

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

ROKU, INC.,

Petitioner,

v.

FLEXIWORLD TECHNOLOGIES, INC.,

Patent Owner.

---

PTAB Case No. PGR2021-00111

Patent No. 10,846,031

---

**DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.  
IN SUPPORT OF PETITION FOR POST-GRANT REVIEW OF  
U.S. PATENT NO. 10,846,031**

## LIST OF APPENDICES

Appendix A	Curriculum Vitae
Appendix B	Excerpts from Jim Geier, <i>Wireless LANs: Implementing Interoperable Networks</i> (MacMillan, 1999)
Appendix C	John Markoff, <i>New Economy: Airborne and grass roots. By popular acclaim, a wireless format with a name only a geek could love is taking hold.</i> (New York Times, Sec. C, p. 5, October 30, 2000)
Appendix D	Jaap C. Haartsen, <i>The Bluetooth Radio System</i> (IEEE Personal Communications, February 2000)
Appendix E	Golden G. Richard III, <i>Service Advertisement and Discovery: Enabling Universal Device Cooperation</i> (IEEE Internet Computing, September / October 2000)
Appendix F	Excerpt from Tom Sheldon, <i>McGraw Hill Encyclopedia of Networking &amp; Telecommunications</i> (Osborne / McGraw Hill, 2001) at pp. 1131-33 ("Service Advertising and Discovery").
Appendix G	Charlie Russel and Sharon Crawford, <i>Running Microsoft Windows NT Server 4.0</i> (1997)
Appendix H	Excerpts from Alan Neibauer, <i>This Wired Home: The Microsoft Guide to Home Networking</i> (2000)
Appendix I	Steve Rigney, <i>Print Servers</i> (PC Magazine, January 19, 1999)
Appendix J	Excerpts from Sue Plumley, <i>Home Networking Bible</i> (IDG Books, 1999)
Appendix K	Excerpts from Aeleen Frisch, <i>Essential Windows NT System Administration</i> (1998)
Appendix L	Apple Computer, <i>AirPort: Wireless Networking, A Technical Overview</i> (May 2000)

Appendix M	Excerpts from Eric A. Hall, <i>Internet Core Protocols: The Definitive Guide</i> (2000)
Appendix N	Hewlett-Packard, <i>Jornada: PC Companion Products</i> (1999)
Appendix O	Proxim, Inc., <i>RangeLAN2 7410 CE PC Card</i> (1999)
Appendix P	Excerpts from <i>Bluetooth Core Specification v1.0 B</i> (December 1, 1999)
Appendix Q	Yaron Goland et al., IETF Draft: Simple Service Discovery Protocol/1.0 (Oct. 28, 1999)
Appendix R	Excerpt from E. Guttman et al., RFC 2608: <i>Service Location Protocol, Version 2</i> (June 1999)
Appendix S	Excerpts from Ron Person, <i>Using Windows 95: Special Edition</i> (1995)
Appendix T	Excerpts from David Pogue, <i>Mac OS 9: The Missing Manual</i> (2000)
Appendix U	Universal Plug and Play Device Architecture v1.0 (June 8, 2000) (archived copy accessible at: <a href="https://web.archive.org/web/20000816073450/http://upnp.org/U_PnPDevice_Architecture_1.0.htm">https://web.archive.org/web/20000816073450/http://upnp.org/U_PnPDevice_Architecture_1.0.htm</a> )
Appendix V	Erik Guttman, <i>Service Location Protocol: Automatic Discovery of IP Network Services</i> (IEEE Internet Computing, July / August 1999)
Appendix W	Excerpt from J. Veizades et al., RFC 2165: <i>Service Location Protocol</i> (June 1997)
Appendix X	Excerpts from <i>HP Jornada 600 Series Handheld PC, User's Guide</i> (1999)

I.	INTRODUCTION AND SUMMARY OF TESTIMONY .....	1
II.	OVERVIEW OF THE TECHNOLOGY.....	5
	1. Wireless Communications .....	5
	4. Network Printing via Wired and Wireless Networks .....	9
B.	Overview of the '031 Patent.....	12
C.	The '031 Patent's Priority Applications Do Not Describe Using an Internet Appliance as an Output Device or Output System. ....	19
D.	Claim Construction .....	25
III.	UNPATENTABILITY OF THE CHALLENGED PATENT CLAIMS.....	25
A.	Legal Standards for Invalidity Subject Matter Eligibility Under 35 U.S.C. § 101 .....	25
B.	The Conventionality of the '031 Patent Claims.....	26
	1. Claim 1 .....	27
	a. The preamble .....	27
	b. The claimed “mobile information apparatus” .....	27
	c. The claimed “output system” .....	31
	d. The five functions .....	35
	(i) Function 1: discover the output system.....	36
	(ii) Functions 2 & 3: display the output system for user selection .....	42
	(iii) Function 4: send security or authentication information .....	46
	(iv) Function 5: establish a wireless communication link.....	49
	e. The final “wherein ...” clause .....	51
	f. The elements of claim 1 as an ordered combination .....	52
	2. Independent Claims 8, 14, 21, 28, and 34.....	53
	a. Claims 8 and 28 .....	53
	b. Claims 14, 21, and 34 .....	58
	3. Dependent Claims .....	65



a.	Claims 2, 3, 10, 15, 16, 22, 29, and 35 .....	65
b.	Claim 4.....	65
c.	Claim 5.....	66
d.	Claim 6.....	67
e.	Claim 7.....	70
f.	Claim 9.....	70
g.	Claim 11.....	72
h.	Claim 12, 20, and 23 .....	72
i.	Claims 13 and 31 .....	74
j.	Claim 17.....	75
k.	Claims 18, 24, and 36 .....	75
l.	Claim 19.....	76
m.	Claims 25 and 37 .....	78
n.	Claim 26.....	80
o.	Claims 27 and 38 .....	80
p.	Claim 30.....	81
q.	Claim 32.....	82
r.	Claim 33.....	83
s.	Claim 39.....	84
IV.	CONCLUSION.....	87

## **I. INTRODUCTION AND SUMMARY OF TESTIMONY**

1. I, Samrat Bhattacharjee, have been retained by Petitioner Roku, Inc. (“Roku”) to investigate and opine on certain issues relating to United States Patent No. 10,846,031 (“the ’031 patent”) in Roku’s Petition for Post Grant Review of that patent. The Petition requests that the Patent Trial and Appeal Board (“PTAB” or “Board”) review and cancel claims 1-39 of the ’031 patent.

2. I am being compensated for my work on this matter by Roku for consulting services including time spent testifying at any hearing that may be held. I am also reimbursed for reasonable and customary expenses associated with my work in this case. I receive no other forms of compensation related to this case. My compensation does not depend on the outcome of this post-grant review or the co-pending district court litigation, and I have no other financial interest in this post grant review.

3. This declaration is based on the information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, which may include a review of documents and information that may be produced, as well as testimony from depositions that have not yet been taken.

4. I understand that the ’031 patent has been assigned to Flexiworld Technologies, Inc. (“Flexiworld” or “Patent Owner”).

**A. Qualifications**

5. My qualifications for forming the opinions in this expert report are summarized here and more fully detailed in my CV attached hereto as Appendix A.

6. I received Bachelor of Science degrees in both Computer Science and in Mathematics from Georgia College in 1994, and a Ph.D. in Computer Science in 1999 from Georgia Tech. My Ph.D. research was in developing a new form of networking architecture, and part of the work I did focused heavily on better delivery of video over the Internet. After receiving my Ph.D., I joined the University of Maryland as an Assistant Professor in 1999. In 2005, I was promoted to Associate Professor with tenure, and to Full Professor in 2009. At Maryland, I have taught both undergraduate and graduate courses in Computer Networking, Operating Systems, Computer Security, and various special topics courses on topics in related fields. My courses cover the basic structure of Computer systems and networking, and some cover media content delivery over the Internet in detail.

7. Both as a graduate student and as a faculty member, I have published in the top venues in Computer Networking, Computer Systems, and in Security. The list of my publications is attached as part of my CV in Appendix A. My research work has been supported by multiple grants from the US National Science

Foundation, and the Department of Defense. I have also started a Joint Ph.D. program with the University of Maryland and the Max Planck Society in Germany, and co-founded the annual Cornell, Maryland, Max Planck Research School that provides research exposure to about 80 students from across the world during a week-long school.

8. As I mentioned earlier, part of my Ph.D. research was to develop new architectures for video delivery on the Internet, and I have published papers on this architecture during my graduate studies. I continued to work on video delivery as a faculty member, and have published various papers on video streaming, content delivery architectures, and on resilient large-scale content delivery. During 2007, I was a visiting researcher at AT&T Labs, and one of the projects I focused on was a video content delivery platform. This work resulted in both publications and a granted US patent (U.S. Pat. No. 8,752,100 B2).

**B. Materials Considered**

9. Among the materials I reviewed in forming my opinions are the '031 patent, the prosecution history of the '031 patent, Exhibit 8 to Flexiworld's complaint which sets forth infringement allegations for the '031 patent, and the Exhibits and Appendices referenced in this declaration. I have also relied on my own professional and academic experience and my experience with working with others involved in the industry.

### **C. Level of Ordinary Skill in the Art**

10. It is my opinion that a person of ordinary skill in the art (“POSA”) at the time of the invention would have had (1) a bachelor’s degree in computer science or computer engineering or a similar field, and (2) two years of experience developing software. The POSA would be familiar with well-known networking technologies. This description is approximate, in the sense that additional experience could make up for less education and vice versa.

11. I understand Flexiworld has not yet identified an alleged priority date for any claims of the ’031 patent in the district court litigation. I have not been asked to analyze whether the claims of the ’031 patent are supported by any of the priority applications. In my view, the level of ordinary skill in the art would be similar regardless of whether the claims are entitled to a priority date as early as November 1, 2000 based on the earliest filed provisional application or if the claims are only entitled to a priority date of May 12, 2017 based on the filing of the ’031 patent’s actual application. Of course, a POSA in 2017 would have additional knowledge of newer technologies (*e.g.*, the iPhone), but none of the claims require technologies that would not have been known to a POSA on November 1, 2000.

### **D. Summary of Opinions**

12. Throughout my analysis and in forming all the opinions stated in this declaration, I have considered the perspective of a person of ordinary skill in the art

as of November 1, 2000, which is the date of the earliest-filed priority application.

13. It is my opinion that claims 1-39 recite technology that was routine and conventional by November 1, 2000.

14. It is my opinion that the applications the '031 patent cites for priority fail to describe using an Internet appliance as an output device or output system.

## **II. OVERVIEW OF THE TECHNOLOGY**

### **A. Relevant State of the Art**

#### **1. Wireless Communications**

15. Although wireless networking technology had existed for years, standardization efforts in the late 1990s spurred increased interest in and use of wireless. The first major international wireless local area network (LAN) standard was IEEE 802.11. *See* Appx. B (Geier, 1999) at 89-96 (introducing the 802.11 standard). The initial 802.11 standard was finalized in 1997 and supplements in 1999 covered extensions (802.11a and b) that provided for increased data rates. IEEE 802.11 quickly came to dominate the wireless LAN space and replace earlier proprietary wireless technologies. By the time of the alleged invention (no earlier than November 1, 2000), IEEE 802.11 was essentially synonymous with wireless LAN technology. A New York Times article from October 30, 2000 describes surging enthusiasm around IEEE 802.11 wireless LAN technology. Appx. C (Markoff); *see id.* at 1 (“There is no doubt, however, that ‘wireless Ethernet’--

formally known as the 802.11b wireless technical standard as specified by the Institute of Electrical and Electronics Engineers -- is finally taking off.”).

16. Another important wireless standard, Bluetooth, was adopted in 1999. Bluetooth was developed to support low power radio connections between electronic devices, including computers and peripherals. *See generally* Appx. D (Haartsen, *The Bluetooth Radio System*, Feb. 2000).

## **2. Service Discovery Technologies**

17. In the late 1990s portable and handheld computing devices were becoming increasingly popular and it was generally understood that the utility of these devices could be enhanced by enabling them to discover and interact with other computing devices. To that end, a number of “service discovery technologies were developed ... to simplify the use of mobile devices in a network by allowing them to be ‘discovered,’ configured and used by other devices with a minimum of manual effort.” Appx. E (Richard, *Service Advertisement and Discovery: Enabling Universal Device Cooperation*, 2000) at 18; *see also* Appx. F (Networking Encyclopedia, 2001) at 1131-33 (“Service Advertising and Discovery”).

18. Universal Plug and Play (UPnP) is a technology platform developed by the UPnP Forum led by Microsoft. UPnP includes Simple Service Discovery Protocol (SSDP) “for service discovery and advertisement.” Appx. E (Richard) at

23; *id.* at 24 (“In SSDP, each service has three associated IDs—service type, service name, and location—which are multicast when services are advertised.”). Apart from service discovery, UPnP includes a range of complementary technologies that facilitate interoperability between networked devices. *Id.* at 24 (discussing description, control, and presentation functionality).

19. In addition to UPnP, there were several other technologies that provided similar service discovery functionality. The Richard article discusses Jini, Salutation, and SLP, for example. Appx. E at 20-25. Bluetooth included a service discovery protocol (SDP) that “provides a simple API for enumerating the devices in range and browsing available services.” *Id.* at 19; *see also* Appx. F (Networking Encyclopedia, 2001) at 1131-33 (discussing Salutation, SLP, Microsoft.NET, SSDP, Bluetooth, Jini, JetSend, and Inferno).

### **3. Print Servers**

20. The '031 patent states that an output controller for a printer can be a print server. '031 patent at 20:20-22 (“Other possible implementations of output controller 230 may include, for example, a ... print server.”); *see also id.* at 18:20-21; 19:60-64; 24:2-4. Because many printers did not include built-in network-interface cards (“NICs”), print servers could be used to connect printers lacking such cards to networks.

There are two basic methods for connecting your printers directly to the network. You can use a high-end printer



that comes with a network card that is either built in or available as an option. Or you can use a stand-alone network print server—the Hewlett-Packard JetDirect EX is a good example—that supports a variety of protocols and usually comes with drivers to support many network operating systems, including Windows NT server.

Appx. G (Russel, *Running Windows NT Server 4.0*, 1997) at 220; *see also, e.g.*, Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 130 (“If the printer doesn’t have a built-in network port, you’ll have to install and configure the internal or external network adapter, or print server, that was described earlier in this chapter.”).

21. Some print servers were embodied as cards that were physically installed in the printer. *Id.* (“Installing an internal print server usually means inserting an adapter card into the printer’s expansion slot.”); Appx. H (Neibauer, *This Wired Home*, 2000) at 245 (“For some HP LaserJet printers, you can purchase an internal print server that fits inside the printer, much the way some NICs fit inside a computer.”). External print servers, on the other hand, connected to the printer by cable (e.g., parallel or USB cable). *Id.* at 247-249 (discussing setup of external print server). Appx. I is a PC Magazine feature from January 1999 comparing various external print servers including products from Axis, D-Link, HP, Intel, Lexmark and Linksys.

