Reference Manual for the NETGEAR RangeMax™ Wireless Access Point WPN802

NETGEAR

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

202-10101-01
May 2005

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT 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.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

EN 55 022 Declaration of Conformance

This is to certify that the NETGEAR RangeMax™ Wireless Access Point WPN802 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das NETGEAR RangeMax™ Wireless Access Point WPN802 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the NETGEAR RangeMax™ Wireless Access Point WPN802 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second 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.

Customer Support

Refer to the Support Information Card that shipped with your NETGEAR RangeMax™ Wireless Access Point WPN802.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Product and Publication Details

Model Number:	WPN802
Publication Date:	May 2005
Product Family:	Wireless Access Point
Product Name:	NETGEAR RangeMax™ Wireless Access Point WPN802
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10101-01

Contents

Chapter 1
About This Manual

Chapter 2
Introduction

Chapter 3
Basic Installation and Configuration

Chapter 4
Wireless Configuration

Appendix A
Technical Specifications

Appendix B
Wireless Networking Basics

Glossary

Chapter 1
About This Manual

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

Audience, Scope, Conventions, and Formats

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

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
fixed	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

This manual is written for the WPN802 Access Point according to these specifications:

Table 1-2. Manual Scope

Product Version	NETGEAR RangeMax™ Wireless Access Point WPN802
Manual Publication Date	May 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/WPN802.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 TOC button that displays the table of contents and an Index 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 Knowledge Base button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

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

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

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

- **Printing a Chapter**.

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

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

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

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

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

- **Printing the Full Manual**.

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

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

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

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

Chapter 2
Introduction

The NETGEAR RangeMax™ Wireless Access Point WPN802 provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.This chapter describes the features of the NETGEAR RangeMax™ Wireless Access Point WPN802.

➡	**Note:** This manual provides information on the complete features as of the date of publication. Earlier versions of this product may not have all the features presented in this manual. Go to *http://kbserver.netgear.com/products/WPN802.asp* where you will find product firmware updates for your WPN802.

Key Features

The WPN802 Access Point is easy-to-use and provides the following features:

- RangeMax™ Multi-In, Multi-Out (MIMO) technology
- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11b only, or 802.11b+g modes.
- Easy, Web-based setup for installation and management.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrades.

RangeMax™ Multi-In, Multi-Out (MIMO) Technology

Netgear’s RangeMax Multi-In, Multi-Out (MIMO) technology provides ten times more coverage than standard 802.11g alone by eliminating “dead spots” in your area of coverage where you use your wireless computers. Your whole house or office suite now becomes a “hot spot” without requiring any range extenders, repeaters, or external antennas. RangeMax maintains your high speed throughout your home, not just when you are close to your wireless access point.

RangeMax is an advanced Smart MIMO (Multi-In, Multi-Out) technology that uses seven internal antennas. RangeMax constantly surveys your home environment for physical barriers and interference and adjusts the wireless signal to compensate for these performance blockers.

For example, if you carry your laptop from the family room to the bedroom, RangeMax automatically senses the change and selects from over 100 possible antenna configurations to deliver you the fastest, clearest connection so that everyone can enjoy consistently high-speed connections, everywhere in your house with no drop-outs and no dead spots.

RangeMax is also 100% compatible with your existing 802.11b/g products (i.e., 802.11b, 802.11g, Centrino, and SuperG™ wireless clients) and boosts their range and speed by up to 50%.

802.11g Wireless Networking

The WPN802 Access Point includes an 802.11g wireless access point, providing continuous, high-speed 108 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g wireless networking at up to 108 Mbps.
- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11b-only, or 802.11g and b modes, providing backwards compatibility with 802.11b devices or dedicating the wireless network to the higher bandwidth 802.11g devices.
- 64-bit and 128-bit WEP encryption security.
- WEP keys can be generated manually or by passphrase.
- WPA-PSK support. Support for Wi-Fi Protected Access (WPA) data encryption which provides strong data encryption and authentication based on a pre-shared key.
- Wireless access can be restricted by MAC address.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

Autosensing Ethernet Connections with Auto Uplink

The WPN802 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

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

Compatible and Related NETGEAR Products

NETGEAR products related to the NETGEAR RangeMax™ Wireless Access Point WPN802 are as follows:

- RangeMax Wireless USB 2.0 Adapter (WPN111)
- RangeMax Wireless PCI Adapter (WPN311)
- RangeMax Wireless PC Card (WPN511)

Package Contents

The product package should contain the following items:

- NETGEAR RangeMax™ Wireless Access Point WPN802.
- AC power adapter.
- Vertical stand.
- Straight through Category 5 (CAT5) Ethernet cable.
- *Resource CD for the NETGEAR WPN802 RangeMax™ Wireless Access Point (240-10213-01)*, including:
  - — This manual.
  - — Application Notes and other helpful information.
- WPN802 Quick Installation Guide.
- 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 WPN802 for repair.

The Front Panel Status Lights

You can use the status lights on the front panel of the WPN802 to verify connections. The table below describes the lights on the front panel.

Table 2-1. Status Light Descriptions

Label	Activity	Description
⏻ Power	On Green Solid Off	Power is supplied and the WPN802 has passed its diagnostic test. Power is not supplied to the WPN802.
√ Test	On Off	The unit is performing the power on self test diagnostic. The unit successfully completed the power on self test diagnostic.
WLAN	On Off	The Wireless port is initialized and the wireless feature is enabled. The wireless feature is turned off or there is a problem.
Ethernet	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Ethernet port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Ethernet port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected.

The Rear Panel

The rear panel of the WPN802 contains the items listed below.

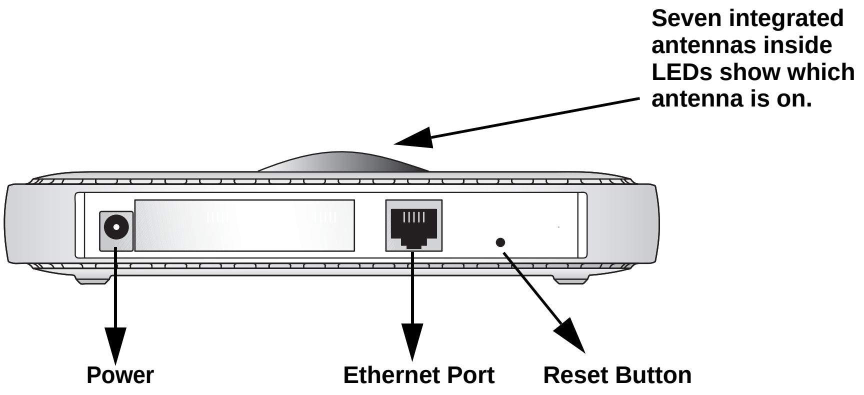

Seven integrated antennas inside LEDs show which antenna is on.
Power
Ethernet Port
Reset Button

Figure 2-1: WPN802 Rear Panel

Viewed from left to right, the rear panel contains the following features:

- AC power adapter outlet.
- Ethernet 10/100 Mbps port for connecting the access point to the network.
- Factory Default Reset push button for Using the Reset Button to Restore Factory Default Settings.

Chapter 3
Basic Installation and Configuration

This chapter explains how to install and configure and the WPN802 Access Point on your network. The first time you configure the WPN802 Access Point it must be connected with an Ethernet cable to a computer with a broadband Internet connection.

Default Factory Settings

The WPN802 default factory settings are shown below. After you install the WPN802 Access Point, customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
User Name (case sensitive)	admin
Password (case sensitive)	password
Operating Mode	Access Point
Access Point Name	netgearxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address
Built-in DHCP client	DHCP client disabled
SIP Configuration (if DHCP server is unavailable)	IP Address: 192.168.0.231 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
Network Name (SSID)	NETGEAR
Broadcast Network Name (SSID)	Enabled
802.11b/g RF Channel	6
Mode	Auto 108
AutoCell Enhanced RF Security 'stealth' mode	Disabled
WEP/WPA	Disabled
Restricting connectivity based on MAC Access Control List	Disabled

System Requirements

Before installing the WPN802, make sure your system meets these requirements.

- A 10/100 Mbps Local Area Network device such as a hub, router, or switch.
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it.
- A 100-240 V, 50-60 HZ AC power source.
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.
- At least one computer with the TCP/IP protocol installed.
- 802.11b or 802.11b-compliant devices, such as the NETGEAR RangeMax Wireless PCI Adapter (WPN311).

