server Settings Screen.
 - **WPA2-PSK:** WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and enter the WPA passphrase (Network key).
 - **WPA-PSK and WPA2-PSK:** This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES. The WPA passphrase (Network key) must also be entered.
 - **WPA2 with Radius:** WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and configure the Radius Server Settings Screen.
 - **WPA and WPA2 with Radius:** This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES, and you must also configure the Radius Server Settings Screen.

Note: All options are available if using Access Point mode. In other modes (e.g. Repeater or Bridge) some options may be unavailable.

- **Data Encryption:** Select the desired option. The available options depend on the Network Authentication setting above (otherwise, the default is None). The supported options are:
 - **None:** No encryption is used.
 - **64 bits WEP:** Standard WEP encryption, using 40/64 bit encryption.
 - **128 bits WEP:** Standard WEP encryption, using 104/128 bit encryption.
 - **152 bits WEP:** Proprietary mode that will only work with other wireless devices that support this mode.
 - **TKIP:** This is the standard encryption method used with WPA.
 - **AES:** This is the standard encryption method for WPA2. Some clients may support AES with WPA, but this is not supported by this Access Point.
 - **TKIP + AES:** This setting allows both WPA and WPA2 to be supported. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.
- **Passphrase:** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
- **Key 1, Key 2, Key 3, Key 4:** If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
- **WPA Passphrase (Network Key):** If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.
- **Wireless Client Security Separation:** If enabled, the associated wireless clients will not be able to communicate with each other. This feature is intended for hotspots and other public access situations. The default is Disabled.

Before You Change the SSID and WEP Settings

For a new wireless network, print or copy this form and fill in the 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. Store this information in a safe place.

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. The default SSID is NETGEAR-0.

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

4. As appropriate, select the Country/Region in which the wireless interface will operate.

5. For now, do not make other changes

6. 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.

7. 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 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.

- Click **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

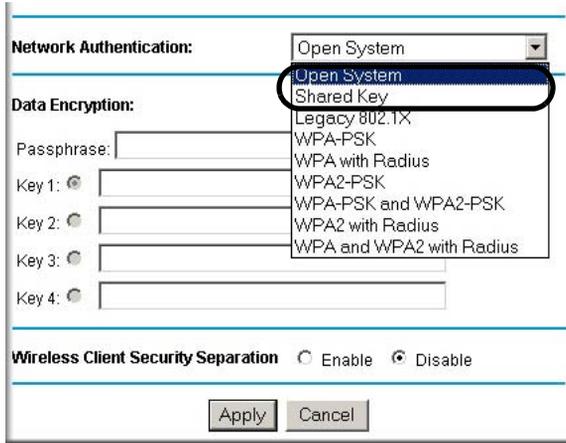


Figure 3-11: WEP/WPA Settings menu

- Choose Open System or Shared Key authentication.
 - Select encryption strength.
 - 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 <http://documentation.netgear.com/reference/enu/wireless/index.htm> for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.
- 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 with Radius

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.

The screenshot shows the 'Radius Server Settings' configuration page. It is divided into several sections:

- Primary Authentication Server:** IP Address (0.0.0.0), Port Number (1812), Shared Secret (empty).
- Secondary Authentication Server:** IP Address (0.0.0.0), Port Number (1812), Shared Secret (empty).
- Authentication Settings:** Reauthentication Time (3600) Seconds. Two checkboxes are present: 'Update Global Key every 1800 Seconds' (unchecked) and 'Update if any station disassociates' (unchecked).
- Primary Accounting Server:** IP Address (0.0.0.0), Port Number (1813), Shared Secret (empty).
- Secondary Accounting Server:** IP Address (0.0.0.0), Port Number (1813), Shared Secret (empty).

At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 3-12: Radius Server Settings menu

3. Enter the Radius settings.

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

5. Click **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

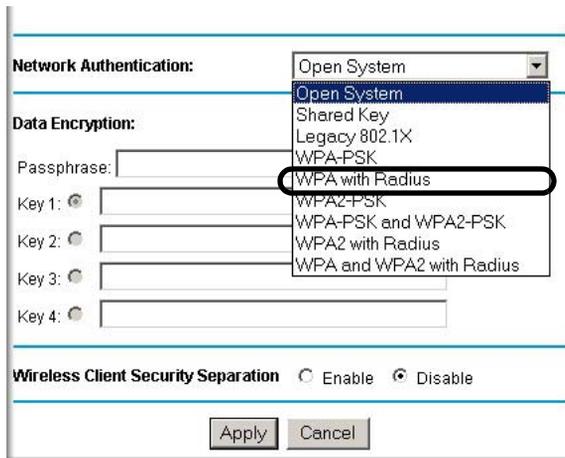


Figure 3-13: WEP/WPA Settings menu

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 **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

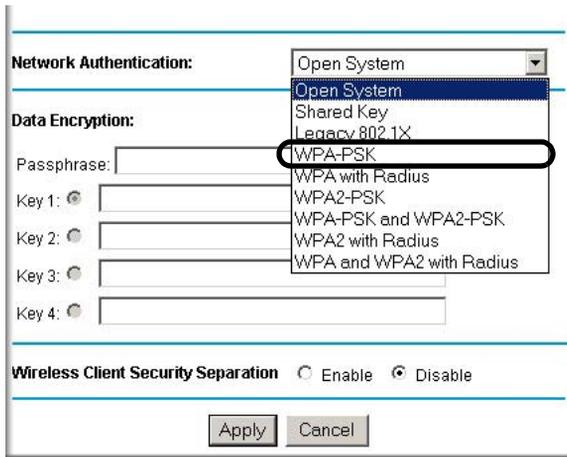


Figure 3-14: WEP/WPA Settings menu

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

How to Configure WPA2 with Radius

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2, 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.

