LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G

PrintServer for USB 2.0

User Guide

WIRELESS

Model No. **WPS54GU2**

Cisco Systems

Copyright and Trademarks

How to Use this User Guide

This User Guide has been designed to make understanding networking with the PrintServer easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a note of interest and is something you should pay special attention to while using the PrintServer.

This exclamation point means there is a caution or warning and is something that could damage your property or the PrintServer.

This question mark provides you with a reminder about something you might need to do while using the PrintServer.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Linksys Wireless-G PrintServer for USB 2.0. The Linksys Wireless-G PrintServer for USB 2.0 lets you connect a USB or parallel printer (or both) directly to your network, eliminating the need to dedicate a PC to print sharing chores. Using a PrintServer frees up your "print share PC" so you don't have to leave it on all the time. It also removes the printing bottleneck, and sets your PC free to do more useful work.

Connect the PrintServer directly to your network by 10/100 Ethernet cable, or wireless over 54Mbps Wireless-G (802.11g). The wireless option lets you put your printers wherever you want to, without having to run cables. Whichever way the PrintServer is attached to your network, both your wireless and wired PCs will have access to it, and the printers it's connected to. And if you don't use wireless for general networking in your office, you can still use the Wireless-G connection in ad-hoc mode to print from visiting Wireless-G and Wireless-B PCs.

802.11g: *an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

The USB port is compatible with USB 1.1 printers, as well as printers that support the new high-speed USB 2.0 specification for even faster throughput. There's also a separate port for a standard parallel printer. For even more versatility, you can connect two printers, one to each port, and send your documents to whichever one is most appropriate for each print server.

A user-friendly Setup Wizard makes installation easy, the compact case fits anywhere, and the three megabyte print buffer size handles even large graphics-intensive print jobs. Let the Linksys Wireless-G PrintServer for USB 2.0 bring efficiency to your printing tasks.

What's in this Guide?

This user guide covers the steps for setting up and using the PrintServer.

- Chapter 1: Introduction
  This chapter describes the PrintServer's applications and this User Guide.
- Chapter 2: Getting to Know the PrintServer
  This chapter describes the physical features of the PrintServer.
- Chapter 3: Connecting the PrintServer
  This chapter instructs you on how to connect the PrintServer to your network.
- Chapter 4: Configuring the PrintServer using the Setup Wizard
  This chapter instructs you on how to use the Setup Wizard to install your PrintServer.

- Chapter 5: Windows Driver Installation
  This chapter explains how to install the Windows driver for the PrintServer.

- Chapter 6: Configuring the PrintServer Using the Web-based Utility
  This chapter explains how to configure the PrintServer using the web-based utility.

- Chapter 7: Bi-Admin Management
  This chapter explains how to configure the PrintServer using the Bi-Admin Management utility.

- Chapter 8: Internet Printing Protocol (IPP)
  This chapter instruct you on how to use the PrintServer as an IPP server so you can remotely print.

- Appendix A: Troubleshooting
  This appendix describes some potential problems and solutions regarding use of the PrintServer.

- Appendix B: Wireless Security
  This appendix explains the security risks in wireless networking and how you can help protect your network

- Appendix C: About Bi-Directional Printing
  This appendix describes bi-directional printing.

- Appendix D: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on the PrintServer should you need to do so.

- Appendix E: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

- Appendix F: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix G: Specifications
  This appendix provides the technical specifications for the PrintServer.

- Appendix H: Warranty Information
  This appendix supplies the warranty information for the PrintServer.

- Appendix I: Regulatory Information
  This appendix supplies the regulatory information regarding the PrintServer.

- Appendix J: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Getting to Know the PrintServer

The Back Panel

The PrintServer's ports are located on the back panel.

Figure 2-1: PrintServer's Back Panel

Power The **Power** port is where you will connect the power adapter.

Parallel The **Parallel** port is where you will connect the parallel printer to the PrintServer.

USB The **USB** port is where you will connect the USB printer to the PrintServer.

The USB icon (right) designates a USB port. The PrintServer comes with a USB cable. One end has a rectangular connector called Type A. The other end has a square connector called Type B. The USB cable's Type A end connects to the PrintServer, and the Type B end connects to the printer.

USB Connector-Type A

USB Connector-Type B

LAN The **LAN** port is where you will connect the PrintServer to your wired network.

Reset Button Use the **Reset Button** to reset the PrintServer to its factory defaults or print a test page. The instructions are provided on the right side of this page.

Important: Resetting the PrintServer will erase all of your settings and replace them with the factory defaults. Do not reset the PrintServer if you want to retain the settings.

To reset the factory default settings

1. Unplug the PrintServer.
2. Press and hold the Reset button. While pressing the button, plug in the PrintServer.
3. If you continue pressing the button for 10 seconds, the PrintServer will be reset to factory defaults.

To generate a diagnostic print-out

1. Ensure that both the PrintServer and the printer attached to the Printer port are ON.
2. Press the Reset button, and hold it in for 2 seconds.
3. The test page, which lists the current settings, will be printed.

PostScript printers are unable to print this page. If you have a PostScript printer on the Printer port, the test page will not be printed.

LAN (Local Area Network): *the computers and networking products that make up the network in your home or office.*

The Front Panel

The PrintServer's LEDs are located on the front panel.

Figure 2-2: PrintServer's Front Panel

Status Green/Orange. If the **Status** LED is continuously lit green, then the PrintServer is ready for use. The LED flashes green when the PrintServer is booting up, a system self-test is running, or the firmware is being upgraded. It lights up orange when there is an error.

LAN Green/Orange. If the **LAN** LED is continuously lit green, the PrintServer is successfully connected to a device through the LAN port. The LED flashes green when the PrintServer is actively sending or receiving data from the wired network. It flashes orange when there are collisions detected on the LAN port.

WLAN Green. The **WLAN** LED serves two purposes. If the LED is continuously lit, the PrintServer is successfully connected to the wireless network. If the LED is flashing, the PrintServer is actively sending or receiving data from the wireless network.

Parallel Green/Orange. The **Parallel** LED lights up green when there is a printer connected to the parallel port. The LED flashes green when the PrintServer is sending data through the parallel port. It lights up orange when there is a problem with the parallel printer.

USB Green/Orange. The **USB** LED lights up green when there is a printer connected to the USB port. The LED flashes green when the PrintServer is sending data through the USB port. It lights up orange when there is a problem with the USB printer.

Chapter 3: Connecting the PrintServer

Overview

Before starting the physical installation, make a note of the PrintServer's Default Name, which is located on the bottom of the PrintServer. There is a bar code sticker with an LK number printed on it (for example, LK71107). This number is used during the PrintServer driver installation.

Connecting the PrintServer to Your Network

1. Plug one end of the Ethernet network cable into the PrintServer's LAN port. (See Figure 3-1.)
2. Connect the other end of the cable to your networked hub, switch, or router. The distance between the PrintServer and the other device should not exceed 328 feet (100 meters).
3. Use the USB cable to connect your USB printer to the PrintServer's USB port. Plug the Type A connector end into the PrintServer (Figure 3-2) and the Type B connector end into the printer.
4. Use the parallel printer cable to connect your parallel printer to the PrintServer's parallel port. Plug one end of the cable into the PrintServer (Figure 3-3) and the other end into the printer.
5. Power on your printer.
6. Plug the power adapter into the PrintServer's Power port. (See Figure 3-4.)
7. Plug the power adapter into an electrical outlet.

IMPORTANT: Make sure you use the power adapter supplied with the PrintServer. Use of a different power adapter could damage the PrintServer.

NOTE: The PrintServer does not have an on/off power switch. Whenever its power adapter is plugged into a power supply, the PrintServer is powered on. The PrintServer can be powered on before, during, or after your network is powered on.

Figure 3-1: Connecting to the LAN Port

Figure 3-2: Connecting to the USB Port

Figure 3-3: Connecting to the Parallel Port

Figure 3-4: Connecting to the Power Port

Chapter 4: Configuring the PrintServer Using the Setup Wizard

Installation

To install the PrintServer, you will use the Setup CD-ROM to run the Setup Wizard. It is highly recommended that you use a computer on the wired network to set up the PrintServer. However, if you only have a wireless network, then you can use a computer on the wireless network to set up the PrintServer.

1. Insert the Setup CD-ROM into the computer's CD-ROM drive. The Setup Wizard should run automatically. If it does not, click the **Start** button and choose **Run**. In the box that appears, enter **D:\setupWizard.exe** (if "D" is the letter of your CD-ROM drive).

2. When you see Figure 4-1, click **Setup Wizard** to continue. Click **Exit** to end the installation. Click **User Guide** button to view the User Guide.

3. After the Setup Wizard has found the PrintServer, the screen in Figure 4-2 will appear. If this is the first time you have run the Setup Wizard, make sure that **List only new (unconfigured) Print Servers** is selected and your PrintServer is listed by its default server name. Next to the PrintServer's Server Name is its IP Address. Note the IP Address so you can use it to access the PrintServer's web-based utility, as described in "Chapter 6: Configuring the PrintServer Using the Web-based Utility."

   If you have previously configured the Print Server, select **List all compatible Print Servers**. Click **Next** to continue.

   Click the **Refresh** button to refresh the screen. Click **Back** to return to the previous screen.

Figure 4-1: Welcome

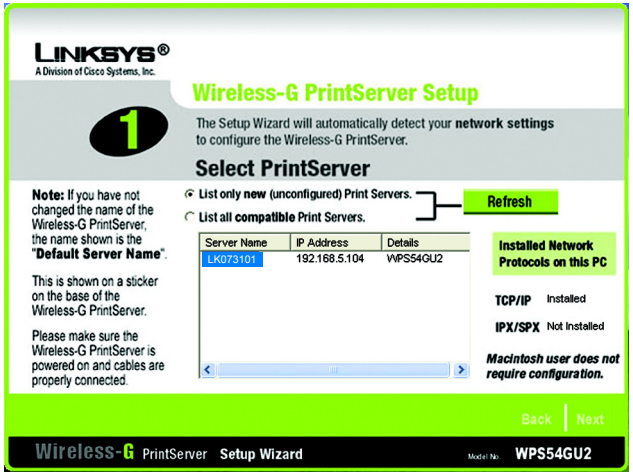

Figure 4-2: Wireless-G PrintServer Setup

IP address: *the address used to identify a computer or device on a network.*

4. The *Password* screen, Figure 4-3, will appear next. Enter the default password **admin** in the field provided. Click **Enter**.

5. The *Basic Settings* screen, shown in Figure 4-4, will appear. If you want to change the Device Name or Domain Name, enter the Device Name and Domain Name in the respective fields. Click **Next**.

   Click **Back** to return to the previous screen.

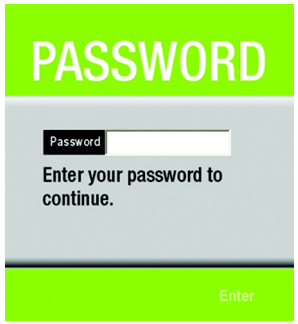

Figure 4-3: Password

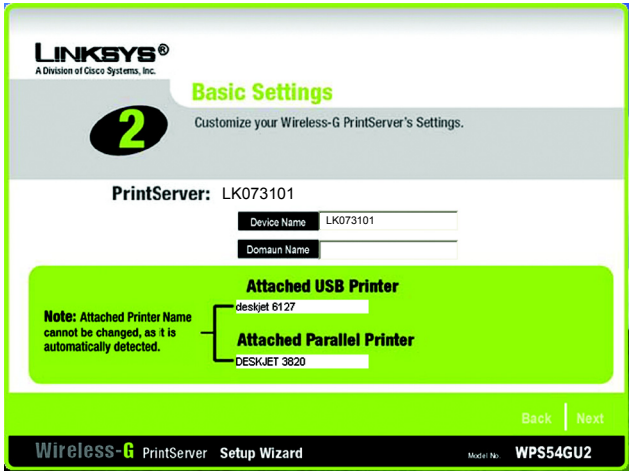

Figure 4-4: Basic Settings

6. The *IP Settings* screen, Figure 4-5, will appear. If your network uses a router with a DHCP setting that automatically assigns IP addresses, select **Automatically obtain an IP address (DHCP)**. If your network uses a static IP address, select **Set IP configuration manually**, and enter the IP Address, Subnet Mask, and Gateway in the fields provided. Click **Next**.

   Click **Back** to return to the previous screen.

7. The *Set PrintServer's Password* screen, shown in Figure 4-6 will appear. If you want to change your password, enter your current password in the *Current Password* field. Enter the new password in the *New Password* field, then enter it again in the *Verify Password* field. Click **Next**.

   Click **Back** to return to the previous screen.

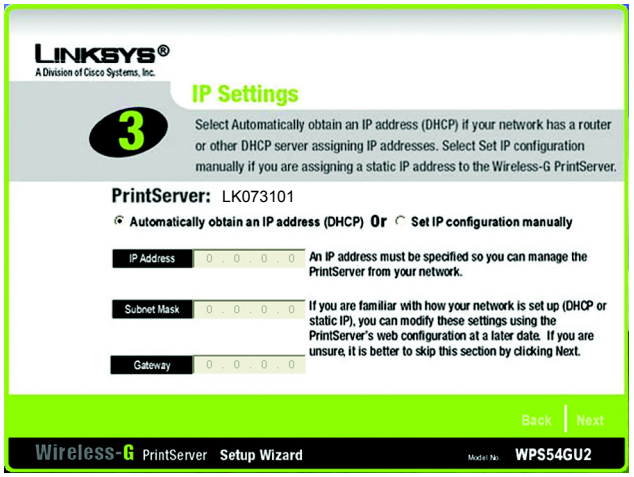

Figure 4-5: IP Settings

Static IP address: *a fixed address assigned to a computer or device connected to a network.*

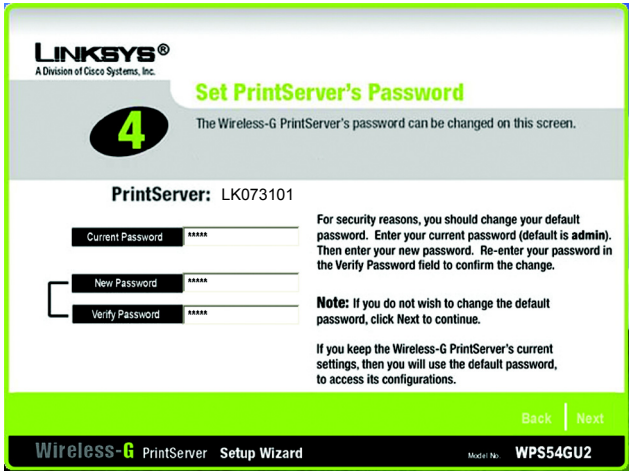

Figure 4-6: Set PrintServer's Password

8. The *Wireless Settings* screen will appear. In the *SSID* field, enter your wireless network's SSID or name. This is the unique name shared by all devices in a wireless network. The SSID is case-sensitive and should have 32 characters or fewer.