Prepare to Install Your Wireless Access Point

- Observe the wireless placement and range guidelines in *"Observe Performance, Placement, and Range Guidelines" on page 4-1*.
- *For Cable Modem Service*: When you perform the wireless access point setup steps be sure to use the computer you first registered with your cable ISP.
- *For DSL Service*: You may need information such as the DSL login name/e-mail address and password in order to complete the wireless access point setup.
- Familiarize yourself with the contents of the *Resource CD for the NETGEAR WPN802 RangeMax™ Wireless Access Point (240-10213-01)*, especially this manual and the animated tutorials for configuring networking on PCs.

First, Connect the Wireless Access Point to Your Computer

Before installing the wireless access point, make sure that your Ethernet network is up and working.

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

2. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the Subnet Mask.
3. Connect an Ethernet cable from the WPN802 to the computer.

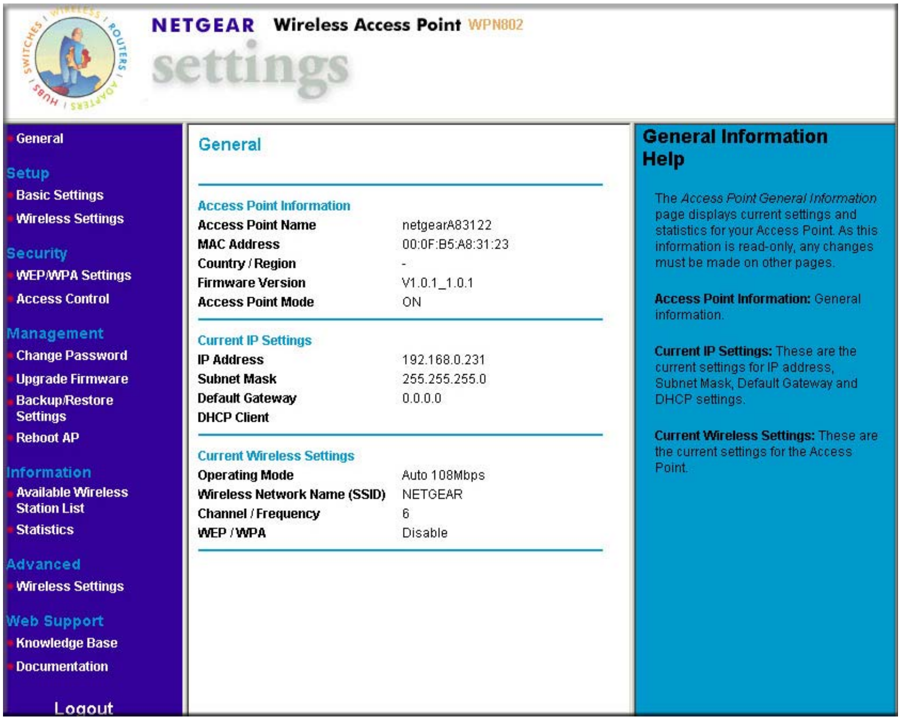
Figure 3-1: WPN802 connected to a computer during configuration

4. Turn on your computer, and connect the power adapter to the WPN802. Then check the lights on the front:
   - *Power*: The power light should be lit. If the power light is not lit, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off.
   - *Test*: The test light blinks when the WPN802 is first turned on.
   - *WLAN:* The wireless light should be lit.
   - *Ethernet*: The Ethernet (LAN) light should be lit (amber for a 10 Mbps connection and green for a 100 Mbps connection). If not, make sure the Ethernet cable is securely attached at both ends.

Then, Configure the Basic Settings

1. Connect to the WPN802 by opening your browser and entering *http://192.168.0.231* in the address field.

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



General

Access Point Information

Access Point Name	netgearA83122
MAC Address	00:0F:B5:A8:31:23
Country / Region	-
Firmware Version	V1.0.1_1.0.1
Access Point Mode	ON

Current IP Settings

IP Address	192.168.0.231
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	

Current Wireless Settings

Operating Mode	Auto 108Mbps
Wireless Network Name (SSID)	NETGEAR
Channel / Frequency	6
WEP / WPA	Disable

General Information Help

The *Access Point General Information* page displays current settings and statistics for your Access Point. As this information is read-only, any changes must be made on other pages.

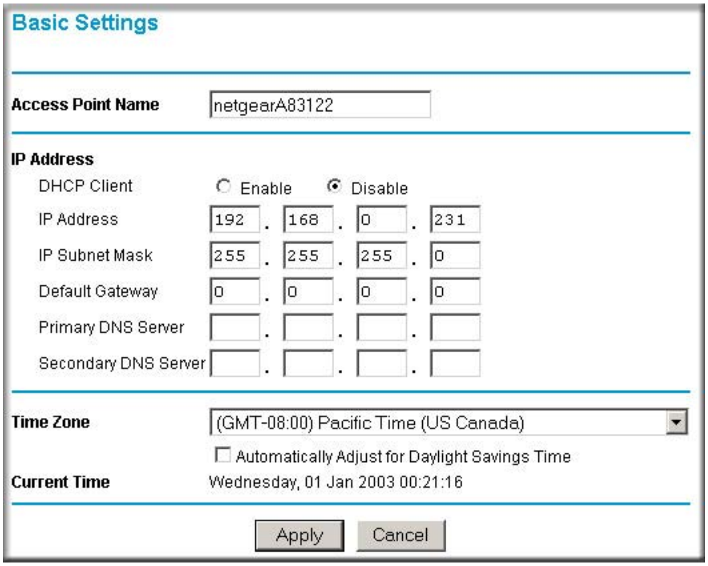
Access Point Information: General information.

Current IP Settings: These are the current settings for IP address, Subnet Mask, Default Gateway and DHCP settings.

Current Wireless Settings: These are the current settings for the Access Point.

Figure 3-2: WPN802 Settings page

3. Click the Basic Settings link to configure the IP Settings for your network. The Basic Settings menu appears:



Basic Settings

Access Point Name: netgearA83122

IP Address

DHCP Client	○ Enable	● Disable		
IP Address	192	168	0	231
IP Subnet Mask	255	255	255	0
Default Gateway	0	0	0	0
Primary DNS Server				
Secondary DNS Server				

Time Zone: (GMT-08:00) Pacific Time (US Canada)

□ Automatically Adjust for Daylight Savings Time

Current Time: Wednesday, 01 Jan 2003 00:21:16

Figure 3-3: Basic Settings menu

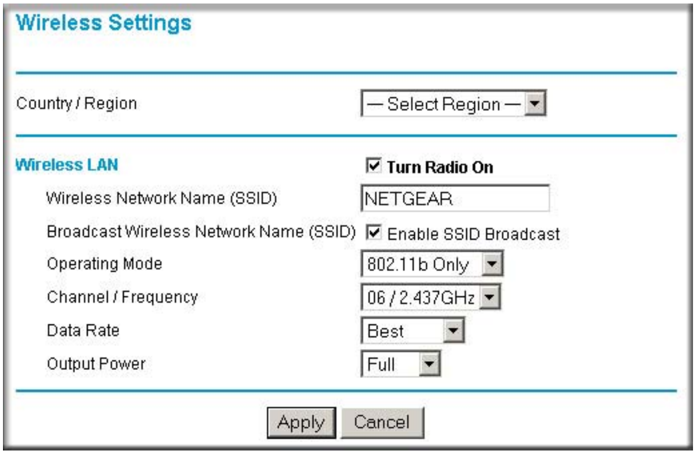
4. Configure the Basic Settings for your network.
   - **Access Point Name:** The unique NetBIOS name. The default Access Point Name is located on the bottom label of the WPN802. You may modify the default name with a unique name up to 15 characters long.
   - **IP Address:** By default, the Access Point is set to be a DHCP (Dynamic Host Configuration Protocol) client disabled. The default IP address is 192.168.0.231.
   - **DHCP Client:** You may enable the DHCP client to let the Access Point get its TCP/IP configuration from the DHCP server on your network.
   - **IP Address:** Type the IP address of your Access Point (factory default: 192.168.0.231).
   - **IP Subnet Mask:** The Access Point automatically calculates the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 as the subnet mask.
   - **Default Gateway Address:** The Access Point will use this IP address default gateway for any traffic beyond the local network.
   - **Primary DNS Server:** The Access Point will use this IP address as the primary Domain Name Server used by stations on your LAN.

- **Secondary DNS Server:** The Access Point will use this IP address as the secondary Domain Name Server used by stations on your LAN.
- **Time Zone:** Select the appropriate local time zone for your Access Point from a list of all available time zones. The default is GMT.

