WNHDE111 5GHz Wireless-N HD Access Point/Bridge User Manual

NETGEAR®

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

202-10300-01
May 2008
v1.1

Download from Www.Somanuals.com. All Manuals Search And Download.

© 2008 by NETGEAR, Inc. All rights reserved.

Product Registration, Support, and Documentation

Register your product at *http://www.netgear.com/register*. Registration is required before you can use our telephone support service. Product updates and Web support are always available at *http://www.netgear.com/support*.

Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the Knowledge Base or the Documentation link under Web Support on the main menu to view support information.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and RangeMax and Smart Wizard are trademarks of NETGEAR. Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Windows Vista is a trademark 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 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 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.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WNHDE111 product package.

Europe – Declaration of Conformity in Languages of the European Community

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

Download from Www.Somanuals.com. All Manuals Search And Download.

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WNHDE111 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 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.

5 GHz Wireless-N HD Access Point/Bridge

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

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

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Product and Publication Details

Model Number:	WNHDE111
Publication Date:	May 2008
Product Family:	Wireless-N Bridge
Product Name:	5 GHz Wireless-N HD Access Point/Bridge WNHDE111
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10300-01

Download from Www.Somanuals.com. All Manuals Search And Download.

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
Getting Acquainted

Unpacking Your New Wireless-N AccessPoint/Bridge 1-1
Prepare for Installation 1-2
Key Hardware Features 1-3
Front Panel 1-3
Back Panel Connectors, Buttons, and Switches 1-4
Key Back Panel Label Information 1-5
Positioning Your Unit 1-6

Chapter 2
Easy Secure Wireless Setup

What If Some of My Devices Don't Support WPS? 2-1
Access Point Mode WPS Setup 2-2
WPS Push Button Client Setup 2-3
WPS PIN Entry Setup of WIreless Clients 2-4
Setting Up Two WNHDE111 Units 2-5
Setting Up a Pair of WNHDE111 Units at Once 2-5
Adding a Second WNHDE111 to Your Network Later 2-6
Connecting Other Devices to a WNHDE111 2-7

Chapter 3
Making Changes

Viewing or Changing Settings 3-1
Using the Smart Wizard Configuration Assistant 3-2
Using the Web Browser Interface 3-4

Download from Www.Somanuals.com. All Manuals Search And Download.

Using Automatic Firmware Update upon Login 3-5

Chapter 4
Securing My Wireless

Choosing Appropriate Wireless Security 4-1
Changing Wireless Security Settings 4-4
Viewing Basic Wireless Settings 4-4
Configuring WEP Wireless Security 4-5
Configuring WPA Wireless Security 4-6
Viewing Advanced Wireless Settings 4-6
Using Push 'N' Connect (Wi-Fi Protected Setup) 4-7
Push Button Configuration 4-8
Security PIN Entry 4-9
Connecting Additional Wireless Client Devices after WPS Setup 4-10
Enabling Wireless Isolation 4-10
Restricting Wireless Access by MAC Address 4-11
Changing the Administrator Password 4-12

Chapter 5
Customizing Your Wireless Network

Using the Network Settings Options 5-1
Configuring the Access Point Parameters 5-2
Using the DHCP Server 5-3
Wireless Repeating (Also Called WDS) 5-3

Chapter 6
Fine-Tuning Your Network

Optimizing Wireless Performance 6-1
Wireless Intelligent Stream Handling (WISH) 6-3
Using WMM QoS for Wireless Multimedia Applications 6-5

Chapter 7
Using Network Management Tools

Viewing Status and Log Information 7-1
Viewing a List of Attached Devices 7-6
Backing Up Your Configuration 7-7
Managing the Configuration File 7-7
Backing Up and Restoring the Configuration 7-7
Erasing the Configuration 7-8

Download from Www.Somanuals.com. All Manuals Search And Download.

Upgrading the Software 7-8
Upgrading Automatically to New Software 7-9
Upgrading Manually to New Software 7-9

Chapter 8
Troubleshooting

Troubleshooting Quick Tips 8-1
Troubleshooting Basic Functions 8-2
Troubleshooting the Web Configuration Interface 8-3
Restoring the Default Configuration and Password 8-4

Appendix A
Technical Specifications

Default Configuration Settings A-1
Restoring the Default User Name and Password A-3

Appendix B
Related Documents

Index

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

About This Manual

The user manual provides information for configuring the features of the NETGEAR® 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 beyond initial configuration settings. Initial configuration instructions can be found in the . You should have basic to intermediate computer and Internet skills.

Conventions, Formats, and Scope

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

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

Italic	Emphasis, books, CDs
Bold	User input, GUI screen text
`Fixed`	Command prompt, CLI text, code
Italic	URL links

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

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

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

	Warning: Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

- **Scope**. This manual is written for the Wireless-N AccessPoint/Bridge according to these specifications:

Product Version	5 GHz Wireless-N HD Access Point/Bridge WNHDE111
Manual Publication Date	May 2008

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

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

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 an 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the Wireless-N AccessPoint/Bridge was introduced.

Table 2-1. Publication Revision History

Part Number	Version Number	Date	Description
202-10300-01	v1.0	January 2008	First publication.
	v1.1	May 2008	Revised to reflect full product feature set.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 1
Getting Acquainted

This chapter describes unpacking the 5 GHz Wireless-N HD Access Point/Bridge WNHDE111, its key hardware features, and positioning the unit.

This chapter includes the following sections:

- "Unpacking Your New Wireless-N AccessPoint/Bridge" on page 1-1
- "Key Hardware Features" on page 1-3
- "Positioning Your Unit" on page 1-6

Before you begin installing your bridge, check the package contents. Become familiar with the front and back panels of your bridge—especially the status lights—and the important information on the bridge label. Then, read the section on positioning your to ensure that you have selected the best location to install your bridge.

Unpacking Your New Wireless-N AccessPoint/Bridge

Your product package should contain the following items:

- The bridge
- A snap-on stand for your bridge
- An AC power adapter (varies by region)
- A blue Ethernet cable
- The *Resource CD*, which includes:
  - The Smart Wizard Installation Assistant
  - A link to the online *User Manual*
- Warranty and Support Information cards

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Download from Www.Somanuals.com. All Manuals Search And Download.

Prepare for Installation

Carefully peel off the protective film covering both sides of your bridge

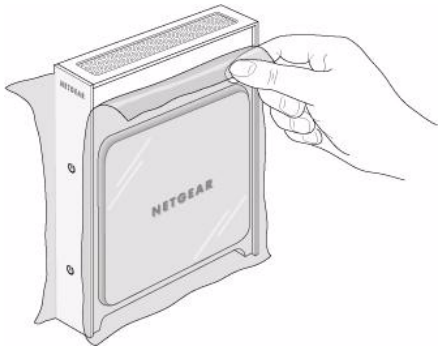


Figure 1

Set up your bridge by inserting the tabs of the stand into the slots on its bottom as shown. Then, remove the protective film covering the status light panel.

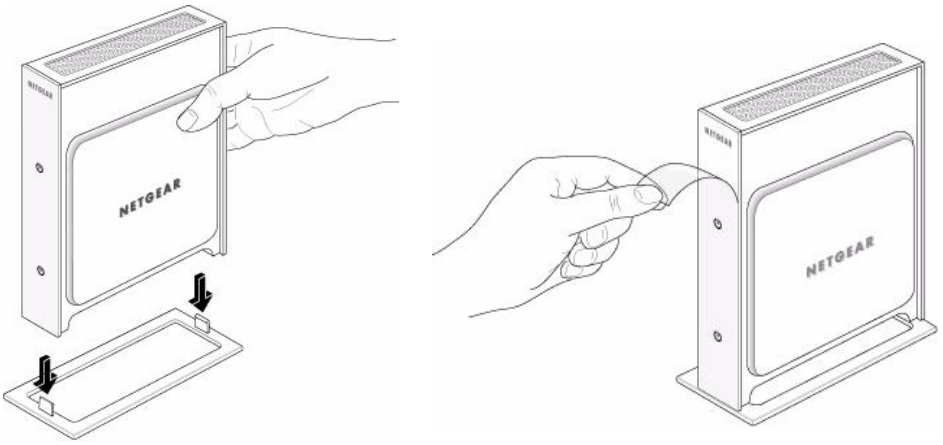


Figure 2

Place your bridge in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired connections).

	Note: To ensure proper heat dissipation and for bridge stability, it is important that you connect the stand, place your bridge in an upright position, and do not block the vent holes at the top.

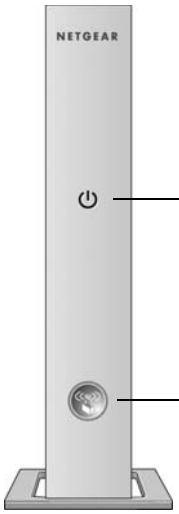
Download from Www.Somanuals.com. All Manuals Search And Download.

Key Hardware Features

Before you install and connect your bridge, take a moment to become familiar with its front and back panels—especially the status light and Push N Connect push button on the front panel.

Front Panel

The lights on the front panel indicate the operating status of the bridge.



Illuminated Power LED

On – Amber	The unit is performing the power-on diagnostic tests.
On – Green	The power is on and the router is ready.
Fast blink – Green	A software update is in progress.
Slow blink – Green	There is a problem with the wireless router software.
Off	Power is not being supplied to the unit, the wireless radio is turned off, or the LED push button switch on the back is off.

Illuminated WPS Push 'N' Connect Button

On – Amber	The unit is performing the power-on diagnostic tests.
On – Green	The wireless range extender has acquired an Internet address.
Blink – Green	Data is being communicated with the Internet.
Off	Power is not being supplied to the unit, or the LED push button switch on the back is off.

REVIEWERS: PLEASE VERIFY

Figure 1-1

Note: Pressing the LED On/Off button on the back of the unit turns off all the LEDs, including the these on the front (Power, and WPS), as well as those on the rear (Ethernet status).

Download from Www.Somanuals.com. All Manuals Search And Download.

Back Panel Connectors, Buttons, and Switches

This illustration identifies the connectors and switches on the back of the unit.

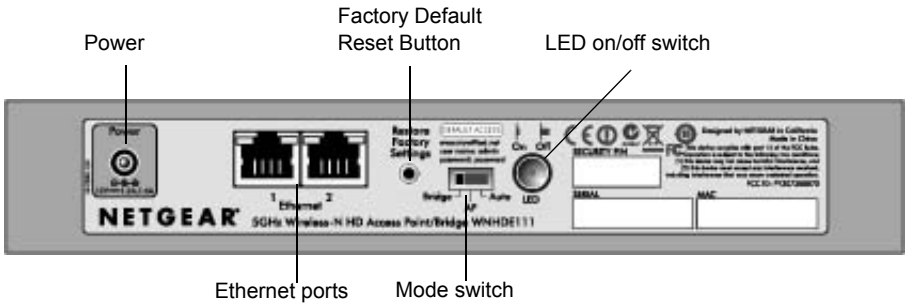


Figure 1-2

Table 1-1. Connectors, Buttons, and Switches

Connector, Button, or Switch	Description
Power connector	Port for connecting the AC power adapter.
Two 10/100 Mbps Ethernet ports	For connecting the unit via Ethernet cables to other equipment like switches, game consoles, media adapters, print servers, or a router.
Factory default reset button	Restore factory settings button. Use a paper clip to press this button for about 10 seconds to reset the unit to its factory default settings.
Mode switch settings	• **Auto**. Auto is the factory default setting. In Auto mode, if it senses it is connected to a router or gateway, it automatically sets itself to run as an AP. Otherwise, if connected to any other wired device, it automatically sets itself to run in Bridge mode. • **AP**. When switched to AP (access point) mode, it acts as an access point. In this mode, connect it to a router. The free Ethernet port can be used to connect other equipment to your network via an Ethernet cable. • **Bridge**. In Bridge mode, connect devices to it via Ethernet cables and they will connect to your wireless network. Typically, when a unit is set to bridge mode, it will be paired with a WNHDE111 working in AP mode.
LED On/Off button	Press this button to turn off all the LEDs, including the those on the front (Power, and WPS), as well as those on the rear (Ethernet status).