22. Server computers were also used as print servers. Appx. J (Plumley, *Home Networking Bible*, 1999) at 283 (“A print server can be the software

included within a network operating system to control prints, printer drivers, and the print queue. NT server, for example, includes a print server applet that enables you to control the printers attached to the server.”); Appx. K (Frisch, *Essential Windows NT System Administration*, 1998) at 260-266 (describing adding a shared printer connected to parallel port of server running Windows NT).

23. Even conventional PCs could share their locally connected printers to other computers on their networks. *See, e.g.*, Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 113-145 (Chapter 6, describing setting up and sharing printers over networks). In these configurations, the host computer that shares the printer is analogous to a print server.

When you share the local printer connected to your computer, your computer provides the network connection to other computers. Other network computers that want to print to your shared local printer must contact your computer over the network and send your computer the pages to be printed. Your computer has to do a bit of processing before it tells its printer to print the pages. This means your computer must be up and running if anyone wants to use your shared local printer, and it also means that processing some of those printing jobs could cause some minor delays on your machine if you’re simultaneously working on your computer as another user is printing.

*Id.* at 115.

#### **4. Network Printing via Wired and Wireless Networks**

24. Network printing is not significantly impacted by the use of wireless

technologies. An Apple document from 2000 describing the use of its “AirPort” wireless platform in connection with network printing makes this point unambiguously:

### Printing

When an AirPort Base Station is plugged into an Ethernet network, users can print to the same printers they would if their computers were connected to the network with an Ethernet cable. Users see no difference when printing to these printers whether they’re using AirPort or are connected to the Ethernet.

Appx. L (*AirPort Technical Overview*, May 2000) at 23.

25. Network printing is largely implemented at upper layers of the networking stack. For example, the figure below illustrates the use of TCP (a Layer 4 / Transport Layer protocol in the OSI model) to print a document over a network.

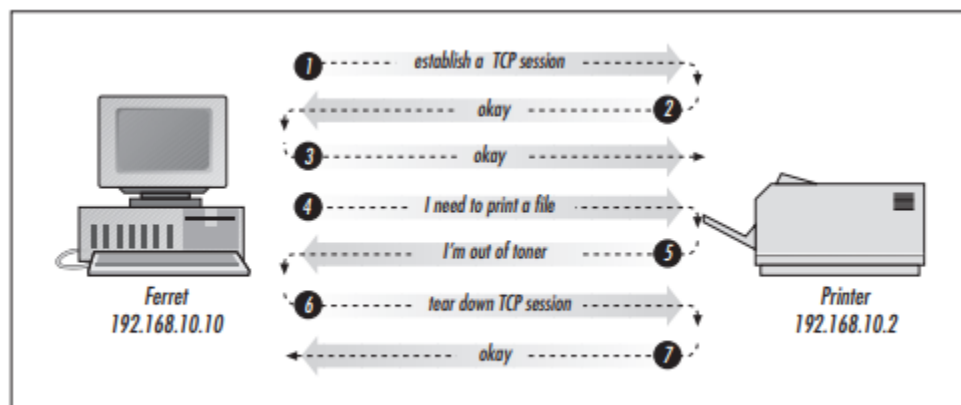
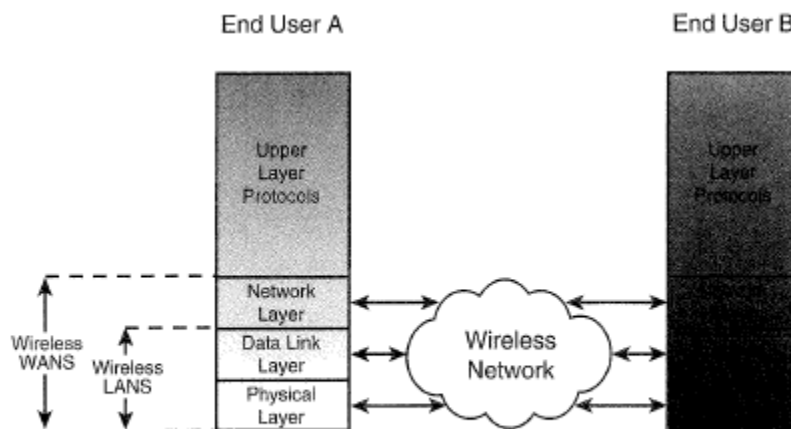


Figure 1-11. Using TCP for transaction-oriented applications

See, e.g., Appx. M (Hall, *Core Internet Protocols*, 2000) at 22; *id.* at 21 (“When the user wants to print, the client software on the end user’s PC establishes a TCP session with the printer, sends the data to the printer’s software, and then closes the

connection once the job was submitted.”).

26. Wireless networking is largely confined with lower layers of the networking stack, *i.e.*, the physical layer, data link layer, and sometimes the data link layer.



**FIGURE 1.11** *Wireless LANs and MANs fulfill Data Link and Physical Layer functionality; whereas, wireless WANs also include functions at the Network Layer.*

Appx. B (Geier, Wireless LANs, 1999) at 39 (“As shown in Figure 1.11, wireless networks operate only within the bottom three layers [of the seven-layer OSI networking model].”). Transport layer protocols such as TCP “shield[] the higher layers from the networking implementation details.” *Id.* at 38.

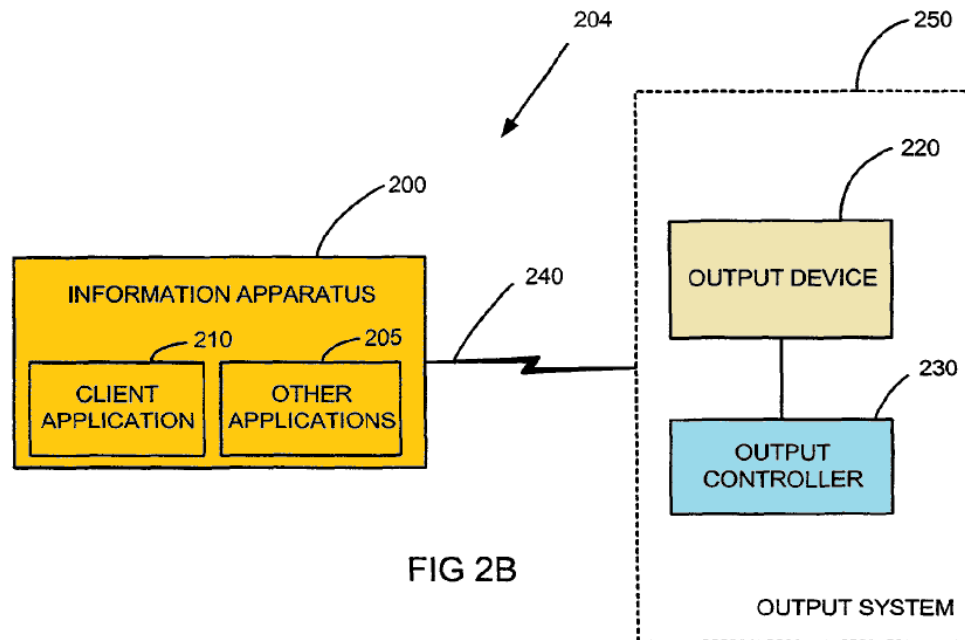
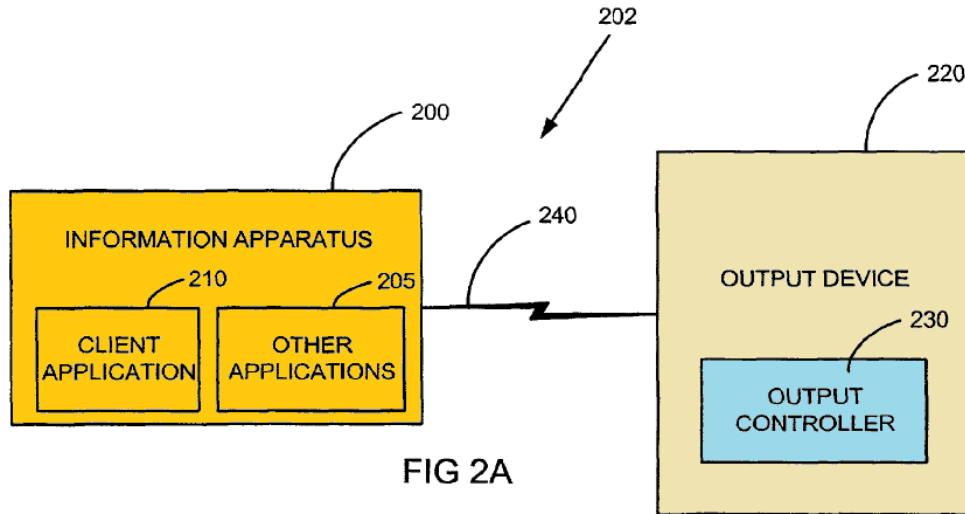
27. As a result, the printing process is functionally identical from the perspective of the client computer and the networked printer regardless of whether wireless networking may be used at some point in the communication path. I further note that the '031 patent describes no specific technical challenges to using wireless technology to transmit output data to printers or other output devices.

## **B. Overview of the '031 Patent**

28. The '031 patent describes a user computing device (“information apparatus 200”) that wirelessly connects to an output device 220 (*e.g.*, a printer) and uses the output device to output content (*e.g.*, a document). The information apparatus 200 can be a PC, laptop, or handheld computing device. '031 patent at 13:25-33. Output device 220 can be a conventional printer. *Id.* at 17:8-14 (conventional printer with a printer controller); 17:53-67 (conventional printer with no printer controller); Figs. 4A, 4B.

29. The output device 220 has an associated “output controller” 230. *Id.* at 13:20-24. The output controller 230 can manage communication with the information apparatuses and process output data for the output device. *Id.* at 18:13-16. Standard Bluetooth or IEEE 802.11 wireless communication can be used between the information apparatus and the output device / output controller. *Id.* at 14:15-19.

30. The output controller 230 can either be integrated into the output device 220 or can be external to the output device. These two alternatives are depicted in Figs. 2A and 2B (below, annotations added), respectively.



See also *id.* at 13:13-24 (introducing Figs. 2A and 2B).

31. The output controller 230 can be implemented with “a conventional personal computer (PC)”:

Other possible implementations of output controller 230 may include, for example, a ***conventional personal computer (PC)***, a workstation, and an output server or print server. In these cases, the functionalities of

output controller 230 may be implemented using application software installed in a computer (e.g., PC, server, or workstation), with the computer connected with a wired or wireless connection to an output device 220. *Using a PC, server, workstation, or other computer to implement the feature sets of output controller 230 with application software* is just another possible embodiment of the output controller 230 and *in no way departs from the spirit, scope and process of the present invention.*

*Id.* at 20:20-32<sup>1</sup>.

32. The alleged invention supposedly enables user information apparatuses to output content to output devices without first having to first install device drivers for those output devices. '031 patent at 1:31-36 (“Present invention relates to providing content to an output device and, in particular, to *providing universal output* in which an information apparatus can pervasively output content to an output device *without the need to install a dedicated device dependent driver or applications* for each output device.”). The patent suggests that users have traditionally been required to install output device drivers to use output devices because output device drivers are needed to process content into the format required by particular output devices. *Id.* at 2:27-51. The patent suggests, however, that searching for and installing drivers is time-consuming and complex.

<sup>1</sup> All emphasis used when quoting source material in this declaration has been added unless otherwise noted.

*Id.* at 2:64-3:46. The patent also notes that installing device drivers uses memory which can be limited in information apparatuses. *Id.* at 3:47-55. The patent further suggests that, even if drivers are located and installed, information apparatuses may lack the processing speed and battery power to execute the device drivers and process the content into the appropriate output format. *Id.* at 3:56-61.

33. The '031 patent explains that the alleged invention eliminates the need for output device-specific drivers at the user's information apparatus by intelligently splitting the responsibility for raster image processing (RIP) of content. *Id.* at 5:50-57 ("Accordingly, this invention provides a convenient universal data output method in which ***an information apparatus and an output device or system share the raster image processing operations***. Moreover, the new data output method ***eliminates the need to install a plurality of device-dependent dedicated drivers or applications*** in the information apparatus in order to output to a plurality of output devices.").

34. The Summary of the Invention explains that the information apparatus performs partial rasterization of content to generate "intermediate output data," but, importantly, the information apparatus does not perform the "***device dependent*** image processing operations of a RIP (e.g., color matching and halftoning)." *Id.* at 6:35-38. The output device dependent image processing is instead performed downstream by the output controller. *Id.* at 6:56-59 ("An output



controller application or component included in the output device or output system implements the remaining part of the raster image processing operations such as digital halftoning, color correction among others.”); *see also id.* at 30:25-43 (explaining that “output controller 230 may generate the proper language or input format required to interface with the printer controller”); *see also id.* at 28:32-56 (similar).

35. The ’031 patent asserts that “[u]nlike conventional raster image processing methods, this invention provides a ***more balanced distribution of the raster image processing computational load*** between the Information apparatus and the output device or the output system.” *Id.* at 6:60-64. This distribution of raster image processing supposedly “reduces the processing and memory requirements for the information apparatus” and allows for a smaller “driver,”<sup>2</sup> since it is only used to perform part of the rasterization process. *Id.* at 6:67-7:11. Additionally, the patent suggests that the partially (*i.e.*, generically) rasterized output generated by the information apparatus may be “more universally accepted by a plurality of output devices.” *Id.* at 7:14-17. As a result, “a user does not need

<sup>2</sup> The ’031 patent sometimes refers to the software that generates the intermediate output data as a “driver.” *See, e.g.*, 6:48-52 (“In an example of raster image process and data output method of the present invention, a client application such as a printer driver is included in an information apparatus and performs part of raster image processing operation such as rasterization on the content.”).

to preinstall in the information apparatus multiple dedicated device dependent drivers or applications for each output device.” *Id.* at 7:23-26.

36. The ’031 patent thus explains that the alleged invention avoids the need to install output device-specific drivers at the information apparatus by freeing the information apparatus from the responsibility of performing rasterization that is specific to the output device.

37. The claims of the ’031 patent have nothing to do with how raster image processing is allocated between the information apparatus and the output device. The ’031 patent’s claims focus instead on what the patent describes as “optional discovery process 1020 [that] may be implemented to help the user select an output device 220.” *Id.* at 29:36-38. The ’031 patent explains that “During the discovery process step 1020, a user's information apparatus 200 may (1) search for available output devices 220; (2) provide the user with a list of available output devices 220; and (3) provide means for the user to choose one or more output devices 220 to take the output job.” *Id.* at 29:38-43; *see also id.* at 30:61-31:15 (similar description).

38. The patent describes “[a]n example of a discovery process 1010” in connection with Fig. 11 (below). *Id.* at 29:43-45.

