NETGEAR WNAP210 ProSafe Wireless-N Access Point Reference Manual

NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

202-10474-01
February 2009
v1.0

Technical Support

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

NETGEAR, INC. Support Information

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

E-mail: support@netgear.com

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

Trademarks

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

Statement of Conditions

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

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

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe Wireless-N Access Point WNDAP210 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.

The 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.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasProSafe Wireless-N Access Point WNDAP210 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

	**Note:** Delete this note and the information below for products that are not wireless.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

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

EN300 328, EN301 489-17, EN60950, EN301 893

Europe – Declaration of Conformity in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES..
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan 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 Radiolan 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 Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan 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 Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan 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 Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WNAP210 ProSafe Wireless-N Access Point WNDAP210 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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 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 to correct the interference by one or more of the following methods:

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

ProSafe Wireless-N Access Point WNAP210

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE
PY308400098

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (ProSafe Wireless-N Access Point WNDAP210) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-WG111

Product and Publication Details

Model Number:	WNAP210
Publication Date:	February 2009
Product Family:	Wireless Access Point
Product Name:	ProSafe Wireless-N Access Point WNAP210
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10474-01
Publication Version Number:	1.0

About This Manual

The *NETGEAR® ProSafe™ Wireless-N Access Point WNAP210 Reference Manual* describes how to install, configure and troubleshoot the ProSafe 802.11n Wireless Access Point WNAP210. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope

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

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

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

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

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

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

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

	**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope**. This manual is written for the WNDAP330 Wireless Access Point according to these specifications:

Product Version	ProSafe 802.11n Wireless Access Point WNAP210
Manual Publication Date	February 2009

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

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

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print This Manual

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

- **Printing a page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - **Printing a PDF chapter.** Use the **PDF of This Chapter** link at the top left corner of any page.
    - Click the **PDF of This Chapter** link at the top left corner of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
  - **Printing a PDF version of the complete manual**. Use the **Complete PDF Manual** link at the top left corner of any page.
    - Click the **Complete PDF Manual** link at the top left corner of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left corner of your browser window.

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

Revision History

Part Number	Version Number	Date	Description
202-104741-01	1.0	February 2009	Initial edition: New product

Chapter 1
Introduction

This chapter describes some of the key features of the NETGEAR ProSafe Wireless-N Access Point WNAP210. It also includes the minimum prerequisites for installation ("System Requirements" on page 1-6.), package contents ("What's In the Box?" on page 1-6) and a description of the front and back panels of the WNAP210 ("Hardware Description" on page 1-7).

About the ProSafe Wireless-N Access Point WNAP210

The ProSafe Wireless-N Access Point WNAP210 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 WNAP210 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 of about a 500 foot radius. Consequently, the ProSafe Wireless-N Access Point WNAP210 can support a small group of users in a range of several hundred feet. Most access points can handle between 10 to 30 users simultaneously.

The ProSafe Wireless-N Access Point WNAP210 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WNAP210 Wireless-N 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 ProSafe Wireless-N Access Point WNAP210 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features and Standards

The WNAP210 Wireless-N Access Point is easy-to-use and provides solid wireless and networking support. It also offers a wide range of security options.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliance.** The Wireless Access Point complies with the IEEE 802.11 b/g standards for Wireless LANs, and is WiFi certified for 802.11n draft 2.0 standard.
- **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 preshared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- **Multiple BSSIDs.** Supports multiple BSSIDs. When a wireless access point is connected to a wired network and a set of wireless stations, it is called a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.

  The multiple BSSID feature allows you to configure up to 8 SSIDs per Radio mode on your access point and assign different configuration settings to each SSID. All the configured SSIDs are active and the network devices can connect to the access point by using any of these SSIDs.
- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WNAP210 can act as a client and obtain information from your DHCP server; it can also act as a DHCP server and provide network information for wireless clients.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.
- **802.1Q VLAN (Virtual LAN) Support.** A network of computers that behave as if they are connected to the same network even though they actually may 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.

Key Features

The WNAP210 provides solid functionality, including the following features:

- **Band Selection.** The Wireless Access Point allows you to configure the band you wish to use. For each Access Point, you can choose to operate in either the 2.4 GHz band or the 5 GHz band.

  The choice of band is reflected in protocol standard supported, as well as the administration screens displayed to you. For example, if you choose to enable the 2.4 GHz band, only 802.11b/g/n protocols are supported. In addition, in the administration screens, the configuration options for 802.11a/n protocols are greyed out. On the other hand, if you enable the 5GHz band, the 802.11 a/n protocols are support and the 802.11b/g/n protocol support is disabled. In this case, the configuration options for 802.11b/g/n protocols are greyed out.

- Multiple operating modes:
  - Wireless Access Point. Operates as a standard 802.11a/b/g/n access point.
  - Point-to-Point Bridge. In this mode, the WNAP210 only communicates with another bridge-mode wireless station or access point. Network authentication should be used to protect this communication.
  - Point-to-Multi-Point Bridge. Select this only if this WNAP210 is the “Master” for a group of bridge-mode wireless stations. The other bridge-mode wireless stations send all traffic to this “Master”, and do not communicate directly with each other. Network Authentication should be used to protect this traffic.
  - Wireless Repeater. In this mode, WNAP210 does not function as an access point. It communicates with only repeater-mode, point-to-point-bridge-mode, and point-to-multi-point-bridge-mode wireless stations. Network authentication should be used to protect this communication.

- **Hotspot Settings.** You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely. In addition to using Web browser to do so, command-line interface can also be used.
- **Rogue AP Detection.** The Rogue AP filtering feature ensures that unknown APs ae not given access to any part of the LAN.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WNAP210 to gain access to your LAN.

- **Security Profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, etc.) for each BSSID.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Secure Telnet Command Line Interface.** The Telnet command line interface enables direct access over the serial port and easy scripting of configuration of multiple WNAP210 across an extensive network via the Ethernet interface. An SSH client is required.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Secure and Economical Operation.** Adjustable power output allows more secure or economical operation.
- **Power over Ethernet.** Power can be supplied to the WNAP210 over the Ethernet port from any 802.3af compliant mid-span or end-span source. Please refer to the Appendix for a list of compliant Netgear PoE switches.
- **Autosensing Ethernet Connection with Auto Uplink Interface.** Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power, test, LAN speed, LAN activity, and wireless activity for each radio mode are easily identified.
- **Wireless Multimedia (WMM) Support.** WMM 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, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.
- **Quality of Service (QoS) Support.** You can configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point. The QoS feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped.
- **VLAN Security Profiles.** Each Security Profile is automatically allocated a VLAN ID as each Security Profile is modified.

802.11a/b/g/n Standards-based Wireless Networking

The ProSafe Wireless-N Access Point WNAP210 provides a bridge between Ethernet wired LANs and 802.11a/b/g/n 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 WNAP210 supports the following wireless features:

- Aggregation Support

- Reduced InterFrame Spacing support
- Multiple Input, Multiple Output (MIMO) support
- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Auto or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The WNAP210 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

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

Compatible and Related NETGEAR Products

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

The following NETGEAR products work with the WNAP210 Wireless-N Access Point:

- FS108P - ProSafe 8 Port 10/100 Switch with 4 Port PoE
- FS116P ProSafe 16 Port 10/100 Desktop Switch with 8 Port PoE
- FS726TP - ProSafe 24 Port 10/100 Smart Switch with 2 Gigabit Ports and 12 Port PoE
- FS728TP - ProSafe 24+4 10/100 Smart Switch with full PoE
- FS752TPS - ProSafe 48 Port 10/100 Stackable Smart Switch with 4 Gigabit Ports and 24 Port PoE
- FSM7328PS - ProSafe 24-port 10/100 L3 Managed Stackable Switch with 24 PoE Ports
- FSM7352PS - ProSafe 48 Port 10/100 L3 Managed Stackable Switch with 4 Gigabit Ports and 48 Port PoE

- GS724TP - ProSafe 24-Port GE PoE Smart Switch
- GS748TP - ProSafe 48-Port GE PoE Smart Switch
- WNDA3100 - RangeMax Dual Band Wireless-N USB 2.0 Adapter
- WN121T RangeMax NEXT Wireless-N USB 2.0 Adapter
- WN111 - RangeMax Next Wireless-N USB Adapter
- WN511B RangeMax NEXT Wireless-N Notebook Adapter
- WN311B RangeMax NEXT Wireless-N PCI Adapter
- 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 USB Adapter
- WPN111 - RangeMax Wireless USB 2.0 Adapter

System Requirements

Before installing the WNAP210, make sure your system meets these requirements:

- A 10/100/1000 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 100-120 V, 50-60 Hz AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 5.0 or above, or Mozilla 3.0 or above
- At least one computer with the TCP/IP protocol installed
- 802.11b/g/n or 802.11b/g/n-compliant devices, such as the NETGEAR WG511 Wireless Adapter

What’s In the Box?

The product package should contain the following items:

- ProSafe Wireless-N Access Point WNAP210

- Power adapter and cord (12 V dc, 1.0 A)
- Straight-through Category 5 Ethernet cable
- NETGEAR WNAP210 Wireless-N Access Point Installation Guide
- *Resource CD* which includes this manual
- Wall mount kit

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 WNAP210 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

This section describes the front and rear hardware functions of the WNAP210.

