

# NETGEAR WNDAP330 ProSafe 802.11n Dual Band Wireless Access Point Reference Manual



## NETGEAR®

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

202-10361-01  
May 2008  
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](mailto: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 802.11n Dual Band Wireless Access Point WNDAP330 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 das ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 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]	<i>NETGEAR Inc.</i> tímto prohlašuje, že tento Radiolan je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES..
Dansk [Danish]	Undertegnede <i>NETGEAR Inc.</i> erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt <i>NETGEAR Inc.</i> , 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 <i>NETGEAR Inc.</i> seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, <i>NETGEAR Inc.</i> , 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 <i>NETGEAR Inc.</i> 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 <i>NETGEAR Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente <i>NETGEAR Inc.</i> 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 <i>NETGEAR Inc.</i> dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>NETGEAR Inc.</i> deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>NETGEAR Inc.</i> deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart <i>NETGEAR Inc.</i> dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, <i>NETGEAR Inc.</i> , jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, <i>NETGEAR Inc.</i> nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym <i>NETGEAR Inc.</i> oświadczam, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	<i>NETGEAR Inc.</i> declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	<i>NETGEAR Inc.</i> izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>NETGEAR Inc.</i> týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	<i>NETGEAR Inc.</i> vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar <i>NETGEAR Inc.</i> 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 <i>NETGEAR Inc.</i> yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	<i>NETGEAR Inc.</i> erklærer herved at utstyret <i>Radiolan</i> 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 WNDAP330 ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 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 802.11n Dual Band Wireless Access Point



Tested to Comply  
with FCC Standards  
FOR HOME OR OFFICE USE  
PY306100037

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 802.11n Dual Band Wireless Access Point WNDAP330) 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.

## Product and Publication Details

<b>Model Number:</b>	WNDAP330
<b>Publication Date:</b>	May 2008
<b>Product Family:</b>	Wireless Access Point
<b>Product Name:</b>	ProSafe 802.11n Dual Band Wireless Access Point WNDAP330
<b>Home or Business Product:</b>	Business
<b>Language:</b>	English
<b>Publication Part Number:</b>	202-10361-01
<b>Publication Version Number:</b>	1.0

# Contents

## About This Manual

- Conventions, Formats, and Scope ..... xi
- How to Use This Manual .....xii
- How to Print This Manual .....xii
- Revision History .....xiii

## Chapter 1

### Introduction

- About the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 ..... 1-1
- Key Features and Standards ..... 1-2
  - Supported Standards and Conventions ..... 1-2
  - Key Features ..... 1-3
  - 802.11a/b/g/n Standards-based Wireless Networking ..... 1-4
  - Autosensing Ethernet Connections with Auto Uplink ..... 1-5
- Compatible and Related NETGEAR Products ..... 1-5
- System Requirements ..... 1-6
- What's In the Box? ..... 1-6
- Hardware Description ..... 1-7
  - Front Panel ..... 1-8
  - Rear Panel ..... 1-10

## Chapter 2

### Basic Installation and Configuration

- Wireless Equipment Placement and Range Guidelines .....2-1
- Understanding WNDAP330 Wireless Security Options .....2-2
- Installing the WNDAP330 Wireless Access Point .....2-4
  - Setting up the WNDAP330 Wireless Access Point .....2-4
  - Configuring LAN and Wireless Access .....2-4
    - Configuring Time Settings .....2-8
    - Configuring Wireless Access .....2-10
  - Deploying the WNDAP330 Wireless Access Point .....2-10

Verifying Wireless Connectivity .....	2-11
Logging In Using the Default IP Address .....	2-12
Setting Basic IP Options .....	2-13
Wireless Settings .....	2-14
Configuring 802.11b/g/n Wireless Settings .....	2-14
Configuring 802.11a/n Wireless Settings .....	2-17
Configuring QoS Settings .....	2-21
Setting Up and Testing Basic Wireless Connectivity .....	2-22
Understanding Security Profiles .....	2-23
SSID and WEP/WPA Settings Setup Form .....	2-28
802.11b/g/n Configuration .....	2-28
802.11a/n Configuration .....	2-29
Configuring the RADIUS Server Settings .....	2-30
Setting up a Security Profile .....	2-32
Configuring WEP .....	2-34
Configuring WPA with RADIUS .....	2-36
Configuring WPA2 with RADIUS .....	2-37
Configuring WPA and WPA2 with RADIUS .....	2-38
Configuring WPA-PSK .....	2-39
Configuring WPA2-PSK .....	2-40
Configuring WPA-PSK and WPA2-PSK .....	2-41
Restricting Wireless Access by MAC Address .....	2-42

### **Chapter 3**

#### **Management**

Remote Management .....	3-1
Remote Console .....	3-2
Using the Secure Telnet Interface .....	3-3
CLI Commands .....	3-4
Upgrading the Wireless Access Point Software .....	3-5
Configuration File Management .....	3-7
Saving the Configuration .....	3-8
Restoring the Configuration .....	3-9
Restoring the WNDAP330 to the Factory Default Settings .....	3-9
Changing the Administrator Password .....	3-10
Enabling the SysLog Server .....	3-11



Using Activity Log Information .....	3-12
Viewing General Summary Information .....	3-13
Viewing Network Traffic Statistics .....	3-15
Viewing Available Wireless Station Statistics .....	3-17
Enabling Rogue AP Detection .....	3-18
Importing Rogue AP List from a File .....	3-20
Viewing Rogue AP Statistics .....	3-21

## **Chapter 4**

### **Advanced Configuration**

IP Settings for Wireless Clients .....	4-1
Hotspot Settings .....	4-4
Configuring Advanced Wireless Settings .....	4-5
Configuring 802.11b/g/n Advanced Wireless Settings .....	4-5
Configuring 802.11a/n Advanced Wireless Settings .....	4-7
Configuring Advanced QoS Settings .....	4-9
Enabling Wireless Bridging and Repeating .....	4-11
Configuring a WNDAP330 as a Point-to-Point Bridge .....	4-14
Configuring a Point-to-Multi-Point Wireless Bridge .....	4-16
Configuring the WNDAP330 as a Wireless Repeater .....	4-18

## **Chapter 5**

### **Troubleshooting and Debugging**

No lights are lit on the wireless access point. ....	5-1
The Wireless LAN activity light does not light up. ....	5-2
The LAN light is not lit. ....	5-2
I cannot access the Internet or the LAN with a wireless capable computer. ....	5-2
I cannot connect to the WNDAP330 to configure it. ....	5-3
When I enter a URL or IP address I get a timeout error. ....	5-3
Using the Reset Button to Restore Factory Default Settings .....	5-4

## **Appendix A**

### **Default Settings and Technical Specifications**

Factory Default Settings .....	A-1
Technical Specifications .....	A-3

**Appendix B**  
**Related Documents**

**Appendix C**  
**Command Line Reference**

Command Sets .....	C-1
--------------------	-----

**Index**

# About This Manual

The *NETGEAR® ProSafe™ 802.11n Dual Band Wireless Access Point WNDAP330 Reference Manual* describes how to install, configure and troubleshoot the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. 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::

<i>Italic</i>	Emphasis, books, CDs, file and server names, extensions
<b>Bold</b>	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<a href="#"><i>italic</i></a>	URL links

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

	<b>Note:</b> This format is used to highlight information of importance or special interest.
---	--

	<b>Tip:</b> This format is used to highlight a procedure that will save time or resources.
---	--

	<b>Warning:</b> 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 Dual Band Wireless Access Point WNDAP330
Manual Publication Date	May 2008

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








**Note:** Product updates are available on the NETGEAR, Inc. website at <http://kbserver.netgear.com/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
202-10361-01	v1.0	May 2008	Product update: New firmware and new user Interface



# Chapter 1

## Introduction

This chapter describes some of the key features of the NETGEAR ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. 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 WNDAP330 ([“Hardware Description” on page 1-7](#)).

### About the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330

---

The ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 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 WNDAP330 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 802.11n Dual Band Wireless Access Point WNDAP330 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 802.11n Dual Band Wireless Access Point WNDAP330 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WNDAP330 Wireless 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 802.11n Dual Band Wireless Access Point WNDAP330 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

## Key Features and Standards

---

The WNDAP330 Wireless 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 a/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 WNDAP330 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 WNDAP330 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 WNDAP330 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 WNDAP330 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, WNDAP330 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 are 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 WNDAP330 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 WNDAP330 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 WNDAP330 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 802.11n Dual Band Wireless Access Point WNDAP330 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 WNDAP330 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 WNDAP330 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 WNDAP330 Wireless 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 WNDAP330, 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 100-240 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
- 802.11a/b/g/n or 802.11a/b/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 802.11n Dual Band Wireless Access Point WNDAP330
- Two Reverse SMA 5dbi dual band dipole antenna and one reverse SMA 3dbi dual band patch antenna.
- Power adapter and cord (12 V dc, 1.5 A)
- Straight-through Category 5 Ethernet cable
- NETGEAR WNDAP330 802.11a/b/g/n Dual Band Wireless Access Point Installation Guide
- *Resource CD* which includes this manual.
- Support Registration card

Contact your reseller or customer support in your area if there are any missing or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WNDAP330 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 WNDAP330.

## Front Panel

The WNDAP330 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	PWR		Power Indicator
		Off	No power.
		On	Power is on.
2	TEST		Self Test Indicator
		Blink	Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off.

**Table 1-1. Front Panel LED Indicators (continued)**

Item	LED		DESCRIPTION
<b>3</b>	<b>100</b>		Ethernet LAN Speed Indicator
		Off	Indicates 10 Mbps or no link detected.
		Yellow	Indicates 100 Mbps link detected.
		Green	Indicates 1000 Mbps link detected.
<b>4</b>	<b>LINK/ACT LAN</b>		Ethernet LAN Link Activity Indicator
		Off	Indicates no Ethernet link detected.
		Blink (Green)	Indicates data traffic on the 100Mbps Ethernet LAN.
<b>5</b>	<b>802.11na WLAN</b>		Wireless LAN Link Activity Indicator (5 GHz)
		Off	Indicates WLAN 802.11n/a (5GHz) mode is disabled.
		Blink (Green)	Indicates Wireless data traffic in 5GHz modes.
<b>6</b>	<b>802.11ng WLAN</b>		Wireless LAN Link Activity Indicator (5 GHz)
		Off	Indicates WLAN 802.11b/g (5GHz) mode is disabled.
		Blink (Green)	Indicates Wireless data traffic in 2.4GHz modes.

## Rear Panel



**Figure 1-2**

The WNDAP330 rear panel functions are described below:

1. Left, Middle, and Right Detachable Antenna

The WNDAP330 provides three detachable antennas (two dipole and one patch).

2. Restore to Factory Defaults Button

The restore to default button located between the Ethernet RJ-45 connector and the power socket restores the WNDAP330 to the factory default settings.

3. Serial Console Port

Male DB-9 serial port for serial DTE connections.



4. RJ-45 Ethernet Port

Use the WNDAP330 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or POE switch.

5. Power Socket

This socket connects to the WNDAP330 12V 1.5A power adapter.



## Chapter 2

# Basic Installation and Configuration

This chapter describes how to set up your ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b/g/n or 802.11a/n wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.



**Note:** Indoors, computers can connect over 802.11b/g/n or 802.11a/g/n 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 WNDAP330 Wireless Access Point provides highly effective security features which are covered in detail in [“Understanding Security Profiles” on page 2-23](#). 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 WNDAP330 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/n or 802.11a/n 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 WNDAP330. 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.

Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.

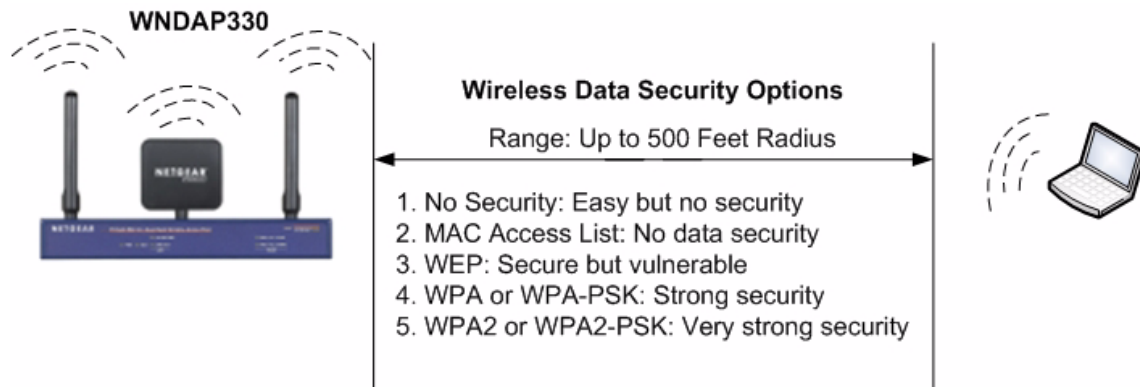
If you are using multiple access points for 11b/bg/ng, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11). For 11a/na, the 6 Channel spacing is not needed.

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.

## Understanding WNDAP330 Wireless Security Options

---

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WNDAP330 Wireless Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

**Figure 2-1**

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 WNDAP330. 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 open authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.



**Note:** WEP and TKIP provide only legacy rates of operation. So, AES is the recommended solution to use the 11n rates and speed.

## Installing the WNDAP330 Wireless Access Point

---

Before installing the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b/g/n or 802.11a/n 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 1-6](#).

## Setting up the WNDAP330 Wireless Access Point



**Tip:** Before mounting the WNDAP330 in a high location, first set up and test the WNDAP330 to verify wireless network connectivity.

To set up the WNDAP330 Wireless Access Point:

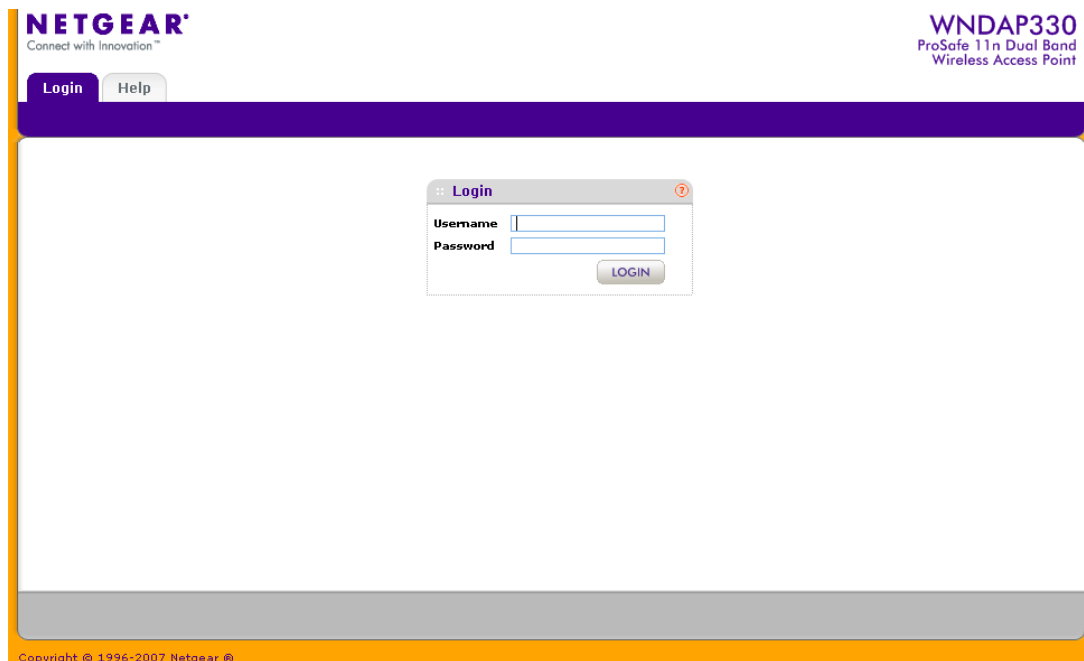
1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.
2. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.
3. Connect an Ethernet cable from the WNDAP330 to the computer.
4. Turn on your computer, connect the power adapter to the WNDAP330 and verify the following:
  - The PWR power light goes on.
  - The LAN light of the wireless access point is lit when connected to a powered on computer.
  - The WLAN LEDs should be blinking.

## Configuring LAN and Wireless Access

To configure the WNDAP330 Ethernet port for LAN access:

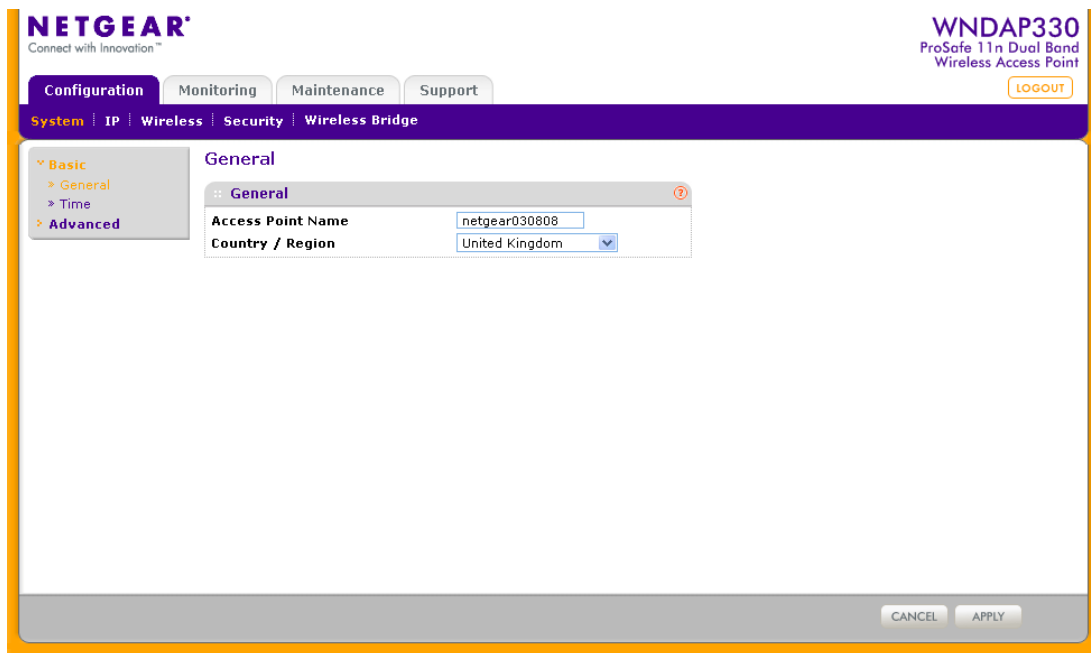
1. Connect to the WNDAP330 by opening your browser and entering **http://192.168.0.230** in the address field. The WNDAP330 login screen will appear.

2. Enter **admin** for the user name and **password** for the password, both in lower case letters as shown in [Figure 2-2](#).



**Figure 2-2**

3. Click **Login**. The main menu of the WNDAP330 will display as shown in [Figure 2-3](#).
  - When the wireless access point is connected to the Internet, under the Support tab, select Documentation to view the documentation for the wireless access point.
  - On the top-right of the screen, select Logout to exit the WNDAP330 setup screens. (You will automatically be logged out of the wireless access point after 5 minutes of no activity.)

**Figure 2-3**

4. Enter the **Access Point Name** of the WNDAP330.

This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of WNDAP330. The default is netgearxxxxxx, where xxxxxx represents the last 6 digits of the WNDAP330 MAC address. You may modify the default name with a unique name up to 16 characters long.

5. From the **Country/Region** pull-down menu, select the region where the WNDAP330 can be used (the default Country/Region is the United States).



**Note:** If your country or region is not listed, please check with Netgear Support.



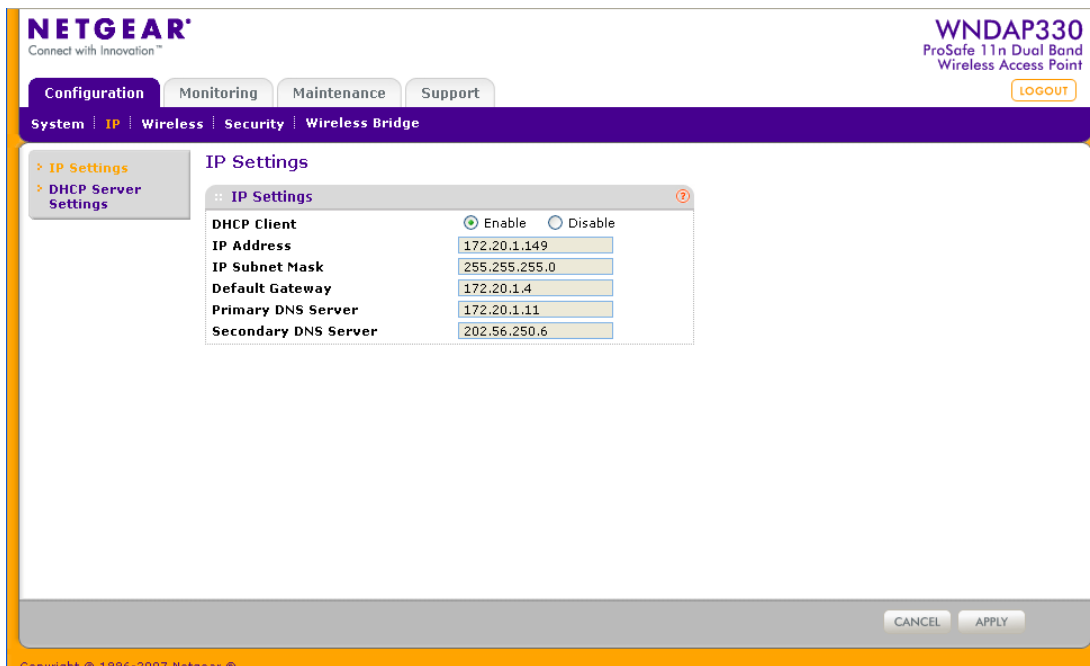
6. Select Time from the left-hand menu. The Time screen will display, as shown in [Figure 2-4](#).

The screenshot displays the Netgear WNDAP330 web interface. At the top, the Netgear logo and 'Connect with Innovation™' are on the left, and 'WNDAP330 ProSafe 11n Dual Band Wireless Access Point' with a 'LOGOUT' button is on the right. Below this is a navigation bar with tabs for 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. Under 'Configuration', there are sub-tabs for 'System', 'IP', 'Wireless', 'Security', and 'Wireless Bridge'. On the left side, a sidebar menu shows 'Basic' (selected), 'General', 'Time', and 'Advanced'. The main content area is titled 'Time' and contains a 'Time Settings' form. The form includes the following fields: 'Time Zone' (set to 'USA-Pacific'), 'Current Time' (displaying 'Mon Apr 21 01:50:12 PDT 2008'), 'NTP Client' (with 'Enable' selected and 'Disable' as an option), 'Use Custom NTP Server' (unchecked), and 'Hostname / IP Address' (set to 'time-b.netgear.com'). At the bottom right of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page reads 'Copyright © 1996-2007 Netgear ©'.

**Figure 2-4**

7. Enter the Time Settings for your area. See the online help or [“Configuring Time Settings” on page 2-8](#) for more information about how to configure the settings on this screen.

8. Select IP on the main menu. The IP Settings screen will display, as shown in [Figure 2-5](#).



**Figure 2-5**

9. Configure the IP Address settings appropriate for your network. The default values are suitable for most users and situations. (See the online help or [“Setting Basic IP Options” on page 2-13](#) for more information about how to configure the settings on this screen.
10. Click **Apply**.

## Configuring Time Settings

To configure your time settings:

1. Under the Configuration tab, select System from the main menu, select Basic, and then select Time. The Time screen will display, as shown in [Figure 2-6](#).