Radius Server Settings

Primary Authentication Server
IP Address: 0 . 0 . 0 . 0
Port Number: 1812
Shared Secret:

Secondary Authentication Server
IP Address: 0 . 0 . 0 . 0
Port Number: 1812
Shared Secret:

Authentication Settings
Reauthentication Time: 3600 Seconds
 Update Global Key every 1800 Seconds
 Update if any station disassociates

Primary Accounting Server
IP Address: 0 . 0 . 0 . 0
Port Number: 1813
Shared Secret:

Secondary Accounting Server
IP Address: 0 . 0 . 0 . 0
Port Number: 1813
Shared Secret:

Figure 3-15: Radius Server Settings menu

3. Enter the Radius settings.
 - **Authentication/Access Control Radius Server Configuration:** This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0.
 - **Port Number:** Port number of the Radius Server. The default is 1812.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
 - **Re-authentication Time:** The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.

- **Global-key Re-Key Time:** Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
 - **Update if any station disassociates:** Check on this option to refresh global key when any stations disassociated with wireless Access Point.
 - **Accounting Radius Server Configuration:** This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0.
 - **Port Number:** Port number of the Radius Server. The default is 1813.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
4. Click **Apply** to save your settings.
 5. Click **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

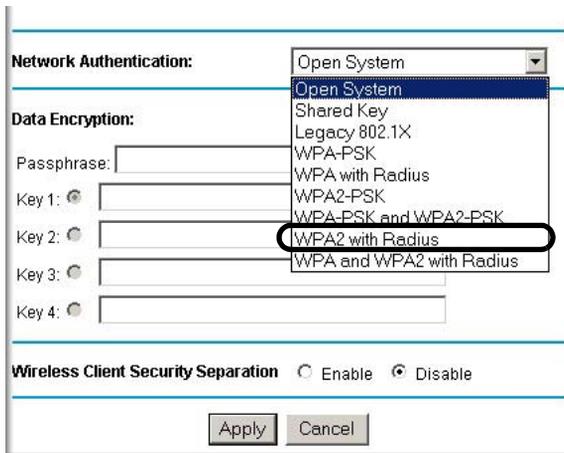


Figure 3-16: WEP/WPA Settings menu

6. Choose **WPA2 with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA2-PSK

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2-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 **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.



Figure 3-17: WEP/WPA Settings menu

3. Choose **WPA2-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.

How to Configure WPA and WPA2

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.

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA and WPA2, 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.

The screenshot shows the 'Radius Server Settings' configuration window. It is divided into several sections:

- Primary Authentication Server:** IP Address (0.0.0.0), Port Number (1812), and Shared Secret (empty).
- Secondary Authentication Server:** IP Address (0.0.0.0), Port Number (1812), and Shared Secret (empty).
- Authentication Settings:** Reauthentication Time (3600 Seconds), Update Global Key every (1800 Seconds) checkbox, and Update if any station disassociates checkbox.
- Primary Accounting Server:** IP Address (0.0.0.0), Port Number (1813), and Shared Secret (empty).
- Secondary Accounting Server:** IP Address (0.0.0.0), Port Number (1813), and Shared Secret (empty).

At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 3-18: Radius Server Settings menu

3. Enter the Radius settings.
 - **Authentication/Access Control Radius Server Configuration:** This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0.
 - **Port Number:** Port number of the Radius Server. The default is 1812.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
 - **Re-authentication Time:** The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.

- **Global-key Re-Key Time:** Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
 - **Update if any station disassociates:** Check on this option to refresh global key when any stations disassociated with wireless Access Point.
 - **Accounting Radius Server Configuration:** This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0.
 - **Port Number:** Port number of the Radius Server. The default is 1813.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
4. Click **Apply** to save your settings.
 5. Click **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

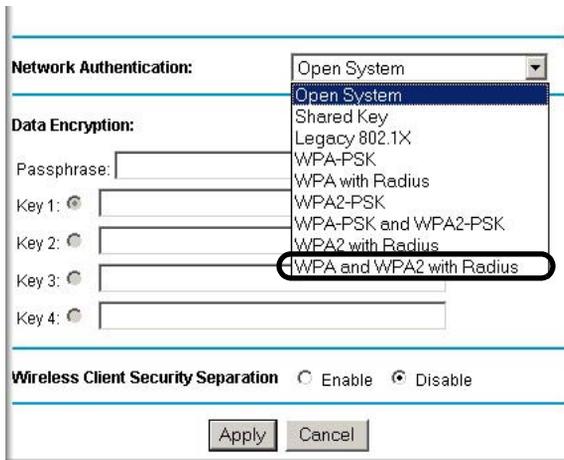


Figure 3-19: WEP/WPA Settings menu

6. Choose **WAP and WPA2 with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA2-PSK and WPA2-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.

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA-PSK and WPA2-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 **Security Profiles Settings** in the Security menu of the WG102, select the profile you choose to configure, and click **Edit** to view the Security Profiles Configuration menu.

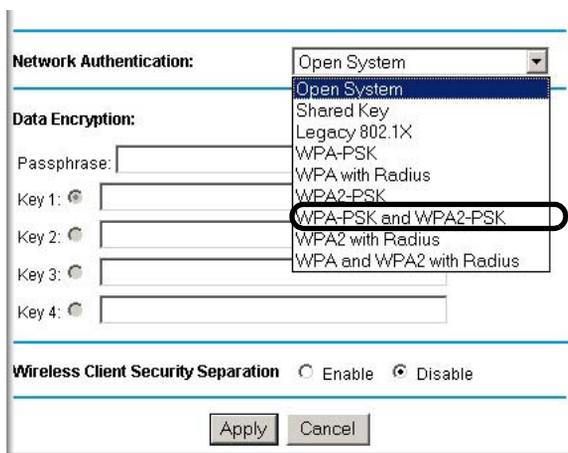


Figure 3-20: WEP/WPA Settings menu

3. Choose **WPA-PSK and WPA2-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.

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 3-21: 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.

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 Activity Log link to view this screen.

Activity Log

Activity Log Window

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

Refresh Save As...

Enable SysLog

Syslog Server IP Address . . .