Next, Configure the Wireless Settings

After you configure the Basic Settings for the WPN802, then you need to configure the Wireless Settings.

1. On the Settings page, click Wireless Settings. The Wireless Settings menu appears:



Wireless Settings

Country / Region: — Select Region —

Wireless LAN: ☑ Turn Radio On

Wireless Network Name (SSID): NETGEAR

Broadcast Wireless Network Name (SSID): ☑ Enable SSID Broadcast

Operating Mode: 802.11b Only

Channel / Frequency: 06 / 2.437GHz

Data Rate: Best

Output Power: Full

Figure 3-4: Wireless Settings menu

2. Enter the wireless settings. For more information, see "Understanding Wireless Settings" on page 4-2.
3. Test the wireless connectivity. To do this, use a computer with a wireless adapter that is configured according to the wireless settings you just set in the WPN802. With this computer, establish a wireless connection to the WPN802.

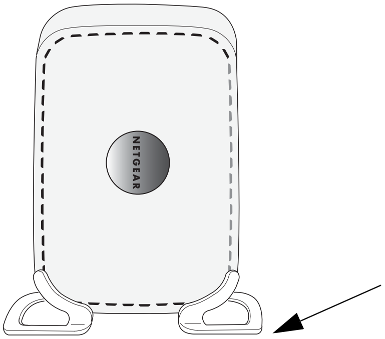
   Now that you have finished the setup steps, you are ready to deploy the WPN802 in your network. If needed, you can now reconfigure the PC you used in step 1 back to its original TCP/IP settings.

Deploy the WPN802 and Verify Wireless Connectivity

When you have configured the Basic Settings and the Wireless Settings, then you can deploy the WPN802.

1. Disconnect the WPN802 and position it where you will deploy it.

   The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.



Use the plastic clips provided to place the WPN802 vertically if it is on a metal surface.

Figure 3-5: WPN802 placed in a vertical orientation

2. Connect an Ethernet cable from your WPN802 Access Point to a LAN port on your router, switch, or hub.

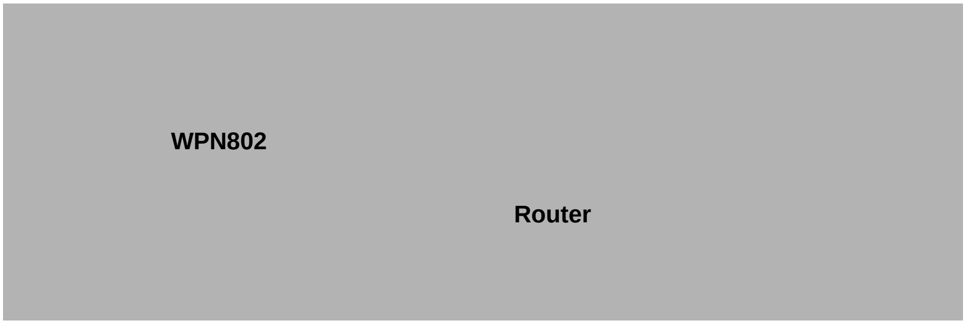


Figure 3-6: WPN802 connected to a router

Note: By default, the WPN802 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you will need to change this setting.

3. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The Power, WLAN and Ethernet lights should light up.
4. Using a computer with an 802.11g or 802.11b wireless adapter with the correct wireless settings, verify connectivity by using a browser such as Netscape® or Internet Explorer to connect to the Internet, or check for file and printer access on your network.

   Note: If you are unable to connect, see Chapter 3.
5. Configure the wireless settings for each computer that will use the wireless access point.
6. Implement wireless security according to the instructions in "Understanding Wireless Settings" on page 4-2.

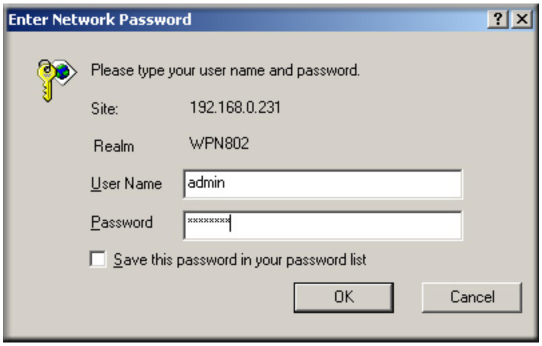
How to Log In to the WPN802 Using Its Default IP Address

The WPN802 has DHCP client disabled, and the default IP address is 192.168.0.231.

Note: The computer that you use to connect to the WPN802 should be configured with an IP address that starts with 102.168.0.x and a Subnet Mask of 255.255.255.0.

1. Connect to the WPN802 by typing *http://192.168.0.231* in the address field of your browser, and clicking **Enter**.

   For security reasons, the access point has its own user name and password. A login window like the one below opens:



Enter Network Password

Please type your user name and password.

Site: 192.168.0.231

Realm WPN802

User Name: admin

Password: ********

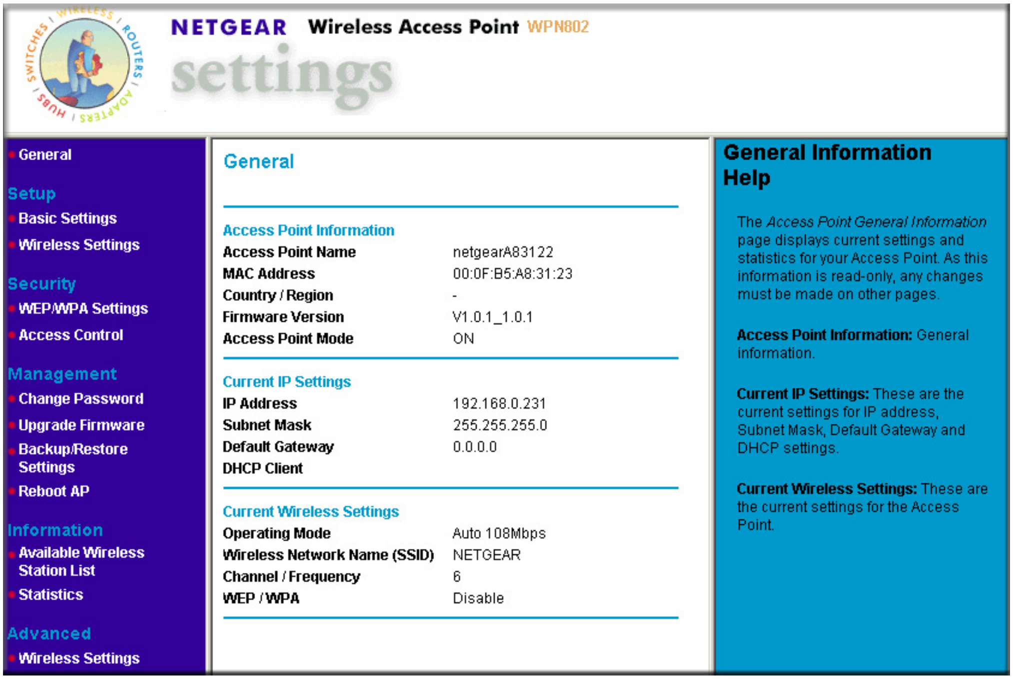
□ Save this password in your password list

Figure 3-7: Login window

2. Enter **admin** for the user name and **password** for the password, both in lower case letters. To change the password, see "This page displays both wired and wireless interface network traffic. Click Refresh to update the current statistics." on page 5-6.

Note: The user name and password for the access point are not the same as any user name or password you may use to log in to your Internet connection.

The browser display the WPN802 settings home page.



General

Access Point Information

Access Point Name	netgearA83122
MAC Address	00:0F:B5:A8:31:23
Country / Region	-
Firmware Version	V1.0.1_1.0.1
Access Point Mode	ON

Current IP Settings

IP Address	192.168.0.231
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	

Current Wireless Settings

Operating Mode	Auto 108Mbps
Wireless Network Name (SSID)	NETGEAR
Channel / Frequency	6
WEP / WPA	Disable

General Information Help

The *Access Point General Information* page displays current settings and statistics for your Access Point. As this information is read-only, any changes must be made on other pages.

Access Point Information: General information.

Current IP Settings: These are the current settings for IP address, Subnet Mask, Default Gateway and DHCP settings.

Current Wireless Settings: These are the current settings for the Access Point.

Figure 3-8: WPN802 home page

When the wireless access point is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless access point.