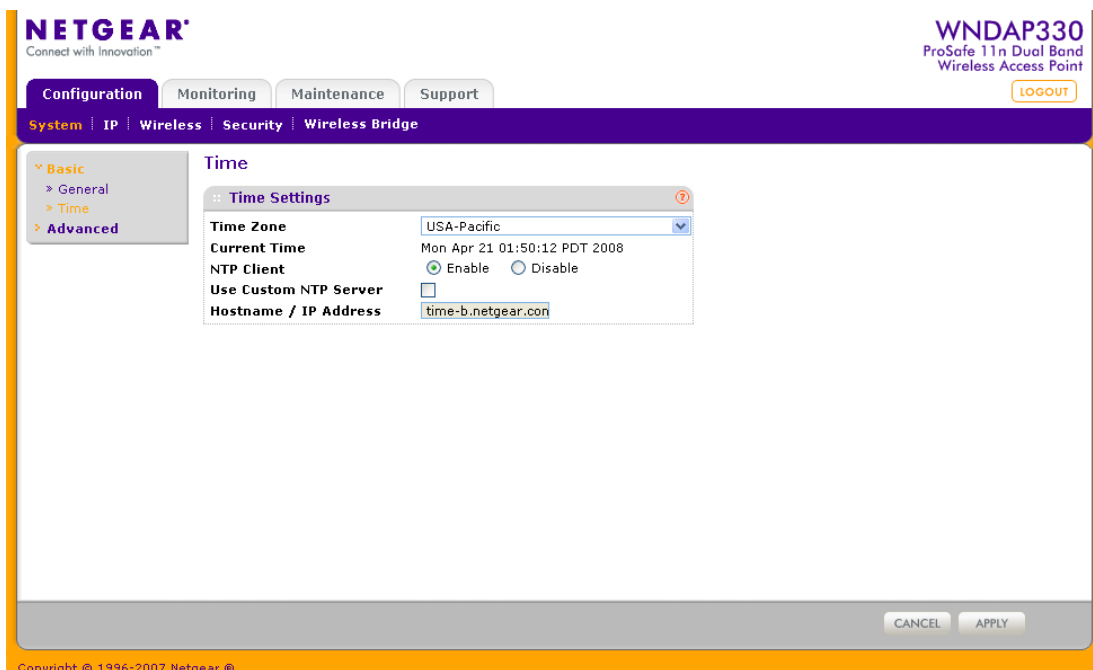



Figure 2-6

2. Configure the following information:

- **Time Zone.** 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 USA-Pacific.
- **NTP Client.** Enable NTP Client to synchronize the time of the access point with an NTP Server. The Default is Enabled.

	<p><b>Note:</b> You must have an Internet connection to get the current time.</p>
---	---

- **Use Custom NTP Server.** Check the option if you have a custom NTP server. The default is Disabled.
- **Hostname / IP Address.** Enter the host name or the IP address of the custom NTP server. The default is time-b.netgear.com.

3. Click **Apply**.

## Configuring Wireless Access

To configure your wireless settings for 11b/g/n and 11a/n:

1. From the main menu under Configuration, select Wireless. The Wireless Settings screen will display, as shown in [Figure 2-7](#).
2. Enter the wireless settings for your area. See the online help or “[Wireless Settings](#)” on [page 2-14](#).
3. Click **Apply** to save your settings.

The figure shows two side-by-side screenshots of the Wireless Settings configuration interface. The left screen is for the 2.4GHz band (802.11b/bg/ng) and the right screen is for the 5GHz band (802.11a/na). Both screens have a 'Wireless Mode' section with 'Turn Radio On' checked. The 'Wireless Network Name (SSID)' is set to 'NETGEAR\_11g' on the left and 'NETGEAR\_11a' on the right. The 'Broadcast Wireless Network Name (SSID)' is set to 'Yes' on both. The 'Channel / Frequency' is set to 'Auto'. The 'MCS Index / Data Rate' is set to 'Best'. The 'Channel Width' is set to '20 MHz' on the left and 'Dynamic 20/40 MHz' on the right. The 'Guard Interval' is set to 'Auto'. The 'Output Power' is set to 'Full'.

**Figure 2-7**

When you have completed the setup steps, you can deploy the WNDAP330 in your network. If needed, you can now reconfigure the computer you used in step 1 (from the Static IP) back to its original TCP/IP settings.

## Deploying the WNDAP330 Wireless Access Point

To deploy the WNDAP330 Wireless Access Point:

1. Disconnect the WNDAP330 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. Lift the antenna on either side so that they are vertical.



**Note:** Refer to the antenna positioning and wireless mode configuration information in the [Advanced Configuration](#) chapter of the Reference Manual.

3. Connect an Ethernet cable from your WNDAP330 Wireless Access Point to a LAN port on your router, switch, or hub.



**Note:** By default, WNDAP330 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting. To connect to the WNDAP330 after the DHCP server on your network assigns it a new IP address, enter the wireless access point 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 default name is printed on the bottom label of the WNDAP330.

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

## Verifying Wireless Connectivity

Using a computer with an 802.11b/g/n or 802.11a/n wireless adapter with the correct wireless settings needed to connect to the WNDAP330 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Mozilla Firefox, Netscape, or Internet Explorer to browse the Internet, or check for file and printer access on your network.

The default SSID for the 802.11b/g/n is NETGEAR-11g; the default SSID for the 802.11a/n is NETGEAR-11a. The SSID of any wireless access adapters must match the SSID configured in the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. If they do not match, no wireless connection will be made.



**Note:** If you are unable to connect, see [Chapter 5, “Troubleshooting and Debugging.”](#)

## Logging In Using the Default IP Address

---

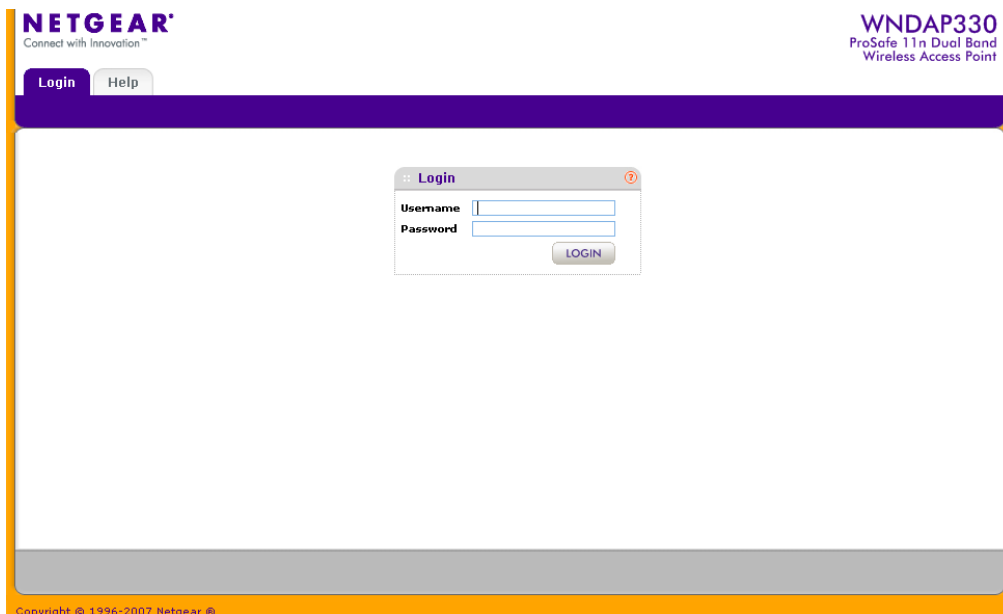
After you install the WNDAP330, log in to the wireless access point to configure the basic settings and the wireless settings. The WNDAP330 is set, by default, with the IP address of 192.168.0.230 with DHCP disabled.



**Note:** The computer you are using to connect to the WNDAP330 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

To log in using the default IP Address:

1. Open a Web browser such as Internet Explorer, Mozilla Firefox, or Netscape Navigator.
2. Connect to the WNDAP330 by entering its default address of **http://192.168.0.230** into your browser. The login screen will display. Enter **admin** for the user name and **password** for the password, both in lower case letters.



**Figure 2-8**

3. Click **Login**.

Your Web browser should automatically find the WNDAP330 Wireless Access Point and display the home screen.

## Setting Basic IP Options

The basic IP settings for your wireless access point are entered on this screen. Most of the default settings will work in most cases. However, if your wireless access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields.

To configure the basic IP settings of your wireless access point:

1. Under Configuration, select IP, and then IP Settings. The IP Settings screen will display as shown in [Figure 2-9](#) below.

The screenshot shows the Netgear WNDAP330 web interface. At the top, the Netgear logo and 'Connect with Innovation' tagline are on the left, and the device model 'WNDAP330 ProSafe 11n Dual Band Wireless Access Point' with a 'LOGOUT' button is on the right. Below the header is a navigation bar with tabs for 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. Under 'Configuration', there are sub-tabs for 'System', 'IP', 'Wireless', 'Security', and 'Wireless Bridge'. The 'IP' tab is selected, and the 'IP Settings' sub-tab is active. On the left side of the main content area, there is a sidebar with expandable sections: 'IP Settings' (expanded) and 'DHCP Server Settings'. The main content area displays the 'IP Settings' form. It includes a 'DHCP Client' section with 'Enable' (selected) and 'Disable' radio buttons. Below this are input fields for 'IP Address' (172.20.1.149), 'IP Subnet Mask' (255.255.255.0), 'Default Gateway' (172.20.1.4), 'Primary DNS Server' (172.20.1.11), and 'Secondary DNS Server' (202.56.250.6). At the bottom right of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page shows 'Copyright © 1996-2007 Netgear, Inc.'

Figure 2-9

2. Enter the IP Address fields of the WNDAP330.

- **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 WNDAP330 to your LAN.
- **IP Address.** Enter the IP Address of your wireless access point. The default IP address is 192.168.0.230. 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 WNDAP330 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 WNDAP330 will use this IP address as the secondary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.

3. Click **Apply** to save your basic IP settings.

## Wireless Settings

---

The following sections describe how to configure the wireless settings available in both the 802.11b/g/n and 802.11a/n modes.

### Configuring 802.11b/g/n Wireless Settings

To configure the wireless settings of your 802.11 b/g/n wireless access point:

1. From main menu under Configuration, select Wireless. The Wireless Settings screen of your 802.11 b/g/n wireless access point will display, as shown in [Figure 2-10](#) below.



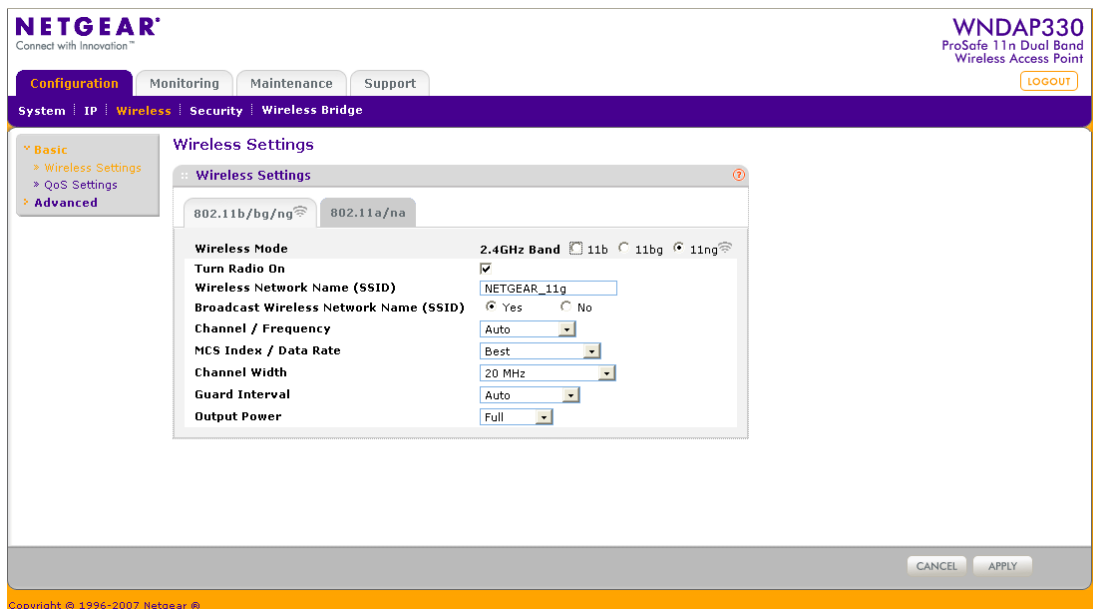


Figure 2-10

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

- **Wireless Mode.** Select the desired wireless operating mode. The default is 11ng. The options are:
  - **11b** – All 802.11b wireless stations can be used. (The 802.11g wireless stations can still be used if they can operate in 802.11b mode.)



**Note:** If you select this option and if other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen.

- **11bg** – Both 802.11b and 802.11g wireless stations can be supported.
- **11ng** – All 11b, 11g, and 11ng wireless stations can be used. This is the default. If you select this option, then two additional options, Channel Width and Guard Interval, are displayed.
- **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).** This is the name of your wireless network. It is set to the default name of NETGEAR\_11a for 802.11a/n and NETGEAR\_11g for 802.11b/g/n.
- **Broadcast 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. Default is enabled.
- **Channel/Frequency.** From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. The default is channel Auto.

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 need to experiment with different channels to see which is the best. Alternatively, you can select the Auto channel option for the AP to intelligently pick the channel with least interference. 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.”](#)). When selecting or changing channels, some points to bear in mind:

- Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available
- If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
- Wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **MCS Index/Data Rate.** From the pull-down menu, select the available transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary. (When Auto Channel is enabled in the 802.11ng mode, then the default Channel Width mode is 20MHz. In this case, you can not modify this parameter unless you change to a Static channel.) The possible data rates supported are:
  - **Data Rates for Channel Width=20MHz and Guard Interval=short (400ms):** Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps

- **Data Rates for Channel Width=20MHz and Guard Interval=long (800ms):** Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
- **Data Rates for Channel Width=40MHz and Guard Interval=short:** Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
- **Data Rates for Channel Width=40MHz and Guard Interval=long:** Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
- **Channel Width.** From the pull-down menu, select the desired channel width.
  - 20 MHz - This is the static, legacy mode. It gives the least throughput.
  - 40 MHz - This is the static, high-throughput mode. Legacy clients will not be able to connect in this mode.
  - 20/40 MHz - This is the dynamic, compatibility mode. Legacy clients can connect to 20 MHz and 11n clients can connect to 40 MHz.
- **Guard Interval.** From the pull-down menu, select the desired guard interval. The guard interval protects from interference from other transmissions. The default is Auto.
- **Output Power.** From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full. (The transmit power may vary depending on the local regulatory regulations).

3. Click **Apply** to save your 802.11b/g/n wireless settings.

## Configuring 802.11a/n Wireless Settings

To configure the 802.11.a wireless settings of your wireless access point:

- From the main menu under Configuration, select Wireless, and then select the **802.11a/na** tab. The Wireless Settings screen for your 11a/n access point will display as shown in Figure 2-11 below.

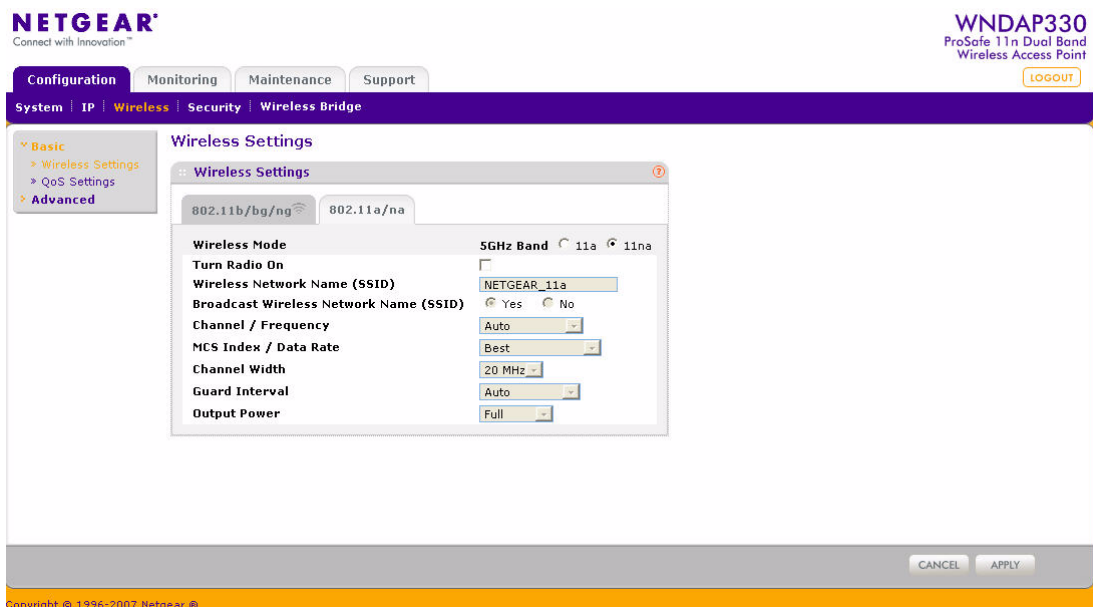


Figure 2-11

- Configure the Wireless LAN settings based on the following field descriptions:
  - Wireless Mode.** Select the desired wireless operating mode. Only 802.11a/n wireless stations can be selected from this menu. The default is 11na. The options are:
    - 11a** – All 802.11a wireless stations can be used.



**Note:** If you select this option and if other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen.

- 11na** – All 11a and 11na wireless stations can be used. This is the default.
- 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).** This is the name of your wireless network. It is set to the default name of NETGEAR\_11a for 802.11a/n and NETGEAR\_11g for 802.11b/g/n.
- **Broadcast 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. Default is enabled.
- **Channel/Frequency.** From the pull-down menu, select the channel you wish to use on your wireless LAN. The default is Auto. When you select Auto as the Channel Frequency, then the only available Channel Width is Dynamic 20/40MHz.

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.”](#)). When selecting or changing channels, some points to bear in mind:

- Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 13 channels are available.
  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 8 channels (for example, use channels 36 and 44, or 44 and 52).
  - In “Infrastructure” mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only occur when the various access points are using the same SSID.
- **MCS Index/Data Rate.** From the pull-down menu, select the transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary. The default is Best.



**Note:** Data rate is selected using MCS Index. The actual data rate is computed based on MCS Index, Channel Width, and Guard Interval. When Channel Width selected is Dynamic 20/40MHz or when Guard Interval is selected is Auto, then the data rate for a client depends on associated clients channel width and guard interval capabilities.

The possible data rates supported are:

- **Data Rates for Channel Width=20MHz and Guard Interval=short (400ms):** Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
- **Data Rates for Channel Width=20MHz and Guard Interval=long (800ms):** Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
- **Data Rates for Channel Width=40MHz and Guard Interval=short:** Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
- **Data Rates for Channel Width=40MHz and Guard Interval=long:** Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
- **Channel Width.** From the pull-down menu, select the desired channel width. To maximize performance, select high throughput channel width. The default is Dynamic 20/40 MHz.
- **Guard Interval.** From the pull-down menu, select the desired guard interval. The guard interval protects from interference from other transmissions. The default is Auto.

Following are data rates for different Channel Width and Guard Interval combinations:

- **Output Power.** From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full. (The transmit power may vary depending on the local regulatory regulations).
3. Click **Apply** to save your 802.11a/n wireless settings.

## Configuring QoS Settings

Wi-Fi Multimedia Support (WMM). Wireless Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the type of data.

Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.

To configure your wireless QoS settings for 11b/g/n and 11a/n:

1. Under the Configuration tab, select Wireless from the main menu, select Basic, and then select QoS Settings from the left-hand menu. The QoS Settings screen will display, as shown in [Figure 2-12](#).

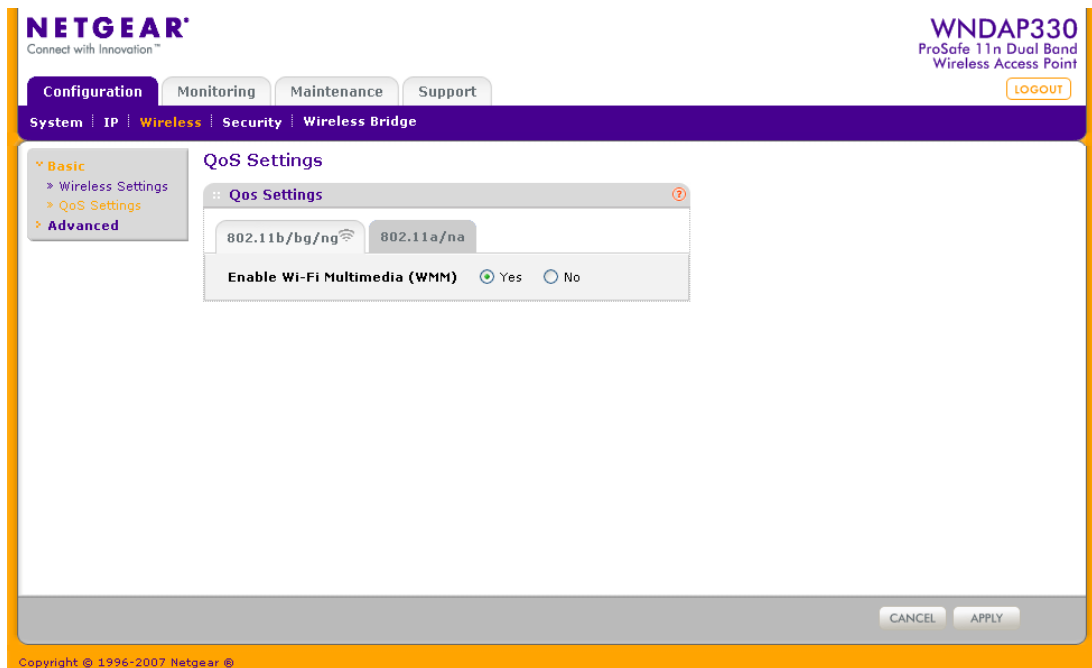


Figure 2-12

2. Wi-Fi Multimedia (WMM) is enabled (Yes) by default. Select the No radio button to disable WMM support.
3. Click **Apply** to save your settings

## Setting Up and Testing Basic Wireless Connectivity

---

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

1. From your Web browser, log in to the WNDAP330 using its default address of **http://192.168.0.235**. 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 Configuration, select System. Verify that the correct Country/Region in which the wireless interface will operate has been selected.
3. Click **Apply** to save any changes.
4. Under the Configuration tab, select Wireless from the main menu, and then select your network—either the Wireless Settings 11b/g/n or Wireless Settings 11a/n. Ensure that the auto channel (default) feature is selected for your network. This feature selects a channel that has the least interference.

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.

5. Click **Apply** to save any changes.
6. Under the Configuration tab, select Security from the main menu, and then select your network Security Profile settings—either Security Profile settings 11b/g/n or Security Profile settings 11a/n. For initial configuration and testing, the Security Profile Settings for Profile 1 (the default profile) are set to Open System and the SSID for 11a/n set to NETGEAR\_11a and the SSID for 11b/g/n set to NETGEAR\_11g (see [“Understanding Security Profiles”](#) on [page 2-23](#) to configure a profile).



**Note:** The SSID of any wireless access point must match the SSID you configured in the WNDAP330 Wireless Access Point. If they do not match, you will not get a wireless connection to the WNDAP330.

7. Click **Apply** to save any changes.
8. Configure and test your PCs for wireless connectivity



Program the wireless adapter of your PCs to have the same SSID that you configured in the WNDAP330. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WNDAP330.



**Note:** If you are configuring the WNDAP330 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 WNDAP330, you can configure the advanced wireless security functions.

## Understanding Security Profiles

---

Security Profiles let you configure unique security settings for each SSID. You can configure up to eight unique 802.11b/g/n wireless security profiles or up to eight unique 802.11a/n wireless security profiles on the WNDAP330. The Security Profiles screens are shown below in [Figure 2-13](#).



**Note:** If you are using a RADIUS Server, configure the RADIUS settings first, as described in the [“Configuring WPA with RADIUS”](#) on page 2-36.