Front Panel

The WNAP210 front hardware functions are described below.

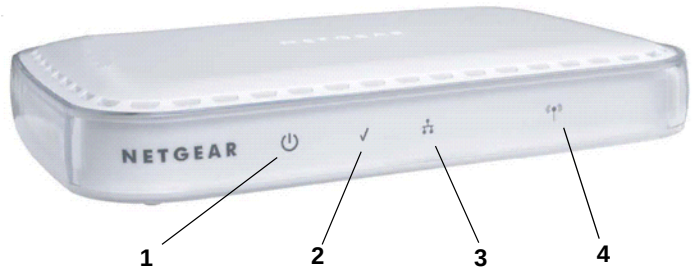

Figure 1-1

The following table explains the LED indicators:

Table 1-1. Front Panel LED Indicators

Item	LED	DESCRIPTION
1		Power Indicator Off: Power is off. On: Power is on.
2		Self Test Indicator Blink: Indicates self test, loading software. This LED may blink for a minute before going off. If it continues to blink it indicates a system fault.
3		Ethernet LAN Speed Indicator Off: Indicates 10 Mbps or no link detected. Yellow: Indicates 100 Mbps link detected. Green: Indicates 1000 Mbps link detected.
4		Blink (Green): Indicates data traffic on the 100Mbps Ethernet LAN.

Rear Panel

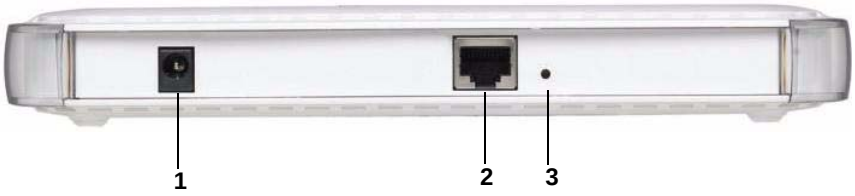

Figure 1-2

The WNAP210 rear panel functions are described below:

1. Restore to Factory Defaults Button: The restore to default button located between the Ethernet RJ-45 connector and the power socket restores the WNAP210 to the factory default settings.
2. RJ-45 Ethernet Port: Use the WNAP210 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or PoE switch.
3. Power Socket: This socket connects to the WNAP210 12V 1.0A power adapter.

Chapter 2
Installation and Configuration

This chapter describes how to set up your ProSafe Wireless-N Access Point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b/g/Next or 802.11b/g wireless adapters to connect to the Internet, or access printers and files on your LAN.

Note: Indoors, computers can connect over 802.11b/g/Next or 802.11b/g 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 Access Point provides highly effective security features which are covered in detail in "Understanding WNAP210 Wireless Security Options" on page 3-1. 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 WNAP210 that conforms to the "Wireless Equipment 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/g/Next or 802.11b/g wireless adapters.

Wireless Equipment 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 WNAP210. For complete performance specifications, see Appendix A, "Default Settings and Technical 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.

A Wall Mount Kit is provided with your wireless access point. For installation instructions, see "Installing the Wall Mount Kit (Optional)" on page 2-10.

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. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer.

System Requirements

Before installing the WNAP210, make sure your system meets these requirements:

- A 10/100/1000 Mbps Local Area Network device such as a hub, router, or switch.
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it.
- The 100-120 V, 50-60 HZ AC Power Source that came with your device.
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape Navigator 4.78 or above or Mozilla Firefox.
- At least one computer with the TCP/IP protocol installed.
- 802.11n-compliant wireless adapters or 802.11b/g-compliant devices.

Configuring the Access Point

Before installing the ProSafe Wireless-N 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 802.11Next/b/g or 802.11b/g 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 "System Requirements" on page 1-2.

To log into the Access Point:

1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.
2. Turn on your computer and configure your computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.
3. Connect an Ethernet cable from the WNAP210 to the computer.
4. Connect the power adapter to the WNAP210 and verify the following:
   - The PWR power light goes on.
   - The Ethernet port of the wireless access point is lit when connected to a powered on computer.
   - The WLAN LED should be blinking.

Setting Your Basic LAN Settings

The following sections describe how to log in to the wireless access point and to configure your basic LAN settings.

To configure the WNAP210 for LAN access:

1. Connect to the WNAP210 by opening a browser window on your PC and entering **http://192.168.0.236** in the address field. The WNAP210 login screen will appear.
2. Enter **admin** for the user name and **password** for the password, both in lower case letters.

Figure 2-1

3. Click **OK**. The main menu of the WNAP210 will display as shown in Figure 2-2.

- When the wireless access point is connected to the Internet, you can select the Documentation link under the Web Support menu to view the documentation for the wireless access point.
- When connected to the Internet, you can also select KnowledgeBase to access Application Notes relevant to wireless networking.
- Select Logout to exit the WNAP210 setup screens. (You will automatically be logged out of the wireless access point after 5 minutes of no activity.)

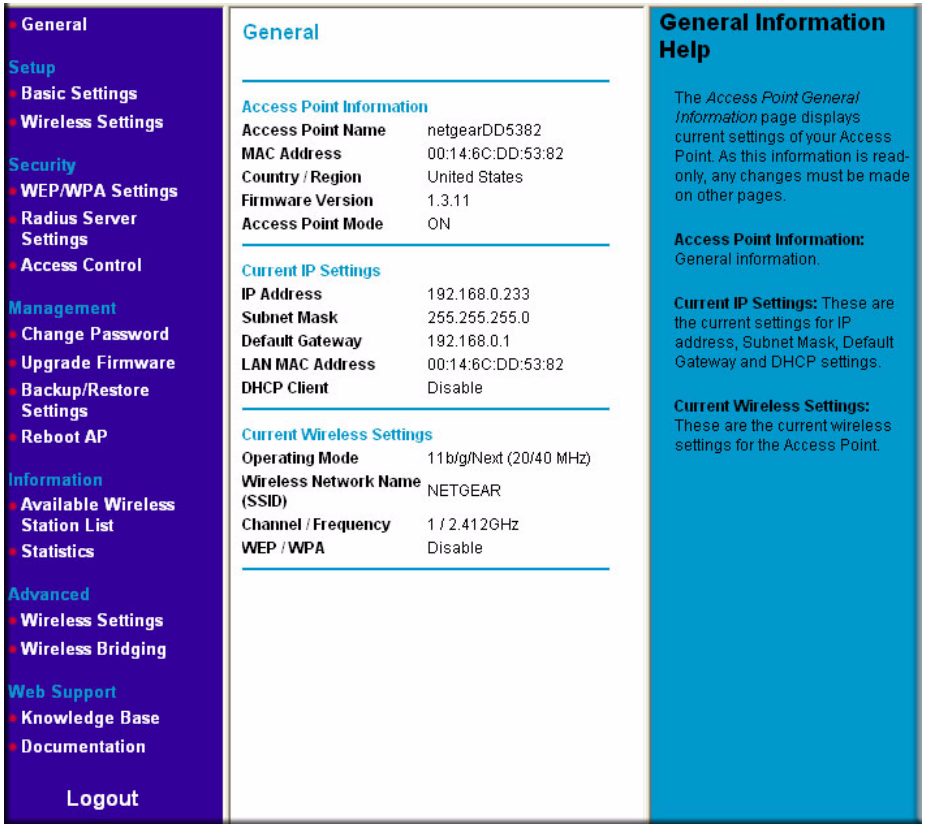

Figure 2-2

To configure the Basic LAN settings:

1. Select **Basic Settings** under **Setup** on left side of the main menu. The Basic Settings screen will display. The default settings should be suitable for most users and environments.

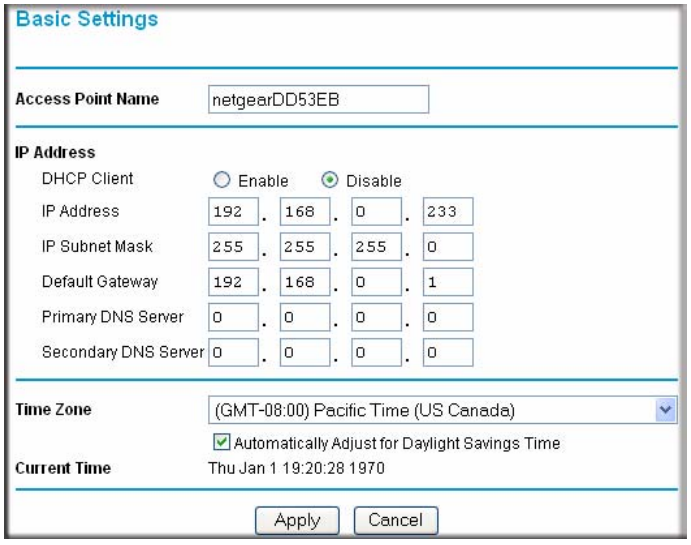

Figure 2-3

2. Enter the **Access Point Name** of the WNAP210.

   This unique name is the access point NetBIOS name. The Access Point Name is printed on the rear label of the WNAP210. The default is **netgearxxxxxx,** where **xxxxxxx** represents the last 6 digits of the WNAP210 MAC address. You may modify the default name with a unique name up to 15 characters long.