Download from Www.Somanuals.com. All Manuals Search And Download.

Key Back Panel Label Information

Note: The WNHDE111 comes with a WPA/WPA2 security key enabled by default. This key is the serial number printed on the label on the back of on the unit. The default wireless network name (SSID) is NETGEAR-HD.

This illustration identifies key information printed on the back panel label of the unit.

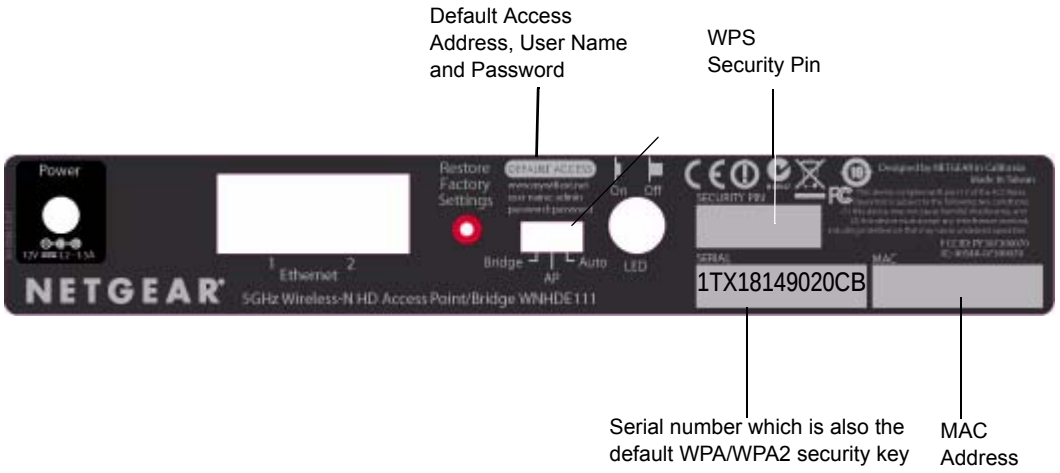


Figure 1-3

Table 1-2. Product label information

Item	Description
Default Access.	Use this URL, user name and password to log in to the unit. **Note:** During initial setup, the URL will only connect you to the unit when your computer is attached directly to one of the unit's Ethernet ports. **Tip:** Generally, using the NETGEAR setup wizard will be more convenient than logging in to the unit with this information.
WPS Security PIN.	This PIN is used for devices that require manual entry of the WPS PIN, or with WPS registrar discovery services, found in Windows Vista for example.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 1-2. Product label information

Item	Description
Serial Number which is also default WPA/WPA2 security key.	The serial number is also the factory default WPA/WPA2 security key. This enables easy automated WPS Push 'N' Connect setup.
MAC Address.	The Media Access Control (MAC) address of this unit, which will be visible in status monitoring screens on the unit or on a router.

Positioning Your Unit

The operating distance or range of your wireless connection can vary significantly depending on the physical placement of your unit. For example, the thickness and number of walls the wireless signal must pass through might limit the range.

Note: Failure to follow these guidelines can result in significant performance degradation or an inability to wirelessly connect to the bridge.

For best results, place your bridge:

- Near the center of the area where your computers and other devices will operate, preferably within line of sight to your wireless devices.
- Accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the wireless range extender and your other devices to a minimum.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.
- If placing 2 Wireless-N AccessPoint/Bridges with a direct line of sight between them, do not place them closer than 15 feet, as the antennas are tuned for this optimum distance. Orient the 2 units with the front panels (the side with the Power light) facing each other.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 2
Easy Secure Wireless Setup

This chapter describes how to easily and securely set up your Wireless-N AccessPoint/Bridge using WPS (Wi-Fi Protected Setup). WPS is a standard for easy and secure setup of wireless home networks, created by the Wi-Fi Alliance and launched in January, 2007. For more information on WPS, go to *http://www.wi-fi.org/wifi-protected-setup*.

This chapter provides instructions for using the WPS push button and the WPS PIN configuration methods. See Chapter 4, "Securing My Wireless" for other wireless setup and security options.

Note: Only wireless devices that support the 5GHz 802.11n or the 802.11a standards can connect to the WNHDE111 5 GHz Wireless-N HD Access Point/Bridge product. You cannot use the WNHDE111 with 802.11b/g devices.

This chapter includes the following sections:

- "What If Some of My Devices Don't Support WPS?" on page 2-1
- "Access Point Mode WPS Setup" on page 2-2
- "Setting Up Two WNHDE111 Units" on page 2-5
- "Connecting Other Devices to a WNHDE111" on page 2-7

What If Some of My Devices Don't Support WPS?

Use this chart to identify the setup method you should use.

My Wireless Devices	Setup to Use	Comment
All my wireless devices support WPS.	Use the WPS automated setup.	This is the easiest and fastest way to set up very secure wireless.
Some of my devices support WPS and some do not.	Use the WPS automated setup for devices that support WPS. Then, manually configure the other devices to use the WPA security key.	The default WPA security key is printed on the back of your WNHDE111.

Download from Www.Somanuals.com. All Manuals Search And Download.

Access Point Mode WPS Setup

These instructions will guide you through connecting the access point to a router. Then, you will connect wirelessly using WPS technology.

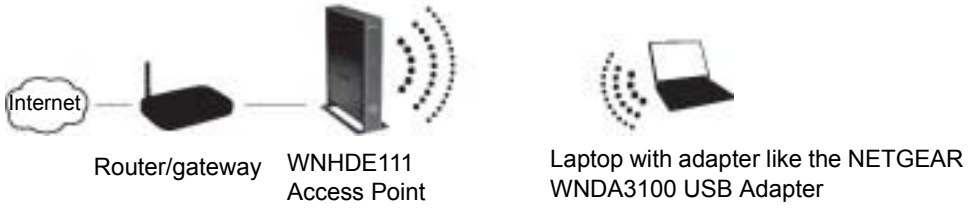
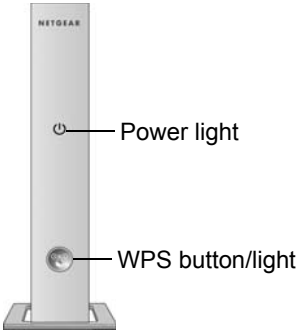


Figure 2-1

1. Connect the Ethernet cable from a LAN port on your existing router or gateway to either Ethernet port on the Wireless-N Access Point. You can leave the mode switch set to the default of Auto, or set it to AP mode (but not to Bridge mode).
2. Connect the power adapter to the unit. Verify that the power light is on.

Note: Make sure that the LED on/off switch is on. When it is off, all the status lights on the unit will be off, including the power light, the Ethernet port lights, and the WPS button will not light when pushed.



You are finished with setting up the access point.

Download from Www.Somanuals.com. All Manuals Search And Download.

WPS Push Button Client Setup

1. On the WNHDE111, press the NETGEAR Push 'N' Connect WPS push button.

Figure 2-2

The WPS button will blink for no more than 2 minutes.

2. Now, activate the WPS push button feature on your wireless client computer. For example, using the NETGEAR WNDA3100 USB Adapter, within the 2-minute period, push the picture of this button that the Smart Wizard displays.

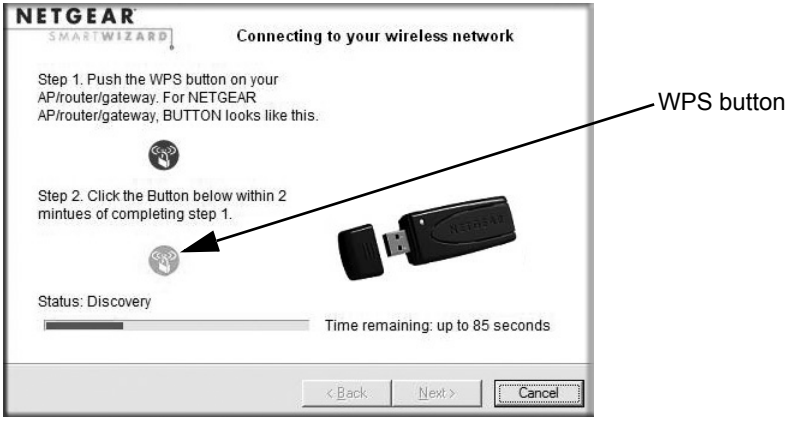


Figure 2-3

Download from Www.Somanuals.com. All Manuals Search And Download.

The WPS button on the Wireless-N Access Point blinks while the two devices are connecting and exchanging the security key. Upon successfully connecting, WPS button on the AP will be on solid for about 6 minutes and then turn off. The settings page of the Wireless-N Bridge confirms your connection.

On a NETGEAR adapter, you will notice on its settings page that WPS sent the security key from the access point to the USB adapter. In the future, you can add more WPS enabled wireless devices to your network just as easily.

Repeat this step for each additional WPS push button enabled device you add to your network.

You are done! It was just that easy to set up a secure wireless connection between the Wireless-N AccessPoint/Bridge and your wireless computer.

WPS PIN Entry Setup of WIreless Clients

To enable a WPS enabled wireless client to join your network using a PIN, follow these steps.

1. Locate the WPS security PIN on the back of the unit.

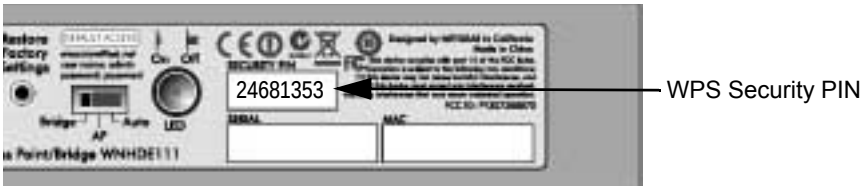


Figure 2-4

2. Follow the instructions in the product documentation of your device for entering the WPS PIN.

WPS initiates the wireless connection.

Download from Www.Somanuals.com. All Manuals Search And Download.

Setting Up Two WNHDE111 Units

You can set up a pair of WNHDE111 units, for example if you purchase them as a bundle. Or, you can set up one unit as an access point, then add a second unit as a bridge. Follow the instructions below for either of these scenarios.

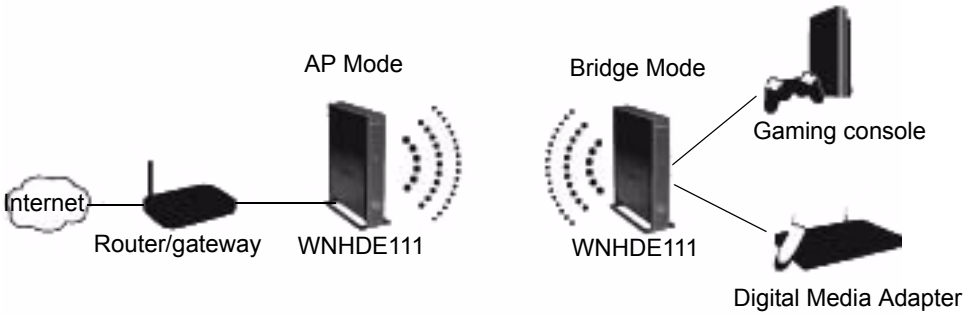


Figure 2-5

Setting Up a Pair of WNHDE111 Units at Once

Follow these steps to set up a pair of WNHDE111

1. Set the switch on the back of each Wireless-N AccessPoint/Bridge to Auto mode.
2. Connect the Ethernet cable from a LAN port in the router or gateway to either LAN port on one Wireless-N AccessPoint/Bridge.
3. Place the other Wireless-N AccessPoint/Bridge near the media player, game console, or switch and connect it with an Ethernet cable.
4. To complete installation, connect a power adapter to the Wireless-N Bridge(s). Allow a few minutes for your devices to connect to the Internet.

