NETGEAR Wireless-N Access Point WN802Tv2 Reference Manual (802.11bgn)

NETGEAR®

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

202-10415-01
June 2008

Technical Support

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

NETGEAR, INC. Support Information

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

E-mail: support@netgear.com

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

Trademarks

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

Statement of Conditions

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

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

Certificate of the Manufacturer/Importer

It is hereby certified that the NETGEAR Wireless-N Access Point WN802Tv2 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasNETGEAR Wireless-N Access Point WN802Tv2 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Voluntary Control Council for Interference (VCCI) Statement

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

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity   C E ①

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

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.

v1.0, June 2008

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

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WN802Tv2 NETGEAR Wireless-N Access Point WN802Tv2 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.

> NETGEAR Wireless-N Access Point WN802Tv2
>
> FC Tested to Comply
>   with FCC Standards
>   FOR HOME OR OFFICE USE
>   PY308200086

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

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR Wireless-N Access Point WN802Tv2) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-08200086

Product and Publication Details

Contents

About This Manual

The *NETGEAR, Inc.® Wireless-N Access Point WN802Tv2 Reference Manual* describes how to install, configure, and troubleshoot the NETGEAR Wireless-N Access Point WN802Tv2. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

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

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

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

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

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

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

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

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

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

Product Version	NETGEAR Wireless-N Access Point WN802Tv2
Manual Publication Date	June 2008

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

> → **Note:** Product updates are available on the NETGEAR, Inc. website at
> *http://kbserver.netgear.com/products/WN802Tv2.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

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

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

  – Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  – Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

  – Click the print icon in the upper left of the window.

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

- **Printing the Full Manual**. Use the *Complete PDF Manual* link at the top left of any page.

  – Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

  – Click the print icon in the upper left of the window.

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

Revision History

Part Number	Version Number	Date	Description
202-10415-01	1.0	June 2008	New features: MIMO, WMM/QoS; WPA2; RADIUS authentication, Wireless Bridge and Repeater Mode

About This Manual

Chapter 1
Introduction

This chapter describes some of the key features of the NETGEAR Wireless-N Access Point WN802Tv2. It also includes the minimum prerequisites for installation ("System Requirements" on page 1-3.), package contents ("What is in the Box" on page 1-3), and a description of the front and back panels of the WN802Tv2 ("Front Panel of the NETGEAR Wireless-N Access Point" on page 1-4).

About the NETGEAR Wireless-N Access Point WN802Tv2

The NETGEAR Wireless-N Access Point WN802Tv2 is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The WN802Tv2 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area of about 600 feet radius. Consequently, the NETGEAR Wireless-N Access Point can support a small group of users in a range of several hundred feet. Most access points can handle up to 32 users simultaneously.

The NETGEAR Wireless-N Access Point WN802Tv2 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WN802Tv2s via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network.

The auto-rate capability of the NETGEAR Wireless-N Access Point WN802Tv2 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features

The NETGEAR Wireless-N Access Point is easy to use and provides the following features:

- **Multi-In, Multi-Out (MIMO) technology**. Provides improved communication performance without additional bandwidth or transmit power. .

- **Standards Compliance**. Complies with Draft 2.0 802.11n for wireless LANs, and is backward compatible with 802.11bg.

- **Full WPA and WPA2 support.** WPA and WPA2 personal and enterprise-class strong security with dynamic encryption key generation. TKIP and AES encryption are supported.

- **RADIUS authentication support.**

- **DHCP client support.** The WN802Tv2 can act as a DHCP client and obtain information from your DHCP server for the WLAN.

- **Access control MAC address filtering**. The access control MAC address filtering feature can ensure that only trusted wireless stations can use the WN802Tv2 to gain access to your LAN. Local and remote MAC address authentication are supported.

- **Easy-to-use web-based GUI.** A web-based GUI makes installation and management easy for all users.

- **Auto-sensing ethernet connection with Auto-Uplink interface**. Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks.

- **WMM Power Save.** Allows power-critical devices to fine-tune power consumption and save power by buffering data transmitted to them.

- **Front panel LEDs.** Front panel LEDs allow easy monitoring of status and activity.

- **Flash memory.** Allows for easy firmware upgrades.

- **Quality of Service (QoS) Support.** You can configure parameters that affect traffic flowing from the wireless access point to the client station and from the client station to the wireless access point. The QoS feature allows you to prioritize time-sensitive traffic such as voice and video traffic.

- Three modes for maximum flexibility:

  – **Access Point.** In this mode, operates as a standard 802.11n wireless access point.

  – **Wireless Multi-Point Bridging.** In this mode, acts as a wireless AP or wireless bridge.for a group of bridge-mode wireless partners.

  – **Wireless Repeater Bridging.** In this mode, operates as both a wireless access point and a wireless bridge without client association.

System Requirements

Before installing the WN802Tv2, make sure your system meets the following requirements:

- A 10/100/1000 Mbps Local Area Network device such as a hub, switch or, router.
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it.
- A 100-240 V, 50-60 Hz AC Switching Power Supply.
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or later, or Mozilla Firefox 1.5 or later.
- Microsoft Windows Vista, XP, 2000, 98, Me, Mac OS, Unix, or Linux and TCP/IP (protocol) installed.
- 802.11bgn or 802.11bg - compliant devices.

What is in the Box

The product package should contain the following items:
- NETGEAR Wireless-N Access Point WN802Tv2.
- 12V, 1A Switching Power Supply.
- Vertical stand.
- Category 5 (CAT5) Ethernet cable.
- *Resource CD*.
- *NETGEAR Wireless-N Access Point WN802Tv2 Reference Manual*.
- Wall mount kit.
- Warranty and Support Information Card.

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 Access Point for repair.

Front Panel of the NETGEAR Wireless-N Access Point

The front panel of the NETGEAR Wireless-N Access Point houses three LEDs that display the status of power to the wireless access point, Ethernet connectivity and whether a wireless signal is being sent. To identify the status lights on the front panel of the WN802Tv2 and verify connection refer to Table 1-1.
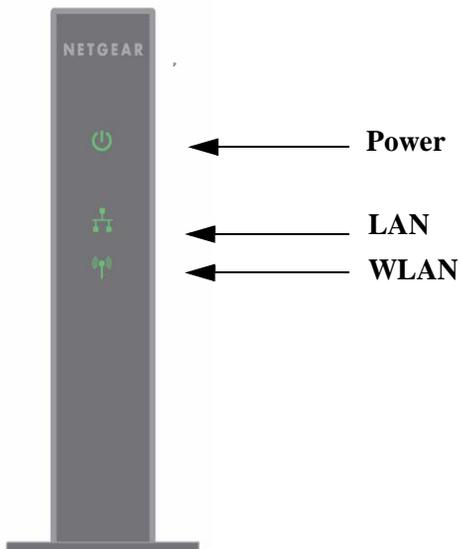
Figure 1-1 Front panel status LEDs

You can use the status lights on the front of the wireless access point to verify various conditions described in the following table:

Table 1-1. Port and system LEDs

Feature	Detailed Description	Comment
LAN Port LED	Link/Act Green – Giga Ethernet link is properly made Amber – Fast Ethernet link is properly made Sparkle – Active Off – No Link is detected	H/W control
WLAN LED	Wireless Link/Act Blue – A 802.11n WLAN link is properly made Sparkle – Network activity is occurring Off – No Link is detected	S/W control
Power/Diag	Green – Power is on Amber – System is booting up Sparkle Amber – Firmware is upgrading Off – Power is off	S/W control

Back Panel of the NETGEAR Wireless-N Access Point

The back of the WN802Tv2 contains the following listed items, viewed from top to bottom:
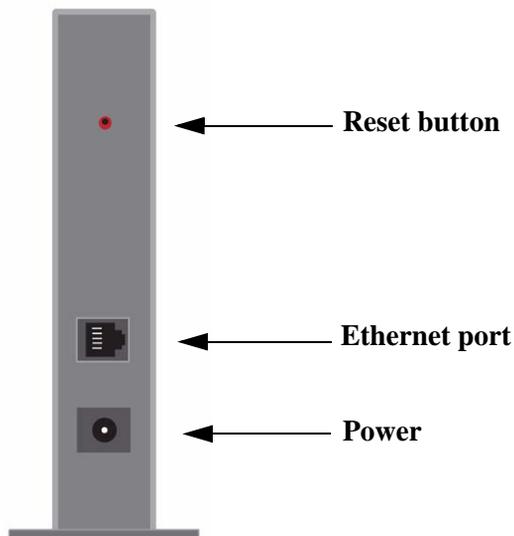
Figure 1-2 Back panel of the WN80Tv2

1. The Reset button, which is used to reset the WN802Tv2 or restore the factory default settings. See Appendix A, "Default Settings and Technical Specifications" for more information on restoring the factory default settings.

2. The Ethernet port, used to establish a 10 Mbps, 100 Mbps or 1000 Mbps connection with the network.

3. AC Universal Power Supply outlet.

NETGEAR Wireless-N Access Point Default Settings Location

The label on the rear panel of the wireless access point contains the serial number, MAC address, and default login information for your WN802Tv2 device.

Figure 1-3 Label on back panel

Wall Mount Kit

A Wall Mount kit that allows you to conveniently and securely mount your WN802Tv2 to a wall is included with your wireless access point. The kit includes a top and bottom bracket. Four screws are required to install the brackets and are not supplied with the kit. For instructions to install the the wall mount kit, see "Install the Wall Mount Kit (Optional)" on page 2-13.

Introduction

Chapter 2
Installation and Configuration

This chapter describes how to set up your NETGEAR Wireless-N Access Point WN802Tv2 for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11bgn or 802.11bg wireless adapters to connect to the Internet, or access printers and files on your LAN.

> **Note:** Indoors, computers can connect over 802.11bgn or 802.11bg wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The NETGEAR Wireless-N Access Point provides highly effective security features which are covered in detail in "Wireless Security Settings" on page 3-1. Deploy the security features appropriate to your needs

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

*   A location for the WN802Tv2 that conforms to the guidelines in the next section.

*   The wireless access point connected to your LAN through a device such as a hub, switch, router, or cable/DSL gateway.

*   One or more computers with properly configured 802.11bgn or 802.11bg wireless adapters.

Wireless Equipment Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

→ **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WN802Tv2. For complete performance specifications, see Appendix A, "Default Settings and Technical Specifications".

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

A Wall Mount Kit is provided with your wireless access point. For installation instructions, see "Install the Wall Mount Kit (Optional)" on page 2-13.

If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. NETGEAR recommends a channel spacing of 5 channels between access points (for example, use channels 1, 6, and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer.

Configuring the NETGEAR Wireless-N Access Point

To set up and configure the Wireless-N Access Point follow the steps outlined in the following sections:

Ethernet Setup

Before installing the NETGEAR Wireless-N Access Point, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11bgn or 802.11bg wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on "System Requirements" on page 1-3.

To connect the NETGEAR Wireless-N Access Point to the Ethernet network:

1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

2. Turn on your computer and configure it with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.

3. Connect an Ethernet cable from the WN802Tv2 to the computer.

4. Connect the power adapter to the WN802Tv2 and verify the following:

   • The PWR power light goes on.

   • The Ethernet port of the wireless access point is lit when connected to a powered on computer.

   • The WLAN LED should be blinking.

Configuring Your Basic WLAN Settings

The following section describes how to log in to the wireless access point and configure the basic WLAN settings.

To log in and configure the WN802Tv2 for LAN access:

1. Connect to the WN802Tv2 by opening a browser window on your PC and entering **http:// 192.168.0.233** in the address field. The WN802Tv2 Login screen displays (see Figure 2-1).

2. Enter **admin** for the user name and **password** for password, both in lower case letters.
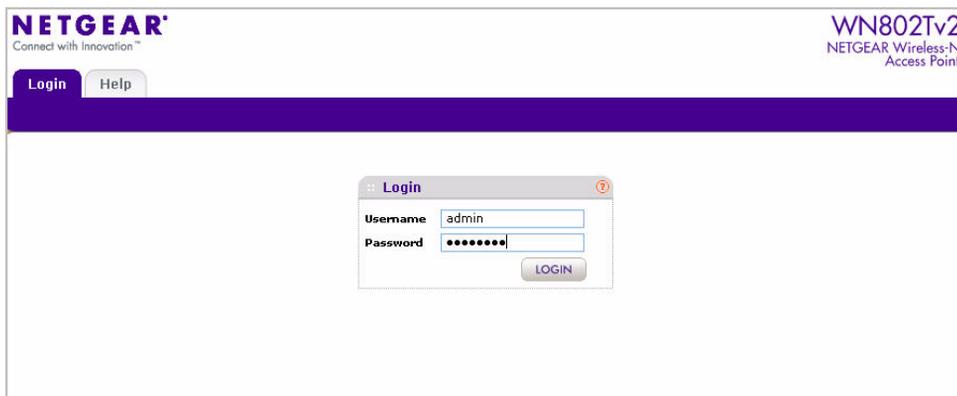
Figure 2-1 Login screen

3. Click **Login**. The main menu of the WN802Tv2 displays as shown in Figure 2-2.

   • When the wireless access point is connected to the Internet, you can click the **Documentation** link under the **Support** menu to view the documentation for the wireless access point online (see Figure 6-2).

v1.0, June 2008

- When connected to the Internet, you can also click **Knowledge Base** to access NETGEAR's knowledge base online.