3. Enter the IP Address fields of the WNAP210.

   – **DHCP Client**. By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point will get its IP address, subnet mask and default gateway settings automatically from the DHCP server on your network when you connect the WNAP210 to your LAN.

   – **IP Address.** Enter the IP Address of your wireless access point.The default IP address is 192.168.0.236. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP.

   – **IP Subnet Mask**. The Access Point will automatically calculate the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 (the default) as the subnet mask.

- **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected. The default is 0.0.0.0.
- **Primary DNS Servers.** The WNAP210 will use this IP address as the primary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.
- **Secondary DNS Servers.** The WNAP210 will use this IP address as the secondary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.

4. From the pull-down menu, select the local **Time Zone** for your wireless access point from a list of all available time zones. The default is GMT.-08:00
5. Check the **Adjust for Daylight Saving Time** if your location uses daylight savings. The default is no adjustment.

	**Note:** If you do not have an Internet connection to get the current time, the wireless access point will get the current time from the connecting PC.

6. Click **Apply** to save your Basic IP settings.

	**Note:** If you change the default subnet of the LAN IP address, you will be disconnected from the Access Point user interface. To reconnect, reconfigure your computer with a static IP address within the new LAN IP subnet.

By default, the WNAP210 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting (see “Logging in to the Access Point” on page 2-12),

Configuring Your Wireless Settings

The following sections describe how to configure the wireless settings for both the 802.11b/g/Next and 802.11b/g modes.

To configure the Access Point wireless settings of your wireless access point:

1. From the main menu under Setup, select **Wireless Settings**.The Wireless Settings screen will display as shown in Figure 2-4 below

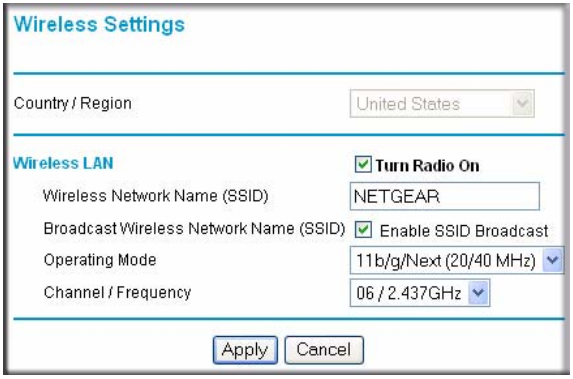

Figure 2-4

2. From the **Country/Region** pull-down menu, select the region where the WNAP210 can be used (the Country/Region is not Configurable in the United States; but is configurable in the rest of the world).

	Note: If your country or region is not listed, please check with your local government agency.

3. Configure the Wireless LAN settings based on the following field descriptions:

- **Turn Radio On**. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID)**. Enter a 32-character (maximum) service set ID in this field; the characters are case sensitive. When the wireless access point is deployed in “infrastructure” mode, the SSID assigned to a wireless device must match the wireless access point SSID in order for the wireless device to communicate with the WNAP210. If they do not match, you will not get a wireless connection to the WNAP210. The default is NETGEAR.
- **Broadcast Wireless Network Name (SSID).** If Enabled, the Wireless Access Point broadcasts its SSID allowing Wireless Stations which have a “null” (blank) SSID to adopt the correct SSID. If set to disable, the SSID is not broadcast. The default is Enabled.
- **Wireless Mode**. From the pull-down menu, select the desired wireless operating mode:
  - 11b/g – Both 802.11b and 802.11g wireless stations can be used.

– 11b/g/Next – 802.11b, 802.11g and 802.11n wireless stations can be used.

The default is 11b/g/Next

- **Channel/Frequency**. From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channels to use in the U.S. and Canada are 1 to 11; for Europe and Australia, 1 to 13. The default is channel 6.

  It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may want to experiment with different channels to see which is the best. See the article on "Wireless Channels" available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, "Related Documents.")

4. Click **Apply** to save your wireless settings.

Verifying Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs (see "Wireless Security Settings").

1. From a web browser, log in to the WNAP210 using its default address of **http://192.168.0.236**. Use the default user name of **admin** and default password of **password**—or use a new LAN address and password if you have set them up.
2. From the main menu under Setup, select Basic Settings. Verify that the correct Country/Region in which the wireless interface will operate has been selected.
3. Click **Apply** to save any changes.
4. From the main menu under Setup, verify your Operating Mode—either 11b/g/Next or 11b/g. Verify that the correct (default) channel has been selected for your network.

   It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point.

Click **Apply** to save any changes.

	**Note:** If you are unable to connect, see Chapter 6, "Troubleshooting."

Deploying the Access Point

Now that you have completed the setup steps, you can deploy the WNAP210 in your network. If needed, you can now reconfigure the computer you used in step 1 in "Configuring the Access Point" on page 2-3 back to its original TCP/IP settings.

To deploy the Access Point:

1. Disconnect the WNAP210 and position it where it will be deployed. 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.
2. Connect an Ethernet cable from your Access Point to a LAN port on your router, switch, or hub. Connect the power adapter to the wireless access point and plug the power adapter into a power outlet. The PWR, LAN, and Wireless LAN LEDs and should light up

Tip: Before mounting the WNAP210 in a high location, first set up and test the WNAP210 to verify wireless network connectivity.

Installing the Wall Mount Kit (Optional)

Before you begin installation, check to make sure that the four screws selected to secure the brackets fit flush within the molding of the bracket. An illustration of the installation steps is shown in Figure 2-5 on page 2-11.

To install the wireless access point mounting brackets:

1. Place the bottom bracket on the wall where you want to install the WNAP210. Securely screw the bottom bracket into the wall, making sure the screws are flush with the bracket (Step 1).
2. Snap the WNAP210 into place on the bottom bracket (Step 2). The tabs on the bottom of the bracket will snap into the slots on the bottom of the WNAP210.
3. Firmly secure the top bracket onto the WNAP210 and attach the bracket with two additional screws (Step 3). Ensure that the bracket flange engages with the top lip of the WNAP210 before screwing in the bracket.

Should you need to remove the WNAP210, unscrew the top bracket, and then unsnap the WNAP210 from the bottom bracket. Never try to remove your wireless access point before removing the top bracket.

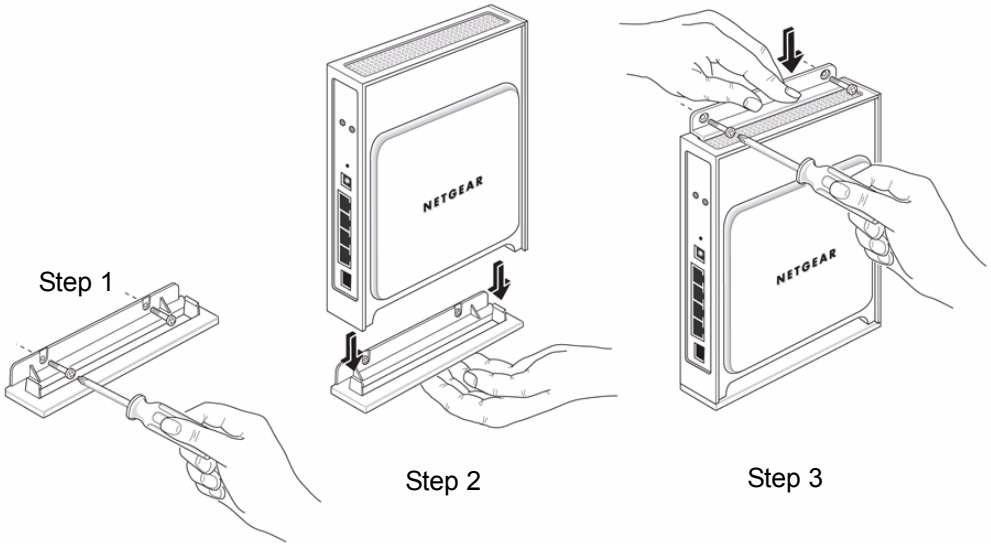

Figure 2-5

Configuring and Testing Your PCs for Wireless Connectivity

Program the wireless adapter of your PCs to have the same SSID and channel that you configured in **Wireless Settings** for the WNAP210. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WNAP210.

	Note: If you are configuring the WNAP210 from a wireless computer and you change the SSID, channel, or Security Profile 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.

Once your PCs have basic wireless connectivity to the WNAP210, you can deploy the WNAP210 and configure the advanced wireless security functions.

Logging in to the Access Point

The WNAP210 is set, by default with the IP address of 192.168.0.236 with DHCP disabled.

	Note: If logging in using the default IP address, the computer you are using to connect to the WNAP210 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

If DHCP is enabled, there are two methods you can use to connect to the WNAP210 after the DHCP server on your network assigns it a new IP address.

- If your wireless access point is to be deployed on a local network, you can enter the NetBIOS[1] name into your Web browser. The default wireless access point name is **netgearxxxxxx**, where **xxxxxx** represents the last 6 bytes of the MAC address. The MAC address is printed on the rear label of the WNAP210. (Using the NetBIOS naming convention to access your router across several network segments is known to be unreliable.)
- Reserve an IP address (based on the WNAP210's MAC address) on the DHCP server. That way, if your router is deployed across several segments, you can configure the wireless access point with a static IP address which you can always use to log in to make future configuration changes.