	Note: By following the steps in this installation with both Wireless-N Bridge units set to Auto mode, the Wireless-N Bridge connected to your router has set itself to AP mode, while the second Wireless-N Bridge is set to Bridge mode.

Download from Www.Somanuals.com. All Manuals Search And Download.

Adding a Second WNHDE111 to Your Network Later

Wireless-N AccessPoint/Bridges, if purchased as a kit, are pre-configured to securely connect to each other automatically, according to the instructions above. To add a second WNHDE111, simply use the WPS (Wi-Fi Protected Setup) push button.

1. Make sure the WNHDE111 you are adding is set to Auto or Bridge mode but *not* set to AP mode, and place it near the devices you will connect to it.
2. Connect the power adapter. The power light should blink quickly in groups of 3 (if the power light is off, press the power light on/off switch on the back panel to turn it on).

Figure 2-6

3. On the new WNHDE111, press the WPS button; its WPS light will blink.Within 2 minutes, press the WPS button on the existing Wireless-N Bridge which is operating in AP mode. Its WPS light will start to blink.

   After 1-2 minutes the new unit in Bridge mode should be associated with the existing unit in AP mode. The WPS light for the Bridge mode unit will turn off. On the AP mode unit, the WPS light will be on solid for about 6 minutes, then turn off. The power lights on both units will be steadily on.

Download from Www.Somanuals.com. All Manuals Search And Download.

Connecting Other Devices to a WNHDE111

There are three ways you can connect other devices to the access point:

- For wireless devices that support the WPS automated method, repeat the steps above for the WPS setup method. WPS will automatically transfer the security settings from the Wireless-N Access Point to the device you are adding.
- For wireless devices that do not support WPS, manually configure them. Refer to the instructions in the product documentation of the wireless device you will add. The WNHDE111 default WPA/WPA2 security key is the serial number printed on the back of the unit. The default wireless network name (SSID) is NETGEAR-HD.

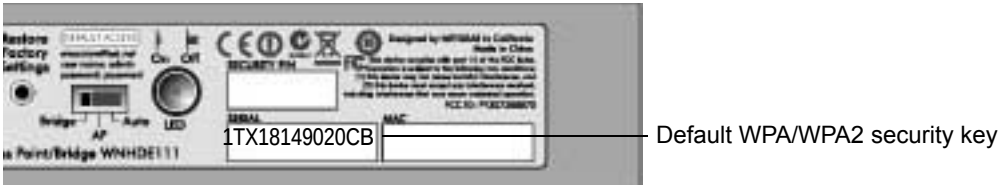


Figure 2-7

- For wired devices, use an Ethernet cable to connect to a free Ethernet port on the WNHDE111.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 3
Making Changes

This chapter describes how to connect to your WNHDE111, view or change its settings, and keep its firmware up to date. You can use the Smart Wizard or web-based GUI manage you WNHDE111.

This chapter includes:

- "Viewing or Changing Settings" on page 3-1
- "Using Automatic Firmware Update upon Login" on page 3-5

Viewing or Changing Settings

There are two ways you can view or change configuration settings on your WNHDE111.

- Use the *NETGEAR Smart Wizard Configuration Assistant*, which is included on the *Resource CD* that came with your Wireless-N AccessPoint/Bridge.

Tip: Unlike the web browser bridge manager interface, this utility will automatically discover the WNHDE111 units in your network, making it the most convenient way to view or change WNHDE111 settings.

- Use the web browser bridge manager interface by entering *http://www.mywifiext.net* into the browser of a PC directly connected by Ethernet cable to the Wireless-N AccessPoint/Bridge.

Follow the steps below to use either of these methods for viewing or changing WNHDE111 settings.

Download from Www.Somanuals.com. All Manuals Search And Download.

Using the Smart Wizard Configuration Assistant

The Configuration Assistant is included on the *Resource CD* that came with your Wireless-N AccessPoint/Bridge. It can be run from a PC or the *Resource CD* that came with the unit. You can downloaded it from *http://www.netgear.com/support*.

Tip: For convenience, and ease of future access to this utility, copy it from the *Resource CD* to your PC.

You use the Configuration Assistant to connect wirelessly or via an Ethernet cable to any Wireless-N Bridge that is in AP mode. Once connected, you can access all of your Wireless-N AccessPoint/Bridges. Otherwise, connect directly via an Ethernet cable to a Wireless-N AccessPoint/Bridge that is in bridge mode.

To use the Configuration Assistant:

1. Run the NETGEAR Smart Wizard Configuration Assistant.

   If the PC is directly connected to the WNHDE111 is not in the same range as the IP address of the WNHDE111, the Configuration Assistant prompts you to change the IP address first. Change the IP address for the PC to match the IP network of the Wireless-N Bridge.

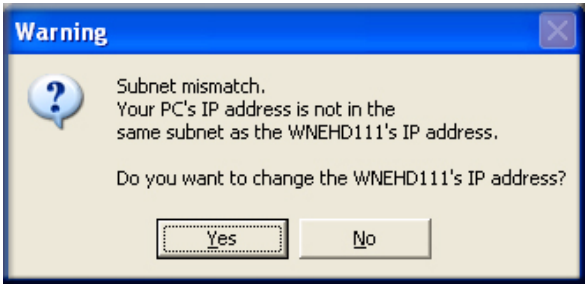


Figure 3-8

   By default, the IP address is assigned dynamically by the router. Without a router, the IP address of the Wireless-N Bridge in AP mode will default to **192.168.0.240** and the IP address of the Wireless-N Bridge in bridge mode will default to **192.168.0.241**.

Download from Www.Somanuals.com. All Manuals Search And Download.

The Configuration Assistant lists all the WNHDE111 units it finds.

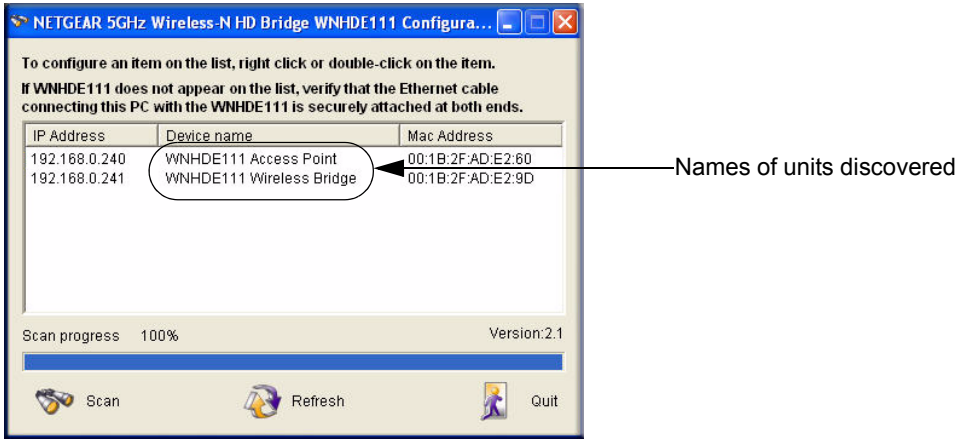


Figure 3-9

2. To configure a unit on the list, do one of the following:

   - Right-click its name to display a menu of settings you can change.

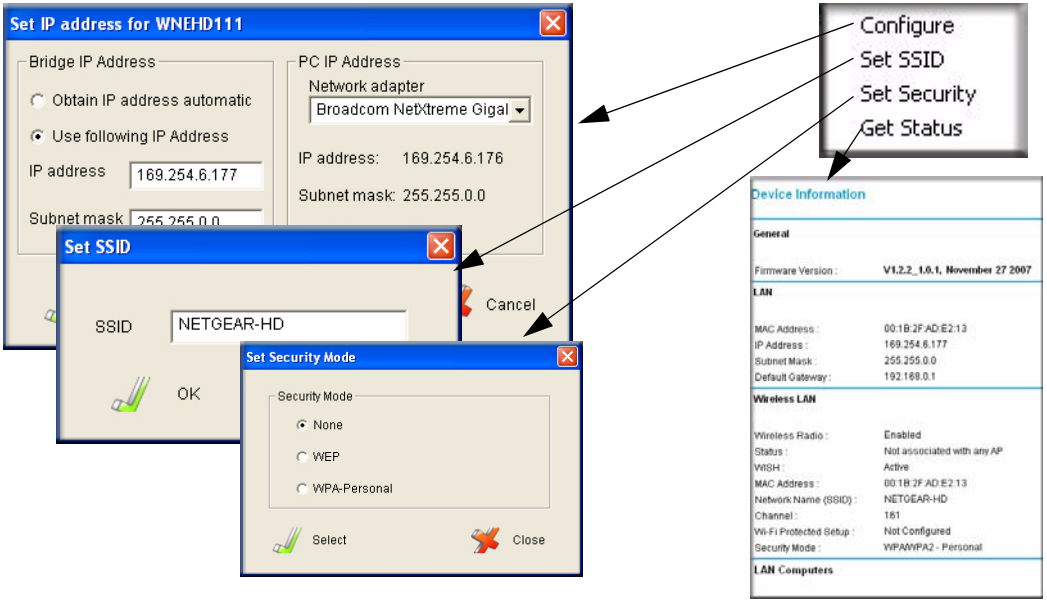


Figure 3-10

Download from Www.Somanuals.com. All Manuals Search And Download.

- Double-click the name of the unit in the discovery list to open the login menu. The default password is **password**.

Figure 3-11

Refer to the topics in this guide, or the online help pages for further information about settings.

Using the Web Browser Interface

You can use a web browser to log in to a WNHDE111 and view or changes its settings. To access the web browser interface:

1. When connected directly to the unit via an Ethernet cable, you can open the web browser interface by typing **http://www.mywifiext.net** in the address field of your browser, and then press Enter. The login window above opens:
2. Enter **password** for the password.

   The Checking for Firmware Updates screen appears unless you previously cleared the **Check for New Version Firmware Upon Log-in** check box in the Firmware Update screen.

   If the unit discovers a newer version of software, you are asked if you want to upgrade to the new software is available, the no new firmware message displays.

Download from Www.Somanuals.com. All Manuals Search And Download.