- Click **Logout** to exit the WN802Tv2. (You will automatically be logged out of the wireless access point after 5 minutes of no activity.)

To set the Access Point Name and Country/Region:

1. On logging in, the General settings screen under **Configuration** > **System** > **Basic** displays**.**.
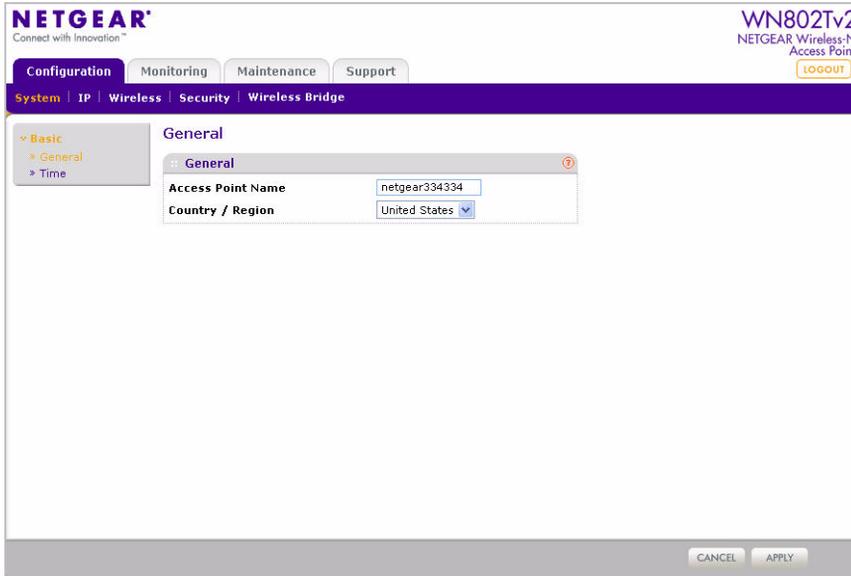
Figure 2-2 Access Point name and Country/Region

2. Enter the Access Point Name of the WN802Tv2.

The access point name is printed on the back label of the WN802Tv2. The default is **netgearxxxxxx,** where xxxxxx represents the last 6 digits of the WN802Tv2 MAC address. You may modify the default name with a unique name up to 15 characters long.

3. Select the country/region where the WN802Tv2 can be used.

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

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

To select the local time zone:

1. Select **Configuration** > **System** > **Basic** > **Time**. The Time Settings screen displays.
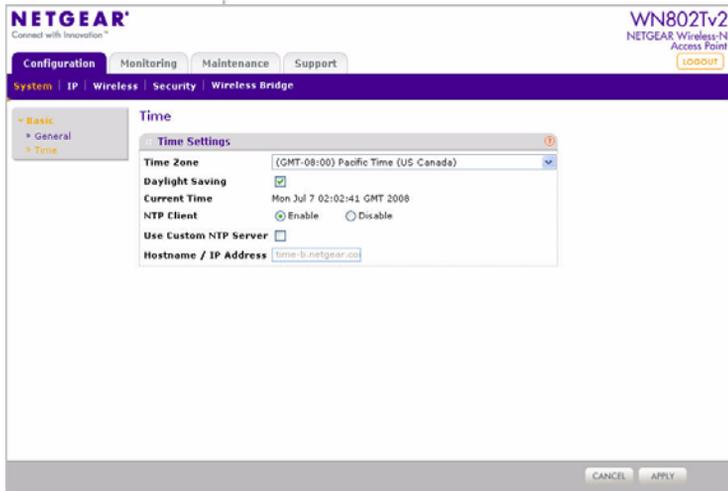
Figure 2-3 Local time zone settings

2. Configure the following information:

– **Time Zone.** From the pull-down menu, select the local time zone for your wireless access point from a list of all available time zones. The default is USA-Pacific.

– Check the **Daylight Saving** checkbox if your location uses daylight saving. The default is no adjustment.

– **NTP Client.** Enable NTP Client to synchronize the time of the access point with an NTP Server. The default is Enabled.

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

– **Use Custom NTP Server.** Check the option if you have a custom NTP server. The default is Disabled.

– **Hostname/IP Address.** Enter the host name or the IP address of the custom NTP server. The default is time-b.netgear.com

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

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

To configure the Basic LAN settings:

1. Select **IP** under **Configuration** on the main menu. The IP Settings screen displays (see Figure 2-4).The default settings should be suitable for most users and environments.
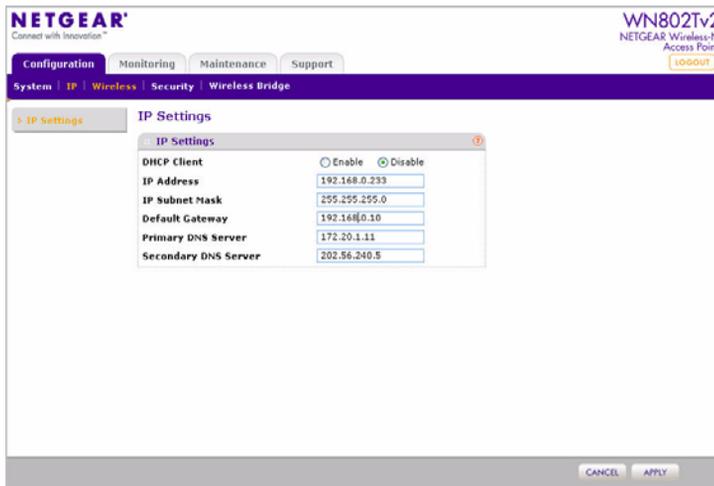
Figure 2-4 Basic IP settings

2. Enter the IP Settings fields of the WN802Tv2.

  – **DHCP Client**. By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN you can enable DHCP and the wireless access point will get its IP address, gateway and DNS server settings automatically when you connect the WN802Tv2 to your LAN.

  – **IP Address.** Enter the IP Address of your wireless access point. The default IP address is **192.168.0.233**. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP.

  – **IP Subnet Mask**. Enter the subnet mask based on the IP address that you assign. The default is 255.255.255.0.

- – **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected.

- – **Primary DNS Server.** The WN802Tv2 uses this IP address as the primary Domain Name server used by stations on your LAN.

- – **Secondary DNS Servers.** The WN802Tv2 uses this IP address as the secondary Domain Name Server used by stations on your LAN.

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

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

Configuring Basic Wireless Settings

The following section describes how to configure the basic wireless settings for the 802.11b, 802.11bg and 802.11ng modes.

To configure the NETGEAR Wireless-N Access Point wireless settings of your wireless access point:

1. From the main menu under **Configuration**, select **Wireless**.The Wireless Settings screen displays as shown in Figure 2-5.
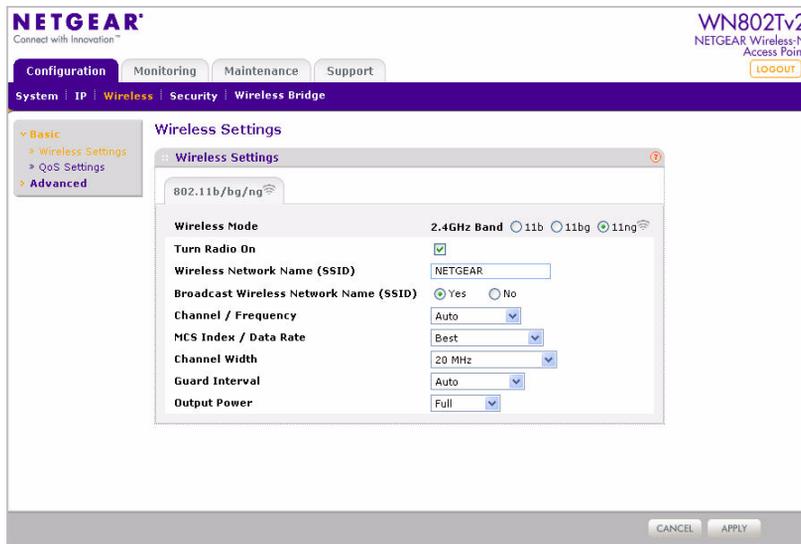
Figure 2-5 Basic wireless settings

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

- **Wireless Mode**. Select the desired wireless operating mode by clicking inside the appropriate radio button:

  - 11b – 802.11b wireless stations can be used (802.11g and 802.11ng wireless stations can still be used if they can operate in 802.11b mode.).

  - 11bg – both 802.11b and 802.11bg wireless stations can be used (802.11n wireless stations can still be used if they can operate in 11bg mode).

  - 11ng – 802.11ng, 802.11g and 802.11b wireless stations can be used.

  The default is 11ng.

- **Turn Radio On**. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.

- **Wireless Network Name (SSID)**. Enter a 32-character (maximum) service set ID in this field; the characters are case sensitive. When the wireless access point is deployed in "infrastructure" mode, the SSID assigned to a wireless device must match the wireless access point SSID in order for the wireless device to communicate with the WN802Tv2. If they do not match, you will not get a wireless connection to the WN802Tv2. The default is NETGEAR.

• **Broadcast Wireless Network Name.** If enabled, the wireless access point broadcasts its SSID allowing wireless stations which have a "null" (blank) SSID to adopt the correct SSID. If set to Disable, the SSID is not broadcast. The default is Enable.

• **Channel/Frequency**. From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. The default is channel Auto.

Do not change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. Alternatively, you can select the Auto channel option for the AP to intelligently pick the channel with least interference. See the article on "Wireless Channels" available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, "Related Documents"). When selecting or changing channels, some points to bear in mind:

– Access points use a fixed channel. You can select the channel used. This allows you to select a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available

– If using multiple access points, it is better if adjacent access points use different channels to reduce interference. NETGEAR recommends a channel spacing of 5 channels (for example, channels 1, 6, and 11). between adjacent access points.

– Wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.

• **MCS Index/Data Rate**. From the pull-down menu, select the available transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary. (When Auto Channel is enabled in the 802.11ng mode, then the default Channel Width mode is 20MHz). The possible data rates supported are:

• **Data Rates for Channel Width=20MHz and Guard Interval=short (400ms):** Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps

• **Data Rates for Channel Width=20MHz and Guard Interval=long (800ms):** Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps

• **Data Rates for Channel Width=40MHz and Guard Interval=short:** Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps

- **Data Rates for Channel Width=40MHz and Guard Interval=long:** Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps

The default is **Best** which is the optimal setting.

- **Channel Width.** From the pull-down menu, select the desired channel width.

    - 20 MHz - This is the static, legacy mode. It gives the least throughput.

    - 40 MHz - This is the static, high-throughput mode.

    - 20/40 MHz - This is the dynamic, compatibility mode. Legacy clients can operate at 20 MHz and 11n clients can operate at 40 MHz.

- **Guard Interval.** From the pull-down menu, select the desired guard interval. The guard interval protects from interference from other transmissions. The default is Auto.

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

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

Configuring QoS Settings

WMM Support. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature and part of the 802.11e standard. It provides for prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. Time-dependent information, such as video or audio, has a higher priority than normal traffic.

For an application to receive the benefits of WMM QoS, both the application and the client running that application must be WMM-enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

The default setting is Enabled.