To log in using the default IP Address:

1. Open a Web browser such as Mozilla Firefox, Internet Explorer or Netscape Navigator.
2. Connect to the WNAP210 by entering the default address of **http://192.168.0.236** into your browser.

Figure 2-6

1. NetBIOS name login is not supported in the initial release of the firmware. Check the Release Notes of your firmware version for NetBIOS support at *http://kbserver.netgear.com/products/WNAP210.asp*.

3. The login screen will display. Enter **admin** for the user name and **password** for the password, both in lower case letters.

Figure 2-7

4. Click **OK**.

   Your Web browser should automatically find the Access Point and display the home screen, as shown in Figure 2-7 above.

Chapter 3
Wireless Security Settings

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 ProSafe Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

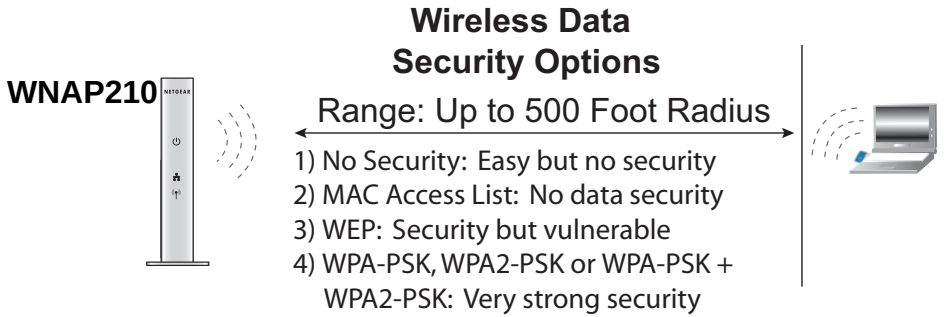

Figure 3-1

Understanding WNAP210 Wireless Security Options

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

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WNAP210. 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-PSK or WPA2-PSK.** Wi-Fi Protected Access (WPA) provides stronger data encryption than WEP. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. The preshared key (PSK) is common to all users. Because this is a recent standard, wireless device driver and software availability may be limited.
- **Use WPA-PSK or WPA2-PSK with Radius.** Using a Remote Authentication Dial In User Service (RADIUS) authentication server allows centralized authentication management with individual user names and passwords.

WEP/WPA Settings

The WNAP210 Access Point is set by default “None” or no authentication. When setting up Network Authentication, bear in mind the following:

Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

- **Network Authentication**. You can configure the ProSafe Access Point to use the types of network authentication shown in the table below.

Table 3-1. Network Authentication Types

Type	Description
None	No data encryption
WEP	Wired Equivalent Privacy using either 64-bit or 128-bit data encryption.
WPA-PSK (TKIP)	Wi-FI Protected Access with Pre-Shared Key, uses WPA-PSK standard encryption with TKIP encryption type.
WPA2-PSK (AES)	Wi-FI Protected Access with Pre-Shared Key, uses WPA-PSK standard encryption with AES encryption type. Only select this if all clients support WPA2.
WPA-PSK (TKIP) + WPA2-PSK (AES)	This selection allows clients to use either WPA-PSK (TKIP) or WPA2-PSK (AES).
WPA with Radius	If selected, you must configure the Radius Server Settings Screen.
WPA2 with Radius	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	If selected, encryption must be TKIP + AES. If selected, you must configure the Radius Server Settings Screen.

- **Data Encryption**. The available options depend on the Network Authentication setting selected (see Table 3-1 above); otherwise, the default is None. The Data Encryption settings are explained in the table below:

Table 3-1. Data Encryption Settings

Data Encryption Type	Description
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.
TKIP	Automatic encryption with WPA-PSK; requires passphrase
AES	Automatic encryption with WPA2-PSK; requires passphrase

- **WEP Authentication Type.** WEP can be authenticated using Open System or Automatic. If set to Open System, clients can only associate to the wireless access point by using the Open System option. If set to Automatic, clients can associate to the wireless access point using both Open System and Shared Key. Setting the Authentication Type to Automatic will detect which WEP authentication method is being used. The default is Automatic.
- Use of Passphrases and Keys are explained below:
  - **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
  - **Key 1, Key 2, Key 3, Key 4**. If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
  - **WPA Preshared Key Passphrase.** If using WPA-PSK, WPA2-PSK or WPA-PSK + WPA2-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.

SSID and WEP/WPA Settings Setup Form

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

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR** is the default WNAP210 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  _____

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID,

- Circle the type of Security Authentication used in your wireless network, and then fill out the appropriate required encryption parameters:

  WEP, WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK

- **WEP Encryption Type:**

  Circle one: Automatic or Open System

  Note: If you selected Open System, the other devices in the network will not connect unless they are set to Open System, and have the same keys in the same positions as those in the WNAP210.

- **WEP Encryption Keys:**

  Circle one: 64 or 128 bits. (Enter all four keys for the Key Size chosen.)

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____

- **WPA Security Encryption** for **WPA-PSK, WPA2-PSK or WPA-PSK + WPA2-PSK.** Record a **Passphrase** between 8 and 63 characters:

  Passphrase: _____

Use the procedures described in the following sections to configure the WNAP210. Store this information in a safe place.

Configuring WEP

To configure WEP data encryption:

1. Select **WEP/WPA Settings** under the Security menu on the left navigation pane. The WEP/WPA Settings screen will display.

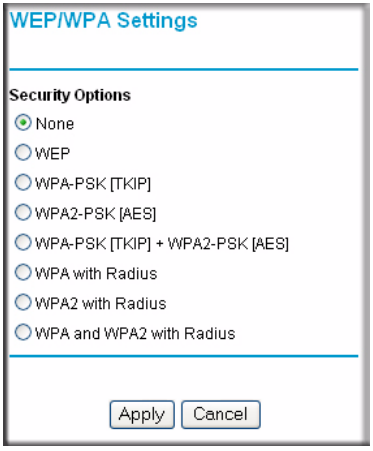

Figure 3-2

2. Check the **WEP** radio button**.** The WEP Security Encryption options will display. Select the **Authentication Type** from the pull-down menu. The default is Automatic.
3. Selection the Encryption Strength from the pull-down menu; either 64-bit or 128 bit.
4. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and wireless access points in your network. Choose either:
   - **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 the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit and 26 digits for 128-bit (any combination of 0-9, a-f, or A-F) Select which of the four keys will be the default.

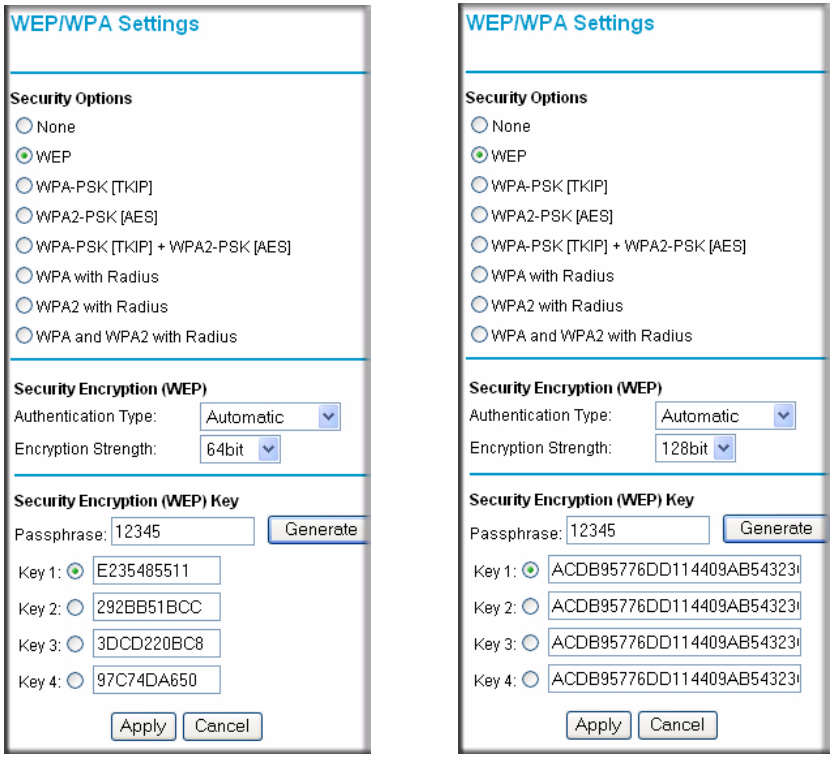

Figure 3-3

5. Select the key to be used as the default key by checking the radio box. (Data transmissions are always encrypted using the default key.)

   See the document “Wireless Communications” for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard. A link to this document on the NETGEAR website is in Appendix B, “Related Documents.”

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

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

Configuring WPA-PSK, WPA2-PSK and WPA-PSK + WPA2-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above 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, WPA2-PSK or WPA-PSK + WPA2-PSK:

1. Select **WEP/WPA Settings** under the **Security** menu on the left navigation pane. The **WEP/WPA Settings** screen will display.