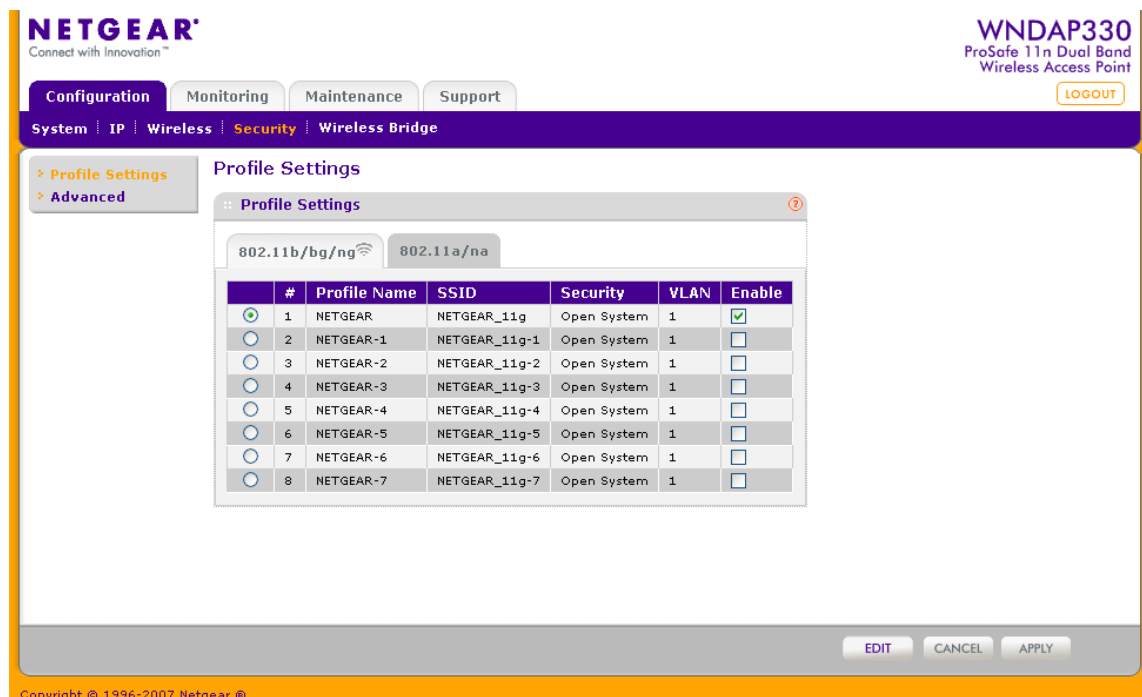


Figure 2-13

An overview of the information that is required to set up a Security Profile follows—including a description of the Network Authentication choices that are available:

- **Profile Definition.** Configure the following settings:
  - **Security Profile Name.** Use a name that makes it easy to recognize the profile—and to tell profiles apart. (The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on.) You can enter a value of up to 32 alphanumeric characters.



**Note:** Only the first profile is enabled by default. The rest of the profiles are disabled and must be enabled if configured.

- **Wireless Network Name (SSID).** This is the name of your wireless network. It is set to the default name of NETGEAR\_11a for 802.11a/n and NETGEAR\_11g for 802.11b/g/n.

- **Broadcast 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. Default is enabled.
- **Authentication Settings.** Configure the following settings:
  - **Network Authentication.** The WNDAP330 Access Point is set by default as an open system with no authentication. When setting up Network Authentication, bear in mind the following:
    - If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options may be unavailable.
    - Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

You can configure the WNDAP330 to use the types of network authentication shown in the table below.

**Table 2-1. Network Authentication Types**

Type <sup>a</sup>	Description
Open System	Can be used with WEP encryption or no encryption.
Shared Key	You must use WEP encryption and enter at least one shared key.
Legacy 802.1x	You must configure the RADIUS Server Settings to use this option.
WPA with RADIUS	You must configure the RADIUS Server Settings to use this option.
WPA2 with RADIUS (WPA2 is a later version of WPA.)	Only select this if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS Server Settings.
WPA and WPA2 with RADIUS	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS Server Settings.
WPA-PSK	You must use TKIP or TKIP + AES encryption and enter the WPA passphrase (Network key).

**Table 2-1. Network Authentication Types**

Type <sup>a</sup>	Description
WPA2-PSK (WPA2 is a later version of WPA )	Only select this if all clients support WPA2. If selected, you must use AES and TKIP + AES encryption and enter the WPA passphrase (Network key).
WPA-PSK and WPA2-PSK	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter the WPA passphrase (Network key).

a. All options are available if using Access Point mode. In other modes (for example, Repeater or Bridge) some options may be unavailable.

- **Data Encryption.** The available options depend on the Network Authentication setting selected (see [Table 2-1](#) above); otherwise, the default is None. The Data Encryption settings are explained in the table below:

**Table 2-2. 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.
152 bits WEP	Proprietary mode that will only work with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA and WPA2.
AES	This is the standard encryption method for WPA2.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

- 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, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 64 characters in length.
- **Wireless Client Security Separation.** If enabled, the associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.) The default is No.
- **VLAN ID.** If the hubs/switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default VLAN ID for WNDAP330 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices.

## SSID and WEP/WPA Settings Setup Form

### 802.11b/g/n Configuration

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\_11g** is the default WNDAP330 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

\_\_\_\_\_

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

- **Authentication:**

Circle one: Open System or Shared Key. (Choose Shared Key for more security.)

**Note:** If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WNDAP330.

- **WEP Encryption Keys.**

Circle one: 64, 128, or 152 bits. (Enter all four 802.11a/n keys for the Key Size chosen.)

Key 1: \_\_\_\_\_

Key 2: \_\_\_\_\_

Key 3: \_\_\_\_\_

Key 4: \_\_\_\_\_

- **WPA-PSK (Preshared Key)**

Record the WPA-PSK key. Key: \_\_\_\_\_

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

Server Name/IP Address: Primary \_\_\_\_\_ Secondary \_\_\_\_\_

Port: \_\_\_\_\_

Shared Secret: \_\_\_\_\_

## 802.11a/n Configuration

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\_11a** is the default WNDAP330 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.  
  
\_\_\_\_\_

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

- **Authentication**

Circle one: Open System or Shared Key. Choose Shared Key for more security.

**Note:** If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WNDAP330.

- **WEP Encryption Keys**

Circle one: 64, 128, or 152 bits. (Enter all four 802.11b/g/n keys for the Key Size chosen.)

Key 1: \_\_\_\_\_

Key 2: \_\_\_\_\_

Key 3: \_\_\_\_\_

Key 4: \_\_\_\_\_

- **WPA-PSK (Preshared Key)**

Record the WPA-PSK key. Key: \_\_\_\_\_

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

Server Name/IP Address: Primary \_\_\_\_\_ Secondary \_\_\_\_\_

Port: \_\_\_\_\_

Shared Secret: \_\_\_\_\_

Use the procedures described in the following sections to configure the WNDAP330. Store this information in a safe place.

## Configuring the RADIUS Server Settings

You can setup or modify the RADIUS Server settings to compliment Network Authentication security options. The RADIUS Server must be used with Legacy 802.1x, and can be used with WPA and WPA2 Network Authentication. When using a RADIUS Server, the RADIUS Server settings must be configured before completing the Network Authentication security profile (see [“Configuring WPA with RADIUS” on page 2-36](#), [“Configuring WPA2 with RADIUS” on page 2-37](#), or [“Configuring WPA and WPA2 with RADIUS” on page 2-38](#) for specifics on implementing these security options).



**Note:** The RADIUS Server Settings apply to all profiles. They only need to be configured once per wireless access point.

To set up or modify the RADIUS Server Settings:

1. From your Web browser, log in to the WNDAP330 using the default LAN address of **http://192.168.0.235**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select RADIUS Server Settings. The RADIUS Server Settings screen will display, as shown in [Figure 2-14](#).



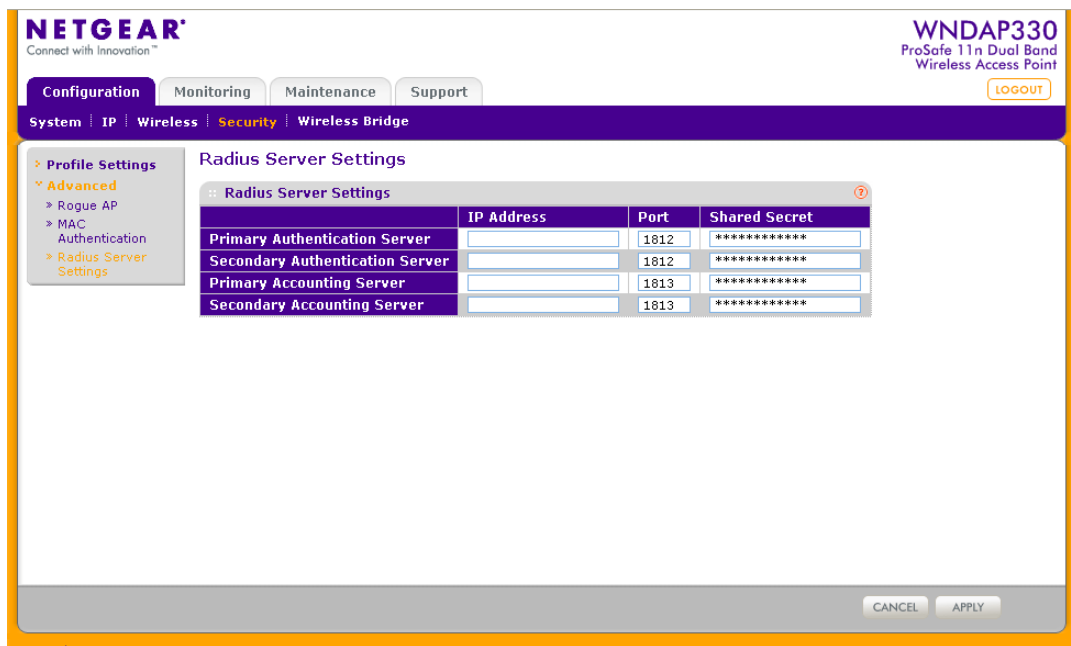


Figure 2-14

### 3. Enter the following RADIUS Server settings:

- **Authentication Server.** This configuration is required for authentication using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use, if the Primary RADIUS Server fails.
  - **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0.
  - **Port Number.** The port number of the RADIUS Server. The default is 1812.
  - **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).
- **Accounting Server.** This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
  - **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0

- **Port Number.** Port number of the RADIUS Server. The default: 1813
- **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).

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

## Setting up a Security Profile

The WNDAP330 allows you to set up eight different security profiles for 802.11b/g/n and eight different profiles for 802.11a/n. Each profile can be configured with a different security option for network authentication.



**Note:** If you are using a RADIUS Server, configure the RADIUS settings first, as described in the “[Configuring the RADIUS Server Settings](#)” on page 2-30.

**NETGEAR**  
Connect with Innovation™

**WNPAP330**  
ProSafe 11n Dual Band  
Wireless Access Point

Configuration Monitoring Maintenance Support

System IP Wireless **Security** Wireless Bridge

> Profile Settings  
> Advanced

**Profile Settings**

802.11b/g/n 802.11a/n

#	Profile Name	SSID	Security	VLAN	Enable
1	NETGEAR	NETGEAR_11g	Open System	1	<input checked="" type="checkbox"/>
2	NETGEAR-1	NETGEAR_11g-1	Open System	1	<input type="checkbox"/>
3	NETGEAR-2	NETGEAR_11g-2	Open System	1	<input type="checkbox"/>
4	NETGEAR-3	NETGEAR_11g-3	Open System	1	<input type="checkbox"/>
5	NETGEAR-4	NETGEAR_11g-4	Open System	1	<input type="checkbox"/>
6	NETGEAR-5	NETGEAR_11g-5	Open System	1	<input type="checkbox"/>
7	NETGEAR-6	NETGEAR_11g-6	Open System	1	<input type="checkbox"/>
8	NETGEAR-7	NETGEAR_11g-7	Open System	1	<input type="checkbox"/>

EDIT CANCEL APPLY

Copyright © 1996-2007 Netgear, Inc.

Figure 2-15

To configure a Security Profile:

1. From your Web browser, log in to the WNDAP330 using the default LAN address of **http://192.168.0.230**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. Under the Configuration tab, select Security from the main menu, and then select either Security Profile Settings for 802.11b/g/n or 802.11a/n. The screen for the Profile Settings you selected will display as shown in [Figure 2-16](#) above.
3. Check the radio button of the profile you want to modify and click **Edit**. The Security Profile Configuration screen for the selected profile will display.

**Figure 2-16**

4. Give your profile a meaningful name so that you can remember it later.
5. The Wireless Network Name (SSID) is set by default to identify it as NETGEAR-11a.
6. Enable or disable the Broadcast Wireless Network Name (SSID). It is enabled by default. (If it is broadcast, it can be easily detected by other clients.)
7. From the pull-down menu shown in [Figure 2-16](#), select the Network Authentication Type you want to use for this profile:

- To configure WEP encryption for Open Systems or Shared Key, see [“Configuring WEP” on page 2-34](#).
  - To configure WPA with RADIUS, see [“Configuring WPA with RADIUS” on page 2-36](#).
  - To configure WPA2 with RADIUS, see [“Configuring WPA2 with RADIUS” on page 2-37](#).
  - To configure WPA and WPA2 with RADIUS, see [“Configuring WPA and WPA2 with RADIUS” on page 2-38](#).
  - To configure WPA-PSK, see [“Configuring WPA-PSK” on page 2-39](#).
  - To configure WPA2-PSK, see [“Configuring WPA2-PSK” on page 2-40](#).
  - To configure WPA-PSK and WPA2-PSK, see [“Configuring WPA-PSK and WPA2-PSK” on page 2-41](#).
8. **Wireless Client Security Separation** is disabled by default. If enabled, the associated wireless clients will not be able to communicate with each other.
  9. If the hubs/switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default **VLAN ID** for WNDAP330 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices.
  10. Click **Apply** to save your Security Profile settings.
  11. Click **Back**. Your new settings will appear in the Security Profiles table identified by the Profile Name of the profile. A VLAN ID will also be assigned to your profile.



**Note:** Security Profiles that share the same type of network authentication need not share the same passphrase or keys. Security Profiles that use WEP must share the same four keys, but they do not need to use the same default key.

To enable your Security Profile:

1. Check the radio box in the **Enable** column next to your profile.
2. Click **Apply**. Your Security Profile will be enabled. If you enabled VLAN 802.1Q, your VLAN Profile will also be enabled. (See [“Setting Basic IP Options” on page 2-13](#) to enable VLAN 802.1Q.)

## Configuring WEP

To configure WEP data encryption:

1. From the Network Authentication drop-down menu, choose either Open System or Shared Key authentication.
2. From the Data Encryption drop-down menu, select encryption strength (64 bits, 128 bits, or 152 bits).
3. You 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.

The screenshot shows the 'Edit Security Profile' window with two tabs: 'Profile Definition' and 'Authentication Settings'.

**Profile Definition Tab:**

- Profile Name: NETGEAR
- Wireless Network Name (SSID): NETGEAR\_11g
- Broadcast Wireless Network Name (SSID): ☒ Yes ☐ No

**Authentication Settings Tab:**

- Network Authentication: Open System
- Data Encryption: 128 bits WEP
- Passphrase: [masked]
- Key 1 ☒: 955FB36FA5AD7BC94C
- Key 2 ☐: 955FB36FA5AD7BC94C
- Key 3 ☐: 955FB36FA5AD7BC94C
- Key 4 ☐: 955FB36FA5AD7BC94C
- Wireless Client Security Separation: ☐ Yes ☒ No
- VLAN ID: 1

Figure 2-17

4. 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.”](#)
5. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.)
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 with RADIUS

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 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select RADIUS Server Settings. The RADIUS Server Settings screen will display.
2. Enter the RADIUS Server Settings as shown in [“Configuring the RADIUS Server Settings” on page 2-30](#).
3. Click **Apply** to save your RADIUS Server settings.
4. Under the Configuration tab, select Security from the main menu, and then select either Security Profile Settings for 802.11b/g/n or 802.11a/n. The screen for the Profile Settings you selected will display. When the Security Profile screen displays, check the radio button of the Security Profile you want to modify and click **Edit**.

**Edit Security Profile**

**Profile Definition**

Profile Name: NETGEAR

Wireless Network Name (SSID): NETGEAR\_11g

Broadcast Wireless Network Name (SSID): ☒ Yes ☐ No

**Authentication Settings**

Network Authentication: WPA with Radius

Data Encryption: TKIP

Wireless Client Security Separation: ☐ Yes ☒ No

VLAN ID: 1

**Figure 2-18**

5. Choose **WPA with RADIUS** from the from the Network Authentication drop-down menu. Data Encryption will be set to TKIP by default.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

## Configuring WPA2 with RADIUS

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

The figure displays two screenshots of the 'Edit Security Profile' configuration window. The left screenshot shows the 'Profile Definition' tab, which includes fields for 'Profile Name' (NETGEAR), 'Wireless Network Name (SSID)' (NETGEAR\_11g), and 'Broadcast Wireless Network Name (SSID)' (Yes/No). The right screenshot shows the 'Authentication Settings' tab, which includes fields for 'Network Authentication' (WPA2 with Radius), 'Data Encryption' (AES), 'Wireless Client Security Separation' (Yes/No), and 'VLAN ID' (1).

**Figure 2-19**

To configure WPA2 with RADIUS:

1. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select RADIUS Server Settings. The RADIUS Server Settings screen will display.
2. Enter the RADIUS settings as shown in [“Configuring the RADIUS Server Settings” on page 2-30](#).
3. Click **Apply** to save your RADIUS settings.
4. Under the Configuration tab, select Security from the main menu, and then select either Security Profile Settings for 802.11b/g/n or 802.11a/n. The screen for the Profile Settings you selected will display. When the Security Profile screen displays, check the radio button of the Security Profile you want to modify and click **Edit**.

5. From the Network Authentication drop-down menu, select WPA2 with RADIUS from the list. By default, Data Encryption will be set to AES.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.)
7. Click **Apply** to save your settings.

## Configuring WPA and WPA2 with RADIUS

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3, or above, do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

The figure displays two screenshots of the 'Edit Security Profile' configuration window. The left screenshot shows the 'Profile Definition' tab, which includes fields for 'Profile Name' (NETGEAR), 'Wireless Network Name (SSID)' (NETGEAR\_11g), and 'Broadcast Wireless Network Name (SSID)' (Yes/No). The right screenshot shows the 'Authentication Settings' tab, which includes fields for 'Network Authentication' (WPA & WPA2 with Radius), 'Data Encryption' (TKIP + AES), 'Wireless Client Security Separation' (Yes/No), and 'VLAN ID' (1).

**Figure 2-20**

To configure WPA and WPA2 with RADIUS:

1. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select RADIUS Server Settings. The RADIUS Server Settings screen will display.
2. Enter the RADIUS settings as shown in “[Configuring the RADIUS Server Settings](#)” on [page 2-30](#).
3. Click **Apply** to save your RADIUS settings



4. Under the Configuration tab, select Security from the main menu, and then select either Security Profile Settings for 802.11b/g/n or 802.11a/n. The screen for the Profile Settings you selected will display. When the Security Profile screen displays, check the radio button of the Security Profile you want to modify and click **Edit**.
5. From the **Network Authentication** drop-down menu, select **WPA & WPA2 with RADIUS** from the list. By default, **Data Encryption** will be set to **TKIP+AES**.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
7. Click **Apply** to save your settings.

## Configuring WPA-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.

Edit Security Profile		Edit Security Profile	
<b>:: Profile Definition</b>		<b>:: Profile Definition</b>	
Profile Name	NETGEAR	Profile Name	NETGEAR
Wireless Network Name (SSID)	NETGEAR_11g	Wireless Network Name (SSID)	NETGEAR_11a
Broadcast Wireless Network Name (SSID)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Broadcast Wireless Network Name (SSID)	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>:: Authentication Settings</b>		<b>:: Authentication Settings</b>	
Network Authentication	WPA-PSK	Network Authentication	WPA-PSK
Data Encryption	TKIP + AES	Data Encryption	TKIP
WPA Passphrase (Network Key)	XXXXXXXXXXXXXXXXXXXX	WPA Passphrase (Network Key)	XXXXXXXXXXXXXXXXXXXX
Wireless Client Security Separation	<input type="radio"/> Yes <input checked="" type="radio"/> No	Wireless Client Security Separation	<input type="radio"/> Yes <input checked="" type="radio"/> No
VLAN ID	1	VLAN ID	1

Figure 2-21

To configure WPA-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK**. By default, **Data Encryption** will be set to **TKIP**.
2. Enter the preshared key passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

## Configuring WPA2-PSK

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

The figure displays two screenshots of the 'Edit Security Profile' configuration window. The left screenshot shows the 'Profile Definition' tab with the following settings: Profile Name: NETGEAR, Wireless Network Name (SSID): NETGEAR\_11g, Broadcast Wireless Network Name (SSID): Yes (selected). The right screenshot shows the 'Authentication Settings' tab with the following settings: Network Authentication: WPA2-PSK, Data Encryption: AES, WPA Passphrase (Network Key): [masked], Wireless Client Security Separation: No (selected), VLAN ID: 1.

**Figure 2-22**

To configure WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA2-PSK** from the list. By default, **Data Encryption** will be set to **AES**.
2. Enter the preshared key passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

## Configuring WPA-PSK and WPA2-PSK

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

The figure displays two side-by-side screenshots of the 'Edit Security Profile' configuration window. The left window shows the 'Profile Definition' tab, and the right window shows the 'Authentication Settings' tab. Both windows have a grey header with the title 'Edit Security Profile' and a help icon. The left window's 'Profile Definition' tab includes fields for 'Profile Name' (NETGEAR), 'Wireless Network Name (SSID)' (NETGEAR\_11g), and 'Broadcast Wireless Network Name (SSID)' with radio buttons for 'Yes' and 'No'. The right window's 'Authentication Settings' tab includes a 'Network Authentication' dropdown menu (WPA-PSK & WPA2-PSK), a 'Data Encryption' dropdown menu (TKIP + AES), a 'WPA Passphrase (Network Key)' field (\*\*\*\*\*), a 'Wireless Client Security Separation' section with radio buttons for 'Yes' and 'No', and a 'VLAN ID' field (1).

Figure 2-23

To configure WPA-PSK and WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK & WPA2-PSK**. By default, **Data Encryption** will be set to **TKIP+AES**.
2. Enter the WPA Passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

## Restricting Wireless Access by MAC Address

The optional Access Control window lets you block the network access privilege of any specified stations through the WNDAP330 Wireless Access Point. When you enable access control, the access point only accepts connections from clients on the selected access control list. This provides an additional layer of security.



**Note:** If configuring the WNDAP330 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click **Apply**. You must then access the wireless access point from a wired computer or from a wireless computer that is on the access control list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the WNDAP330 using the default address of **http://192.168.0.235**, user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select MAC Authentication. The MAC Authentication screen will display.

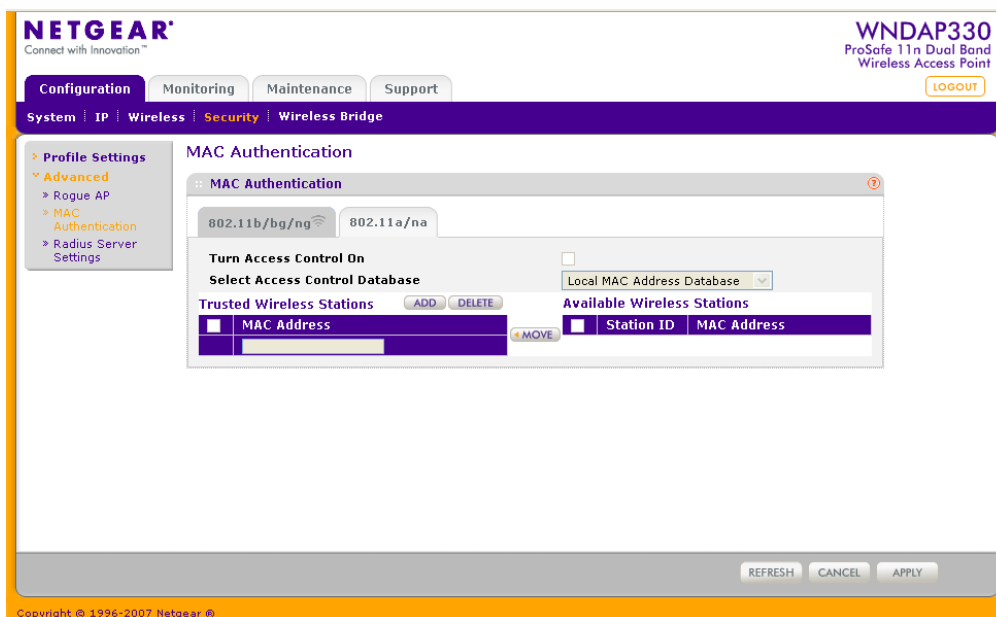


Figure 2-24

3. Check the **Turn Access Control On** radio box to enable Access Control feature.
4. Select the desired Access Control Database options. The options are:
  - **Local MAC Address Database** – The Access Point will use the local MAC address table for Access Control. This is the default.
  - **RADIUS MAC Address Database** – The Access Point will use the MAC address table located on the external RADIUS server on the LAN for Access Control. If you choose this database, you must configure the RADIUS Server Settings first (see [“Configuring the RADIUS Server Settings”](#) on page 2-30).
5. The **Trusted Wireless Stations** list shows any wireless stations you have entered. If you have not entered any wireless stations this list will be empty. To delete an existing entry, select it and then click **Delete**.
6. Click Refresh to refresh the **Available Wireless Stations** list found in your area.
7. Select the stations from the list of **Available Wireless Stations** found in your area, or enter the MAC address of a station to add a new station manually. (You can usually find the MAC address printed on the bottom of the wireless adapter.)