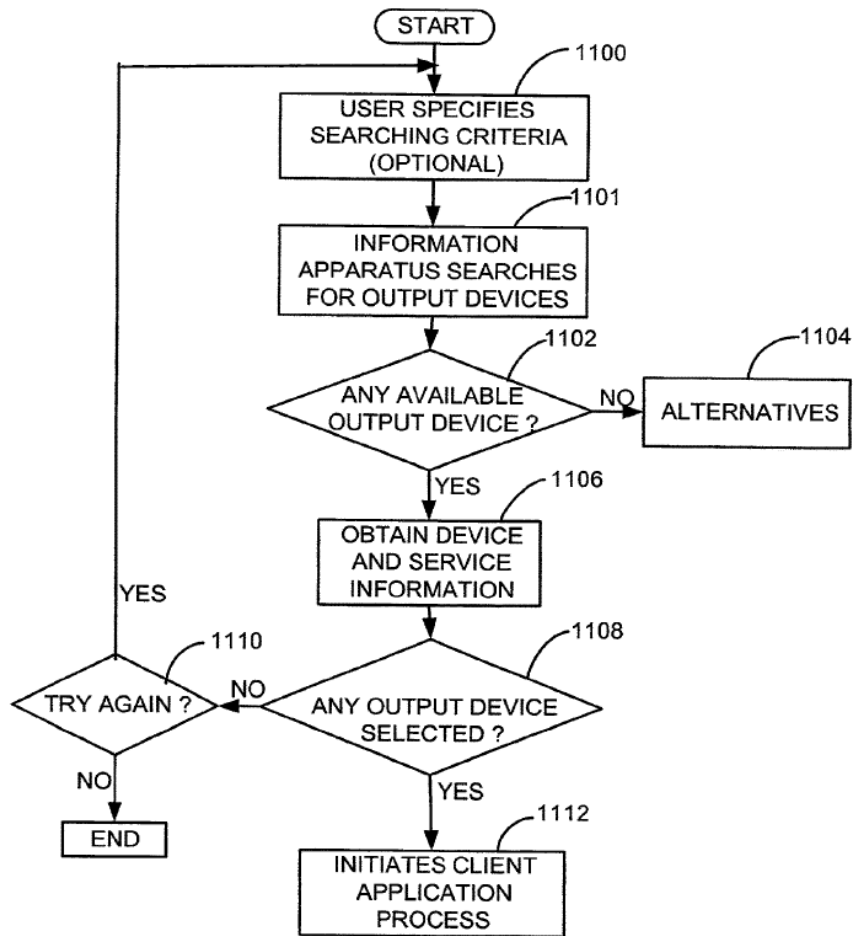


FIG 11

See also *id.* at 30:61-32:43 (describing Fig. 11).

39. The '031 patent states that “[v]arious protocols and or standards may be used during discovery process 1020.” *Id.* at 31:17-18. The patent further states that “[e]xamples of applicable protocols or standards may include, without limitation, Bluetooth, HAVi, Jini, Salutation, Service Location Protocol, and Universal Plug-and-play among others.” *Id.* at 31:20-23. The '031 patent specification thus suggests that existing, standardized discovery technologies could be used in the alleged invention by the information apparatus to locate output

devices. As I discussed above, the specifically-referenced standards included the same type of discovery functionality described by the '031 patent. *See supra* ¶¶ 17-19.

40. Although the '031 patent specification describes the invention almost exclusively in terms of printing, it asserts in a few places that the invention applies to other types of output devices as well. *See, e.g., id.* at 16:42-48 (“However, it should be recognized that present invention applies also to other output devices 220 such as fax machines, digital copiers, display screens, monitors, televisions, projectors, voice output devices, among others.”); *see also id.* at 1:54-57; 16:34-41. Certain claims of the '031 patent are restricted to transmission of audio and/or video data and to output devices such as televisions, but there is no meaningful discussion of audio or video data or of televisions in the patent. There is no discussion at all of how audio or video data is processed or how such data is output by a television or any other type of output device.

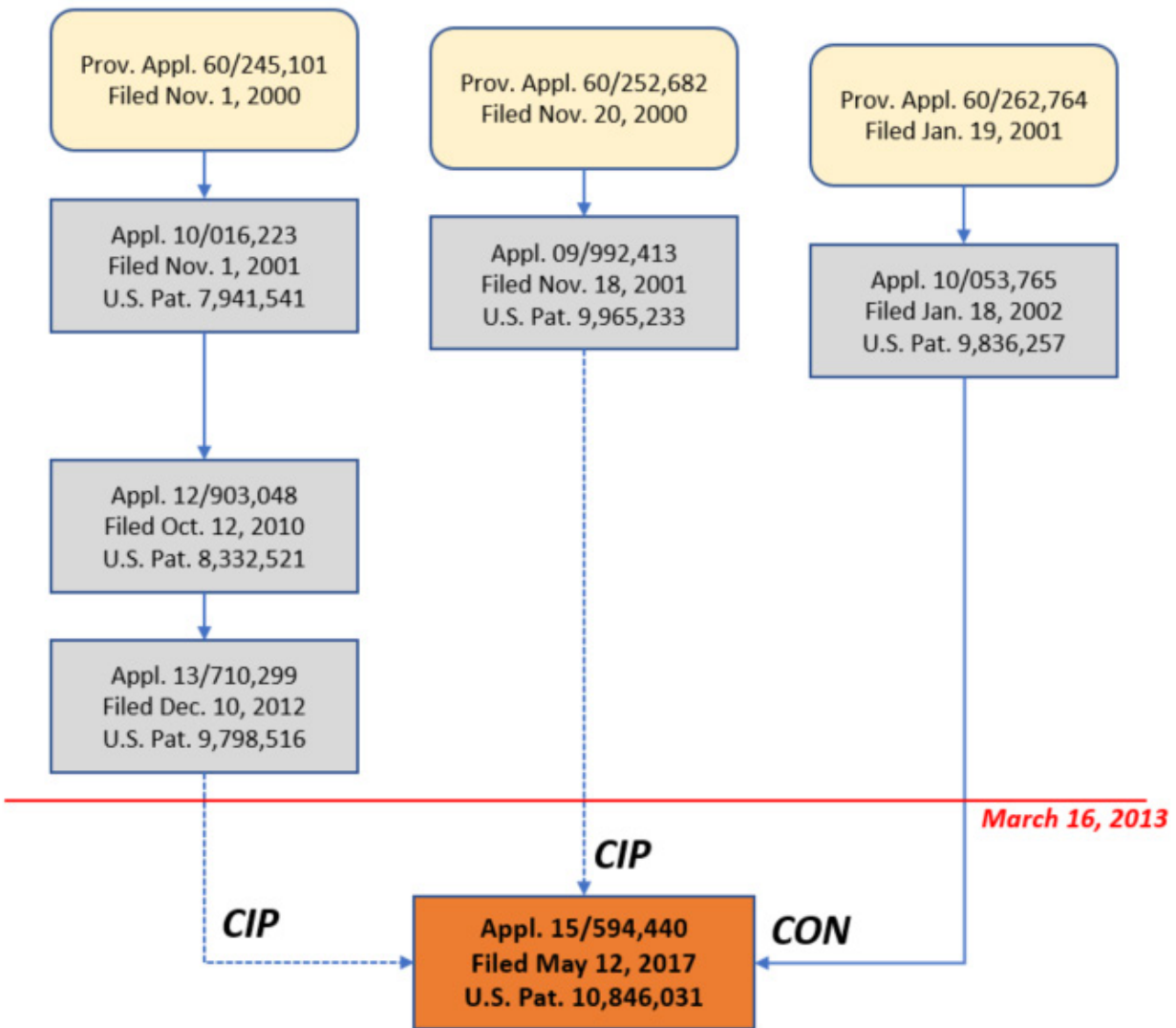
**C. The '031 Patent's Priority Applications Do Not Describe Using an Internet Appliance as an Output Device or Output System.**

41. The '031 patent states that information apparatuses can be an “Internet appliances.” '031 patent at 1:47-54 (“Examples of such information apparatuses include ... Internet appliances ....”); 3:47-52 (“Another challenge for mobile users is that many mobile information apparatuses have limited memory space, processing capacity and power. These limitations are more apparent for small and

low-cost mobile devices including ... Internet appliances ...."); 13:26-31 ("In one embodiment, information apparatus 200 may be a mobile computing device such as ... Internet appliance ...."); 14:23-26 ("Information apparatus 200 may be a dedicated device (e.g., email terminal, web terminal, digital camera, e-book, web pads, Internet appliances etc.) with functionalities that are pre-configured by manufacturers."). Setting aside the applications incorporated by reference, these four statements are the only statements in the '031 patent specification referring to Internet appliances.

42. Claims 6 of the '031 patent states that "the output system is at least one of a sound output system, a television system, an output controller connectable to a television, a projection system, a printing system, or an information apparatus that is at least an *Internet appliance*." Claim 19 similarly states that "the output device is at least one of a sound output device, a television device, a controller device connectable to a television, a projector device, or *an Internet appliance*, individually or in any combination." These claims thus state that the "output system" or "output device" can be an Internet appliance.

43. In my opinion the disclosures in the priority applications to the '031 patent do not demonstrate that the inventors were in possession of the idea that the *output system* or *output device* could be an Internet appliance. The diagram below from Roku's Petition shows the various priority applications:



44. The specification of the '031 patent is almost the same as the specification of the '765 application, except the '031 patent has a different abstract and incorporates by reference the other priority applications listed above. The '765 application contains the same four references to Internet appliances that I discussed above. *See* Ex. 1011 ('765 application) at [0004], [0014], [0077], [0083]. The other priority applications are similar in that they consistently identify Internet appliances as examples of information apparatuses, not as output devices or output

systems. *See, e.g.*, Ex. 1009 ('299 application) at [0003], [0038]; Ex. 1010 ('413 application) at [0002], [0012], [0047], [0052], [0165].

45. In my opinion, that these applications suggest that an information apparatus can be an "Internet appliance" does not suggest that an output system or output device can also be one. There is actual little if any overlap between the devices identified as information apparatuses and those identified as output devices. For example, the '765 application (and the '031 patent itself) contains the following paragraph listing information apparatuses (yellow highlighting added) and output devices (orange highlighting added):

[0004] As described herein, information apparatuses refer generally to computing devices, which include both stationary computers and mobile computing devices (pervasive devices). Examples of such information apparatuses include, without limitation, desktop computers, laptop computers, networked computers, palmtop computers (hand-held computers), personal digital assistants (PDAs), Internet enabled mobile phones, smart phones, pagers, digital capturing devices (e.g., digital cameras and video cameras), Internet appliances, e-books, information pads, and digital or web pads. Output devices may include, without limitation, fax machines, printers, copiers, image and/or video display devices (e.g., televisions, monitors and projectors), and audio output devices.

Ex. 1011 ('765 application) at [0004]; '031 patent at 1:44-57. Here, none of the devices listed as examples of information apparatuses are listed as examples of output devices. Elsewhere, the '765 application lists examples of output devices with no mention of using Internet appliances, PDAs, smart phones, pagers, or the other devices given as examples of information apparatuses. Ex. 1011 ('765

application) at [0090] (“However, it should be recognized that present invention applies also to other output devices 220 such as fax machine, digital copiers, display screens, monitors, televisions, projectors, voice output devices, among others.”). Since the inventors decided to list examples of output devices in their applications, and they were clearly familiar with Internet appliances, one would expect them to have mentioned “Internet appliances” among the other exemplary output devices if they had in fact contemplated using Internet appliances as output devices.

46. The ’765 application (and the ’031 patent itself) points to Internet appliances as examples of “small and low-cost mobile devices” that would “have limited memory space, processing capacity and power.” Ex. 1011 (’765 application) at [0014]; ’031 patent at 3:46-64. Because of these constraints, it is suggested that Internet appliances may not have the memory necessary to install or run “complex printer or device drivers” and may not have the “processing speed” and “power supply” necessary to drive an output device. The paragraph concludes: “Therefore, a method is needed so that a small mobile device, with limited processing capabilities, can still reasonably output content *to various output devices.*” *Id.* Here, the inventors suggested that the benefit the alleged invention provides to Internet appliances is that it enables them to output content to various output devices, not that it better enables them to receive output content from other



devices and output it *themselves*. In my opinion, a POSA would have recognized that the same resource constraints associated with Internet appliances described in the '765 application and '031 patent would have made them poor candidates for use as output devices due to their processing and power constraints.

47. The '413 application similarly lists Internet appliances as examples of “small and low-cost mobile devices” with “limited memory space, processing capacity and power. Ex. 1010 ('413 application) at [0012]. In the very next paragraph, the application explains that “small mobile devices with limited display screens” are limited in their abilities to display complex documents. *Id.* at [0013]. Here again, the suggested fix is not to improve the ability of these devices to output content themselves, but instead “to allow mobile users to output from their small information apparatuses to an output device the full richness of the original document content.” *Id.*

48. Finally, paragraph [0089] of the '765 application reads as follows:

[0089] Output device 220 is an electronic system capable of outputting digital content regardless of whether the output medium is substrate (e.g., paper), display, projection, or sound. A typical example of output device 220 is a printer, which outputs digital documents containing text, graphics, image or any combination onto a substrate. Output device 220 may also be a display device capable of displaying still images or video, such as, without limitation, televisions, monitors, and projectors. Output device 220 can also be a device capable of outputting sound. Any device capable of playing or reading digital content in audio (e.g., music) or data (e.g., text or document) formats is also a possible output device 220.

This paragraph describes how output device 220 outputs content and gives

examples of output devices that are consistent with the lists elsewhere in the application. *See* Ex. 1011 ('765 application) at [0004], [0090] (both listing examples of output devices). The last sentence of paragraph [0089] suggests that a device that can play music or read text aloud could potentially be an output device 220. Regardless, this paragraph does not state or suggest using an Internet appliance as an output device.

49. Based on the above, it is my opinion that the applications cited for priority in the '031 patent fail to demonstrate that the inventors were in possession of the idea that an Internet appliance could be used as an output system or device.

#### **D. Claim Construction**

50. I understand that in a PGR proceeding, the challenged claims are construed “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.200(b). In evaluating the challenged claims, I have applied my understanding as to what a person of ordinary skill in the art would have understood these claims to mean as of November 1, 2000 when the earliest-filed priority application was filed.

### **III. UNPATENTABILITY OF THE CHALLENGED PATENT CLAIMS**

#### **A. Legal Standards for Invalidity Subject Matter Eligibility Under 35 U.S.C. § 101**

51. I understand that where a patent claim is directed to an abstract idea,

the claim is invalid unless the claim contains an “inventive concept” which must be an element or some combination of elements that ensures the patent claim amounts to significantly more than a patent claim on the abstract idea itself. I understand that an inventive concept cannot be well-understood, routine, conventional activities previously known to the industry. I also understand that “wholly generic computer implementation” is not generally sufficient to provide an inventive concept. I understand that the elements of a claim must be considered both individually and also as an ordered combination in determining whether they include an inventive concept.

**B. The Conventionality of the '031 Patent Claims**

52. I understand Roku asserts that the claims of the '031 patent are directed to the abstract idea of accessing resources over communication networks. I am not a lawyer and I have not been asked to offer an opinion regarding the abstractness of the patent claims. Nonetheless, Roku's position that the claims of the '031 patent focus on the idea of accessing resources over communication networks is consistent with my analysis of the claims.