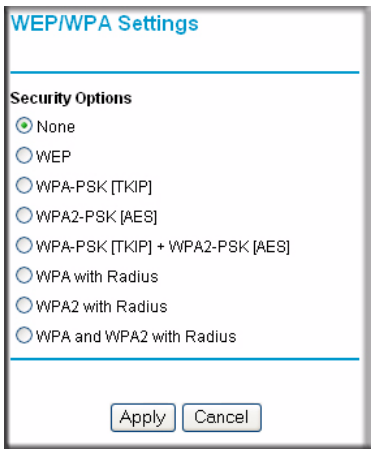

Figure 3-4

2. Select one of the following radio buttons: **WPA-PSK**, **WPA2-PSK** or **WPA-PSK + WPA2-PSK**. The Security encryption Passphrase field will display.

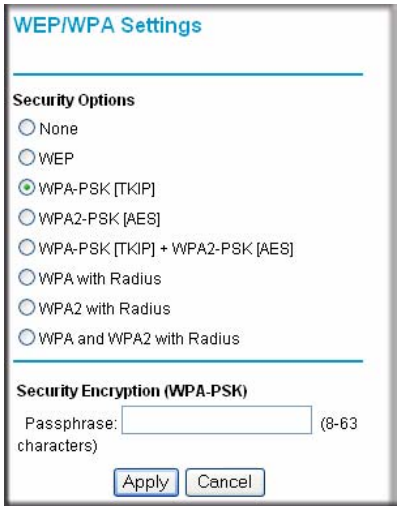

Figure 3-5

3. Enter the preshared key **Passphrase** (Network Key).
4. Click **Apply** to save your settings.

Configuring WPA with Radius, WPA2 with Radius, and WPA + WPA2 with Radius

In an organization with many wireless users, using a single preshared key may not be a practical security method. Deploying a RADIUS server will allow you to manage user authentication individually and centrally.

To configure WPA with Radius, WPA2 with Radius, or WPA + WPA2 with Radius:

1. Select **WEP/WPA Settings** under the **Security** menu on the left navigation pane. The **WEP/WPA Settings** screen will display.

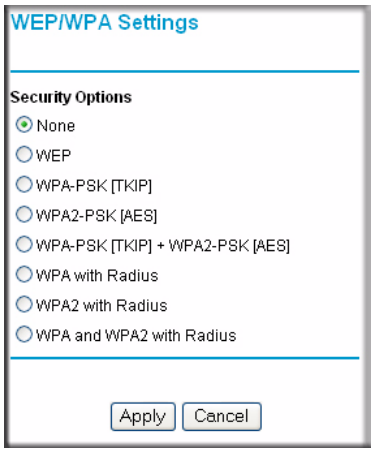

Figure 3-6

2. Select one of the following radio buttons: **WPA with Radius**, **WPA2 with Radius,** or **WPA + WPA2 with Radius**. Your selection will display.

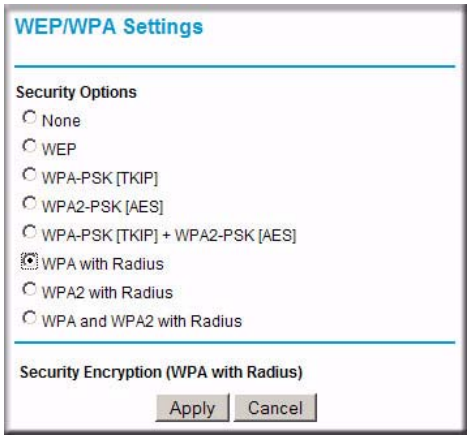

Figure 3-7

3. Click **Apply** to save your settings. A message appears informing you that you must configure the Radius Server Settings menu.
4. Click **OK**.
5. Configure the Radius Server Settings menu using the procedure described in "Configuring the RADIUS Server Settings" on page 4-9.

Restricting Wireless Access by MAC Address

By default, all wireless PCs that are configured with the correct SSID are allowed access to your wireless network. For increased security, you can restrict access to your wireless network to only those trusted wireless PCs based on their MAC address.

The **Access Control List** screen lets you block the network access privilege of any specified stations to only those displayed in the Trusted **Wireless Stations** table. When you enable the **Turn Access Control On** radio box, the access point will only accept connections from those clients on the Trusted Wireless Stations access control list. This provides an additional layer of security.

Note: If configuring the WNAP210 from a wireless computer whose MAC address is not in the **Trusted Wireless Stations** access control list, when 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.

To restrict access based on MAC addresses:

1. Log in to the WNAP210 using the default address of **http:/192.168.0.236,** user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Under Security on the main menu, select **Access Control.** The Access Control menu will display.

Figure 3-8

3. Check the **Turn Access Control On** radio button.
4. Click **Apply** to enable the Access Control feature.

5. The **Trusted Wireless Stations** table will display any wireless stations you have entered. If you have not entered any wireless stations this list will be empty.

> **Note:** If **Turn Access Control On** is enabled and the Access Control List is blank, then no wireless PCs will be able to connect to your wireless network

To delete an existing entry:

Check the radio button adjacent to the entry and then click **Delete**.

To set up the trusted wireless stations control list:

1. Click **Add** on the Access Control List screen. The **Wireless Card Access Setup** screen will display. The **Available Wireless Cards** table will display all available wireless PCs and their MAC addresses.

Figure 3-9

2. If the wireless PC you want to add appears in the list, check its adjacent radio button and click **Add.**
   - If the PC is not displayed, make sure that it is configured correctly and click **Refresh**.
   - If no wireless PCs appear in the **Available Wireless Cards** access list, then you can manually enter the **Device Name** and **MAC Address** of the wireless PC in the appropriate fields and then click **Add.** (You can usually find the MAC address printed on the bottom of the wireless adapter.)

3. Repeat these steps for each additional device you want to add to the **Trusted Wireless Stations** list.

	**Note:** The wireless stations must be selected and added one at a time to the T**rusted Wireless Stations** list.

4. Click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WNAP210.

Chapter 4
Management

This chapter describes how to use the management and information features as well as the advanced wireless settings features of your ProSafe Wireless-N Access Point. These features can be found under the Management, Information and Advanced menus on the left navigation pane of the browser interface.

Changing the Password

	Note: Before changing the WNAP210 password, use the backup utility to save your configuration settings. If you forget your new password, you must reset the WNAP210 back to the factory defaults and use the default password. Consequently, you will have to restore any WNAP210 configuration settings you have made. The backup file can be used in this event.

The default password for the WNAP210 is **password.** NETGEAR recommends that you change this password to a more secure password.

To change the password:

1. Select **Change Password** under the **Management** menu on the left navigation pane. The **Change Password** screen will display.

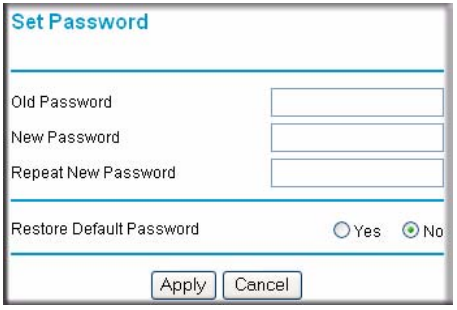

Figure 4-1

Figure 4-2

2. First enter the old password, in the **Old Password** field.
3. Then enter the new password twice in the **New Password** and **Repeat New Password** fields.
4. Click **Apply** to save your changes.

	**Note:** Be sure to write down the new password and store it in a safe place.

To restore the default password:

1. Check the **Restore Default Password** radio button.
2. Click **Apply.** The default password will be restored.

Upgrading the Wireless Access Point Firmware

The software of the ProSafe 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 ProSafe Access Point must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

To upgrade the firmware:

1. Go to the NETGEAR Web site at *http://kbserver.netgear.com/downloads_support.asp* to get new versions of the Access Point software.
2. Download, save and unzip (if the download file is a .zip file) the new software file.
3. From the main menu of the browser interface, click **Upgrade Firmware** under the **Management** menu on the left navigation panel. The **Upgrade Firmware** screen will display.

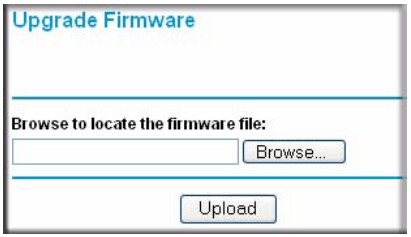

Figure 4-3

4. Click **Browse** and go to the location of the downloaded software upgrade file.
5. Click **Upload**.

	Warning: When uploading firmware to the wireless 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 WNAP210 inoperable.

In some cases, it may be necessary to reconfigure the wireless access point after upgrading.

Backing Up or Restoring Settings

You can back up your configuration settings of the ProSafe Access Point and restore the factory default settings. Once you have your wireless access point working properly, backing up the configured settings would be prudent should you have to perform a factory reset. When you backup the settings, they are saved as a file on your computer that you can access to restore the wireless access point's configured settings.

To backup/restore settings:

1. From the main menu of the browser interface, select **Backup/Restore Settings** from under the **Management** menu. The **Backup/Restore Settings** screen will display.