8. Click **Add** to add the wireless device to the **Trusted Wireless Stations** list. Repeat these steps for each additional device you want to add to the list.
9. Click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WNDAP330.

# Chapter 3

## Management

This chapter describes how to use the management features of your ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. To access these features, connect to the WNDAP330 as described in [“Logging In Using the Default IP Address”](#) on page 2-12. Then select the category under either the Management or Information headings in the main menu of the browser interface.

## Remote Management

Both the SNMP and Remote Console are enabled by default, which allows for remote management of the WNDAP330 from a client running SNMP management software, as well as from a secure Telnet console.

To set up an SNMP management interface:

1. Under the Maintenance tab, select Remote Management, and then select SNMP from the left-hand menu. The SNMP screen will display, as shown in [Figure 3-1](#).

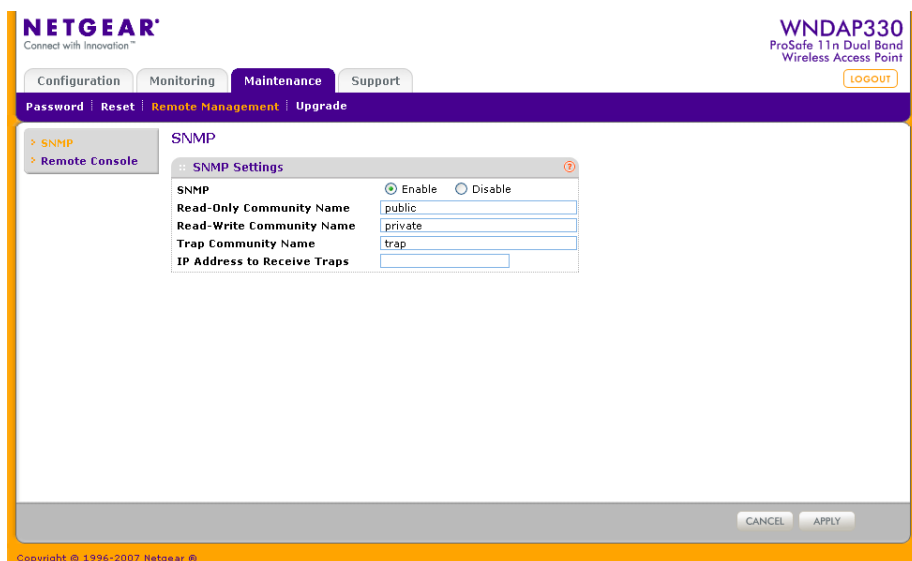


Figure 3-1

2. Enter the following information in the SNMP fields:

- **SNMP:** Enable SNMP to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point via SNMPv1/v2 protocol.
- **Read-Only Community Name:** The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is Public.
- **Read-Write Community Name:** The community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The default is Private.
- **Trap Community Name:** The community string to allow the SNMP manager to send traps. The default is trap.
- **IP address to Receive Traps:** The IP address of the SNMP manager to receive traps sent from the wireless access point. The default is 0.0.0.0.

## Remote Console

---

The Remote Console configuration features are located under the Maintenance tab, Remote Management, and then under Remote Console. Enter the following information in the Remote Console screen, as shown in [Figure 3-2](#):

- **Secure Shell (SSH):** If set to Enable, the Wireless Access Point will only allow remote access via Secure Shell and Secure Telnet. The default is Enable.
- **Telnet:** If set to Enable, the Wireless Access Point will only allow remote access via Telnet. The default is Enable.



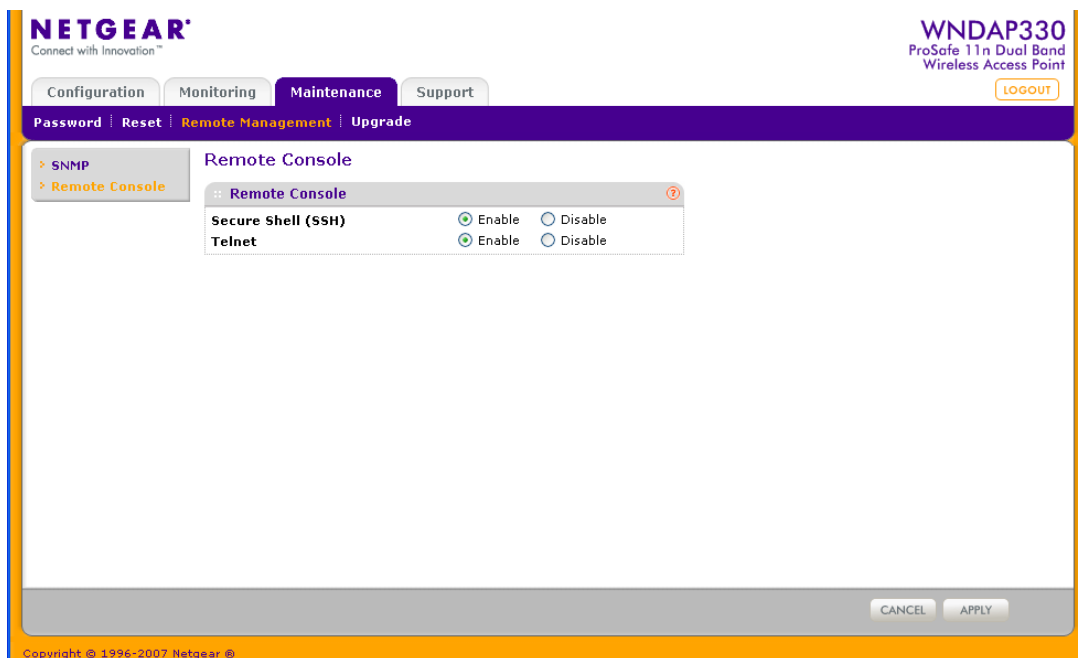


Figure 3-2

## Using the Secure Telnet Interface

The WNDAP330 includes a secure Telnet command line interface (CLI). You can access the CLI from a secure Telnet client over the Ethernet port or over the serial console port.



**Note:** You must use a secure Telnet client such as Absolute Telnet. Also, when you configure the client, use the SSH1, 3DES option. If you use the Telnet client to connect over the Ethernet port, use the IP address of the WNDAP330 as the host name.

To use the CLI from a Console Port:

1. Using the null-modem cable, connect a VT100/ANSI terminal or a workstation to the port labeled Console.

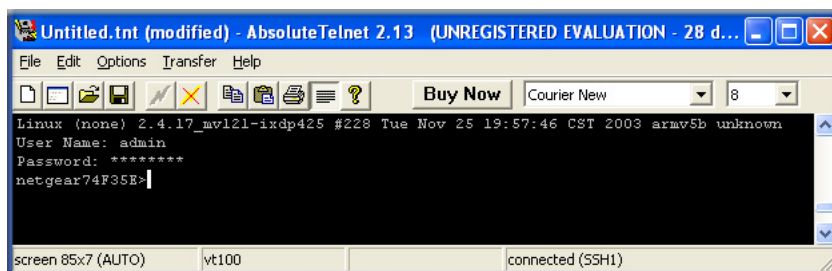
If you attached a PC, Apple Macintosh, or UNIX workstation, start a secure terminal-emulation program.

2. Configure the terminal-emulation program to use the following settings:

- Baud rate: 9600 bps
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

These settings appear below the connector on the back panel.

3. Press **Enter**. The screen shown below in [Figure 3-3](#) should appear.



**Figure 3-3**

4. Enter the login name and password (**admin** and **password** are the defaults).

After successful login, the *<Access Point Name>* prompt should appear. In this example, the prompt is *netgear74F35E*.

5. Enter `help` to display the CLI command help.

## CLI Commands

The CLI commands are listed in [Appendix C, “Command Line Reference.”](#)

## Upgrading the Wireless Access Point Software

---

The software of the WNDAP330 Wireless Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.RMT) file before sending it to the wireless access point. The upgrade file can be sent using your browser.



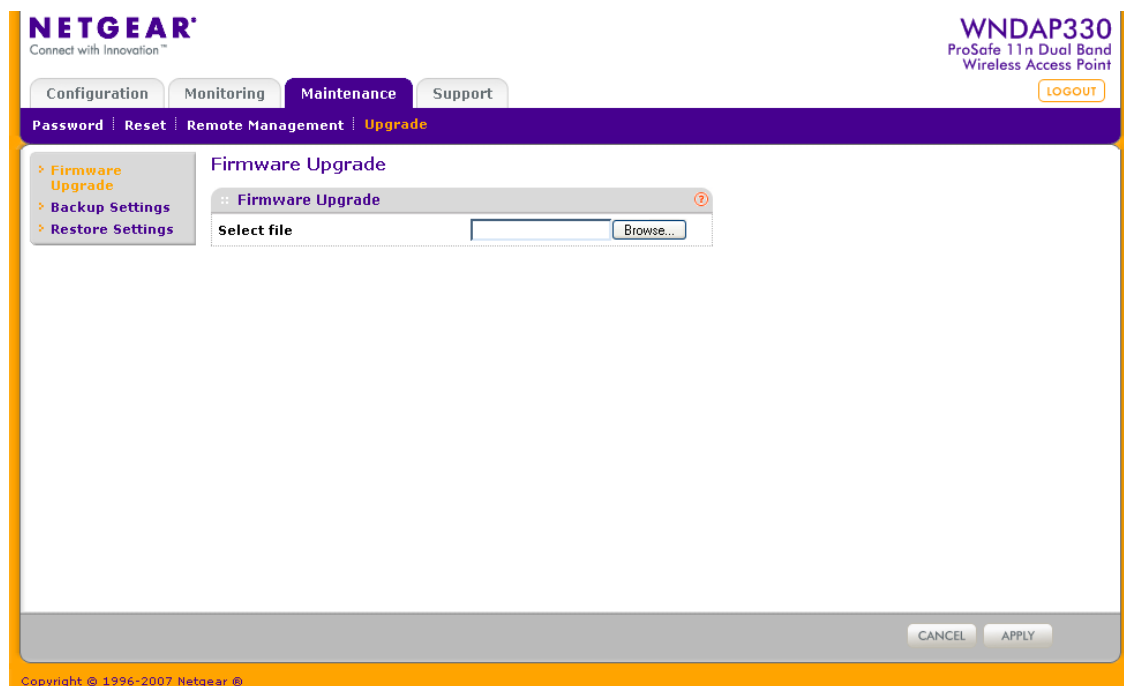
**Note:** The Web browser used to upload new firmware into the WNDAP330 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above, or Mozilla 1.5 or above.

You cannot perform the software upgrade from a computer that is connected to the WNDAP330 Wireless Access Point with a wireless link. You must use a computer that is connected to the WNDAP330 Wireless Access Point with a Ethernet cable.



**Warning:** When uploading software to the WNDAP330 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 WNDAP330 completely inoperable.

The Web browser used to upload new firmware into the WNDAP330 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.



**Figure 3-4**

To upgrade the WNDAP330 firmware:

1. Download the new software file from the NETGEAR website, save it to your hard disk, and unzip it.
2. Under the Maintenance tab, select Upgrade from the main menu, and then select Firmware Upgrade. The Firmware Upgrade screen will display as shown in [Figure 3-4](#).
3. Click **Browse** and browse to the location of the image (.RMG) upgrade file.
4. Click **Apply**.

When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about 1 minute and 30 seconds.

## Configuration File Management

The WNDAP330 Wireless Access Point settings are stored in the wireless access point in a configuration file. This file can be saved (backed up) to a user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

To backup or restore your settings:

Under the Maintenance tab, from Upgrade on the main menu, select Backup Settings from the left-hand menu to back up your current settings. Similarly, select Restore Setting to restore your settings. The respective are shown in [Figure 3-5](#) and [Figure 3-6](#).

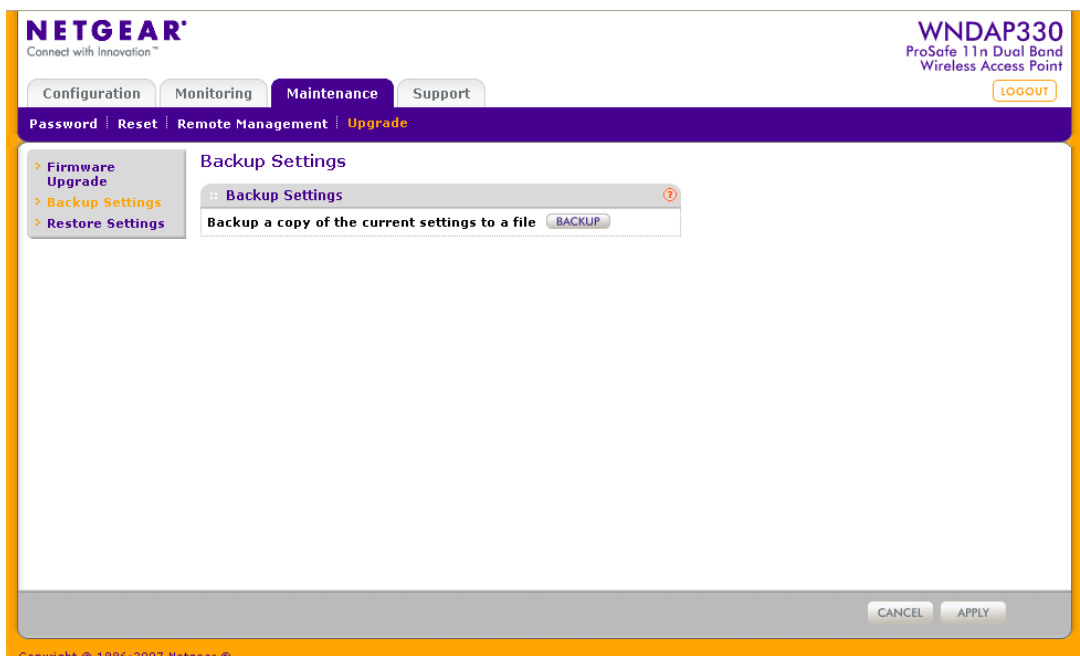


Figure 3-5

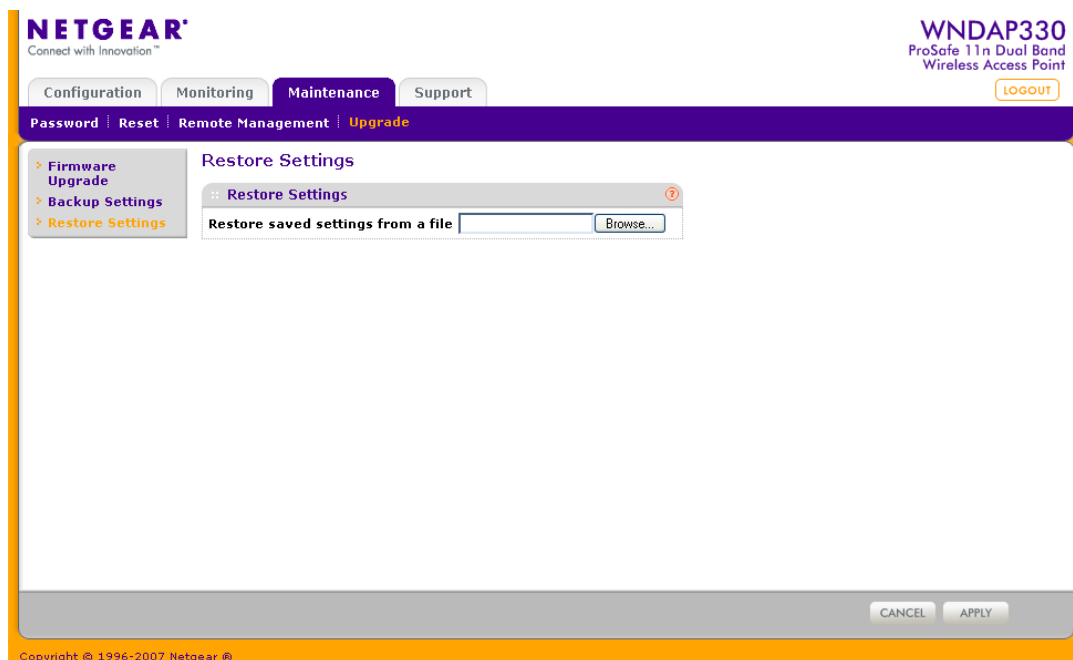


Figure 3-6

The two screens are described in the following sections:

## Saving the Configuration

Under the Maintenance tab, from Upgrade on the main menu, select Configuration Backup/Restore. The Configuration Backup/Restore screen will display, as shown in [Figure 3-5](#).

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

To save your settings:

1. Click **Backup**. Your browser will extract the configuration file from the wireless access point and prompt you for a location on your computer to store the file.
2. Give the file a meaningful name, such as `WNDAP330.cfg`, and click **Save**.

## Restoring the Configuration

To restore your settings from a saved configuration file:

1. Enter the full path to the file on your computer or click the Browse button to locate the file.
2. When you have located the file, click **Restore** to upload the file. After completing the upload, the WNDAP330 will reboot automatically.

## Restoring the WNDAP330 to the Factory Default Settings

It is sometimes desirable to restore the wireless access point to the factory default settings. This can be done by using the Restore function, which restores all factory settings.

To access this function:

1. Under the Maintenance tab, select Reset from the main menu, and then select Restore Defaults from the left-hand menu. The Restore Defaults screen will display, as shown in [Figure 3-7](#).

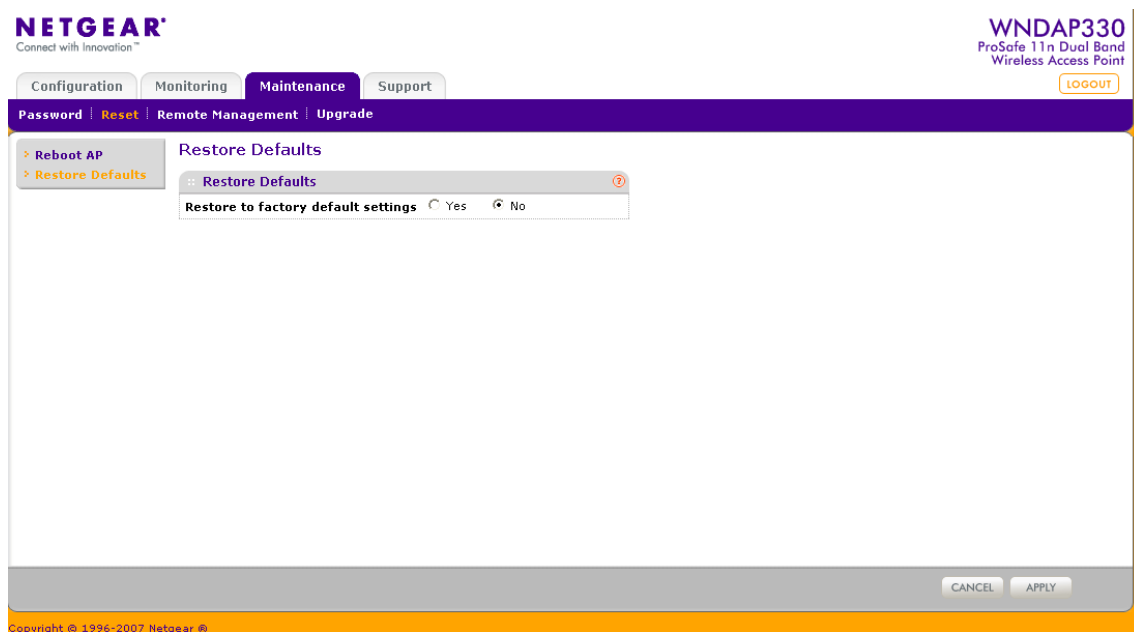


Figure 3-7

2. On the Restore Defaults screen, enable the Restore to factory default settings option by selecting the Yes radio button.
3. Click **Apply** to reset to the factory default settings.

After a restore, the wireless access point password will be **password**, the WNDAP330 DHCP client will be enabled, the default LAN IP address will be 192.168.0.230, and the access point name will reset to the name printed on the label on the bottom of the unit.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless access point (see [Figure 1-1 on page 1-8](#)). The reset button has two functions:

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

To clear all data and restore the factory default values:

1. Power off the WNDAP330.
2. Use something with a small point, such as a pen, hold the Reset button for 5 seconds while your Power On the WNDAP330.
3. Continue holding the Reset Button until the LEDs blink twice.
4. Release the Reset Button.

The factory default configuration has now been restored and the WNDAP330 is ready for use.

## Changing the Administrator Password

---

The default password is **password**. You should change this password to a more secure password, since you cannot change the administrator login name.

To change the Administrator password:

1. Under the Maintenance tab, select Password on the main menu, and then select select Change Password. The Change Password screen will display as shown in [Figure 3-8](#) below.



The screenshot displays the Netgear WNDAP330 web interface. At the top, the Netgear logo is on the left, and the device model 'WNDAP330 ProSafe 11n Dual Band Wireless Access Point' is on the right. Below the logo is a navigation bar with tabs: Configuration, Monitoring, Maintenance (selected), and Support. A secondary bar contains links: Password (selected), Reset, Remote Management, and Upgrade. A 'Logout' button is in the top right. The main content area is titled 'Change Password' and features a 'Change Password' button. A modal window titled 'Change Password' contains four input fields: 'Current Password', 'New Password', and 'Repeat New Password'. Below these is a 'Restore Default Password' section with 'Yes' and 'No' radio buttons, where 'No' is selected. At the bottom of the modal are 'CANCEL' and 'APPLY' buttons. The footer shows 'Copyright © 1996-2007 Netgear'.

**Figure 3-8**

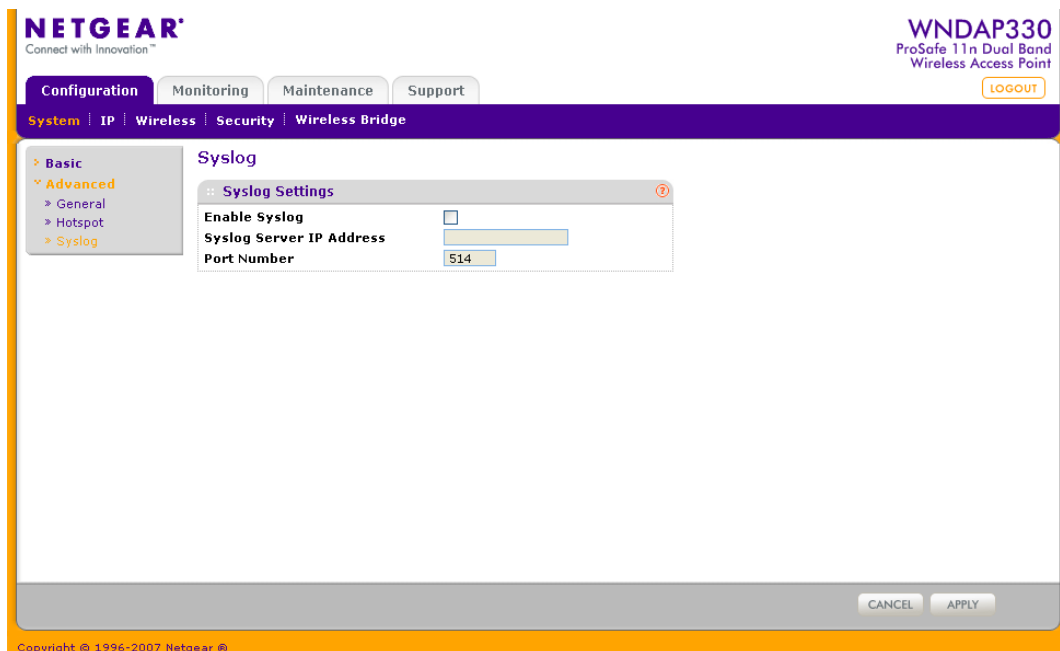
2. First enter the old password in the Current Password field.
3. Then enter the new password twice—once in the New Password field and again in the Repeat New Password field.
4. Click **Apply** to save your change.

## Enabling the SysLog Server

The SysLog screen allows you to enable the SysLog option if you have a SysLog server on your LAN.

To enable a SysLog server:

1. Under the Configuration tab from System on the main menu, select the Advanced option, and then select SysLog to view the screen shown in [Figure 3-9](#).



