Reference Manual for the NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

202-10083-01
March 2005

NETGEAR, INC.

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *www.netgear.com*. If you do not have access to the World Wide Web, you can register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at:
www.netgear.com/support/main.asp through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

Trademarks

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

NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Note: Changes or modifications not expressly approved by NETGEAR, Inc. could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

Note: 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.

RF Exposure Requirements

WARNING! To ensure compliance with FCC RF exposure requirements, the antenna used for this device must be installed to provide a separation distance of at least 20 cm (8 in) from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. Installers and end-users must follow the installation instructions provided in this user guide.

Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 2.4 GHz frequency range. FCC requires this product to be used indoors in 2.4 GHz the frequency range to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

Product and Publication Details

Model Number:	WGPS606
Publication Date:	March 2005
Product Family:	wireless USB print server
Product Name:	NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10083-01

Contents

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 Wireless USB Print Server according to these specifications:

Table 1-2. Manual Scope

Product Version	WGPS606
Manual Publication Date	March 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com*

How to Print this Manual

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

Chapter 2
Introduction

This chapter introduces the NETGEAR NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606. Minimal prerequisites for installation are presented in "System Requirements" on page 2-3.

About the Wireless USB Print Server

This manual describes the installation and use of the WGPS606 for operation with a Microsoft® Windows® XP, Windows® 2000, Windows® Me, or Windows® 98SE system.

For quick installation and setup, please see the WGPS606 54 Mbps Wireless USB Print Server Installation Guide. This manual describes in detail how to set up the WGPS606 and provides you with further reference information.

Any wired or wirelessly connected device in your network can print using printers connected to your wireless USB print server. The WGPS606 provides connectivity to multiple network devices interacting with the built-in switch and with a wireless router or access point. Typically, an in-doors access point provides a maximum connectivity area with about a 300 foot radius. Your wireless USB print server provides direct wired connectivity for up to 4 computers and up to 2 USB printers as well as wireless connectivity for other devices in the network.

The auto-sensing capability of the NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 allows packet transmission at up to 54 Mbps, or at reduced speeds to compensate for distance or electromagnetic noise interference.

Support for Standards

The following standards and conventions are supported:

- **Standards Compliant.** The Wireless USB Print Server complies with the IEEE 802.11g (DSSS).
- **WEP support.** Support for WEP is included. Both 64-bit and 128-bit keys are supported.
- **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.

- **DHCP Support.**
  - — **Client:** The WGPS606 can act as a client and obtain information from your DHCP server.
  - — **Pass Through**: For devices connected to its switch, the WGPS606 will pass through exchanges to your DHCP server.

Key Features

The WGPS606 provides solid functionality, including these features:

- **Easy Configuration.** The NETGEAR Smart Wizard software that assures fast and easy setup for Windows 98SE, Windows Me, Windows 2000, and Windows XP
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely.
- **Autosensing Ethernet Connection with Auto Uplink lnterface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power and wireless activity are easily identified.

802.11g Standards-based Wireless Networking

The NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 provides a bridge between Ethernet wired LANs and 802.11g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and wireless router or access point systems. Additionally, the WGPS606 supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Packet fragmentation and reassembly
- Authentication Algorithms (Open System, WEP Shared Key, WPA-PSK)
- Short or long preamble

Autosensing Ethernet Connections with Auto Uplink

The WGPS606 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation. The wireless USB print server incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

System Requirements

Before installing the WGPS606, make sure your network meets these requirements:

- A 100-240 V, 50-60 HZ AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.78 or above
- At least one Pentium class computer (or equivalent) with the TCP/IP protocol installed and a CD-ROM drive
- An 802.11b or 802.11g-compliant router or access point

What's In the Box?

The product package should contain the following items:

- NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606
- Power adapter and cord (12Vdc, 1A)
- Printed WGPS606 54 Mbps Wireless USB Print Server Installation Guide
- *Resource CD for the NETGEAR 54 Mbps Wireless Access Point*
  - Setup Wizards
  - Reference Manual for the NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 (202-10083-01)—this manual
  - Soft copy of the WGPS606 54 Mbps Wireless USB Print Server Installation Guide
- Support Information card
- Warranty and Registration card

Contact your reseller or customer support in your area if there are any wrong, missing, or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WGPS606 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.netgear.com*.

Bottom Label Description

The NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 front and rear hardware functions are described on the bottom label illustrated below.

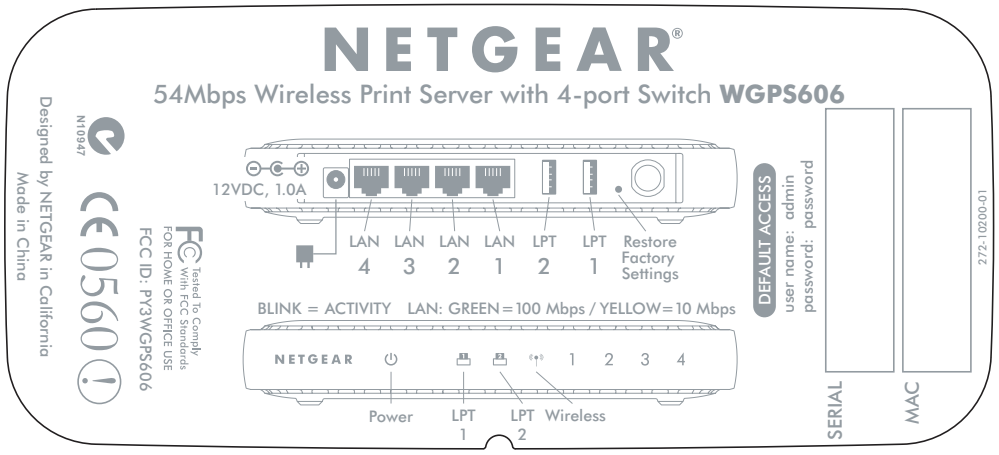


Figure 2-1: WGPS606 bottom label

The following table describes the bottom label information:

ITEM	DESCRIPTION
Power Status Light	Power Indicator
Off	No power.
On Green	Power is on and it has completed its power on self test diagnostic.
Yellow Blink	Power is on and it is performing its power on self test diagnostic.
Yellow Solid	Power is on and it has failed its power on self test diagnostic.
Printer LPT1 & LPT2 Status Lights	Print Activity Indicators
Off	Printer detached or turned off.
Green On	Printer ready.
Green Blink	Print activity.
Yellow 0n	Print error.
Wireless Status Light	Wireless LAN Link Activity Indicator
Blue, Off/On	Off wireless feature turned off/On Blue wireless link enabled, no activity.
Off, Blue Alternating Blink	Seeking wireless connection.
Blue Fast Blink	Wireless link activity.