   Select the channel at which the network broadcasts its wireless signal (available only if you selected Ad-Hoc for the Network Type setting).

   The Network Type setting shows a choice of two wireless modes. Select **Infrastructure** if you want the PrintServer to communicate using an access point or wireless router. Select **Ad-Hoc** if you want the PrintServer to communicate without using an access point or wireless router.

   Click the **Next** button to continue.

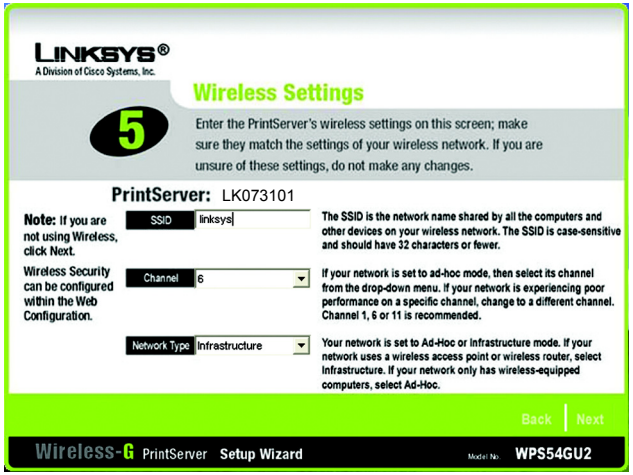

Figure 4-7: Wireless Settings

SSID: *your wireless network's name.*

Infrastructure: *configuration in which a wireless network is bridged to a wired network via an access point.*

Ad-hoc: *a group of wireless devices communicating directly to each other (peer-to-peer) without the use of an access point.*

9. The *Wireless Security Settings* screen, shown in Figure 4-8, will appear. If you want to enable WEP encryption for greater wireless security, select the level of WEP encryption, **64 Bit Keys** or **128 Bit Keys**, and then enter a Passphrase. If you use a Passphrase, a WEP key will be automatically generated after you click the Next button. The Passphrase is case-sensitive and should have 16 alphanumeric characters or fewer. It must match the passphrase of your wireless network and is compatible with Linksys wireless products only. (You will have to enter the WEP key(s) manually on any non-Linksys wireless products.)

   If you want to enter the WEP key manually, then leave the *Passphrase* field blank; you will be able to enter a WEP key on the following screen. If you want to disable WEP encryption, keep the default, **Disabled**.

   Click the **Next** button to continue.

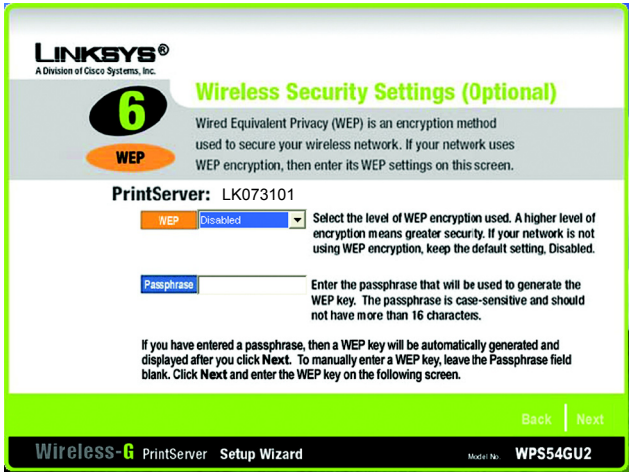

Figure 4-8: Wireless Security Settings

WEP (Wired Equivalent Privacy): *a method of encrypting data transmitted on a wireless network for greater security.*

Passphrase: *used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption for Linksys products.*

10. If you entered a Passphrase, you will see the automatically generated WEP key on the following screen, as shown in Figure 4-9. Otherwise, enter the WEP key manually in the field provided. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F". Click **Next**.

11. The *Confirmation* screen will appear. See Figure 4-10. Your old and new settings will be displayed. If you want to make a change, click **No** and you will exit the Setup Wizard; you will have to start the Setup Wizard again. If the settings are correct and you want to save the changes, click **Yes**.

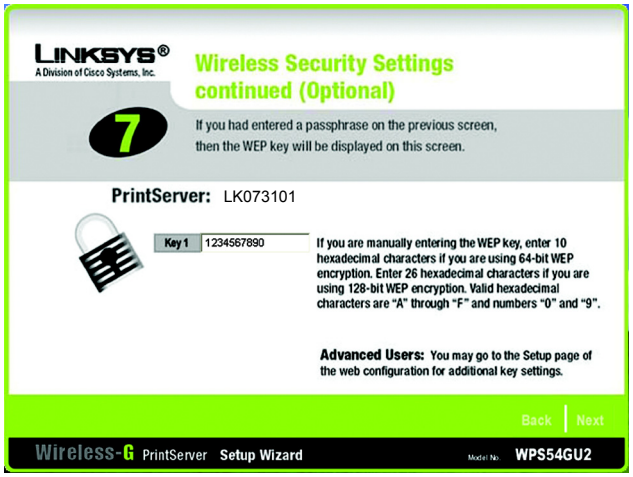

Figure 4-9: Wireless Security Settings - WEP Key

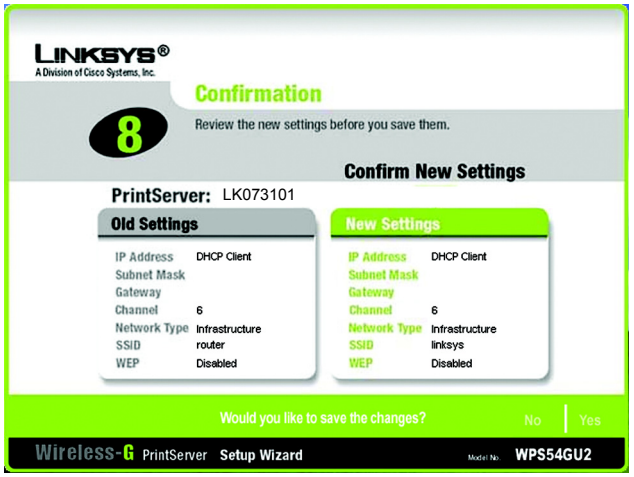

Figure 4-10: Confirmation

12. The *Congratulations* screen, shown in Figure 4-11, will appear. The setup is complete.

    You will need to install the driver next. Click **User Install** at the bottom of the *Congratulations* screen, and go to "Chapter 5: Windows Driver Installation."

Figure 4-11: Congratulations

Chapter 5: Windows Driver Installation

Overview

This section installs the PrintServer's software on your Windows 98, Me, 2000, or XP computers so they can use the PrintServer for print jobs. (The PrintServer is fully compatible with Windows 98, Me, 2000, and XP.)

At this point, you must have the following:

- the PrintServer hardware installed on your network. If not, see "Chapter 3: Connecting the PrintServer."
- TCP/IP installed on each of your computers.
- an IP address assigned to each of the computers on your network.
- an IP address assigned to the PrintServer by you or your network router. By default the PrintServer has DHCP enabled so the network router will automatically assign an IP address. If you need to manually assign an IP address, run the Setup Wizard on the Setup CD-ROM or go to "Chapter 7: Bi-Admin Management."

It is assumed that your CD-ROM drive's letter name is designated as "D". If your CD-ROM drive is named another letter, replace all instances of "D" with the appropriate letter.

If you need to install the PrintServer's driver on computers without a CD-ROM drive, you can create a setup disk by using a computer with a CD-ROM drive to copy the contents of D:\Driver\PTP onto a floppy disk.

HAVE YOU: already set up your printer? Linksys recommends that you set up your printer and install your printer's driver before you install the PrintServer's driver.

Installation

1. Make sure you have no programs or applications running on your computer.

2. If you haven't already done so, insert the Setup CD-ROM into the computer's CD-ROM drive. The Setup CD-ROM should run automatically. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setupWizard.exe** (if "D" is the letter of your CD-ROM drive).

3. When you see Figure 5-1, click **User Install** to continue. Click **Exit** to end the installation.

Figure 5-1: Welcome

4. The *Welcome* screen of the driver installation program, Figure 5-2, will appear first. Click **Cancel** to quit the setup program and then close the open programs. Click **Next** to continue with the driver installation.

5. The *Choose Destination Location* screen, as shown in Figure 5-3, will appear. Choose the location where the driver's folder will be installed. To install the driver in the default location, click **Next**. If you want the folder to be installed in a different location, click the **Browse** button and select the location. Then click **Next**.

   Click **Back** to return to the previous screen. Click **Cancel** to end the driver installation.

Figure 5-2: Driver Setup Welcome

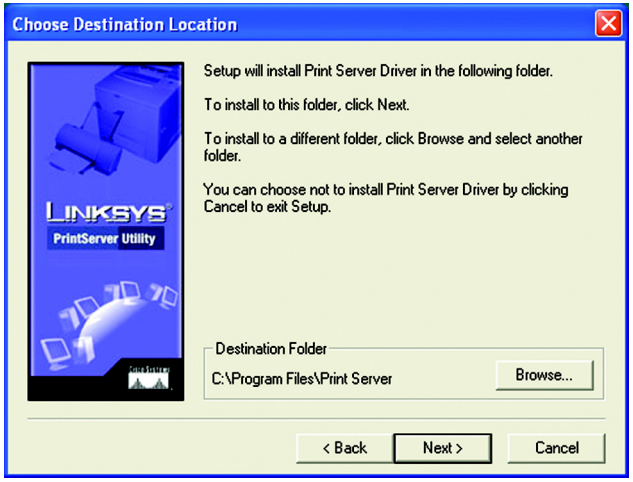

Figure 5-3: Choose Destination Location

6. The *Select Program Folder* screen will appear, as shown in Figure 5-4. An icon will be added to the program folder listed. You may change the name for the program folder, if you wish. Click **Next**.

   Click **Back** to return to the previous screen. Click **Cancel** to end the driver installation.

7. When the driver is installed, the *Setup Complete* screen, Figure 5-5, will appear. The Print Driver must still be configured, so make sure that **Configure Print Driver now** is selected. Click **Finish** to end the driver installation and begin the driver configuration.

Figure 5-4: Select Program Folder

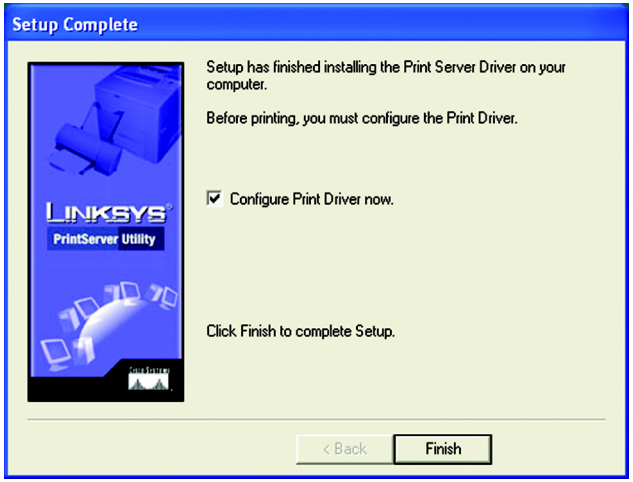

Figure 5-5: Setup Complete

Starting the Print Driver Utility

1. Click **Start**, **Programs**, **Print Server Utility**, and then **Print Driver Setup**. If the Print Driver Setup icon has been created, you can double-click it instead.

2. The *Information* screen will appear; see Figure 5-6. Read the on-screen information, and then click **OK**.

3. The *Printer Port Setup* screen will appear, as shown in Figure 5-7, and list the PrintServer and its ports. Select a printer port to add, and then click **Next**.

   If the PrintServer or printer isn't listed, make sure that the cable connections are good and the PrintServer and printer are powered on.

4. You will be informed that the PrintServer Port has been added successfully. Click **OK**.

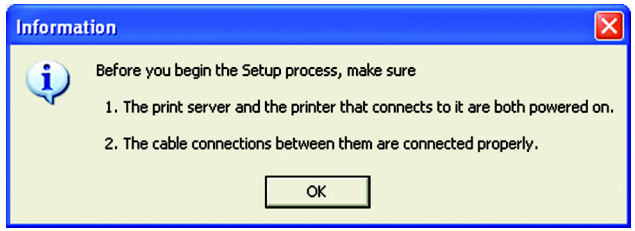

Figure 5-6: Information

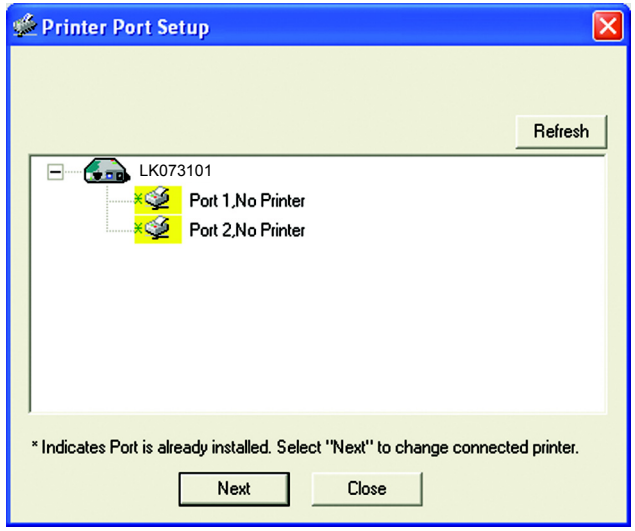

Figure 5-7: Printer Port Setup

5. The *Configure Printer Port* screen will appear, as shown in Figure 5-8. Your installed printer(s) will appear in the field. Select the printer you want, and click the **Connect** button to associate the printer with your selected printer port. To add another printer, click the **Add New Printer** button.