**Figure 3-9**

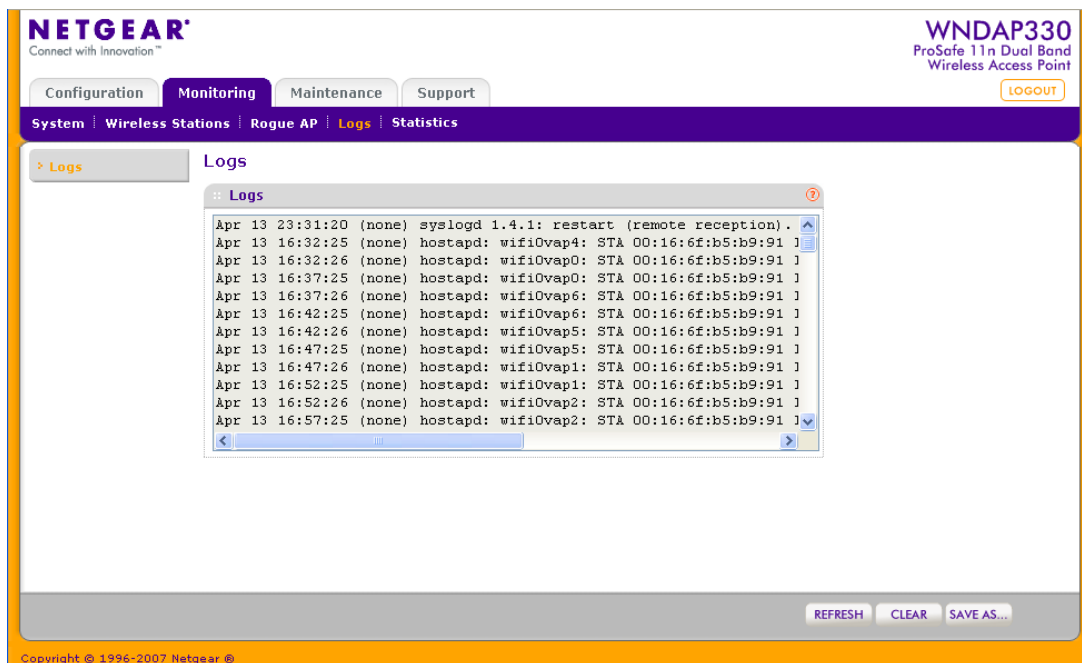
2. **Enable SysLog** – Enable this option if you have a SysLog server on your LAN. If enabled, you must enter the IP address of your SysLog server and the port number your SysLog server is configured to use. The default is Disabled.
3. **SysLog Server IP Address** –The access point will send all the SysLog to the specified IP address if SysLog option is enabled. Default is 0.0.0.0.
4. **Port Number** – The port number configured in the SysLog server on your LAN. Default is 514.
5. Click **Apply** to save your Syslog settings.

## Using Activity Log Information

---

The Activity Log screen displays the Access Point system activity.

To view the Activity Log , under the Monitoring tab, click Logs on the main menu to view the screen shown in Figure 3-10.



**Figure 3-10**

The Activity Log Window displays the Access Point system activity.

Click **Refresh** to update the display, click **Clear** to clear the log content, or click **Save As** to save the log contents into a file on your PC or to save the file to a disk drive.

## Viewing General Summary Information

The System screen, under the Monitoring tab provides a summary of the current WNDAP330 configuration settings, including current IP settings and current Wireless settings. This information is read only, so any changes must be made on other screens.

To access the System screen:

Under the Monitoring tab, select System on the main menu to view the System screen, shown in [Figure 3-11](#) below. This screen shows the parameters listed in [Table 3-1](#):

**Table 3-1. System Information Fields**

Field	Description
<b>Access Point Information</b>	
Access Point Name	Indicates the NetBIOS name. The default name may be changed, if desired.
MAC Address	Displays the Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Country/Region	Displays the domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Access Point Mode	Identifies the operating mode of the WNDAP330: Access Point, Point-to-point bridge, Point-to-point bridge with Access Point, Multi-point bridge or Repeater.
<b>Current IP Settings</b>	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
<b>Current Wireless Settings for 802.11n/g</b>	
Operating Mode	Identifies the 802.11 operating mode of the WNDAP330.
Channel/Frequency	Identifies the channel the wireless port is using. 11 is the default channel setting. (Channel frequencies used on each channel can be found in "Wireless Communications"; a link to this article is in <a href="#">Appendix B, "Related Documents"</a> ).
Rogue AP Detection	Identifies whether the Rogue AP detection feature is enabled or disabled.

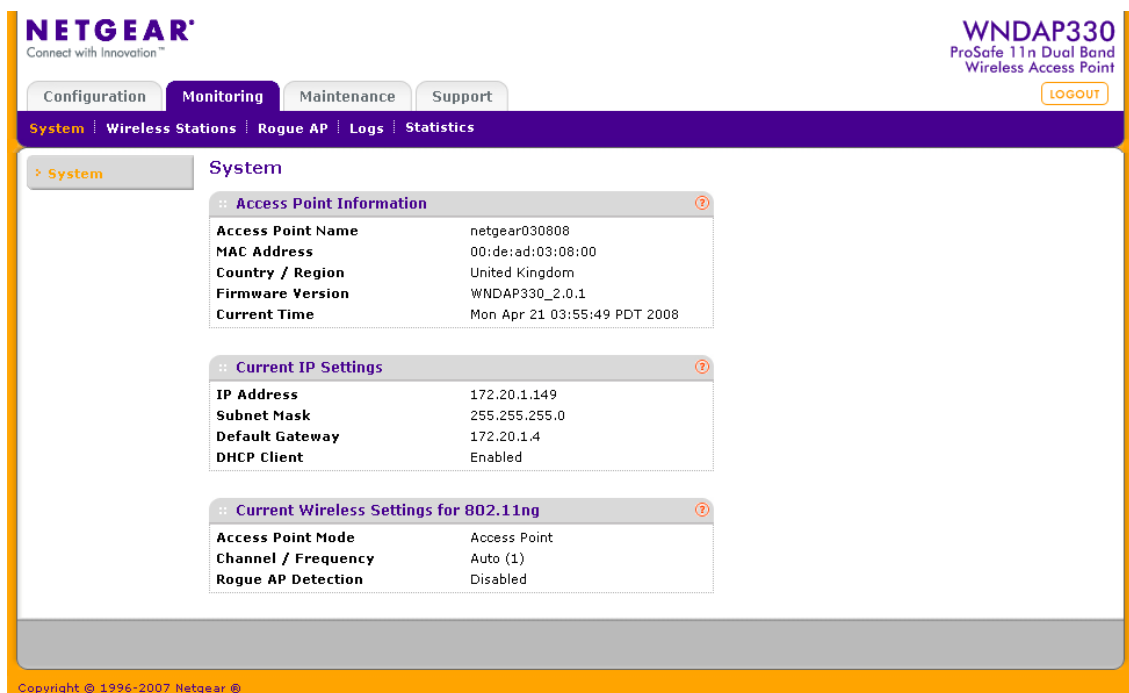


Figure 3-11

## Viewing Network Traffic Statistics

The Statistics screen displays information for both wired (LAN) and wireless (WLAN) interface network traffic.

To access Statistics information:

1. Under the Monitoring tab, select Statistics on the main menu. The Statistics screen will display, as shown in [Figure 3-12](#).

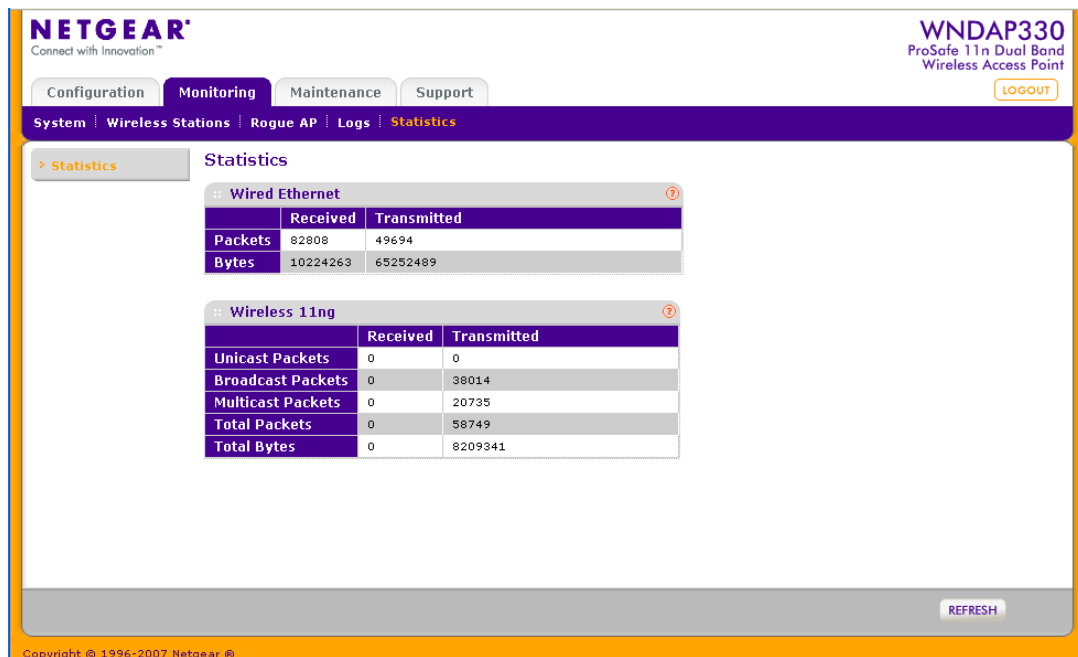


Figure 3-12

2. Click **Refresh** to update the Statistics information for each interface. .

Table 3-2, shown below, describes the information fields detailed on the Statistics screen.

Table 3-2. Statistics Fields

Field	Description
<b>Wired Ethernet</b>	
Packets	The number of packets sent and received since the WNDAP330 was restarted.
Bytes	The number of bytes sent and received since the WNDAP330 was restarted.
<b>Wireless 11n/g</b>	
Unicast Packets	The Unicast packets sent and received since the WNDAP330 was restarted.

**Table 3-2. Statistics Fields**

Field	Description
Broadcast Packets	The Broadcast packets sent and received since the WNDAP330 was restarted.
Multicast Packets	The Multicast packets sent and received since the WNDAP330 was restarted.
Total Packets	The Wireless packets sent and received since the WNDAP330 was restarted.
Total Bytes	The Wireless bytes sent and received since the WNDAP330 was restarted.

## Viewing Available Wireless Station Statistics

The Available Wireless Station List contains a table of all IP devices associated with this wireless access point in the wireless network defined by the Wireless Network Name (SSID). For each device, the table shows the Station ID, MAC address, IP Address, BSSID, SSID, AID, Channel rate, Status (whether the device is allowed to communicate with the wireless access point or not), Type, Mode, and State.



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

To view the Wireless Station List:

1. Under the Monitoring tab, select Wireless Stations on the main menu. The Wireless Stations list will display, as shown in [Figure 3-13](#).

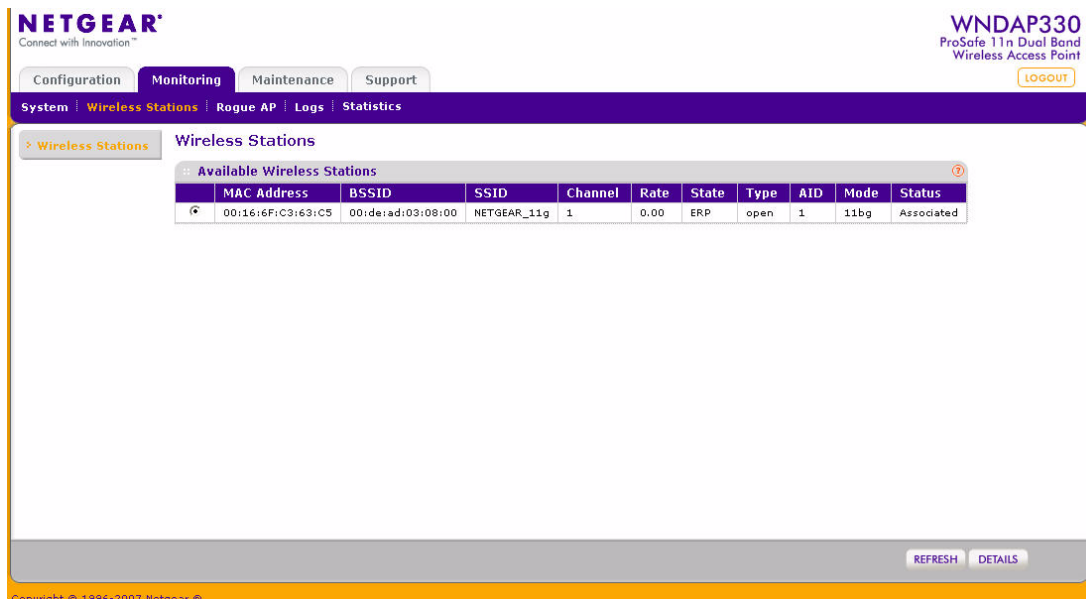


Figure 3-13

2. Click **Refresh** to update the list.



**Tip:** If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the **Refresh** button.

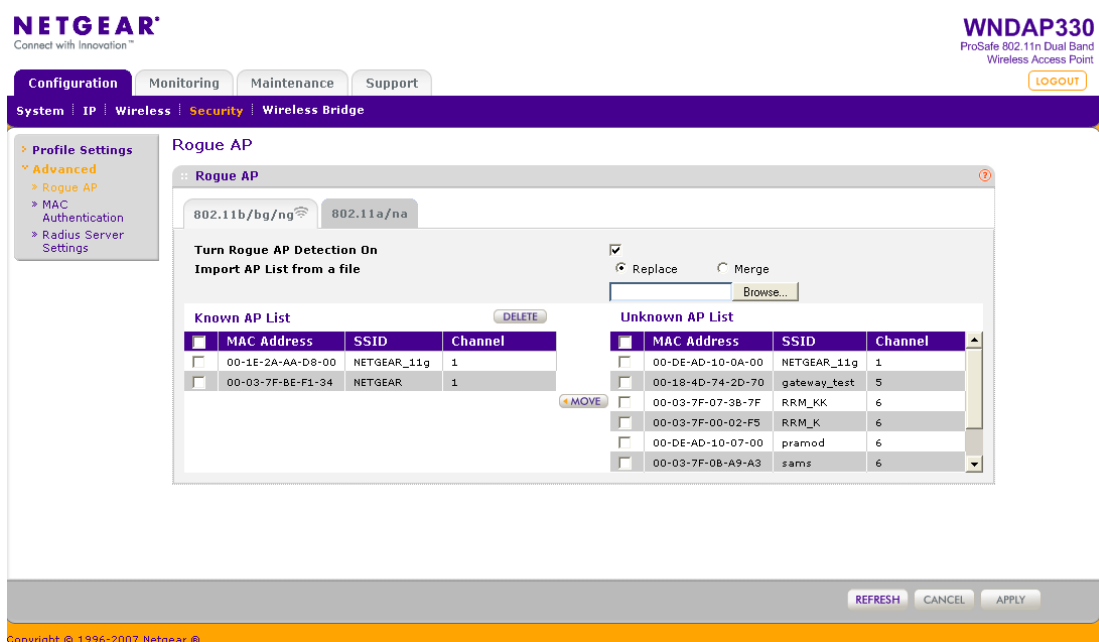
## Enabling Rogue AP Detection

The WNDAP330 can detect rogue APs and wireless stations and can exclude them from connecting to the WNDAP330 Wireless Access Point.

To enable Rogue AP Detection:



1. Under the Configuration tab, select Security on the main menu, select Advanced from the left-hand menu, and then select Rogue AP. The Rogue AP screen will display, as shown in [Figure 3-8](#) below.



**Figure 3-14**

2. Check the Turn Rogue AP Detection On radio box to enable Rogue AP Detection and click **Apply**.  
If you enable Rogue AP Detection, the AP continuously scans the wireless network and collects information about all APs heard on its channel.
3. You can Import AP List from a File. See [“Importing Rogue AP List from a File”](#) on page 3-20 for more information.
4. Under the Unknown AP List, click **Refresh** to discover the APs.
5. Click **Move** to add any AP to the Known AP List.
6. Click **Delete** to remove an AP from the Known AP List.
7. Click **Save** to export the list of known APs to a file. A window opens so you can browse to the location where you want to save the file. The default file name is WNDAP330Rogue.cfg.
8. Click **Apply** to save your change.

## Importing Rogue AP List from a File

To replace the existing AP list:

1. Create a text file that contains the MAC address of each known AP, separated by a space. The following example shows a list of six known APs that an administrator might upload to the AP:

```
00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d  
00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4
```

2. Check the Replace radio button to replace the existing list of known APs, or check Merge to add the new MAC addresses to the existing list.
3. Click **Browse** and navigate to the location where you saved the text file.
4. Select the file and click **Open**.
5. Click **Import** to upload the list to the AP.

To merge with an existing AP list:

1. Create a text file that contains the MAC address of each known AP, separated by a space. The following example shows a list of six known APs that an administrator might upload to the AP:

```
00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d  
00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4
```

2. Check the Merge radio button to add the new MAC addresses to the existing list.
3. Click **Browse** and navigate to the location where you saved the text file.
4. Select the file and click **Open**.
5. Click **Import** to upload the list to the AP.

To import the list from an existing file:

1. Click **Browse** and navigate to the location where you saved the text file.
2. Select the file and click **Open**.
3. Click **Import** to upload the list to the AP.

## Viewing Rogue AP Statistics

The WNDAP330 can detect rogue APs and wireless stations and can exclude them from connecting to the WNDAP330 Wireless Access Point.

To view Rogue AP list:

1. Under the Monitoring tab, select Rogue AP. Select Unknown AP List or Known AP List as required. The respective screens will display, as shown in [Figure 3-15](#) and [Figure 3-16](#) below.

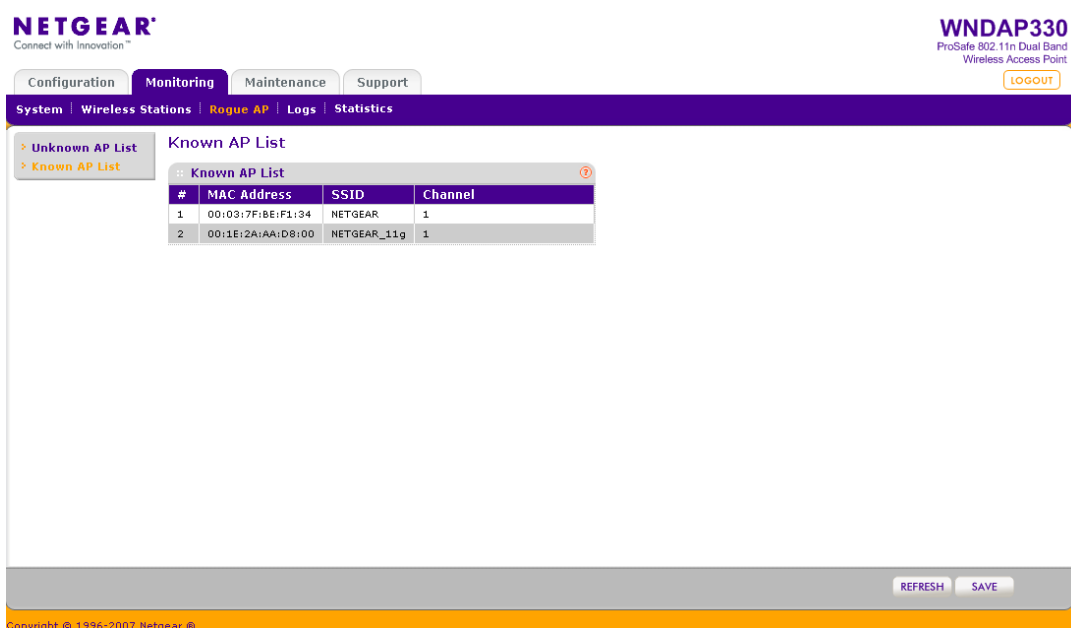


Figure 3-15

The screenshot displays the Netgear WNDAP330 web interface. The top navigation bar includes tabs for Configuration, Monitoring (selected), Maintenance, and Support. Below this, a secondary navigation bar shows System, Wireless Stations, Rogue AP (selected), Logs, and Statistics. The main content area is titled 'Unknown AP List' and contains a table with the following data:

#	MAC Address	SSID	Privacy	Channel	Rate	Beacon Int.	# of Beacons	Last Beacon
1	00:DE:AD:10:0A:00	NETGEAR_11g	0	1	130.00	100	103	651119
2	00:18:4D:74:2D:70	gateway_test	0	5	54.00	100	2	368849
3	00:03:7F:07:38:7F	RRM_KK	0	6	54.00	100	1	128389
4	00:03:7F:00:02:F5	RRM_K	0	6	54.00	100	1	370953
5	00:DE:AD:10:07:00	pramod	1	6	130.00	100	3	609036
6	00:03:7F:0B:A9:A3	sams	0	6	130.00	100	1	454682
7	00:1B:2F:FE:09:E2	NETGEAR	0	11	54.00	100	3	565510
8	00:0F:B5:DE:95:A1	ARADA	1	11	54.00	100	3	647039

At the bottom of the interface, there are buttons for 'REFRESH' and 'SAVE'. The footer indicates 'Copyright © 1996-2007 Netgear ©'.

Figure 3-16

- In the Unknown AP List or the Known AP List sections, click **Refresh** to refresh the corresponding list.
- In the Unknown AP List or the Known AP List sections, click **Save** to export the list of unknown or known APs to a file. A window opens so you can browse to the location where you want to save the file. The default file name is WNDAP330Rogue.cfg.
- Click **Apply** to save your change.

# Chapter 4

## Advanced Configuration

This chapter describes how to configure the advanced features of your ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. The advanced configuration features are located under various sub-menus under Configuration and provide the following functions:

- **IP Settings.** Using the wireless access point as a DHCP server for wireless clients.
- **Hotspot settings.** Enabling HTTP redirect.
- **Wireless Settings:** Configuring advanced wireless LAN parameters.
- **Access Point Settings:** Enabling wireless bridge and repeater modes.

### IP Settings for Wireless Clients

---

You can turn this access point into a DHCP Server for wireless clients for both DHCP-enabled wireless clients as well as for static-IP enabled clients. The default advanced IP wireless settings usually work well. This feature is intended for use by a systems administrator. By default, this feature is not enabled.

To use this wireless access point as a DHCP server:

1. From the main menu under Configuration, select IP, and then select DHCP Server Settings. The DHCP Server Settings screen will display.
2. DHCP Server is disabled by default, as shown in [Figure 4-1](#). Select the Enable radio button to enable this wireless access point as a DHCP server.