ITEM	DESCRIPTION
Switch Status Lights	Ethernet LAN Link Activity Indicators
Off/ Green On	Indicates no Ethernet link detected. 100 Mbps Fast Ethernet link detected, no activity.
Green Blink	Indicates data traffic on the 100Mbps Ethernet LAN.
Yellow 0n	10 Mbps Ethernet link detected, no activity.
Yellow Blink	Indicates data traffic on the 10Mbps Ethernet LAN.

Power Socket

This socket connects to the WGPS606 power adapter.

Reset and Restore to Factory Defaults Button

The reset and restore to defaults button located between the Ethernet RJ-45 connector and the power socket resets the WGPS606 when pushed once or restores to the factory default settings when pushed and held for 10 seconds.

RJ-45 Ethernet Port

Use the WGPS606 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, or router.

Antenna

The WGPS606 includes antenna. Be sure the antenna is positioned vertically for best side-to-side coverage and horizontally for best up-and-down coverage.

Chapter 3
Basic Installation and Configuration

This chapter describes how to install your NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 and set up basic connectivity on your Local Area Network (LAN).

Overview of Wireless USB Print Server Setup

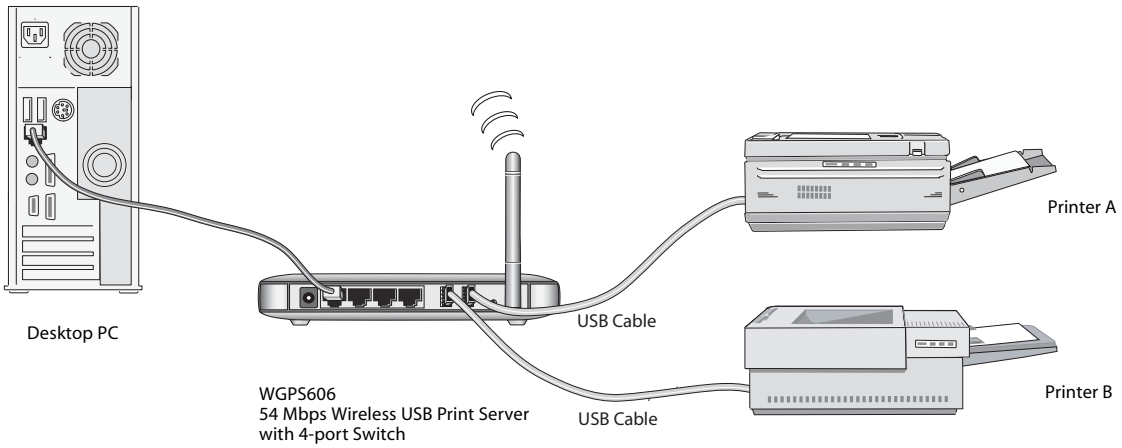


Figure 3-1: Network overview

When you finish the installation, your network will resemble this illustration.

WGPS606 Default Factory Settings

When you first receive your WGPS606, the default factory settings are shown below. You can restore these defaults with the Factory Default Restore button on the rear panel as explained in "How to Restore the Factory Default Settings" on page 2-6.

Network Setting	Default Factory Setting
IP Address	**Provided automatically via DHCP for initial setup but will be set to Static IP by the Smart Wizard during initial setup for regular operation**

Before you begin, gather your existing network settings such as the TCP/IP addresses and networking protocols in use.

Verify Printer and Network Readiness

Assure that the following are available:

- You have a working Ethernet network running TCP/IP with at least one Windows 98SE, Me, 2000, or XP PC.
- You have a printer with a USB port.

  Note: The NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 does not support printers using parallel connectors. If your printer uses a parallel connector, you should use one of the other NETGEAR Print Servers such as the Model PS101 Mini Print Server.
- You may also need to have your printer driver software handy. For most popular printers, Windows already has the printer driver software available.

Note: Set up the printer you will use directly on a computer and verify that it is working properly before connecting it to the WGPS606.

Understanding WGPS606 Wireless Security Options

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 Wireless USB Print Server provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

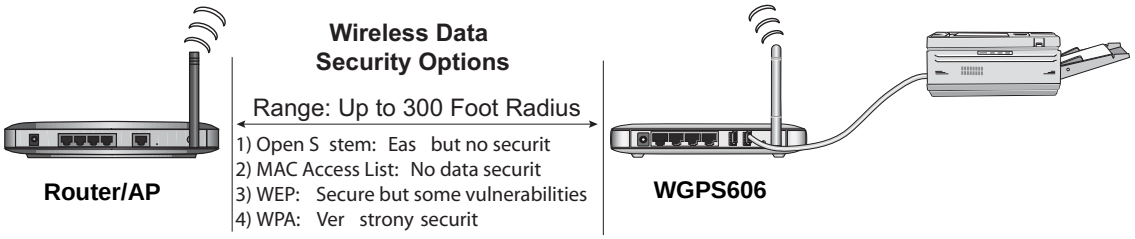


Figure 3-2: WGPS606 wireless data security options

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

- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block an eavesdropper but because the keys are static, a determined snoop can learn the keys in less than a day of eavesdropping.
- **Use WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. WPA-PSK will block eavesdropping. Because this is a new standard, wireless device driver and software availability may be limited. However, WPA is not available in bridge mode.

Observe these Precautions

For your own safety, and to protect your wireless USB print server, please observe the following precautions.

- Use only the correct power supply. Do not pinch, crimp or otherwise damage the power cord. If exposed to foot traffic, ensure that the cable is properly shielded and does not pose a tripping hazard.

- Unplug this device from its power source before cleaning. Use only a slightly dampened cloth for cleaning. Do not use liquid or aerosol cleaners.
- Avoid using this product near water. Exposure to water poses an electric-shock hazard.