If you do not click Logout, the wireless access point waits five minutes after there is no activity before it automatically logs you out.

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your WPN802 Access Point. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your wireless access point in order to maximize the network speed. For further information on wireless networking, refer to Appendix B, "Wireless Networking Basics.

Observe Performance, Placement, and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless 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 wireless access point. For complete range/performance specifications, please see Appendix A, "Technical Specifications."

For best results, place your wireless access point:

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

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP and WPA-PSK \encryption can consume more battery power on a notebook computer.

When used on a metallic surface, MIMO units must be oriented vertically to ensure proper operation:

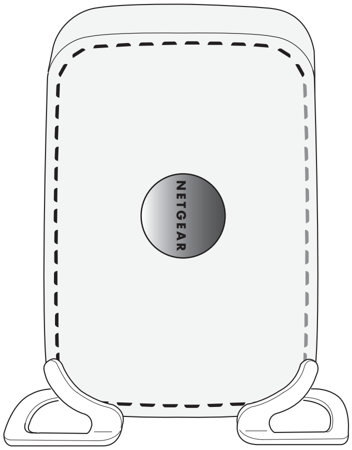
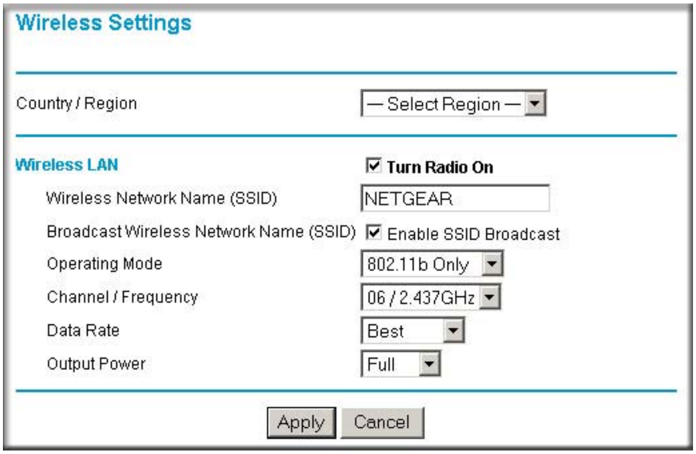


Figure 4-1: Vertical orientation required on metallic surfaces

Understanding Wireless Settings

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



Wireless Settings

Country / Region: — Select Region —

Wireless LAN ☑ Turn Radio On

Wireless Network Name (SSID): NETGEAR

Broadcast Wireless Network Name (SSID): ☑ Enable SSID Broadcast

Operating Mode: 802.11b Only

Channel / Frequency: 06 / 2.437GHz

Data Rate: Best

Output Power: Full

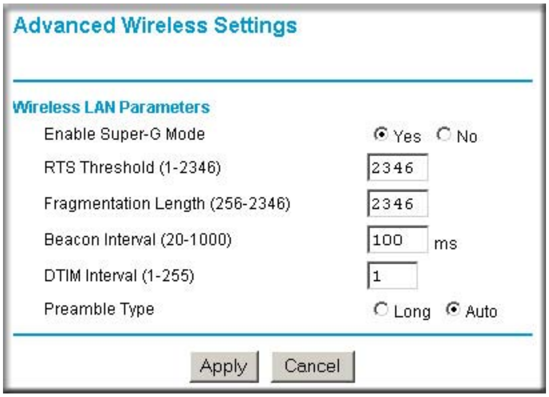
Figure 4-2: Wireless Settings menu

- **Country/Region:** It may not be legal to operate the access point in a country/region other than the country/region shown here. See online help for more details. To change the Country/ Region, select from the drop-down list. The region selection feature may not be available in all countries.
- **Wireless Network Name (SSID):** The default is NETGEAR. Enter a 32-character (maximum). The characters are case sensitive.

  Note: You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.
- **Broadcast Wireless Network Name (SSID):** If enabled, the Wireless Access Point will broadcast its SSID. If set to disable, the SSID is not broadcast.
- **Operating Mode:** Select the desired wireless operating mode. The default is Auto (11g/11b). You can change this to 11g Only, or 11b Only.
- **Channel/Frequency:** Select the channel for your wireless LAN. This feature is disabled if AutoCell is enabled. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page B-7.
  - **Data Rate:** The available transmit data rate of the wireless network. Note that 108 Mbps option is available when the Channel/Frequency is set to channel 6 and the operating mode is set to 11g Only.
  - **Output Power:** Shows the available transmit power of the access point. The possible Tx power options are: Full, 50%, 25%, 12.5%, and minimum. The transmit power may varies depends on the local regulatory regulations. Note that this feature will be disabled if AutoCell is enabled.

Understanding Advanced Wireless Settings

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



Advanced Wireless Settings

Wireless LAN Parameters

Enable Super-G Mode ● Yes ○ No

RTS Threshold (1-2346) 2346

Fragmentation Length (256-2346) 2346

Beacon Interval (20-1000) 100 ms

DTIM Interval (1-255) 1

Preamble Type ○ Long ● Auto

Figure 4-3: Advanced Wireless Settings menu

- **Enable SuperG Mode:** SuperG Mode may increase the overall wireless performance. The default setting is Yes.
- **RTS Threshold:** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2346.
- **Fragmentation Length:** The maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346
- **Beacon Interval:** The interval time between 20ms and 1000ms for each beacon transmission. The default is 100.
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type:** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto will automatically handle both long and short preamble. The default is Auto.

Implementing Appropriate Wireless Security

Note: Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network.

Unlike wired network data, 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 WPN802 Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

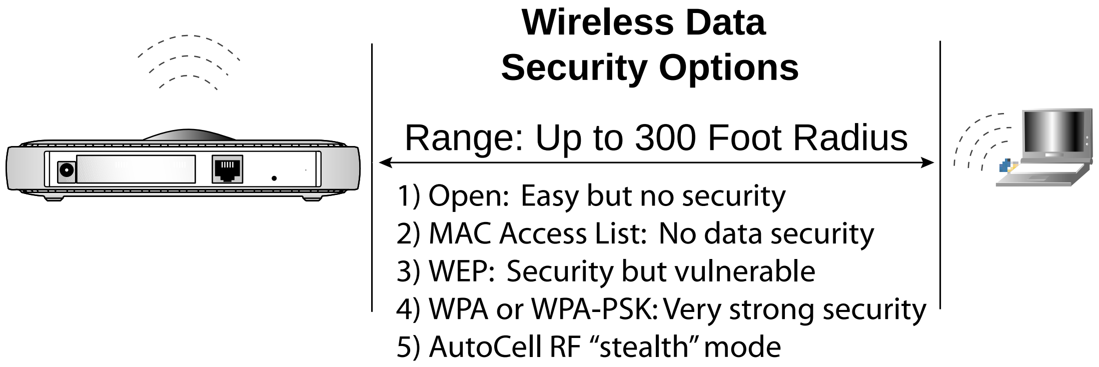

Wireless Data
Security Options
Range: Up to 300 Foot Radius
1) Open: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but vulnerable
4) WPA or WPA-PSK: Very strong security
5) AutoCell RF "stealth" mode

Figure 4-4: WPN802 wireless data security options

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

- **Restrict Access Based on MAC address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WPN802. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

- **WPA-PSK.** Wi-Fi Protected Access, Pre-Shared Key (WPA-PSK) data encryption provides strong data security. WPA-PSK will block eavesdropping. Because this is a new standard, wireless device driver and software availability may be limited.
- **AutoCell Enhanced RF Security.** In addition to standard encryption and security mechanisms such as WEP and WPA, the WG302 AutoCell Feature provides self-organizing micro cells for an additional level of privacy for enterprises. In this mode, AutoCell shrinks the size of coverage to the minimum to reach clients but also shrinks the size of the beacons that access points use to announce their presence. This mode makes an enterprise wireless LAN nearly invisible to users outside an office building. AutoCell clients such as the NETGEAR WAG511 are highly recommended for Enhanced RF Security.

Information to Gather Before Changing Basic Wireless Settings

Before customizing your wireless settings, print this form and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you will choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Wireless Network Name (SSID)*:*** ______________________________ The SSID, identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless access point. In some configuration utilities (such as in Windows XP), the term “wireless network name” is used instead of SSID.
- **If WEP Authentication is Used.** Circle one: **Open System**, **Shared Key, or Auto**.

  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 are configured with the correct key.

  – **WEP Encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless access point.