**NETGEAR**  
Connect with Innovation™

**WNDAP330**  
ProSafe 11n Dual Band  
Wireless Access Point

LOGOUT

Configuration | Monitoring | Maintenance | Support

System | IP | Wireless | Security | Wireless Bridge

IP Settings  
DHCP Server Settings

### DHCP Server Settings

DHCP Server Settings

DHCP Server ☐ Enable ☒ Disable

DHCP Server VLAN ID

Starting IP Address

Ending IP Address

Subnet Mask

Gateway IP Address

Primary DNS Server

Secondary DNS Server

Primary WINS Server

Secondary WINS Server

Lease  days  hours  minutes

CANCEL APPLY

Copyright © 1996-2007 Netgear

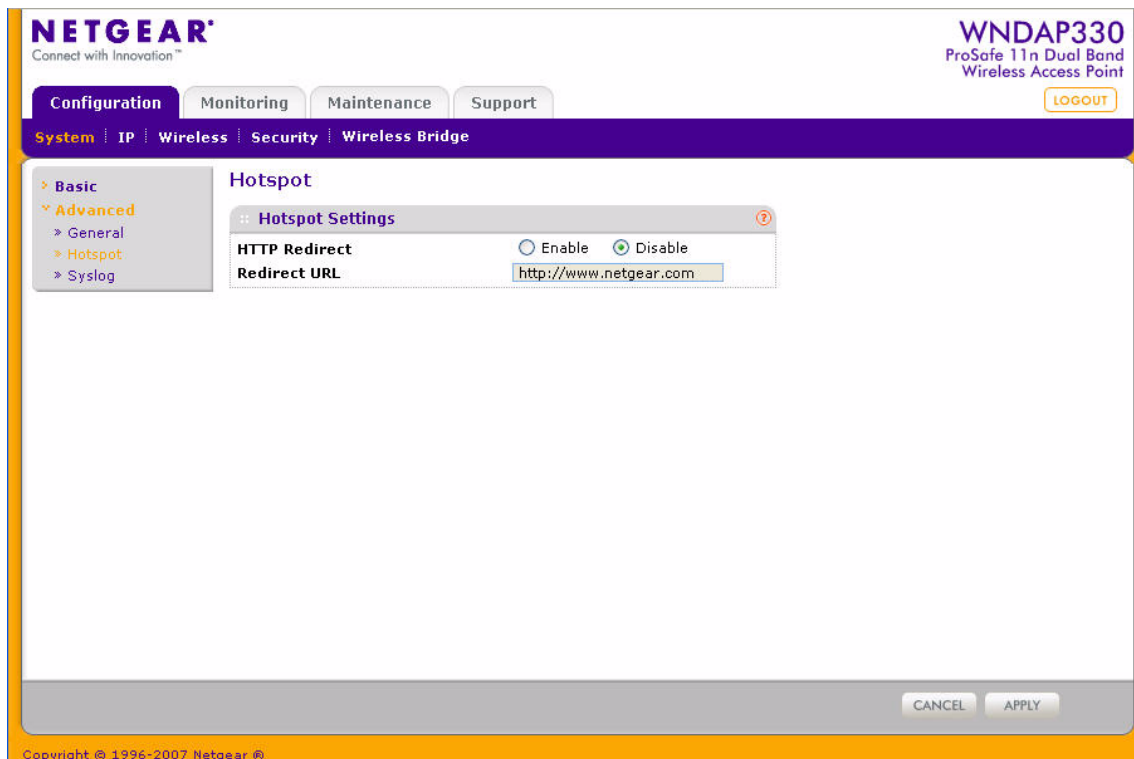
**Figure 4-1**

3. Configure the following TCP/IP configurations for using the WNDAP330 as a DHCP Server for wireless clients.
  - **DHCP Server:** By default, the Dynamic Host Configuration Protocol (DHCP) server 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 WNDAP330 to your LAN.
  - **Starting IP Address:** Enter the starting IP address that can be assigned from the DHCP server on this Access Point.
  - **Ending IP Address:** Enter the Ending IP address that can be assigned from the DHCP server on this Access Point
  - **Subnet Mask:** The Access Point will assign the specified subnet mask to the connected wireless stations.

- **Gateway Address:** The Access Point will assign this IP address as the default gateway for any traffic beyond the local network.
  - **Primary DNS Server:** The Access Point will assign this IP address as the primary Domain Name Server used by the connected wireless stations.
  - **Secondary DNS Server:** The Access Point will assign this IP address as the secondary Domain Name Server used by the connected wireless stations.
  - **Primary WINS Server:** The Access Point will assign this IP address as the primary WINS Server used by the connected wireless stations.
  - **Secondary WINS Server:** The Access Point will assign this IP address as the secondary WINS Server used by the connected wireless stations.
  - **Lease:** The lease time for the IP address assigned. The wireless client user is required to renew the IP address as soon as the lease is expired.
4. Click **Apply** to save your settings.

## Hotspot Settings

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



**Figure 4-2**

To set up a Hotspot server:

1. From the main menu under Configuration, select System, and then select Advanced. The Hotspot screen will display, as shown in [Figure 4-2](#).
2. From the left-hand menu, select Hotspot Settings.
3. Enable HTTP Redirect.
4. Enter the URL of the Web server where you wish to redirect HTTP (port 80) requests.
5. Click **Apply**. All port 80 requests will now be redirected to the specified URL.



## **Configuring Advanced Wireless Settings**

---

The Advanced screen of the Wireless Settings menu is used to configure and enable various wireless LAN parameters for both the 11a/n and 11b/g/n modes. The default wireless LAN parameters usually work well. However, you can use these settings to fine tune the overall performance of your wireless access point for your environment.

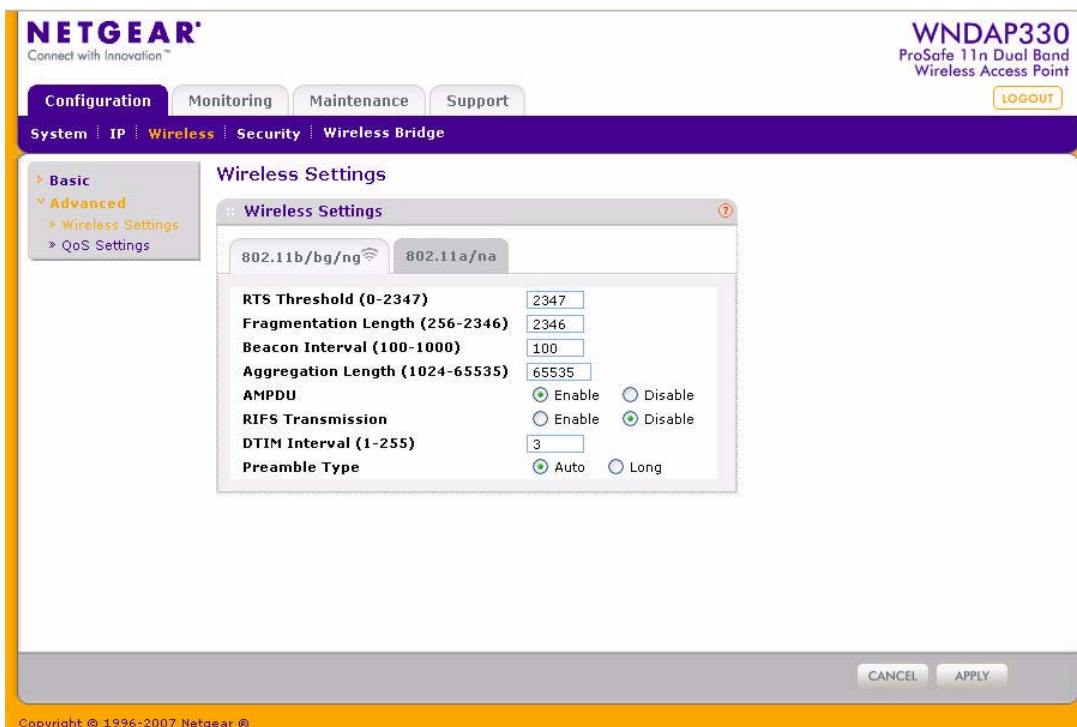
The Wireless Settings option of the Advanced menu is used to configure the Wireless LAN parameters. The default advanced wireless LAN parameter settings usually work well.

### **Configuring 802.11b/g/n Advanced Wireless Settings**

To configure advanced Wireless Settings:

1. Under the Configuration tab, select Wireless.
2. From the left-hand menu, select Advanced, and then select Wireless Settings.

3. Select the 802.11b/g/n tab. The Advanced Wireless Settings screen you selected will display, as shown in [Figure 4-3](#).



**Figure 4-3**

4. Enter the appropriate information in the fields described below:
  - **RTS Threshold (0 - 2347):** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2347.
  - **Fragmentation Length (256 - 2346):** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.

- **Beacon Interval (100 - 1000):** The Beacon Interval. Specifies the interval time between 100ms and 1000ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.
- **Aggregation Length (1024-65535) (11b/g only):** The aggregation length defines the size of aggregated packets. Larger aggregation lengths may sometimes lead to better network performance. The default is 65535.
- **AMPDU (11b/g only):** Aggregated MAC Protocol Data Unit. Aggregates several MAC frames into a single large frame to achieve higher throughput. The default is enabled.
- **RIFS Transmission (11b/g only):** Reduced Interframe Space. RIFS transmissions are shorter than other interframe spaces, and if enabled allow transmission of successive frames at different transmit powers. The default is disabled.
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 3.
- **Preamble Type (11b/g only):** A long transmit preamble may provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto settings automatically handles both long and short preambles. The default is Auto.

5. Click **Apply** to enable the Wireless Settings.

## Configuring 802.11a/n Advanced Wireless Settings

To configure advanced Wireless Settings:

1. Under the Configuration tab, select Wireless.
2. From the left-hand menu, select Advanced, and then select Wireless Settings.

3. Select the 802.11a/n tab. The Advanced Wireless Settings screen you selected will display, as shown in Figure 4-3.,

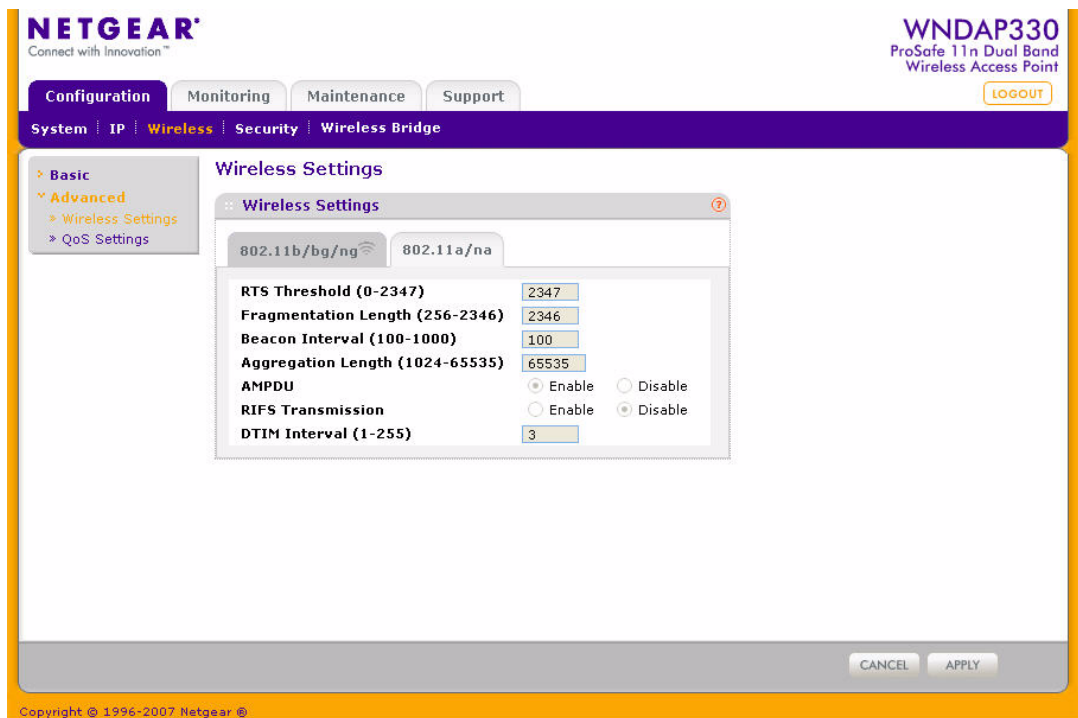


Figure 4-4

4. Enter the appropriate information in the fields described below:
  - **RTS Threshold (0 - 2347):** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2347.
  - **Fragmentation Length (256 - 2346):** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.

- **Beacon Interval (100 - 1000):** The Beacon Interval. Specifies the interval time between 100ms and 1000ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.
- **Aggregation Length (1024-65535) (11n/a only):** The aggregation length defines the size of aggregated packets. Larger aggregation lengths may sometimes lead to better network performance. The default is 65535.
- **AMPDU (11n/a only):** Aggregated MAC Protocol Data Unit. Aggregates several MAC frames into a single large frame to achieve higher throughput. The default is enabled.
- **RIFS Transmission (11n/a only):** Reduced Interframe Space. RIFS transmissions are shorter than other interframe spaces, and if enabled allow transmission of successive frames at different transmit powers. The default is disabled.
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 3.

5. Click **Apply** to enable the Wireless Settings.

## Configuring Advanced QoS Settings

---

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

Figure 4-5 shows the Quality of Service (QoS) screen. For most networks, the default QoS queue parameter settings work well. Quality of Service provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data.

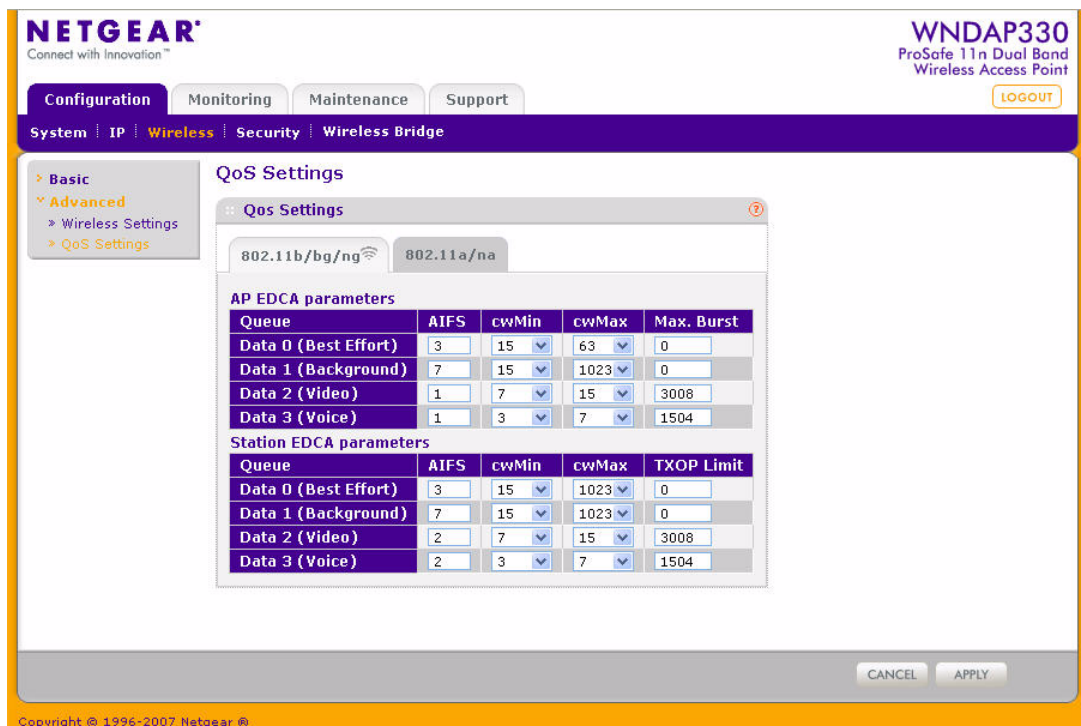


Figure 4-5

The QoS options on the WNDAP330 are as follows:

- **AP EDCA Parameters.** Specify the AP EDCA parameters for different types of data transmitted from the WNDAP330 Wireless Access Point to the wireless client.
- **Station EDCA Parameters.** Specify the Station EDCA parameters for different types of data transmitted from the wireless client to the WNDAP330 Wireless Access Point. If WMM is disabled, you cannot configure Station EDCA parameters.

Table 4-1 describes the settings for QoS Queues.

Table 4-1. QoS Queues and Parameters

QoS Queue	Description
Data 0 (Voice)	High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
Data 1 (Video)	High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.

**Table 4-1. QoS Queues and Parameters (continued)**

QoS Queue	Description
Data 2 (Best Effort)	Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
Data 3 (Background)	Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Arbitration Inter-Frame Space)	Specifies a wait time (in milliseconds) for data frames. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	Upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the “cwmin” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMin must be lower than the value for cwMax.
cwMax (Maximum Contention Window)	Upper limit (in milliseconds) for the doubling of the random backoff value. Valid values for the “cwmax” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMax must be higher than the value for cwMin.
Max. Burst Length	Specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9.

## Enabling Wireless Bridging and Repeating

The ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 lets you build large bridged wireless networks. Select the desired wireless access point mode for your environment:

- **Wireless Point-to-Point Bridge.** In this mode, the WNDAP330 can communicate with another Bridge mode Wireless Station and with Wireless clients if you select the **Enable Wireless Client Association** check box.

When you click the **Edit** button, you must enter the Profile Name and the MAC address (physical address) of the other Bridge mode Wireless Station in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication.

- **Wireless Point-to-Multi-Point Bridge.** Select this only if this WNDAP330 is the “Master” for a group of Bridge-mode Wireless Stations. This mode supports default association with Wireless clients.

The other Bridge-mode Wireless Stations must be set to Point-to-Point Bridge mode, using the MAC address of this WNDAP330. They then send all traffic to this “Master”, rather than communicate directly with each other.

When you click the **Edit** button, you must enter the Profile Name and the MAC address (physical address) of the other Bridge mode Wireless Station in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication.

- **Repeater.** If selected, this wireless access point will operate as a Repeater only, and send all traffic to the remote access point.

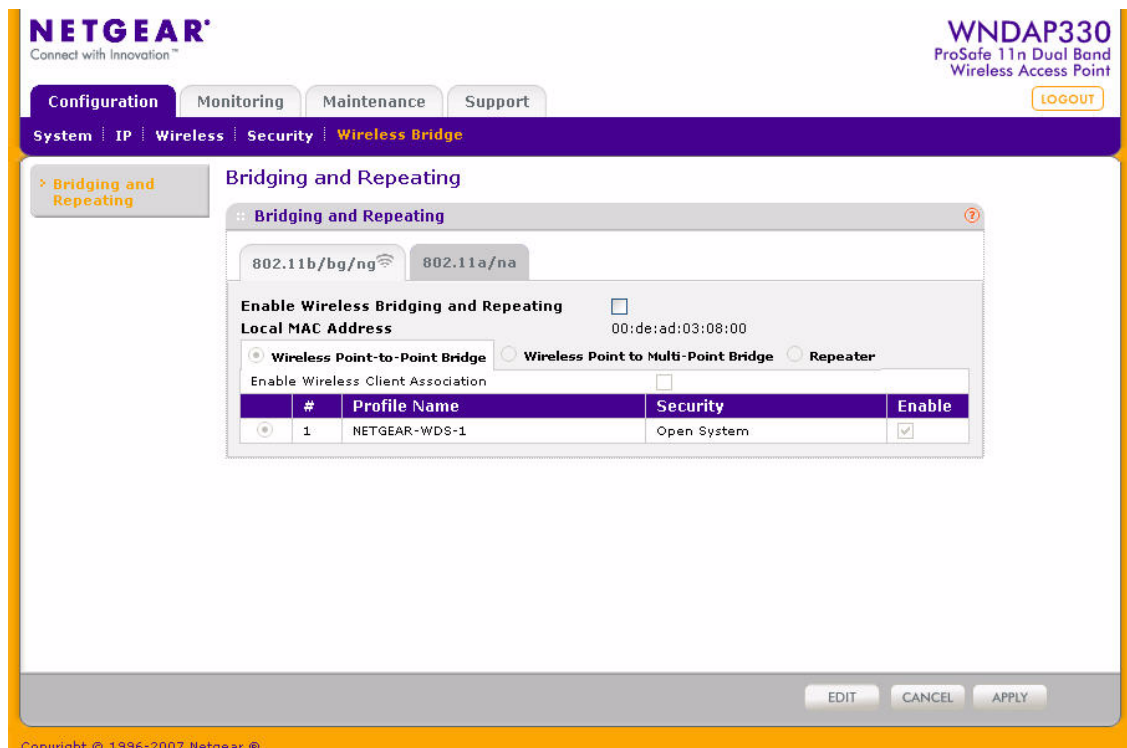


**Note:** This option does not support communication with Wireless clients, that is, Client cannot associate to the AP when it is operating as a Repeater.

When you click the **Edit** button, you must enter the Profile Name and the MAC address (physical address) of the other Bridge mode Wireless Station in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication.

The screens used to configure these options are located by selecting Wireless Bridge on the main menu under the Configuration tab (see [Figure 4-6](#) below).



**Figure 4-6**

On the screens shown in [Figure 4-6](#) above, when you select the radio button for any option, an **Edit** button displays. Click this button to edit the security profile of the wireless bridge settings, as shown in [Figure 4-7](#) below.

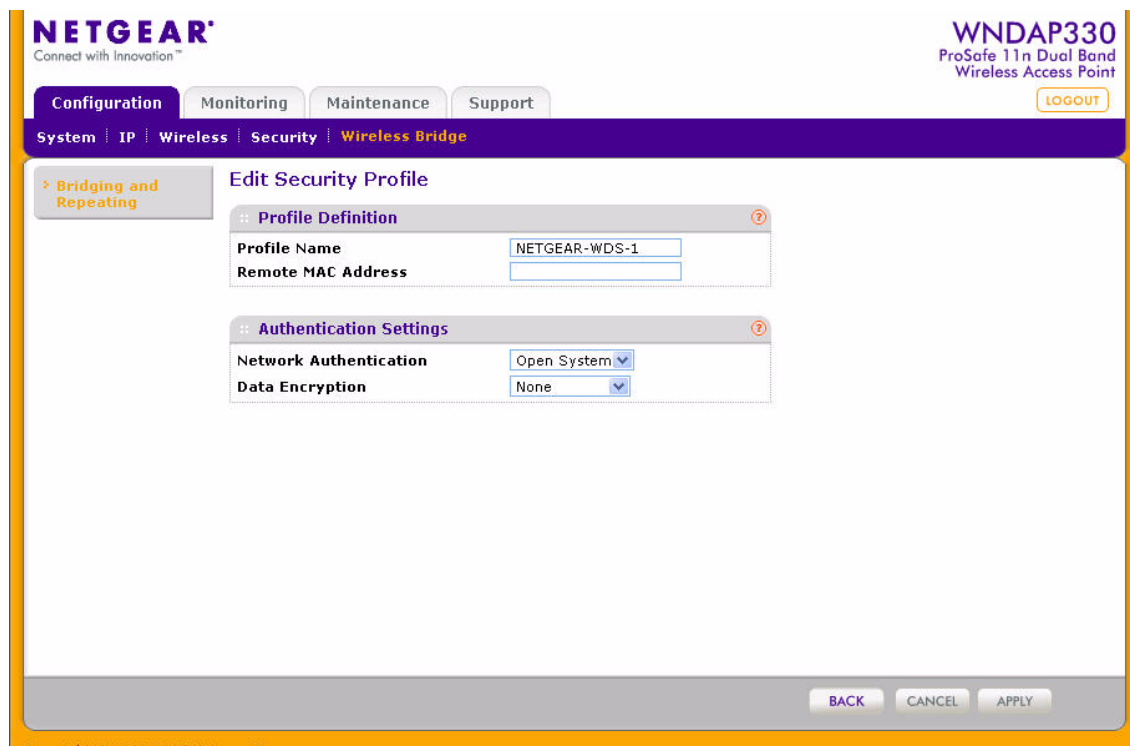
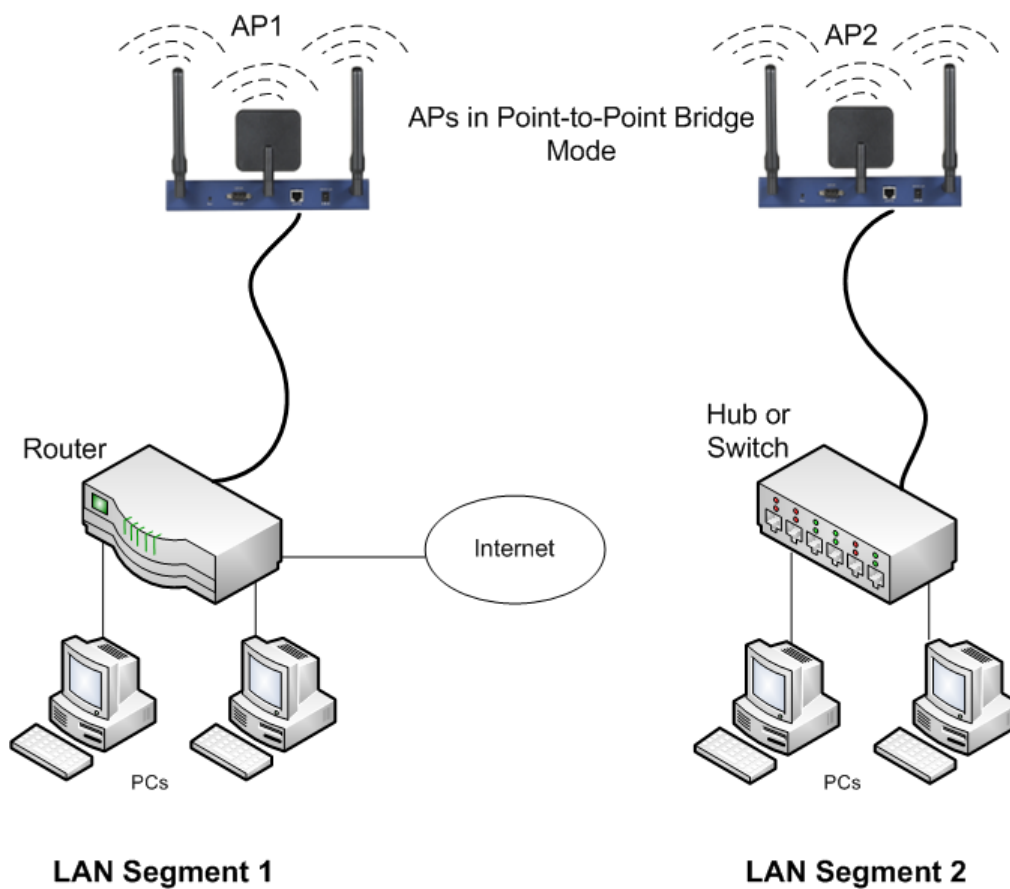


Figure 4-7

## Configuring a WNDAP330 as a Point-to-Point Bridge

To configure a point-to-point bridge as shown in [Figure 4-8](#):

1. Under the Configuration tab, select Wireless Bridge on the main menu. Then, select Bridging and Repeating. The Bridging and Repeating screen will display.
2. Configure the WNDAP330 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.