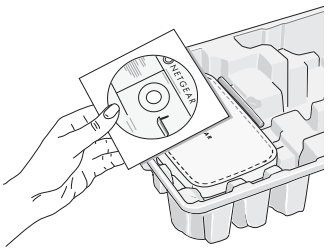
Set Up the Print Server

Note: Do not connect the Wireless USB Print Server in until you are prompted to do so by the wizard on the CD.

1. **REMOVE THE NETGEAR CD.**

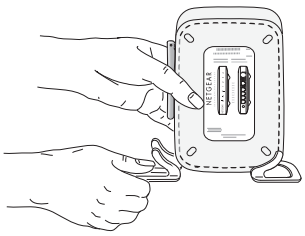
   What's on the CD?

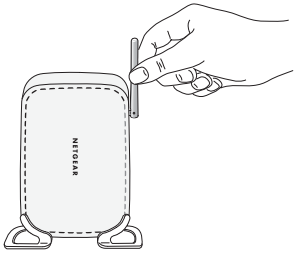
   - A setup wizard
   - Software utilities you use for customizing your print server
   - The installation and reference guides



2. **FAMILIARIZE YOURSELF WITH THE WIRELESS USB PRINT SERVER.**

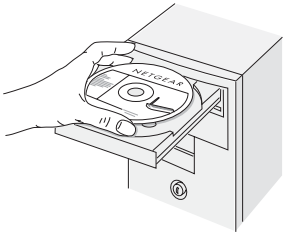
   - Take note of the useful information on the bottom label such as the port functions, default login information, etc.
   - If you plan to stand the wireless USB print server up, attach its feet.
   - Set the antenna vertically for best side-to-side coverage or horizontally for best top-to-bottom coverage.





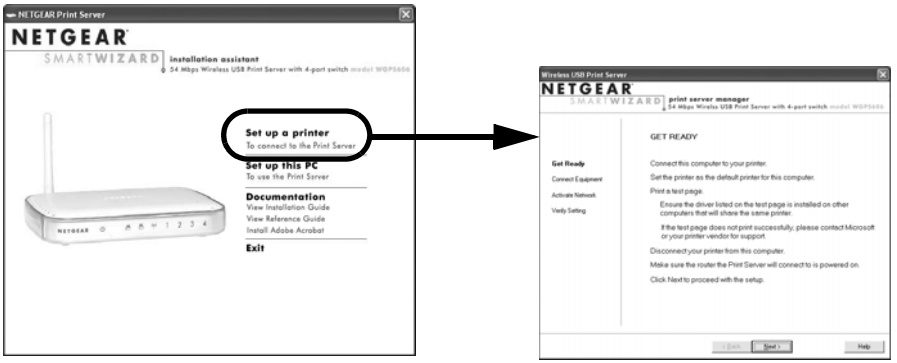
3. **NOW, INSERT THE NETGEAR CD INTO YOUR COMPUTER.**

   If the wizard screen does not appear, double click **autorun.exe** on the CD.



4. First, use the Smart Wizard to set up a printer.

a. Click **Set up a printer**.



The Smart Wizard installation assistant opens the print server manager wizard.

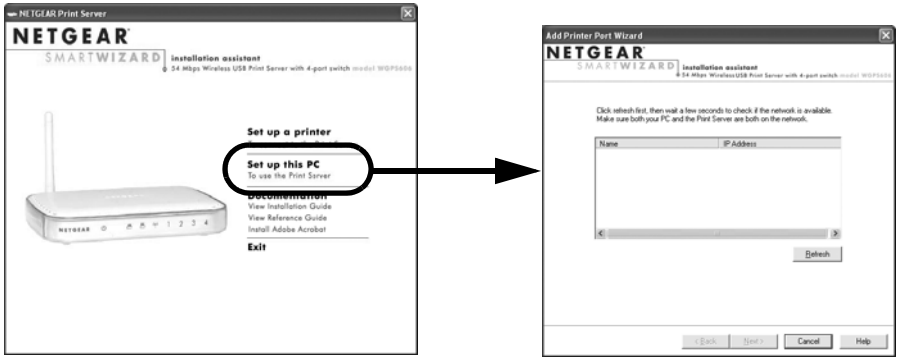
b. Follow the on-screen instructions, and click **Next** when you are ready to proceed.

c. Follow the step-by-step instructions to complete setting up the printer with the wireless USB print server.

Now, Set Up a PC

1. Use the Smart Wizard to set up a PC.

a. Click **Set up this PC**.



The Smart Wizard installation assistant opens the add printer port wizard.

b. Follow the on-screen instructions, and click **Next** when you are ready to proceed.

c. Follow the step-by-step instructions to complete setting up the PC to use the printer you just set up on the wireless USB print server.

d. Verify connectivity to the printer.

Troubleshooting Tips

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

Once the wireless USB print server is connected, always restart your network in this sequence:

1. Turn off *and* unplug the modem, turn off your router, shut off the wireless USB print server, turn off the printer, and shut down the computer.
2. Plug in and turn on the modem. Wait about 2 minutes.
3. Turn on your router. Wait about 1 minute.
4. Turn on the wireless USB print server and printer.
5. Turn on the computer.

Make sure the cables are plugged in.

For each powered on computer connected to the wireless USB print server with an Ethernet cable, the corresponding LAN status light will be lit. The label on the bottom of the wireless USB print server identifies the number of each LAN port.

Verify the wireless settings.

The Wireless Network Name (SSID) and security settings of the router and wireless USB print server must match exactly. For example, entering nETgear for the SSID is not the same as entering NETGEAR.

Make sure the network settings of the computer are correct.

Both Ethernet cable and wirelessly connected computers *must* be configured to obtain IP *and* DNS addresses automatically via DHCP.

Check the router status lights to verify correct router operation.

The Power light should turn solid green. If after 2 minutes it is not, reset the wireless USB print server as described in the *Setup Manual* on the CD.

If after completing the setup, the Wireless light does not come on, log in to the wireless USB print server and verify that the wireless feature is turned on.

I don't have a working CD drive.

Follow the setup instructions in the manual on the CD.