   Click **Cancel** to cancel the setup.

6. Click **Close** to close the *Printer Port Setup* screen. Click **Refresh** to refresh the screen.

7. The driver installation and configuration is complete. You can now use the PrintServer.

   If you would like to change the PrintServer's settings, use the PrintServer's web-based utility. For more information, refer to "Chapter 6: Configuring the PrintServer Using the Web-based Utility."

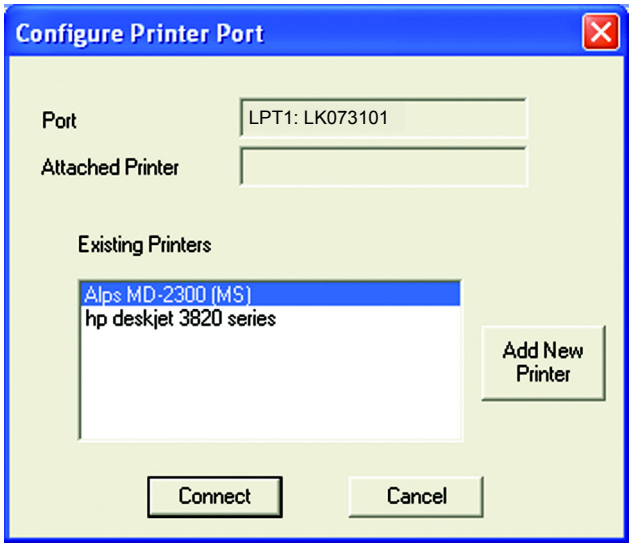

Figure 5-8: Configure Printer Port

Chapter 6: Configuring the PrintServer Using the Web-based Utility

Overview

After setting up the PrintServer with the Setup Wizard, the PrintServer will be ready for use. However, if you'd like to change its advanced settings, use the PrintServer's web-based utility. This chapter will describe each web page of the utility and each page's key functions. The utility can be accessed via your web browser through the use of a networked computer.

There are six main tabs: Setup, Protocol, Wireless, Printer, Status, and Exit. Additional tabs will be available after you click one of the main tabs.

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the PrintServer's IP address in the *Address* field. Then press **Enter**.

NOTE: Use the PrintServer's IP address that you noted when you ran the Setup Wizard. Otherwise, insert the Setup CD-ROM, and when the *Welcome* screen appears, click **Setup Wizard**. Follow the instructions until you reach the *Wireless-G PrintServer Setup* screen. Note the IP address, and then click **Back** until you reach the *Welcome* screen. Click **Exit**.

You will be asked to enter a User name and Password (see Figure 6-1). Leave the *User name* field blank, and enter **admin** in the *Password* field. Then click the **OK** button.

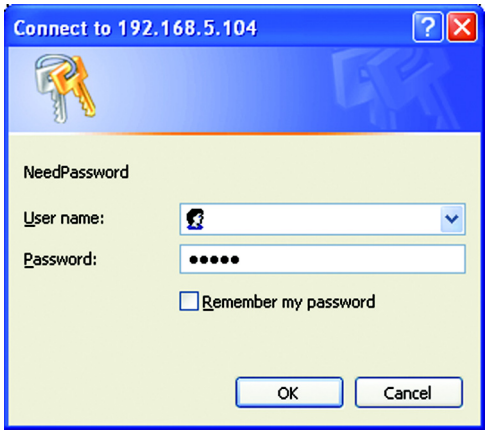

Figure 6-1: Password to Access Web-based Utility

The Setup Tab

The first screen that appears is the Setup tab and allows you to change the PrintServer's general settings.

Device Name. Enter the PrintServer's name in the field provided. The name is located on a sticker on the bottom of the PrintServer.

Password. To change the PrintServer's password, enter the current password in the *Current Password* field. Enter the new password in the *New Password* field, and then enter the new password again in the *Verify Password* field.

Protocols. Check the box(es) for AppleTalk or NetBEUI, if they are used by your network.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

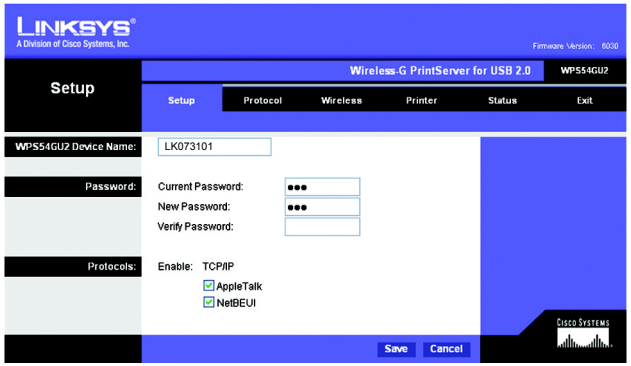

Figure 6-2: Setup

The Protocol Tab - TCP/IP

Click the TCP/IP tab to view or change the TCP/IP values of the PrintServer. (See Figure 6-3.)

IP Address. If your network router is using DHCP to assign IP addresses, select **Obtain an IP Address Automatically**. By default, **Obtain an IP Address Automatically** is enabled. If you need to assign the PrintServer a fixed IP address (also known as static IP address), select **Use the Following IP Address**, and enter the appropriate values under IP Address, Subnet Mask, and Gateway. Make sure the IP Address and Subnet Mask are appropriate for your network. If you change the PrintServer's IP address, make sure you that you reconnect to the PrintServer using that new IP address. Otherwise, you will not be communicating with the PrintServer. In most cases, the Gateway IP address is the IP address of your router, and you should complete the *Gateway* field if you will use the PrintServer for Internet printing. (To find out your router's IP address, consult your router's documentation.)

Connection. You can set how long you want the PrintServer to wait between connection attempts. You can also specify the number of times that the PrintServer will attempt to connect to the network. Enter your chosen values in the fields provided.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

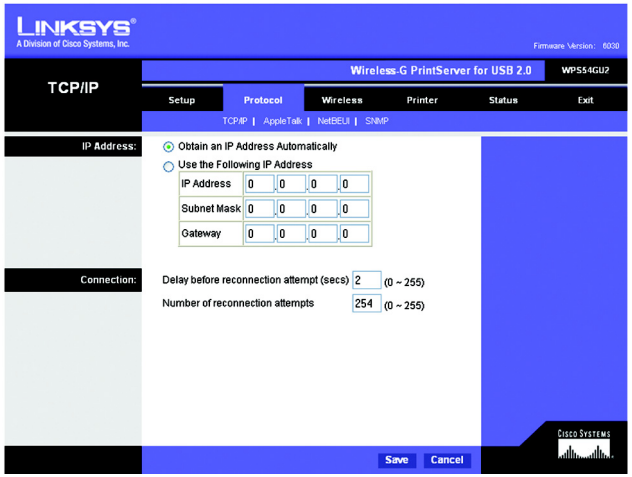

Figure 6-3: Protocol Tab - TCP/IP

The Protocol Tab - AppleTalk

AppleTalk is a network communications protocol that allows computers to talk to each other using Ethernet. Typically only Macintoshes use AppleTalk, although other platforms can use it if they have the necessary, third-party software. (See Figure 6-4.)

Communication. Port 1 is the parallel port, while Port 2 is the USB port.The PrintServer's two ports have the same settings to configure for AppleTalk.

The Printer Object Type can be obtained from the manufacturer of the printer. Enter the type of printer in the field provided. For each printer connected to the PrintServer, you will choose the Communications Protocol that allows the devices on the network to communicate. Select the type of Communication Protocol you will use, **ASCII** or **Binary** for each printer, according to the recommendation of the printer's manufacturer. For more information, refer to the printer's documentation.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

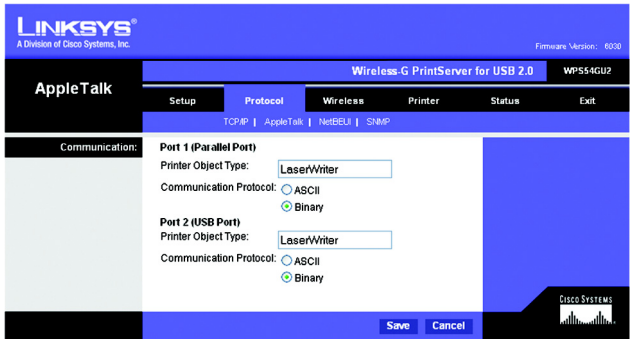

Figure 6-4: Protocol Tab - AppleTalk

The Protocol Tab - NetBEUI

NetBEUI connection settings of the PrintServer are available on this tab. (See Figure 6-5.)

Domain Name. Enter the name of the domain that you want the PrintServer associated with in the *Domain Name* field.

If you are unsure of the Domain Name, you can find it out by looking on any computer already on the network. In Windows 98, right-click **Network Neighborhood** and select **Properties**. Under the Identification tab, there will be listed that computer's name, and the Domain to which it is connected. For Windows Me, 2000, or XP, right-click **My Network Places**. In Windows Me, choose **Properties** from the menu that appears. In Windows 2000 or XP, choose **Properties** from the menu that appears. Then, right-click **Local Area Connection** and choose **Properties**. The Domain name will appear. If you want the PrintServer to be connected to that same Domain, enter that Domain name here. If no Domain name exists there, you will use the Workgroup name from that window.

Options. You can specify the Response Time that you prefer for the PrintServer. This is the amount of time (measured in seconds) that the PrintServer will wait for a response from the network before "timing out."

You also have the option to use this feature, Abort Print Job if Error. Selecting Yes here will terminate the printing if there is an error of any kind. If you select No, print jobs that have errors will be sent to the printer, but might not print properly.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

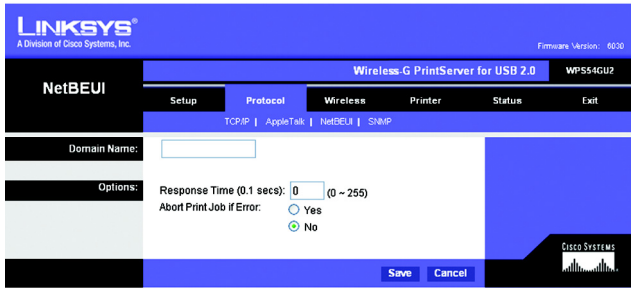

Figure 6-5: Protocol Tab - NetBEUI

The Protocol Tab - SNMP

Use the screen shown in Figure 6-6 to view or change the PrintServer's SNMP (Simple Network Management Protocol) settings.

The PrintServer supports SNMP, which allows network administrators to monitor and control the PrintServer through the use of network management platforms, such as HP OpenView.

The appropriate MIB file must be imported into your SNMP management program using the Import-Compile command. Check your program's documentation for details on this procedure. The MIB file is named Mib2p.mib and is provided in the MiB folder on the Setup CD-ROM.

General. Enter the name of the contact person in the *SysContact* field. Enter the location of the contact person in the *SysLocation* field.

Management Stations. Select the number of the management station from the *Station No.* drop-down menu (1-4). Click the **Get Data** button to display the information for the selected station.

In the *IP Address* fields, enter the IP address of the management station with the SNMP program installed. In the Community field, enter the name of the SNMP community, which is usually **public** or **private**. From the Access drop-down menu, select the desired level of access for this management station, **Not Accessible**, **Read-only**, or **Read/Write**.

Trap Receivers. Select the number of the trap receiver from the *Receiver No.* drop-down menu (1-4). Click the **Get Data** button to display the information for the selected trap receiver.

In the *IP Address* fields, enter the IP address of the trap receiver that will be sent the trap messages or notifications. In the *Community* field, enter the name of the SNMP community, which is usually **public** or **private**. To designate a severity level, click the checkbox next to *Enable with Severity level*. From the following drop-down menu, select the desired level of severity, with 1 meaning least severe.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

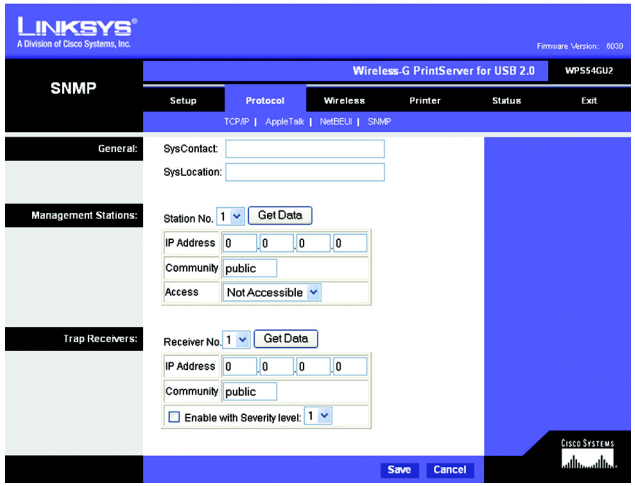

Figure 6-6: Protocol Tab - SNMP

The Wireless Tab - Basic

This screen allows you to change the PrintServer's basic wireless settings.