53. Roku has asked me to analyze the claims of the '031 patent to provide an opinion as to whether the claim elements recite routine and conventional technology.

**1. Claim 1**

**a. The preamble**

54. Claim 1 begins with the following preamble:

A non-transitory computer readable storage medium having recorded therein software that is executable at a mobile information apparatus to wirelessly set up an output system for providing output service to the mobile information apparatus, the output system includes wireless communication circuitry for wireless communication, and the output system is associated with at least an output device for output of digital content, and the output system is a separate device from the mobile information apparatus, the mobile information apparatus comprises:

55. Nothing in the preamble was unconventional by late 2000. The preamble makes clear that the claim is directed to a “storage medium” with software executed by a “mobile information apparatus.” The preamble indicates that the intended purpose of the claimed software is “to wirelessly set up an output system for providing output service to the mobile information apparatus.” Given the context of the ’031 patent, in my opinion a POSA would understand the language “set up an output system” to refer to setting up the output system for use by the mobile information apparatus. The “output system” is capable of wireless communication and is at least associated with an output device. I discuss these devices below.

**b. The claimed “mobile information apparatus”**

56. There was nothing unconventional about the claimed “mobile

information apparatus” in late 2000.

57. The patent specification explains that “[a]s described [t]herein, information apparatuses refer generally to computing devices, which include both stationary computers and mobile computing devices (pervasive devices).” ’031 patent at 1:44-47; 13:25-26 (“Information apparatus 200 is a computing device with processing capability.”).

58. “[I]nformation apparatus 200 may be a mobile computing device such as palmtop computer, handheld device, laptop computer, personal digital assistant (PDA), smart phone, screen phone, e-book, Internet pad, communication pad, Internet appliance, pager, digital camera, etc.” *Id.* at 25:26-31. “It is possible that information apparatus 200 may also include a static computing device such as a desktop computer, workstation, server, etc.” *Id.* at 13:31-33; *see also id.* at 1:47-54 (listing similar types of devices as “examples” of information apparatuses).

59. The ’031 patent does not describe any new “mobile information apparatus” device. Devices such as “smart phones” and “information pads” are mentioned as possible information apparatuses but not otherwise described or discussed in any meaningful way. The patent specification focuses on a generic information apparatus 200. There is no suggestion anywhere in the patent specification that the invention works any differently whether the information apparatus 200 is a smart phone or a desktop or laptop computer.

60. The required hardware components of the mobile information apparatus that are recited in claim 1 were all routine and conventional by late 2000. PDAs and other handheld computers included processors, memory, and often touch screens as well. For example, HP's "Jornada" line of handheld computers included these standard components. Appx. N (HP Jornada brochure, 1999); *see also, e.g.*, Appx. B (Geier, *Wireless LANs*, 1999) at 29-31 (discussing features of Handheld PCs).

61. Handheld computing devices often featured PCMCIA (or PC Card) slots which could receive PC Card-based wireless modules. Appx. B (Geier, *Wireless LANs*, 1999) at 34 ("Many portable computers have PCMCIA slots that accept credit card-sized NICs."); *see also, e.g.*, Appx. N (HP Jornada brochure, 1999). Below is a picture of a wireless PC Card, the Proxim RangeLAN2 7410 CE PC Card, for handheld devices running Windows CE.



Appx. O (Proxim RangeLAN2 7410 CE PC Card data sheet, 1999).

62. Claim 1 mentions that the wireless communication units of the mobile

information apparatus “include one or more radio frequency link controllers for wireless communication.” The ’031 patent describes an RF Link Controller 810 only briefly and in functional terms. ’031 patent at 25:5-12 (“RF link controller 810 implements real-time lower layer (e.g., physical layer) protocol processing that enables the hosts (e.g., information apparatus 200, output controller 230, output device 220, etc.) to communicate over a radio link. Functions performed by the link controller 810 may include, without limitation, error detection/correction, power control, data packet processing, data encryption/decryption and other data processing functions.”).

63. The ’031 patent specification thus reveals that the claimed “link controller” is a functional block within the wireless communication unit that enables conventional wireless communication. *See* ’031 patent at 25:56-59 (noting that a wireless unit like that shown in Fig. 8A “may be included in devices ... to support various wireless communications standards”). Conventional wireless NICs included what the ’031 patent describes as the “RF link controllers” used to process data sent and received according to the relevant networking standards including their physical layer protocols (*e.g.*, IEEE 802.11). *See, e.g.*, Appx. B (Geier, *Wireless LANs*, 1999) at 34-35.

64. The specification does not suggest that the information apparatus 200 requires any new technology to perform the functions recited in claim 1. Instead,

the specification suggests this functionality is implemented with software on the information apparatus. *Id.* at 31:1-3 (“The information apparatus 200 may utilize the client application 210 or other application 205 in this process.”); *see also id.* at 31:28-39 (discovery process can be implemented by “communication manager” either incorporated into client application 210 or utilized by client application 210). There is no detailed or technical description of the software that performs these functions. In general, the ’031 patent specification describes what the software does, not how the software does it. *See id.* at 15:29-16:28 (listing various “components or operations” of client application 210).

**c. The claimed “output system”**

65. Claim 1 also refers to an “output system.” The preamble states that the “output system is associated with at least an output device for output of digital content.” The ’031 patent specification often uses the term “output system” to refer to the combination of an output device 220 and its output controller 230. *See, e.g.,* ’031 patent at 13:20-24 (“The output system 250 includes an output device 220 and an output controller 230 which may be externally connected to, or otherwise associated with, the output device 220 in the output system 250.”); Fig. 2B (showing “output system” 250). Sometimes, however, the term “output system” is seemingly used interchangeably with “output device.” *See, e.g., id.* at 8:41-42 (“FIG. 4B is a block diagram of a second conventional output system or



output device.”). Dependent claim 6 indicates the “output system” of claim 1 could be “at least one of a sound output system, a television system, an output controller connectable to a television, a projection system, a printing system, or an information apparatus that is at least an Internet appliance, individually or in any combination.”

66. Of the output devices listed in claim 6, only “printing system[s]” are meaningfully discussed in the ’031 patent specification. *See, e.g.*, ’031 patent at 16:42-18:48 (discussing printers and output controllers for use with printers); Figs. 4A & 4B, Figs. 5A & 5B. The term “television” appears just three times in the specification and each time in a sentence that merely lists possible types of output devices. *Id.* at 1:54-57; 16:34-37; 16:44-48. Although the specification discusses output controllers in general and in connection with printers, there is no specific discussion of any output controller for use in or with a television.

67. Even when the alleged invention is used with printers, the patent indicates that the printers themselves can be conventional. *Id.* at 18:24-27 (“FIG. 5A illustrates the implementation of an output controller 230 inside a ***conventional printer*** with reference to FIG. 4A, which includes a ***conventional printer controller*** 410(5A).”); 18:35-38 (“FIG. 5B illustrates the implementation of an output controller 230 included internally in a ***conventional output device 220*** with reference to FIG. 4B, which does not include a printer controller.”).

68. Claim 1 does not expressly require the output system to include an “output controller.” Even if it did, however, the ’031 patent specification makes clear that the “output controller” is not a specific device or program; it is essentially a black box that can be implemented with conventional technology in order to perform certain functions. The patent identifies 16 different “components and operations” that *may* be part of output controller 230. ’031 patent at 20:46-21:51 (“Functionalities and components of output controller 230 for the purpose of providing universal data output *may* include or utilize ...”). As an example, the first set of “components and operations” is “Components and operations to receive output data from a plurality of information apparatus 200 ....” *Id.* at 20:49-53.

69. The ’031 patent states that the output controller can be hardware, software or both. *Id.* at 18:16-18 (“Output controller 230 may include dedicated hardware or software or combination of both for at least one output device 220.”); 19:4-8 (“FIG. 6 includes three functional block diagrams illustrating the hardware/software components of output controller 230 in three different implementations. Each components of an output controller 230 may include software, hardware, or combination.”); Fig. 6. To the extent the patent discusses a hardware implementation, it merely lists well-known hardware components such as ASICs and DSPs that can optionally be used. *Id.* at 19:8-16 (“For example, an output controller 230 may include components using one or more or combinations

of an application-specific integrated circuit (ASIC), a digital signal processor (DSP), a field programmable gate array (FPGA), firmware, system on a chip, and various communication chip sets. Output controller 230 may also contain embedded processors 670 A with software components or embedded application software to implement its feature sets and functionalities.”).

70. The output controller can be integrated into the output device or can be a separate device. *Id.* at 18:18-20 (“Output controller 230 may be internally installed, or externally connected to one or more output devices 220.”); *see also id.* at 23:4-24:41 (describing Figs. 7A-7F which depict internal and external output controllers and output devices); Figs. 7A-7F. The output controller can even be partially internal to the output device and partially external. *Id.* at 24:44-48 (“For example, partial functionalities of output controller 230 may be implemented in an external box or station while the remaining functionalities may reside inside an output device 220 as a separate board or integrated with a printer controller 410.”).

71. The ’031 patent also states very clearly that the output controller 230 can be implemented with a “conventional personal computer (PC)”:

Other possible implementations of output controller 230 may include, for example, a **conventional personal computer (PC)**, a workstation, and an output server or print server. In these cases, the functionalities of output controller 230 may be implemented using application software installed in a computer (e.g., PC, server, or workstation), with the computer connected with a wired or wireless connection to an output device 220. *Using a*

*PC, server, workstation, or other computer to implement the feature sets of output controller 230 with application software is just another possible embodiment of the output controller 230 and in no way departs from the spirit, scope and process of the present invention.*

*Id.* at 20:20-32.

72. There is no detailed description of any hardware or software that performs the functionalities of the output controller 230. The implication is that a POSA would know how to design hardware and/or write software to perform those functions without needing detailed guidance from the patent specification.

73. Finally, the specification states repeatedly that a print server can be an output controller. *Id.* at 20:20-32 (quoted in full above); 18:20-21 (“The output controller 230 is sometimes referred to as a print server or output server.”); 19:60-64 (“An output controller 230 implemented as an external box or station to an output device 220 may contain its own user interface. One example of such an implementation is a print server connected to an output device 220 in an output system 250.”); 24:2-4 (“For example, the output controller 230 may be implemented as an application in a print server or as a standalone box or station.”). As I discussed above, print servers were well known by 2000. *See supra* ¶¶ 20-23.

**d. The five functions**

74. Claim 1 includes a first “wherein ...” clause:

wherein, when the one or more processors included in the mobile information apparatus execute at least part of the software at the mobile information apparatus, the mobile information apparatus:

This language is followed by five enumerated functions that the mobile information apparatus performs when its software is executed.

**(i) Function 1: discover the output system**

75. In the first recited function of claim 1 the mobile information apparatus wirelessly discovers the output system:

(1) wirelessly discovers, using the one or more wireless communication units of the mobile information apparatus, the output system, the wireless discovery of the output system is based, at least in part, on physical proximity between the mobile information apparatus and the output system;

This language does not specify *how* the information apparatus discovers the output system.

76. As I discussed above, the specification of the '031 patent describes an optional discovery process 1020 that may be used by information apparatus 200 to locate an output device 220. The patent acknowledges that standard protocols such as "Bluetooth, HAVi, Jini, Salutation, Service Location Protocol, and Universal Plug-and-play among others" can be used to implement the discovery process. '031 patent at 31:20-23.

77. The '031 patent discusses an exemplary discovery process in connection with Fig. 11. The discovery process can involve devices "multi-casting

or broadcasting” searches for devices that provide particular services. *Id.* at 31:54-60. “Alternatively or in combination,” output devices can send “broadcasts” advertising their services. *Id.* at 31:60-63. This high-level discussion is generally consistent with discovery functionality provided in UPnP and the other discovery standards and protocols mentioned in the patent specification. Notably, nothing in the ’031 patent’s description of the discovery process suggests any need to approach discovery differently because wireless communications are involved.

78. As the ’031 patent acknowledges, numerous technologies were available to allow devices to discover other devices over networks. For example, the Bluetooth specification, published in 1999, describes the Service Discovery Protocol (SDP). Appx. P (Bluetooth Core Specification, 1999) at 323-384. The Bluetooth specification even notes that the service discovery “problem is widely recognized; many companies, standards bodies and consortia are addressing it at various levels in various ways. Service Location Protocol (SLP), Jini, and Salutation, to name just a few, all address some aspect of service discovery.” *Id.* at 370. Service Location Protocol (SLP) was initially described in RFC 2165, published in June 1997, and then updated via RFCs 2608 and 2609, published in

June 1999.<sup>3</sup> Universal Plug and Play (UPnP) relies on the Simple Service Discovery Protocol (SSDP) which was documented in IETF drafts published in 1999. *See, e.g.,* Appx. Q (*Simple Service Discovery Protocol/1.0, v1.03*, Oct. 28, 1999). An article published in the September / October 2000 issue of IEEE Internet Computing discusses the discovery capabilities of several of these protocols. Appx. E (Richard, *Service Advertisement and Discovery: Enabling Universal Device Cooperation*).

79. Although the claim language requires the discovery to be “based, at least in part, on physical proximity between” the devices, the ’031 patent specification does not describe any new or improved way of accounting for “physical proximity” during the discovery process. As a practical matter, all wireless communications technologies (even satellite) are constrained by physical proximity and different wireless transmitters have different ranges.<sup>4</sup> I understand that Flexiworld asserts that the “physical proximity” limitation is met if the devices are connected to the “same Wi-Fi network.” Ex. 1013 (’031 claim chart) at 35. Well-known discovery protocols—including most of those mentioned in the ’031

<sup>3</sup> *See* <https://datatracker.ietf.org/doc/html/rfc2165>; <https://datatracker.ietf.org/doc/html/rfc2608>; <https://datatracker.ietf.org/doc/html/rfc2609>.

<sup>4</sup> The Proxim RangeLAN2 had a range of approximately 400 - 700 feet. Appx. O at 2 (“Range (snap-on)...~400 feet (~122 m) radius indoors 700 feet (~213 m) radius outdoors (more with optional dipole antenna).”)

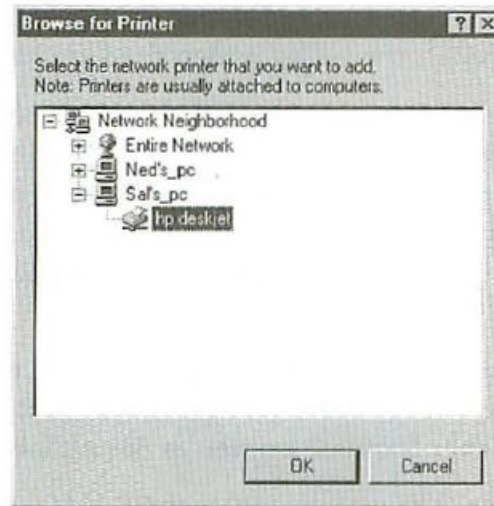
patent—were designed to discover devices and services on a particular network. *See, e.g.*, Appx. Q (SSDP spec) at 6 (“Our goal is to provide for discovery for local area networks not for the entire Internet.”); Appx. R (RFC 2608) at 3 (“SLP has been designed to serve enterprise networks with shared services, and it may not necessarily scale for wide-area service discovery throughout the global Internet, or in networks where there are hundreds of thousands of clients or tens of thousands of services.”).