Two Ways to Log In to the WGPS606

The NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 can be configured from Microsoft Internet Explorer browser version 5.0 or above, or Netscape Navigator Web browser version 4.78 or above. You can log in to the WGPS606 in these two ways:

- Using the Smart Wizard on the WGPS606 CD is the easiest.
- Using the IP address of the WGPS606.

The procedure for using the IP address to log in to the WGPS606 is presented here.

How to Log in Using the IP Address of the WGPS606

1. The Smart Wizard on the WGPS606 CD guides you through the process of assigning an IP address based on the addressing scheme used in your network. If you used the Setup Wizard to perform the initial configuration, you will need to use the IP address assigned at that time.

   Otherwise, 192.168.0.102 is the default IP address of your wireless USB print server. So, if the WGPS606 has not yet been installed, and there is no DHCP server on the network, you can log in to the WGPS606 using its default IP address.

   Note: The computer you are using to connect to the WGPS606 should be configured with a static IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Connect to the WGPS606 by entering its IP address into your browser.
4. A login window like the one shown below opens:

Figure 3-3: Login window

Log in using the default user name of **admin** and default password of **password**.

Your Web browser should automatically find the wireless USB print server and display this home page.

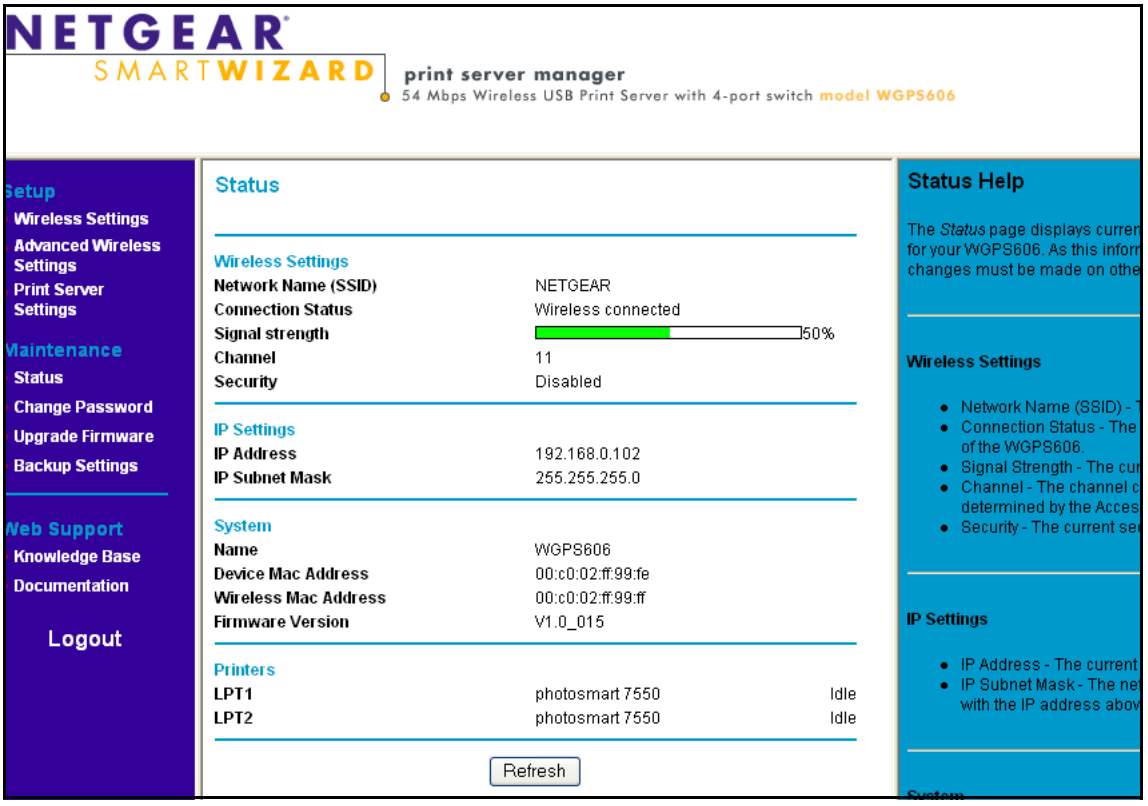


Figure 3-4: Login result: WGPS606 home page

When the wireless USB print server 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 USB print server.

If you do not click Logout, the wireless USB print server will wait 5 minutes after there is no activity before it automatically logs you out.

Using the IP Settings Options

The IP Settings page is under the Setup heading of the main menu. Use this page to configure static IP addresses.

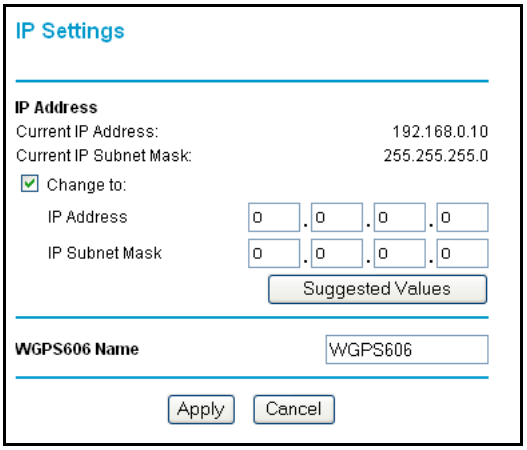


Figure 3-5: Basic IP Settings page

- **IP Settings Current IP Addresses**

  The wireless USB print server is shipped preconfigured to act as a DHCP client.

  If the wireless USB print server does not find a DHCP server in your network, it defaults to this IP configuration: IP Address of 192.168.0.102 and IP Subnet Mask of 255.255.255.0.

  If your network has a requirement to use a different IP addressing scheme, you can make those changes in this page.

- **IP Settings Suggested Values**

  The wireless USB print server is set to act as a DHCP client. DHCP addresses change dynamically based on which device connects to your network first. Your wireless USB print server needs to use the same IP address all the time. This assures that each computer can communicate with the printers attached to the wireless USB print server.

  Use the Suggested Values button to let the wireless USB print server assign an IP address in the range that your network uses. The wireless USB print server will pick a high number that is unlikely to be assigned in a home network because home networks usually have fewer than 100 devices on the network in the home.

- **WGPS606 Name**

  You can change the wireless USB print server name after the initial configuration. Enter a new name for the wireless USB print server and click Apply to save your changes.