  – **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.

    - **Passphrase method**. ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters and click the Generate Keys button. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

    Key 1: ____________________________________

    Key 2: ____________________________________

    Key 3: ____________________________________

    Key 4: ____________________________________

- **If WPA-PSK Authentication is Used.**

  – **Passphrase**: ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase.

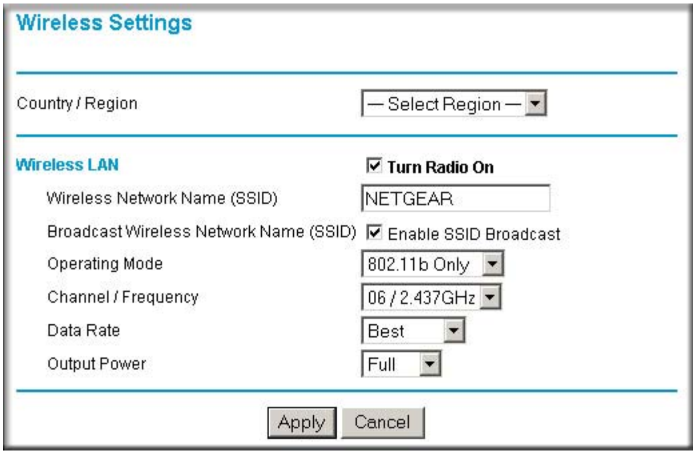
Use the procedures described in the following sections to configure the WPN802. Store this information in a safe place.

How to Set Up and Test Basic Wireless Connectivity

Note: If you use a wireless computer to configure WPA 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.

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

1. Log in to the WPN802 at its default LAN address of *http://192.168.0.231* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WPN802.



Wireless Settings

Country / Region: — Select Region —

Wireless LAN

☑ Turn Radio On

Wireless Network Name (SSID): NETGEAR

Broadcast Wireless Network Name (SSID): ☑ Enable SSID Broadcast

Operating Mode: 802.11b Only

Channel / Frequency: 06 / 2.437GHz

Data Rate: Best

Output Power: Full

Figure 4-5: Wireless Settings menu

3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

   Note: The SSID is case sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you configure in the NETGEAR RangeMax™ Wireless Access Point WPN802. If they do not match, you will not get a wireless connection to the WPN802.

4. Set the Region. Select the region in which the wireless interface will operate.

5. Set the Channel. The default channel is 11.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page B-7.

6. For initial configuration and test, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."

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

➡	**Note:** If you are configuring the WPN802 from a wireless computer and you change the WPN802's SSID, channel, or security settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your computer to match the WPN802's new settings.

8. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and channel that you configured in the WPN802. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WPN802.

   Warning: The Network Name (SSID) is case sensitive. If NETGEAR is the Network Name (SSID) in your wireless access point, you must enter NETGEAR in your computer's wireless settings. Typing nETgear will not work.

Once your computers have basic wireless connectivity, you can configure the advanced wireless security functions.

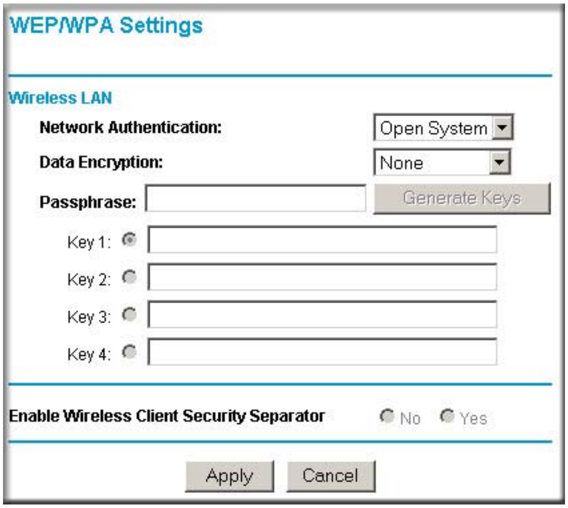
How to Configure WEP or WPA

Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP and Windows 2000 with service pack 3 do include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs for WPA-PSK security, consult the documentation for the product you are using.

To configure WEP or WPA data encryption, follow these steps:

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

1. Log in to the WPN802 at its default LAN address of *http://192.168.0.231* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WPN802.
3. From the Security Options menu, select **WEP/WPA**. The WEP/WPA Settings page opens.



WEP/WPA Settings

Wireless LAN

Network Authentication: Open System

Data Encryption: None

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Enable Wireless Client Security Separator ○ No ○ Yes

Figure 4-6: Wireless Settings encryption menu

4. Select the Network Authentication and Data Encryption from the drop-down lists.

   Please refer to "Authentication and WEP Data Encryption" on page B-2 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

5. Either enter a Passphrase and click Generate Keys, or manually enter the keys. The keys must be identical on all computers and access points in your network.

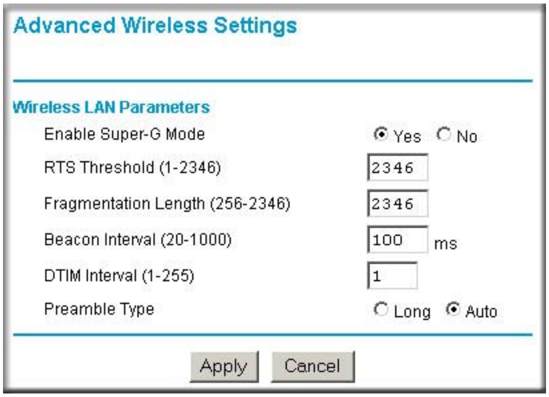
   - Passphrase - The passphrase is case sensitive; NETGEAR is not the same as nETgear. The four key boxes will be automatically populated with key values.
   - Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F). These entries are not case sensitive; AA is the same as aa.

Select which of the four keys will be active.

6. Enable Wireless Client Security Separator: The associated wireless clients will not be able to communicate with each other if this feature is enabled. The default setting is Disable.
7. Click **Apply** to save your settings.

Configuring Advanced Wireless Settings

Click on Wireless Settings under the Advanced Heading in the Main Menu to go to the Advanced Wireless Settings page:



Advanced Wireless Settings

Wireless LAN Parameters

Enable Super-G Mode	● Yes ○ No
RTS Threshold (1-2346)	2346
Fragmentation Length (256-2346)	2346
Beacon Interval (20-1000)	100 ms
DTIM Interval (1-255)	1
Preamble Type	○ Long ● Auto

Figure 4-7: Advanced Wireless Settings page

Warning: The wireless access point is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings may disable the wireless access point unexpectedly.

The advanced wireless settings are explained below:

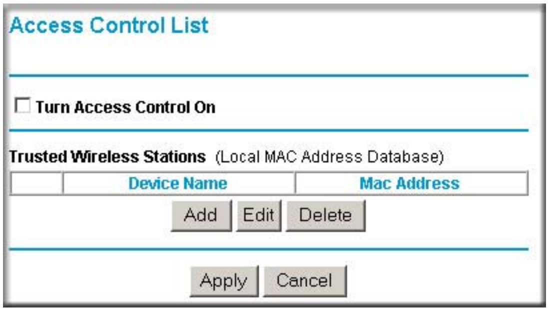
- **Enable SuperG Mode:** Enable SuperG mode may increase the overall wireless performance. Default: Disabled.
- **RTS Threshold:** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. Default: 2346.

- **Fragmentation Length:** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. Default: 2346
- **Beacon Interval:** The interval time between 20ms and 1000ms for each beacon transmission. Default: 100
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. Default: 1
- **Preamble Type:** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto will automatically handle both long and short preamble. Default: Auto.

Wireless Card Access (Restricting by MAC Address)

The Wireless Card Access Setup page displays a list of wireless computers that are allowed to connect to the wireless access point based on their MAC addresses. These wireless computers must also have the correct SSID and WEP settings configured on the Wireless Settings page to access the wireless network.

From the Wireless Settings menu, click the Setup Access List button to display the Wireless Access List screen:



Access Control List

□ Turn Access Control On

Trusted Wireless Stations (Local MAC Address Database)

	Device Name	Mac Address

Figure 4-8: Wireless Access Control List screen

By default, any wireless computer that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific computers based on their MAC addresses.

Turning Access Control On

1. Click the Turn Access Control On check box to restrict wireless computers by their MAC addresses.
2. Click **Apply** to save changes and return to the Wireless Settings page.

Note: If Turn Access Control On is enabled and the Access Control List is blank; then no wireless computers can connect to your wireless network.