80. Even apart from the known discovery technologies called out in the ’031 patent specification, there was nothing unconventional about discovering output devices available via a network. Windows included an “Add Printer Wizard” that enabled users to find and add networked printers:



Browse for the  
Printer's Location

5. If you don't know the printer's network path, click the Browse button. You'll see a list of the computers and independent printers on your network.
  - You can click a particular printer's icon to specify its network path. Or, to find a printer connected to another computer, double-click the computer icons in this list until you find the printer you want. Then select the printer icon.
  - Click the OK button, and the network path for the printer you selected will appear in the Add Printer Wizard.

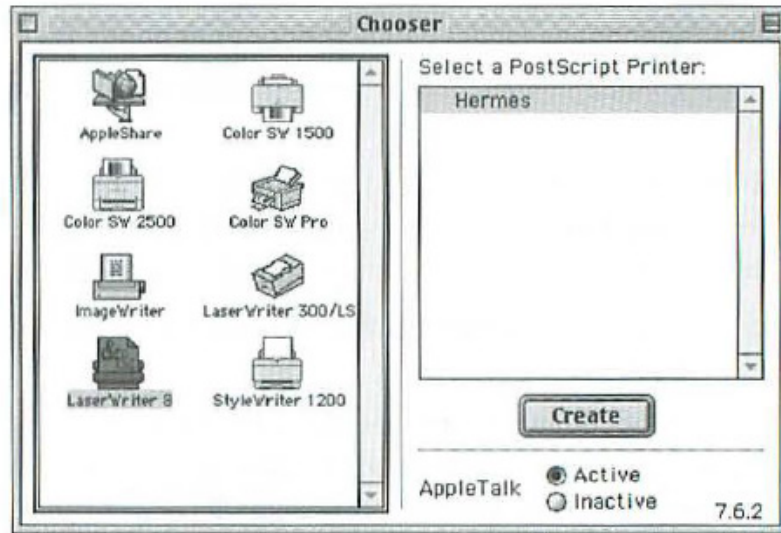


*If you don't know the network path, you can look for it in this Browser dialog box.*

Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 136-137. Mac OS included similar functionality:

**Select a Specific Printer**

4. After selecting a printer driver on the left side of the Chooser, you select a specific printer on the right side of the Chooser. For independent network printers, you'll see a list of printer names. Shared local printers are listed by name along with the Mac's printer and modem ports.



*Click the LaserWriter 8 icon to see the names of PostScript printers available on the network.*

*Id.* at 140. See also, e.g., Appx. S (Person, *Using Windows 95: Special Edition*, 1995) at 775-776 (describing use of Add Printer Wizard to add network printers in Windows 95); Appx. T (Pogue, *Mac OS 9: The Missing Manual*, 2000) at 347-349 (describing printer installation in Mac OS 9).

81. The network printers added through these conventional processes could be independent network printers directly connected to the network. Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 114-115. The network printers could also be printers connected to a host computer (e.g., a PC) on the network. *Id.* This is consistent with the '031 patent's suggestion of

using a “conventional personal computer” as an output controller for an output device. *See, e.g.*, ’031 patent at 20:20-32 (“Other possible implementations of output controller 230 may include, for example, a conventional personal computer (PC) .... Using a PC... to implement the feature sets of output controller 230 with application software is just another possible embodiment of the output controller 230 and in no way departs from the spirit, scope and process of the present invention.”).

**(ii) Functions 2 & 3: display the output system for user selection**

82. Functions 2 and 3 require the mobile information apparatus to display a discovered output system in the user interface and receive user selection of the output system:

(2) displays, on the touch sensitive screen interface of the mobile information apparatus, a user interface item or icon related to the output system wirelessly discovered in (1) for user selection;

(3) obtains, using the touch sensitive screen interface of the mobile information apparatus and from the user, at least an indication of a selection of the user interface item or icon, related to the output system wirelessly discovered in (1) and displayed on the touch sensitive screen interface in (2);

83. There was nothing unconventional about displaying items to the user in a user interface for selection. Computers with graphical user interfaces have traditionally displayed applications, files, devices, and other items to the user for

selection.

84. The '031 patent itself does not describe any new or improved way of presenting output devices to a user for selection. This functionality is described only at a very high level:

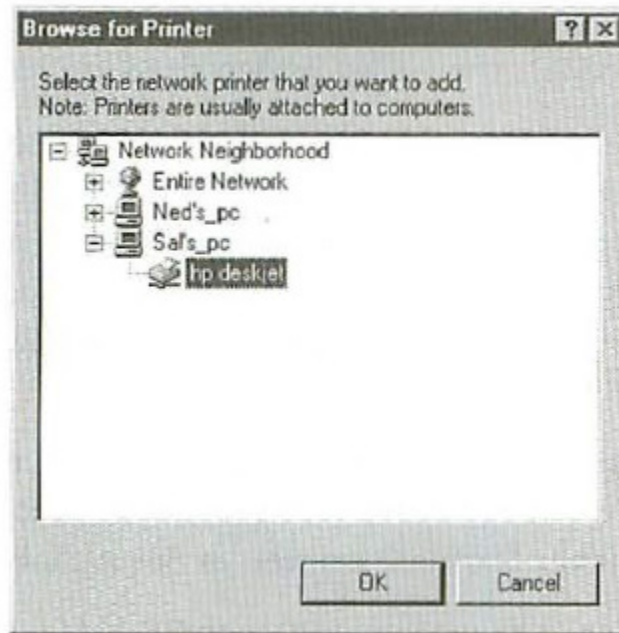
In step 1106, if available output devices 220 are discovered, the communication manager may obtain some basic information, or part of or the entire output device profile, from each discovered output device 220. ... Such ***information is preferably provided to the user through the user interface*** (e.g., display screen, speaker, etc.) of information apparatus 200.

In step 1108, the ***user may select one or more output devices 220*** based on information provided, if any, to take the output job.

'031 patent at 32:21-32. Notably, this functionality is not described specifically in connection with a touch screen. The '031 patent describes no new or improved touch screen technology and no new or improved ways to use touch screens. Nothing in the '031 patent suggests that the invention works differently when the user selects the output device via touch screen as opposed to using a mouse or keyboard. *See id.* at 13:43-47 (describing information apparatus 200: “Examples of such [user] interfaces include, without limitation, one or more of a mouse, a keyboard, a touch-sensitive or non-touch-sensitive screen, push buttons, soft keys, a stylus, a speaker, a microphone, etc.”).

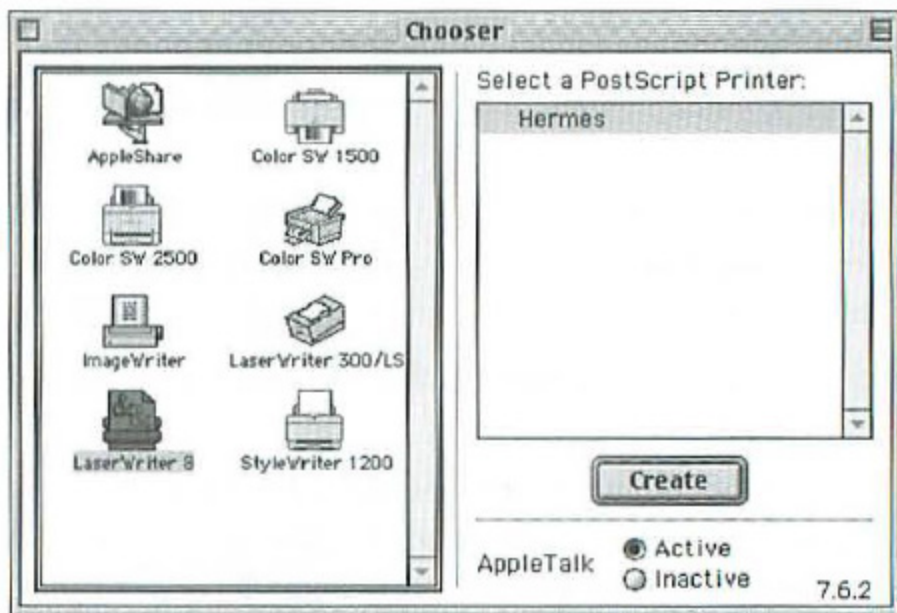
85. As discussed above for Function 1, both Windows and Mac OS

displayed available printers to the user for selection. In the exemplary screen below, a Windows user could select the printer named “hp deskjet” in the “Browse for Printer” window:



*If you don't know the network path, you can look for it in this Browser dialog box.*

Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 137. Similarly, in the exemplary Chooser window below, a Mac user could select the printer named “Hermes”:



*Click the LaserWriter 8 icon to see the names of PostScript printers available on the network.*

*Id.* at 140. In Mac OS, users selected both an icon (e.g., the LaserWriter 8 icon) and a user interface item (the printer name in the list box) and both are associated with a printer (e.g., Hermes) that is discovered.

86. As also discussed for Function 1, there were well-known protocols that supported service discovery. It was well understood that these protocols would be used in situations such as where a user is searching for a printer or printing service, and that the discovered devices and/or services might be presented to a user for selection. The Bluetooth specification provides an example to illustrate the use of SDP where “an SDP client is searching for available Synchronization services that can be presented to the user for selection.” Appx. P at 376; *see also id.* at 371-375 (discussing two examples based on “an SDP client

searching for a generic printing service”). The SSDP specification similarly describes setting up a network and using SSDP to “discover SSDP services in the form of Printers, Scanners, Fax Machines, etc.” Appx. Q at 4; *see also id.* at 6 (discussing the use of discovery in order “to display to our user all the VCRs in her house”).

**(iii) Function 4: send security or authentication information**

87. Function 4 requires the mobile information apparatus to provide security or authentication information to the output system to access its services:

(4) wirelessly provides, using the one or more wireless communication units of the mobile information apparatus, security information or authentication information, from the mobile information apparatus to the output system that is wirelessly discovered in (1) and selected in (3), the security information or the authentication information is to facilitate, at least in part, the mobile information apparatus to access services provided by the output system.

88. The '031 patent describes no new or improved security scheme for limiting access to output devices. The patent states that “an optional authentication step may be included when the selected output device 220 provides service to a restricted group of users.” '031 patent at 36:19-22. The patent specification further explains that “[a] simple authentication may be implemented by, for example, comparing the identity of an information apparatus 200 with an approved control list of identities stored in the output device 220 or output controller 230.”

*Id.* at 36:29-33. The specification also states that the information used can include things like a “user name,” “password,” or “ID number” and that this information “may be manually provided by user ....” *Id.* at 36:34-41.

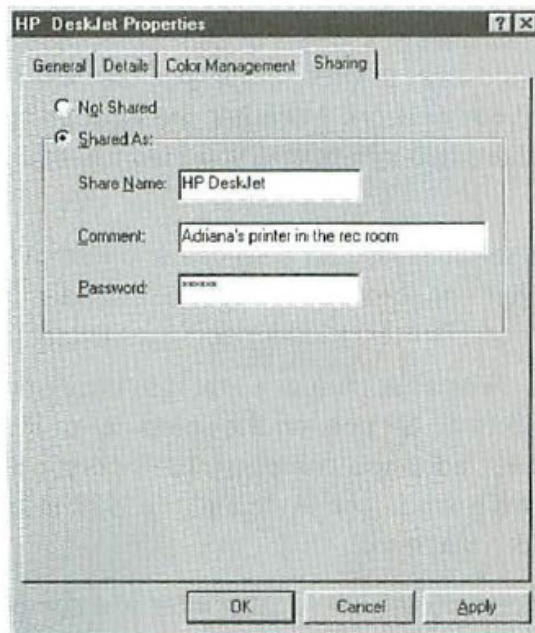
89. The patent thus describes using an admittedly “simple” access control scheme and that scheme is described in purely functional terms. Although the specification also states that “[o]ther more complex authentication schemes may also be used,” (*id.* at 29:33-34), it never describes any such “more complex” authentication schemes.

90. There was nothing unconventional about a client device providing security or authentication information to access the services of a networked device. As shown in the figure below, Windows enabled printers to be shared on the network with password restrictions:



5. In the Share Name field, enter a name for the printer. This name will appear on other network users' machines when they access your computer in their Network Neighborhood.

In the Comment field, you can type a phrase that describes the printer or its location. If you have more than one printer, this comment will help users identify the printer.



*The printer name and comment can be seen by other network users. A password is optional.*

Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 125-126. Mac OS likewise allowed for restricting access to a shared printer via password:



*Id.* at 129.

**(iv) Function 5: establish a wireless communication link**

91. Function 5 requires the mobile information apparatus to “establish ... a wireless communication link” which may be either “[i] a direct short range wireless communication link or [ii] a wireless location area network communication link”:

(5) wirelessly establishes, using the one or more wireless communication units of the mobile information apparatus, a wireless communication link between the mobile information apparatus and the output system that is wirelessly discovered in (1), the wireless communication link being a direct short range wireless communication link or a wireless local area network communication link, and the wireless establishing of the wireless communication link is based, at least in part, on the mobile information apparatus having obtained the indication of the selection of the user interface item or icon in (3);

92. There was nothing unconventional about establishing the claimed

wireless communication links. The '031 patent does not describe any new or improved wireless technologies. Instead, the patent embraces the use of standard wireless technologies such as IEEE 802.11 and Bluetooth:

A variety of radio links may be utilized. A group of competing technologies operating in the 2.4 GHz unlicensed frequency band is of particular interest. This group currently includes ***Bluetooth, Home radio frequency (Home RF) and implementations based on IEEE 802.11 standard.*** Each of these technologies has a different set of protocols and they all provide solutions for wireless local area networks (LANs). Interference among these technologies could limit deployment of these protocols simultaneously. It is anticipated that new local area wireless technologies may emerge or that the existing ones may converge. ***Nevertheless, all these existing and future wireless technologies may be implemented in the present invention without limitation, and therefore, in no way depart from the scope of present invention.***

'031 patent at 25:13-27; *see also id.* at 13:55-60 (“In one embodiment of the present invention, communication interface 240 between information apparatus 200 and output device 220 or output system 250 is a wireless communication interface such as a short-range radio interface including those implemented according to the Bluetooth or IEEE 802.11 standard.”); 14:15-19 (“For example, information apparatus 200 may communicate with one output device 220 through a Bluetooth standard interface or through an IEEE 802.11 standard interface while communicating with another output device 220 through a parallel cable interface.”).