Remember to click **Apply** to save your changes.

Understanding the Basic Wireless Settings

To configure the wireless settings of your wireless USB print server, click the Wireless Settings link in the Setup section of the main menu to view the Wireless Settings page.

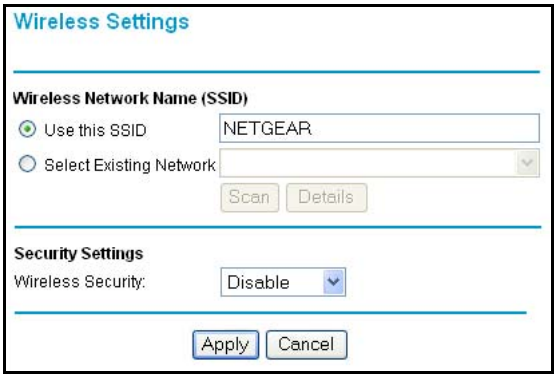


Figure 3-6: Wireless Settings page

The Basic Wireless Settings options are discussed below:

- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters; the characters are case sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network needs to use the SSID.
  - **Use this SSID**: Manually enter the SSID or accept the factory default setting.
  - **Select an Existing Network**. Click Scan. Use the drop-down list to select the one you will use from the list. If security options are enabled in the network you select, the screen will automatically change to show which security options you must use.
- **Security Settings.** This field identifies which security option will be used. Select the option from the list that matches the wireless network you will use and fill in the settings so that they match the settings of your wireless network.

Chapter 4
Management

This chapter describes how to use the management features of your NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606. These features can be found under the Maintenance heading in the main menu of the browser interface.

Viewing General Information

The Status screen summarizes of the current WGPS606 configuration settings. From the main menu of the browser interface, click Status to view the system status screen.

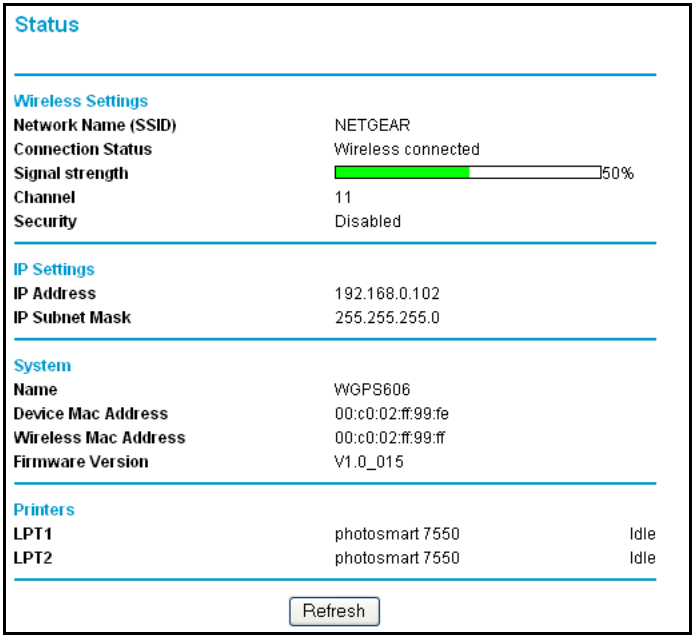


Figure 4-1: Wireless USB Print Server Status screen

This screen shows the following parameters:

Table 4-1. General Information Fields

Field	Description
Wireless Settings	These parameters apply to the target remote WGPS606, VPN gateway, or VPN client.
Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless USB print server. The default is NETGEAR.
Connection Status	Identifies if the wireless USB print server has a wireless connection.
Signal Strength	The wireless signal strength.
Channel	Identifies the channel the wireless port is using.
Security	Identifies the option the wireless USB print server is using.
IP Settings	These parameters apply to the WGPS606 wireless USB print server.
IP Address	The IP address of the wireless USB print server.
Subnet Mask	The subnet mask for the wireless USB print server.
System	
Name	The default name can be changed if desired.
Device MAC Address	Displays the Media Access Control address (MAC Addresses) of the wireless USB print server.
Wireless MAC Address	Displays the Media Access Control address (MAC Addresses) of the wireless USB print server's wireless port.
Firmware Version	The version of the firmware currently installed.
Printers	These parameters apply to the Local WGPS606 wireless USB print server.
LPT1	Idle, printing, no paper, or error information for the printer connected to USB port 1.
LPT2	Idle, printing, no paper, or error information for the printer connected to USB port 2.

Backing Up the Wireless USB Print Server Settings

	**Note:** Before you upgrade firmware or restore the factory settings, be sure to back up the current settings of your wireless USB print server.

1. From the main menu Maintenance section, click the Backup Settings link.
2. Click Save to save a copy of the current settings to a file.

Upgrading the Wireless USB Print Server Software

	**Note:** When uploading software to the Wireless USB Print Server, 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 WGPS606 completely inoperable.

You cannot perform the firmware upgrade from a workstation connected to the WGPS606 via a wireless link. The firmware upgrade must be performed via a workstation connected to the WGPS606 via the Ethernet LAN interface.

The software of the Wireless USB Print Server is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.IMG) file before sending it to the wireless USB print server. The upgrade file can be sent using your browser.

Note: The Web browser used to upload new firmware into the WGPS606 must support HTTP uploads, such as Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file from NETGEAR, save it to your hard disk, and unzip it.

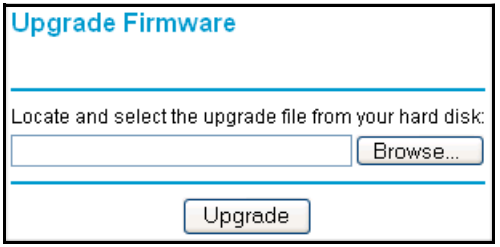


Figure 4-2: WGPS606 Upgrade Firmware page

2. From the main menu Maintenance section, click the Upgrade Firmware link to display the screen above.
3. Click Browse and locate the image upgrade file.
4. Click Upgrade.

   When the upload completes, your wireless USB print server will automatically restart. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the wireless USB print server after upgrading. You can click the Status link to check the Firmware Version and verify that your wireless USB print server now has the new firmware installed.