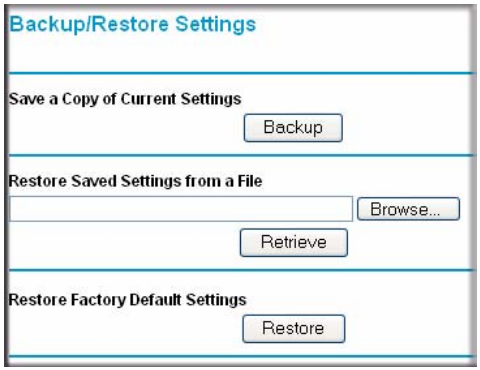

Figure 4-4

2. Select the task you want to perform:

   - To create a backup file of the current settings, click **Backup** under the **Save a Copy of Current Settings** heading.
     - If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click Backup.
     - If you have your browser set up to save downloaded files automatically, the file will be automatically saved to the download location
   - To restore settings from a backup file:
     - Click **Browse** under the **Restore Saved Settings from a File** heading. Locate and select the previously saved backup file (by default, netgear.cfg).
     - Click **Retrieve**. A window will appear with the message that the wireless access point has been successfully restored to its previous settings. The wireless access point will restart. This will take about one minute.

⚠	**Warning:** Do not try to go online, turn off the Access Point, shut down the computer or do anything else to the Access Point until it finishes restarting. When the Test light turns off, wait a few more seconds before doing anything with the Access Point.

     - Close the message window.
   - To erase the current settings and reset the wireless access point to the original factory default settings**:**
     - Click **Restore.** The default factory settings will be restored.

– A list of the factory default settings can be found in Appendix A, “Default Settings and Technical Specifications”.

	**Warning:** Do not try to go online, turn off the Access Point, shut down the computer or do anything else to the Access Point until it finishes restarting. When the Test light turns off, wait a few more seconds before doing anything with the Access Point.

Rebooting the ProSafe Access Point

You can reboot the wireless access point from the browser interface or by using the reset button on the rear panel.

To reboot the wireless access point from the user interface:

1. From the main menu of the browser interface, click **Reboot AP** under the **Management** menu on the left navigation pane. The **Reboot AP** screen will display..

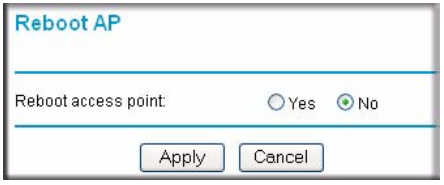

Figure 4-5

2. Select the **Yes** radio button, and then click **Apply**.

Viewing the Available Wireless Station List

The Available Wireless Station List contains a table of all IP devices associated with this wireless access point network defined by its Wireless Network Name (SSID).

To view the list of available wireless stations:

1. From the main menu of the browser interface, select **Available Wireless Station List** under the **Information** menu of the left navigation pane. The **Available Wireless Station List** will display.

2. Click **Refresh** to update the list and force the wireless access point to look for associated devices.

Figure 4-6

- 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).
- If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices.

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This extends the reach of the wireless network and lets users roam from one access point to another which provides seamless network connectivity. Under these circumstances, be aware that only the stations associated with this wireless access point will be presented in the Available Wireless Station List.

Viewing the Statistics

The Statics screen displays both wired and wireless interface network traffic.

To display statics for the wireless access point:

1. Select **Statistics** under the **Information** menu on the left information pane. The **Statistics** screen will display.

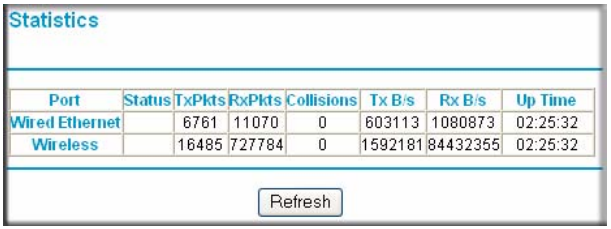

Figure 4-7

- The **Wired Ethernet** section of the table displays traffic statistics for the wired Ethernet interface.
- The **Wireless** section displays traffic statistics for the wireless interface.

2. Click **Refresh** to update the current statistics.

Configuring the Advanced Wireless Settings

We recommend that the Advanced Wireless Settings should be modified only by an administrator very familiar with the ramifications of changing the Wireless LAN parameters. If set incorrectly, they can adversely affect the performance or connectivity of your wireless access point. The default settings should be adequate in most situations. Following is a description of each of the Wireless LAN Parameters.

- **WMM Support.** Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both the application and the client running that application must be WMM-enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

  The default setting is Enabled.

- **RTS Threshold.** The Request to Send Threshold packet size determines if the wireless access point 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 value 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 value is 2346

- **Beacon Interval.** The Beacon Interval specifies the interval of time between 20ms and 1000ms for each beacon transmission.

  The default value is 100 ms.

- **DTIM Interval.** The Delivery Traffic Indication Message Interval specifies the data beacon rate between 1 and 255.

  The default value 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. The Auto setting will automatically handle both long and short preamble.

  The default setting is Auto.

The Wireless Optimization Settings feature allows you to adapt the wireless performance depending on the type of wireless clients that will be used in your network. The available settings are:

- **11Next Max Speed.** This setting yields the best Wireless N performance when only 802.11n clients are present. This is the default setting.
- **11b/g/Next Mixed Mode.** This setting yields the best overall performance when a mixture of 802.11b, 802.11g, and 802.11n clients are present.

To modify the Advanced Wireless Settings:

1. Select **Wireless Settings** under the **Advanced** menu on the left navigation pane of the user interface. The **Advanced Wireless Settings** screen will display.

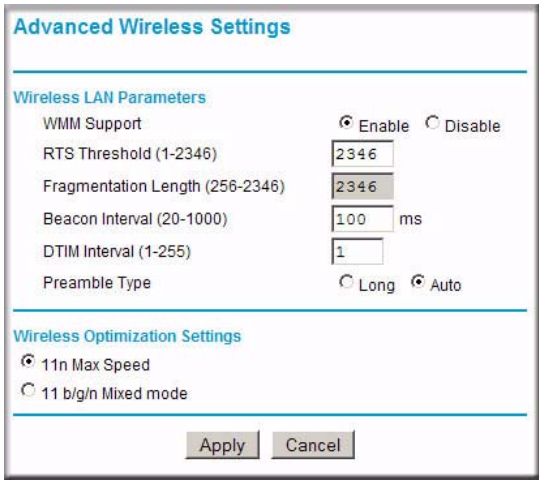

Figure 4-8

2. Make the changes to the Wireless LAN Settings based on the field descriptions outlined above.
3. Click **Apply** for your changes to take effect.

Configuring the RADIUS Server Settings

RADIUS (Remote Authentication Dial In User Service) is a protocol for managing Authentication, Authorization and Accounting (AAA) of multiple users in a network. A RADIUS server stores a database of user information, and can validate a user at the request of a gateway device in the network when a user requests access to network resources. The wireless access point can relay login information from wireless clients to an external RADIUS server for AAA services. In an environment with many users, using a RADIUS server allows centralized control for individual users, providing better network security than using a single preshared key for all users.

Configure the RADIUS Server Settings menu with the parameters described in Table 4-1:

Table 4-1. RADIUS Server Settings Fields

Field		Description
Primary and Secondary Authentication Servers		The Authentication RADIUS Server provides authentication and access control. The primary server is mandatory. A secondary server, which will be used if the primary server fails, is optional.
	IP Address	The IP address of the authentication server. If no server is present, enter 0.0.0.0.
	Port Number	The port number used for communication to the authentication server. The default port number for an authentication server is 1812.
	Shared Secret	The shared secret to establish a client connection to the Radius server, as entered on the server itself.
Re-authentication Time		The time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server. The default interval is 3600 seconds.
Update Global Key		Enable this option to have the Global Key changed according to the time interval specified. If enabled, enter the desired time interval. The default is enable, and the default interval is 3600 Seconds
Update if any station disassociates		Enable this option to refresh the Global Key whenever any station disassociates with the wireless access point. The default is disable.
Primary and Secondary Accounting Servers		The Accounting RADIUS Server provides accounting services. The same RADIUS server may be used for both authentication and accounting, but the port numbers for authentication and accounting must be different. The accounting servers are optional.
	IP Address	The IP address of the accounting server. If no server is present, enter 0.0.0.0.
	Port Number	The port number used for communication to the accounting server. The default port number for an accounting server is 1813.
	Shared Secret	The shared secret to establish a client connection to the RADIUS server, as entered on the server itself.

To configure the RADIUS Server Settings:

1. Select **Radius Server Settings** under the **Security** menu on the left navigation pane of the user interface. The **Radius Server Settings** screen will display.

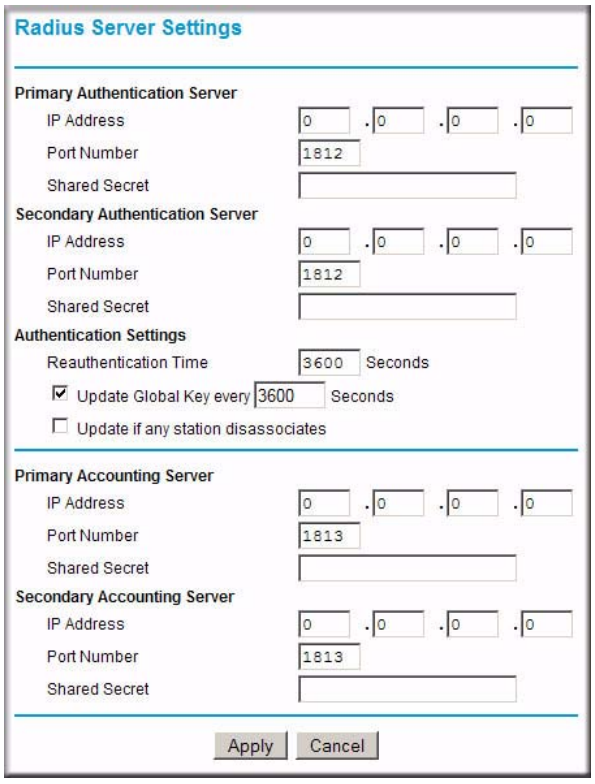

Figure 4-9

2. Make the changes to the RADIUS Server Settings based on the field descriptions outlined above.
3. Click **Apply** for your changes to take effect.