93. By late 2000, IEEE 802.11 was the dominant wireless LAN standard. *See, e.g.*, Appx. C (New York Times article published Oct. 30, 2000) at 2 (“The 802.11b format is catching on so quickly that it is displacing alternative wireless competitors that include Bluetooth and HomeRF.”); *see also e.g.*, Appx. B (Geier, *Wireless LANs*, 1999) at 91-92 (discussing advantages of 802.11 vs. proprietary standards). By the same time, it was well understood that Bluetooth could be used to support direct wireless links between computing devices. *See, e.g.*, Appx. D (Haartsen, *The Bluetooth Radio System*, February 2000) (discussing how Bluetooth supports ad hoc networking).

**e. The final “wherein ...” clause**

94. Claim 1 concludes with a second “wherein ...” clause:

wherein the mobile information apparatus wirelessly accesses the services, which is provided by the output system, over the wireless communication link wirelessly established in (5), based on having wirelessly provided the security information or the authentication information from the mobile information apparatus to the output system in (4).

95. This second wherein clause adds nothing that was unconventional by late 2000. It describes the result of performing the previous functions, namely that the mobile information apparatus accesses services of the output system. This is substantially the same result that would be achieved when a conventional PC successfully connects to a printer over the network. This language requires

“wirelessly” accessing the services of the output system, but, as I have explained, the ’031 patent discloses no new or improved wireless technologies. Additionally, a POSA would have known it was possible to use wireless networking to connect to output devices such as printers in 2000. *See supra* ¶¶ 24-27 (discussing network printing).

**f. The elements of claim 1 as an ordered combination**

96. In my opinion, there is nothing unconventional in claim 1 when its claim elements are considered as an ordered combination. The mobile information apparatus discovers the output system, displays it, the user selects it, and a communication link to that system is established. The mobile information apparatus is given access to the services of the output system if it provides security or authentication information. All of this is consistent with the process I discussed above whereby a conventional Windows or Mac computer adds a network printer that requires a password.

97. Although claim 1 lists function (4) which involves sending the security or authentication information before function (5) which involves establishing the wireless communication link to the output system, I see nothing in the claim that requires the functions to be performed in this order. The ’031 patent specification describes establishing the communication link *before* the authentication information is provided. Specifically, the ’031 patent states that the

communication link between the information apparatus and the output device is “locked” at step 1112 of the discovery process shown in Fig. 11. ’031 patent at 32:37-43. The authentication step is described as being performed as part of the client application process shown in Fig. 12A. *Id.* at 36:12-49. The patent describes the client application process as coming after the discovery process as shown in Fig. 10.

## **2. Independent Claims 8, 14, 21, 28, and 34**

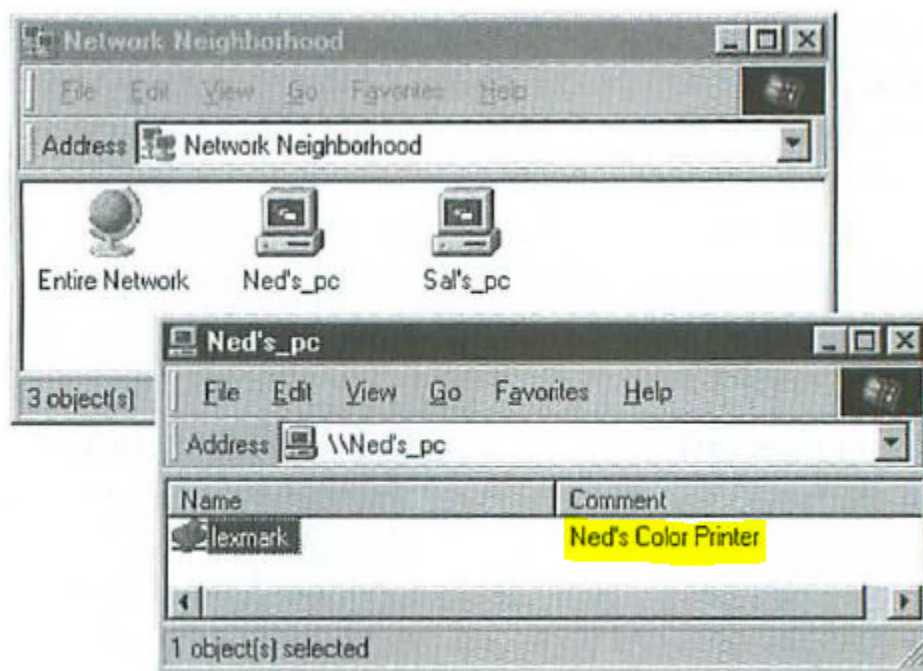
98. The five other independent claims of the ’031 patent are similar to claim 1. Although there are some differences between the claims that I discuss below, none of these claims require anything beyond routine and conventional computer technology at the time of the alleged invention.

### **a. Claims 8 and 28**

99. Claim 8 uses the term “mobile device” instead of “mobile information apparatus.” Just as I discussed for claim 1 in addressing its “mobile information apparatus,” the ’031 patent does not describe any new “mobile device” or suggest that the alleged invention works any differently when the information apparatus is a “mobile device” as opposed to a desktop computer.

100. Claim 8 adds an additional step, step (2), of “wirelessly receiving ... device information from the output system that has been wirelessly discovered by the mobile device” and then states that the information displayed to the user in step

(3) is “related, at least in part, to the device information wirelessly received from the output system in (2).” There was nothing unconventional about receiving information about a discovered device. In the Windows and Mac OS examples I discussed above, the user’s computer receives information including the name of the printer. In Windows, a comment about the shared printer is also displayed in Network Neighborhood:



*The Network Neighborhood shows network printers that you can add to the Printers folder.*

Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 134 (highlighting added); *see also id.* at 125 (“This name [in the Share Name field] will appear on other network users’ machines when they access your computer in their Network Neighborhood. In the comment field, you can type a phrase that describes the printer or its location. If you have more than one printer, this

comment will help users identify the printer.”). Mac OS allowed users to “Get Info” about a printer shown in the Chooser and see additional information, including the Mac OS version and computer type of its host computer and whether the selected printer includes the fonts on the user’s own machine. Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 141.

101. The discovery protocols and standards mentioned in the ’031 patent specification provided for obtaining device information about the discovered device. For example, UPnP included “description” functionality that control point devices could use to obtain information about controlled devices and their services:

Step 2 in UPnP networking is description. After a control point has discovered a device, the control point still knows very little about the device. For the control point ***to learn more about the device*** and its capabilities, or to interact with the device, the control point must ***retrieve the device's description*** from the URL provided by the device in the discovery message. Devices may contain other, logical devices, as well as functional units, or services. ***The UPnP description for a device*** is expressed in XML and ***includes vendor-specific, manufacturer information like the model name and number, serial number, manufacturer name, URLs to vendor-specific Web sites, etc.*** The description also includes a list of any embedded devices or services, as well as URLs for control, eventing, and presentation. For each service, the description includes a list of the commands, or actions, the service responds to, and parameters, or arguments, for each action; the description for a service also includes a list of variables; these variables model the state of the service at run time, and are described in terms of their data type, range, and event characteristics. The section on Description below explains how devices are described



and how those descriptions are retrieved by control points.

Appx U (*UPnP Specification v 1.0*, June 8, 2000) at 3. Bluetooth's service discovery protocol (SDP) also allowed client devices to request attributes from other devices they discovered. Appx. P at 337 ("Once an SDP client has a service record handle, it may easily request the values of specific attributes ..."); 351-353 (discussing service attribute requests and responses); 376-383 (example where SDP client requests and receives attributes such as the service name and service description). Similar to Bluetooth's SDP, SLP provides for attribute requests. Appx. V (Guttman, *Service Location Protocol: Automatic Discovery of IP Network Services*, 1999) at 79 ("A UA [user agent] can use the Attribute Request to retrieve all the attributes of a given service in a manner similar to a directory lookup operation.").

102. Claim 8 also recites that the user interface item displayed on the touch screen is related to the device information received from the output system. It was well understood that device information received from a discovered device might be displayed to the user to aid in the selection of a particular discovered device such as when more than one device is discovered. For example, when a user shared a printer in Windows, in addition to providing a printer name, the user could provide a comment about the printer to be viewed by another user to help them select the correct printer. Ex. 1012 (Poole, *The Little Network Book for*

*Windows and Macintosh*, 1999) at 125 (“This name [in the Share Name field] will appear on other network users’ machines when they access your computer in their Network Neighborhood. In the comment field, you can type a phrase that describes the printer or its location. ***If you have more than one printer, this comment will help users identify the printer.***”). As I mentioned above, the Bluetooth specification, describes an example of using SDP where “an SDP client is searching for available Synchronization services that can be presented to the user for selection.” Appx. P at 376. That discussion explains that “[t]he SDP client is retrieving ... those attributes that ***are relevant for presenting information to the user about the services.***” *Id.*

103. Claim 28 is similar to claims 1 and 8 discussed above. Like claim 1, it recites a “mobile information apparatus” and it requires receiving device information about the discovered output device similar to claim 8. Claim 28 lists the function of establishing the wireless communication link (function (4)) before the function of sending the security or authentication information (function (5)), but I see nothing in the claim that requires these two functions to be performed in the order they are listed.

104. In my opinion, claims 8 and 28 contain nothing that was not already routine and conventional by the time of the alleged invention.

**b. Claims 14, 21, and 34**

105. Claims 14, 21, and 34 are similar to the claims discussed above, but they do not require the client device to send security or authentication information to the output system in order to access its services. These claims add functions or steps that require the client device to send “first information or a query” to the output system and receive second “information or a response” back. Dependent claims 26 and 39 indicate that the claimed “second information” can be “status information, response information related to the first information, device attribute information, or user interface information, individually or in any combination.” There was certainly nothing unconventional by late 2000 about one device querying or exchanging information with another device over a network.

106. The '031 patent does not describe queries sent to the output system in any detail. The patent merely mentions that one of the possible functionalities of output device 220 may be “Components and operations to receive multiple requests or *queries* (e.g., a service request, a data query, an object or component query etc.) from a plurality of information apparatus 200 and *properly respond* to them by *returning* components, which may contain *data*, software, instructions, and/or objects.” '031 patent at 22:12-19. There is no description of any new approach or new technology needed or used in making or responding to these queries. Nor is there any meaningful discussion in the '031 patent regarding how

to request and receive “status information” or “user interface information.”

107. As I discussed above, UPnP included “description” functionality whereby devices would request and obtain device attribute information in an XML device description document. UPnP devices could also “query” other devices to receive “status information” about their services. *Id.* at 38 (“To determine the current value of a state variable, a control point may poll the service. Similar to invoking an action, a control point sends a suitable query message to the control URL for the service. In response, the service provides the value of the variable ....”). UPnP also allowed devices to request and receive “user interface information.” Appx. U at 3 (“Step 5 in UPnP networking is presentation. If a device has a URL for presentation, then the control point can retrieve a page from this URL, load the page into a browser, and depending on the capabilities of the page, allow a user to control the device and/or view device status.”).

108. Bluetooth enabled devices to request and receive device attribute information. For example, Bluetooth provided a request to obtain the user-friendly name of another Bluetooth device. Appx. P at 207 (“LMP supports name request to another Bluetooth device. The name is a user-friendly name associated with the Bluetooth device ....”). As I discussed above, Bluetooth’s SDP discovery protocol allowed devices to request attribute information about the services of another Bluetooth device. *Id.* at 351-353 (discussing service attribute transactions). As I

also discussed above, Service Location Protocol (SLP)—also mentioned in the '031 patent—included functionality for allowing devices to request attribute information from other devices. Appx. V (Guttman, *Service Location Protocol: Automatic Discovery of IP Network Services*, 1999) at 79 (discussing “Attribute Requests”).

109. Additionally, Windows allowed users to receive status information for a network printer they were using. Appx. S (Person, *Using Windows 95: Special Edition*, 1995) at 784 (“You can check the print job status on both local and remote printers by using the Windows Printer Driver.”); *id.* (“To view the [network printer] queue, simply double-click the printer’s icon in the Printers folder or on the desktop. Windows displays the Printer Driver and print queue.”). A POSA would have known that the status information comes from the printer or its associated print server (*i.e.*, part of the “output system”). Mac OS included a PrintMonitor feature that showed status information, such as whether a print request was currently printing. Appx. T (Pogue, *Mac OS 9: The Missing Manual*, 2000) at 355-356.

110. Claim 14 requires the mobile information apparatus to “manag[e] or driv[e]” the output device and recites the sending of the first information or query as part of that process. The '031 patent does not clearly describe how an information apparatus “manages or drives” an output device, at least not in

technical terms. The Abstract of the '031 patent refers to “wirelessly managing or wirelessly setting up an output system,”<sup>5</sup> “management of settings of the output system” and “wirelessly driv[ing] or control[ling] the output system.”

111. Conventional Windows and Mac computers could “drive” or control networked printers to cause them to print selected documents, as I have discussed above. Client computers could also “manage” settings of networked printers. *See, e.g.,* Appx. S (Person, *Using Windows 95: Special Edition*, 1995) at 783 (discussing print quality issues when using a network printer: “Before printing, check the printer’s Properties sheet. Change the settings if required.... Change your printer’s properties and make test printouts to see how these changes affect the printouts.”); Appx. T (Pogue, *Mac OS 9: The Missing Manual*, 2000) at 357-362 (discussing user configuration of printer options).

112. Additionally, it was well understood that the discovery standards and protocols mentioned in the '031 patent could be used in scenarios where a device would command and/or control the discovered device. UPnP, for example, provided for one device (the control point) to control another (the controlled

<sup>5</sup> As I noted above in addressing similar language in the preamble of claim 1, the language here concerning “setting up an output system” seems to refer to setting up the output system for use by a given information apparatus, as opposed to setting up a new output system in the abstract (turning it on, connecting it to the network, etc.).

device). Appx. U (*UPnP Specification v.1.0*, June 8, 2000) at 3 (“Step 3 in UPnP networking is control. After a control point has retrieved a description of the device, the control point can send actions to a device’s service.”). As another example, Guttman describes using Service Location Protocol (SLP) to locate “an overhead projection server *to display a presentation.*” Appx. V at 74.

113. Claim 21 is similar to claim 14 but also requires the mobile information apparatus to receive device information about the discovered output system, similar to claims 8 and 28. As I discussed for claim 8, this added function of receiving device information about a discovered device was routine and conventional.

114. Claim 34 is similar to claims 14 and 21, except for its seventh step which adds the following:

(7) repeating any combination of steps or operations in (5) and in (6), by the mobile information apparatus, for the mobile information apparatus to wirelessly manage or wirelessly drive the output system without a need to repeat at least steps or operations in (1)—(4).

115. Essentially, this seventh step states that the mobile information apparatus can repeatedly send queries or information to and/or receive responses from the output system without having to repeat steps (1) - (4) which recite discovering the output system, selecting it, and establishing a wireless communication link to it.