Restoring Factory Default Settings

It is sometimes desirable to restore the wireless USB print server to the factory default settings. This can be done by using the Erase button in the Backup Settings menu, which restores all factory default settings. Be sure to back up your settings before restoring the factory defaults.

After a restore, the password will be **password**, the DHCP client is enabled, the WGPS606 defaults to the LAN IP address of 192.168.0.102 when there is no DHCP server.

Using the Reset Button to Reboot or Restore Factory Defaults

To restore the factory default configuration settings, you use the Default Reset button on the rear panel of the wireless USB print server. The reset button has two functions:

- **Reboot.** When pressed and released quickly, the wireless USB print server 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, when held down longer.

To clear all data and restore the factory default values:

1. Use something with a small point, such as a pen, to press the Reset button in for at least 10 seconds.
2. The power light will turn yellow and blink.
3. Release the Reset button.

The factory default configuration has now been restored, and the WGPS606 is ready for use.

Changing the Administrator Password

The default password is **password**. Change this password to a more secure password. You cannot change the administrator login name.

From the main menu of the browser interface, under the Maintenance heading, click Change Password to bring up the page shown below.

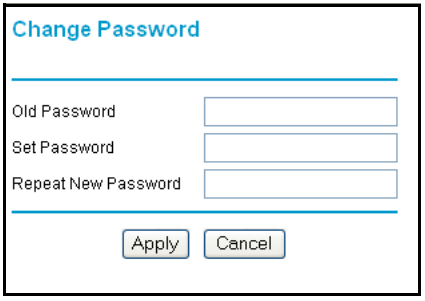


Figure 4-3: Set Password page

To change the password, first enter the old password, and then enter the new password twice. Click Apply to save your change.

Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your WGPS606. These features can be found under the Setup heading in the main menu.

Understanding Advanced Wireless Settings

From the main menu of the browser interface, under the Setup heading, click Advanced Wireless Settings to bring up this page.

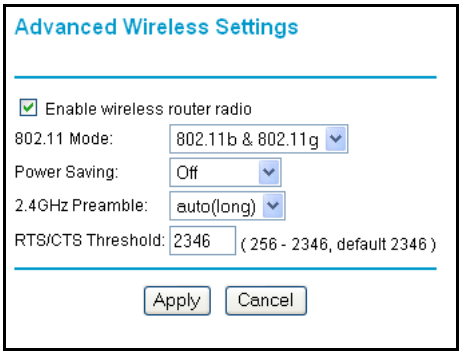


Figure 5-1: Advanced Wireless Settings menu

The default advanced wireless settings usually work well. These settings should not be changed unless you are sure it is necessary.

- **Enable wireless radio.** If you disable the wireless radio, only devices that are directly connected to the switch via an Ethernet cable can use the print server.
- **Mode.** The default is g and b. You can change the mode to g or b only.
- **Power Saving**: Generally this is best left off. Select the option you will use.
- **2.4 GHz Preamble**: A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. The default is auto.

- **RTS Threshold**: Generally this should not be changed. Changing this incorrectly could cause the wireless communications to fail.
  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.

Chapter 6
Troubleshooting

This chapter provides information about troubleshooting your NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WGPS606 on?
- Have I connected the wireless USB print server correctly?

  Go to "Basic Installation and Configuration" on page 3-1.
- I cannot remember the wireless USB print server's configuration password.

  Go to "Using the Reset Button to Reboot or Restore Factory Defaults" on page 4-4.

Note: For up-to-date WGPS606 installation details and troubleshooting guidance visit *http://kbserver.netgear.com*

This chapter gives information about troubleshooting your NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless USB print server on and is the Status light lit?

  Go to "Bottom Label Description" on page 2-4.
- Have I connected the wireless USB print server correctly?

  Go to "Set Up the Print Server" on page 3-4.
- I can't access the wireless USB print server from my computer.

  Go to "Now, Set Up a PC" on page 3-5

Basic Functioning

If you have trouble setting up your WGPS606, check the tips below.

The wireless USB print server has no power

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

No lights are lit on the wireless USB print server

It takes a few seconds for the status light to be lit. Wait a minute and check the status light on the wireless USB print server.

Printing Errors

The printer is printing “garbage” characters

- It is possible that the printer does not match the printer driver in the operating system. Run the Set Up This PC Wizard to correct this problem.
- If two printers are connected to the WGPS606, the printer driver may have been incorrectly selected. Run the Set Up This PC Wizard to verify that the correct driver is selected for the printer your want to use.

Windows error message appears when printing

Consult Windows help.

Also, look at the status screen of the WGPS606 to see if the printer is listed as “idle” “printing” “no paper” or “error.” Correct any problem indicated.

Differences in How Windows Handles Printing to the WGPS606

- **For Windows XP and 2000: TCP/IP Line Printer Remote (LPR) Printing**
  - — You print directly to your wireless USB print server. Print jobs are spooled (queued) on each computer. The computer sends the print job directly to the LAN IP address of the WGPS606.
  - — If multiple large print jobs are sent at the same time, Windows will report an error while it waits for the printer to become available and retries automatically until the job prints. You can ignore the Windows error message.
- **For Windows 95/98/Me: Printer Port Driver**
  - — The Smart Wizard installs the Printer Port Driver on the Windows computer.
  - — You print directly to your wireless USB print server. Print jobs are spooled (queued) on each computer. If multiple large print jobs are sent at the same time, the Printer Port Driver suppresses Windows printer busy error messages while waiting for the printer to become available and retries automatically until the job prints.

The print server is not found

Make sure you can access the Internet or other places on your network from your computer. If you cannot, then troubleshoot your computer or network connectivity.

If you are running a software firewall, disable it. This includes the Windows XP firewall — which may have been turned on during Windows upgrade or installation without you being aware of it.

If you have more than one network, be sure the WGPS606 is on the network you are trying to use.

Nothing is printing

- Try printing from another computer. If this is successful, then there is a problem with your computer configuration, not the print server. Consult the computer and operating system documentation.
- Turn off the print server, then turn it on. Test whether the print server works.
- If the printer does not match the printer driver in the operating system, then run the Set Up this PC wizard. See “Now, Set Up a PC” on page 3-5.
- Disable the printer's bidirectional feature, if it is turned on.