To configure your wireless QoS settings for 11b, 11bg, or 11ng modes:

1. Under the **Configuration** tab on the main menu, select **Wireless**, then select **QoS Settings** under **Basic** from the side menu. The QoS Settings screen displays, as shown in Figure 2-6:
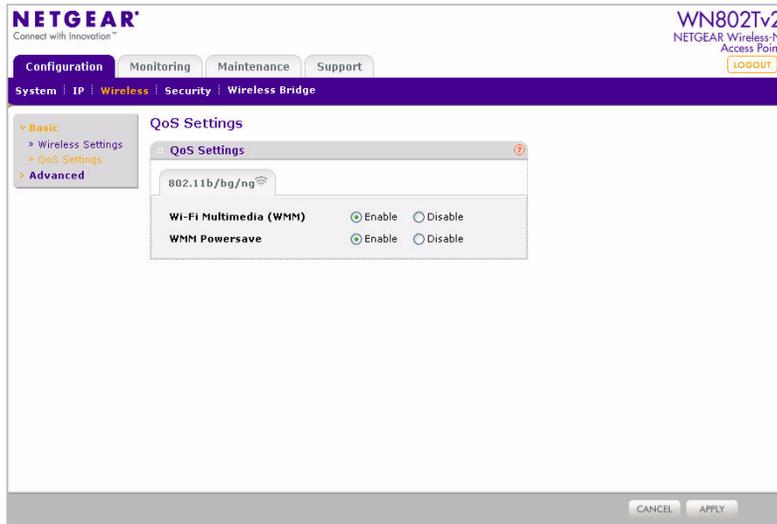
Figure 2-6 QoS settings

2. Wi-Fi Multimedia (WMM) is enabled by default. Check the Disable checkbox to disable WMM support.

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

Configuring WMM Power Save

WMM power save is a set of features in 802.11e that help to conserve power for battery-operated devices in a wireless LAN.

To configure WMM Power Save settings:

1. Under the **Configuration** tab on the main menu, select **Wireless**, then select **QoS Settings** under **Basic** from the side menu. The QoS settings screen displays (see Figure 2-6).

2. WMM Power Save is enabled by default. Check the **Disable** checkbox to disable it.

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

Verifying Basic Wireless Connectivity

Follow the instructions in this section to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs (see Chapter 3, "Wireless Security Settings").

1. From a web browser, log in to the WN802Tv2 using its default address of **http://192.168.0.233**. Use the default user name of **admin** and default password of **password**—or use a new LAN address and password if you have set them up.

2. From the General screen under **Configuration** > **System** > **Basic** verify that the correct **Country/Region** in which the wireless interface will operate has been selected.

3. From the Wireless Settings screen under **Configuration** > **Wireless** > **Basic** verify your Wireless Mode—**11b**, **11bg**, or **11ng**. Verify that the correct (default) channel has been selected for your network.

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

Click **Apply** to save any changes.

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

Deploying the NETGEAR Wireless-N Access Point

Now that you have completed the setup steps, you can deploy the WN802Tv2 in your network. If needed, you can now reconfigure the computer you used in step 1 in "Configuring the NETGEAR Wireless-N Access Point" on page 2-2 back to its original TCP/IP settings.

To deploy the NETGEAR Wireless-N Access Point:

1. Disconnect the WN802Tv2 and position it where it will be deployed. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.

2. Connect an Ethernet cable from your NETGEAR Wireless-N Access Point to a LAN port on your router, switch, or hub. Connect the power adapter to the wireless access point and plug the power adapter into a power outlet. The PWR, LAN, and Wireless LAN LEDs and should light up

> **Tip:** Before mounting the WN802Tv2 in a high location, first set up and test the WN802Tv2 to verify wireless network connectivity.

Install the Wall Mount Kit (Optional)

Before you begin installation, check to make sure that the four screws selected to secure the brackets fit flush within the molding of the bracket. An illustration of the installation steps is shown in Figure 2-7.

To install the wireless access point mounting brackets:

1. Place the bottom bracket on the wall where you want to install the WN802Tv2. Securely screw the bottom bracket into the wall, making sure the screws are flush with the bracket (Step 1).

2. Snap the WN802Tv2 into place on the bottom bracket (Step 2). The tabs on the bottom of the bracket will snap into the slots on the bottom of the WN802Tv2.

3. Firmly secure the top bracket onto the WN802Tv2 and attach the bracket with two additional screws (Step 3). Ensure that the bracket flange engages with the top lip of the WN802Tv2 before screwing in the bracket.

Should you need to remove the WN802Tv2, unscrew the top bracket, and then unsnap the WN802Tv2 from the bottom bracket. Never try to remove your wireless access point before removing the top bracket.
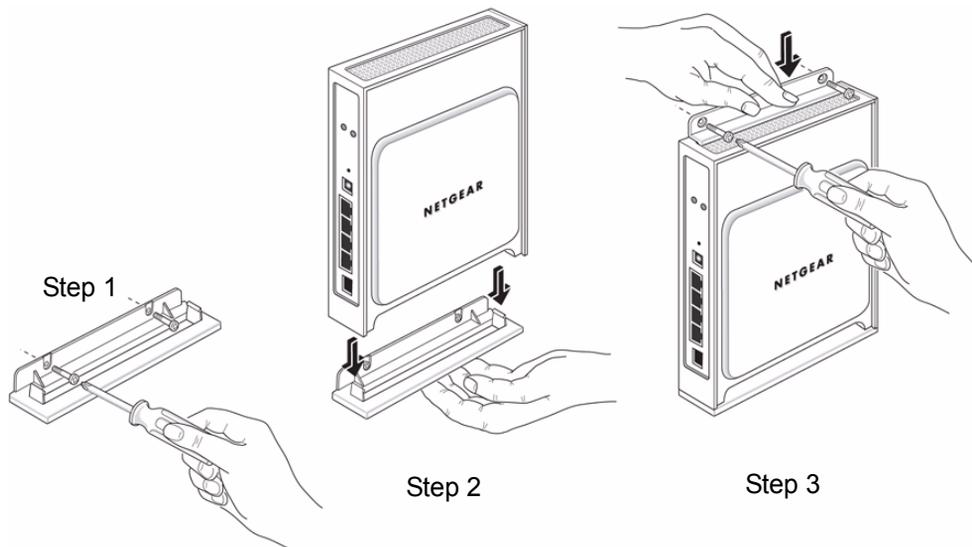
Figure 2-7 Installing the wall mount kit

Configuring and Testing Your PCs for Wireless Connectivity

Program the wireless adapter of your PCs to have the same SSID and channel that you configured for the WN802Tv2 (see "Configuring Basic Wireless Settings"). Check that they have a wireless link and are able to obtain an IP address by DHCP from the WN802Tv2, when DHCP is enabled.

> **→ Note:** If you are configuring the WN802Tv2 from a wireless computer and you change the SSID, channel, or security profile settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

Once your PCs have basic wireless connectivity to the WN802Tv2, you can deploy the WN802Tv2 and configure the advanced wireless security functions (see Chapter 3, "Wireless Security Settings").

Logging in to the NETGEAR Wireless-N Access Point

The WN802Tv2 is set, by default, with the IP address of **192.168.0.233** with DHCP disabled.

> **Note:** If logging in using the default IP address, the computer you are using to connect to the WN802Tv2 should be configured with an IP address that starts with 192.168.0.x and a subnet mask of 255.255.255.0.

If DHCP is enabled, you can connect to the WN802Tv2 after the DHCP server on your network assigns it a new IP address:
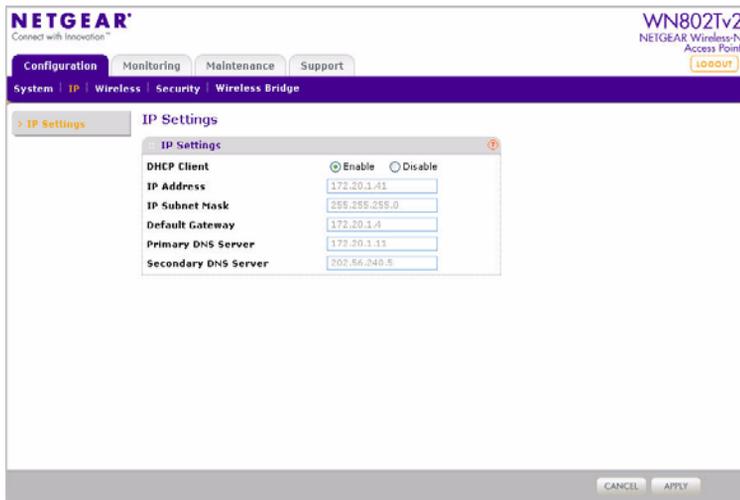
Figure 2-8 Enable DHCP client

Reserve an IP address (based on the WN802Tv2's MAC address) on the DHCP server. That way, if your router is deployed across several segments, you can configure the wireless access point with a static IP address which you can always use to log in to make future configuration changes.

To log in using the default IP address:

1. Open a Web browser such as Mozilla Firefox or Internet Explorer.

2. Connect to the WN802Tv2 by entering the default address of **http://192.168.0.233** into your browser.

http://192.168.0.233

Figure 2-9 Default IP address of the WN802Tv2

3. The login screen displays (see Figure 2-1). Enter **admin** for the user name and **password** for the password, both in lower case letters.

4. Click **Login.**

Your Web browser should automatically find the NETGEAR Wireless-N Access Point and display the main menu (see Figure 2-2).

Chapter 3
Wireless Security Settings

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

Wireless Security Options

The following is a list of wireless security options you can select from, depending on your security needs:

1. No Security: Easy, but no security.

2. MAC Access List: No data security.

3. WEP: Security, but vulnerable.

4. WPA or WPA-PSK: Strong security.

5. WPA2 or WPA2-PSK: Very strong security.

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

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WN802Tv2. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Vista and Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP open authentication and WEP data encryption will block all but the most determined eavesdropper.

- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.
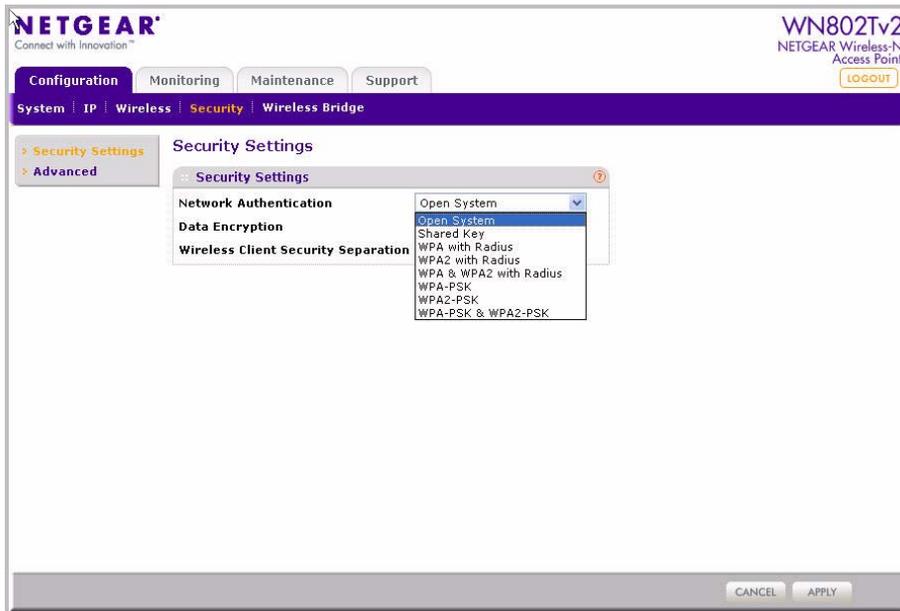
Figure 3-1 Network authentication types

Security options are available under **Configuration** > **Security** > **Security Settings** (see Figure 3-1). An overview of the information that is required to set up security options follows—including a description of the Network Authentication choices that are available:

- **Wireless Network Name or Service Set Identifier (SSID).** This is the name of your wireless network. It is used to identify the particular 802.11 wireless LAN to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.It is set to the default name of NETGEAR (see "Configuring Basic Wireless Settings" in Chapter 2). It is normal for multiple access points to share the same SSID if they provide access to the same network.

- **Broadcast Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Vista and Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. The default is enabled.

- **Security Settings.** Configure the following settings:

  - **Network Authentication**. The WN802Tv2 Access Point is set by default as an open system (no authentication) with no data encryption. When setting up Network Authentication, bear in mind the following:

    – If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options may be unavailable.

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

    You can configure the WN802Tv2 to use the types of network authentication shown in the following table:

Table 3-1. Network Authentication Types

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

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

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

Table 3-2. Data Encryption Settings

Data Encryption Type	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that will only work with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA and WPA2.
AES	This is the standard encryption method for WPA2.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

➡️ **Note:** WEP and TKIP provide only legacy rates of operation. So, AES is the recommended solution to use the 802.11n rates and speed.

Use of passphrases and keys are explained in the following section:

- **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click **Generate Keys**. You can also enter the keys directly. These keys must match the other wireless stations.

- **Key 1, Key 2, Key 3, Key 4**. If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

- **Preshared Key Passphrase.** If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.

- **Wireless Client Security Separation**. If enabled, the associated wireless clients will not be able to communicate with each other (this feature is intended for hotspots and other public access situations). The default is No.

> **Note:** If you are using a RADIUS server, configure the RADIUS settings first, as described in the "Configuring WPA with RADIUS" on page 3-9.