116. The '031 patent explains that there are scenarios where the discovery process may be skipped:

The optional discovery process 1020 may sometimes be unnecessary. For example, a user may skip the discovery process 1020 if he or she already knows the output device (e.g., printer) 220 to which the output is to be directed. In this case, the user may simply connect the information apparatus 200 to that output device 220 by wired connections or directly point to that output device 220 in a close proximity such as in the case of infrared connectivity. As another example, a user may pre-select or set the output device or devices 220 that are used frequently as preferred defaults. As a result, the discovery process 1020 may be partially or completely skipped if the default output device 220 or printer is found to be available.

'031 patent at 29:46-58.

117. Both Windows and Mac OS allow users to add a network printer to their system which essentially designates it as a printer likely to be used to avoid having to repeat the discovery process later. Once the network printer is “added,” it did not need to be “discovered” again. *See* Ex. 1012 (Poole, *The Little Network Book for Windows and Macintosh*, 1999) at 133 (discussing Windows: “If your Printers folder already contains an icon for a shared printer that you want to use, you’re all set. You can begin printing to this printer whenever you like.”); *id.* at 141 (discussing Mac: “When you finish selecting a driver, selecting a specific printer, and doing the necessary printer setup, you should close the Chooser. The printer you selected is now the default printer and will be used by Page Setup and



Print commands in all Mac applications.”).

118. The discovery standards and protocols mentioned in the '031 patent included the same functionality. In UPnP, for example, service announcements and responses to discovery searches included “CACHE-CONTROL” information to specify how long the information is valid in cache. Appx. U (*UPnP Specification v1.0*, June 8, 2000) at 11, 15. The UPnP specification states that the cache control window should be at least 30 minutes. *Id.* The idea here is that if device A learns about the services of device B, device A can cache that information to avoid having to re-discover the same device / service at least for a period of time (*e.g.*, 30 minutes).

119. Service Location Protocol (SLP) included similar functionality via the “lifetime” field specified when a service URL is advertised. Appx. W (RFC 2165, 1997) at 19 (“The Lifetime field is set to the number of seconds the reply can be cached by any agent. A value of 0 means the information must not be cached. User Agents MAY cache service information, but if they do, they must provide a way for applications to flush this cached information and issue the request directly onto the network.”).

120. In my opinion, claims 14, 21, and 34 contain nothing that was not routine and conventional by the time of the alleged invention.

### **3. Dependent Claims**

121. In general, the dependent claims require particular types of devices (e.g., “smart phone”) or added functions that are mentioned or described in passing using functional language. None of the dependent claims adds any limitations that require any new or improved technology actually described in the ’031 patent.

#### **a. Claims 2, 3, 10, 15, 16, 22, 29, and 35**

122. All of these claims require use of either Bluetooth or IEEE 802.11 for wireless communications, or permit the use of either standard. As I discussed above, IEEE 802.11 and Bluetooth were well-known by the time of the alleged invention. *See supra* ¶¶ 15-16. As a result, these dependent claims add nothing that was not already routine and conventional.

#### **b. Claim 4**

123. Claim 4 recites that “the mobile information apparatus further synchronizes or exchanges information with the output system wirelessly discovered in (1).” With respect to “synchronizing,” the ’031 patent does not describe any new or improved approach to synchronizing information between the information apparatus and output system. The patent discusses synchronization only at a high level. *See, e.g.*, ’031 patent at 6:5-8 (“the client application in the information apparatus may be capable of communicating with, managing and synchronizing data or software components with an output device equipped with an output controller of present invention.”)

124. There was nothing unconventional about synchronizing or exchanging information with a device that has been discovered. As I discussed above in addressing independent claims 14, 21, and 34, the discovery standards and protocols mentioned in the '031 patent such as UPnP, Bluetooth, and SLP provided functionality that enabled devices to request and receive information from discovered devices. *See supra* ¶¶ 107-109. Accordingly, claim 4 adds nothing that was not already routine and conventional in my opinion.

**c. Claim 5**

125. Claim 5 recites that the mobile information apparatus is a smart phone or an information pad, that the output system includes at least one audio output device, and that the mobile information apparatus wirelessly transmits audio digital content to the output system for output at the output system:

The medium according to claim 2, wherein the mobile information apparatus is embodied as a smart phone or an information pad, and the output system includes at least one audio output device for outputting audio digital content, and wherein, subsequent to the mobile information apparatus having wirelessly provided the security information or the authentication information to the output system in (4), the mobile information apparatus is operable to access the services, provided by the output system, which include outputting, at the output system, audio digital content wirelessly received from the mobile information apparatus via the wireless communication link wirelessly established in (5).

126. The '031 patent describes no new technology related to anything

recited in claim 5. The '031 patent mentions smart phones and information pads as examples of information apparatuses (*see, e.g.*, '031 patent at 1:47-54), but never discusses these devices in any meaningful way. As I noted above, nothing in the '031 patent suggests that the invention works any differently when the information apparatus 200 is a smart phone as opposed to desktop or laptop computer.

127. As to wirelessly transmitting audio digital content, the '031 patent describes no new or improved way of doing this either. The patent does not describe audio digital content in any detail or how to transmit audio data any differently than any other type of output data. As I have discussed, the patent merely suggests the use of standard wireless technologies such as IEEE 802.11 and Bluetooth for wireless communication.

128. Accordingly, claim 5 adds nothing that was not already routine and conventional in my opinion.

**d. Claim 6**

129. Claim 6 recites that “the mobile information apparatus is embodied as a smart phone, and wherein the output system is at least one of a sound output system, a television system, an output controller connectable to a television, a projection system, a printing system, or an information apparatus that is at least an Internet appliance, individually or in any combination.” Again, with the exception of “a printing system,” these devices are not meaningfully described.

The '031 patent does not describe new or improved smart phones or televisions, for example.

130. Claim 6 also recites two additional functions performed after the mobile information apparatus sends the security or authentication information in step (4) of claim 1:

- (i) obtain, via the touch sensitive screen interface at the mobile information apparatus, the digital content for outputting at the output system; and

- (ii) wirelessly transmit, using the one or more wireless communication units of the mobile information apparatus and over the wireless communication link wirelessly established in (5), output data, related to the digital content obtained in (i), to the output system for processing or outputting at least part of the digital content at the output system; and wherein the wireless communication link wirelessly established in (5), using the one or more wireless communication units of the mobile information apparatus, is compatible with at least a protocol within IEEE 802.11 standards.

131. The two functions recited in claim 6 require using the touch screen to obtain digital content for output and wirelessly transmitting that digital content to the output system for output there. Neither of these functions requires anything more than routine and conventional computer technology.

132. As to the first function, the '031 patent does not describe any new way of obtaining digital content using a touch screen. The specification describes this functionality only at a very high level with functional language: “the client

application 210 may obtain a digital document from other applications 205 (e.g. document browsing application, content creation and editing application, etc.), or the client application 210 may provide its own capability for user to browse, edit and or select a digital document.” ’031 patent at 15:31-37. This generic description of obtaining a digital document from another application does not mention use of a touch screen and is consistent with the scenario where a user is browsing or creating a document in another application and takes some action to cause that document to be output (e.g., printed). Conventional applications like Microsoft Word provided this functionality for many years before the alleged invention. The alternative mechanism suggested in the specification (where client application 210 has its own document browsing and selection functionality) was also well-known. Many popular applications such as Microsoft Word had a File menu with an Open command that would allow a user to browse for a file and select it.

133. As to the second function, the ’031 patent does not describe any new or improved way to wirelessly transmit data to an output system. As I have discussed, the patent merely suggests the use of standard wireless technologies such as IEEE 802.11 and Bluetooth.

134. Accordingly, claim 6 adds nothing that was not already routine and conventional in my opinion.

**e. Claim 7**

135. Claim 7 recites that the mobile information apparatus is a “smart phone” and that it “wirelessly manages or wirelessly drives the output system using the one or more wireless communication units of the mobile information apparatus and via the wireless communication link in (5).”

136. As I discussed in addressing claim 4 above, the '031 patent describes no new technology related to smart phones. Smart phones are merely mentioned in passing as a possible type of information apparatus.

137. In discussing claim 14 above I discussed a similar limitation requiring the information apparatus managing or driving the output system. As I discussed, conventional Windows computers could drive output devices (*e.g.*, printers). In addition, it was well-understood that the discovery protocols mentioned in the '031 patent would be used in scenarios where one device would subsequently command or control the discovered device. *See supra* ¶¶ 110-112.

138. Accordingly, claim 7 adds nothing that was not already routine and conventional in my opinion.

**f. Claim 9**

139. Claim 9 recites the following:

The medium according to claim 8, wherein the wireless discovering of the output system in (1) is based, at least in part, on physical proximity between the mobile device and the output system, and wherein, subsequent to the

mobile device having wirelessly provided the security information or the authentication information to the output system in (5), the mobile device wirelessly accesses the output services provided by the output system over the wireless communication link wirelessly established in (6).

140. The first part of claim 9 which requires the discovery to be based on physical proximity between the mobile device and the output system is something I discussed above in addressing claim 1 which recites the same requirement. The '031 patent does not describe any new or improved way of accounting for “physical proximity” between the information apparatus and output system during discovery. If, as Flexiworld asserts, this limitation is satisfied when the output system is discovered on the same local area network, that would be consistent with well-known discovery protocols including those mentioned in the '031 patent. *See supra* ¶ 79.

141. The second part of claim 9 states that the mobile device wirelessly accesses output services of the output system after providing the security or authentication information. I addressed similar limitations above in addressing claim 1. After entering a password to access a restricted network printer, a Windows or Mac OS user could access the print services of the network printer. *See supra* ¶¶ 87-90.

142. Accordingly, claim 9 adds nothing that was not already routine and conventional in my opinion.



**g. Claim 11**

143. Claim 11 recites that, after providing the security or authentication information to the output system, the mobile device establishes a wireless LAN connection to the output system and uses that connection to transmit output data related to digital content to the output system for output.

144. There was nothing unconventional about establishing wireless LAN connections at the time of the alleged invention. The '031 patent acknowledges that “Bluetooth, Home radio frequency (Home RF) and implementations based on IEEE 802.11 standard ... all provide solutions for wireless local area networks (LANs).” '031 patent at 25:15-20. The patent also states that any of these wireless LAN standards can be used “in the present invention.” *Id.* at 25:23-27.

145. As to transmitting output data to the output system over a wireless LAN connection, '031 patent does not describe any new or improved way to transmit data over a wireless LAN to an output system.

146. Accordingly, claim 11 adds nothing that was not already routine and conventional in my opinion.

**h. Claim 12, 20, and 23**

147. Claim 12 recites that the mobile device is a smart phone and that the security or authentication information provided to the output system includes “one or more of a name, a password, identification information, an ID number, a PIN, an

IP address, a security key, biometric information, fingerprint information, or voice, individually or in any combination.”

148. As I discussed in addressing claim 4 above, the '031 patent describes no new technology related to smart phones. Smart phones are merely mentioned in passing as a possible type of information apparatus. There is nothing unconventional about the specific examples of security or authentication information listed in claim 12, either. User names (*i.e.*, “a name”) and passwords have traditionally been used to authenticate users. As I discussed above, Windows and Mac OS allowed printers to be restricted with passwords so that a user at a client device would have to input the password in order to utilize the printer. *See supra* ¶¶ 87-90.

149. Accordingly, claim 12 adds nothing that was not already routine and conventional in my opinion.

150. Claims 20 and 23 require the mobile information apparatus to send security or authentication information to access output services of the output device (claim 20) / output system (claim 23). This feature was routine and conventional as I discussed above for claim 1. *See supra* ¶¶ 87-90.

151. Claims 20 and 23 also require the security or authentication information to be one of the same examples listed in claim 12 (*e.g.*, “a name, a password, identification information”) which, as I just discussed in addressing

claim 12, was routine and conventional.

152. Accordingly, claims 20 and 23 add nothing that was not already routine and conventional in my opinion.

**i. Claims 13 and 31**

153. Claims 13 and 31 require that the mobile information apparatus is a “smart phone” or “information pad.” As I have discussed, the ’031 patent describes no new “smart phone” or “information pad” technology. These devices are only mentioned in passing as a possible type of information apparatus. The patent does not indicate that the alleged invention works any differently for these types of devices than for a laptop or desktop computer.

154. Claim 13 requires the output system to be “at least one of a sound output system, a television system, a controller system connectable to a television, or a projector system, individually or in any combination, for outputting the digital content that includes audio data or video data, individually or in combination.” Claim 31 includes similar requirements. As I have noted, the ’031 patent does not describe audio or video data in any meaningful way or describe these particular output devices beyond mentioning some of them when listing off possible types of output devices. Although “output controllers” are discussed generally and in connection with printers, there is no specific discussion in the ’031 patent of any “controller system connectable to a television.” Moreover, as I discussed above,

the patent confirms that output controllers can be implemented with conventional technology such as a “conventional personal computer (PC).”

155. Accordingly, claims 20 and 23 add nothing that was not already routine and conventional in my opinion.

**j. Claim 17**

156. Claim 17 recites:

The medium according to claim 16, wherein subsequent to the wireless discovery of the output device in (1), the mobile information apparatus further wirelessly receives, using the one or more wireless communication units of the mobile information apparatus, device information from the output device, the device information includes an attribute related, at least in part, to the output device wirelessly discovered in (1), and wherein the user interface item, displayed on the touch sensitive screen interface in (2), is related to the device information wirelessly received from the output device.

157. I addressed similar limitations above in discussing claim 8. *See supra*

¶¶ 100-102. For the same reasons, claim 17 adds nothing that was not already routine and convention in my opinion.

**k. Claims 18, 24, and 36**

158. These claims recite that the mobile information apparatus receives user selection of the output system via the touch screen prior to establishing the wireless communication link to the output system.

159. There is nothing unconventional about a user selecting an output system using a touch screen. As I discussed for claim 1, the '031 patent does not

even describe selection of the output system using a *touch screen* specifically. *See supra* ¶ 84. Nor is there anything unconventional about requiring the user to select a discovered output system prior to connecting to it. This is again consistent with the process used to add network printers in Windows and Mac OS.

### **I. Claim 19**

160. Similar to claims 13 and 31, claim 19 requires the mobile information apparatus to be a smart phone or an information pad, and requires the output device to be “at least one of a sound output device, a television device, a controller device connectable to a television, a projector device, or an Internet appliance, individually or in any combination.” The ’031 patent describes no new technology related to these types of devices; they are merely mentioned as possible information apparatuses or output devices.

161. Claim 19 also recites that the mobile information apparatus’ “software is either pre-installed, at least partly, at the mobile information apparatus or downloadable, at least partly, to the mobile information apparatus from the one or more servers accessible by the mobile information apparatus over a network.”<sup>6</sup> There was nothing unconventional about a mobile information apparatus having

<sup>6</sup> It is not clear what “servers” claim 19 is referring to when it references “the one or more servers accessible by the mobile information apparatus over a network.” Claim 19 depends from claim 15 which depends from independent claim 14. Neither claim 14 nor claim 15 mentions any servers.