I am using a DHCP server, and the Wireless USB Print Server gets an IP Address conflict

If the wireless USB print server is left on when the DHCP server is turned off, the wireless USB print server will retain its IP Address without informing the DHCP server. If possible, reserve the IP address in the DHCP server for the wireless USB print server.

Restoring the Default Configuration

This section explains how to restore the factory default configuration settings to the WGPS606.

Use the Default Reset button on the rear panel of the wireless USB print server. Use this method for cases when the administration password or IP address is not known. See "Reset and Restore to Factory Defaults Button" on page 2-6 for a description of this button.

Windows Printer Port Management

- If you change the printer attached to the WGPS606, run the Smart Wizard program again and set up the new printer.
- Print jobs can be managed from Windows. Open the Printers folder (Start -> Settings -> Printers) and double-click any printer to see the current print jobs.
- For a Windows XP or 2000 computer, use Start -> Printers to open the Printers folder, then right-click the Printer and select Properties. Use the Advanced and Device Settings tab pages to configure printing preferences for this computer.
- For a Windows 98/Me computer, use Start -> Settings -> Printers to open the Printers folder, then right-click the Printer and select Properties. The Port Settings button is on either the Details or Port tab, depending on your version of Windows. Increase the retry interval if print jobs fail to print because they have to wait a long time to gain access to a printer that is heavily used.

Appendix A
Specifications

This appendix provides the NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606 technical specifications.

Specifications for the WGPS606

Parameter	NETGEAR 54 Mbps Wireless USB Print Server with 4-Port Switch WGPS606
Radio Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data Encoding:	Direct Sequence Spread Spectrum (DSSS) for 802.11b and Orthogonal Frequency Division Multiplexing (OFDM) for 802.11g
Wireless Security:	WEP and WPA-PSK
Network Management	Web-based configuration and status monitoring
Status LEDs	Power/Ethernet LAN/Wireless LAN/LPT1 and LPT2
Dimensions:	28x175x119 mm (1.1x6.9x4.7 inches)
Power Adapter	12V, 1.0 A
Weight	0.6 lb (0.27kg)
Electromagnetic Compliance	FCC Part 15 Class B and Class C, C-tic, VCCI
Environmental Specifications	Operating temperature: 0 to 40° C Operating humidity: 5-95%, non-condensing

Appendix B
Wireless Networking Basics

This chapter provides an overview of wireless networking and security.

Wireless Networking Overview

The Wireless USB Print Server conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11g standard for wireless LANs (WLANs). On an 802.11 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 802.11g wireless link is 54 Mbps, but it will automatically back down from 54 Mbps when the radio signal is weak or when interference is detected.

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.

Wireless Channels

IEEE 802.11g/b 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 are listed in Table B-1:

Table B-1. 802.11b 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
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.

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.

WEP Wireless Security

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 two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. 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. Recently, Wi-Fi, the Wireless Ethernet Compatibility Alliance (*http://www.wi-fi.net*) developed the Wi-Fi Protected Access (WPA), a new strongly enhanced Wi-Fi security. WPA will soon be incorporated into the IEEE 802.11 standard. WEP and WPA are discussed below.

WEP 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 WGPS606:

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 WEP 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.

WEP Open System Authentication

This process is illustrated in below.

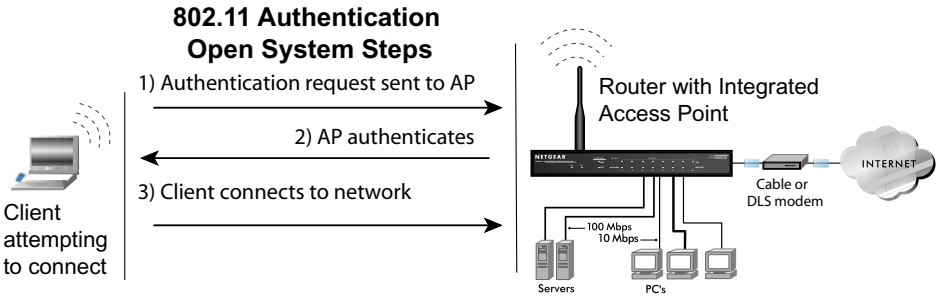


Figure B-1: 802.11 open system authentication

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.

WEP Shared Key Authentication

This process is illustrated in below.

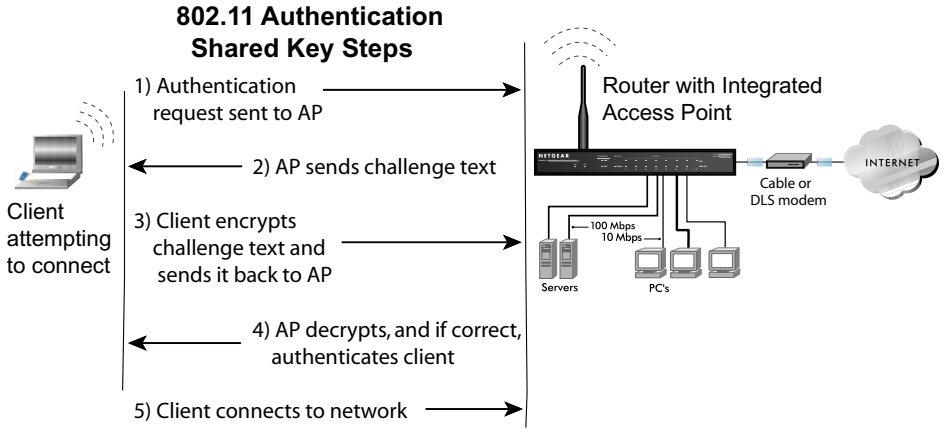


Figure B-2: 802.11 shared key authentication

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 (i.e., 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.

Key Size and Configuration

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, 802.11b 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.

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.

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, etc.

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.

How to Use WEP Parameters

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

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 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b 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 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption). However, the WGPS606 does not offer this option.

WPA Wireless Security

Wi-Fi Protected Access (WPA) 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. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the short comings 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 being defined in the IEEE. Wireless vendors have agreed on WPA as an interoperable standard.

WPA offers the following benefits:

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

Starting August of 2003, all new Wi-Fi certified products had to support WPA. NETGEAR implemented WPA on client and access point products and made this available in the second half of 2003.