**Figure 4-8**

3. Configure the WNDAP330 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.  
AP1 must have AP2's MAC address in its Remote MAC Address field and AP2 must have AP1's MAC address in its Remote MAC Address field.
4. Configure and verify the following parameters for both access points:
  - Verify that the LAN network configuration of the WNDAP330 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices
  - Both use the same ESSID, Channel, authentication mode, if any, and security settings if security is in use.

5. Verify connectivity across the LAN 1 and LAN 2.

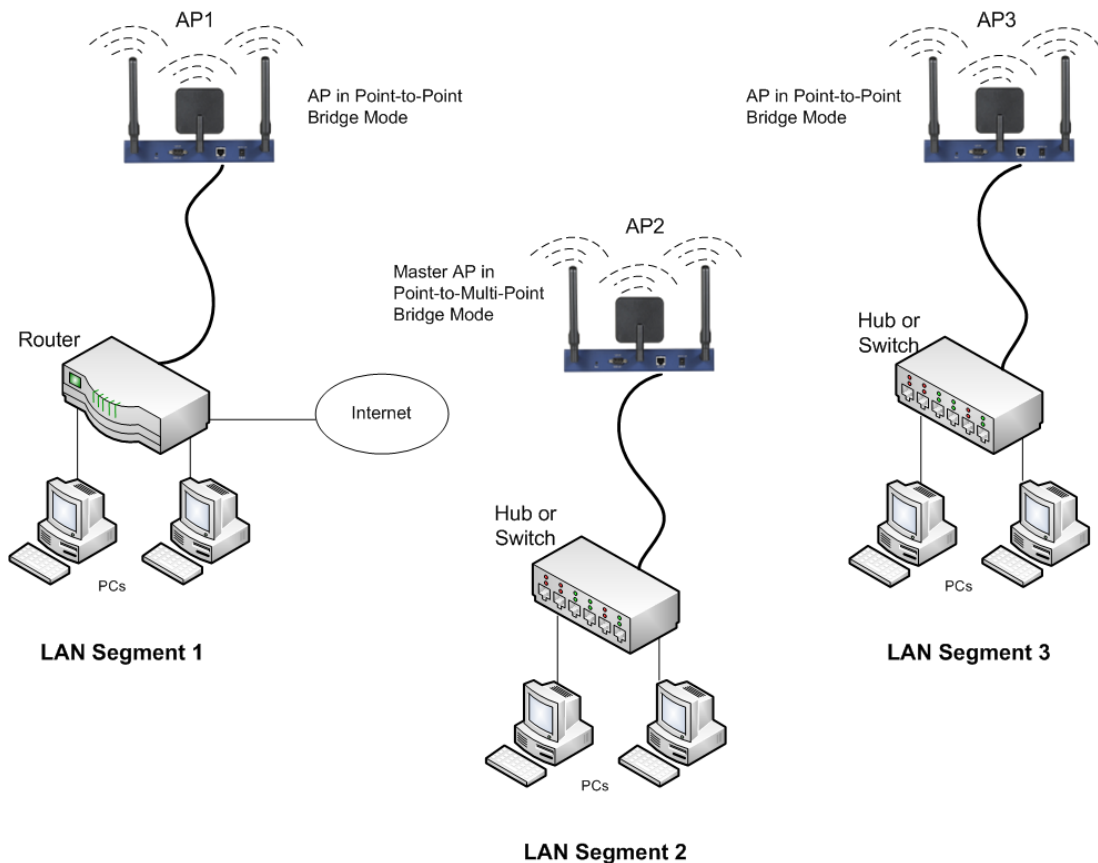
A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

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

## Configuring a Point-to-Multi-Point Wireless Bridge

To configure a point-to-multi-point wireless bridge as shown in [Figure 4-9](#):

1. Under the Configuration tab, select Wireless Bridge on the main menu. Then, select Bridging and Repeating. The Bridging and Repeating screen will display.



**Figure 4-9**

2. Configure the Operating Mode of the WNDAP330 Wireless Access Points.

- WNDAP330 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
  - Because it is in the central location, configure WNDAP330 (AP2) on LAN Segment 2 in Point-to-Multi-Point Bridge mode. The MAC addresses of the adjacent APs are required in AP2.
  - Configure the WNDAP330 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
3. Verify the following parameters for all access points:
- Verify that the LAN network configuration the WNDAP330 Wireless Access Points are configured to operate in the same LAN network address range as the LAN devices
  - Only one access point is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
  - All access points must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
  - If using DHCP, all WNDAP330 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.
  - All WNDAP330 Wireless Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
  - All Point-to-Point Access Points must have the AP2 MAC address in its Remote AP MAC address field.
4. Verify connectivity across the LANs.
- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
  - Wireless stations will be able to connect to the WNDAP330 Wireless Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can add additional WNDAP330 Wireless Access Points configured in Wireless Access Point mode to any LAN segment.
5. Click **Apply** to save your settings.

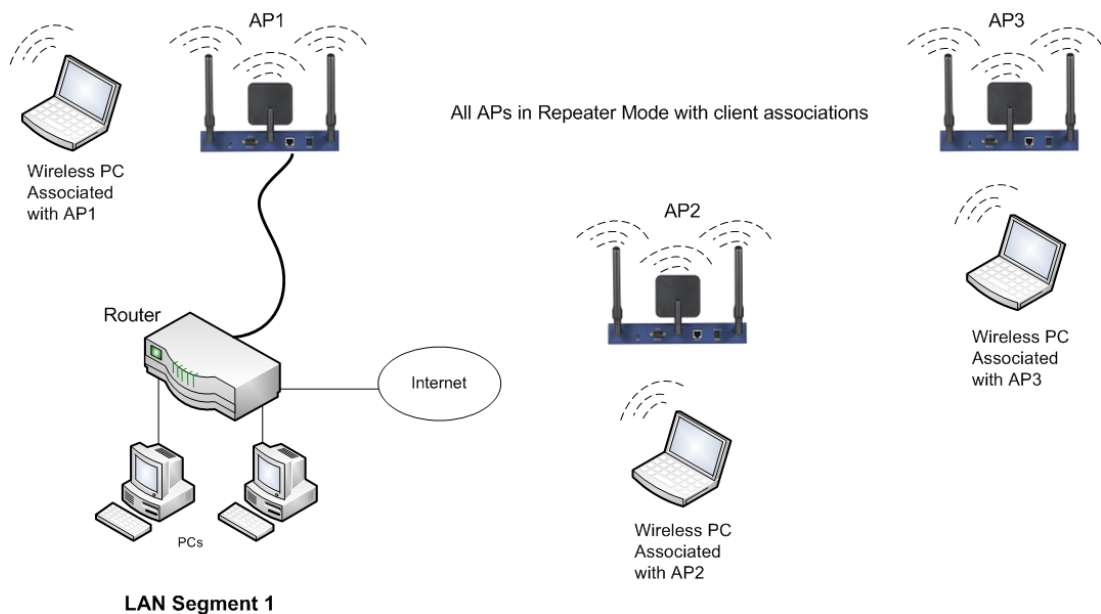


**Note:** You can extend this multi-point bridging by adding additional WNDAP330s configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

## Configuring the WNDAP330 as a Wireless Repeater

To configure the WNDAP330 as a Wireless Repeater as shown in [Figure 4-10](#):

1. Under the Configuration tab, select Wireless Bridge on the main menu. Then, select Bridging and Repeating. The Bridging and Repeating screen will display.
2. Configure the Operating Mode of the WNDAP330 Wireless Access Points.
  - WNDAP330 (AP1) on LAN Segment 1 in Repeater mode with the Remote MAC Address of AP2.
  - Configure WNDAP330 (AP2) in Repeater mode with MAC addresses of AP1 and AP3.
  - Configure the WNDAP330 (AP3) in Repeater mode with the Remote MAC Address of AP2.



**Figure 4-10**

3. Verify the following parameters for all access points:
  - Verify that the LAN network configuration the WNDAP330 Wireless Access Points are configured to operate in the same LAN network address range as the LAN devices.
  - All access points must be on the same LAN. That is, all the LAN IP addresses of the access points must be in the same network.

- If using DHCP, all WNDAP330 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.
- All WNDAP330 Wireless Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.

**4.** 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.

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



**Note:** You can extend repeating by adding up to two additional WNDAP330s configured in repeater mode. However, since Repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add Repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.





# Chapter 5

## Troubleshooting and Debugging

This chapter provides information about troubleshooting your ProSafe 802.11n Dual Band Wireless Access Point WNDAP330. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WNDAP330 on?

Go to “[Installing the WNDAP330 Wireless Access Point](#)” on page 2-4

- Have I connected the wireless access point correctly?

Go to “[Installing the WNDAP330 Wireless Access Point](#)” on page 2-4.

- I cannot remember the wireless access point’s configuration password.

Go to “[Changing the Administrator Password](#)” on page 3-10.



**Note:** For up-to-date WNDAP330 installation details and troubleshooting guidance visit <http://kbserver.netgear.com/products/WG302.asp>.

If you have trouble setting up your WNDAP330, check the tips below.

### No lights are lit on the wireless access point.

---

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

If the access point has no power.

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

## **The Wireless LAN activity light does not light up.**

---

The access point antennas are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the WNDAP330.
- Contact NETGEAR technical support if the Wireless LAN activity light remains off.

## **The LAN light is not lit.**

---

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- LAN light does not light up if it is a 10 Mbps link. In such cases, the Lan activity light will still blink if there is activity.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

## **I cannot access the Internet or the LAN with a wireless capable computer.**

---

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to “Obtain an IP address automatically.”

- The access point's default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

## **I cannot connect to the WNDAP330 to configure it.**

---

Check these items:

- The WNDAP330 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the WNDAP330 is for a static IP address of 192.168.0.230 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the WNDAP330 to connect, ensure that your computer and the WNDAP330 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WNDAP330. The WNDAP330 default IP Address is 192.168.0.230 and the default Subnet Mask is 255.255.255.0. If you are not sure about these settings, follow the instructions for ["Installing the WNDAP330 Wireless Access Point" on page 2-4.](#)

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

---

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

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WNDAP330 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 WNDAP330 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

## Using the Reset Button to Restore Factory Default Settings

---

The Reset button (see [“Rear Panel” on page 1-10](#)) has two functions:

- **Reboot.** When pressed and released quickly, the WNDAP330 will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WNDAP330 and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Release the Reset button.

The factory default configuration has now been restored, and the WNDAP330 is ready for use.

# Appendix A

## Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the ProSafe 802.11n Dual Band Wireless Access Point WNDAP330.

### 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 TEST LED blinks rapidly). 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	192.168.0.230
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Connection		
	Static IP Address	192.168.0.210
	Ethernet MAC Address	See bottom label.
	Port Speed	10/100/1000
Local Network (LAN)		
	Lan IP	192.168.0.230
	Subnet Mask	255.255.255.0
	Gateway Address	0.0.0.0
	DHCP Server	Disabled

**Table A-1. Access Point Default Configuration Settings (continued)**

Feature		Description
	DHCP Client	Disabled
	Time Zone	USA-Pacific
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Enabled, but Trap forwarding disabled
	Spanning Tree Protocol	Disabled
	Secure Telnet	Enabled
Wireless		
	Operating Mode	Access Point
	Access Point Name	netgearxxxxxx where xxxxxx are the last 6 digits of the wireless access point MAC address.
	Wireless Communication	Enabled
	11a/n Wireless Network Name (SSID)	NETGEAR_11a
	11 b/g/n Wireless Network Name (SSID)	NETGEAR_11g
	Broadcast Network Name SSID	Enabled
	Security	Disabled
	Transmission Speed	Best <sup>a</sup>
	Country/Region	Varies by region
	80211.a Radio Frequency Channel	Auto
	80211.g Radio Frequency Channel	Auto
	Output Power	Full
	Wireless Card Access List	All wireless stations allowed
	WMM Support	Enabled

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. WNDAP330 Technical Specifications**

Parameter	ProSafe 802.11n Dual Band Wireless Access Point WNDAP330
802.11a Data Rates	6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11na Data Rates	Data Rates for Channel Width=20MHz and Guard Interval=short (400ms): Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
	Data Rates for Channel Width=20MHz and Guard Interval=long (800ms): Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
	Data Rates for Channel Width=40MHz and Guard Interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
	Data Rates for Channel Width=40MHz and Guard Interval=long: Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
802.11a/na Operating Frequencies	5.15 ~ 5.25 5.25 ~ 5.35 5.57 ~ 5.825
802.11a/na Encryption	64-bits, 128- and 152-bits WEP, AES, TKIP data encryption
802.11g Data Rates	1, 2, 5.5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable)
802.11ng Data Rates	Data Rates for Channel Width=20MHz and Guard Interval=short (400ms): Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
	Data Rates for Channel Width=20MHz and Guard Interval=long (800ms): Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
	Data Rates for Channel Width=40MHz and Guard Interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps

**Table A-2. WNDAP330 Technical Specifications**

Parameter	ProSafe 802.11n Dual Band Wireless Access Point WNDAP330
	Data Rates for Channel Width=40MHz and Guard Interval=long: Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
802.11b/bg/ng 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)
802.11 b/bg/ng Encryption	64-bits, 128- and 152-bits WEP, AES, TKIP data encryption
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; maximum 64 supported.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1.5 A
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	<a href="http://documentation.netgear.com/reference/enu/tcpip/index.htm">http://documentation.netgear.com/reference/enu/tcpip/index.htm</a>
Wireless Communications	<a href="http://documentation.netgear.com/reference/enu/wireless/index.htm">http://documentation.netgear.com/reference/enu/wireless/index.htm</a>
Preparing a Computer for Network Access	<a href="http://documentation.netgear.com/reference/enu/wsdhcp/index.htm">http://documentation.netgear.com/reference/enu/wsdhcp/index.htm</a>
Glossary	<a href="http://documentation.netgear.com/reference/enu/glossary/index.htm">http://documentation.netgear.com/reference/enu/glossary/index.htm</a>



# Appendix C

## Command Line Reference

The ProSafe 802.11n Dual Band Wireless Access Point WNDAP330 (AP) can be configured either through the command line interface (CLI), a Web browser, or an MIB browser. The CLI allows viewing and modification of the configuration from a terminal or PC through a telnet connection.

### Command Sets

---

keyword	Description
-----	-----
-backup-configuration	--backup configuration
-config>	--configuration setting
-apname	--access point name
-country	--country/region
-dhcp>	--DHCP server
-dns-server	--DNS server
-gateway	--default gateway
-ip-address	--IP range
-lease-time	--lease time
-status	--status
-subnet-mask	--subnet mask
-wins-server	--WINS server
-http-redirect	--enable HTTP redirection
-http-redirect-url	--HTTP redirection URL
-interface>	--select wireless lan interface
-wlan>	--wireless LAN interface setting
-2.4GHz>	--2.4 GHz wireless LAN interface setting
-aggregation-length	--aggregated packet size
-ampdu	--aggregated MAC Protocol Data Unit
-beacon-interval	--wireless beacon period in TU(1024 us)
-channel	--wireless channel (depends on country
and wireless mode)	
-channelwidth	--wireless channel width
-dtim-interval	--wireless DTIM period in beacon interval
-extension-protection-spacing	--wireless extension protection spacing
-fragmentation-length	--wireless fragmentation threshold(even
only)	

```
| | | | -guardinterval          --interval (from interference from other
transmissions)
| | | | -knownap-add            --add known access point
| | | | -knownap-del            --delete known access point
| | | | -macacl-add             --add wireless access control (ACL)
| | | | -macacl-database        --delete wireless access control (ACL)
database
| | | | -macacl-del             --delete wireless access control (ACL)
| | | | -mcsrate                --transmit data rate
| | | | -mode                   --enable wireless access control (ACL)
| | | | -operation-mode         --wireless operation mode
| | | | -power                  --wireless transmit power
| | | | -preamble               --wireless preamble (only effect on
802.11b rates)
| | | | -radio                  --enable wireless radio
| | | | -rate                   --wireless transmission data rate
| | | | -rifs-transmission       --enable successive frame transmission at
different transmit powers
| | | | -rogue-ap-detection      --enable rogue access point detection
| | | | -rts-threshold          --wireless RTS/CTS threshold
| | | | -security-profile>      --create security profile
| | | | | -1>                   --1st security profile
| | | | | | -authentication      --authentication type
| | | | | | -encryption          --data encryption
| | | | | | -hide-network-name   --hide network name
| | | | | | -key1                --wireless wep key 1
| | | | | | -key2                --wireless wep key 2
| | | | | | -key3                --wireless wep key 3
| | | | | | -key4                --wireless wep key 4
| | | | | | -keyno               --key number
| | | | | | -name                --profile name
| | | | | | -presharedkey        --pre-shared key
| | | | | -security-separation   --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -2>                 --2nd security profile
| | | | | | | -authentication    --authentication type
| | | | | | | -encryption        --data encryption
| | | | | | | -hide-network-name --hide network name
| | | | | | | -key1              --wireless wep key 1
| | | | | | | -key2              --wireless wep key 2
| | | | | | | -key3              --wireless wep key 3
| | | | | | | -key4              --wireless wep key 4
```

```

| | | | | | -keyno          --key number
| | | | | | -name          --profile name
| | | | | | -presharedkey   --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid          --network name (1-32 chars)
| | | | | | -status        --profile status
| | | | | | -vlan-id       --VLAN id
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkeytype     --wireless wep key type
| | | | | |
| | | | | | -3>           --3rd security profile
| | | | | | -authentication --authentication type
| | | | | | -encryption     --data encryption
| | | | | | -hide-network-name --hide network name
| | | | | | -key1           --wireless wep key 1
| | | | | | -key2           --wireless wep key 2
| | | | | | -key3           --wireless wep key 3
| | | | | | -key4           --wireless wep key 4
| | | | | | -keyno          --key number
| | | | | | -name          --profile name
| | | | | | -presharedkey   --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid          --network name (1-32 chars)
| | | | | | -status        --profile status
| | | | | | -vlan-id       --VLAN id
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkeytype     --wireless wep key type
| | | | | |
| | | | | | -4>           --4th security profile
| | | | | | -authentication --authentication type
| | | | | | -encryption     --data encryption
| | | | | | -hide-network-name --hide network name
| | | | | | -key1           --wireless wep key 1
| | | | | | -key2           --wireless wep key 2
| | | | | | -key3           --wireless wep key 3
| | | | | | -key4           --wireless wep key 4
| | | | | | -keyno          --key number
| | | | | | -name          --profile name
| | | | | | -presharedkey   --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid          --network name (1-32 chars)
| | | | | | -status        --profile status
| | | | | | -vlan-id       --VLAN id
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkeytype     --wireless wep key type

```

```
| | | | | |
| | | | | | -5>                --5th security profile
| | | | | | | -authentication    --authentication type
| | | | | | | | -encryption      --data encryption
| | | | | | | | -hide-network-name --hide network name
| | | | | | | | -key1            --wireless wep key 1
| | | | | | | | -key2            --wireless wep key 2
| | | | | | | | -key3            --wireless wep key 3
| | | | | | | | -key4            --wireless wep key 4
| | | | | | | | | -keyno         --key number
| | | | | | | | | -name          --profile name
| | | | | | | | | -presharedkey  --pre-shared key
| | | | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | | -ssid              --network name (1-32 chars)
| | | | | | | | -status          --profile status
| | | | | | | | | -vlan-id       --VLAN id
| | | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | | -wepkeytype    --wireless wep key type
| | | | | | |
| | | | | | | -6>                --6th security profile
| | | | | | | | -authentication    --authentication type
| | | | | | | | | -encryption      --data encryption
| | | | | | | | | -hide-network-name --hide network name
| | | | | | | | | -key1            --wireless wep key 1
| | | | | | | | | -key2            --wireless wep key 2
| | | | | | | | | -key3            --wireless wep key 3
| | | | | | | | | -key4            --wireless wep key 4
| | | | | | | | | -keyno         --key number
| | | | | | | | | -name          --profile name
| | | | | | | | | -presharedkey  --pre-shared key
| | | | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | | -ssid              --network name (1-32 chars)
| | | | | | | | -status          --profile status
| | | | | | | | | -vlan-id       --VLAN id
| | | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | | -wepkeytype    --wireless wep key type
| | | | | | |
| | | | | | | -7>                --7th security profile
| | | | | | | | -authentication    --authentication type
| | | | | | | | | -encryption      --data encryption
| | | | | | | | | -hide-network-name --hide network name
| | | | | | | | | -key1            --wireless wep key 1
| | | | | | | | | -key2            --wireless wep key 2
| | | | | | | | | -key3            --wireless wep key 3
| | | | | | | | | -key4            --wireless wep key 4
| | | | | | | | | -keyno         --key number
```

```

| | | | | | -name --profile name
| | | | | | -presharedkey --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid --network name (1-32 chars)
| | | | | | -status --profile status
| | | | | | -vlan-id --VLAN id
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkeytype --wireless wep key type
| | | | | |
| | | | | | -8> --8th security profile
| | | | | | | -authentication --authentication type
| | | | | | | -encryption --data encryption
| | | | | | | -hide-network-name --hide network name
| | | | | | | -key1 --wireless wep key 1
| | | | | | | -key2 --wireless wep key 2
| | | | | | | -key3 --wireless wep key 3
| | | | | | | -key4 --wireless wep key 4
| | | | | | | -keyno --key number
| | | | | | | -name --profile name
| | | | | | | -presharedkey --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid --network name (1-32 chars)
| | | | | | -status --profile status
| | | | | | -vlan-id --VLAN id
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkeytype --wireless wep key type
| | | | | |
| | | | | | -wireless-bridge> --wireless bridge setting
| | | | | | | -security-profile> --create security profile
| | | | | | | | -1> --1st security profile
| | | | | | | | | -authentication --authentication type
| | | | | | | | | -encryption --data encryption
| | | | | | | | | -name --profile name
| | | | | | | | | -presharedkey --preshared key
| | | | | | | | | -remote-mac --remote MAC
| | | | | | | | | -status --profile status
| | | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | | -wepkey --wireless wep key
| | | | | | | | | -wepkeytype --wireless wep key type
| | | | | | |
| | | | | | | -2> --2nd security profile
| | | | | | | | -authentication --authentication type
| | | | | | | | -encryption --data encryption
| | | | | | | | -name --profile name
| | | | | | | | -presharedkey --preshared key