Port

Apply Cancel

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 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 netgearffa19e
Country / Region United States
Firmware Version V4.0.4
Access Point Mode Access Point
VLAN(802.1Q) Disable
Management VLAN ID 1

Current IP Settings

IP Address 192.168.0.229
Subnet Mask 255.255.255.0
Default Gateway 0.0.0.0
DHCP Client Disabled
MAC Address 00:C0:02:FF:A1:9E

Current Wireless Settings

Channel / Frequency 1 / 2.412GHz (Automatic)

Security Profiles

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

Figure 4-2: Wireless Access Point General information screen

Table 4-1. General Information Fields

| Field | Description |
|----------------------------------|---|
| Access Point Information | |
| Access Point Name (NetBIOS name) | The default name may be changed if desired. |
| 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. |
| VLAN (802.1Q) | Indicates if VLAN support is enabled. The default is disabled. |
| Management VLAN ID | Displays the VLAN ID. |
| Current IP Settings | |
| IP Address | The IP address of the wireless access point. |
| Subnet Mask | The subnet mask for the wireless access point. |
| Default Gateway | The default gateway for the wireless access point communication. |
| DHCP Client | Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicates a static IP configuration. |
| MAC Address | Displays the Media Access Control address (MAC address) of the wireless access point's Ethernet port. |
| Current Wireless Settings | |
| Channel/Frequency | Identifies the channel the wireless port is using. 11 is the default channel setting. See http://documentation.netgear.com/reference/enu/wireless/index.htm for the frequencies used on each channel. |
| Security Profiles | For each Security Profile, the following are displayed: Profile name, SSID, security option, VLAN ID, and enabled/disabled. |

Statistics

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

The screenshot displays the 'Statistics' page with the following data:

| Wired Ethernet | | |
|----------------|----------|-------------|
| | Received | Transmitted |
| Packets | 1483 | 1423 |
| Bytes | 196716 | 77484 |

| Wireless | | |
|--------------------|----------|-------------|
| Security Profile 1 | | |
| | Received | Transmitted |
| Unicast Packets | 0 | 0 |
| Broadcast Packets | 0 | 212 |
| Multicast Packets | 0 | 6 |
| Total Packets | 0 | 218 |
| Total Bytes | 0 | 27876 |

| Security Profile 2 | | |
|--------------------|----------|-------------|
| | Received | Transmitted |
| Unicast Packets | 0 | 0 |
| Broadcast Packets | 0 | 0 |
| Multicast Packets | 0 | 0 |
| Total Packets | 0 | 0 |
| Total Bytes | 0 | 0 |

| Security Profile 3 | | |
|--------------------|----------|-------------|
| | Received | Transmitted |
| Unicast Packets | 0 | 0 |
| Broadcast Packets | 0 | 0 |
| Multicast Packets | 0 | 0 |
| Total Packets | 0 | 0 |
| Total Bytes | 0 | 0 |

| Security Profile 8 | | |
|--------------------|----------|-------------|
| | Received | Transmitted |
| Unicast Packets | 0 | 0 |
| Broadcast Packets | 0 | 0 |
| Multicast Packets | 0 | 0 |
| Total Packets | 0 | 0 |
| Total Bytes | 0 | 0 |

Refresh

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

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.

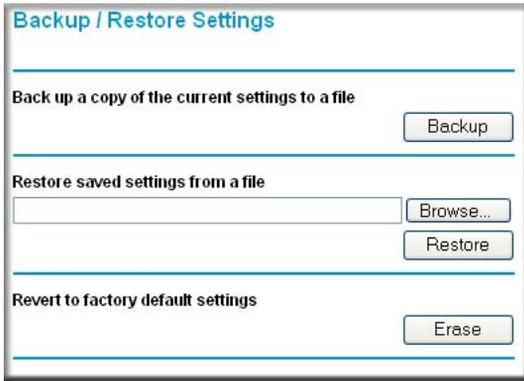


Figure 4-4: Settings Backup menu

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 SSID will be NETGEAR, the DHCP client will be disabled, the default LAN IP address will be 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. Hold the Reset Button until the LEDs blink twice, usually more than 5 seconds.
2. 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.



The screenshot shows a web form titled "Change Password". It contains three input fields: "Current Password", "New Password", and "Repeat New Password". Below these fields is a radio button group for "Restore Default Password" with "Yes" and "No" options, where "No" is selected. At the bottom are "Apply" and "Cancel" buttons.

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.

The screenshot shows the 'Remote Management' configuration page. The 'SNMP' section has 'Disable' selected. The 'Public Community Name' is 'public', 'Private Community Name' is 'private', 'Manager IP address' is '255.255.255.255', and 'IP address to Receive Traps' is '0.0.0.0'. 'Apply' and 'Cancel' buttons are at the bottom.

Figure 4-6: Remote Management settings

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

Using AutoCell Rogue Device Detection

The AutoCell feature provides added security by being able to detect rogue APs and wireless stations and exclude them from connecting to the NETGEAR WG102 ProSafe 802.11g Wireless Access Point.

Using Rogue AP Detection

From the main menu of the browser interface, under the Information heading, click the Rogue AP detection link to view this menu.

Rogue AP Detection

Unknown AP List

| Action | SSID | MAC Address | Channel | AutoCell Enabled |
|--|------------------|-------------------|---------|------------------|
| <input type="button" value="Authorize"/> | NETGEAR_11g | 00:0F:B5:CA:85:73 | 1 | No |
| <input type="button" value="Authorize"/> | | 00:0F:B5:92:C1:71 | 1 | Yes |
| <input type="button" value="Authorize"/> | | 06:0F:B5:50:62:B2 | 1 | Yes |
| <input type="button" value="Authorize"/> | lisaWG102 | 00:0F:B5:50:62:B2 | 1 | Yes |
| | | | | |
| <input type="button" value="Authorize"/> | Valerie2 | 00:D0:59:E1:1C:2C | 11 | No |
| <input type="button" value="Authorize"/> | w-NETGEAR-TRAVEL | 00:09:5B:FE:E3:4A | 11 | No |

Authorized AP List

| Action | SSID | MAC Address | Channel | AutoCell Enabled |
|---------------------------------------|---------|-------------------|---------|------------------|
| <input type="button" value="Delete"/> | NETGEAR | 00:0F:B5:B2:36:36 | 11 | No |
| <input type="button" value="Delete"/> | NETGEAR | 00:0F:B5:DA:D3:16 | 11 | No |

Export Authorized AP List

Import Authorized AP List File

Replace existing list
 Merge with existing list

Figure 4-7: Rogue AP Detection

1. Click **Rescan** to discover the APs.

2. Click **Authorize** to add any AP to the Authorized AP List. Click **Delete** to remove an AP from the list.
3. Optionally, you can export or import lists of authorized APs.