SSID and WEP/WPA Settings Setup Form

802.11b/bg/ng Configuration

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

- **SSID***:* The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR** is the default WN802Tv2 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the following line.

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

- **Authentication:**

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

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WN802Tv2.

- **WEP Encryption Keys.**

  Circle one: 64, 128, or 152 bits. (Enter all four WEP encryption keys for the key size chosen.)

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____

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

Record the WPA-PSK/WPA2-PSK key _____

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

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

RADIUS Server Settings

You can setup or modify the RADIUS server settings to complement network authentication security options. The RADIUS server can be used with WPA/WPA2 network authentication. When using a RADIUS server, the RADIUS server settings must be configured before completing the Network Authentication security profile (see "Configuring WPA with RADIUS" on page 3-9, "Configuring WPA2 with RADIUS" on page 3-10, or "Configuring WPA and WPA2 with RADIUS" on page 3-11 for specifics on implementing these security options).

> **Note:** The RADIUS server settings only need to be configured once per wireless access point.

To set up or modify the RADIUS server settings see: "Configuring the RADIUS Server Settings" on page 4-13.

Configuring Wireless Security

The following section covers configuration of each of the available wireless security options.

Configuring WEP

To configure WEP data encryption:

1. From the **Network Authentication** drop-down menu on the Securit Settings screen (see Figure 3-1), select either **Open System** or **Shared Key**.

2. From the **Data Encryption** drop-down menu, select encryption strength (64-bit, 128-bit, or 152-bit, see Figure 3-2). For **Open System**, the default is None. If encryption is selected, fields for the passphrase and four keys display on the same screen.
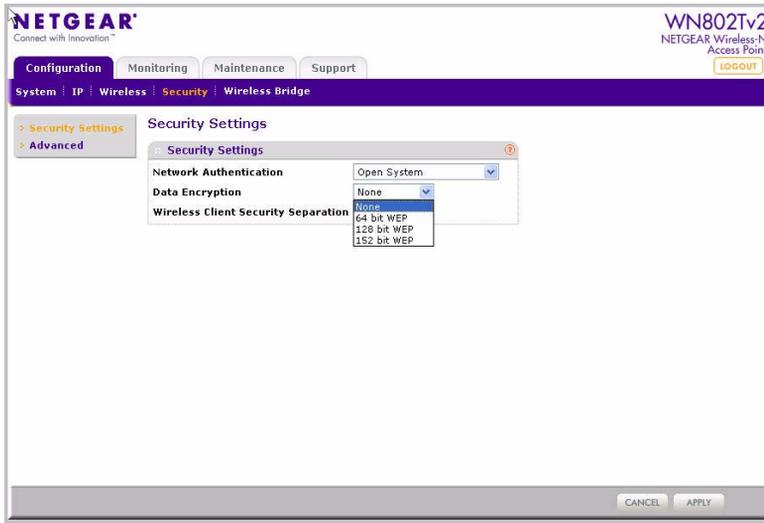
Figure 3-2 WEP - Data encryption strength options

3. You manually or automatically program the four data encryption keys (see Figure 3-3). These values must be identical on all PCs and wireless access points in your network. Select either:

- Automatic – Enter a word or group of printable characters in the **Passphrase** field and click **Generate Keys**. The four key fields will be automatically populated with key values.

- Manual – Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit, 26 digits for 128-bit, and 32 for 152-bit (any combination of 0-9, a-f, or A-F).
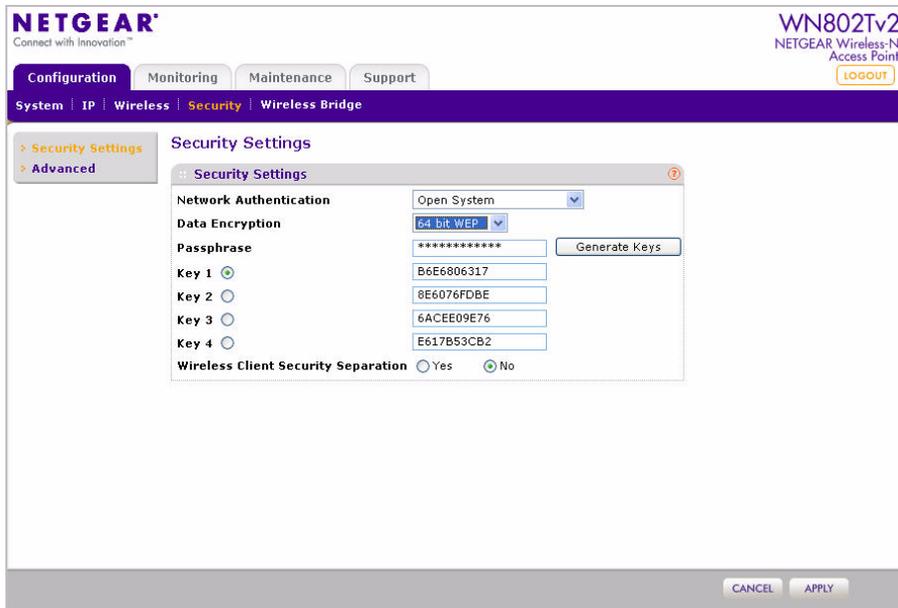
Figure 3-3 WEP - Data encryption keys

4. Select the key to be used as the default key by clicking the radio box of that key. (Data transmissions are always encrypted using the default key.).

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

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

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

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

Configuring WPA with RADIUS

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

To configure WPA, follow these steps:

1. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the side menu, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.

2. Enter the RADIUS server settings as shown in "Configuring the RADIUS Server Settings" on page 4-13.

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

4. Under the **Configuration** tab, select **Security** from the main menu, and then select **Security Settings** from the side menu.
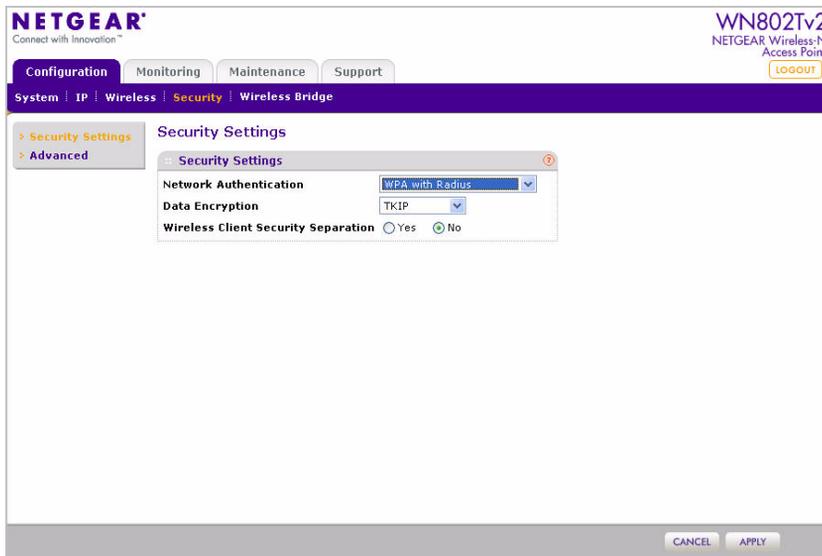
Figure 3-4 WPA with RADIUS security settings

5. Select **WPA with RADIUS** from the **Network Authentication** drop-down menu. Data encryption will be set to **TKIP** by default (see Figure 3-4).

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

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

Configuring WPA2 with RADIUS

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.
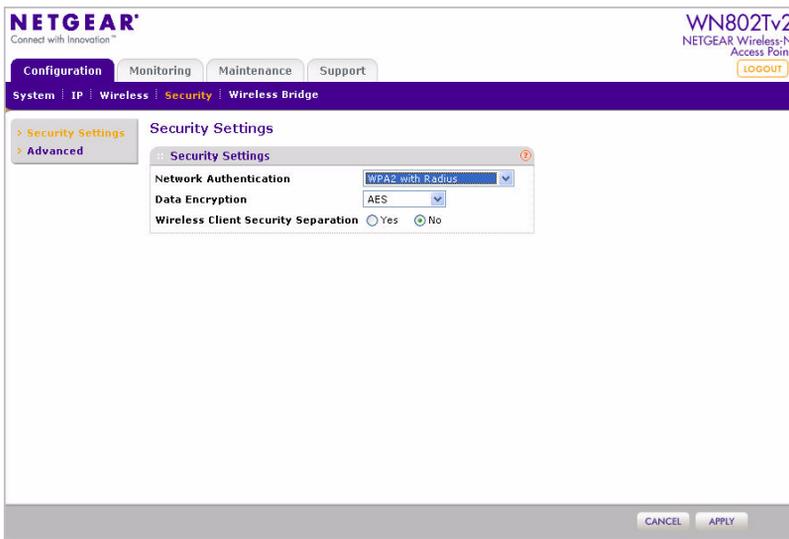
Figure 3-5 WPA2 with RADIUS security settings

To configure WPA2 with RADIUS:

1. Under the **Configuration** tab, select Security on the main menu, select **Advanced** from the side menu, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.

2. Enter the RADIUS settings as shown in "Configuring the RADIUS Server Settings" on page 4-13.

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

4. Under the **Configuration** tab, select **Security** from the main menu, and select **Security Settings** from the side menu. From the **Network Authentication** drop-down menu, select **WPA2 with RADIUS** from the list. By default, Data Encryption will be set to **AES**.

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

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

Configuring WPA and WPA2 with RADIUS

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

- Vista, Windows XP and Windows2000 with Service Pack 3 or later, do include the client software that supports WPA/WPA2. The wireless adapter hardware and driver must also support WPA/WPA2.

- Service Pack 3 does not include the client soft ware that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.
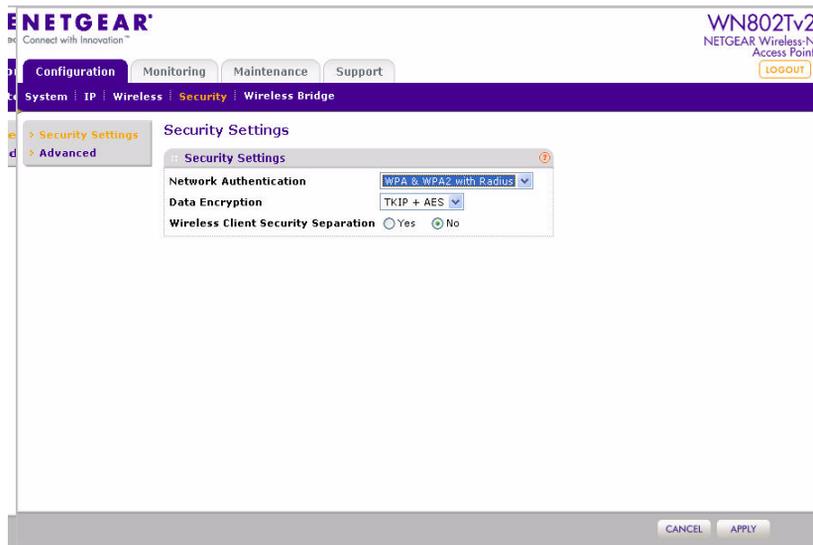
Figure 3-6 WPA and WPA2 with RADIUS security settings

To configure WPA and WPA2 with RADIUS:

1. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the side menu, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.

2. Enter the RADIUS server settings as shown in "Configuring the RADIUS Server Settings" on page 4-13.

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

4. Under the **Configuration** tab, select **Security** from the main menu, and then select **Security Settings** from the side menu. From the **Network Authentication** drop-down menu, select **WPA & WPA2 with RADIUS** from the list. By default, **Data Encryption** will be set to **TKIP+AES**.

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

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

Configuring WPA-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Vista, Windows XP and Windows 2000 with Service Pack 3 or later include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.
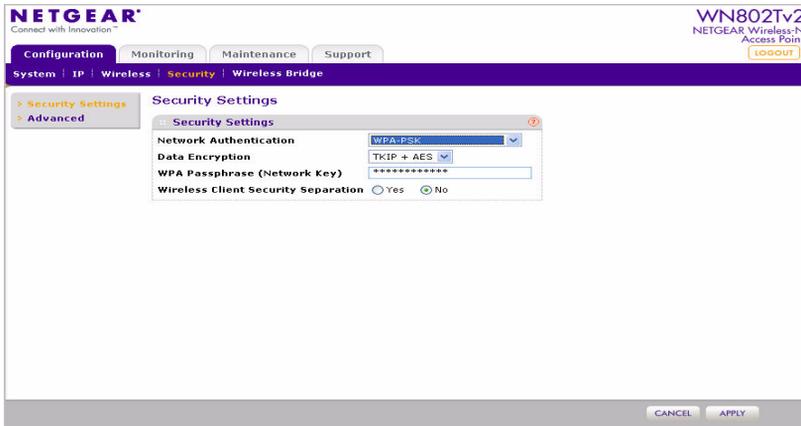
Figure 3-7 WPA-PSK security settings

To configure WPA-PSK:

1. From the **Configuration** menu select **Security** and from the side menu select **Security Settings**.

2. From the **Network Authentication** drop-down menu, select **WPA-PSK**. By default, **Data Encryption** will be set to **TKIP**.