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 don't 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 IEEE 802.11i?

WPA is forward compatible with the IEEE 802.11i security specification. WPA is a subset of 802.11i and uses certain pieces of the 802.11i were ready to bring to market, such as 802.1x and TKIP. The main pieces of 802.11i 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 require hardware upgrades and as of January 2005 are now becoming widely available.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael *message integrity code* (MIC)
  - AES Support
- Support for a Mixture of WPA and WEP Wireless Clients

These features are discussed below.

WPA 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 (e.g., user names and passwords) and authenticates wireless users before they gain access to the network.

The strength WPA 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'll talk more 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 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 Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

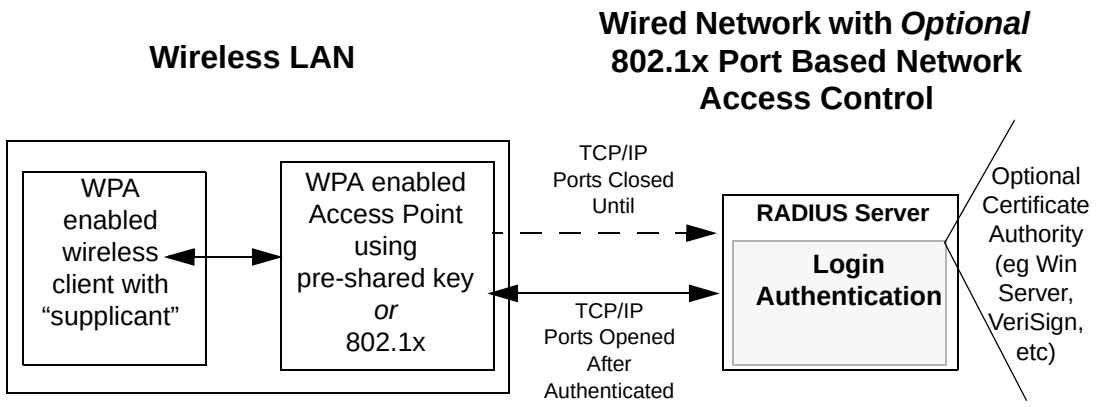


Figure B-3: WPA Overview

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's important to note that 802.1x doesn't 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 preshared 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.

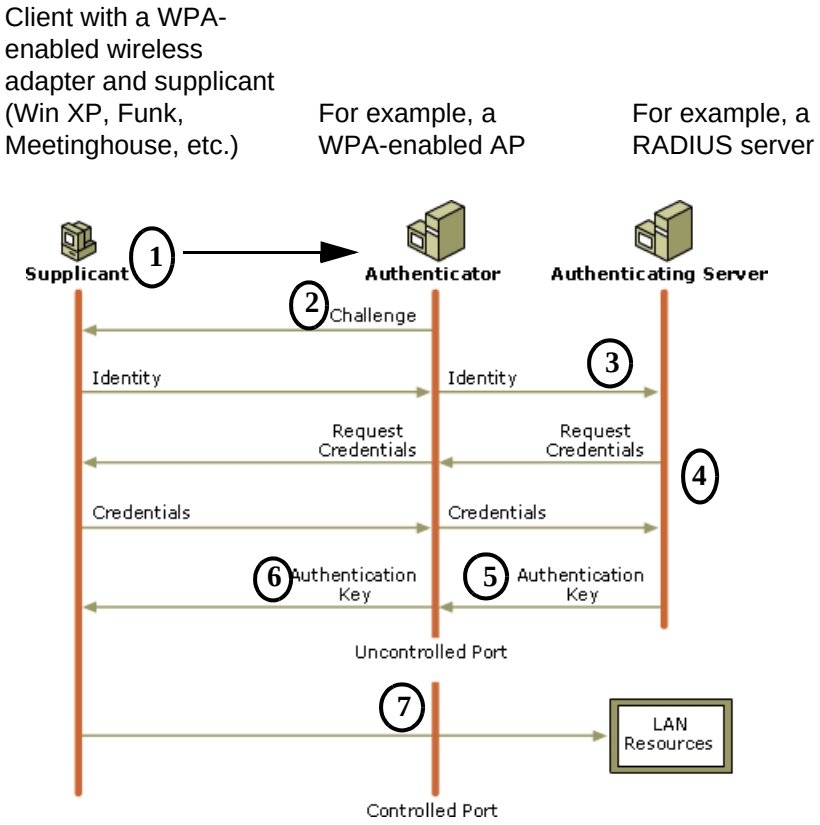


Figure B-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA 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 (i.e., client device) attempting to connect with an authenticator (i.e., 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 (e.g., 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 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, 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 code* (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

One of the encryption methods supported by WPA beside TKIP is the advanced encryption standard (AES), although AES support is required for WPA2 for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but AES requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP was a pragmatic compromise that allowed organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA 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) check 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 includes 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 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

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 requires software changes to the following:

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

Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA 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 and non-WPA clients would offer network security that is no better than that obtained with a non-WPA 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 information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

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

Changes to Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

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

To upgrade your wireless network adapters to support WPA, obtain a WPA 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 firmware update in the wireless adapter driver. So, to update you Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

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

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

Glossary

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

Numeric

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

802.11g
An IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

10BASE-T
The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-TX
The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
gain access.

A

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

B

Bandwidth
The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

C

Class of Service
A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

D

DHCP
See “Dynamic Host Configuration Protocol.”

DSL
Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol.
DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

Ethernet
A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

G

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

I

Infrastructure Mode
An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Internet Protocol
The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in

the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP
See "Internet Protocol"

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP
Internet service provider.

L

LAN
See "Local Area Network"

Local Area Network
A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC
(1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

N

NAT
See “Network Address Translation”

netmask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation
Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

NIC
Network Interface Card. An adapter in a computer which provides connectivity to a network.

P

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Protocol
A set of rules for communication between devices on a network.

Q

QoS
See “Quality of Service”

Quality of Service
QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

S

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Segment
A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Subnet Mask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

T

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

U

Universal Plug and Play
UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP
Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

W

WAN
See “Wide Area Network”

Web
Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

WEB Proxy Server
A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall. The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP
Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

WPA

Wi-Fi Protected Access (WPA) 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.