Using Rogue Station Detection

From the main menu of the browser interface, under the Information heading, click the Rogue Station detection link to view this menu.

Rogue Station Detection

Unknown Station List

| Action | Station ID | MAC Address | Channel | AutoCell Enabled |
|--|------------|-------------------|---------|------------------|
| <input type="button" value="Authorize"/> | 1 | 00:0F:B5:99:D9:60 | N/A | No |
| <input type="button" value="Authorize"/> | 2 | 00:D0:59:E1:03:DF | N/A | No |
| <input type="button" value="Authorize"/> | 21 | 00:60:B3:58:13:F5 | N/A | No |
| <input type="button" value="Authorize"/> | 22 | 00:0F:B5:B2:40:1B | N/A | No |

Authorized Station List

| Action | Station ID | MAC Address | Channel | AutoCell Enabled |
|---------------------------------------|------------|-------------------|---------|------------------|
| <input type="button" value="Delete"/> | 1 | 00:0F:B5:88:BA:A4 | N/A | No |
| <input type="button" value="Delete"/> | 2 | 00:11:24:A1:35:3A | N/A | No |

Export Authorized Station List

Import Authorized Station List File

Replace existing list
 Merge with existing list

Add Authorized Station List to Access Control Trusted Stations

Figure 4-8: Rogue AP Detection

1. Click **Rescan** to discover the stations.
2. Click **Authorize** to add any station to the Authorized Station List. Click **Delete** to remove a station from the list.
3. Optionally, you can export or import lists of authorized stations.

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.

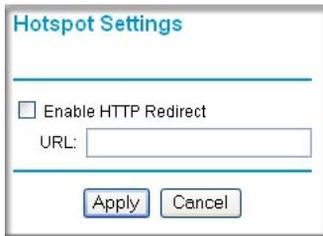


Figure 5-1: Hotspot Settings screen

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

Understanding Advanced Wireless Settings

The advanced wireless settings menu enables configuration of the following:

- AutoCell RF management

- Advanced wireless parameters

These options are discussed below.

AutoCell Overview

AutoCell provides advanced RF wireless management features that improve performance and enhance security.

Table 5-1. What does AutoCell do?

| Problem | AutoCell Settings |
|--|---|
| Erosion of privacy | Optional setting allows Wi-Fi network to be nearly undetectable by neighbors and hackers as well as the block rogue wireless devices from connecting to your network. (Enhanced RF Security -- Default: Disable) (Rogue Device Detection -- Default: Disable) |
| Diminishing performance from multiple APs installed in one area. | APs and clients load-balance traffic across under utilized APs. (Auto RF Management -- Default: Enable). |
| Complexity of installation | Customers can put APs anywhere they want and in any density APs. (Auto RF Management -- Default: Enable) |
| Increasing interference | Clients and APs avoid interference from neighbors and other unexpected sources. (Auto RF Management -- Default: Enable). |

AutoCell's self-organizing micro cells provide an additional level of privacy for enterprises. AutoCell clients are highly-recommended for Enhanced RF Security.

AutoCell AP/Client Interaction

AutoCell's self-organizing micro cells provide performance benefits and an additional level of privacy for enterprises.

- **Automatic Transmit Power Control.** An AutoCell-enabled client's RF transmit power level is automatically coordinated with an AutoCell-enabled AP. This creates client micro-cells and reduces co-channel interference with other clients and APs on the same frequency and improves overall throughput and performance. (Requires: AutoCell-enabled AP)

- **Automatic Load-Balancing.** An AutoCell-enabled client will seek out and associate to the lightest loaded AutoCell-enabled AP available. (Requires: AutoCell-enabled AP)
- **Rapid Roaming.** An AutoCell-enabled client will accurately and rapidly detect movement as distinguished from RF anomalies such as arbitrary and momentary changes in the surrounding RF domain. When it detects true movement, the client immediately seeks the best available AP at the highest data rate possible instead of waiting for the data rate to decline. (Does not Require AutoCell-enabled APs)

Additional AutoCell View Management Options

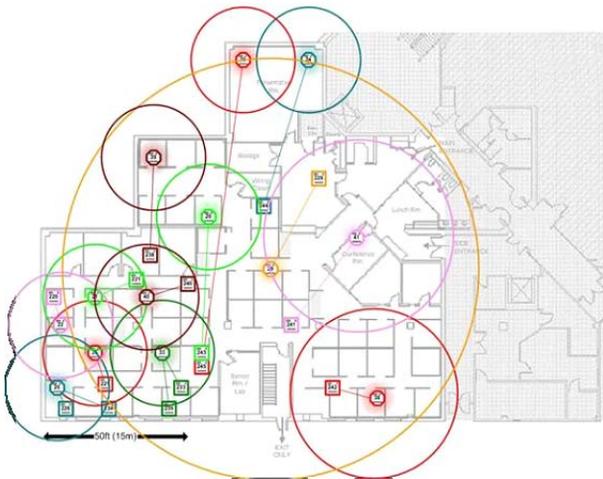


Figure 5-2: AutoCell View wireless network

AutoCell View is an available management tool that provides sophisticated views of your wireless network and enables managing the wireless communications easily from a simple console.

Understanding AutoCell Configuration Options

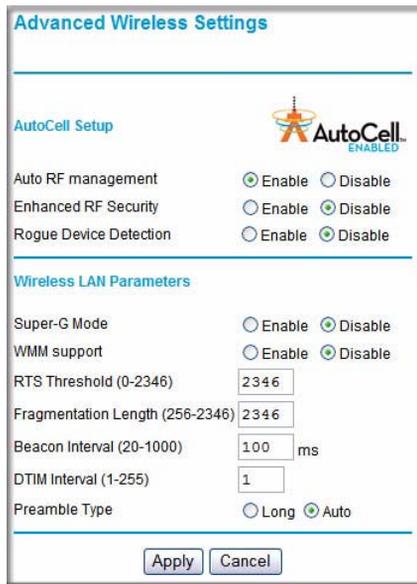


Figure 5-3: Advanced Wireless Settings screen AutoCell Setup options

There are three AutoCell configuration setting choices:

- Enable/disable Auto RF Management: Enabled by default
- Enable/disable Enhanced RF Security: Disabled by default
- Enable/disable Rogue Device Detection: Disabled by default

These options are discussed below.