3. Enter the preshared key passphrase (**Network Key**).

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

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

Configuring WPA2-PSK

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.
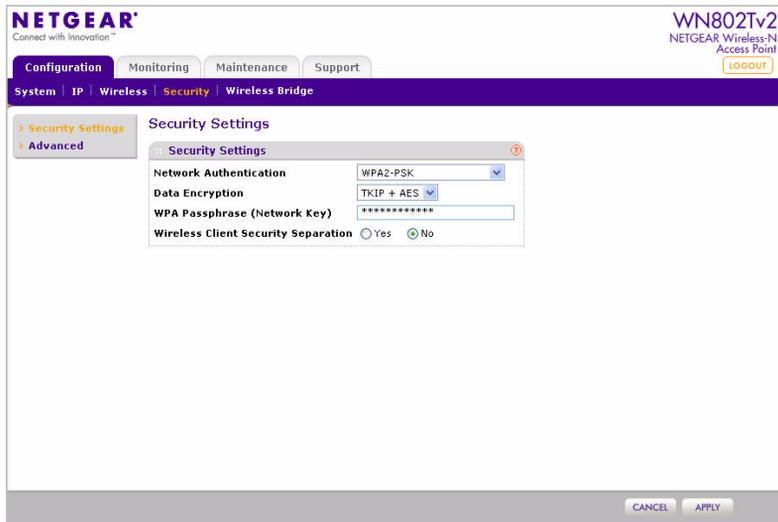
Figure 3-8   WPA2-PSK security settings

To configure WPA2-PSK:

1. From the **Configuration** menu select **Security** and from the side menu select **Security Settings**.

2. From the **Network Authentication** drop-down menu, select **WPA2-PSK** from the list. By default, **Data Encryption** will be set to **AES**.

3. Enter the preshared key passphrase (**Network Key**).

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

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

Configuring WPA-PSK and WPA2-PSK

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

• Vista, Windows XP and Windows 2000 with Service Pack 3 or higher do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.

• Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.
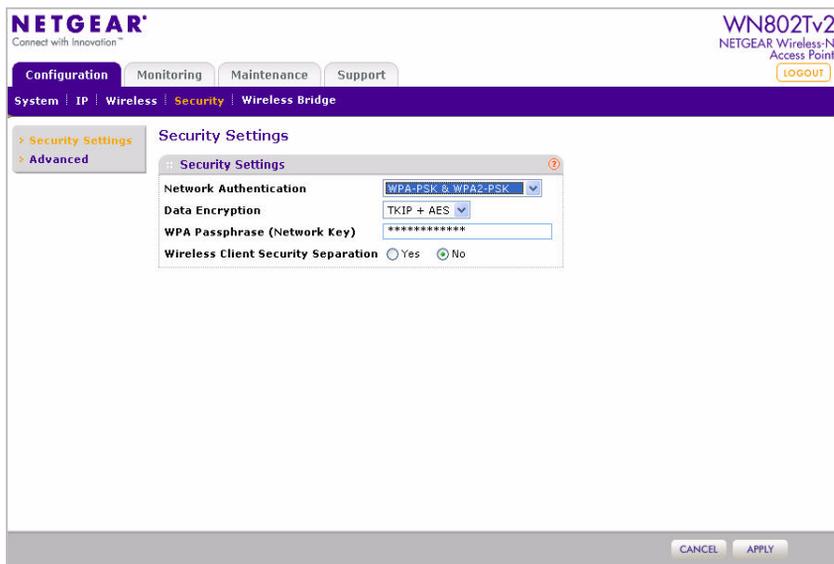
Figure 3-9 WPA-PSK and WPA2-PSK security settings

To configure WPA-PSK and WPA2-PSK:

1. From the **Configuration** menu select **Security** and from the side menu select **Security Settings**.

2. From the **Network Authentication** drop-down menu, select **WPA-PSK & WPA2-PSK**. By default, **Data Encryption** will be set to **TKIP+AES**.

3. Enter the WPA Passphrase (**Network Key**).

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

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

Restricting Wireless Access by MAC Address

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

> **Note:** When configuring the WN802Tv2 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click **Apply**. You must then access the wireless access point from a wired computer or from a wireless computer that is on the access control list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the WN802Tv2 using the default address of **192.168.0.233,** user name of **admin** and default password of **password**, or whatever LAN address and password you have set up (see Figure 2-1).

2. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the side menu, and then select **Access Control List.** The Access Control List screen displays. (Figure 3-10).
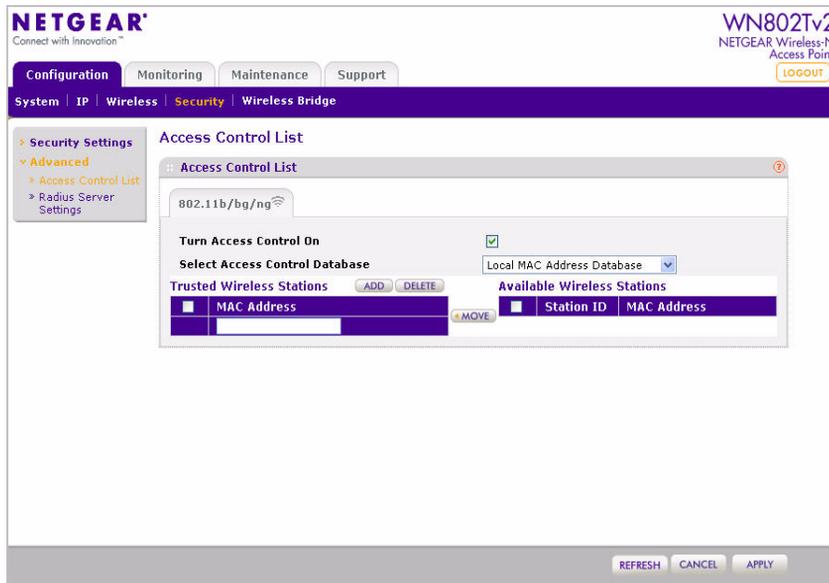
Figure 3-10 Access control list

3. Check the **Turn Access Control On** checkbox to enable the access control feature.

4. Select the desired access control database from the **Select Access Control Database** drop-down menu.The options are:

- **Local MAC Address Database** – The access point will use the local MAC address table for access control. This is the default.

- **Remote MAC Address Database** – The access point will use the MAC address table located on the external RADIUS server on the LAN for access control. If you select this database, you must configure the RADIUS server settings first (see "Configuring the RADIUS Server Settings" on page 4-13)

5. The **Trusted Wireless Stations** list shows any wireless stations you have entered. If you have not entered any wireless stations this list will be empty. To delete an existing entry, select it and then click **Delete**.

6. Click **Refresh** to refresh the **Available Wireless Stations** (wireless stations that are associated) list found in your area.

7. Select the station you wish to add to the **Trusted Wireless Stations** list from the list of **Available Wireless Stations** and click **Move**. Do this for each station you wish to add.

8. If the station you want is not in the **Available Wireless Stations** list, enter the MAC address of the station manually in the **Trusted Wireless Stations** list. (You can usually find the MAC address printed on the bottom of the wireless adapter.)

9. Click **Add** to add the wireless device to the **Trusted Wireless Stations** list. Repeat these steps for each additional device you want to add to the list.

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

Now, only devices on this list will be allowed to wirelessly connect to the WN802Tv2.

Chapter 4
Management

This chapter describes how to use the management and information features as well as the advanced wireless settings features of your NETGEAR Wireless-N Access Point WN802Tv2. The management and information features can be found under the **Maintenance** tab on the main menu.

Changing the Administrator Password

→ **Note:** Before changing the WN802Tv2 password, use the backup utility to save your configuration settings. If you forget your new password, you must reset the WN802Tv2 back to the factory defaults and use the default password. Consequently, you will have to restore any WN802Tv2 configuration settings you have made. The backup file can be used in this event.

The default password for the WN802Tv2 is **password**. NETGEAR recommends that you change this password to a more secure password.

To change the password:

1. Select **Password** > **Change Password** under the **Maintenance** menu. The Change Password screen displays..
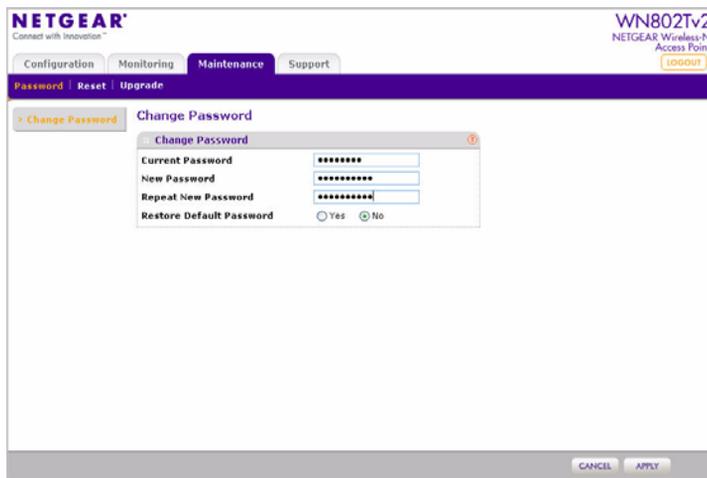
Figure 4-1 Change password

2. Enter the current password, in the **Current Password** field.

3. Enter the new password, twice, in the **New Password** and **Repeat New Password** fields.

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

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

To restore the default password (see Figure 4-1):

1. Select the **Restore Default Password** radio button.

2. Click **Apply.** The default password is restored.

Upgrading the Wireless Access Point Firmware

The software of the NETGEAR Wireless-N Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Firmware upgrade files can be downloaded manually from the NETGEAR Web site. The upgrade file can then be sent using your browser as shown in the following steps.

> **Note:** The Web browser used to upload new firmware into the NETGEAR Wireless-N Access Point must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or later, or Mozilla Firefox.1.5 or later.

To upgrade the firmware:

1. Go to the NETGEAR web site at *http://kbserver.netgear.com/downloads_support.asp* to get new versions of the WN802Tv2 access point software.

2. Download the new software file for your WN802Tv2 access point.

3. From the **Maintenance** menu of the browser interface, click **Upgrade**. The Firmware Upgrade screen displays:
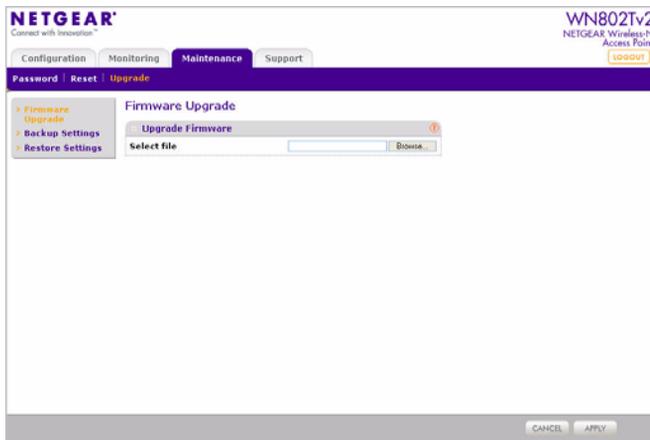
Figure 4-2 Upgrade firmware - browse file

4. Click **Browse** and go to the location of the downloaded file.

5. Click **Apply**.

6. The WN802Tv2 will check if the file is valid and load it in to the firmware. Once the file has been loaded the AP reboots.

> ⚠️ **Warning:** When uploading firmware to the WN802Tv2, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the WN802Tv2 inoperable.

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

Configuration File Management

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

To backup settings:

1. From the main menu of the browser interface, select **Maintenance** > **Upgrade**. Select **Backup Settings** from the side menu:

Figure 4-3   Backup configuration settings

2. Click **BACKUP** to select the backup option and save your configuration settings.

– If you do not have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click **BACKUP**.

– If you have your browser set up to save downloaded files automatically, the file will be automatically saved to the download location

The current settings are saved to a file under the default name *Config*.