```

```
| | | | | | | -remote-mac      --remote MAC
| | | | | | | -status      --profile status
| | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | -wepkey      --wireless wep key
| | | | | | | -wepkeytype  --wireless wep key type
| | | | | | |
| | | | | | | -3>          --3rd security profile
| | | | | | | | -authentication --authentication type
| | | | | | | | -encryption   --data encryption
| | | | | | | | -name        --profile name
| | | | | | | | -presharedkey --preshared key
| | | | | | | | -remote-mac  --remote MAC
| | | | | | | | -status      --profile status
| | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | -wepkey      --wireless wep key
| | | | | | | | -wepkeytype  --wireless wep key type
| | | | | | |
| | | | | | | -4>          --4th security profile
| | | | | | | | -authentication --authentication type
| | | | | | | | -encryption   --data encryption
| | | | | | | | -name        --profile name
| | | | | | | | -presharedkey --preshared key
| | | | | | | | -remote-mac  --remote MAC
| | | | | | | | -status      --profile status
| | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | -wepkey      --wireless wep key
| | | | | | | | -wepkeytype  --wireless wep key type
| | | | | | |
| | | | | | |
| | | | | | | -wmm>          --wmm settings
| | | | | | | | -ap-data0-best-effort --access point best effort voice data
| | | | | | | | -ap-data1-background  --access point low-priority data
| | | | | | | | -ap-data2-video      --access point video data
| | | | | | | | -ap-data3-voice      --access point voice data
| | | | | | | | -station-data0-best-effort --station best effort voice data
| | | | | | | | -station-data1-background --station low-priority data
| | | | | | | | -station-data2-video    --station video data
| | | | | | | | -station-data3-voice  --station voice data
| | | | | | | | -support          --support
| | | | | | |
| | | | | | |
| | | | | | | -5GHz>        --5 GHz wireless LAN interface setting
| | | | | | | | -aggregation-length --aggregated packet size
| | | | | | | | -ampdu          --aggregated MAC Protocol Data Unit
| | | | | | | | -beacon-interval  --wireless beacon period in TU(1024 us)
| | | | | | | | -channel          --wireless channel (depends on country and
wireless mode)
```



```

| | | | -channelwidth          --wireless channel width
| | | | -dtim-interval         --wireless DTIM period in beacon interval
| | | | -extension-protection-spacing  --wireless extension protection spacing
| | | | -fragmentation-length   --wireless fragmentation threshold(even
only)
| | | | -guardinterval         --interval (from interference from other
transmissions)
| | | | -knownap-add           --add known access point
| | | | -knownap-del          --delete known access point
| | | | | -macacl>            --modify wireless access control (ACL)
| | | | | | -add              --add wireless access control (ACL)
| | | | | | -del              --delete wireless access control (ACL)
| | | | |
| | | | | -macacl-add          --add wireless access control (ACL)
| | | | | -macacl-database     --delete wireless access control (ACL)
database
| | | | | -macacl-del          --delete wireless access control (ACL)
| | | | | -mcsrata            --transmit data rate
| | | | | -mode               --enable wireless access control (ACL)
| | | | | -operation-mode      --wireless operation mode
| | | | | -power              --wireless transmit power
| | | | | -radio              --enable wireless radio
| | | | | -rate               --wireless transmission data rate
| | | | | -rifs-transmission   --enable successive frame transmission at
different transmit powers
| | | | | -rogue-ap-detection   --enable rogue access point detection
| | | | | -rts-threshold       --wireless RTS/CTS threshold
| | | | | -security-profile>   --create security profile
| | | | | | -1>              --1st security profile
| | | | | | | -authentication  --authentication type
| | | | | | | -encryption      --data encryption
| | | | | | | -hide-network-name --hide network name
| | | | | | | -key1            --wireless wep key 1
| | | | | | | -key2            --wireless wep key 2
| | | | | | | -key3            --wireless wep key 3
| | | | | | | -key4            --wireless wep key 4
| | | | | | | -keyno           --key number
| | | | | | | -name            --profile name
| | | | | | | -presharedkey     --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | | -ssid            --network name (1-32 chars)
| | | | | | | -status          --profile status
| | | | | | | -vlan-id         --VLAN id
| | | | | | | -wep-pass-phrase  --wireless wep passphrase key
| | | | | | | -wepkeytype      --wireless wep key type
| | | | | |
| | | | | | -2>              --2nd security profile

```

```
| | | | | | -authentication      --authentication type
| | | | | | -encryption        --data encryption
| | | | | | -hide-network-name   --hide network name
| | | | | | -key1              --wireless wep key 1
| | | | | | -key2              --wireless wep key 2
| | | | | | -key3              --wireless wep key 3
| | | | | | -key4              --wireless wep key 4
| | | | | | -keyno             --key number
| | | | | | -name              --profile name
| | | | | | -presharedkey       --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid              --network name (1-32 chars)
| | | | | | -status            --profile status
| | | | | | -vlan-id           --VLAN id
| | | | | | -wep-pass-phrase    --wireless wep passphrase key
| | | | | | -wepkeytype        --wireless wep key type
| | | | | |
| | | | | | -3>                --3rd security profile
| | | | | | | -authentication    --authentication type
| | | | | | | -encryption        --data encryption
| | | | | | | -hide-network-name  --hide network name
| | | | | | | -key1              --wireless wep key 1
| | | | | | | -key2              --wireless wep key 2
| | | | | | | -key3              --wireless wep key 3
| | | | | | | -key4              --wireless wep key 4
| | | | | | | -keyno             --key number
| | | | | | | -name              --profile name
| | | | | | | -presharedkey       --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid              --network name (1-32 chars)
| | | | | | -status            --profile status
| | | | | | -vlan-id           --VLAN id
| | | | | | -wep-pass-phrase    --wireless wep passphrase key
| | | | | | -wepkeytype        --wireless wep key type
| | | | | |
| | | | | | -4>                --4th security profile
| | | | | | | -authentication    --authentication type
| | | | | | | -encryption        --data encryption
| | | | | | | -hide-network-name  --hide network name
| | | | | | | -key1              --wireless wep key 1
| | | | | | | -key2              --wireless wep key 2
| | | | | | | -key3              --wireless wep key 3
| | | | | | | -key4              --wireless wep key 4
| | | | | | | -keyno             --key number
| | | | | | | -name              --profile name
| | | | | | | -presharedkey       --pre-shared key
```

```

| | | | | | -security-separation  --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -5>                  --5th security profile
| | | | | | | -authentication     --authentication type
| | | | | | | -encryption         --data encryption
| | | | | | | -hide-network-name  --hide network name
| | | | | | | -key1               --wireless wep key 1
| | | | | | | -key2               --wireless wep key 2
| | | | | | | -key3               --wireless wep key 3
| | | | | | | -key4               --wireless wep key 4
| | | | | | | -keyno              --key number
| | | | | | | -name                --profile name
| | | | | | | -presharedkey        --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -6>                  --6th security profile
| | | | | | | -authentication     --authentication type
| | | | | | | -encryption         --data encryption
| | | | | | | -hide-network-name  --hide network name
| | | | | | | -key1               --wireless wep key 1
| | | | | | | -key2               --wireless wep key 2
| | | | | | | -key3               --wireless wep key 3
| | | | | | | -key4               --wireless wep key 4
| | | | | | | -keyno              --key number
| | | | | | | -name                --profile name
| | | | | | | -presharedkey        --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -7>                  --7th security profile
| | | | | | | -authentication     --authentication type

```

```
| | | | | | -encryption          --data encryption
| | | | | | -hide-network-name    --hide network name
| | | | | | -key1                --wireless wep key 1
| | | | | | -key2                --wireless wep key 2
| | | | | | -key3                --wireless wep key 3
| | | | | | -key4                --wireless wep key 4
| | | | | | -keyno              --key number
| | | | | | -name                --profile name
| | | | | | -presharedkey        --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -8>                 --8th security profile
| | | | | | -authentication      --authentication type
| | | | | | -encryption          --data encryption
| | | | | | -hide-network-name    --hide network name
| | | | | | -key1                --wireless wep key 1
| | | | | | -key2                --wireless wep key 2
| | | | | | -key3                --wireless wep key 3
| | | | | | -key4                --wireless wep key 4
| | | | | | -keyno              --key number
| | | | | | -name                --profile name
| | | | | | -presharedkey        --pre-shared key
| | | | | | -security-separation --disable associated wireless client
communication
| | | | | | -ssid                --network name (1-32 chars)
| | | | | | -status              --profile status
| | | | | | -vlan-id             --VLAN id
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkeytype          --wireless wep key type
| | | | | |
| | | | | | -wireless-bridge>    --wireless bridge setting
| | | | | | -security-profile>   --create security profile
| | | | | | -1>                 --1st security profile
| | | | | | -authentication      --authentication type
| | | | | | -encryption          --data encryption
| | | | | | -name                --profile name
| | | | | | -presharedkey        --preshared key
| | | | | | -remote-mac          --remote MAC
| | | | | | -status              --profile status
| | | | | | -wep-pass-phrase     --wireless wep passphrase key
| | | | | | -wepkey              --wireless wep key
```

```

| | | | | | | -wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | | -2>                --2nd security profile
| | | | | | | | -authentication    --authentication type
| | | | | | | | -encryption        --data encryption
| | | | | | | | -name              --profile name
| | | | | | | | -presharedkey      --preshared key
| | | | | | | | -remote-mac        --remote MAC
| | | | | | | | -status            --profile status
| | | | | | | | -wep-pass-phrase   --wireless wep passphrase key
| | | | | | | | -wepkey            --wireless wep key
| | | | | | | | -wepkeytype        --wireless wep key type
| | | | | | |
| | | | | | | -3>                --3rd security profile
| | | | | | | | -authentication    --authentication type
| | | | | | | | -encryption        --data encryption
| | | | | | | | -name              --profile name
| | | | | | | | -presharedkey      --preshared key
| | | | | | | | -remote-mac        --remote MAC
| | | | | | | | -status            --profile status
| | | | | | | | -wep-pass-phrase   --wireless wep passphrase key
| | | | | | | | -wepkey            --wireless wep key
| | | | | | | | -wepkeytype        --wireless wep key type
| | | | | | |
| | | | | | | -4>                --4th security profile
| | | | | | | | -authentication    --authentication type
| | | | | | | | -encryption        --data encryption
| | | | | | | | -name              --profile name
| | | | | | | | -presharedkey      --preshared key
| | | | | | | | -remote-mac        --remote MAC
| | | | | | | | -status            --profile status
| | | | | | | | -wep-pass-phrase   --wireless wep passphrase key
| | | | | | | | -wepkey            --wireless wep key
| | | | | | | | -wepkeytype        --wireless wep key type
| | | | | | |
| | | | | | | -wmm>              --wmm settings
| | | | | | | | -ap-data0-best-effort --access point best effort voice data
| | | | | | | | -ap-data1-background --access point low-priority data
| | | | | | | | -ap-data2-video      --access point video data
| | | | | | | | -ap-data3-voice     --access point voice data
| | | | | | | | -station-data0-best-effort --station best effort voice data
| | | | | | | | -station-data1-background --station low-priority data
| | | | | | | | -station-data2-video  --station video data
| | | | | | | | -station-data3-voice  --station voice data
| | | | | | | | -support            --???

```

```

| | |
| | |
| | |
| -ip> --set host IP
| | -address --host IP address
| | -default-gateway --IP address of default gateway
| | -dhcp-client --enable dhcp client
| | -dns-server --IP address of DNS server
|
| -log> --syslog setting
| | -syslog --enable syslog client
| | -syslog-server-ip --syslog server IP address
| | -syslog-server-port --syslog server port number
|
| -radius>
| | -accounting-server-primary --primary accounting server
| | -accounting-server-primary-port --primary accounting server port
| | -accounting-server-primary-sharedsecret --primary accounting server shared
secret
| | -accounting-server-secondary --secondary accounting server
| | -accounting-server-secondary-port --secondary accounting server port
| | -accounting-server-secondary-sharedsecret --secondary accounting server
shared secret
| | -authentication-server-primary --primary authentication server
| | -authentication-server-primary-port --primary system accounting
server shared secret
| | -authentication-server-primary-sharedsecret --primary authentication
server shared secret
| | -authentication-server-secondary --secondary authentication server
port
| | -authentication-server-secondary-port --secondary authentication server
port
| | -authentication-server-secondary-sharedsecret --secondary authentication
server shared secret
| |
| | -remote> --enable remote access via SSH
| | -ssh-port --SSH port
| | -sshd --SSH daemon
| | -telnet --enable remote access via Telnet
|
| -snmp> --SNMP setting
| | -description --SNMP system description
| | -read-community --SNMP ReadCommunity
| | -snmp-status --SNMP status
| | -trap-community --SNMP ReadCommunity
| | -trap-server --SNMP TrapServer IP address
| | -write-community --SNMP WriteCommunity
|
| -spanning-tree --enable spanning tree protocol

```

```

| | -time> --time Setting
| |   |-custom-ntp-server --custom NTP server host name
| |   |--daylightsaving --daylight saving
| |   |-ntp-client --NTP client host name
| |   |-ntp-server --NTP server host name
| |   |--time-zone --time zone
| |
| | -vlan> --vlan settings
| |   |--management-vlan --vlan management id
| |   |--untagged-vlan --untagged vlan id
| |   |--untagged-vlan-status --untagged vlan status
| |
|
|-exit --logout from CLI
|-file --
|-firmware-upgrade --upload new system firmware file
|-password --system password
|-restore-configuration --restore system configuration
|-restore-default-password --restore default system password
|-show> --show system settings
| | |-configuration --show system configuration
| |   |-interface> --show wireless lan interface
| |     |-eth> --ethernet interface
| |       |--statistics --show ethernet statistics
| |
| |   |-wlan> --wlan interface settings
| |     |-2.4GHz> --2.4GHz wlan interface settings
| |       |--configuration --interface configuration
| |       |--knownaplist --known access point list
| |       |--stationlist --station list
| |       |--statistics --interface statistics
| |       |--trusted-stationlist --trusted station list
| |       |--unknownaplist --unknown access point list
| |
| |     |-5GHz> --5GHz wlan interface settings
| |       |--configuration --interface configuration
| |       |--knownaplist --known access point list
| |       |--stationlist --station list
| |       |--statistics --interface statistics
| |       |--trusted-stationlist --trusted station list
| |       |--unknownaplist --unknown access point list
| |
|
|-log --system log
|-system --system setting

```





## Numerics

192.168.0.210, Static IP Address *2-4*  
192.168.0.230, default address *2-4*  
255.255.255.0  
    default subnet *2-4*  
3DES *3-3*  
802.11a default name *2-11*  
802.11a/g *1-4*  
802.11b/g default name *2-11*  
802.1Q VLAN *1-2*

## A

Access Controll screens *2-43*  
Access Point name, default *2-6*  
ACK *1-5*  
Activity Log *3-12*  
Activity Log screen *3-13*  
Adavailable Wireless Stations *2-43*  
Advanced Access Point Settings screens *4-12*  
Advanced screens of Wireless Settings *4-5, 4-7*  
AES *2-38, 2-40*  
    WPA2-PSK, use with *2-40*  
Aggregation Length  
    default settings *4-7, 4-9*  
AMPDU  
    default settings *4-7, 4-9*  
Antenna  
    2.4 GHz *1-10*  
    5 GHZ *1-10*  
antenna position *2-2, 2-10*  
AP EDCA parameters *4-10*  
Auto Uplink *1-4, 1-5*

## B

Band selection *1-3*  
Beacon Interval  
    default setting *4-7, 4-9*  
Broadcast Wireless Network Name (SSID) *2-16, 2-19, 2-25*  
Broadcast Wireless Network Name. See SSID  
BSSID *1-2*

## C

Carrier Sense Multiple Access with Collision Detection.  
See CSMA/CD.  
Category 5 Ethernet cable *1-7*  
Change Password screen *3-10*  
channel  
    interference,multiple access points  
    channel spacing *2-2*  
Channel Width *2-17, 2-20*  
Channel/Frequency *2-16, 2-19*  
CLI *3-3*  
    command set *3-4*  
    command sets *C-1*  
configuration  
    erasing *3-9*  
    restore *3-7*  
configuration file  
    backup and restore settings *3-7*  
    retrieving *3-8, 3-9*  
    saving *3-8*  
crossover cable *1-5*  
CSMA/CD *4-6, 4-8*  
Customer support *1-ii*

## D

### Data Encryption

AES 2-38, 2-40

TKIP 2-37

TKIP+AES 2-39, 2-41

### Data Rate 2-16, 2-19

### default login 2-4

### default password 2-5, 2-12

### Default Settings A-1

### default settings 2-22

### default subnet mask

255.255.255.0 2-4

### default user name 2-5, 2-12

### DHCP Client 1-2, 2-14

enabling 2-14, 4-2

### DHCP Server 4-2

enabling access point 4-1

use as 4-1

### Documentation 2-5

### DTIM Interval

default setting 4-7, 4-9

### dynamic IP addresses

enabling 2-11

## E

### Edit Security Profile 2-24

### emulation program settings

Telnet, use with 3-3

### enabling Wi-Fi Multimedia 2-21

### equipment placement

reception range 2-1

### Ethernet

Autosensing connection 1-4

LAN 1-11

Power over 1-4

RJ-45 port 1-11

## F

### factory default settings

reset button 1-10, 5-4

resetting 5-4

restoring 3-9

### features 1-2

### Firmware Upgrade screen 3-6

### firmware, upgrading 1-3

### Fragmentation Length

default setting 4-6, 4-8

### front panel

diagram of 1-8

## G

### Gateway

default address 2-14

### Guard Interval 2-17, 2-20

## H

### hotspot

setting up server 4-4

settings 1-3

### Hotspot settings 4-1

### Hotspot Settings screen 4-4

### hotspots 2-37, 2-39, 2-40, 2-41

Wireless Client Security Separation 2-35

### http

//192.168.0.230 2-12

### HTTP redirect, enabling 4-1

## I

### Import AP List from a File 3-19

### interference sources 2-2

### IP Address

default 2-12

### IP address

default 2-12, 2-14, 2-22

### IP Address, settings 2-8

### IP menu 2-8

### IP Settings

DHCP server, use of 4-1

### IP Settings screen 2-13

IP Subnet mask  
default 2-14

## L

LAN IP address  
default 2-42, 5-3

LED indicators  
table of 1-8

Login screen 2-5

login screen 2-12

## M

MAC address 2-42  
restricting access 2-3  
trusted PCs 2-3

MAC Address Database  
Local 2-43  
RADIUS 2-43

MAC Authentication 2-42

MAC Authentication screen 2-42

MCS Index 2-16, 2-19

multiple access points  
placement of 2-2

## N

NetBIOS 2-6

Network Authentication 2-25  
types of 2-25

Network Key. See passphrase.

NTP Client  
enabling 2-9

NTP Server  
enabling 2-9

NTP Server Hostname IP Address 2-9

null-modem cable 3-3

## O

Output Power 2-17, 2-20

## P

package contents 1-6

Packet fragmentation 1-5

passphrase  
use with WEP 2-35  
WPA2-PSK, use with 2-40  
WPA-PSK/WPA2-PSK, use with 2-41

password  
default 2-12, 2-22, 2-42

performance degradation  
causes of 2-2

point-to-multi-point bridge 4-11  
configuring 4-16

point-to-multi-point bridge. 1-3

point-to-point bridge 1-3, 4-11  
configuring 4-14

power adapter 1-11

Preamble Type  
default setting 4-7

Primary DNS Servers  
default 2-14

## Q

QoS Settings screen 2-21

QoS. See Quality of Service 1-4

Quality of Service 1-4

## R

RADIUS Server 2-23

RADIUS Server Settings 2-30, 2-36, 2-37, 2-38

RADIUS Server Settings screen 2-30, 2-36, 2-37, 2-38  
Range 2-1

Read-Only Community Name  
default setting 3-2

Read-Write Community Name  
default name 3-2

rear panel  
diagram of 1-10

Reboot 3-10, 5-4

- Receive Traps 3-2
  - reception range
    - equipment placement 2-1
  - registering 1-ii
  - Remote Console 3-1
  - remote management
    - via Telenet 3-1
  - Remote Management screen 3-1
  - Repeater 4-12
  - repeater mode
    - enabling 4-1
  - Repeater, wireless
    - configuring 4-18
  - Reset to Factory Defaults 3-10
  - restore configuration 3-7
  - restore default settings 3-9
  - Restore Defaults screen 3-10
  - restricting access
    - MAC address, using 2-42
  - RIFS Transmission
    - default settings 4-7, 4-9
  - Rogue AP Detection screen 3-19
  - Rogue AP menu 3-19, 3-21
  - RTS Threshold
    - default setting 4-6, 4-8
  - RTS/CTS handshake 1-5
- S**
- Secondary DNS Servers
    - default 2-14
  - security
    - network enhancements 2-3
    - WPA 2-3
    - WPA-PSK 2-3
  - security options
    - WEP data encryption 2-3
    - WPA-PSK 2-3
  - Security Profile
    - Authentication Settings 2-25
    - Profile Definition 2-24
    - with WPA 2-36, 2-37, 2-39
  - security profile
    - about 2-23
    - default settings 2-22
  - Security Profile Name 2-24
  - Security Profiles
    - screens 2-23
  - serial
    - DTE connection 1-10
    - port 1-10
  - serial console
    - port 1-10
  - SNMP 1-2, 3-1
    - default setting 3-2
  - software upgrade 3-5
  - SSH1 3-3
  - SSID 1-4, 2-23
    - 11a default name 2-16, 2-19, 2-24, 2-25
    - 11b/g default name 2-16, 2-19, 2-24, 2-25
    - 802.11a default 2-11
    - 802.11b/g default 2-11
    - disabling, consequences of 2-3
  - Static IP Address, 192.168.0.210 2-4
  - Station EDCA Parameters 4-10
  - Statistics
    - field descriptions 3-16
    - screen 3-15
  - Subnet Mask
    - default 5-3
  - Support 1-ii
  - supported standards 1-2
  - Syslog 3-11
  - system information screen
    - field descriptions 3-13
  - system requirements 1-6
  - System status screen 3-14
- T**
- TCP/IP
    - configuration for DHCP server 4-2
  - Technical Specifications A-3
  - Telnet

- 3DES 3-3
- CLI 1-4
- SSH1 3-3
  - using CLI 3-3

- Telnet client
  - recommendations 3-3

- Telnet console 3-1

- Time menu 2-7

- Time Settings 2-7

- Time settings 2-8

- Time settings screen 2-8

- Time Zone
  - setting 2-9

- TKIP 2-37, 2-40

- TKIP+AES 2-39, 2-41

- Trap Community Name
  - default name 3-2

- troubleshooting 5-1
  - access point, connecting to 5-3
  - configuring, 5-3
  - LAN activity 5-2
  - power connection 5-1
  - timeout error 5-3
  - wireless Internet connection 5-2
  - wireless LAN activity 1 5-2

- Trusted Wireless Stations 2-43, 2-44

- trusted wireless stations
  - MAC address filtering, use with 1-3

- Turn Access Control On 2-43

- Turn Radio On 2-15, 2-18

## U

- Upgrade Firmware screen 3-6

- user name
  - default 2-12, 2-22, 2-42

## V

- VLAN
  - IDs 1-4
  - security profiles 1-4

- VT100/ANSI

- terminal, connecting 3-3
- workstation, connecting 3-3

## W

- WEP 2-3

- Wireless
  - point-to-multi-point bridge 4-11
  - point-to-point bridge 4-11

- wireless access point
  - default name 2-11
  - deployment of 2-10
  - verifying connectivity 2-11

- wireless bridge, enabling 4-1

- Wireless Client Security Separation 2-35, 2-38, 2-39, 2-40, 2-41

- wireless configuring
  - 80211.a mode 2-14
  - 80211.b/g modes 2-14

- wireless connectivity
  - testing 2-22
  - testing Wireless Settings 11a 2-22
  - testing Wireless Settings 11b/g 2-22

- Wireless Mode 2-15, 2-18

- Wireless Multimedia 1-4

- Wireless Network Name (SSID) 2-16, 2-19, 2-24

- Wireless Network Name. See SSID

- wireless QoS settings
  - 11a 2-21
  - 11b/g 2-21

- Wireless Repeater 1-3

- wireless security
  - options 2-2

- wireless settings
  - 11a 2-10
  - 11b/g 2-10
  - configuring 802.11a 2-17
  - configuring 802.11b/g 2-14
  - screen 2-17

- Wireless Settings 11a screen 2-18

- Wireless Settings screen 2-14

- wireless settings screen
  - 11a 2-10

Wireless Station

adding new 2-43

Wireless Station List screen 3-18

WPA 2-3

use restrictions 2-25

WPA and WPA2 with RADIUS

configuration of 2-38

Network Authentication screens 2-38

restrictions 2-38

TKIP+AES 2-39

WPA with RADIUS

configuration of 2-36

Network Authentication screen 2-36, 2-37, 2-39

restrictions 2-36

security profiles 2-36, 2-37, 2-39

TKIP 2-37

WPA2

use restrictions 2-25

WPA2 with RADIUS

AES 2-38

configuration of 2-37

Network Authentication screen 2-37

restrictions 2-37

WPA2-PSK

AES 2-40

configuration of 2-40

Network Authentication screens 2-40

restrictions 2-40

WPA-PSK 2-3

configuration of 2-39

Network Authentication screens 2-39

restrictions 2-39

TKIP 2-40

WPA-PSK and WPA2-PSK

configuration of 2-41

Network Authentication screens 2-41

restrictions 2-41

WWM. See Wireless Multimedia.