Chapter 5
Advanced Wireless Bridging

This chapter describes how to configure the advanced features of your WNAP210 to one of six Access Point Modes or in Wireless Bridge and Repeater Mode.These features can be found under the Advanced heading in the main menu on the Wireless Settings Wireless Bridging screens.

The ProSafe Wireless-N Access Point lets you build large wireless networks. Examples of wireless bridging configurations are:

- **Access Point**. Standard Access Point mode (default mode). Operates as a standard 802.11b/g or 802.11b//g/n Access Point. In this mode, the WNAP210 will communicate only with wireless clients.
- **Wireless multi-point bridging**. Acts as the “master” and communicates with up to six bridge-mode wireless access points. All of the other wireless access points communicate through the WNAP210 when theWNAP210 is in this mode.
- **Repeater with Wireless Client Association**. Acts as a “repeater” and forwards all traffic to a remote access point.

Configuring Wireless Multi-Point Bridging

In this mode, the WNAP210 will communicate with up to six bridge-mode wireless access points by entering the MAC address (physical address) of each of the bridge-mode APs in the fields provided. In addition, if you check the Enable Wireless Client Association checkbox, wireless clients will also be serviced by this access point. Each wireless access point you enter will be listed in the Wireless Remote Access Point List.

To configure wireless Multi-point Bridging:

1. Open a web browser and log into the WNAP210 using the addressing scheme you have set up

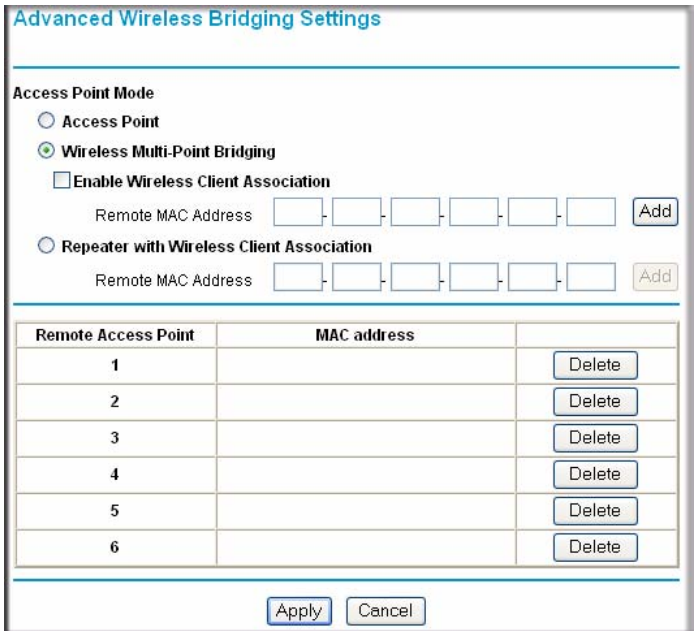

Figure 5-1

2. Under **Advanced** on the main menu, click **Wireless Bridging.** The **Advanced Wireless Bridging** screen will display showing the default settings for the wireless access point.
3. Select the **Wireless Multi-Point Bridging** radio button to enable multi-point bridging.
4. Enter the MAC address of the first wireless access point and click **Add.** The AP's MAC address and connection information will appear in the **Wireless Accept Point List.**

   You can add wireless access points to the list for a total of six. (These wireless access points must be configured for Multi-Point Bridging.)
5. Check the **Enable Wireless Client Association** radio box to allow wireless clients access to this wireless access point.
6. Click **Apply** to save your changes.

To delete a remote AP from the list, click **Delete** adjacent to the AP's MAC address in the Wireless Remote Access Point List.

The following figure illustrates a multi-point bridge setup over three LAN segments.

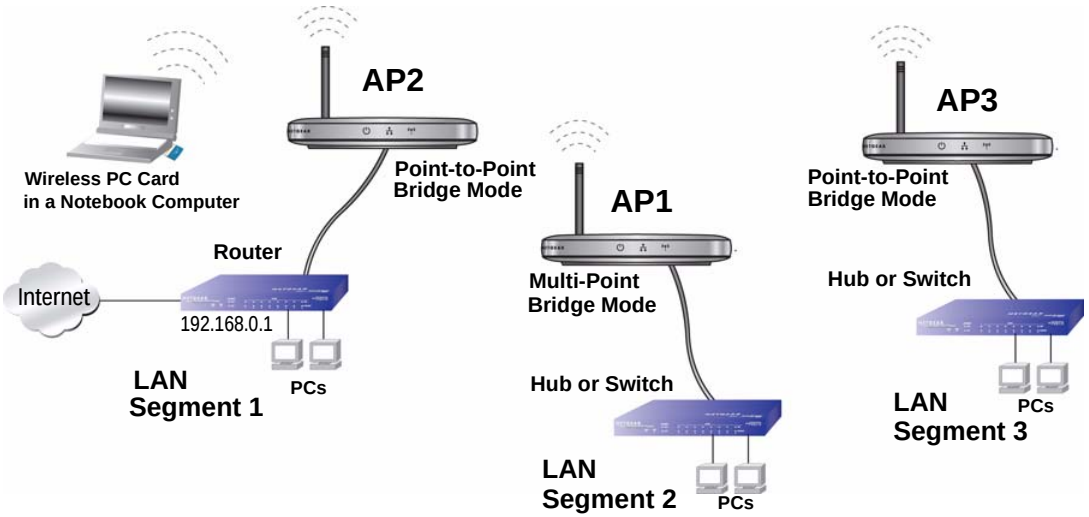

Figure 5-2

To configure wireless access points in a multi-point configuration:

1. Set the Operating Mode of the three ProSafe Access Points as follows:

- Configure AP2 on LAN Segment 1 in Point-to-Point Bridge Mode. Enable Wireless Client Association and add the Remote MAC Address of AP1 on LAN Segment 2.
- Because it is in the central location, configure AP1 on LAN Segment 2 in Multi-Point Bridging mode. Enable Wireless Client Association and add the MAC addresses of the adjacent Point-to-Point APs (AP2 and AP3).
- Configure AP3 on LAN 3 in Point-to-Point Bridge mode. Enable Wireless Client Association and add the Remote MAC Address of AP1 on LAN Segment 2.

2. Verify the following parameters for all three wireless access points:

- That the LAN network configuration of each of the ProSafe Access Points is configured to operate in the same LAN network address range as the other LAN devices (routers, hubs and switches).
- That only one wireless access point is configured in Multi-Point Bridging mode, and that all the others are in Point-to-Point Bridge mode.
- That all APs are be on the same LAN. That is, all the wireless access point LAN IP addresses are in the same network.

- If using DHCP, all wireless 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.
- That all wireless access points are using the same SSID, Channel, WEP authentication mode, if any, and encryption (WPA is not available in bridge modes).
- That each Point-to-Point AP has the Multi-Point AP MAC address in its Remote AP MAC address table.
- If Access Control has been enabled on the APs, verify that the Wireless Cards table (MAC Address List) for each AP is complete and accurate.

3. Verify connectivity across the LANs.

- If you checked the Enable Wireless Client Association radio box on each AP, wireless clients will be able to use the AP.
- A computer on any LAN segment should then 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.
- If Access Control Lists are enabled on the APs, only computers in the access control list will be able to use the AP.

Note: You can extend multi-point bridging by adding a total of six WNAP210 APs configured in Point-to-Point mode to connect additional wireless LAN segments.

Configuring Repeater with Wireless Client Association

In this mode, the WNAP210 will operate as a Repeater only, and send all traffic to the remote wireless access point. You must enter the MAC address (physical address) of the remote wireless access point.