Configuration. The PrintServer's Regulatory Domain and MAC Address are listed and cannot be changed. In the *SSID* field, enter the name of your wireless network. This is the unique name shared by all devices in a wireless network. The SSID is case-sensitive and should have 32 characters or fewer.

If your network is set to ad-hoc mode, select your network's channel setting from the *Channel No.* drop-down menu.

The Network Type setting shows a choice of two wireless modes. Select **Infrastructure** if you want the PrintServer to communicate using an access point or wireless router. Select **Ad-Hoc** if you want the PrintServer to communicate without using an access point or wireless router.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

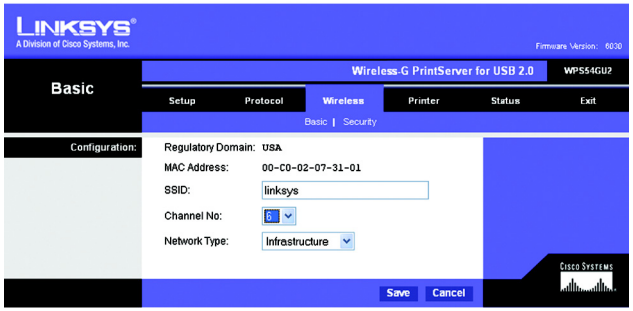

Figure 6-7: Wireless Tab - Basic

The Wireless Tab - Security

Configure or alter the PrintServer's wireless security settings on this screen.

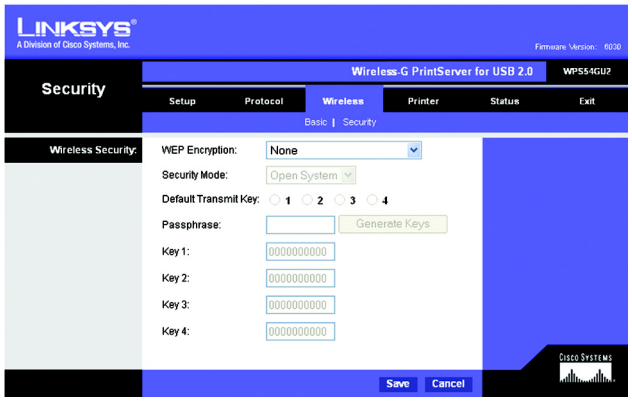

Figure 6-8: Wireless Tab - Security

Wireless Security

- **WEP Encryption**. If you want to enable WEP encryption for greater wireless security, select the level of WEP encryption, **64 Bit Keys (10 Hex chars)** or **128 Bit Keys (26 Hex chars)** from the drop-down menu. If you want to disable WEP encryption, keep the default, **None**.

- **Security Mode**. From the drop-down menu, select your wireless network's authentication type. The default is set to **Open System**, for which the sender and the recipient do NOT use a WEP key for authentication. You can also choose **Shared Key**, when the sender and recipient use a WEP key for authentication. If the PrintServer is set to the third setting, **Auto**, then the PrintServer will automatically use Open System or Shared Key authentication, depending on the authentication being used by your wireless network. The Security Mode setting should match the one on your network's access point or wireless router.

- **Default Transmit Key**. Select the Default Transmit Key used by your wireless network. This indicates which WEP key your network uses for WEP encryption.

- **Passphrase**. Enter a Passphrase in the field provided. If you use a Passphrase, WEP Keys 1-4 will be automatically generated after you click the **Generate Keys** button. The Passphrase is case-sensitive and should have 16 alphanumeric characters or fewer. It must match the passphrase of your wireless network and is compatible with Linksys wireless products only. (You will have to enter the WEP key(s) manually on any non-Linksys wireless products.)

- **Key 1 to Key 4**. If you want to enter the WEP keys manually, then leave the *Passphrase* field blank and enter the WEP keys in the fields provided. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

The Printer Tab - Internet Printing

Internet Printing allows you to automatically print any e-mails that are sent to a specific e-mail account on your network. This is especially useful for printing information when you are not connected to the network. You can print from any location where you can access e-mail. (See Figure 6-9.)

Mail Server. Enter the address of your mail server in the Mail Server IP Address. (This value must be a fixed IP address.) Enter the Account Name and Account Password next. Enter the password again in the *Verify Password* field. Then, enter the time interval for the PrintServer to check for e-mail to be printed, in hours and minutes in the *Check Mail every:* field. You may also specify an e-mail address to which mails that cannot be printed are routed; this is useful for both graphic-intensive e-mails and for troubleshooting purposes. Enter this e-mail address in the *Redirect unprintable Mail to:* field.

Printer. Enter the Printer Model in the field provided. You can find this in the Device Manager. Then choose the appropriate Printer Port from the drop-down menu:

- **Parallel 1**. This is the PrintServer's Parallel port.
- **USB 1**. This is the PrintServer's USB port.
- **Logical Printer 1-6**. The PrintServer has six logical or virtual printer ports. For example, you can have three different configurations for your parallel printer: Logical Printer 1 for landscape orientation, Logical Printer 2 for double-sided copies, and Logical Printer 3 for manual feed. Then configure the Logical Printers on the Logical Port tab, so Logical Printers 1, 2, and 3 will be mapped to the physical printer on the PrintServer's Parallel port.

Options. Place a check mark next to the options you want to enable: **Print every E-Mail**, **Print Banner Page** (enabled by default), or **Mail response when printed**.

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

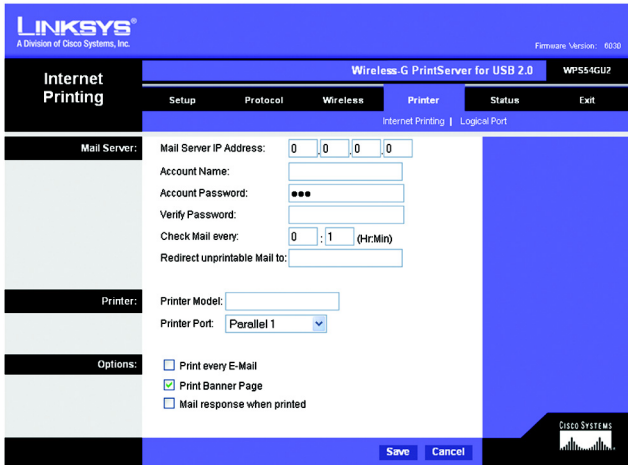

Figure 6-9: Printer - Internet Printing

The Printer Tab - Logical Port

The Logical Printers tab contains the logical printer settings of the PrintServer. Configure them for each Logical Printer. (See Figure 6-10.)

The PrintServer has six logical or virtual printer ports. For example, you can have three different configurations for your parallel printer: Logical Printer 1 for landscape orientation, Logical Printer 2 for double-sided copies, and Logical Printer 3 for manual feed. Then you will map Logical Printers 1, 2, and 3 to the physical printer on the PrintServer's Parallel port.

Select Printer. From the *Logical Printer Port No:* drop-down menu, select the number (1-6) of the printer you wish to configure. From the *Port* drop-down menu, select the PrintServer's physical port, **Parallel 1** or **USB 1**. Click the **Get Data** button to update the display with the current data for the selected logical printer.

Details

- **Pre-string (Hex)**. Enter the printer control string (in hexadecimal characters) to be sent to the printer before each print job. This string cannot exceed 30 characters.
- **Post String (Hex)**. Enter the printer control string (in hexadecimal characters) to be sent to the printer after each print job. This string cannot exceed 30 characters.
- **Convert LF to CR+LF**. If checked, LF (line feed) characters are changed to CR+LF (carriage return + line feed).

Click the **Save** button to apply your changes, or click **Cancel** to cancel your changes.

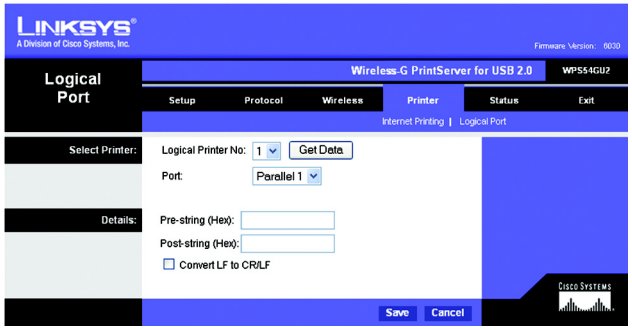

Figure 6-10: Printer - Logical Port

The Status Tab - Device

The Device tab allows you to view information about the PrintServer. No values can be changed on this screen. This screen is for information only. (See Figure 6-11.)

Clicking the **Refresh** button causes the PrintServer to retrieve this information again.

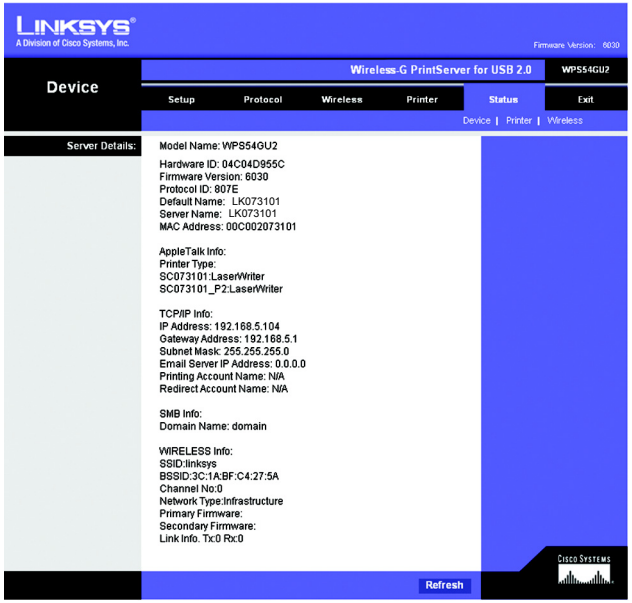

Figure 6-11: Status Tab - Device

The Status Tab - Printer

The Printer tab allows you to view information about the Printers. No values can be changed on this screen. This screen is for information only. (See Figure 6-12.)

Click the **Print Test Page** button to print a test page on the respective printer.

Clicking the **Refresh** button causes the PrintServer to retrieve the status information again.

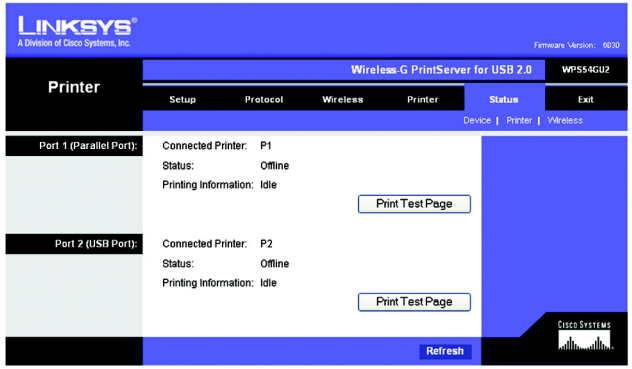

Figure 6-12: Status Tab - Printer

The Status Tab - Wireless

The Wireless tab allows you to view information about the PrintServer's wireless connection. No values can be changed on this screen. This screen is for information only. (See Figure 6-13.)

Clicking the **Refresh** button causes the PrintServer to retrieve information about the wireless connection again.

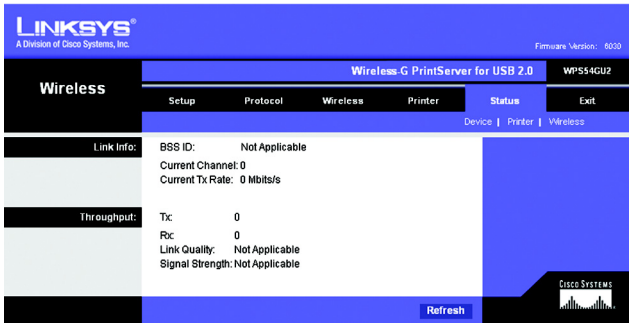

Figure 6-13: Status Tab - Wireless

The Exit Tab

This tab is used exclusively for exiting the Web-based Utility.

Select the **Exit** tab, and the screen in Figure 6-14 will appear. Click the **Yes** button if you want to exit the Utility. Click **No** if you don't want to exit the Utility.

Figure 6-14: Exit

Chapter 7: Bi-Admin Management

Overview

If you use Windows, then you can manage the PrintServer using its web-based utility (see "Chapter 6: Configuring the PrintServer Using the Web-based Utility") or a utility program called Bi-Admin, which is provided on the PrintServer's Setup CD-ROM. (If you use a Macintosh or other non-Windows operating system, you can manage the PrintServer only by using its web-based utility.)

Fully compatible with Windows 98, Me, 2000, and XP, Bi-Admin allows you to change the PrintServer's internal settings, check on the unit's status, and perform basic diagnostic tests. Note that the Bi-Admin program must be installed only on the network administrator's computer. First, you will install Bi-Admin on your computer. Then, you will be able to use the management utility.

Bi-Admin Installation

1. Make sure you have no programs or applications running on your computer.
2. If you haven't already done so, insert the Setup CD-ROM into the computer's CD-ROM drive. The Setup CD-ROM should run automatically. If it does not, click the **Start** button and choose **Run**. In the box that appears, enter **D:\setupWizard.exe** (if "D" is the letter of your CD-ROM drive).
3. When you see Figure 7-1, click **Bi-Admin Install** to continue. Click **Exit** to end the installation.
4. The *Welcome* screen of the Bi-Admin Setup program, Figure 7-2, will appear first. Click **Cancel** to quit the setup program, and then close the open programs. Click **Next** to continue with the Bi-Admin installation.

Figure 7-1: Welcome

Figure 7-2: Bi-Admin Setup Welcome

5. The *Choose Destination Location* screen will appear, as shown in Figure 7-3. Choose the location where the B-Admin folder will be installed. To install the driver in the default location, click **Next**. If you want the folder to be installed in a different location, click the **Browse** button and select the location. Then click **Next**.