To restore settings from a backup file:

1. In Step 1 of the previous section, click **Restore Settings** on the side menu**.**.
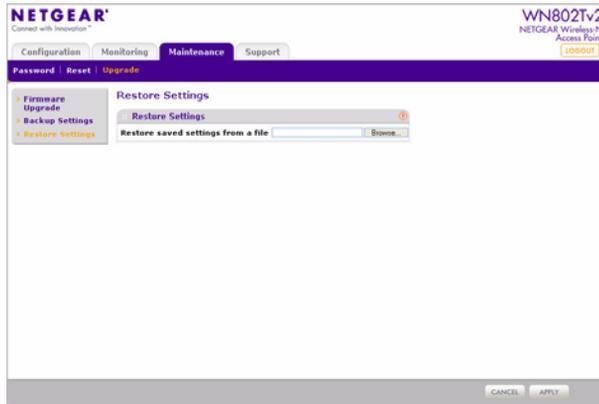
Figure 4-4 Restore saved configuration settings

2. Click **Browse** at the **Restore Saved Settings from a File** box. Locate and select the previously saved backup file (by default, *Config*).

3. Click **Apply**.

The wireless access point is restored to its previous settings and restarts. This takes about one minute.

> ⚠️ **Warning:** Do not try to go online, turn off the access point, shut down the computer or do anything else to the access point until it finishes restarting. When the PWR light turns green (access point has rebooted), wait a few more seconds before doing anything with the access point.

Rebooting the NETGEAR Wireless-N Access Point

You can reboot the wireless access point from the browser interface or by using the Reset button on the rear panel (see Figure 1-2 on page 1-6).

To reboot the wireless access point from the user interface:

1. From the main menu of the browser interface, select **Maintenance > Reset** and then **Reboot AP** on the side menu. The Reboot AP screen displays (Figure 4-5):.
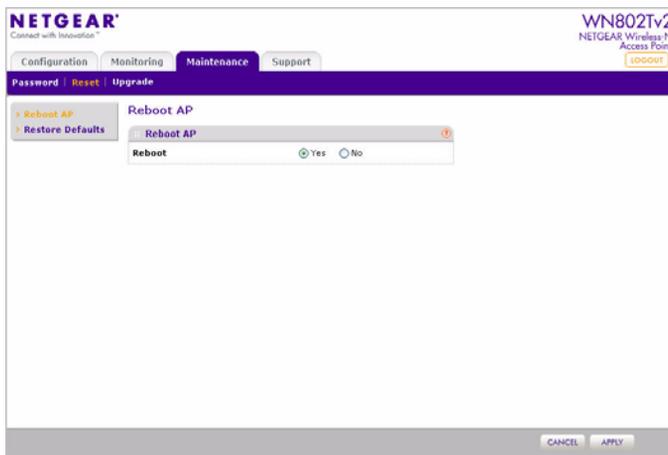
Figure 4-5 Reboot the AP

2. Select the **Yes** radio button next to the **Reboot** option, and then click **Apply**.

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

To erase the current settings and reset the wireless access point to the original factory default settings**:**

1. In Step 1 of the previous section, select **Restore Defaults** from the side menu **(**see **Figure 4-5).**

2. Select the **Yes** radio button next to the **Restore to factory default settings** option.

3. Click **Apply**.

The factory settings are restored and the access point reboots. This takes about a minute. A list of the factory default settings can be found in the appendix in.Table A-1.

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

Viewing the Available Wireless Stations List

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

To view the list of available wireless stations:

1. From the **Configuration** menu of the browser interface, select **Monitoring** and then **Wireless Stations.** The **Available Wireless Stations** list displays (see Figure 4-6).

2. Click **Refresh** to update the list and force the wireless access point to look for associated devices.
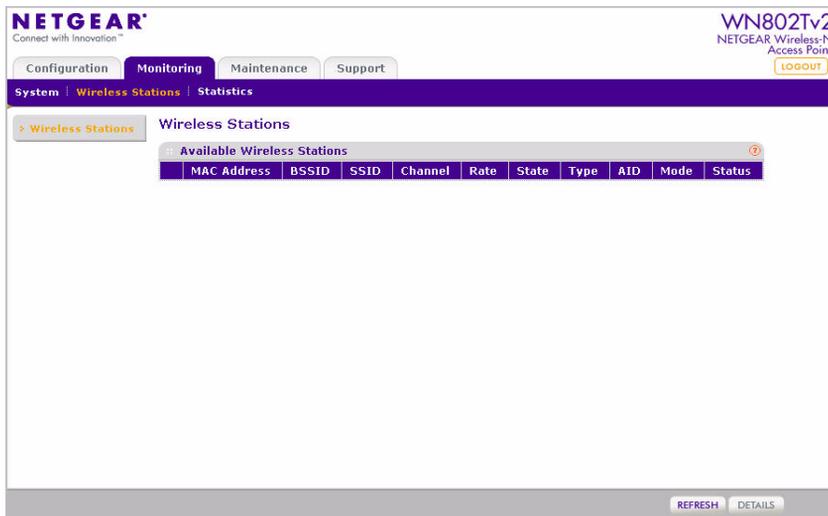
Figure 4-6 Available wireless stations list

• For each device, the **Available Wireless Stations** table shows data such as the MAC address, the **BSSID**, and the **SSID**.

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

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

Viewing General Summary Information

The **System** screen, under the **Monitoring** tab provides a summary of the current WN802Tv2 configuration settings, including current IP and wireless settings. This information is read only, so any changes must be made on other screens.

To access the System screen:

Under the **Monitoring** tab, select **System** on the main menu to view the System screen, shown in Figure 4-7. This screen shows the current values of parameters described in Table 4-1:

Table 4-1. System Information fields

Field	Description
Access Point Information	
Access Point Name	The default name may be changed, if desired.
MAC Address	Displays the Media Access Control (MAC) address of the wireless access point's Ethernet port.
Country/Region	Displays the domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Current Time	The current date and time in the time zone.

Table 4-1.   System Information fields (continued)

Field	Description
Current IP Settings	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
Current Wireless Settings for 802.11b/bg/ng	
Access Point Mode	Identifies the operating mode of the WN802Tv2: Standard Access Point, Point to Multi-point bridge, or Repeater without wireless association
Channel/Frequency	Identifies the channel the wireless port is using. 11 is the default channel setting. (Channel frequencies used on each channel can be found in "Wireless Communications"; a link to this article is in Appendix B, "Related Documents".).

Figure 4-7 General system information

Viewing Network Traffic Statistics

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

To display statistics for the wireless access point:

1. Select **Statistics** under the **Monitoring** tab on the main menu. The Statistics screen displays.

- The Wired Ethernet section of the table displays traffic statistics for the wired ethernet interface.

- The Wireless 11ng section displays traffic statistics for the wireless interface.
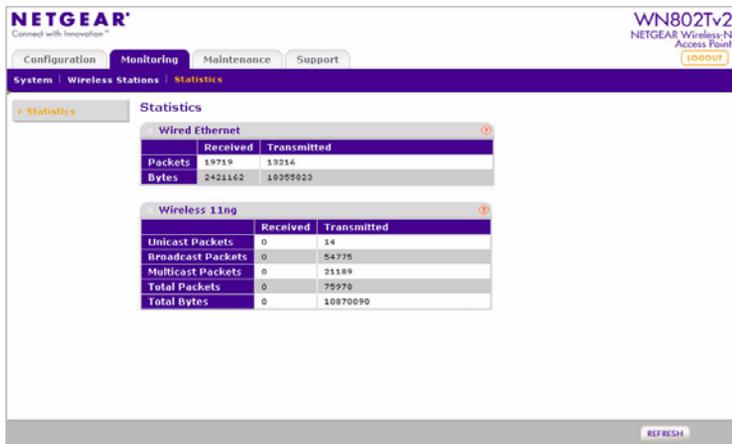
Figure 4-8 Network traffic statistics

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

The following table describes the information fields detailed on the Statistics screen:

Table 4-2. Statistics Fields

Field	Description
Wired Ethernet	
Packets	The number of packets sent and received since the WN802Tv2 was restarted.
Bytes	The number of bytes sent and received since the WN802Tv2 was restarted.
Wireless 11n/g	
Unicast Packets	The number of unicast packets sent and received since the WN802Tv2 was restarted.
Broadcast Packets	The number of broadcast packets sent and received since the WN802Tv2 was restarted.

Table 4-2. Statistics Fields

Field	Description
Multicast Packets	The number of multicast packets sent and received since the WN802Tv2 was restarted.
Total Packets	The total number of wireless packets sent and received since the WN802Tv2 was restarted.
Total Bytes	The total number of wireless bytes sent and received since the WN802Tv2 was restarted.

Configuring the Advanced Wireless Settings

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

*   **RTS threshold.** The Request to Send threshold packet size determines if the wireless access point should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission:

    –   With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period.

    –   With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

    The default value is 2346 bytes.

*   **Fragmentation Length.** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

    The default value is 2347 bytes.

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

    The default value is 100 ms.

*   **Aggregation Length.** The default value is 65535 bytes.

- **AMPDU (**Aggregated-MAC Packet Data Unit**).** This is a feature in IEEE 802.11e and 802.11n Wireless LAN Standard, which allows to build a group of frames before they are transmitted. The default is Enabled

- **RIFS** (Reduced Inter-Frame Spacing) transmission**.** The default is Disabled**.**

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

  The default value is 3.

- **Preamble Type**. A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. The Auto setting will automatically handle both long and short preamble.

  The default setting is Auto.

To modify the Advanced Wireless Settings:

1. Select **Wireless** under the Configuration tab, then select **Advanced** from the side menu. The Wireless Settings screen displays as shown in Figure 4-9.
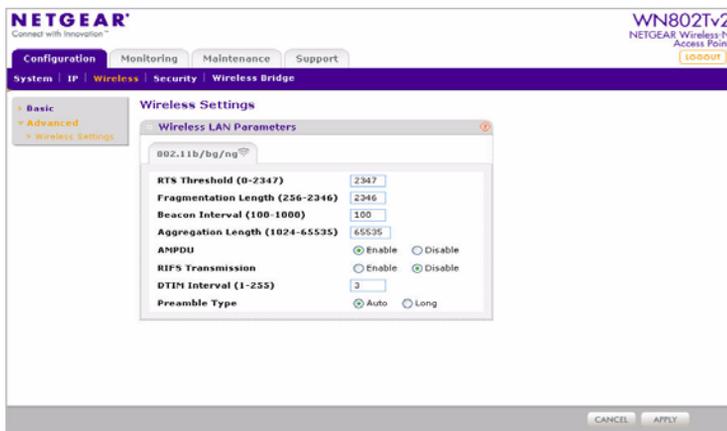
Figure 4-9 Advanced wireless settings

2. Make the required changes or selections to the Wireless LAN Parameters section, based on the field descriptions outlined earlier.

3. Click **Apply** for your changes to take effect.

Configuring the RADIUS Server Settings

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

The RADIUS Server Settings fields are described in Table 4-3.

To configure the RADIUS Server Settings:

1. Select **Security** under the main **Configuration** tab, then select **Advanced** from the side menu. The Radius Server Settings screen displays, as in Figure 4-10.

Figure 4-10 RADIUS server settings

2. Enter the following RADIUS Server settings:

   - **Authentication Server.** This configuration is required for authentication using a RADIUS Server.The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use, if the Primary RADIUS Server fails.

     – **IP Address.** The IP address of the RADIUS Server.

- **Port Number.** The port number of the RADIUS Server. The default is 1812.

- **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).

- **Accounting Server**. This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.

  - **IP Address.** The IP address of the RADIUS Server.

  - **Port Number.** Port number of the RADIUS Server. The default: 1813.

  - **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).

3. Authentication Settings:

   - **Re-authentication Time** (**Seconds**). The time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server.
     The default interval is 3600 seconds.

   - **Update Global Key Every** (**Seconds**). Enable this option to have the Global Key changed according to the time interval specified. If enabled, enter the desired time interval.
     The default is enable, and the default interval is 3600 Seconds

4. Click **Apply** for your changes to take effect.

RADIUS Server Settings Fields

Table 4-3.   RADIUS server settings fields

		Description
Primary and Secondary Authentication Servers		The Authentication RADIUS server provides authentication and access control. The primary server is mandatory. A secondary server, which will be used if the primary server fails, is optional.
	IP Address	The IP address of the authentication server. If no server is present leave blank.
	Port Number	The port number used for communication to the authentication server. The default port number for an authentication server is 1812.
	Shared Secret	The shared secret to establish a client connection to the RADIUS server, as entered on the server itself.
Re-authentication Time		The time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server. The default interval is 3600 seconds.
Update Global Key		Enable this option to have the Global Key changed according to the time interval specified. If enabled, enter the desired time interval. The default is enable, and the default interval is 1800 seconds
Primary and Secondary Accounting Servers		The Accounting RADIUS Server provides accounting services. The same RADIUS server may be used for both authentication and accounting, but the port numbers for authentication and accounting must be different. The accounting servers are optional.
	IP Address	The IP address of the accounting server. If no server is present leave blank.
	Port Number	The port number used for communication to the accounting server. The default port number for an accounting server is 1813.
	Shared Secret	The shared secret to establish a client connection to the RADIUS server, as entered on the server itself.