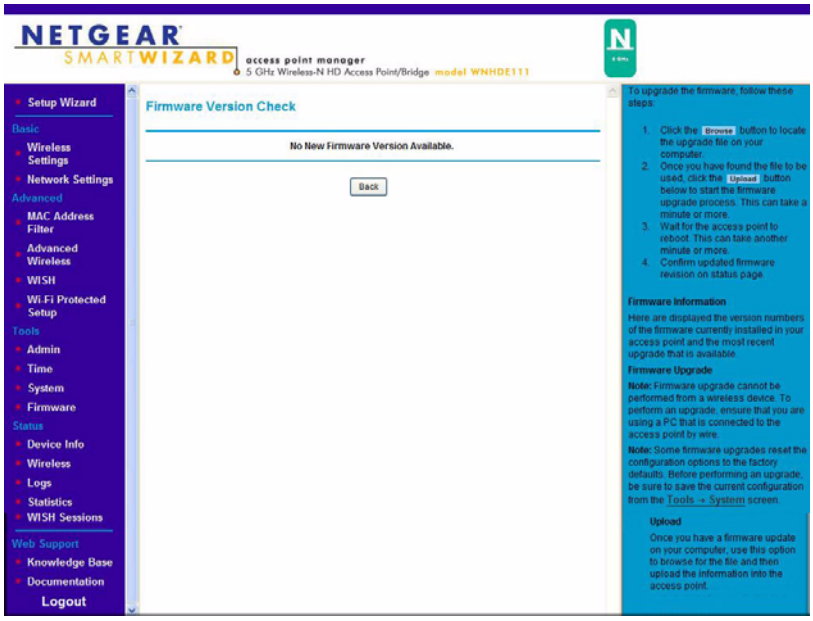


Figure 3-12

	Note: If the **Check for New Version Upon Log-in** check box is selected, the home page is the Firmware Version Check screen. Otherwise, it is the Setup Wizard screen.

If the unit is connected to the Internet, you can select **Knowledge Base** or **Documentation** under Web Support in the main menu to view support information or the user manual.

If you do not click **Logout**, the unit will wait for 5 minutes after no activity before it automatically logs you out. You can adjust this timeout setting on the Tools Admin page.

Using Automatic Firmware Update upon Login

The Checking for Firmware Updates screen appears when you log in unless you previously cleared the Check for Updated Firmware Upon Log-in check box. For information about checking for new firmware through the main menu, see “Firmware Update” on page 3-13.

Download from Www.Somanuals.com. All Manuals Search And Download.

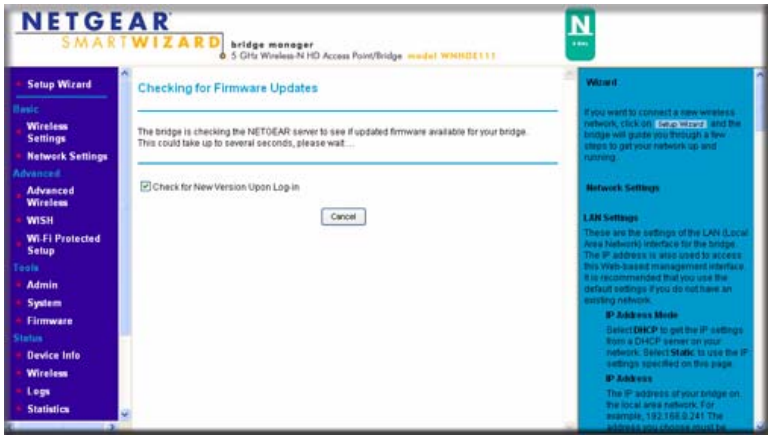


Figure 3-13

1. Allow the update feature to check for firmware updates more recent than the firmware currently installed in your Wireless-N AccessPoint/Bridge.

If the update feature discovers a newer version of software, you are asked if you want to upgrade to the new software.

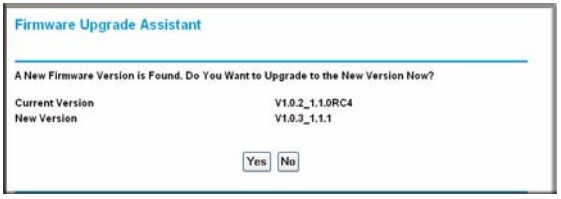


Figure 3-14

2. To download and install a newer version, click **Yes**.

The update feature automatically installs the most recent firmware.

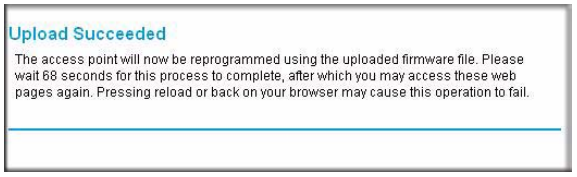


Figure 3-15

Download from Www.Somanuals.com. All Manuals Search And Download.

⚠	**Warning:** Do not try to go online, turn off the bridge, shut down the computer, or do anything else to the bridge until the bridge finishes downloading!

If no new firmware is available, the following message appears.

Figure 3-16

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 4
Securing My Wireless

The 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 provides highly effective security features, which are covered in detail in this chapter.

This chapter includes the following sections:

- "Choosing Appropriate Wireless Security" on page 4-1
- "Changing Wireless Security Settings" on page 4-4
- "Viewing Advanced Wireless Settings" on page 4-6
- "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 4-7
- "Enabling Wireless Isolation" on page 4-10
- "Restricting Wireless Access by MAC Address" on page 4-11
- "Changing the Administrator Password" on page 4-12

Choosing Appropriate Wireless Security

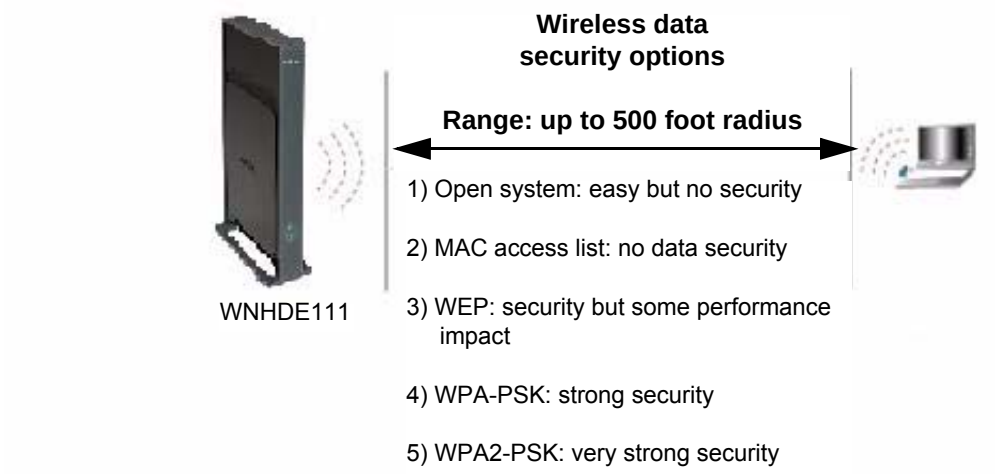
Unlike wired networks, wireless networks allow anyone with a compatible adapter to receive your wireless data transmissions well beyond your walls. Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. Indoors, computers can connect over 802.11n/a wireless networks at ranges of up to 500 feet. Such distances can allow for others outside your immediate area to access your network. Use the security features of your wireless equipment that are appropriate to your needs.

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

Stronger security methods can entail a cost in terms of throughput, latency, battery consumption, and equipment compatibility. In choosing an appropriate security level, you can also consider the effort compared to the reward for a hacker to break into your network. As a minimum, however, NETGEAR recommends using WEP with Shared Key authentication. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.

Download from Www.Somanuals.com. All Manuals Search And Download.

WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK, and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer.



Note: Use these with other features that enhance security (Table 4-2 on page 4-3).

Figure 4-1

To configure the wireless network, you can:

- **Manually specify your SSID and your wireless security settings**. The Wireless-N AccessPoint/Bridge provides two screens for configuring the wireless settings: the basic Wireless Settings screen, which you access under Setup in the main menu, and the Advanced Wireless Settings screen.
- **Use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security on both the router and the client device**. If the clients in your network are WPS capable, you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security on both the bridge and the client device.

Download from Www.Somanuals.com. All Manuals Search And Download.

Basic security options are listed in order of increasing effectiveness below. For more details on wireless security methods, "Wireless Networking Basics" in Appendix B.

Table 4-1. Wireless Security Options

Security Type	Description
None.	No wireless security. Recommended only for troubleshooting wireless connectivity. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.
WEP. Wired Equivalent Privacy. For more information, see "Configuring WEP Wireless Security" on page 4-5.	Wired Equivalent Privacy (WEP) data encryption provides moderate data security. WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.
WPA-PSK (TKIP). **WPA2-PSK (AES)**. **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Mixed mode. For more information, see "Configuring WPA Wireless Security" on page 4-6.	Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them.

Table 4-2. Other Features That Enhance Security

Security Type	Description
Turn off the broadcast of the wireless network name SSID. For more information, see "Viewing Advanced Wireless Settings" on page 4-6.	If you disable the broadcast of the SSID, only devices that know the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but your data is still fully exposed to an intruder using available wireless eavesdropping tools.
Restrict access based on MAC address. For more information, see "Restricting Wireless Access by MAC Address" on page 4-11.	You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the Wireless-N AccessPoint/Bridge. MAC address filtering adds an obstacle against unwanted access to your network by the general public, but the data broadcast over the wireless link is fully exposed. This data includes your trusted MAC addresses, which can be read and impersonated by a hacker.
Use the Push 'N' Connect feature (Wi-Fi Protected Setup). For more information, see "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 4-7.	Wi-Fi Protected Setup provides easy setup by means of a push button. Older wireless adapters and devices might not support this. Check whether devices are WPS enabled.

Download from Www.Somanuals.com. All Manuals Search And Download.

Changing Wireless Security Settings

This section describes the wireless settings that you can view and configure in the Wireless Settings screen, which you access under Setup in the main menu.

Viewing Basic Wireless Settings

To specify the wireless security settings of your router:

1. Log in to the router as described in "Viewing or Changing Settings" on page 3-1.
2. Select **Wireless Settings** under Setup in the main menu.

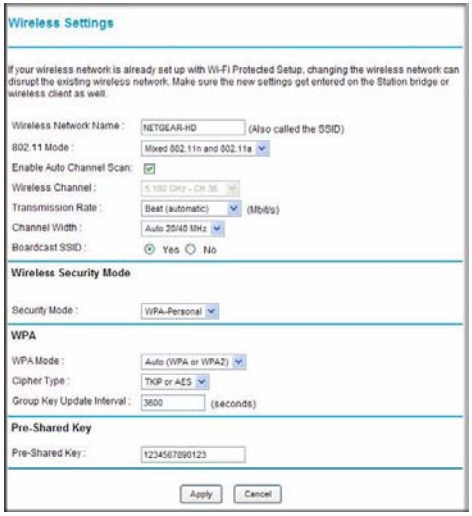


Figure 4-2

The available settings in this screen are:

- **Wireless Network Name (SSID)**. Enter a value of up to 32 alphanumeric characters. When more than one wireless network is active, different wireless network names provide a way to separate the traffic. For a wireless device to participate in a particular wireless network, it must be configured with the SSID for that network. The default SSID is **NETGEAR-HD**.
- **802.11 Mode**. You can choose from: Mixed 802.11n and 802.11a; 802.11n only; or 802.11a only.

Download from Www.Somanuals.com. All Manuals Search And Download.

- **Enable Auto Channel Scan**. The unit automatically finds the channel with least interference and uses that channel. This is enabled by default. If you disable this feature, you can use the Wireless Channel option to manually pick a channel.
- **Wireless Channel**. When Auto Channel Scan is disabled, use this option to manually pick a channel.
- **Channel Width**. This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless network. The WNHDE111 uses channel bonding technology to extend the bandwidth for data transmission.
- **Enable SSID Broadcast**. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP.
- **Wireless Security Mode: WEP or WPA**. The selection of wireless security options can significantly affect your network performance. The time it takes to establish a wireless connection can vary depending on both your security settings and unit placement.

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

Configuring WEP Wireless Security

WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.