   Click **Back** to return to the previous screen. Click **Cancel** to end the Bi-Admin installation.

6. The *Select Program Folder* screen, shown in Figure 7-4, will appear. An icon will be added to the program folder listed. You may change the name for the program folder, if you wish. Click **Next**.

   Click **Back** to return to the previous screen. Click **Cancel** to end the Bi-Admin installation.

7. When the Bi-Admin is installed, the *Setup Complete* screen will appear. Click **Finish**.

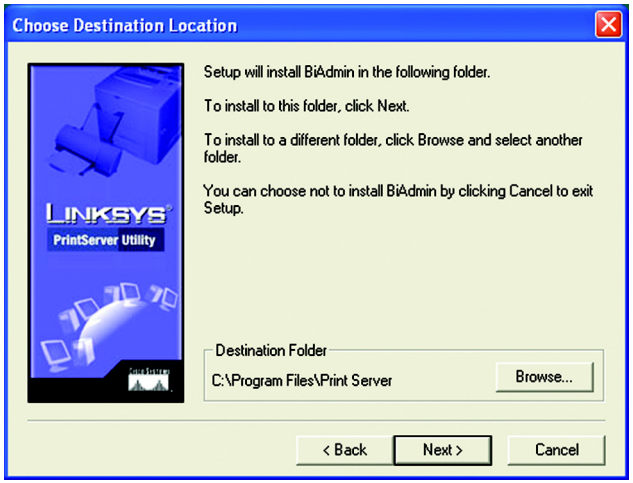

Figure 7-3: Choose Destination Location

Figure 7-4: Select Program Folder

Starting the Bi-Admin Management Utility

1. To start the Bi-Admin program, click **Start**, **Programs**, **Print Server Utility**, and then **Bi-Admin Management Utility**. If the Bi-Admin Management Utility icon has been created, you can just double-click it instead. You can drag the shortcut icon onto your Desktop for easy access to the Bi-Admin Management Utility.

2. When the Bi-Admin Management Utility appears, it will ask for the Connected Protocol. (See Figure 7-5.) Make sure the box next to *TCP/IP* is checked. Click the **OK** button.

3. The Bi-Admin Management Utility will automatically scan the network for the PrintServer. (See Figure 7-6.)

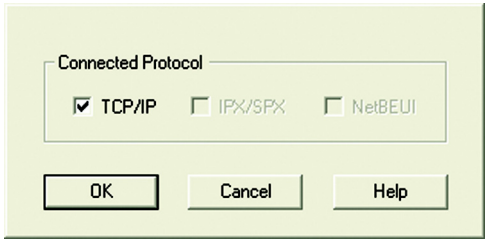

Figure 7-5: Connected Protocol

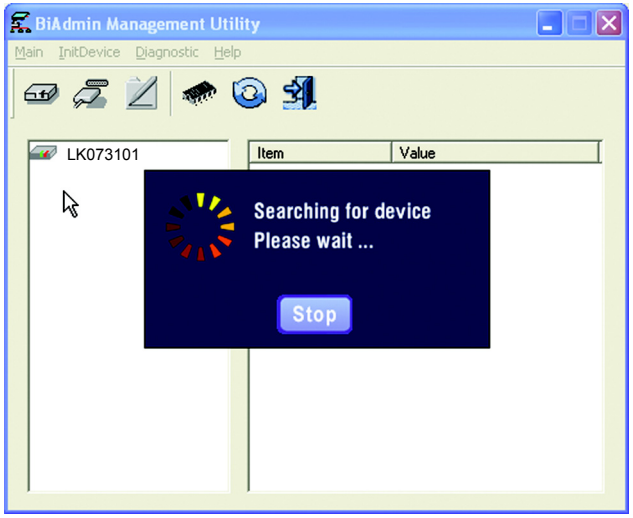

Figure 7-6: Searching for Device

The Bi-Admin Management Utility

The *Bi-Admin Management Utility* screen will appear next. Any hardware found on the network will appear on the left-hand side of the screen, as shown in Figure 7-7. The Utility can be managed from this screen. The menu and icon options will be explained in this section.

Menu Options

Main. The options are Device Status, Printer Status, Configure, Upgrade, Refresh, and Exit. These options are the same as the icons that are displayed below the menu options (viewed from left to right), and are described below:

- **Device Status**. This option allows you to view all of the device settings, optionally save the device settings to a file, or restore a previously saved file to the device.

  If you click **Device Status**, the *Device Information* screen in Figure 7-8 will appear. A list of the PrintServer's device settings is displayed, including Hardware ID, Firmware version, Protocol ID, Default Name, Server Name, and MAC Address. To save the information in a .txt (text) file, click the **Save to file** button.

  To choose a different device that you configured, click the **Open** button. You may then browse for your file, select it, and then click **Open**. The contents of the file will display on the right-hand side of the screen. To save the file to the PrintServer, click **Restore to Device**.

  Click the **Exit** button to return to the *Bi-Admin Management Utility* screen. For more information, click the **Help** button.

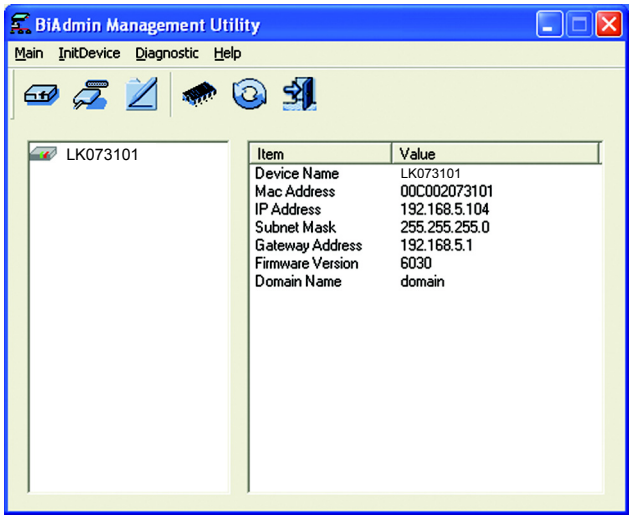

Figure 7-7: Bi-Admin Management Utility

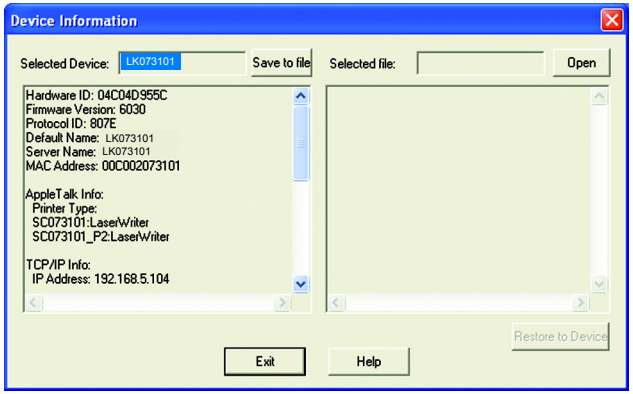

Figure 7-8: Device Information

- **Printer Status**. This option allows you to view the printer status, as well as set port and printer parameters.

  If you click this option, a *Verify Password* screen will appear. Make sure that you enter the password in the field before you click OK, or else an Incorrect Password message will appear. If the message appears, then click **OK**. Enter the correct password in the field provided, and click **OK** again.

  After the password has been successfully entered, the *Printer Status* screen will appear, as shown in Figure 8-10. The Device Name will be displayed and the Current Selected Port will be highlighted. The status information for this port will be displayed.

  Click the **Back** button to return to the *Bi-Admin Management Utility* screen. Click **Refresh** to refresh the screen. For more information, click the **Help** button.

  If the printer is bi-directional and not busy, the Printer Configuration button will appear on the *Printer Status* screen. Click this button to view the printer's Environmental Variable and Variable Value items. If the items are not read-only, you can change them based on the options of your printer.

  For more information, click the **Help** button.

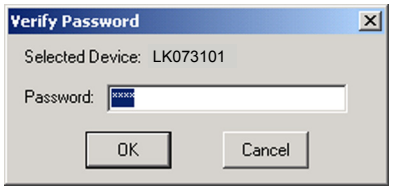

Figure 7-9: Verify Password

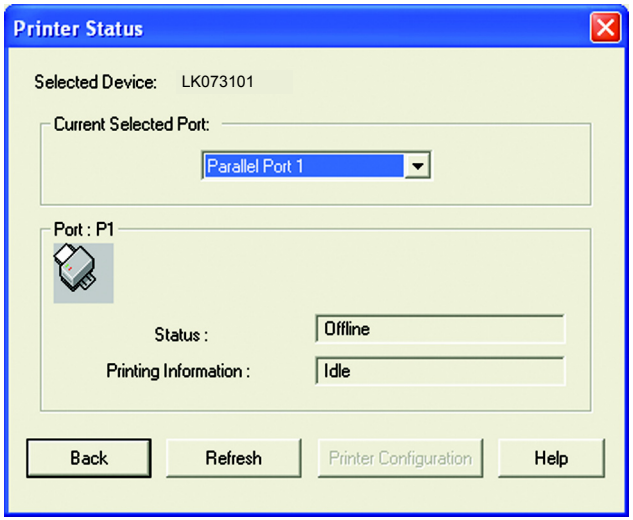

Figure 7-10: Printer Status

- **Configure**. You may configure the PrintServer with this option. If you click this option, a *Verify Password* screen will appear. Make sure that you enter the password in the field before you click OK, or else an Incorrect Password message will appear. If the message appears, click **OK**. Enter the correct password in the field provided, and click **OK** again.

  After the password has been successfully entered, the *Configuration* screen will appear, as shown in Figure 7-12. It displays eight tabs: System, TCP/IP, AppleTalk, NetBEUI, Internet Printing, Port, Wireless, and SNMP. The tabs will be described below.

  System

  - **Device Name**. Enter the Device Name in the field provided.
  - **Comment**. Enter any comments in the *Comment* field.
  - **Device Password**. To change the password, select **Change Device Password**, enter the new password in the *Password* field, and then re-enter the password in the *Confirm Password* field.
  - **Protocol**. Select the protocol you want to use for your network: TCP/IP, AppleTalk, NetBEUI, IPX/SPX.

  Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

  When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

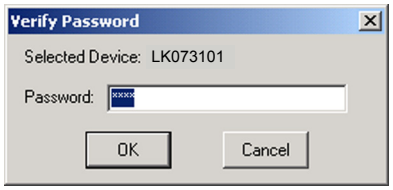

Figure 7-11: Verify Password

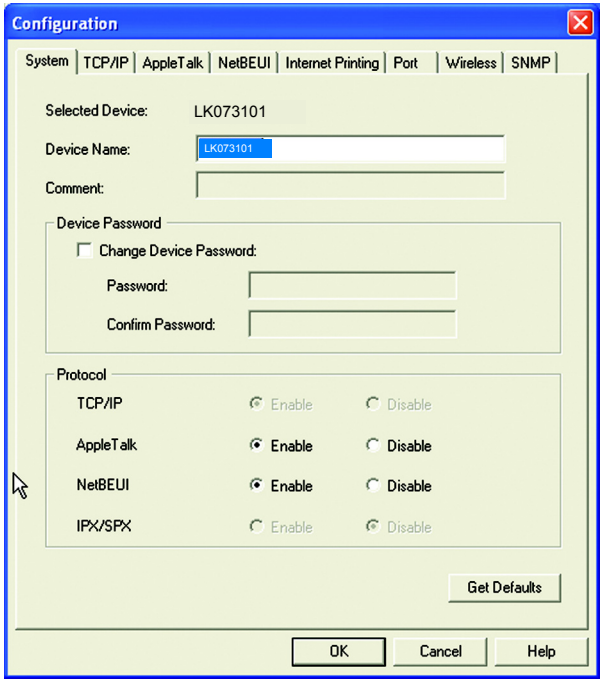

Figure 7-12: Configuration - System

TCP/IP (Figure 7-13)

- **Dynamic IP Address (DHCP)**. If your network router is using DHCP to assign IP addresses, select **Dynamic IP Address (DHCP)**. By default, **Dynamic IP Address (DHCP)** is enabled.
- **Fixed IP Address**. If you need to assign the PrintServer a fixed IP address (also known as static IP address), select **Fixed IP Address**, and enter the appropriate values under IP Address, Subnet Mask, and Gateway. Make sure the IP Address and Subnet Mask are appropriate for your network. If you change the PrintServer's IP address, make sure you that you reconnect to the PrintServer using that new IP address. Otherwise, you will not be communicating with the PrintServer. In most cases, the Gateway IP address is the IP address of your router, and you should complete the *Gateway* field if you will use the PrintServer for Internet printing. (To find out your router's IP address, consult your router's documentation.)
- **TCP session**. If your TCP session has ended, you can attempt a new connection. In the *Retry interval* field, enter how often you want the PrintServer to attempt a connection. In the *Retry count* field, enter the maximum number of attempts.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

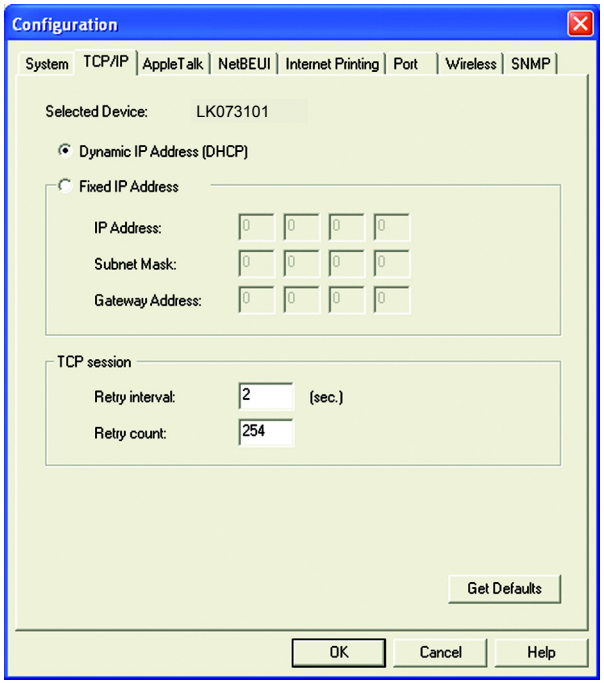

Figure 7-13: Configuration - TCP/IP

Apple Talk (Figure 7-14)