Chapter 5
Advanced Wireless Bridging

This chapter describes how to configure the advanced features of your WN802Tv2 to one of six access point bridge mode profiles, or in Wireless Bridge and Repeater Mode.These features can be found under the **Wireless Bridge** option on the **Configuration** menu.

> **Note:** Only *one* of a number of WN802Tv2 APs in point-to-point bridge mode connected to one another can have six profiles.

The NETGEAR Wireless-N Access Point WN802Tv2 lets you build large wireless networks. Examples of wireless bridging configurations are:

- **Access Point**. Standard Access Point mode (default mode). Operates as a standard 802.11b, 802.11bg or 802.11ng access point. In this mode, the WN802Tv2 will communicate only with wireless clients.

- **Wireless multi-point bridging**. Acts as the "master" and communicates with up to six bridge-mode wireless access points. All of the other bridge-mode wireless access points communicate through the WN802Tv2 when it is in this mode. The other bridge-mode wireless access points must be set to point to multi-point bridge mode, using the MAC address of this WN802Tv2. They then send all traffic to this "Master", rather than communicate directly with each other. Client wireless stations can also associate.

- **Repeater without Client Association**. Acts as a "repeater" and forwards all traffic to a remote access point. This mode is the same as Multi-Point to Point mode except that client association is not available.

Configuring Wireless Multi-Point Bridging

In this mode, the WN802Tv2 will communicate with up to six bridge-mode wireless access points by entering the MAC (physical) address of each of the bridge-mode APs in the fields provided (see Figure 5-1). Each wireless access point you add is assigned an independent security profile with its own name and configuration. In this mode wireless client association is available by default.

To configure wireless Point to Multi-point Bridging:

1. Open a web browser and log in to the WN802Tv2 using the addressing scheme you have set up.
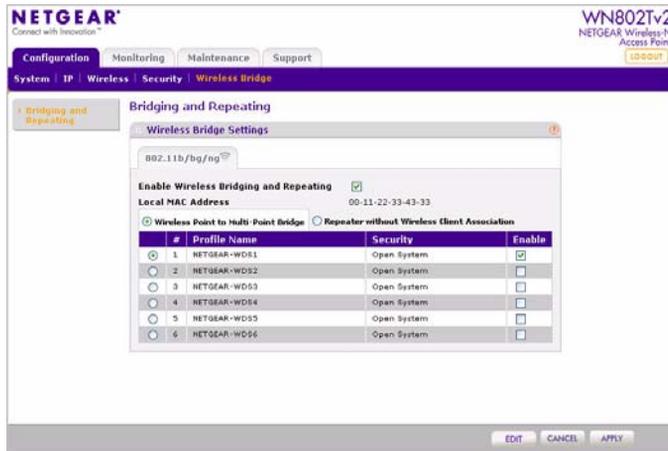
Figure 5-1 Enable wireless bridging and repeating

2. Under the **Configuration** tab on the main menu, click **Wireless Bridge.** The Bridging and Repeating screen displays showing the default settings for the wireless access point (Figure 5-1).

3. Check the **Enable Wireless Bridging and Repeating** checkbox to enable multi-point bridging. Wireless Point to Multi-Point Bridge is the default mode. Down the left of the screen select the profile you want to add/edit and click **Edit**.

4. You are taken to the Edit Security Profile screen (see Figure 5-2). Enter a profile name or leave the default. Enter the MAC (physical) address of the other bridge mode wireless access point in the Remote MAC Address field.
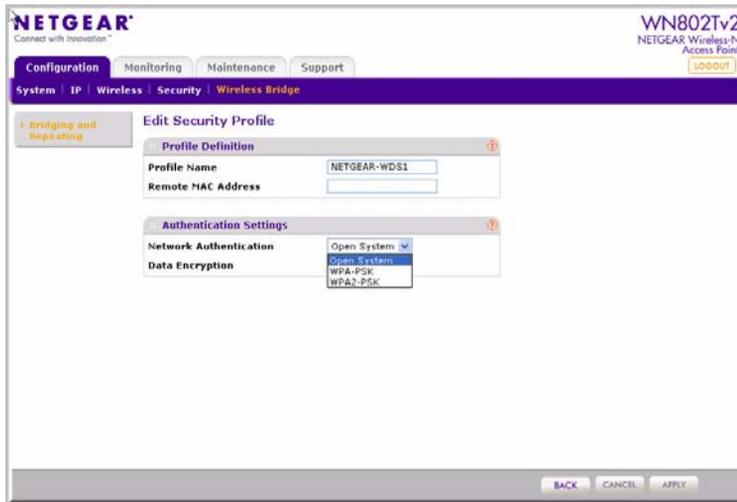
Figure 5-2 Edit security profile

5. Under Authentication Settings, select one of the network authentication types from the **Network Authentication** drop-down menu. One of the supported types (WEP, WPA-PSK, or WPA2-PSK) should be used to protect this communication.

6. Select encryption strength from the **Data Encryption** options available.

7. Click **Apply**.

8. You are taken back to the Wireless Bridge Settings screen (Figure 5-1) with the new profile information. Enable the profile now if you wish to.

   You can add more wireless access points in the same way for a total of six. (These wireless access points must be configured for Multi-Point Bridging.)

9. Click **Apply** to save your changes.

The following figure illustrates a multi-point bridge setup over three LAN segments.
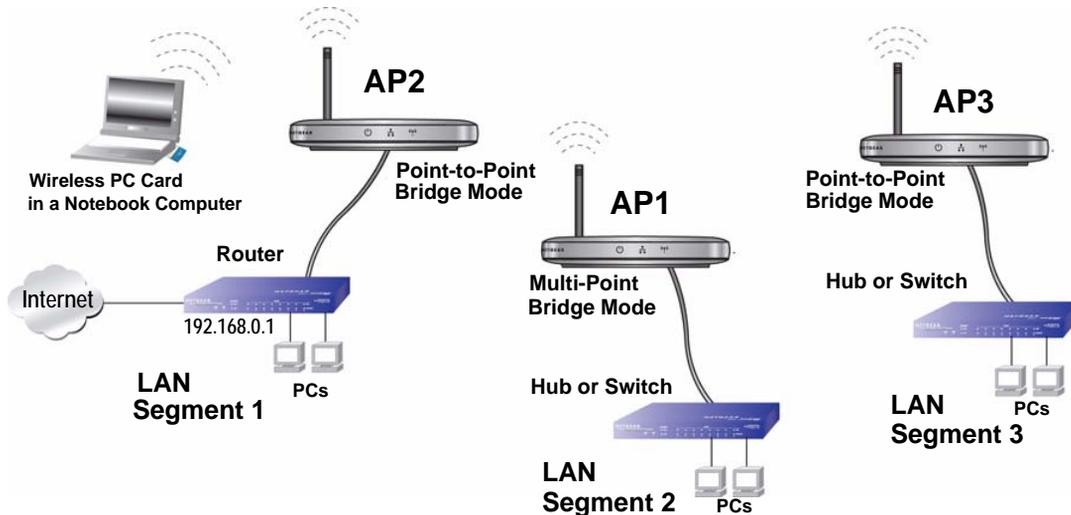
Figure 5-3 Multi-point bridge configuration

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

1. Set the Operating Mode of the three NETGEAR Wireless-N Access Points as follows (see Figure 5-1):

   • Configure AP2 on LAN Segment 1 in Point to Multi-Point Bridge Mode. Add the Remote MAC Address of AP1 on LAN Segment 2. (see Figure 5-2)

   • Because it is in the central location, configure AP1 on LAN Segment 2 in Multi-Point Bridging mode. Add the MAC addresses of the adjacent Point-to-Point APs (AP2 and AP3).

   • Configure AP3 on LAN 3 in Point to Multi-Point Bridge mode. Add the Remote MAC Address of AP1 on LAN Segment 2.

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

   • That the LAN network configuration of each of the NETGEAR Wireless-N Access Points is configured to operate in the same LAN network address range as the other LAN devices (routers, hubs and switches).

   • That only one profile of AP1 is configured in Multi-Point Bridging mode.

   • That all APs are on the same LAN. That is, all the wireless access point LAN IP addresses are in the same network.

- That all wireless access points are using the same SSID, Channel, WEP authentication mode, if any, and encryption (WPA is not available in bridge mode).

- That each Point-to-Point AP has the Multi-Point AP MAC address in its Remote AP MAC address table.

- That the Multi Point-to-Point AP has the MAC addresses of each Point-to-Point AP.

- If Access Control has been enabled on the APs, verify that the Available Wireless Stations list (MAC Address List, Figure 3-10) for each AP is complete and accurate.

3. Verify connectivity across the LANs:

- That wireless clients are able to use the AP.

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

- If Access Control Lists are enabled on the APs, only computers in the access control list will be able to use the AP.

> **Note:** You can extend multi-point bridging by adding a total of six WN802Tv2 APs configured in bridge mode to connect additional wireless LAN segments.

Configuring Repeater without Wireless Client Association

In this mode, the WN802Tv2 will operate as a Repeater only, and send all traffic to the remote wireless access point. You must enter the MAC (physical) address of the remote wireless access point.

To configure the WN802Tv2 in wireless repeater mode:

1. Open a web browser and log in to the WN802Tv2 using the addressing scheme you have set up.
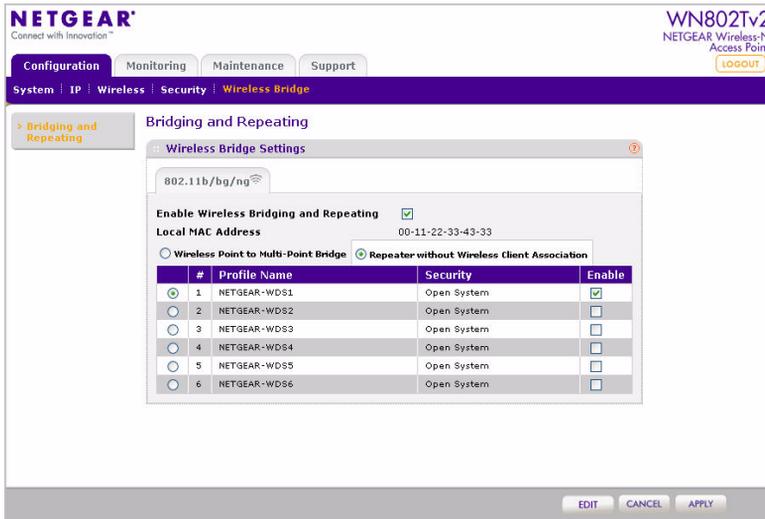
Figure 5-4 Repeater without wireless association

2. Under the **Configuration** tab on the main menu, click **Wireless Bridge.** The Bridging and Repeating screen displays showing the default settings for the wireless access point (see Figure 5-4).

3. Check the **Enable Wireless Bridging and Repeating** checkbox to enable wireless bridging and repeating.

4. Select the **Repeater without Wireless Client Association** radio button to enable this mode. Down the left of the screen select the profile you want to add/edit, and click **Edit**.
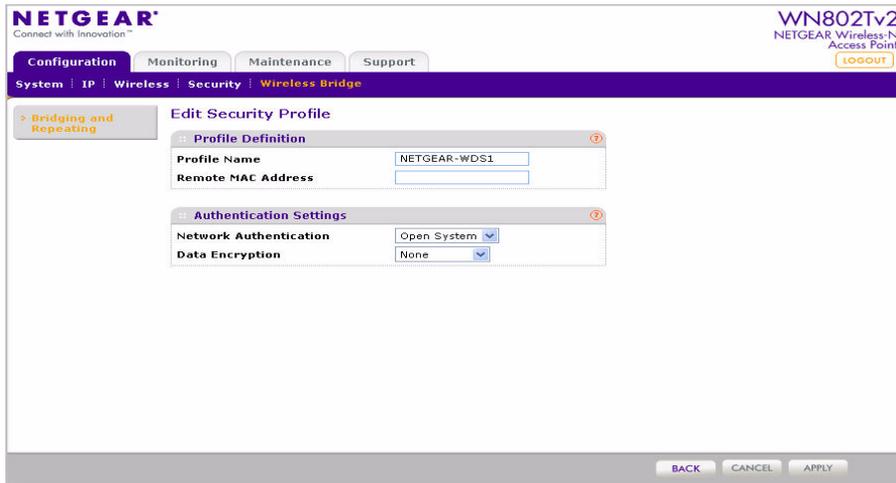
Figure 5-5 Edit security profile

5. You are taken to the Edit Security Profile screen (see Figure 5-5). Enter a profile name or leave the default. Enter the MAC (physical) address of the other bridge mode wireless access point in the Remote MAC Address field.