1. Select **Wireless Settings** under Setup in the main menu.

2. In the Wireless Security Mode section, select **WEP**. The WEP options display.

3. Select the encryption strength (64 or 128 bit data encryption).

4. Enter the data encryption keys. These values must be identical on all computers and access points in your network.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Configuring WPA Wireless Security

	Note: Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (personal digital assistants) for WPA-PSK security, consult the documentation for the product you are using. Check whether newer drivers are available from the manufacturer.

Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) provides extremely strong security, very effectively blocking eavesdropping. Both methods dynamically change the encryption keys making them nearly impossible to circumvent. WPA2 adds support for hardware based AES, which adds improved performance and the strongest data encryption.

Mixed mode allows clients using either WPA-PSK (TKIP) or WPA2-PSK (AES). This provides the most reliable security, and is easiest to implement, but it might not be compatible with older adapters.

To configure WPA-PSK, WPA2-PSK, or WPA-PSK+WPA2-PSK:

1. Select **Wireless Settings** under Setup in the main menu.
2. Select one of the WPA-PSK or WPA2-PSK options for the security type. The WPA + WPA2 options the most flexible, since it allows clients using either one.
3. In the **Passphrase** field, enter a word or group of 8–63 printable characters. The passphrase *is* case-sensitive.
4. Click **Apply** to save your settings.

Viewing Advanced Wireless Settings

This section describes the wireless settings that you can view and specify in the Advanced Wireless Settings screen, which you access under Advanced in the main menu.

1. Log in to the unit.
2. Select **Advanced Wireless** under Advanced in the main menu.

   The available settings in this screen are:

Download from Www.Somanuals.com. All Manuals Search And Download.

- **Enable Wireless Router Radio**. If you disable the wireless router radio, wireless devices cannot connect to the Wireless-N AccessPoint/Bridge. If you will not be using your wireless network for a period of time, you can clear this check box and disable all wireless connectivity.
- **WPS Settings**. For information about these settings, see the following section, "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 4-7.
- **Wireless Card Access List**. For information about this list, see "Restricting Wireless Access by MAC Address" on page 4-11.

Note: The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Using Push 'N' Connect (Wi-Fi Protected Setup)

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the router's network name (SSID) and security settings and, at the same time, connect a wireless client securely and easily to the router. Look for the symbol on your client device. WPS automatically configures the network name (SSID) and wireless security settings for the router (if the router is in its default state) and broadcasts these settings to the wireless client.

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

When you add wireless clients, whether or not they are WPS enabled, the added devices must share the same network name (SSID) and security passphrase. For more information, see "Connecting Additional Wireless Client Devices after WPS Setup" on page 4-10.

Note: If you choose to use WPS, the only security methods supported are WPA-PSK and WPA2-PSK. WEP security is not supported by WPS.

The Wireless-N AccessPoint/Bridge provides two methods for connecting to a wireless client that supports WPS, described in the following sections:

Download from Www.Somanuals.com. All Manuals Search And Download.

- "Push Button Configuration"
- "Security PIN Entry" on page 4-9

Push Button Configuration

There are two methods to enable a wireless client to join a network using a push button on the router: using the physical push button or using the software button in the Add WPS Client screen.

Using the Physical Push Button

1. Press the button on the Wireless-N AccessPoint/Bridge for over 5 seconds. For information about the WPS button light, see the .

   The green button light begins to blink in a regular pattern. While the light is blinking, you have 2 minutes to enable WPS on the client that you are trying to connect to the router.

2. On the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router.

   The Wireless-N AccessPoint/Bridge's green button light ceases blinking and remains on when one of these conditions occurs:

   - The router and the client establish a wireless connection.
   - The 2-minute window period expires for establishing a WPS connection. If the connection is not established, no WPS security settings will be specified in the Wireless-N AccessPoint/Bridge.

Using the Software Button in the Add WPS Client Screen

1. Log in to the router as described in "Viewing or Changing Settings" on page 3-1.
2. Select **Add WPS Client** in the main menu, and click **Next.**
3. Select the **Push Button** setup method.

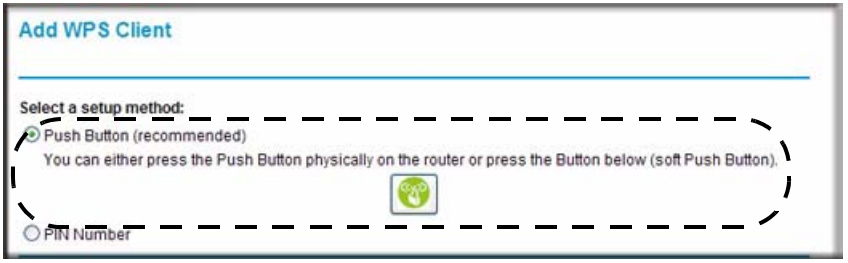


Figure 4-3

Download from Www.Somanuals.com. All Manuals Search And Download.

4. Click the button in the Add WPS Client screen. The following screen displays:

Figure 4-4

The green button light on the Wireless-N AccessPoint/Bridge begins to blink in a regular pattern. While the button light is blinking, you have 2 minutes to enable WPS on the device you are trying to connect to the router.

5. In the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router.

   The Wireless-N AccessPoint/Bridge's green button light ceases blinking and remains on when one of these conditions occurs:

   - The router and the client establish a wireless connection.
   - The 2-minute window period expires for establishing a WPS connection. If the connection is not established, no WPS security settings will be specified in the Wireless-N AccessPoint/Bridge.

Security PIN Entry

There are two ways to enable a wireless client to join a network using a PIN: using the unit's security PIN or using the wireless client's security PIN.

Using the Unit's Security PIN

1. Obtain your unit's security PIN from the rear panel of the router or from the Advanced Wireless Settings screen.
2. On the wireless client, follow its specific networking instructions to enter the router's security PIN and to establish a wireless connection with the router.

Using the Wireless Client's Security PIN

1. Log in to the WNHDE111.

Download from Www.Somanuals.com. All Manuals Search And Download.

2. Select **Add WPS Client** in the main menu, and click **Next**.
3. Select the **PIN Number** setup method.
4. On the wireless client, obtain its security PIN, or follow its specific networking instructions to generate a client security PIN.
5. In the Add WPS Client screen of the Wireless-N AccessPoint/Bridge, enter the client security PIN in the **Enter Client's PIN** field.
6. Click **Next**. The following screen displays, and the Smart Wizard initiates the wireless connection:

Connecting Additional Wireless Client Devices after WPS Setup

You can add WPS-enabled and non-WPS-enabled client devices.

Adding Additional WPS-Enabled Clients

To add an additional wireless client device that is WPS enabled, follow the procedures in "WPS Push Button Client Setup" on page 2-3 or "WPS PIN Entry Setup of WIreless Clients" on page 2-4.

Adding Additional Non-WPS-Enabled Clients

If you are connecting a combination of WPS-enabled clients and clients that are not WPS enabled, you cannot use the WPS setup procedures to add clients that are not WPS enabled. You need to record and then manually enter your security settings.

To connect non-WPS-enabled and WPS-enabled clients to the Wireless-N AccessPoint/Bridge, use the default security key on the back label of the unit, and configure the client for WPA2 using this key:

Enabling Wireless Isolation

Wireless isolation prevents wireless clients from communication with one another. However, this does not prevent wireless clients from communicating with other computers connected via Ethernet cables, or computers on the Internet.

Note: Do not use this feature if you will use wireless connections for such things as multi-user gaming, or transferring files from one computer to another over a wireless connection.

Download from Www.Somanuals.com. All Manuals Search And Download.

To enable wireless isolation, go to the Advanced Wireless menu and check the “Wireless Isolation” checkbox, and click **Apply** to save your changes.

Restricting Wireless Access by MAC Address

When a Wireless Card Access List is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computers list.

The Wireless Card Access List displays a list of wireless computers that you allow to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router.

The MAC address is a network device’s unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). It can usually be found on the bottom of the wireless card or network interface device. If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer. In WindowsXP, for example, typing the **`ipconfig/all`** command in an MSDOS command prompt window displays the MAC address as Physical Address. You might also find the MAC addresses in the router’s Attached Devices screen.

To restrict access based on MAC addresses:

1. Select **Wireless Settings** under Advanced in the main menu.
2. In the Advanced Wireless Settings screen, click **Setup Access List** to display the Wireless Card Access List.
3. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.
4. If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device.

Tip: You can copy and paste the MAC addresses from the router’s Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices screen.

Download from Www.Somanuals.com. All Manuals Search And Download.

5. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.
6. Repeat step 3 through step 5 for each additional device you want to add to the list.
7. Select the **Turn Access Control On** check box.

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

8. Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the Wireless-N AccessPoint/Bridge.

Warning: MAC address filtering adds an obstacle against unwanted access to your network by the general public. However, your trusted MAC addresses appear in your wireless transmissions, so an intruder can read them and impersonate them. Do not rely on MAC address filtering alone to secure your network.

Changing the Administrator Password

The default password for the router's Web Configuration Manager is **password**.

Tip: Before changing the router password, back up your configuration settings with the default password of **password**. If you save the settings with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults, and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings.

To change the administrator password:

1. On the main menu, under Maintenance, select **Set Password** to display the Set Password screen.
2. To change the password, first enter the old password, then enter the new password twice.
3. Click **Apply**.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 5
Customizing Your Wireless Network

This chapter describes how to configure advanced networking features of the 5 GHz Wireless-N HD Access Point/Bridge WNHDE111, including LAN, WAN, and routing settings.

It contains the following sections:

- "Using the Network Settings Options" on page 5-1"
- "Wireless Repeating (Also Called WDS)" on page 5-3

Using the Network Settings Options

Use the Network Settings screen to configure LAN IP services such as IP address of the unit, and the optional DHCP server.

By default, the IP address is assigned dynamically by the DHCP server in the network, typically built in to the routers found in home networks. Without a router, the IP address of the unit operating in AP mode will default to **192.168.0.240** and when the unit is in bridge mode it will default to **192.168.0.241**.

To configure network settings, from the main menu of the browser interface, under Advanced, click **Network Settings,** then pick **Static IP** from the drop-down list. The following screen displays:

Download from Www.Somanuals.com. All Manuals Search And Download.

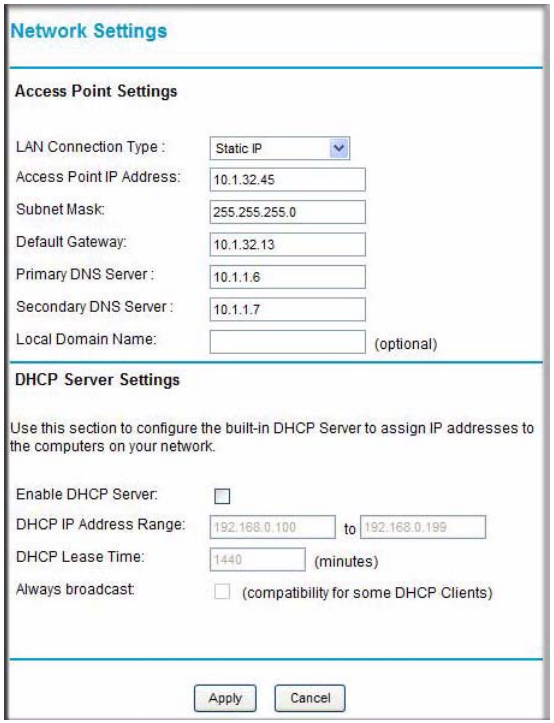


Figure 5-1

Configuring the Access Point Parameters

The Access Point Settings are:

- **Access Point IP Address**. The LAN IP address of the WNHDE111.
- **IP Subnet Mask**. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

	Note: If you change the LAN IP address of the unit while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again, and your computer must be in the same range of addresses as the unit is.