- **Zone Name**. Typically only Macintoshes use AppleTalk, although other platforms can use it if they have the necessary, third-party software installed. Enter the Zone Name in the field provided.
- **Port Setting**. Select the port number from the drop-down menu. The Printer Type can be obtained from the manufacturer of the printer. Enter the type of printer in the *Printer Type* field. For each printer connected to the PrintServer, you will choose the Communications Protocol that allows the devices on the network to communicate. Select the type of Communication Protocol you will use, **ASCII** or **Binary** for each printer, according to the recommendation of the printer's manufacturer. For more information, refer to the printer's documentation.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

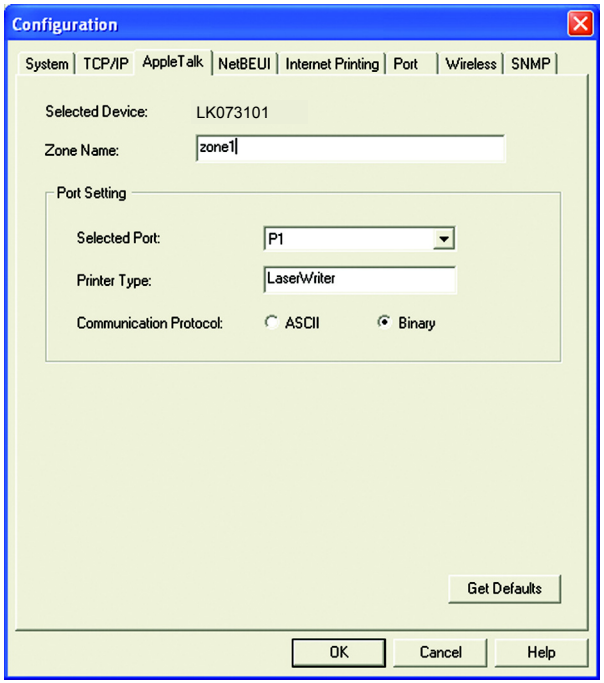

Figure 7-14: Configuration - AppleTalk

NetBEUI (Figure 7-15)

- **Domain Name**. Enter the name of the domain that you want the PrintServer associated with in the *Domain Name* field. If you are unsure of the Domain Name, you can find it out by looking on any computer already on the network. In Windows 98, right-click **Network Neighborhood** and select **Properties**. Under the Identification tab, there will be listed that computer's name, and the Domain to which it is connected. For Windows Me, 2000, or XP, right-click **My Network Places**. In Windows Me, choose **Properties** from the menu that appears. In Windows 2000 or XP, choose **Properties** from the menu that appears. Then, right-click **Local Area Connection** and choose **Properties**. The Domain name will appear. If you want the PrintServer to be connected to that same Domain, enter that Domain name here. If no Domain name exists there, you will use the Workgroup name from that window.

- **Port Setting**. You can specify the Response Time that you prefer for the PrintServer. This is the amount of time (measured in seconds) that the PrintServer will wait for a response from the network before "timing out." You also have the option to use this feature, Abort Print Job if Error. Selecting Yes here will terminate the printing if there is an error of any kind. If you select No, print jobs that have errors will be sent to the printer, but might not print properly.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

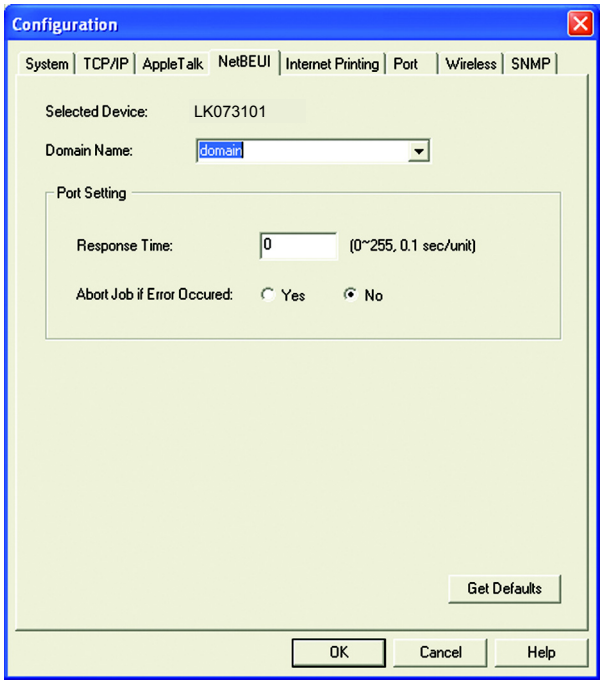

Figure 7-15: Configuration - NetBEUI

Internet Printing (Figure 7-16)

- **Mail Server**. Enter the address of your mail server in the *Mail Server IP Address* fields. (This value must be a fixed IP address.) Enter the Mail Account name and Password next. Enter the password again in the *Confirm Password* field. Then, enter the time interval for the PrintServer to check for e-mail to be printed, in hours and minutes in the *Check Mail Interval* field. You may also specify an e-mail address to which mails that cannot be printed are routed; this is useful for both graphic-intensive e-mails and for troubleshooting purposes. Enter this e-mail address in the *Redirect Mail Account* field.
- **Printer**. Select the Default Printer Port from the drop-down menu. In the field provided, enter the Printer Model, which can be found through the Device Manager.
- **Options**. Place a check mark next to the options you want to enable: **Print Every Mail**, **Banner Printing** (enabled by default), or **Mail response when Printed**.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

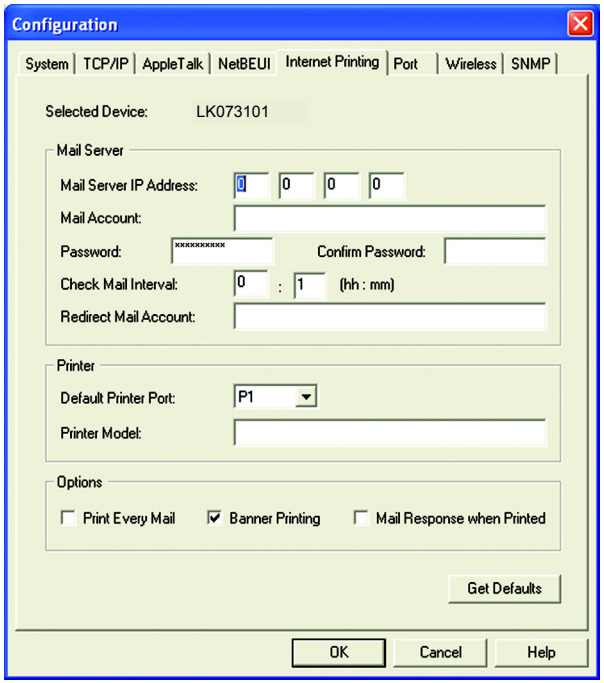

Figure 7-16: Configuration - Internet Printing

Port (Figure 7-17)

- **Physical Port**. Select the number of the Selected Physical Port from the drop-down menu. Select the Handshake Signal, **Busy Only** or **Busy & Ack**. Select the Printer Type, **High Speed** or **Low Speed**.
- **Logical Port**. Select the Selected Logical Port from the drop-down menu and then the physical port you want to map it to from the drop-down menu for *Map to Physical Port*. If you select Yes for Convert LF to LF+CR, the LF (line feed) characters are changed to LF+CR (line feed + carriage return). In the field for *Prefix of Job*, enter the printer control string (in hexadecimal characters) to be sent to the printer before each print job. This string cannot exceed 30 characters. In the field for *Suffix of Job*, enter the printer control string (in hexadecimal characters) to be sent to the printer after each print job. This string cannot exceed 30 characters.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

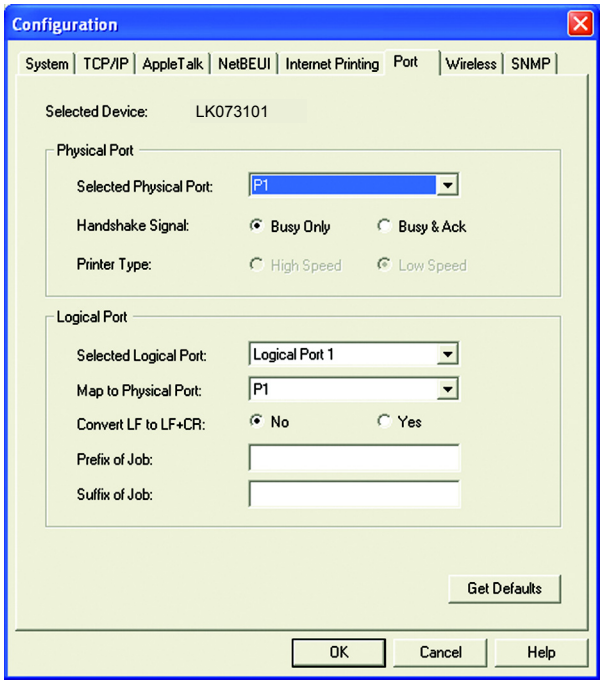

Figure 7-17: Configuration - Port

Wireless (Figure 7-18)

- **SSID (Service Set Identifier)**. In the *SSID* field, enter the name of your wireless network. This is the unique name shared by all devices in a wireless network. The SSID is case-sensitive and should have 32 characters or fewer.

- **Channel No**. If your network is set to ad-hoc mode, select your network's channel setting from the *Channel No.* drop-down menu.

- **Network Type**. The Network Type setting shows a choice of two wireless modes. Select **Infrastructure** if you want the PrintServer to communicate using an access point or wireless router. Select **Ad-Hoc** if you want the PrintServer to communicate without using an access point or wireless router.

- **WEP Encryption**. If you want to enable WEP encryption for greater wireless security, click the **Enable** radio button. If you want to disable WEP encryption, keep the default, **Disable**. From the *WEP Authentication* drop-down menu, select your wireless network's authentication type. The default is set to **Open System**, for which the sender and the recipient do NOT use a WEP key for authentication. You can also choose **Shared Key**, when the sender and recipient use a WEP key for authentication. This setting should match the one on your network's access point or wireless router.

  In the *WEP Keys* section, select the level of WEP encryption, **64 bits** or **128-bits**. From the drop-down menu, select the Default Key used by your wireless network. This indicates which WEP key your network uses for WEP encryption. In the **Key1 (hex) to Key4 (hex)** fields, enter your network's WEP keys. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

Click the **Link Info** button if you want to view information about the wireless connection.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

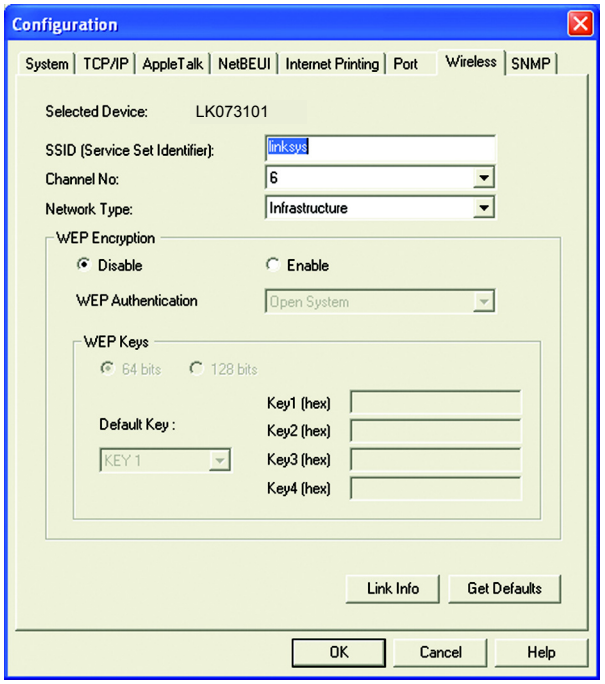

Figure 7-18: Configuration - Wireless

SNMP (Figure 7-19)

- **SysContact**. Enter the name of the contact person in the *SysContact* field.
- **SysLocation**. Enter the location of the contact person in the *SysLocation* field.
- **Configuration Item**. From the *Configuration Item* box, select the number of the management station (M1-M4) or trap receiver (T1-T4). The selected item's information will be displayed below.

  For management stations, you can change the station's IP address, Community String, and Access Permission level. In the *Manager IP Address* fields, enter the IP address of the management station with the SNMP program installed. In the *Community String* field, enter the name of the SNMP community, which is usually **public** or **private**. In the *Access Permission* section, select the desired level of access for this management station, **Read Only**, **Read/Write**, or **Not Accessible**.

  For trap receivers, you can change the trap receiver's IP address, Community String, Trap Option, and Trap Severity level. In the *Trap Receive IP Address* fields, enter the IP address of the trap receiver that will be sent the trap messages or notifications. In the *Community String* field, enter the name of the SNMP community, which is usually **public** or **private**. For the Trap Option setting, select **Enable** or **Disable**. For the Trap Severity setting, select the desired level of severity, with 1 meaning least severe.

Click the **Get Defaults** button if you want to cancel your changes and use the default settings.

When finished making your changes on this tab, click the **OK** button to save these changes, or click the **Cancel** button to undo your changes. For more information, click the **Help** button.