Setting up the Access Control List

1. On the Access Control List screen, click the Add button to go to the Access Setup menu.

   This menu displays a list of currently active wireless cards and their Ethernet MAC addresses.
2. If the desired computer is in the list, click the radio button of that computer to capture its MAC address. Or you can manually enter the MAC address of the authorized computer.

   Note: The MAC address can usually be found on the bottom of the wireless device. If no Device Name appears, you can type a descriptive name for the computer that you are adding.
3. Click the Add button.
4. Repeat these steps for each wireless computer.
5. You can use the Edit and Delete buttons as needed.
6. Make sure to click the **Apply** button to save changes and return to the Wireless Settings page.

Chapter 5
Management and Information

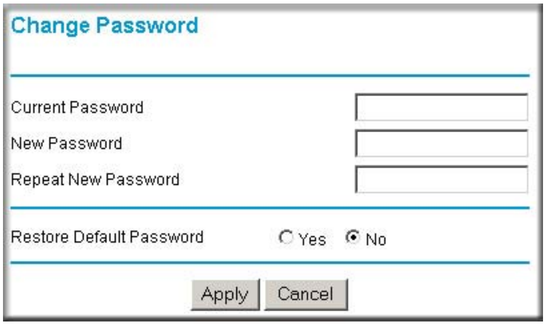
This chapter describes how to use the management and information features of your NETGEAR RangeMax™ Wireless Access Point WPN802. These features can be found under the Management heading and Information heading in the main menu of the browser interface.

Changing the Password

> **Note:** Before changing the WPN802 password, use the backup utility to save your configuration settings. If after changing the password, you forget the new password you assigned, you will have to reset the WPN802 back to the factory defaults to be able to log in using the default password of password. This means you will have to restore all the WPN802 configuration settings. If you ever have to reset the WPN802 back to the factory defaults, you can restore your settings from the backup.

The default password for the WPN802 is **password**. NETGEAR recommends that you change this password to a more secure password.

To change this, click the Change Password link. The Change Password dialog box opens.



Change Password

Current Password

New Password

Repeat New Password

Restore Default Password ○ Yes ● No

Figure 5-1: Change Password dialog box

To change the password, first enter the old password, then enter the new password twice. You can also restore the default password. Click **Apply** to save your changes.

Upgrading the Wireless Access Point Firmware

First, Prepare for the Firmware Upgrade

> **Note:** When uploading firmware to the wireless access point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the WPN802 completely inoperable.

You cannot perform the firmware upgrade from a workstation connected to the WPN802 via a wireless link. The firmware upgrade must be preformed via a workstation connected to the WPN802 the Ethernet LAN interface.

The software of the WPN802 Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.RMG) file before sending it to the wireless access point. The upgrade file can be sent using your browser.

Note: The Web browser used to upload new firmware into the WPN802 Access Point must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

Then, Upgrade the Firmware

1. Go to the NETGEAR Web site *http://www.NETGEAR.com* Customer Service downloads section to get new versions of the Access Point software.
2. Download and unzip (if the download file is a .zip file) the new software file.
3. From the main menu of the browser interface, click the Upgrade Firmware link under the Management heading.

The Upgrade Firmware dialog box opens:

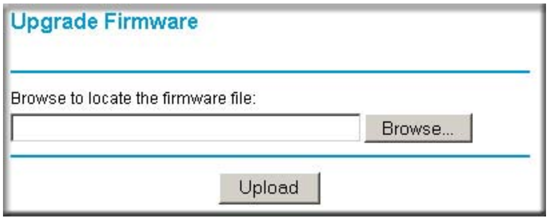


Figure 5-2: Upgrade Firmware dialog box

4. Click the Browse button and browse to the location of the upgrade file
5. Click Upload.

In some cases, you may need to reconfigure the wireless access point after upgrading.

Backing up Settings or Restoring Settings

This page lets you back up the Access Point's current settings and restore the factory default settings. Once you have the Access Point working properly, you should back up the information to have it available if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can restore the Access Point's settings from this file.

From the main menu of the browser interface, click the Backup/Restore Settings link under the Management heading. The Backup/Restore Settings dialog box opens:

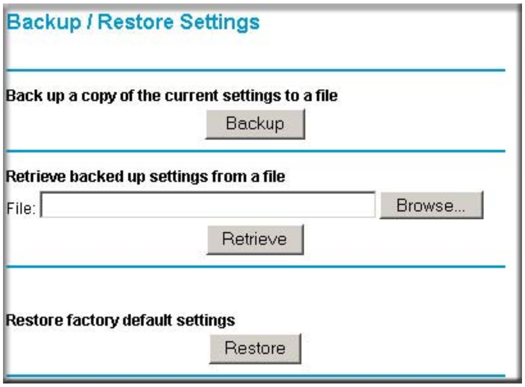

Backup / Restore Settings
Back up a copy of the current settings to a file
Backup
Retrieve backed up settings from a file
File:
Browse...
Retrieve
Restore factory default settings
Restore

Figure 5-3: Backup/Restore Settings dialog box

Backing up Settings

1. On the Backup/Restore Settings dialog box, click Backup.
   - If you don’t have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click Backup.
   - If you have your browser set up to save downloaded files automatically, the file is saved to the your browser’s download location on the hard disk.
2. Retrieve backed up settings from a file

Restoring Settings from a Backup File

You can restore the wireless access point’s settings from a backup file.

1. On the Backup/Restore Settings dialog box, click Browse.
2. Locate and select the previously saved backup file (by default, netgear.cfg).
3. Click Retrieve.

   A window appears letting you know that the Access Point has been successfully restored to previous settings. The Access Point will restart. This will take about one minute.

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

4. Close the message window.

Restoring Factory Default Settings

You can use the Restore feature to erase the current settings and reset the Access Point to the original factory default settings. These settings are listed in “Default Factory Settings” on page 3-1. On the Backup/Restore Settings dialog box, click Restore.

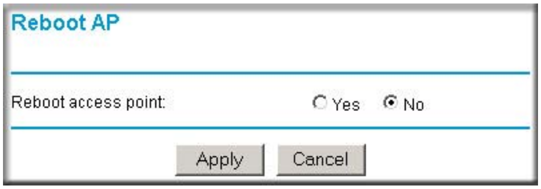
IMPORTANT! Do not try to go online, turn off the Access Point, shut down the computer or do anything else to the Access Point until it finishes restarting. When the Test light turns off, wait a few more seconds before doing anything with the Access Point

Rebooting the WPN802 Access Point

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

1. From the main menu of the browser interface, click the Reboot AP link under the Management heading.

   The Reboot AP dialog box appears:



Reboot AP

Reboot access point: ○ Yes ● No

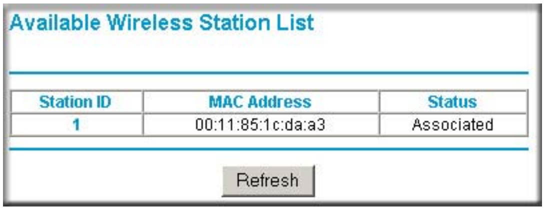
Figure 5-4: Reboot AP dialog box

2. Select Yes, and then click **Apply**.

Viewing a List of Available Wireless Stations

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

From the main menu of the browser interface, click the Available Wireless Stations List link under the Information Heading. The following screen opens:



Available Wireless Station List

Station ID	MAC Address	Status
1	00:11:85:1c:da:a3	Associated

Figure 5-5: Available Wireless Station List

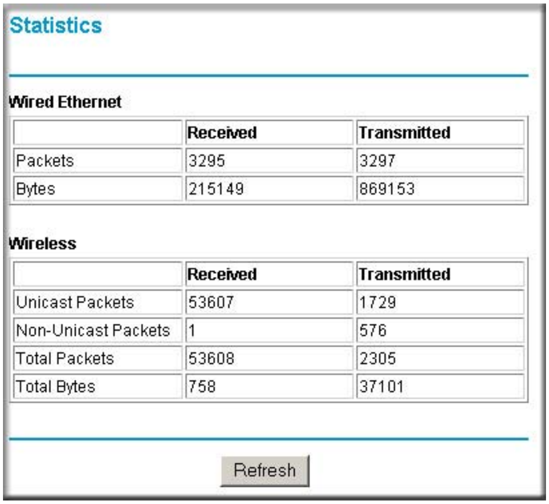
For each device, the table shows the Station ID, MAC address, IP Address, and Status (whether the device is allowed to communicate with the wireless access point or not).