To configure the WNAP210 in wireless repeater mode:

1. Open a web browser and log into the WNAP210 using the addressing scheme you have set up.

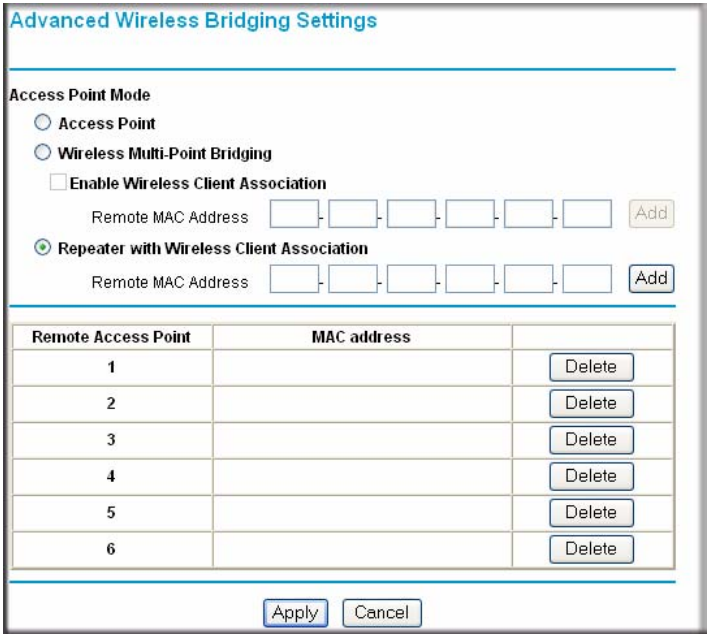

Figure 5-3

2. Under **Advanced** on the main menu, click **Wireless Bridging.** The **Wireless Bridging** screen will display showing the default settings for the wireless access point.
3. Select the **Repeater with Wireless Client Association** radio button to enable Repeater Mode.
4. Enter the MAC address of the remote wireless access point and click **Add.** The AP's MAC address and connection information will appear in the **Wireless Remote Access Point List.**
5. Click **Apply** to save your changes.

The following drawing illustrates two wireless access points daisy-chained together in wireless repeater mode

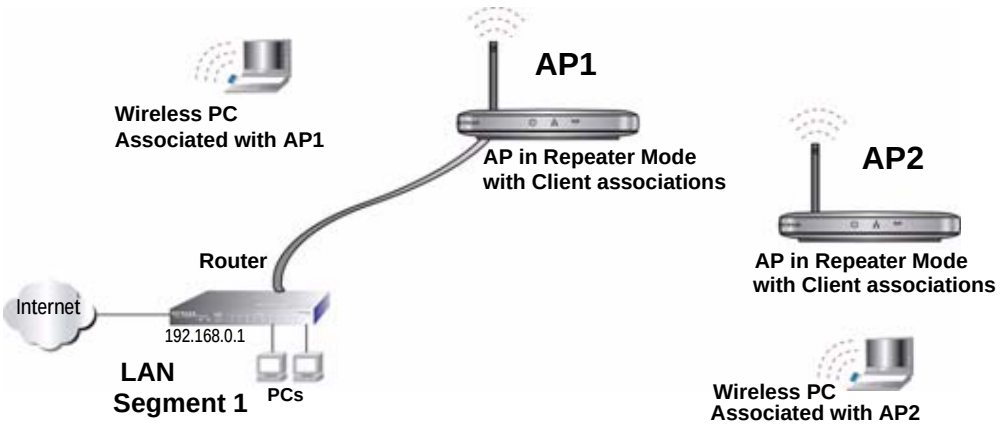

Figure 5-4

To configure a LAN segment utilizing the WNAP210 in Repeater Mode:

1. Configure the Operating Mode of the ProSafe Access Points.

- Configure AP1 on LAN Segment 1 in Repeater mode with the Remote MAC Address of the “downstream” remote AP (AP2).
- Configure AP2 in Repeater mode with the MAC address of the “upstream” AP (AP1).

2. Verify the following parameters for all access points:

- That the ProSafe Access Points are configured to operate in the same LAN network address range as the LAN devices.
- That all APs are on the same LAN. That is, all AP LAN IP addresses must be in the same network.
- If using DHCP, that all ProSafe Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address section of the **IP Settings** screen.
- That all ProSafe 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.

Chapter 6
Troubleshooting

This chapter provides information for troubleshooting issues with your ProSafe Wireless-N Access Point. Following each problem description, instructions are provided to assist you in diagnosing and solving the problem.

Following are some tips for correcting simple problems that could occur.

No lights are lit on the access point.

The access point has no power.

- Make sure the power cord is connected to the access point and plugged in to a working power outlet or power strip.
- Make sure .you are using the correct NETGEAR power adapter supplied with your access point or if you are using PoE, check to make sure the switch powering the access point is working properly.

The Ethernet light is not lit.

There is a hardware connection problem.

- Make sure the cable connectors are securely plugged in at the wireless access point and the network device (hub, switch, or router).
- Make sure the connected device is turned on.

The WLAN light is not lit.

The wireless access point build-it antennas are not functioning properly.

- Check the “Turn Radio On” radio button setting on the **Wireless Settings** screen under the **Setup** menu. It must be turned on (checked).

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Contact NETGEAR if the WLAN light remains off.

I cannot configure the access point from a browser.

Check these items:

- The WNAP210 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is blinking green to verify that the Ethernet connection is OK.
- If you are using the NetBIOS name of the WNAP210 to connect (DHCP Client is enabled), ensure that your PC and the WNAP210 are on the same network segment or that there is a WINS server on your network. Using the default NetBIOS name: **netgearxxxxxx,** where **xxxxxx** is the last 6 digits of the wireless access point MAC address; or, if you have modified the name, make sure you have input it correctly. (The name may be up to 15 characters long.)
- If DHCP is not enabled, make sure you are using the correct LAN IP Address to access the wireless access point, and that you are on the same network segment.
- If DHCP is enabled, and you cannot connect using the default NetBIOS name, configure your DHCP server (either built into the router or a separate server) with a reserve IP (based on the wireless access point's MAC address). You can then use it to create a fixed IP for the wireless access point.
- If you have not yet deployed the wireless access point, and it is connected to your PC via an Ethernet cable, make sure the connection is secure, and that you have configured your PC with a static IP in the same subnet as the LAN IP of wireless access point. The default static IP address to use for your PC is 192.168.0.210; the default wireless access point LAN IP is 192.168.0.236; and the default Subnet Mask is 255.255.255.0.

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 on the Network Properties is set to “Obtain an IP address automatically.”
- The wireless access point’s default values may not work with your network. Check the wireless access point’s default configuration against the configuration of other devices in your network.
- For full instructions on changing the wireless access point’s default values, see Chapter 2, “Installation and Configuration” and Chapter 3, “Wireless Security Settings”.

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 computers work. If they do, ensure that your computer’s IP Address, Subnet Mask and Default Gateway settings are correct. If using a DNS Server, check the Primary and Secondary DNS Server Addresses.
- If the computers are configured correctly, but still not working, ensure that the WNAP210 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 WNAP210 is configured correctly, check your Internet connection (DSL/Cable modem, etc.) to make sure that it is working.
- Try again.
- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Using the Reset Button to Restore Factory Default Settings

The reset button on the rear panel of the WNAP210 has two functions:

- **Reboot:** When pressed and released quickly, the WNAP210 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. These settings are shown in Appendix A, "Default Settings and Technical Specifications".

To clear all data and restore the factory default values:

1. Power off the WNAP210 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 five seconds—or until the power light changes from blinking green to amber.
3. Release the reset button.

The factory default configuration has now been restored, and the WNAP210 is ready for use.

Appendix A
Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the ProSafe Wireless-N Access Point.

Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the Power LED changes from blinking green to solid amber). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. Access Point Default Configuration Settings

Feature		Description
AP Login		
	User Login URL	192.168.0.236 or netgearxxxxxx"; where xxxxxx is the last 6 hexadecimal digits of the WN802T MAC address.
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Connection		
	Access Point Name	netgearxxxxxx where xxxxxx are the last 6 digits of the wireless access point MAC address.
	Ethernet MAC Address	See rear label.
	Access Point Mode	On
	Port Speed	10/100/1000 Mbps
Local Network (LAN)		

Table A-1. Access Point Default Configuration Settings

Feature		Description
	Lan IP	192.168.0.236
	Subnet Mask	255.255.255.0
	Gateway Address	192.168.0.1
	DHCP Client	Disabled
	Time Zone	GMT-08:00
	Time Zone Adjusted for Daylight Saving Time	Disabled
Wireless		
	Operating Mode	11b/g/Next (20/40 MHz)
	Wireless Communication	Enabled
	Wireless Network Name (SSID)	NETGEAR
	Broadcast Network Name SSID	Enabled
	Security	Disabled
	Transmission Speed	Auto[a]
	Country/Region	United States (in North America; otherwise, varies by region)
	Channel/Radio Frequency	6/2.43 GHz (until the region is selected)
	Output Power	Full
	Wireless Card Access List	All wireless stations allowed

a. Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Table A-2. WN802T Technical Specifications

Parameter	ProSafe Wireless-N Access Point
802.11Next Data Rates	7.2, 14.4, 21.7, 28.9,43.3, 57.8, 65, 72.2, 87.7, 115.6, 130 & 144.4 Mbps (20Hz) 15, 30, 45, 60, 90, 120. 135. 150, 180, 240, 270 & 300 Mbps (40Hz)
802.11b/g Data Rates	1, 2, 5.5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable)
802.11b/g/Next Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.457 ~ 2.462 GHz (Spain) 2.412 ~ 2.484 GHz (Japan) 2.457 ~ 2.472 GHz (France) 2.412 ~ 2.472 GHz (Europe ETSI)
802.11b/g/Next Encryption	40-bits (also called 64-bits), 128-bits WEP data encryption; TKIP (WPA-PSK) and AES (WPA2-PSK)
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
Power Adapter	12V DC, 1.5 A Switching Power Supply
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

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*