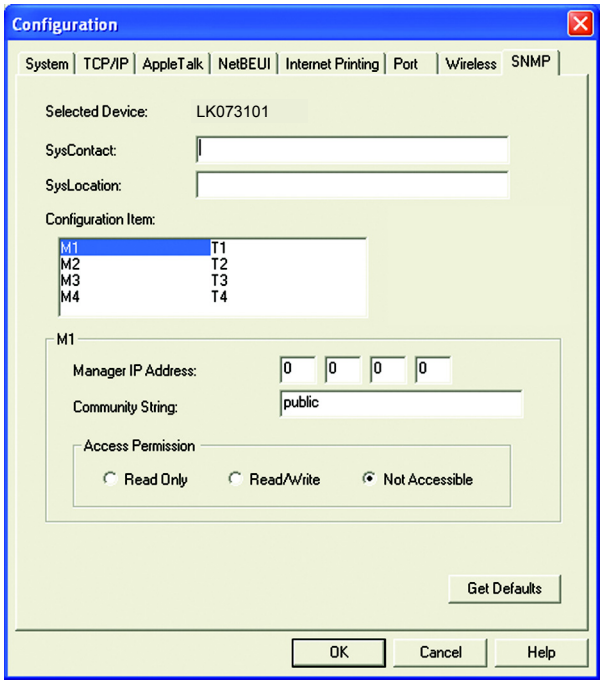

Figure 7-19: Configuration - SNMP

- **Upgrade**. You may use this option to upgrade the firmware of the PrintServer. Follow these instructions:

  1 On the *Upgrade* screen shown in Figure 7-20, click the **Files** button.

  2 The *Detected LAN Cards* screen will appear, as shown in Figure 7-21. Select the LAN card the PrintServer is connected to, and then click the **OK** button.

  3 Follow the on-screen instructions, and select the firmware file you want to use.

  4 View the *BIN File Information* screen (see Figure 7-22), and click the **OK** button if you have selected the correct firmware file. Click the **Cancel** button to select a different firmware file.

  5 On the *Upgrade* screen, click the **Upgrade** button. Click the **Cancel** button to cancel the firmware upgrade. For more information, click the **Help** button.

- **Refresh**. This option allows you to refresh the device list after you change the name or IP address of a device. The screen does not refresh automatically.

- **Exit**. This option allows you to exit the Bi-Admin program.

InitDevice. The available options are Reset Device, Restore to Factory Default, Attached Remote, and Connected Protocol.

If you click Attached Remote, the screen in Figure 7-23 appears. To add a cross segment print server, enter its IP address in the fields provided, and click the **Set** button.

Click **Cancel** to undo any changes. For more information, click the **Help** button.

Diagnostic. Diagnostic allows you to print a test page from either of the PrintServer's ports.

Help. The two options are Help Topics and About Bi-Admin. These help files offer extensive advice and details about all of the PrintServer's functions and capabilities.

Figure 7-20: Upgrade

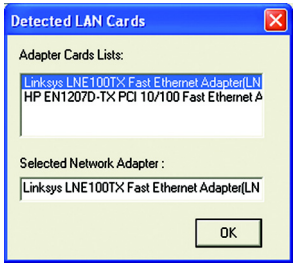

Figure 7-21: Detected LAN Cards

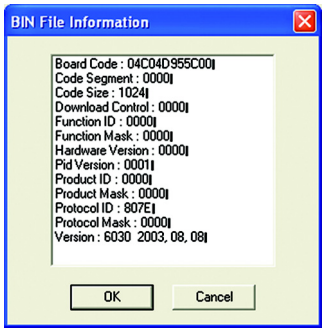

Figure 7-22: BIN File Information

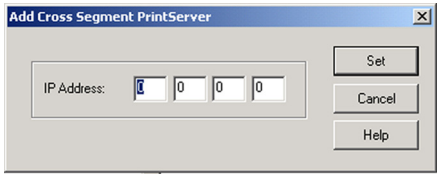

Figure 7-23: Add Cross Segment PrintServer

Chapter 8: Internet Printing Protocol (IPP)

Overview

Internet Printing Protocol (IPP) is a standards-based system that allows remote printing from a PC to any accessible printer. Normally, the printer will be attached to a computer or other device that functions as an IPP Server. For client PCs, it is necessary to install a compatible IPP Client program. The Client must also know the IP Address or URL of the IPP Server.

The PrintServer contains the necessary firmware to act as an IPP Server. No additional configuration is necessary. However, the following requirements must be met:

- The PrintServer must have a valid IP Address. For printing via the Internet, the PrintServer's IP Address must be external (allocated by your ISP), rather than an IP Address on your local LAN.
- Any Router, Gateway, or Firewall linking your LAN to the Internet must NOT block IPP. (IPP uses Port Services 631/TCP.)
- You must advise clients of the correct URL or IP Address of the IPP Server. To use a URL rather than an IP Address, you need to register the domain name for the URL.
- Unless clients are using Windows 2000, you must provide your clients with the supplied IPP Client software. If it is not convenient to provide the CD-ROM, supply the setup.exe file, located in the IPP folder.

Windows IPP Client Setup

Installing using setup.exe

1. Run this program, located at d:\driver\ipp\setup.exe, to unzip the included files.
2. The IPP Setup program will then run.
3. Follow the prompts to complete the installation.

IPP Client Configuration for Windows 98, Me, 2000, and XP

1. Run the **Add IPP Port program** entry created by the installation. A screen like the one shown in Figure 8-2 will be displayed.

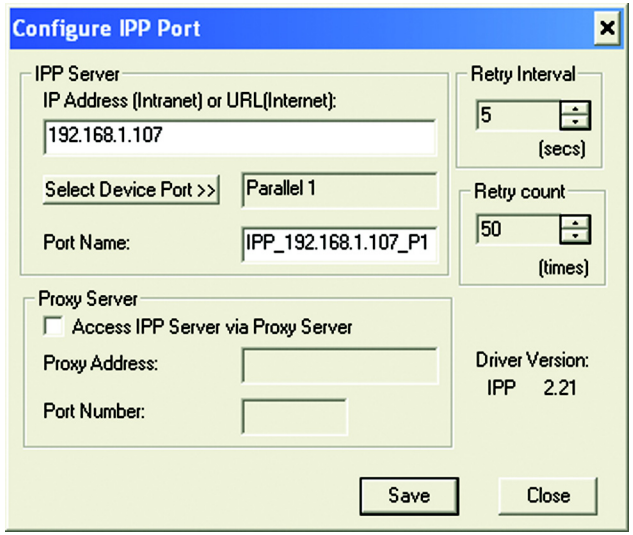

Figure 8-1: Configure IPP Port

2. Enter the IP Address or URL of the IPP Server.

3. If Internet access from your location is via a Proxy Server, check **Access IPP Server via Proxy Server**, and enter details of your Proxy Server. (This will be the same as your browser configuration.)

4. Click **Select Device Port** to view the available ports on the IPP Server, and select the appropriate port. (See Figure 8-2.) A connection to the IPP Server will be established at this time.

5. Click **OK** to create the IPP port on your system. You will see a message confirming that the port has been created, and then you will see Figure 8-3.

6. Perform one of these steps.

   Select an existing printer to use the new port, and click **OK**.
   OR
   Click the **Add New Printer** button to create a new printer that will use the IPP port. This will start the Add Printer Wizard. Follow the prompts to complete the process. Make sure that the new printer uses the IPP port.

Installation is now complete.

- To create additional IPP ports, repeat the entire procedure.
- The Proxy Server and other options are set individually for each IPP port.

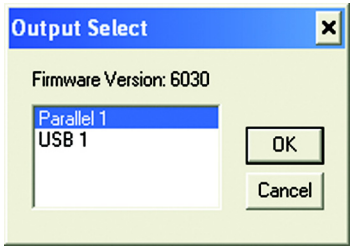

Figure 8-2: Output Select

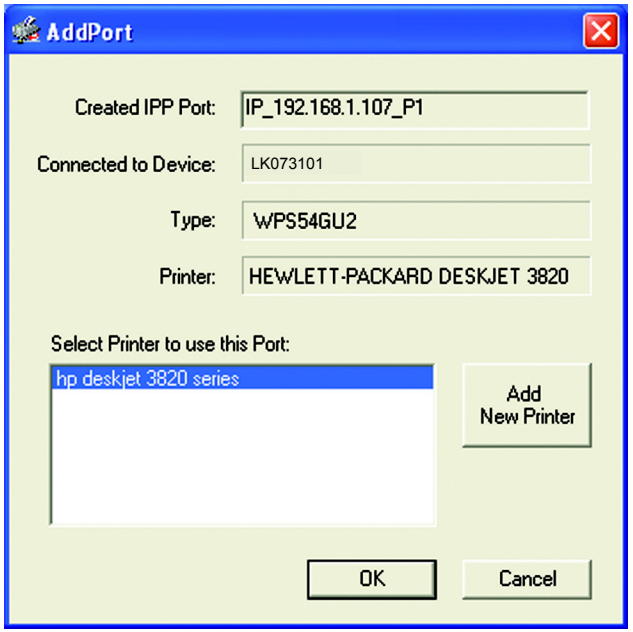

Figure 8-3: AddPort

Changing the IPP Port Settings

After the IPP port is created, you can reach the *Configure IPP Port* screen by performing these steps:

1. Open the **Printers** folder (**Start** => **Settings** => **Printers**).
2. Right-click **IPP Printer** and select **Properties**.
3. Click the **Port Settings** or **Configure Port** button (Details or Port tab, depending on your version of Windows). The *Configure IPP Port* screen (shown in Figure 8-4) will appear.

There are two settings, Retry Interval and Retry Count, which can be adjusted if you have problems connecting to the IPP Server.

- The Retry Interval sets the time interval (in seconds) between connection attempts. Increase this number if you have a poor connection, or the remote server is very busy.
- The Retry Count sets how many connection attempts will be made. Increase this number if you have a poor connection, or the remote server is very busy.

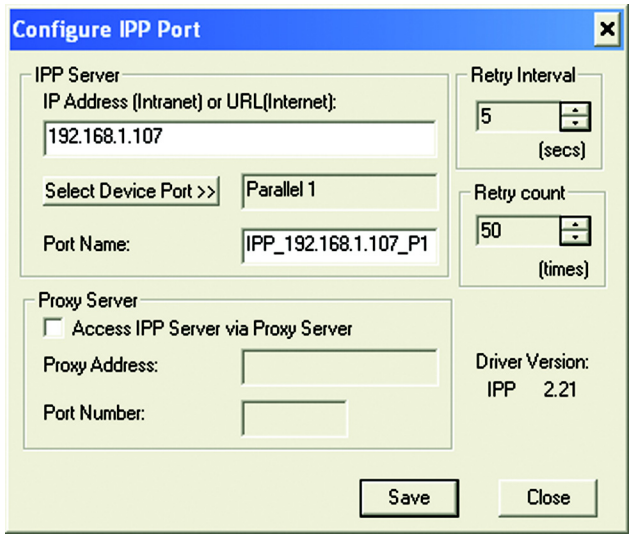

Figure 8-4: Configure IPP Port

IPP Client Setup for Windows 2000 and XP

Windows 2000 and XP have their own IPP Client, and there is no need to install the supplied IPP Client Software. To use this IPP Client with the PrintServer, follow this procedure:

1. Start the Add Printer Wizard.
2. Select **Network Printer** and click **Next** to see the *Locate your Printer* screen, as shown in Figure 8-5.
3. Select **Connect to a printer on the Internet or on your intranet**, and enter the URL of the IPP Server as follows, where ip_address represents the IP Address of the IPP Server, and 631 represents the port number.

   Port 1 ip_address:631/ipp/P1

NOTE: These entries are case-sensitive. They must be entered as shown, with “ipp” in lowercase and P1 in uppercase.

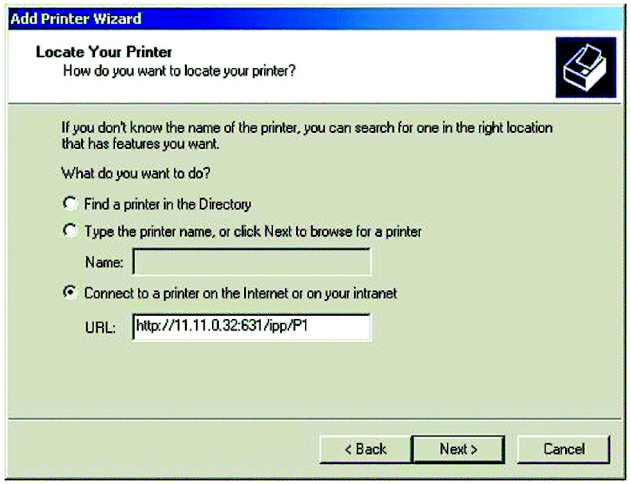

Figure 8-5: Locate Your Printer

4. If the connection can be established, and the printer on that port is online, the dialog box shown in Figure 8-6 will be displayed. This screen notifies you that the printer driver is not installed. Click the **OK** button.

5. Select the printer manufacturer and model to match the printer connected to the appropriate port on the IPP Server.

6. Click **Next** and complete the Wizard.

The IPP printer is now ready for use.

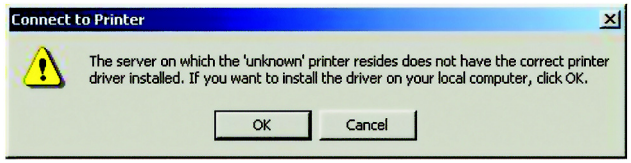

Figure 8-6: Connect to Printer

Using IPP Printers

The IPP Printer can be selected and used like any other Windows printer. If the IPP Server is not on your network, your Internet connection needs to be active.

If you wish to check the availability of the remote IPP Server, you can use the Query IPP Printer program installed with the Add IPP Port program.

An IPP Server may be unavailable for any of the following reasons:

- It is powered off.
- A printer problem has caused the IPP Server to cease responding, and a restart (reboot) is required.
- The Server's IP Address has changed.
- The Internet connection for the IPP Server is down.
- Network congestion causes the connection attempt to time out.