- **Default Gateway**. The LAN IP address of the router.
- **Primary and Secondary DNS Servers:** The DNS addresses the WNHDE111 will use.

Download from Www.Somanuals.com. All Manuals Search And Download.

Using the DHCP Server

	Warning: If two DHCP servers in a network are configured to give out conflicting addresses, the network will crash an none of the devices on the network will be able to use it until one of the DHCP servers is removed from the network. Be sure to avoid DHCP server conflicts with the DHCP server in your router by having them manage different address ranges in the same subnet.

For most applications, the default DHCP and TCP/IP settings of the WNHDE111 are satisfactory. Click the link to the online document "TCP/IP Networking Basics" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

By default, the DHCP server of WNHDE111 is disabled. You can enable it to assign IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address.

Wireless Repeating (Also Called WDS)

The Wireless-N AccessPoint/Bridge can be used with a wireless access point (AP) to build large bridged wireless networks. Wireless repeating is a type of Wireless Distribution System (WDS).

	Warning: If you use the wireless repeating function, your options for wireless security are limited to None or WEP. For more information about wireless security, see Chapter 4, "Securing My Wireless." Also, if the WPA security option is enabled, the WDS Enable checkbox is hidden.

To use WDS, the following conditions must be met for all APs:

- The APs must use the same SSID, wireless channel, and encryption mode.
- The APs must be on the same LAN IP subnet. That is, all the AP LAN IP addresses are in the same network.

Download from Www.Somanuals.com. All Manuals Search And Download.

- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the APs.
- The wireless MAC address of each target AP must be entered in Advanced Wireless menu WDS AP MAC Address field. One WNHDE111 can connect to 5 other units.

Once you have input the WDS configuration settings, be sure to click **Apply** to save your changes.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 6
Fine-Tuning Your Network

This chapter describes how to modify the configuration of the 5 GHz Wireless-N HD Access Point/Bridge WNHDE111 to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes the following sections:

- "Optimizing Wireless Performance" on page 6-1
- "Wireless Intelligent Stream Handling (WISH)" on page 6-3
- "Using WMM QoS for Wireless Multimedia Applications" on page 6-5

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.

	Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, click the link to the online document "Wireless Networking Basics" in Appendix B.

The following list describes how to optimize wireless router performance.

- **Identify critical wireless links.**
  If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without loss of connectivity. This also means that devices that are farther away might be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.
- **Choose placement carefully.**
  For best results, place your router:
  - Near the center of the area in which your computers will operate.

Download from Www.Somanuals.com. All Manuals Search And Download.

  - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
  - Avoid obstacles to wireless signals.
  - Keep wireless devices at least 2 feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
  - Keep away from large amounts of water such as fish tanks and water coolers.

- **Reduce interference.**
  - Avoid windows unless communicating between buildings.
  - Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
    - Computers and fax machines (no closer than 1 foot)
    - Copying machines, elevators, and cell phones (no closer than 6 feet)
    - Microwave ovens (no closer than 10 feet)

- **Choose your settings.**
  - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.
  - Turn off SSID broadcast, and change the default SSID. Other nearby devices might automatically try to connect to your network several times a second, which can cause significant performance reduction.

- Use WMM to improve the performance of voice and video traffic over the wireless link.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wireless Intelligent Stream Handling (WISH)

WISH is an advanced feature that can be used to prioritize some types of traffic ahead of others. WISH prioritization applies to the wireless link only.

You can give prioritized access to the following types of traffic:

- For specific applications by traffic type
- For specific online games by port addresses
- From a specific device by IP addresses

To specify prioritization of traffic, you must create a rule for the type of traffic and add the rule to the WISH Rules List in the WISH screen.

From the main menu of the browser interface, under Advanced, select **WISH**.

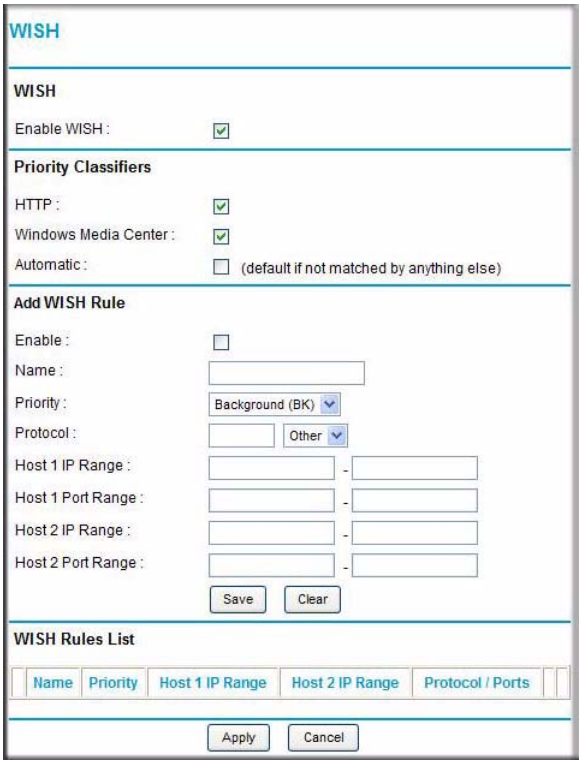


Figure 6-1

Download from Www.Somanuals.com. All Manuals Search And Download.

This table below describes the WISH options.

Table 6-1. WISH Options

Item		Description
Enable WISH		Enables WISH prioritization.
Priority Classifiers		Applies WISH prioritization to different categories of traffic.
	HTTP	Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.
	Windows Media Center	Enables the access point to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.
	Automatic	When enabled, this option causes the access point to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.
Add Wish Rule		A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.
	Enable	Specifies whether the entry will be active or inactive.
	Name	Create a name for the rule that is meaningful to you.
	Priority	Choose one for each rule: Background; Best Effort; Video; and Voice
	Protocol	Pick from the list (Any; TCPIP; UDP; Both; ICMP; Other) or specify another
	Host 1 & 2 IP Ranges	The rule applies to a flow of messages between computers that have IP address within the ranges set here.
	Host 1 & 2 Port Ranges	The rule applies to a flow of messages using the port ranges specified here between the corresponding host computers identified by their IP address the ranges.
Wish Rules List		This section lists the defined WISH Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit WISH Rule" section is activated for editing.

Download from Www.Somanuals.com. All Manuals Search And Download.

Using WMM QoS for Wireless Multimedia Applications

The Wireless-N AccessPoint/Bridge supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is disabled by default. You can enable it in the Advanced Wireless screen by checking the **Enable WMM** check box and clicking **Apply**.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 7
Using Network Management Tools

This chapter describes how to use the maintenance features of your 5 GHz Wireless-N HD Access Point/Bridge WNHDE111. You can access these features by selecting the items under Maintenance in the main menu of the browser interface.

This chapter includes the following sections:

- "Viewing Status and Log Information" on page 7-1"
- "Viewing a List of Attached Devices" on page 7-6
- "Backing Up Your Configuration" on page 7-7
- "Managing the Configuration File" on page 7-7
- "Upgrading the Software" on page 7-8

Viewing Status and Log Information

To view status and log information:

- From the main menu of the browser interface, under Status, select **Device Info**. The unit status screen displays.

Figure 7-1

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 7-1 describes the router status fields.

Table 7-1. Device Info Status Fields

Field		Description
General		
	Time	The current time.
	System up time	How long the unit has been running since its last restart.
	Firmware Version	The version of the firmware running in the unit.
LAN		
	Connection Type	If set to None, the unit has a fixed IP address. If set to DHCP Client, the unit obtains an IP address dynamically from DHCP.
	MAC Address	The Media Access Control address. This is the unique physical address being used by the Ethernet ports of the unit.
	IP Address	The IP address being used by the Ethernet port of the unit.
	IP Subnet Mask	The IP subnet mask. For an explanation of subnet masks and subnet addressing, click the link to the online document "TCP/IP Networking Basics" in Appendix B.
	Default Gateway	The IP address of the router in your network.
	Primary DNS Server	The Primary Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.
	DHCP Server	The Secondary Domain Name Server addresses being used by the router.
	Domain Name Server	The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table 7-1. Device Info Status Fields (continued)

Field		Description
Wireless LAN		
	Wireless Radio	Indicates whether the radio feature of the router is enabled. If not enabled, the Wireless LED on the front panel is off.
	WISH	Identifies if WISH is active or not.
	MAC Address	This is the unique physical address being used by the Ethernet ports of the wireless interface.
	Network Name (SSID)	The wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR-HD.
	Channel	Identifies the channel of the wireless port being used. Click the link to the online document "Wireless Networking Basics" in Appendix B for the frequencies used on each channel. In **Up to 300 Mbps** mode, there are two channels: a primary channel (P) and a secondary channel (S).
	Security Mode	Indicates the wireless security mode: • None • WEP • WPA/WPA2 (the default)
	Wi-Fi Protected Setup	Indicates whether the radio feature of the router is enabled. If not enabled, the Wireless LED on the front panel is off.
LAN Computers		The names and address of devices in the network.

- Click **Wireless** to display wireless client address, mode, rate and signal strength status.

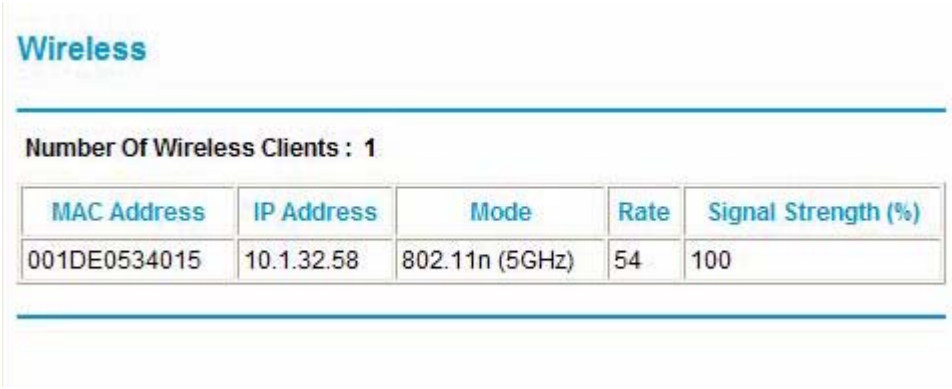


Figure 7-2

Table 7-3 describes the traffic statistics.

Download from Www.Somanuals.com. All Manuals Search And Download.

- Click **Logs** to display log information.

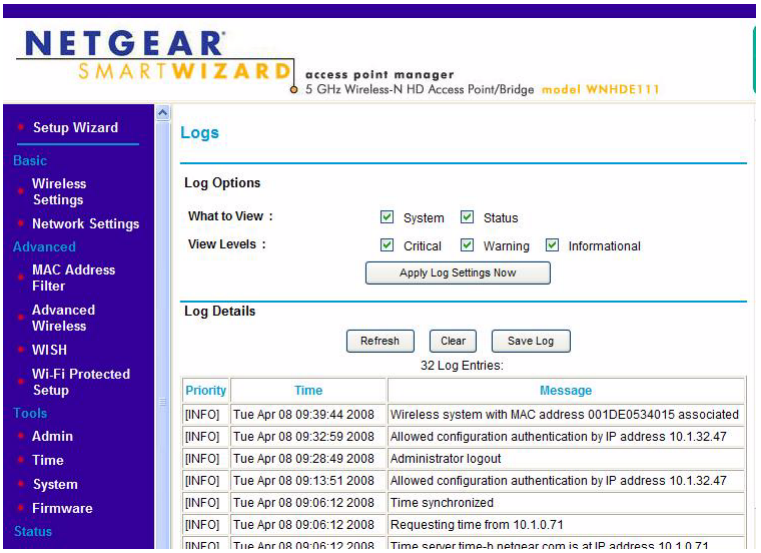


Figure 7-3

Table 7-3 describes the traffic statistics.