Note that if the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the Refresh button.

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

Viewing Statistics

Click on the Statistics link to display usage statistics, as shown below.



Statistics

Wired Ethernet

	Received	Transmitted
Packets	3295	3297
Bytes	215149	869153

Wireless

	Received	Transmitted
Unicast Packets	53607	1729
Non-Unicast Packets	1	576
Total Packets	53608	2305
Total Bytes	758	37101

Figure 5-6: Statistics screen

This page displays both wired and wireless interface network traffic. Click Refresh to update the current statistics.

Chapter 6
Troubleshooting

This chapter gives information about troubleshooting your NETGEAR RangeMax™ Wireless Access Point WPN802. After each problem description, instructions are provided to help you diagnose and solve the problem.

Troubleshooting Tips

Here are some tips for correcting simple problems you may have.

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.

The Ethernet light is not lit.

There is a hardware connection problem.

- Make sure the cable connectors are securely plugged in at the 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 access point's antennas are not working.

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

I cannot configure the access point from a browser.

Check these items:

- The WPN802 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- If you are using the NetBIOS name of the WPN802 to connect, ensure that your PC and the WPN802 are on the same network segment or that there is a WINS server on your network.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WPN802. The WPN802 default IP Address is 192.168.0.231 and the default Subnet Mask is 255.255.255.0. The WPN802 default setting is for a static IP address. If the network where you are connecting it is using DHCP, configure it accordingly. See the CROSS REF for more details.

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

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows on the Network Properties is set to “Obtain an IP address automatically.”
- The access point’s default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.
- For full instructions on changing the access point’s default values, see CROSS REF.

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 TCP/IP settings are correct. If using a fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the computers are configured correctly, but still not working, ensure that the WPN802 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 WPN802 is configured correctly, check your Internet connection (DSL/Cable modem, etc.) to make sure that it is working.
- Try again.
- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Using the Reset Button to Restore Factory Default Settings

The reset button on the rear panel of the WPN802 has two functions:

- **Reboot:** When pressed and released quickly, the WPN802 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 "Default Factory Settings" on page 3-1.

To clear all data and restore the factory default values:

1. Power off the WPN802 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.
3. Release the reset button.

The factory default configuration has now been restored, and the WPN802 is ready for use.

Appendix A
Technical Specifications

This appendix provides technical specifications for the NETGEAR RangeMax™ Wireless Access Point WPN802.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1A output
Physical Specifications	
Dimensions:	28 x 175 x 119 mm (1.1 x 6.89 x 4.68 in.)
Weight:	0.3 kg (0.66 lb)
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45

WAN:	10BASE-T or 100BASE-Tx, RJ-45
Wireless	
Radio Data Rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.
Operating Frequency Ranges:	2.412~2.462 GHz (US) 2.457~2.462 GHz (Spain) 2.412~2.484 GHz (Japan)2.457~2.472 GHz (France) 2.412~2.472 GHz (Europe ETSI)
802.11 Security:	40-bits (also called 64-bits) and 128-bits WEP and WPA-PSK

Appendix B
Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The WPN802 Access Point conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.11g standards for wireless LANs (WLANs). On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11b wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend 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 domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID **ANY.** This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

Authentication and WEP Data Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined these two types of authentication methods:

- **Open System**. With Open System authentication, a wireless computer can join any network and receive any messages that are not encrypted.

- **Shared Key**. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point, such as the one built in to the WPN802:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.

2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated below.

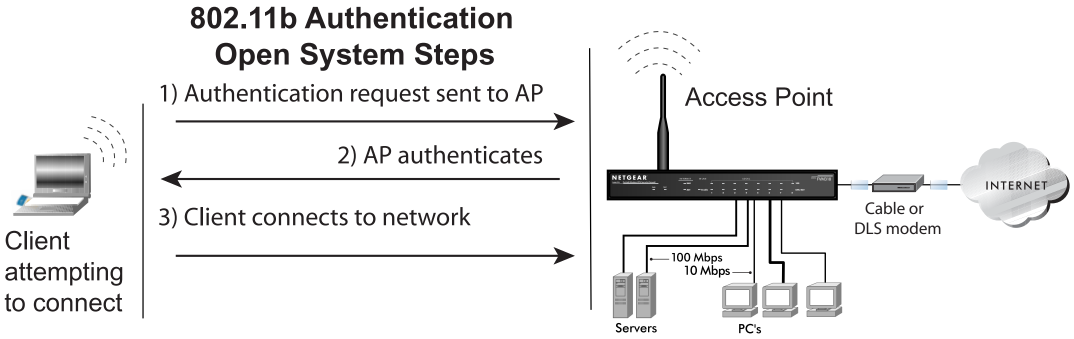


Figure B-1: Open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated below.

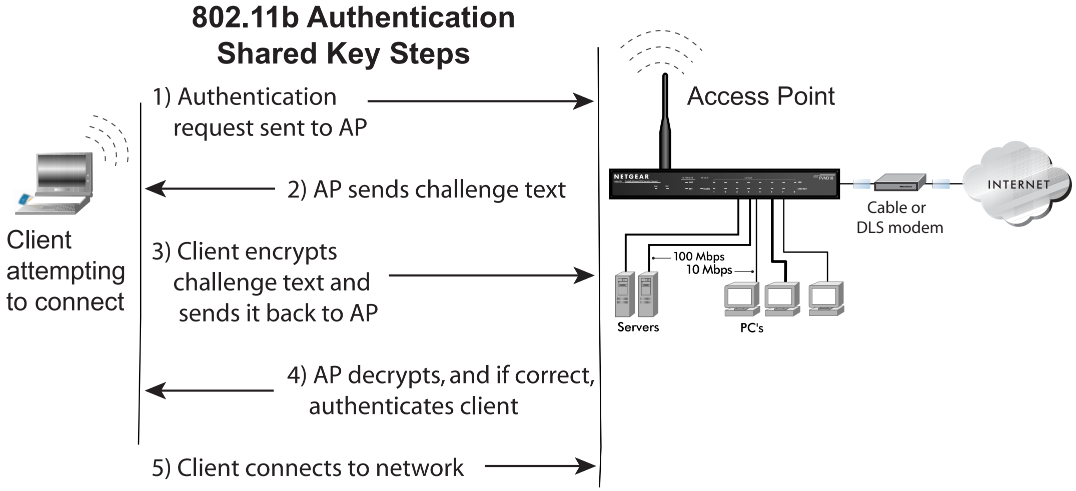

802.11b Authentication
Shared Key Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point
NETGEAR
Cable or DLS modem
INTERNET
100 Mbps
10 Mbps
Servers
PC's

Figure B-2: Shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the wireless network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Table B-1: Encryption Key Sizes

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters’ configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, and so on.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

The wireless frequencies used by 802.11b/g networks are discussed below.

IEEE 802.11b/g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used in 802.11b/g networks are listed in Table B-2:

Table B-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz

Table B-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA and WPA2 Wireless Security

Wi-Fi Protected Access (WPA and WPA2) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture that has been defined by the IEEE.

WPA and WPA2 offer the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products have to support WPA. NETGEAR is implementing WPA and WPA2 on client and access point products. The 802.11i standard was ratified in 2004.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to WPA2 (IEEE 802.11i)?

WPA is forward compatible with the WPA2 security specification. WPA is a subset of WPA2 and used certain pieces of the early 802.11i draft, such as 802.1x and TKIP. The main pieces of WPA2 that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features were either not yet ready for market or required hardware upgrades to implement.

What are the Key Features of WPA and WPA2 Security?

The following security features are included in the WPA and WPA2 standard:

- WPA and WPA2 Authentication
- WPA and WPA2 Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES support (WPA2, requires hardware support)
- Support for a mixture of WPA, WPA2, and WEP wireless clients to allow a migration strategy, but mixing WEP and WPA/WPA2 is discouraged

These features are discussed below.