Auto RF Management



Note: Channel selection and power management is automatically adjusted by the AutoCell Auto RF Management option. The Auto RF Management option is enabled by default.

In this mode, AutoCell APs and clients load-balance traffic across under utilized APs. This mode avoids interference from neighbors clients and APs and other unexpected sources.

Enhanced RF Security



Note: Broadcast Wireless Network Name (SSID) is automatically turned off when you select the AutoCell Enhanced RF Security option.

In this mode, AutoCell shrinks the size of coverage to the minimum to reach clients but also shrinks the size of the beacons that access points use to announce their presence. This mode makes an enterprise wireless LAN nearly invisible to users outside an office building.

Rogue Device Detection

The AutoCell Rogue Device Detection feature lets you identify and block wireless devices in your that should never be given access to the wireless network.

Configuring Advanced Wireless LAN Settings

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

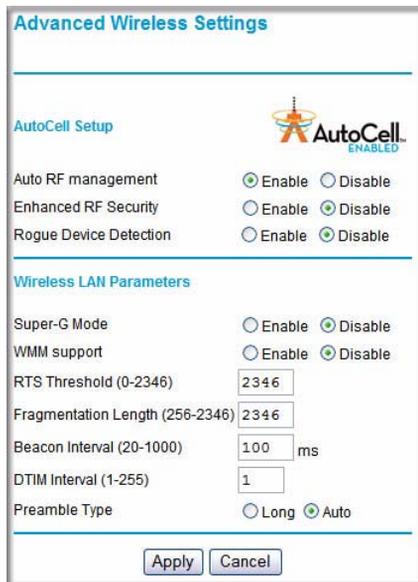


Figure 5-4: Advanced Wireless Settings screen

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

- **Super-G Mode:** Super-G Mode is a proprietary extension to the 802.11g standard which can double the throughput to 108Mbps. Only compatible Wireless stations can use this mode. The default is Disable.
- **WMM support:** WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM. The default is Disable.
- **RTS Threshold:** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting

station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2346.

- **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. The default is 2346.
- **Beacon Interval:** The Beacon Interval specifies the interval time (between 20ms and 1000ms) for each beacon transmission. The default is 100.
- **DTIM Interval:** The DTIM (Delivery Traffic Indication Message) specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type:** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto will automatically handle both long and short preamble. The default is Auto.

AP Settings: Enabling Wireless Bridging and Repeating

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

Advanced Access Point Settings

Access Point Mode

Enable Wireless Bridging and Repeating on Security Profile 1

Wireless Point-to-Point Bridge

Enable Wireless Client Association

Remote MAC Address

Wireless Point to Multi-Point Bridge

Enable Wireless Client Association

Remote MAC Address 1

Remote MAC Address 2

Remote MAC Address 3

Remote MAC Address 4

Repeater with Wireless Client Association

Parent AP MAC Address

Child AP MAC Address

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



Note: All bridge mode options are not available when AutoCell Auto RF Management is enabled (the default setting).

Examples of wireless bridged configurations are:

- **Point-to-Point Bridge**
 - In this mode, the WG102 will communicate with another bridge-mode wireless station.
 - In addition, you have the option of enabling client associations with this WG102.
 - You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use WEP to protect this communication.

- **Multi-Point Bridge**
 - Select this only if this WG102 is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this “master,” rather than directly among each other.
 - In addition, you have the option of enabling client associations with this WG102.
 - For multi-point bridge mode, you must enter the MAC addresses of the other access points in the fields provided.
 - The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using the MAC address of this WG102 as the Remote MAC Address.
 - Use WEP to protect this traffic.
- **Repeater with Wireless Client Association**
 - Selected repeater mode to send all traffic to the remote AP.
 - For repeater mode, you must enter the MAC address of the remote “parent” access point, and optionally enter the address of the “child” access point.
 - In repeater mode, you *do not* have the option of disabling client associations with this WG102.
 - In repeater mode, you cannot configure a sequence of parent/child APs; you are limited to only one parent/child AP pair.

These features are discussed below.