Table 7-2. Logs

Item		Description
Log Options		
	What to view	Log types: system, status, or both.
	View Levels	Log categories: Any combination of Critical, Warning, or Informational
Log Details		Priority, time, and messages.

Download from Www.Somanuals.com. All Manuals Search And Download.

- Click **Statistics** to display traffic statistics.

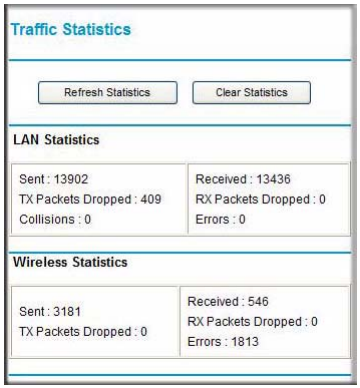


Figure 7-4

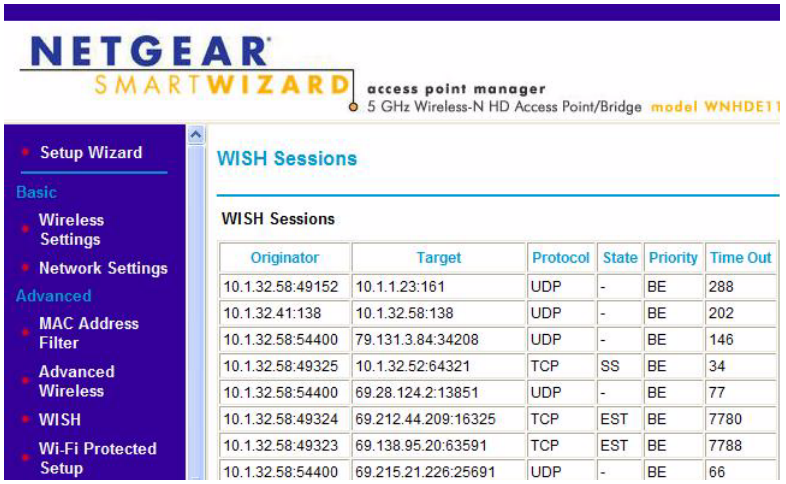
Table 7-3 describes the traffic statistics.

Table 7-3. Traffic Statistics

Item		Description
Refresh Statistics		Refresh the statistics on this screen.
Clear Statistics		Clear the statistics on this screen.
LAN Statistics		All statistics displayed are since the unit was last restarted.
	Sent	The number of packets sent on the Ethernet ports.
	TxPkts Dropped	The number of transmitted Ethernet packets dropped.
	Collisions	The number of collisions on the Ethernet ports.
	Received	The number of packets received on the Ethernet ports.
	RxPkts Dropped	The number of received Ethernet packets dropped.
	Errors	The number of packets received with errors on the Ethernet ports.
Wireless Statistics		The time elapsed since the router was last restarted.
	Sent	The number of wireless packets sent.
	TxPkts Dropped	The number of transmitted wireless packets dropped.
	Received	The number of wireless packets received.
	RxPkts Dropped	The number of received wireless packets dropped.
	Errors	The number of wireless packets received with errors.

Download from Www.Somanuals.com. All Manuals Search And Download.

- Click **WISH Sessions** to display WISH session status showing the originator, target, protocol, state, priority and time out.

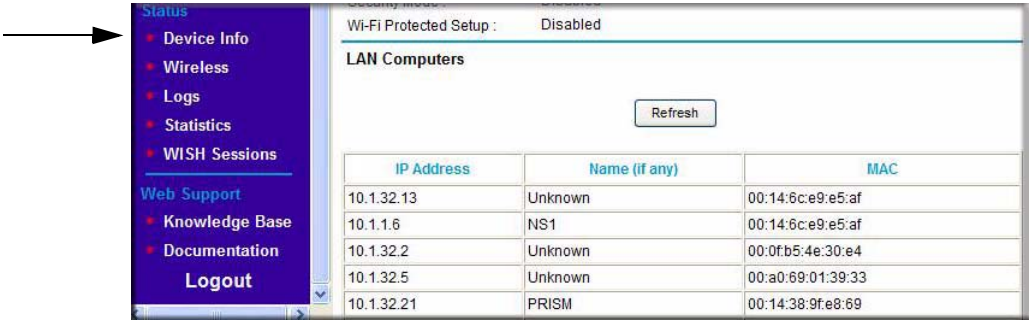


Originator	Target	Protocol	State	Priority	Time Out
10.1.32.58:49152	10.1.1.23:161	UDP	-	BE	288
10.1.32.41:138	10.1.32.58:138	UDP	-	BE	202
10.1.32.58:54400	79.131.3.84:34208	UDP	-	BE	146
10.1.32.58:49325	10.1.32.52:64321	TCP	SS	BE	34
10.1.32.58:54400	69.28.124.2:13851	UDP	-	BE	77
10.1.32.58:49324	69.212.44.209:16325	TCP	EST	BE	7780
10.1.32.58:49323	69.138.95.20:63591	TCP	EST	BE	7788
10.1.32.58:54400	69.215.21.226:25691	UDP	-	BE	66

Figure 7-5

Viewing a List of Attached Devices

The Attached Devices screen contains a table of all IP devices that the unit has discovered on the local network, including both those connected wirelessly and via Ethernet cables. From the main menu of the browser interface, under Status, select **Device Info** and scroll down to view the table.



IP Address	Name (if any)	MAC
10.1.32.13	Unknown	00:14:6c:e9:e5:af
10.1.1.6	NS1	00:14:6c:e9:e5:af
10.1.32.2	Unknown	00:0f:b5:4e:30:e4
10.1.32.5	Unknown	00:a0:69:01:39:33
10.1.32.21	PRISM	00:14:38:9f:e8:69

Figure 7-6

Download from Www.Somanuals.com. All Manuals Search And Download.

For each device, the table shows the IP address, NetBIOS host name or device name (if available), and the Ethernet MAC address. To force the unit to look for attached devices, click **Refresh**.

Note: If the bridge is rebooted, the table data is lost until it rediscovers the devices.

Backing Up Your Configuration

The configuration settings are stored in a configuration file. You can back up (save) this file and retrieve it later. Save your configuration file after you complete the configuration. If the unit fails or becomes corrupted, or an administrator password is lost, you can easily re-create your configuration by restoring the configuration file.

Managing the Configuration File

The configuration settings of the Wireless-N AccessPoint/Bridge are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

From the main menu of the browser interface, under Maintenance, select **Backup Settings**.

The following sections describe the three available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Settings Backup screen let you save and retrieve a file containing your bridge's configuration settings.

To save your settings, click **Back Up**. Your browser extracts the configuration file from the bridge and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as comcast.cfg.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Download from Www.Somanuals.com. All Manuals Search And Download.

To restore your settings from a saved configuration file, enter the full path to the file on your computer, or click **Browse** to browse to the file. When you have located it, click **Restore** to send the file to the router. The router then reboots automatically.

Warning: Do not interrupt the reboot process.

Erasing the Configuration

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings. After an erase, the unit's password is **password**.

To erase the configuration, click the **Erase** button in the Settings Backup screen.

To restore the factory default configuration settings when you do not know the login password or IP address, you must use the restore factory settings button on the rear panel of the router (see "Restoring the Default Configuration and Password" on page 8-4).

Upgrading the Software

The software (also called firmware) of the Wireless-N AccessPoint/Bridge is stored in flash memory, and can be upgraded as NETGEAR releases new software. Your unit can download and install the new software, or you can download upgrade files from the NETGEAR website and manually send the upgrade file to the router using your browser.

Tip: To ensure that you are always using the latest router firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability.

The Checking for Firmware Updates screen appears at login unless you clear the **Check for Updated Firmware Upon Log-in** check box.

A screen is also provided for upgrading the router. From the main menu of the browser interface, under Maintenance, select **Router Upgrade** to display the Router Upgrade screen.

Download from Www.Somanuals.com. All Manuals Search And Download.

From this screen, you can check for new software versions by clicking the **Check** button. If a new version is found, you can download and install it in one step. To enable the Smart Wizard to automatically check for a new software version upon login, select the **Check for New Version Upon Log-in** check box.

Alternatively, you can manually install an upgrade file stored on your computer.

Tip: Before upgrading the router software, use the router Settings Backup screen to save your configuration settings. A router upgrade might cause the router settings to revert to the factory defaults. If this happens, after completing the upgrade, you can restore your settings from the backup.

Upgrading Automatically to New Software

If you have selected **Check for New Version Upon Log-in**, your router alerts you to the new software when you log in. Otherwise, you can click the **Check** button in the Firmware Upgrade screen to search for new software.

If the unit discovers a newer version of software, the message on the left displays when you log in. If no new software is available, the message on the right displays.

To automatically upgrade to the new software, click **Yes** to allow the router to download and install the new software file from NETGEAR.

Warning: When uploading software to the Wireless-N AccessPoint/Bridge, ***do not*** interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your bridge automatically restarts. The upgrade process typically takes about 1 minute. Read the new software release notes to determine whether you must reconfigure the bridge after upgrading.

Upgrading Manually to New Software

To manually select, download, and install new software to your router:

1. Under Maintenance on the main menu, select **Status**. Note the version number of your router firmware.
2. Go to the WNHDE111 support page on the NETGEAR website at *http://www.netgear.com/support*.

Download from Www.Somanuals.com. All Manuals Search And Download.

3. Check the most recent firmware version offered against the firmware version shown on your Router Status screen.
4. If the version on the NETGEAR website is more recent, download the file to your computer.
5. Under Maintenance on the main menu, select **Firmware Upgrade**.
6. Click **Browse**, and locate the firmware image that you downloaded to your PC (the file ends in .bin).
7. Click **Upload** to send the firmware to the unit.

Warning: When uploading software to the Wireless-N AccessPoint/Bridge, ***do not*** interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your bridge automatically restarts. The upgrade process typically takes about 1 minute. Read the new software release notes to determine whether you must reconfigure the bridge after upgrading.

Download from Www.Somanuals.com. All Manuals Search And Download.

Chapter 8
Troubleshooting

This chapter provides information about troubleshooting your 5 GHz Wireless-N HD Access Point/Bridge WNHDE111. After each problem description, instructions are provided to help you diagnose and solve the problem. As a first step, please review the Quick Tips.

Tip: NETGEAR provides helpful articles, documentation, and the latest software updates at *http://www.netgear.com/support*.

This chapter includes the following sections:

- "Troubleshooting Quick Tips"
- "Troubleshooting Basic Functions" on page 8-2
- "Troubleshooting the Web Configuration Interface" on page 8-3
- "Restoring the Default Configuration and Password" on page 8-4

Troubleshooting Quick Tips

This section describes tips for troubleshooting some common problems:

Be sure to restart your network in this sequence.

1. Turn off *and* unplug the modem.
2. Turn off the router.
3. Turn off the WNHDE111 units and computers.
4. Plug in the modem and turn it on. Wait 2 minutes.
5. Turn on the router and wait 1 minute.
6. Turn on the WNHDE111 units and wait 1 minute.
7. Turn on the computers.

Download from Www.Somanuals.com. All Manuals Search And Download.