WPA/WPA2 addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA/WPA2 comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA/WPA2 features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).
- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA/WPA2 Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

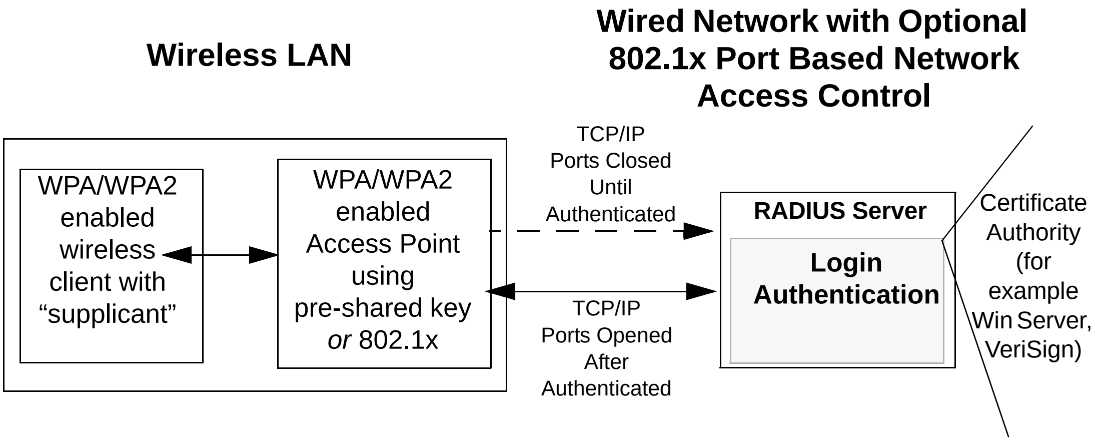

Wireless LAN
Wired Network with Optional 802.1x Port Based Network Access Control
WPA/WPA2 enabled wireless client with "supplicant"
WPA/WPA2 enabled Access Point using pre-shared key *or* 802.1x
TCP/IP Ports Closed Until Authenticated
TCP/IP Ports Opened After Authenticated
RADIUS Server
Login Authentication
Certificate Authority (for example Win Server, VeriSign)

Figure B-3: WPA/WPA2 Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

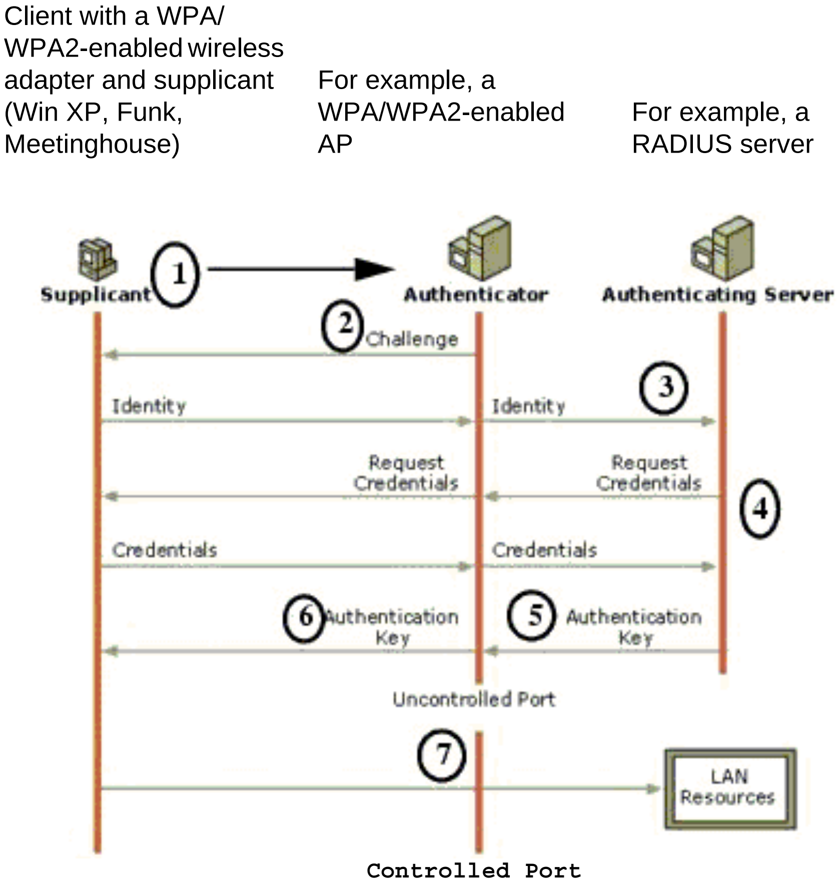


Figure B-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA/WPA2 information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA/WPA2 Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA/WPA2, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

AES Support for WPA2

One of the encryption methods supported by WPA2 is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC’s hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA/WPA2 Perfect?

WPA/WPA2 is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA/WPA2 is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA/WPA2

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA/WPA2 requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA, WPA2, and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA/WPA2, a wireless AP can support both WEP and WPA/WPA2 clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA/WPA2. The disadvantage to supporting a mixture of WEP and WPA/WPA2 clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA/WPA2 and non-WPA/WPA2 clients would offer network security that is no better than that obtained with a non-WPA/WPA2 network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA/WPA2 information element**
  To advertise their support of WPA/WPA2, wireless APs send the beacon frame with a new 802.11 WPA/WPA2 information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA/WPA2 two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

To upgrade your wireless access points to support WPA/WPA2, obtain a WPA/WPA2 firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA/WPA2 information element**
  Wireless clients must be able to process the WPA/WPA2 information element and respond with a specific security configuration.
- **The WPA/WPA2 two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

To upgrade your wireless network adapters to support WPA/WPA2, obtain a WPA/WPA2 update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA driver update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA/WPA2-compatible driver and install the driver.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA/WPA2 authentication (and preshared key) and the new WPA/WPA2 encryption algorithms (TKIP and AES).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Note: The Microsoft WPA2 client is still in beta.

Glossary

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

802.11 Standard

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

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

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

802.11a Standard

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

802.11b Standard

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

802.11d Standard

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

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

802.11e Standard

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

802.11g Standard

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

802.11i

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

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

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

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

802.11n Standard

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

AES (Advanced Encryption Standard)

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

Access Point (AP)

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

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

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

Ad-Hoc mode

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

Bandwidth

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

Bits per second (bps)

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

Bluetooth Wireless Technology

A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet and up to 11Mbps raw data throughput.

Bridge

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

Client or Client devices

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

Collision avoidance

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

Crossover cable

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

CSMA/CA (Carrier Sense Multiple Action/Collision Avoidance)

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

Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission

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

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

DHCP (Dynamic Host Configuration Protocol)

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

Diversity: antenna

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

DNS (Domain Name System)

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

Encryption Key

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

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all WEP known vulnerabilities.

Enterprise-level User Authentication via 802.1x and EAP

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

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

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

Ethernet

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

Firewall

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

Gateway

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

Hot Spot (also referred to as Public Access Location)

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

Hub

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

HZ (‘hertz”)

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

IEEE (Institute of Electrical and Electronics Engineers)

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

IEEE 802.11

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

Infrastructure mode

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

IP (Internet Protocol) address

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

ISO Network Model

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

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

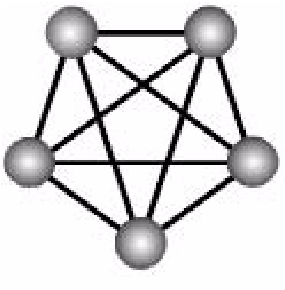
The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

MAC (Media Access Control)

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

Mesh Networks

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



Mesh network

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

Multiple Input Multiple Output (MIMO)

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

NAT (Network Address Translation)

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

Network name

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

NIC (Network Interface Card)

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

PC card (also called PCMCIA)

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

PCI adapter

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

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

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

PHY

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

Plug and Play

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

Proxy server

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

Range

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

Residential gateway

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

RJ-45

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

Roaming

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

Rogue Access Point

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

Router

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

Satellite broadband

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

Server

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

Site survey

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

SSID (also called ESSID)

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

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

SSL (Secure Sockets Layer)

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

Subnetwork or Subnet

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

Switch

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

TCP (Transmission Control Protocol)

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

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

TCP/IP

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

TKIP

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

USB (Universal Serial Bus)

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

VoIP (Voice over IP)

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

VPN (Virtual Private Network)

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

War Chalking

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

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

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

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

War Driving

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

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

WEP (Wired Equivalent Privacy)

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

Wi-Fi (Wireless Fidelity)

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

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

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

Wi-Fi Protected Access (WPA)

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

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

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

Wi-Fi Protected Access and IEEE 802.11i Comparison

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

Wi-Fi Protected Access for the Enterprise

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

Wi-Fi Protected Access for Home/SOHO

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

Wi-Fi Protected Access for Public Access

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

Wi-Fi Protected Access in "Mixed Mode" Deployment

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

WiMAX

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

Wireless Multimedia (WMM)

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

Wireless Networking

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

WLAN (Wireless LAN)

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