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

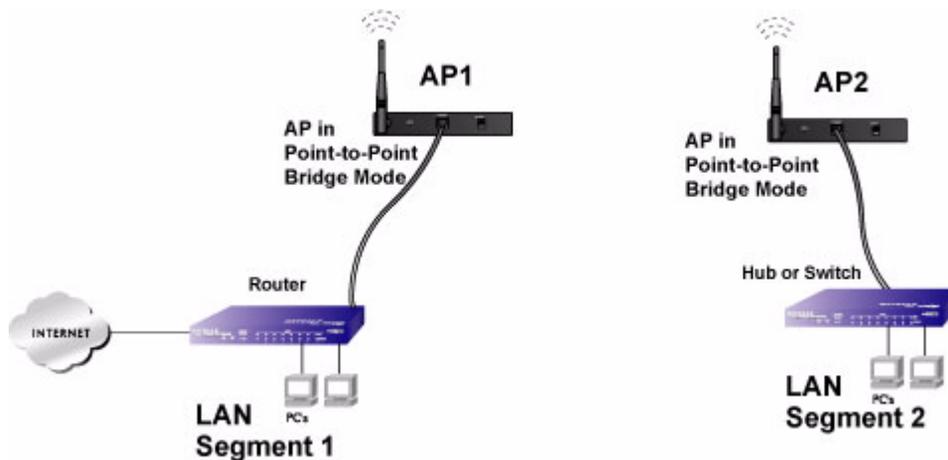


Figure 5-6: Point-to-Point Bridge

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

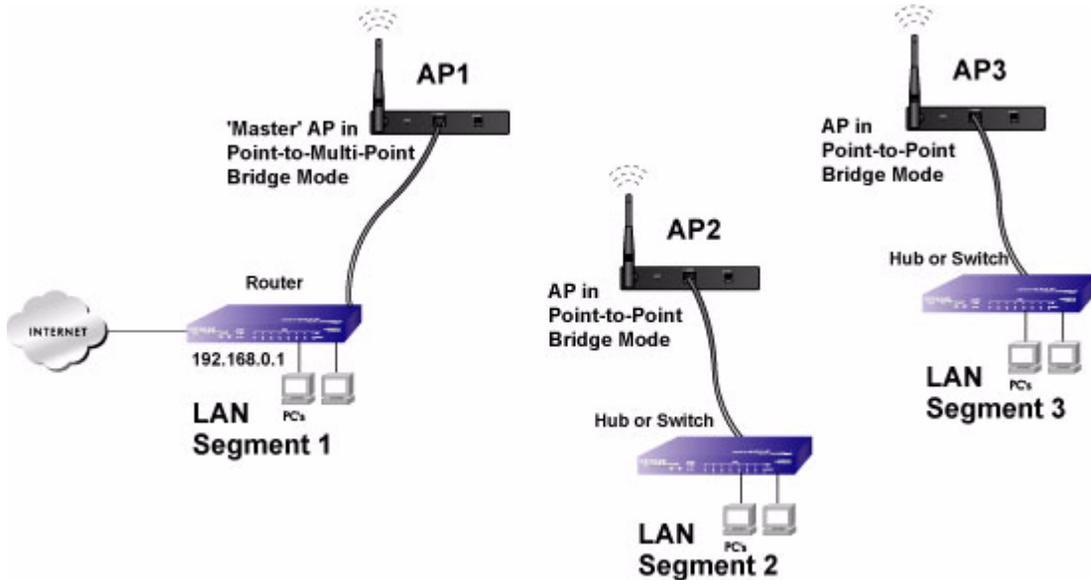


Figure 5-7: Multi-Point bridging

1. Configure the Operating Mode of the WG102 Access Points.
 - Because it is in the central location, configure WG102 (AP1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode. The MAC addresses of AP2 and AP3 are required in AP1.
 - Configure WG102 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.
 - Configure the WG102 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.
2. Verify the following parameters for all access points:
 - Verify that the LAN network configuration of the WG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
 - Only one AP is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
 - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.

- If using DHCP, all WG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
 - All WG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
 - All Point-to-Point APs must have AP2’s MAC address in its Remote AP MAC address field.
3. Verify connectivity across the LANs.
- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
 - Wireless stations will not be able to connect to the WG102 Access Points in the illustration above. If you require wireless stations to access any lan segment, you can 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

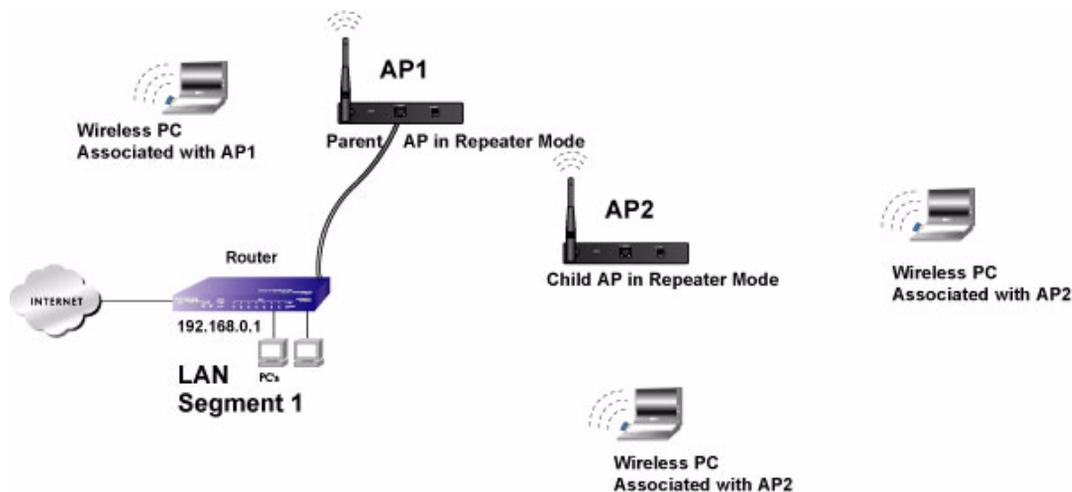


Figure 5-8: Repeater bridging

1. Configure the Operating Mode of the WG102 Access Points.
 - Configure AP1 on LAN Segment 1 as the Parent in Repeater mode with its own MAC address in the Parent AP MAC Address field, and the MAC Address of the 'downstream' AP (AP2) in the Child AP MAC Address field.
 - Configure AP2 in as the Child Repeater mode with its MAC addresses as in the Child AP MAC Address field and the MAC address of the 'upstream' AP (AP1) in the Parent MAC Address field.
2. Verify the following parameters for all access points:
 - Verify that the LAN network configuration of the WG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
 - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
 - If using DHCP, all WG102 Access Points should be set to "Obtain an IP address automatically (DHCP Client)" in the IP Address Source portion of the Basic IP Settings menu.
 - All WG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.

3. Verify connectivity across the LANs.

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

Note: You can extend this repeating by adding up to 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.](#)

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

When I enter a URL or IP address I get a timeout error.

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

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WG102 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WG102 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, CE, C-TICK, Medical EMC EN60601 |
| Environmental Specifications | Operating temperature: 0 to 45° C Operating humidity: 5-95%, non-condensing |
| Wireless | |
| Data Encoding: | 802.11b: 1 and 2 Mbps, Direct Sequence Spread Spectrum (DSSS) 802.11b: 5.5 and 11 Mbps, Complementary Code Keying (CCK) 802.11g: All rates, Orthogonal Frequency Division Multiplexing (OFDM) |
| Maximum Computers Per Wireless Network: | Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes. |
| 802.11b and g Radio Data Rate | 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable) |
| 802.11b and g Operating Frequencies and Channels | 2.412 ~ 2.462 GHz (North America), Channels 1-11 2.412 ~ 2.472 GHz (Europe including France and Spain, and Japan), Channels 1-13 |