If using the supplied IPP Client software, there are two settings, Retry Interval and Retry Count, which can be adjusted if you have problems connecting to the IPP Server.

See the previous section, "Changing the IPP Port Settings," for details.

Appendix A: Troubleshooting

This appendix consists of "Common Problems and Solutions". Provided are possible solutions to problems that may occur during the installation and operation of the PrintServer. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

If the PrintServer is not working correctly, follow the advice in this chapter. If you have trouble printing, see Chapter 3 first, and then go to Chapter 8. If this Troubleshooting section does not resolve your problem, please see Appendix I to contact Technical Support.

1. ***All the LEDs on the front of the PrintServer are off.***
   Check the power supply and the power connection.

2. ***The PrintServer's Status LED lights up orange or flashes continuously.***
   Reset the PrintServer. Unplug the power supply and plug it back in, or press the **Reset** button on the back of the PrintServer for approximately ten seconds.

3. ***I am using DHCP, and the PrintServer gets an IP address conflict involving the PrintServer.***
   If the PrintServer is left on when the DHCP server is turned off, the PrintServer will retain its IP address without informing the DHCP server. Reset the PrintServer so it will obtain a new IP address. This problem may also occur if you assigned a static IP address within the range used by the DHCP server. If so, use another address NOT within the range used by the DHCP server.

4. ***The PrintServer's LAN LED is not lighting up.***
   Check your cabling and make sure that the Link LED on your hub or switch is lit.

5. ***A printer connected to the PrintServer cannot print or prints garbage.***
   Do the following:
   - Check the cable connection between the PrintServer and printer.
   - Make sure the printer driver in the application program or Windows matches the printer.
   - Make sure the cable distance is not too long, less than 10 feet.

6. ***The Configuration button on the Printer Status screen in Bi-Admin is grayed out, even though my printer is bi-directional.***
   The button is unavailable until the printer has finished its print jobs and sits idle.

7. To start over, I need to set the PrintServer to its factory default settings.

Unplug the PrintServer's power adapter. Press the **Reset** button while you plug in the PrintServer's power adapter. Continue to hold the **Reset** button for 10 seconds and then release it. This will reset the password, wireless, and other settings on the PrintServer to the factory defaults. In other words, the PrintServer will revert to its original factory configuration.

8. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*.

Follow these steps:

1. Go to the Linksys website at *http://www.linksys.com* and download the latest firmware.
2. To upgrade the firmware, follow the steps in "Appendix D: Upgrading Firmware."

Appendix B: Wireless Security

A Brief Overview

Whenever data—in the form of files, emails, or messages—is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

What Are The Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or access point, but not always directly to its destination. The receiving PC or access point can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for “beacon messages”. These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier) and the IP address of the network PC or access point. The SSID is analogous to the network's name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called “Warchalking”. This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won’t prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wireless Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

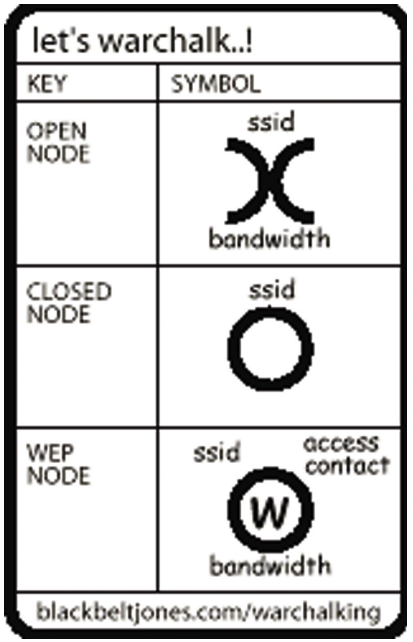

Figure B-1: Warchalking

But even WEP has its problems. WEP's encryption algorithm is referred to as "simple", which also means "weak", because the technology that scrambles the wireless signal isn't too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, emails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a "packet sniffer", software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.

Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network's access point is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP's mail server to send tens of thousands of e-mails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

Man-in-the-Middle Attacks

A hacker doesn't need to log into your network as a user—he can appear as one of the network's own access points, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an access point with your network's settings and send out a stronger signal that your access point. In this way, some of your network's PCs may associate with this rogue access point, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the

examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP, let's look at a few security measures often overlooked.

1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don't host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your access point(s) towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the access point is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

4) Administrator passwords

Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

5) SSID

There are a few things you can do to make your SSID more secure:

a. Disable Broadcast

b. Make it unique

c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

A default SSID is set on your wireless devices by the factory. (The Linksys default SSID is “linksys”.) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

6) MAC addresses

Enable MAC address filtering if your wireless products allow it. MAC address filtering will allow you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker using a random MAC address or spoofing (faking) a MAC address.

7) Firewalls

Once a hacker has broken into your wireless network, if it is connected to your wired network, they’ll have access to that, too. This means that the hacker has effectively used your wireless network as a backdoor through your firewall, which you've put in place to protect your network from just this kind of attack via the Internet.

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. Rather than connecting your access point to an unprotected switch, swap those out for a router with a built-in firewall. The router will show the access point coming in through its Internet port and its firewall will protect your network from any transmissions entering via your wireless network.

PCs unprotected by a firewall router should at least run firewall software, and all PCs should run up-to-date antiviral software.

8) WEP

Wired Equivalent Privacy (WEP) is often looked upon as a panacea for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

a) Use the highest level of encryption possible

b) Use multiple WEP keys

c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a "dynamic" WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

WEP Encryption

There are two ways to enable WEP encryption for the PrintServer. The first way is through the Setup Wizard, and the second way is through the web-based utility. To use the Setup Wizard, refer to "Chapter 4: Configuring the PrintServer Using the Setup Wizard." To use the web-based utility, follow these instructions:

1. Click the **Wireless** tab of the web-based utility.
2. Click the **Security tab**. See Figure B-2.
3. From the *WEP Encryption* drop-down menu, select **64 Bit Keys (10 Hex chars)** or **128 Bit Keys (26 Hex chars)**, depending on the level of encryption your wireless network uses.
4. From the *Security Mode* drop-down menu, select your wireless network's authentication type, **Open System**, **Shared Key**, or **Auto**. If you are not sure which type to choose, select **Auto**, which will enable the PrintServer to automatically use Open System or Shared Key authentication, depending on the authentication being used by your wireless network.
5. Select the Default Transmit Key used by your wireless network.
6. Enter a Passphrase in the *Passphrase* field, and click the **Generate Keys** button. The Passphrase is case-sensitive and should have 16 alphanumeric characters or fewer.
7. If you do not want to use a Passphrase, then enter the WEP keys manually in the *Key 1* to *Key 4* fields. Each WEP key must consist of valid hexadecimal characters, the letters "A" through "F" and numbers "0" through "9". For 64-bit WEP encryption, the key must consist of exactly 10 hexadecimal characters. For 128-bit WEP encryption, the key must consist of exactly 26 hexadecimal characters.
8. Click the **Save** button to apply your changes.

Important: Always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key or your wireless network will not function properly.

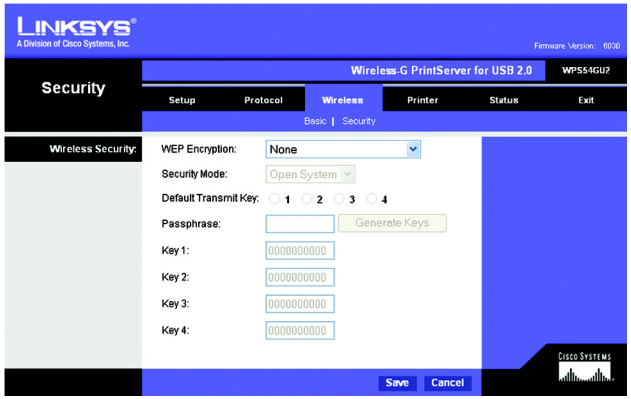

Figure B-2: Wireless Tab - Security

Appendix C: About Bi-Directional Printing

Normal printing only sends print signals from a PC to a printer. Bi-directional printing, also called bitronic printing, refers to a printer's ability to do just the opposite—talk back to a PC to notify it of a print job status, paper jams, etc. This two-way communication technology can be found in HP, IBM, Panasonic, and other laser or color printers where close contact between the PC and printer is key. In color printing, for example, the printer "informs" the PC of its constant status in order to mix color inks correctly for optimal quality output.

Bi-directional communication, communication from a printer to a PC, is normally handled by a combination of the printer hardware and special software on your computer. Bi-directional printers generally have highly advanced parallel interfaces. These printers often require special parallel ports in order to take full advantage of their features.

Using a bi-directional printer on a network poses unique challenges. Unlike a direct PC-to-printer connection during which a bi-directional printer can easily send its signals back to the host PC through the computer's parallel port (which is normally located only a few feet away from the printer), a networked printer faces the problem of having to route messages bound for a particular PC through a large array of hubs, switches, file servers, and computers. Unfortunately, most printers are not equipped to handle the complexities of printer-to-PC communication across a network. That does not mean that they can't be used on a network, however.

Linksys designed the PrintServers to function with both regular as well as bi-directional printers. Standard print servers cannot work with bi-directional printers, but the PrintServer features a custom design to support both parallel as well as bi-directional parallel interfaces. However, the PrintServer cannot pass messages from the printer back to the printing PC—this limitation is simply an industry standard, and not one of the PrintServer itself.

However, the PrintServer can check any printer's online and printing status on the network using the Bi-Admin management utility software packaged with the PrintServer. The status-checking feature built into the management software does not require a bi-directional printer to function. If your printer came with special bi-directional software allowing you to monitor printer status, do not use it with the PrintServer—the software is most likely not network-capable. For best results, turn off the printer's bi-directional function either by (1) removing any bi-directional printing software from your network computers, and/or (2) turning off the printer's bi-directional print feature inside of the printer's on-board menus (if it has menus). Your printer's user guide should be able to provide specific instructions for doing this.

Appendix D: Upgrading Firmware

The PrintServer's firmware is upgraded through the Bi-Admin Management utility. Follow these instructions:

1. Download the firmware from Linksys's website at *www.linksys.com*.
2. Open the Bi-Admin Management utility.
3. Click **Main** => **Upgrade Firmware**.
4. Click the **Files...** button to browse for the file.
5. The *Detected LAN Cards* screen will appear, as shown in Figure D-2. Select the LAN card the PrintServer is connected to, and then click the **OK** button. Select the firmware file you want to use.
6. View the *BIN File Information* screen, and click the **OK** button if you have selected the correct firmware file. Click the **Cancel** button to select a different firmware file.
7. On the *Upgrade* screen, click the **Upgrade** button. Click the **Cancel** button to cancel the firmware upgrade. For more information, click the **Help** button.

Figure D-1: Upgrade Firmware

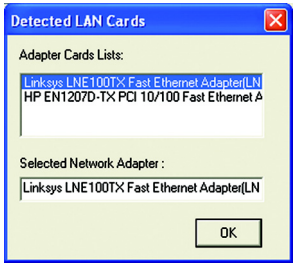

Figure D-2: Detected LAN Cards

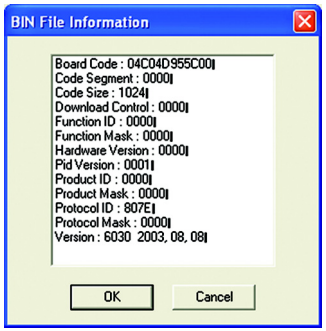

Figure D-3: BIN File Information

Appendix E: Windows Help

All Linksys wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix F: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (Megabits Per Second) - One million bits per second; a unit of measurement for data transmission.

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that uses UDP and has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix G: Specifications

Model	WPS54GU2
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 1284, USB 2.0
Ports	Power, USB, Parallel, LAN
Button	Reset
Cabling Type	USB 2.0, UTP CAT5, DB25 Parallel
LEDs	Status, LAN, WLAN, Parallel, USB
Security Features	WEP
WEP Key Bits	64, 128
Dimensions (W x H x D)	4.13" x 5.31" x 1.18" (105 mm x 135 mm x 30 mm)
Unit Weight	7.05 oz. (0.2 kg)
Power	12V, 1A
Certifications	FCC
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Appendix H: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser ("You") that, for a period of three years, (the "Warranty Period") Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's entire liability under this warranty will be for Linksys at its option to repair or replace the product or refund Your purchase price less any rebates.

If the product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT.

The foregoing limitations will apply even if any warranty or remedy provided under this Section fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623 USA.

Appendix I: Regulatory Information

FCC STATEMENT

This product has been tested and complies with the specifications 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 according to 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 is found 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 or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any change or modification to the product not expressly approved by Linksys could void the user's authority to operate the device.

FCC RF Radiation Exposure Statement

To comply with the FCC and ANSI C95.1 RF exposure limits, the antenna(s) for this device must comply with the following:

- Access points with 2.4 GHz or 5 GHz integrated antenna must operate with a separation distance of at least 20 cm from all persons using the cable provided and must not be co-located or operating in conjunction with any other antenna or transmitter.

End-users must be provided with specific operations for satisfying RF exposure compliance.

Note: Dual antennas used for diversity operation are not considered co-located.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-G PrintServer for USB 2.0 conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

For 2.4 GHz devices with 100 mW radios, the following standards were applied:

- EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.
- EN 609 50 Safety
- ETS 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

- Linksys vakuuttaa täten että Wireless-G PrintServer for USB 2.0 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
- Linksys déclare que la Wireless-G PrintServer for USB 2.0 est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.
- Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

- France F:

  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le department. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

  2.4 GHz Band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used freely in France for indoor use. License required for outdoor installations.

  Please contact ART (http://www.art-telecom.fr) for procedure to follow.

Chapter J: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at: Or fax your request in to:	800-546-5797 (LINKSYS) 949-261-8868
If you experience problems with any Linksys product, you can call us at: Don't wish to call? You can e-mail us at:	800-326-7114 support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-261-1288