Make sure that the Ethernet cables are securely plugged in.

- The Internet status light on the wireless range extender is on if the Ethernet cable connecting the wireless range extender and the network is plugged in securely and the WNHDE111 is turned on.
- Be sure the LED on/off button on the back panel is set to on so that you can monitor the status lights.

Make sure that the wireless settings in the computer and WNHDE111 match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and WEP or WPA security settings of the WNHDE111 and wireless computer must match exactly.
- If you have enabled the wireless range extender to restrict wireless access by MAC address, you must add the wireless computer's MAC address to the router's wireless card access list.

Make sure that the network settings of the computer are correct.

Wired and wirelessly connected computers *must* have network (IP) addresses on the same network as the WNHDE111. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Click the link to the online document "Preparing Your Network" in Appendix B, or see the documentation that came with your computer.

Troubleshooting Basic Functions

After you turn on power to the unit, the following sequence of events should occur:

1. When power is first applied, verify that the LED push button is set to on, and the Power light is on.
2. After approximately 10 seconds, verify that:
   a. The Power light is solidly on.
   b. The status lights of any in-use Ethernet LAN port are on. This indicates that a link has been established to the connected device.

If any of the above conditions does not occur, see the appropriate following section.

The Power light is not on or is blinking.

If the Power and other lights are off when your unit is turned on:

Download from Www.Somanuals.com. All Manuals Search And Download.

- Make sure that the power cord is properly connected and that the power adapter is properly connected to a functioning power outlet.
- Check that you are using the power adapter that NETGEAR supplied for this product.

If the error persists, you have a hardware problem and should contact Technical Support at *www.netgear.com/support*.

The Wireless or Ethernet port lights are not on.

If either the Ethernet port lights or the wireless light does not come on when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the computer and at the unit.
- Make sure that power is turned on to the connected router or computer.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration Interface from a computer on your local network, check the following:

- If you are connecting from a wireless computer, try connecting from a wired computer.
- Make sure that your computer's IP address is on the same subnet as the router. For instructions, click the link to the online document "Preparing Your Network" in Appendix B to configure your computer.

Note: If your computer's IP address is shown as 169.254.x.x: Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in subnet 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try closing the browser and opening it again, or try a different browser.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

Download from Www.Somanuals.com. All Manuals Search And Download.

If the unit does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.
- Click **Refresh** or **Reload** in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function.
- Use the restore factory settings button on the rear panel of the unit. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the restore settings button on the rear panel of the router.

1. Press and hold the restore settings button for 10 seconds.

2. Release the restore settings button, and wait for the router to reboot.

Download from Www.Somanuals.com. All Manuals Search And Download.

Appendix A
Technical Specifications

Default Configuration Settings

This appendix provides factory default settings and technical specifications for the 5 GHz Wireless-N HD Access Point/Bridge WNHDE111.

Table A-1. Wireless-N AccessPoint/Bridge Default Configuration Settings

Feature		Default Setting
Login		
	Login URL	http://www. mywifiext.net *or* http://www.mywifiext.com
	Login Name	admin
	Login Password (case-sensitive) printed on product label	password
Local Network		
	Default LAN IP address (when not connected to a DHCP enabled network)	AP mode: 192.168.0.240 Bridge mode: 192.168.0.241
	Subnet	255.255.255.0
	DHCP Server	Disabled
	Time Zone	(GMT) Greenwich Mean Time
	Time Zone Enabled for Daylight Saving Time	Disabled
Wireless		

Download from Www.Somanuals.com. All Manuals Search And Download.

Table A-1. Wireless-N AccessPoint/Bridge Default Configuration Settings

Feature		Default Setting
	Wireless Communication	Enabled
	SSID Name	NETGEAR-HD
	Security	WPA2 Enabled (key is serial number printed on back label)
	Broadcast SSID	Enabled
	Transmission Speed	Auto[a]
	Country/Region	United States in the U.S., otherwise varies by region
	RF Channel	Auto
	Operating Mode	802.11 n/a mixed mode
	Data Rate	Best
	Output Power	Full
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.		
Network Protocol and Standards Compatibility		
	Data and Routing Protocols	TCP/IP
Power Adapter		
	North America	120V, 60 Hz, input ???
	United Kingdom, Australia	240V, 50 Hz, input ???
	Europe	230V, 50 Hz, input ???
	Japan	100V, 50/60 Hz, input ???
	All regions (output)	12 V DC @ 1.5A output, 22W maximum
Physical Specifications		
	Dimensions	28 x 175 x 119 mm (1.1 x 6.89 x 4.68 in.)
	Weight	0.3 kg (0.66 lb)
Environmental Specifications		
	Operating temperature	0° to 40° C (32° to 104° F) ???
	Operating humidity	90% maximum relative humidity, noncondensing ???

Download from Www.Somanuals.com. All Manuals Search And Download.

Table A-1. Wireless-N AccessPoint/Bridge Default Configuration Settings

Feature		Default Setting
Electromagnetic Emissions		
	Meets requirements of	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B C-Tick N10947 ???
Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx, RJ-45
	Internet	10BASE-T or 100BASE-Tx, RJ-45
	Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. 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.
	Radio Data Rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps Auto Rate Sensing ???
	Frequency	???
	Data Encoding	802.11n: ??? 802.11a: ???
	Maximum Computers Per Wireless Network	Limited by the amount of wireless network traffic generated by each node. Typically 30–70 nodes.
	Operating Frequency Ranges	?
	802.11 Security	40 bit (also called 64 bit) and 128 bit WEP, WPA-PSK and WPA2-PSK.

Restoring the Default User Name and Password

You can restore the factory default configuration settings to reset the bridge's user name to **admin,** the password to **password,** and the IP address to **192.168.0.100**. This procedure erases your current configuration, including your wireless security settings, and restores the factory defaults. When you log in after resetting, the Smart Wizard configuration assistant prompts you to configure these settings.

Download from Www.Somanuals.com. All Manuals Search And Download.

To restore the factory default configuration settings:

1. Use a sharp object such as a pen or a paper clip to press and hold the restore factory settings button, located on the rear panel of the bridge, for about 20 seconds.
2. Release the restore factory settings button, and wait for the bridge to reboot.

   The factory default settings are restored so that you can access the bridge from your Web browser using the factory defaults.

Download from Www.Somanuals.com. All Manuals Search And Download.

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
TCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

In addition, you can find initial setup instructions for your wireless range extender in the .

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Index

A

access
  restricting by MAC address *4-11*
access control
  turning on *4-12*
access points *5-3*
ActiveX *8-3*
adding
  wireless clients *4-7, 4-10*
administrator password, changing *4-12*
advanced wireless settings *4-6*
attached devices *7-6*
autogenerated IP addresses *8-3*
automatic logout *3-5*
automatic software upgrade *7-9*

B

backing up configuration file *7-7*
basic settings *4-4*
bold text *xi*

C

cables, checking *8-2*
channel, frequency *4-5*
channel, wireless port *7-3*
clients, adding *4-7, 4-10*
communication mode *4-4, 7-3*
configuration file
  backing up *7-7*
  erasing *7-8*
  managing *7-7*
configuration, erasing *A-3, A-4*
configuring
  advanced security *4-6*
  basic security *4-4*
  WPA security *4-6*
CTS/RTS Threshold *4-7*
customer support *ii*

D

default factory settings
  restoring *8-4*
deleting configuration *7-8*
DHCP server *5-3*
Documentation Web page *3-5*
documents, reference *B-1*
Domain Name Server (DNS) addresses
  current *7-2*

E

encryption *4-1*
encryption keys *4-5*
erasing configuration *7-8*
Ethernet light, troubleshooting and *8-2, 8-3*
Ethernet MAC address *7-7*

F

factory default settings
  restoring *8-4*
factory settings, restoring *A-3, A-4*
firmware update *3-5*
Firmware Upgrade Assistant *3-4, 7-8*
firmware version *7-2*
fixed font text *xi*

Download from Www.Somanuals.com. All Manuals Search And Download.

Fragmentation Threshold *4-7*
frequency, channel *4-5*

G

generating encryption keys *4-5*

H

host name *7-7*
HTML version, printing *xii*

I

interference, reducing *6-2*
interval, poll *6-4, 7-5*
IP addresses
  autogenerated *8-3*
  current *7-2*
  LAN *5-2*
IP subnet mask *5-2, 7-2*
italic text *xi*

J

Java and JavaScript *8-3*

K

keys, encryption *4-5*
knowledge base *3-5*

L

LAN IP setup *5-1*
LAN port
  settings *7-3*
Legacy mode *4-4*
logout, automatic *3-5*

M

MAC addresses
  attached devices *7-7*
  current *7-2*
  restricting access by *4-11*
manually upgrading software *7-9*
mixed mode encryption *4-3*
mode, communication *4-4, 7-3*

N

Neighbor Friendly mode *4-4*
NetBIOS host name *7-7*

O

optimizing performance *6-1*

P

passphrases *4-6*
password *A-4*
  changing *4-12*
  restoring *8-4*
PDF, printing *xiii*
Performance mode *4-4*
performance, optimizing *6-1*
physical push button (WPS) *4-8*
PIN *4-9*
placement, router *6-1*
poll interval *6-4, 7-5*
Power light, troubleshooting and *8-2*
Preamble mode *4-7*
printing manual *xii*
prioritizing traffic *6-3*
Push 'N' Connect *4-7*
push button configuration (WPS) *4-8*

Q

QoS (Quality of Service) *6-3*

R

radio, wireless *4-7, 7-3*

Download from Www.Somanuals.com. All Manuals Search And Download.

range, router *6-1*
reducing interference *6-2*
reference documents *B-1*
region of operation *4-5*
registering product *ii*
restarting network *8-1*
restoring
  configuration *7-7*
  default factory settings *8-4*
restricting access by MAC address *4-11*
revision history *xiii*
router PIN *4-9*
router status, viewing *7-1*

S

security
  options, compared *4-2*
  setting up *4-1*
security PIN *4-9*
settings
  default *A-1*
  password *A-3, A-4*
  restoring factory settings *A-3, A-4*
software push button configuration (WPS) *4-8*
software, upgrading *7-8*
SSID *4-4*
SSID broadcast *4-5*
statistics, usage *7-3, 7-4, 7-5, 7-6*
status, viewing *7-1*
subnet mask *5-2, 7-2*
system up time *6-4, 7-4, 7-5*

T

trademarks *ii*
traffic, prioritizing *6-3*
troubleshooting *8-1*
typographical conventions *xi*

U

up time, system *6-4, 7-4, 7-5*
updating firmware *3-5*
upgrading router software *7-8*
URLs
  typography for *xi*
usage statistics *7-3, 7-4, 7-5, 7-6*

V

viewing
  advanced wireless settings *4-6*
  attached devices *7-6*
  basic security settings *4-4*
  status *7-1*

W

Web Configuration Interface, troubleshooting *8-3*
WEP encryption *4-3, 4-5*
Wi-Fi Protected Setup (WPS) *4-7*
Wireless Card Access List *4-11*
wireless client PIN *4-9*
wireless clients, adding *4-7, 4-10*
Wireless Distribution System (WDS) *5-3*
wireless network name *4-4*
wireless port settings *7-3*
wireless radio *4-7, 7-3*
wireless repeating function *5-3*
wireless security, setting up *4-1*
wireless settings
  advanced *4-6*
  basic *4-4*
WMM (Wi-Fi Multimedia) *6-5*
WPA2-PSK encryption *4-3, 4-6*
WPA-PSK + WPA2-PSK encryption *4-3, 4-6*
WPA-PSK encryption *4-3, 4-6*

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com