6. Under Authentication Settings select a **Network Authentication** type. One of the supported types (WEP, WPA-PSK, or WPA2-PSK) should be used to protect this communication.

7. From the **Data Encryption** drop-down menu select encryption strength.

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

9. You are taken back to the Wireless Bridge Settings screen (Figure 5-4) with the new profile information. Enable the profile now if you wish to.

10. Click **Apply** to save your changes.

To configure a LAN segment utilizing the WN802Tv2 in Repeater Mode:

1. Configure the Operating Mode of the NETGEAR Wireless-N Access Points.

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

- Configure AP2 in Repeater mode with the MAC address of the "upstream" AP (AP1).

2. Verify the following parameters for all access points:

- They are configured to operate in the same LAN network address range as the LAN devices.

- They are on the same LAN. That is, all AP LAN IP addresses must be in the same network.

- They use the same SSID, channel, authentication mode (if any) and encryption (WPA is not available in bridge mode).

3. Verify connectivity across the LANs.

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

Chapter 6
Troubleshooting

This chapter provides information for troubleshooting issues with your NETGEAR Wireless-N Access Point WN802Tv2. Along with each problem description, instructions are provided to assist you in diagnosing and solving the problem.

Following are some simple problems that could occur, their possible causes, and tips to solve them:

No lights are lit on the access point.

The access point has no power.

- Make sure the power cord is connected to the access point and plugged in to a working power outlet or power strip.

- Make sure you are using the correct NETGEAR power adapter supplied with your access point; in this case the Switching Power Supply.

The Ethernet light is not lit.

There is a hardware connection problem.

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

- Make sure the connected device is turned on.

The WLAN light is not lit.

The wireless access point built-in antennas are not functioning properly.

- Select the "**Turn Radio On**" radio button setting on the Wireless Settings screen under **Wireless > Advanced**. It must be turned on (selected). See Figure 6-1

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

- Contact NETGEAR if the WLAN light remains off.
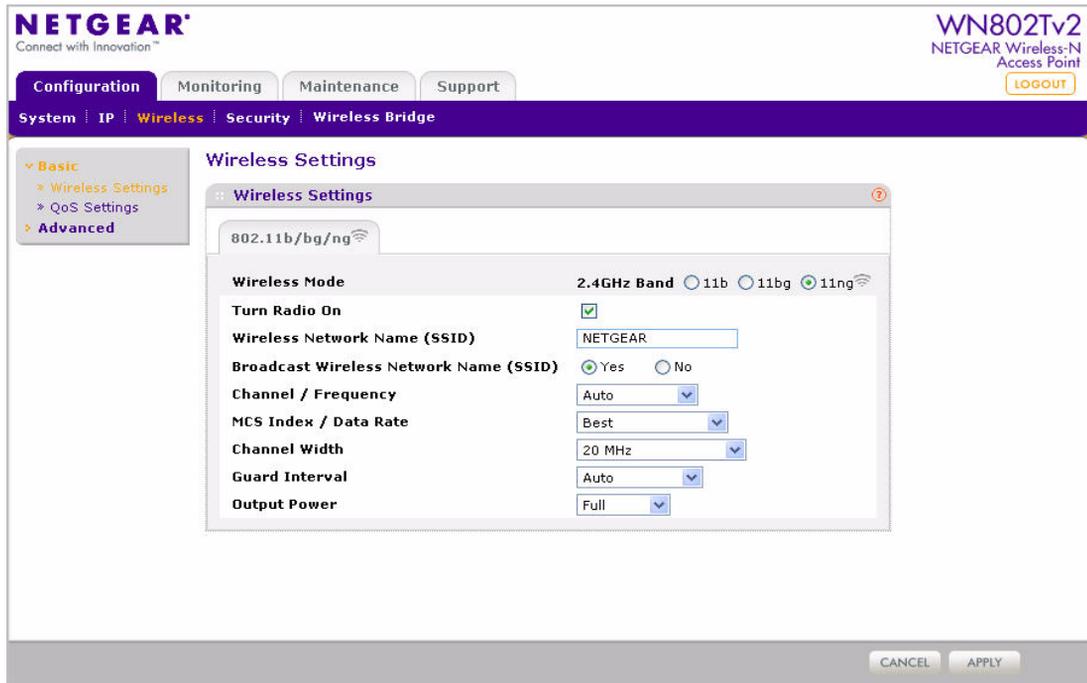
Figure 6-1 Turn Radio On button must be selected

I cannot configure the access point from a browser.

Check these items:

- The WN802Tv2 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is blinking green to verify that the Ethernet connection is OK.

- If DHCP is not enabled, make sure you are using the correct LAN IP address to access the wireless access point, and that you are on the same network segment.

- If DHCP is enabled, configure your DHCP server with a reserved IP address (based on the wireless access point's MAC address). You can then use it to create a fixed IP address for the wireless access point.

- If you have not yet deployed the wireless access point, and it is connected to your PC via an Ethernet cable, make sure the connection is secure, and that you have configured your PC with a static IP address in the same subnet as the LAN IP of the wireless access point. The default static IP address to use for your PC is 192.168.0.210; the default wireless access point LAN IP address is 192.168.0.233; and the default subnet mask is 255.255.255.0.

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

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.

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

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

- For full instructions on changing the wireless access point's default values, see Chapter 2, "Installation and Configuration" and Chapter 3, "Wireless Security Settings".

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

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

- Check whether other computers work. If they do, ensure that your computer's IP Address, Subnet Mask and Default Gateway settings are correct. If using a DNS Server, check the Primary and Secondary DNS Server Addresses.

- If the computers are configured correctly, but still not working, ensure that the WN802Tv2 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.

- If the WN802Tv2 is configured correctly, check your Internet connection (DSL/Cable modem, etc.) to make sure that it is working.

- Try again.

- When entering configuration settings, be sure to click **Apply** before moving to another menu or tab, or your changes are lost.

- Click **Refresh** or **Reload** in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Restore Factory Default Settings

The Reset button on the rear panel of the WN802Tv2 has two functions:

- **Reboot:** When pressed and released quickly, the WN802Tv2 will reboot (restart).

- **Reset to Factory Defaults:** This button can also be used to clear ALL data and restore ALL settings to the factory default values. These settings are shown in Appendix A, "Default Settings and Technical Specifications".

To clear all data and restore the factory default values:

1. Power off the WN802Tv2 and power it back on.

2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least five seconds—or until the power light changes from blinking green to amber.

3. Release the Reset button.

The factory default configuration has now been restored, and the WN802Tv2 is ready for use.

More Help

For more help, click **Support** on the main menu when the access point is connected to the internet (see Figure 6-2):

- Click the **Documentation** link under the **Support** menu to view the documentation for the WN802Tv2 wireless access point online.

- Click the **Knowledge Base** link to access NETGEAR's knowledge base articles online.
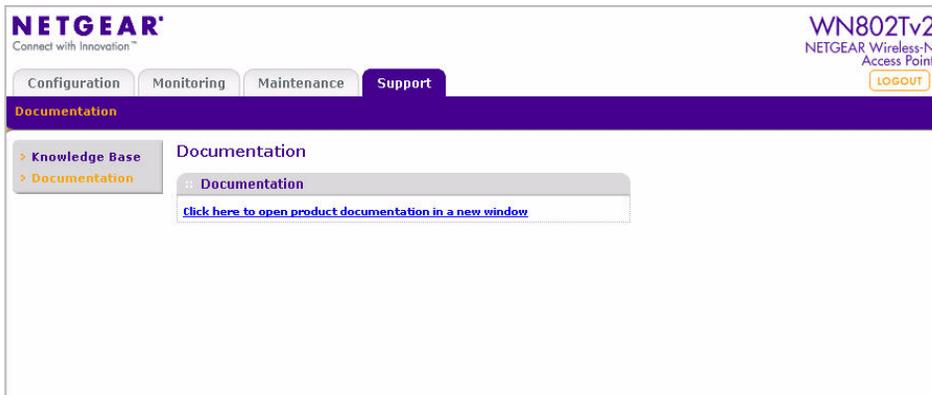
Figure 6-2 Netgear support links

Appendix A
Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the NETGEAR Wireless-N Access Point WN802Tv2.

Factory Default Settings

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

* To perform a hard reset, push and hold the Reset button for approximately 5 seconds (until the Power LED changes from blinking green to solid amber). Your device will return to the factory configuration settings shown in Table A-1.

* Pressing the Reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. Access Point Default Configuration Settings

Feature		Description
AP Login		
	User Login URL	192.168.0.233
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Connection		
	Ethernet MAC Address	See rear label.
	Access Point Mode	On
	Port Speed	10/100/1000 Mbps
Local Network (LAN)		
	Lan IP	192.168.0.233
	Subnet Mask	255.255.255.0
	Gateway Address	192.168.0.1

Table A-1. Access Point Default Configuration Settings

Feature		Description
	DHCP Client	Disabled
	Time Zone	USA-Pacific
	Time Zone Adjusted for Daylight Saving Time	Disabled
Wireless		
	Operating Mode	11b/bg/ng (20/40 MHz)
	Wireless Communication	Enabled
	Wireless Network Name (SSID)	NETGEAR
	Broadcast Network Name SSID	Enabled
	Security	Disabled
	Transmission Speed	Auto
	Country/Region	United States (in North America; otherwise, varies by region)
	Channel/Radio Frequency	Auto
	Output Power	Full
	Wireless Card Access List	All wireless stations allowed
	Encryption	64-bit, 128-bit, 152-bit, default none

Technical Specifications

Parameter	NETGEAR Wireless-N Access Point WN802T v2
802.11n Data Rates (Mbps)	20MHz: 400ms (short): best, 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.6, 115.6, 130, & 144.4 800ms(long): best, 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 13, 26, 39, 52, 78, 104, 117, & 130 40MHz: 400ms (short): best, 15, 30, 45, 60, 90, 120, 135, 150, 30, 60, 90, 120, 180, 240, 270, & 300 800ms (long): best, 13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 27, 54, 81, 108, 162, 216, 243, & 270
802.11bg Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 & 54 Mbps (Auto-rate capable)
802.11b/bg/ngb Operating Frequencies	2.412 ~ 2.462 GHz (US), 2.457 ~ 2.462 GHz (Spain) 2.412 ~ 2.484 GHz (Japan), 2.457 ~ 2.472 GHz (France) 2.412 ~ 2.472 GHz (Europe ETSI)
802.11b/bg/ng Encryption	40-bit (also called 64-bit), 128-bit WEP data encryption; TKIP (WPA-PSK and WPA) and AES (WPA2-PSK and WPA2)
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 15 to 20 nodes.
Status LEDs	Power/Ethernet LAN/Wireless LAN
Flash Memory	8 MB
Power Adapter	12V DC, 1.0 A
Environmental Specifications	Operating temperature: 0 to 45° C Operating humidity: 5-95%, non-condensing

Appendix B
Related Documents

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

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

Index

front panel 1-2

G
guard interval 2-10

H
high-throughput mode
  static 2-10
hotspot
  wireless client security separation 3-5 to 3-16

I
interference
  electromagnetic 1-1
  guard interval 2-10
  sources 2-2
  what to do if 2-9
IP address
  access point, default 2-6, 6-3
  default 2-12, 2-15, 3-16
  default for PC 6-3
  default subnet mask 6-3
  DHCP server, reserve on 2-15
  fixed 6-2
  gateway 2-7
  primary DNS server 2-7
  reserved 6-2
  secondary DNS server 2-7
  static 6-3
  static, host 2-3
  system information 4-9

K
key
  default 3-4
  default, select 3-8
keys
  generate 3-4

L
LAN setting 2-3

latency 2-1
LED
  status 1-5
legacy mode
  channel width, static 2-10
line of sight 2-12
location
  access point 2-1
  placement 2-12
log in 2-15
login URL, default 2-3

M
MAC address
  filtering 3-1
  location 3-18
  restrict access by 3-16
  system information 4-8
  trusted wireless station 3-18
MAC address database
  local 3-17
  remote 3-17
MCS index 2-9
MIMO 1-2
modes
  operating 1-2
multiple access points
  channel spacing 2-2
multi-point bridging
  configure 5-1
  example of 5-4
  extending 5-5
  See also bridging

N
network authentication
  types 3-3
network key 3-3, 3-14
  length 3-4
  see also passphrase 3-15
  WPA2-PSK 3-15
  WPA-PSK/WPA2/PSK 3-16