| Parameter | NETGEAR WG102 ProSafe 802.11g Wireless Access Point |
|--|--|
| 802.11b and g Typical Maximum Transmit Power | 802.11b mode, 1 to 11Mbps: +19 dBm* 802.11g mode, 6 to 24 Mbps: +18 dBm* 802.11g mode, 36/48/54 Mbps: +17/16/15 dBm* *Note: Maximum transmit power varies based on country or region selection to ensure local regulatory compliance. |
| 802.11b and g Typical Receive Sensitivity | 802.11b mode at 1Mbps: -95 dBm 802.11b mode at 2 Mbps: -93 dBm 802.11b mode at 5.5 Mbps: -91dBm 802.11b mode at 11 Mbps: -89 dBm 802.11g mode at 6 Mbps: -91 dBm 802.11g mode at 9 Mbps: -90 dBm 802.11g mode at 12 Mbps: -89 dBm 802.11g mode at 18 Mbps: -87 dBm 802.11g mode at 24 Mbps: -84 dBm 802.11g mode at 36 Mbps: -81 dBm 802.11g mode at 48 Mbps: -77 dBm 802.11g mode at 54 Mbps: -75 dBm 802.11g mode at 108 Mbps: -72 dBm |
| Antenna: | One (1) external 5 dBi 2.4 GHz detachable antenna |
| 802.11 Security | 40-bits (also called 64-bits), 128, and 152-bits WEP data encryption; WPA and WPA2 |

Appendix B

Related Documents

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

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

Glossary

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

802.11 Standard

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), <http://standards.ieee.org>. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi, 802.11, is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for WLANs operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

802.11a Standard

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.85 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b Standard

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11d Standard

802.11d is an IEEE standard supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for client devices. The devices will automatically adjust based on geographic requirements.

The purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries. Equipment manufacturers do not want to produce a wide variety of country-specific products and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

802.11e Standard

802.11e is a proposed IEEE standard to define quality of service (QoS) mechanisms for wireless gear that gives support to bandwidth-sensitive applications such as voice and video.

802.11g Standard

Similar to 802.11b, this physical layer standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

802.11i

This is the name of the IEEE Task Group dedicated to standardizing WLAN security. The 802.11i Security has a frame work based on RSN (Robust Security Mechanism). RSN consists of two parts: 1) The Data Privacy Mechanism and 2) Security Association Management.

The Data Privacy Mechanism supports two proposed schemes: TKIP and AES. TKIP (Temporal Key Integrity) is a short-term solution that defines software patches to WEP to provide a minimally adequate level of data privacy. AES or AES-OCB (Advanced Encryption Standard and Offset Codebook) is a robust data privacy scheme and is a longer-term solution.

Security Association Management is addressed by a) RSN Negotiation Procedures, b) IEEE 802.1x Authentication and c) IEEE 802.1x Key management.

The standards are being defined to naturally co-exist with pre-RSN networks that are currently deployed.

802.11n Standard

A recently formed (Oct 2003) IEEE official task group referred to as: 802.11n or TGn for the 100 Mbps wireless physical layer standard protocol. Current published ratification date is December 2005. As of February 2004, no draft specification has been written - It is expected to use both the 2.4 and 5GHz frequencies.

AES (Advanced Encryption Standard)

A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM. AES is expected to replace WEP as a WLAN encryption method in 2003.

Access Point (AP)

A wireless LAN transceiver or base station that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

There are various types of access points, also referred to as base stations, used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

Ad-Hoc mode

A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is one where PCs communicate with each other through an AP. See access point and Infrastructure mode.

Bandwidth

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

Bits per second (bps)

A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second—bps—is often confused with bytes per second—Bps. While bits is a measure of transmission speed, bytes is a measure of storage capability. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps or 11 Mbits/sec), it is sending data at 1.375 megabytes per second (1.375 Mbps).

Bluetooth Wireless Technology

A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need

for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet and up to 11Mbps raw data throughput.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

BSSID (see also SSID)

When one AP is connected to a wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a 32-character unique identifier attached to the header of packets sent over a WLAN that differentiated one WLAN from another when a mobile device tries to connect to the network.

Client or Client devices

Any computer connected to a network that requests services (files, print capability) from another member of the network. Clients are end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

Collision avoidance

A network node characteristic for proactively detecting that it can transmit a signal without risking a collision, thereby ensuring a more reliable connection.

Crossover cable

A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals cross over. If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They cross over from one side to the other.

CSMA-CA (Carrier Sense Multiple Action)

CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a listen before talk: method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously.

Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive

station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission

CSMA-CD (Carrier Sense Multiple Action/Collision Detection)

A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

DHCP (Dynamic Host Configuration Protocol)

A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

Diversity: antenna

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference

DNS (Domain Name System)

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

Encryption Key

An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). 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 WEP known vulnerabilities.

Enterprise-level User Authentication via 802.1x and EAP

WEP has almost no user authentication mechanism. To strengthen user authentication, Wi-Fi Protected Access implements 802.1x and the Extensible Authentication Protocol (EAP). Together, these implementations provide a framework for strong user authentication. This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs mutual authentication so that the wireless user doesn't accidentally join a rogue network that might steal its network credentials.

ESSID (more commonly referred to as SSID – Short Set Identifier)

The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

Ethernet

International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Hot Spot (also referred to as Public Access Location)

A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as CoolSpots.

Hub

A multiport device used to connect PCs to a network via Ethernet cabling or via Wi-Fi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

HZ ('hertz')

The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.

IEEE (Institute of Electrical and Electronics Engineers)

A membership organization (www.ieee.org) that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

IEEE 802.11

A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. WECA's (Wireless Ethernet Compatibility Alliance – now Wi-Fi Alliance) focus is on 802.11b, an 11 Mbps high-rate DSSS standard for wireless networks.

Infrastructure mode

A client setting providing connectivity to an access point (AP). As compared to Ad-Hoc mode, whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.

IP (Internet Protocol) address

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

ISO Network Model

A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- Physical
- Data Link
- Network
- Transport

- Session
- Presentation
- Application

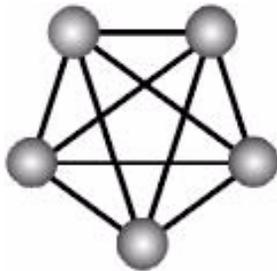
The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

MAC (Media Access Control)

Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

Mesh Networks

Also called mesh topology, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a full mesh topology every node has a connection to every other node in the network. Mesh networks may be wired or wireless.



Mesh network

In a wireless mesh example, each of the spheres below represent a mesh router. Corporate servers and printers may be shared by attaching to each mesh router. For wireless access to the mesh, an access point must be attached to any one of the mesh routers.

Multiple Input Multiple Output (MIMO)

MIMO refers to radio links with multiple antennas at the transmitter and the receiver side to improve the performance of the wireless link.

NAT (Network Address Translation)

A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Network name

Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

NIC (Network Interface Card)

A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

PC card (also called PCMCIA)

A removable, credit-card-sized memory or I/O (input/output) device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

PCI adapter

A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

Peer-to-peer network (also called Ad-Hoc in WLANs)

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

PHY

The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

Plug and Play

A computer system feature that provides for automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

Proxy server

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data

Range

The distance away from your access point that your wireless network can reach. Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile

Residential gateway

A wireless device that connects multiple PCs, peripherals and the Internet on a home network. Most Wi-Fi residential gateways provide DHCP and NAT as well.

RJ-45

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming

Moving seamlessly from one AP coverage area to another with your laptop or desktop with no loss in connectivity.

Rogue Access Point

Rogue AP is a term used to describe an unauthorized access point that is connected on the main home or corporate network or operating in a stand-alone mode (in a parking lot or in a neighbor's building). Rogue APs, by definition, are not under the management of network administrators and do not conform to network security policies and may present a severe security risk. Ideally, it is best to have some type of WLAN system that does not allow rogue access points to easily be added to an existing WLAN.

Router

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

Satellite broadband

A wireless high-speed Internet connection provided by satellites. Some satellite broadband connections are two-way—up and down. Others are one-way, with the satellite providing a high-speed downlink and then using a dial-up telephone connection or other land-based system for the uplink to the Internet.

Server

A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

Site survey

The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

SSID (also called ESSID)

A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

SSL (Secure Sockets Layer)

Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Switch

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a network's traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

TCP (Transmission Control Protocol)

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

TKIP

A security feature that is a WEP enhancement: Temporal Key Integrity Protocol and Message Integrity Check (MIC) is a modification of WEP to defend against known attacks (WEP+ four patches for key mixing, message integrity, rekeying, initialization vector protection)

USB (Universal Serial Bus)

A high-speed bidirectional serial connection between a PC and a peripheral that transmits data at the rate of 12 megabits per second. The new USB 2.0 specification provides a data rate of up to 480 Mbps, compared to standard USB at only 12 Mbps. 1394, FireWire and iLink all provide a bandwidth of up to 400 Mbps.

VLAN (Virtual LAN) IEEE 802.1Q

The VLAN standard is defined by the IEEE. Short for virtual LAN, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation and resource optimization.

VoIP (Voice over IP)

Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

VPN (Virtual Private Network)

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a

private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

War Chalking

The act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

There are three basic designs that are currently used: a pair of back-to-back semicircles, which denotes an open node; a closed circle, which denotes a closed node; a closed circle with a “W” inside, which denotes a node equipped with WEP. Warchalkers also draw identifiers above the symbols to indicate the password that can be used to access the node, which can easily be obtained with sniffer software.

As a recent development, the debate over the legality of warchalking is still going on.

The practice stems from the U.S. Depression-era culture of wandering hobos who would make marks outside of homes to indicate to other wanderers whether the home was receptive to drifters or was inhospitable.

War Driving

War driving is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Some people have made a sport out of war driving, in part to demonstrate the ease with which wireless LANs can be compromised. With an omnidirectional antenna and a geophysical positioning system (GPS), the war driver can systematically map the locations of 802.11b wireless access points.

WEP (Wired Equivalent Privacy)

Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Wi-Fi (Wireless Fidelity)

Another name for IEEE 802.11b. Products certified as Wi-Fi are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

Wi-Fi Alliance (formerly WECA – Wireless Ethernet Compatibility Alliance)

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 193 member companies from around the world, and 509 products have received Wi-Fi certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability (www.weca.net).

Wi-Fi Protected Access (WPA)

WPA is a security technology for wireless networks that improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP.

One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use. This is similar to 802.1x support and requires a RADIUS server in order to implement. The Wi-Fi Alliance will call this, 'WPA-Enterprise.'

One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short - this provides an authentication alternative to an expensive RADIUS server. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or passphrase as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. The Wi-Fi Alliance will call this, 'WPA-Personal.'

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward-compatible with the IEEE 802.11i security specification currently under development by the IEEE. Wi-Fi Protected Access is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi CERTIFIED products as a software upgrade. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS, secure fast handoff, secure de-authentication and disassociation, 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.

Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise with IT resources, Wi-Fi Protected Access should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. With this implementation in place, the need for add-on solutions such as VPNs may be eliminated, at least for the express purpose of securing the wireless link in a network.

Wi-Fi Protected Access for Home/SOHO

In a home or Small Office/ Home Office (SOHO) environment, where there are no central authentication servers or EAP framework, Wi-Fi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually-entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in their access point or home wireless gateway and each PC that is on the Wi-Fi wireless network. Wi-Fi Protected Access takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process, described above.

Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in Wi-Fi Protected Access may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in hot spots where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

Wi-Fi Protected Access in Mixed Mode Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a mixed mode, which supports both clients running Wi-Fi Protected Access and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all the devices. Therefore, organizations will benefit by accelerating the move to Wi-Fi Protected Access for all Wi-Fi clients and access points.

WiMAX

An IEEE 802.16 Task Group that provides a specification for fixed broadband wireless access systems employing a point-to-multipoint (PMP) architecture. Task Group 1 of IEEE 802.16 developed a point-to-multipoint broadband wireless access standard for systems in the frequency range 10-66 GHz. The standard covers both the Media Access Control (MAC) and the physical (PHY) layers. Ratification is expected in second half of 2004.

Wireless Multimedia (WMM)

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video, audio, or voice will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

Wireless Networking

Wireless Networking refers to the infrastructure enabling the transmission of wireless signals. A network ties things together and enables resource sharing.

WLAN (Wireless LAN)

Also referred to as LAN. A type of local-area network that uses wireless or high-frequency radio waves rather than wires to communicate between nodes.