“pre-installed” application software. Laptops and handheld computers were sold with pre-installed operating system software (*e.g.*, Windows, Windows CE) and, often, at least some pre-installed application software. For example, the user guide for the HP Jornada 600 Series states that “[y]our HP Jornada includes the full suite of software that you need to function as a mobile professional.” Appx. X at 5; *id.* at 5-8 (describing various pre-installed applications).

162. There was also nothing unconventional about downloading software from servers over a network. The background section of the '031 patent mentions that drivers (a type of software) can be downloaded over a network. '031 patent at 2:67-3:5 (“[A]lternatively, a user may be able to download a particular driver or application from a network.”). The '031 patent specification does not describe any particular way of downloading software from a server over a network, let alone any new or improved way of doing so. The '031 patent merely states that “information apparatus 200 may allow users to install additional hardware components and or application software 205 to expand its functionality.” *Id.* at 14:26-29. There is no discussion of any particular way of downloading software to *smart phones* or *information pads* specifically; again, these devices are merely mentioned as possible types of information apparatuses. In any event, by late 2000, laptops and some mobile computing devices would have been able to download software in a number of ways. For example, the JP Jornada 600 Series

User's Guide notes that some applications can be directly downloaded from the web and installed:

---

If a program is designed for direct installation, you may be able to download or install the program from the Web to your HP Jornada. The Web site should provide instructions for installing the program.

---



Appx. X at 103.

163. Accordingly, claim 19 adds nothing that was not already routine and conventional in my opinion.

**m. Claims 25 and 37**

164. Claims 25 and 37 require the mobile information apparatus to be a smart phone or an information pad, and require the output system to include a television or an output controller that is wire connectable to a television. Again, the '031 patent describes no new technology related to any of these devices types; they are merely mentioned as possible information apparatuses or output devices.

165. Claims 25 also recites three additional functions:

(a) obtaining, by the software application running a the mobile information apparatus, audio or video digital content;

(b) wirelessly transmitting, using the one or more wireless communication units of the mobile information apparatus and over the wireless communication link wirelessly established in (4), and from the mobile information apparatus to the output system, output data

related to the audio or video digital content obtained by the software application in (a); and

(c) outputting, at the output device included in or connected to the output system, at least part of the audio or video digital content that is related, at least in part, to the output data wirelessly transmitted in (b) and that is obtained by the software application in (a).

Claim 37 recites three similar functions.

166. These functions do not require any technology that was not routine or conventional by the time of the alleged invention. As to function (a), the '031 patent does not describe any way of obtaining audio or video content on a mobile information apparatus, let alone on a “smart phone” or “information pad” as claimed. As I discussed above for claim 6, the discussion in the '031 patent as to how digital content is obtained by the information apparatus describes, in functional terms, approaches that were well-known and conventional. *See supra* ¶¶ 130-132.

167. As to function (b), the '031 patent describes no new way or improved way of transmitting any type of data to an output system; the patent merely suggests the use of standards such as IEEE 802.11 and Bluetooth.

168. As to function (c), the '031 patent does not describe any new or improved way of outputting audio or video digital content.

169. Accordingly, claims 25 and 37 add nothing that was not already routine and conventional in my opinion.



**n. Claim 26**

170. Claim 26 restricts the type of “second information” that is received from the output system in response to the mobile information apparatus sending the “first information” or “query” to the output system. Specifically, claim 26 recites that “the second information includes information that is related to at least one of the following: status information, response information related to the first information, device attribute information, or user interface information, individually or in any combination.”

171. The types of information recited in claim 26 are extremely generic. In addressing claims 14, 21, and 34, I explained that use of the discovery standards and protocols mentioned in the ’031 patent would involve receipt of status information, response information, device attribute information, and user interface information. *See supra* ¶¶ 105-109.

172. Accordingly, claim 26 adds nothing that was not already routine and conventional in my opinion.

**o. Claims 27 and 38**

173. Claim 27 adds a function (7) to claim 21:

(7) wirelessly sending, from the mobile information apparatus, using the one or more wireless communication units of the mobile information apparatus, and over the wireless communication link wirelessly established in (4), voice data to the output system, the voice data is related, at least in part, to a voice activated command

from the user operating the mobile information apparatus.

Claim 38 recites a very similar step.

174. The '031 patent does not describe a new or improved way of transmitting voice data from an information apparatus to an output system. The patent does not meaningfully discuss voice data specifically. Nothing in the '031 patent suggests that “voice data” should be transmitted any differently than document data. In terms of wireless data transmission, the '031 patent merely embraces standards such as IEEE 802.11 and Bluetooth.

175. The '031 patent does not describe any new technology related to voice activated commands either. That computers could be commanded by voice was well-known by the time of the alleged invention. Mac OS included voice command functionality called “PlainTalk.” Appx. T (Pogue, *Mac OS 9: The Missing Manual*, 2000) at 393-394 (“PlainTalk is what’s known as a command-and-control program. It lets you open programs, trigger AppleScripts, and click menu items by speaking their names.”).

176. Accordingly, claims 27 and 38 add nothing that was not already routine and conventional in my opinion.

**p. Claim 30**

177. Claim 30 recites displaying device information received from the output device on the touch screen prior to receiving user selection of the output

device. This functionality was routine and conventional as I discussed above in addressing claim 1.

178. Claim 30 also recites two functions:

- (i) obtaining, by the mobile information apparatus, digital content for output; and

- (ii) wirelessly transmitting, using the one or more wireless communication units of the mobile information apparatus and over the wireless communication link established in (4), output data related to the digital content obtained in (i), from the mobile information apparatus to the output device for processing or outputting at least part of the digital content at the output system.

179. These functions are very similar to those recited in claim 6 that I discussed above and are routine and conventional for the same reasons.

180. Accordingly, claim 30 adds nothing that was not already routine and conventional in my opinion.

**q. Claim 32**

181. Claim 32 recites that the output device is discovered “at least in part, based on physical proximity between the mobile information apparatus and output device.” I discussed this requirement above in addressing claim 1.

182. Claim 32 also requires the security or authentication information to “include[] one or more of a name, a password, identification information, an ID number, a PIN, an IP address, a security key, a biometric ID, a fingerprint, or a voice ID, individually or in any combination.” I discussed these examples of

security or authentication information above in addressing claims 12, 20, and 23.

183. Accordingly, claim 32 adds nothing that was not already routine and conventional in my opinion.

**r. Claim 33**

184. Claim 33 first recites that “the mobile information apparatus is further configurable to synchronize or exchange information with the output device, that is wirelessly discovered in (1), over the wireless communication link established in (4).” I addressed this limitation in discussing claim 4 above.

185. Claim 33 also recites the mobile information apparatus is configured to perform two additional functions:

- (a) wirelessly send, using the one or more wireless communication units of the mobile information apparatus and via the wireless communication link wirelessly established in (4), first information or a query to the output device; and

- (b) wirelessly receive, using the one or more wireless communication units of the mobile information apparatus and via the wireless communication link wirelessly established in (4), second information or a response from the output device, the second information or the response wirelessly received from the output device is in response to the mobile information apparatus having wirelessly sent the first information or the query to the output device in (a).

I addressed these functions in discussing claims 14, 21, and 34 above.

186. Accordingly, claim 33 adds nothing that was not already routine and conventional in my opinion.

s.      **Claim 39**

187. Claim 39 recites two additional steps to the method of claim 34 performed by the mobile information apparatus:

wirelessly synchronizing, by the mobile information apparatus, software or data between the mobile information apparatus and the output system over the wireless communication link wirelessly established in (4); and

wherein the second information includes information that is related to at least one of status information, response information related to the first information, device attribute information, or user interface information, individually or in any combination.

188. As to the first step, a step of synchronizing software or data between the information apparatus and output system is described, for example, in Appl. No. 13/710,299 (“’299 application”) which is incorporated by reference into the ’031 patent. The application describes “synchronization” of output device information to aid the user in selecting an output device. Ex. 1009 (’299 application) at [0117] (“Based on the information provided and obtained in the service negotiation process 514, the user may choose one or more output devices 140 that can take the print or output job.”); *see also id.* at [0116] (giving examples of output device information that may be synchronized). As I discussed above in addressing claim 8, receiving device information in connection with discovery was routine and conventional. *See supra* ¶¶ 100-101.

189. As for synchronizing *software*, the ’031 patent specification itself

states only that “The client application in the information apparatus may be capable of communicating with, managing and synchronizing data or software components with an output device equipped with an output controller of present invention.” ’031 patent at 6:5-8. The ’031 patent does not discuss what software is synchronized between these devices. The ’299 application, however, discusses a “synchronization” process to download a “device driver, printer driver, application software, software components, ... user interface etc.” Ex. 1009 (’299 application) at [0119]. To the extent the claim 39 is referring to this kind of synchronization of software including drivers, it was well-known that drivers for printers could be installed on print servers to enable them to be downloaded by clients as needed. When Windows NT servers was set up as a print server for a network printer, the printer installation process included installing drivers for the various operating systems of client computers expected to access the printer. Appx. K (Frisch, *Essential Windows NT Systems Administration*, 1998) at 262-263 (“The lower portion of this dialog box is used to install printer drivers for other operating systems that may be downloaded to such systems as needed ....”); *see also* Appx. S (Person, *Using Windows 95: Special Edition*, 1995) at 776 (describing use of Add Printer Wizard to add a network printer: “The Wizard accesses the selected printer and determines whether its server can download an appropriate printer driver. If a driver is available, the Wizard automatically loads the driver and sets a

default configuration for the printer.”).

190. As to the second step, the types of information recited are generic. In addressing claims 14, 21, and 34 above, I explained that use of the discovery standards and protocols mentioned in the '031 patent would involve receipt of status information, response information, device attribute information, and user interface information. *See supra* ¶¶ 105-109.

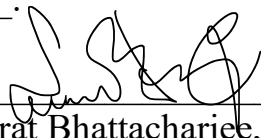
191. Accordingly, claim 39 adds nothing that was not already routine and conventional in my opinion.

#### IV. CONCLUSION

192. I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on August 24, 2021 in Silver Spring, MD.

By: \_\_\_\_\_

  
Samrat Bhattacharjee, Ph.D.



# APPENDIX A

CURRICULUM VITAE  
BOBBY BHATTACHARJEE  
DEPARTMENT OF COMPUTER SCIENCE  
THE UNIVERSITY OF MARYLAND  
COLLEGE PARK

## 1 Personal Information

Professor,  
Computer Science Department and  
the Institute for Advanced Computer Studies,  
University of Maryland  
Appointed Fall, 1999.

Affiliate Professor,  
Department of Electrical and Computer Engineering,  
University of Maryland.

Alfred P. Sloan Research Fellow (2004–2006).

### 1.1 Education

- Ph.D. in Computer Science  
Georgia Institute of Technology, Atlanta, Georgia, Summer 1999  
Dissertation title: Active Networking: Architectures, Composition, and Applications  
Advisors: Kenneth L. Calvert and Ellen W. Zegura
- Bachelor of Science in Mathematics and Computer Science  
Georgia College and State University, Milledgeville, Georgia, Spring 1994  
Graduated *Summa Cum Laude* and Outstanding Department Major

### 1.2 Employment

Summer 2009 to present	Professor University of Maryland, College Park, Maryland
Summer 2005 to present	Associate Professor University of Maryland, College Park, Maryland
Fall 2006	Visiting Professor Max Planck Institut für Software Systems, Saarbrücken, Germany
Spring, Summer 2007	Visiting Researcher

	AT&T Labs, Florham Park, New Jersey
Fall 1999 to Spring 2005	Assistant Professor University of Maryland, College Park, Maryland
Fall 1995 to Summer 1999	Research Assistant Georgia Institute of Technology, Atlanta, Georgia
Summer 1998	Instructor Georgia Institute of Technology, Atlanta, Georgia
Summer 1997	Member of Technical Staff AT&T Labs, Florham Park, New Jersey
Summer 1995	Member of Technical Staff GTE Labs, Waltham, Massachusetts
Fall 1994 to Spring 1995	Teaching Assistant Georgia Institute of Technology, Atlanta, Georgia

## 2 Research, Scholarly, and Creative Activities

### 2.1 Chapters in Books

1. Gisli Hjálmtýsson and Samrat Bhattacharjee. “Control on Demand”, In *Proceedings of the First International Working Conference on Active Networks* volume 1653 of *Lecture Notes in Computer Science* (Stefan Covaci, editor), pages 315-329, Springer-Verlag, June 1999.
2. Pete Keleher, Samrat Bhattacharjee, and Bujor Silaghi. “Are Virtualized Overlay Networks Too Much of a Good Thing?”, *Peer-to-Peer Systems First International Workshop, Lecture Notes in Computer Science*, Vol. 2429, (Peter Druschel et. al. Editors) pages 225–231, Springer-Verlag, 2002.
3. Bobby Bhattacharjee, Sudarshan S. Chawathe, Vijay Gopalakrishnan, Peter J. Keleher, and Bujor D. Silaghi. “Efficient Peer-To-Peer Searches Using Result-Caching”, *Peer-to-Peer Systems II, Second International Workshop, IPTPS 2003, Lecture Notes in Computer Science*, Vol. 2735, (M. Frans Kaashoek and Ion Stoica, Editors), pages 225–236, Springer-Verlag, 2003.
4. Paolo Massa and Bobby Bhattacharjee. “Using Trust in Recommender Systems: an Experimental Analysis”, In *Second International Conference, iTrust 2004, Lecture Notes in Computer Science*, Vol. 2995 Jensen, Christian; Poslad, Stefan; Dimitrakos, Theo (Eds.), pages 221-235, Springer-Verlag, 2004.

5. Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. “Decentralized Message Ordering for Publish/Subscribe Systems”, *ACM/IFIP/Usenix 7th International Middleware Conference, Lecture Notes in Computer Science*, Vol. 4290 (Maarten van Steen and Michi Henning, Editors), pages 162–179, Springer-Verlag, 2006.
6. Misha Rabinovich and Bobby Bhattacharjee. “Overlay Networks and Resiliency”, in *Guide to Reliable Internet Services and Applications*, Charles R Kalmanek, Sudip Misra, and Y. Richard Yang (Editors). Springer-Verlag, 2010.

## 2.2 Articles in Refereed Journals

1. Kenneth L. Calvert, Samrat Bhattacharjee, Ellen W. Zegura, and James Sterbenz. “Directions in Active Networks”, *IEEE Communications Magazine*, No. 10, pages 72-78, 1998.
2. Samrat Bhattacharjee, Ellen W. Zegura, and Kenneth L. Calvert. “Active Networking and End-to-End Arguments”, *IEEE Network Magazine*, No. 3, pages 66-71, 1998.
3. Gisli Hjálmtýsson and Samrat Bhattacharjee. “Control on Demand - An Efficient Approach to Router Programmability”, *IEEE Journal on Selected Areas in Communications, JSAC*, Vol. 17, No. 9, pages 1549-1562, September 1999.
4. S. Bhattacharjee, W. C. Cheng, C.-F. Chou, L. Golubchik, and S. Khuller. “Bistro: a Platform for Building Scalable Wide-Area Upload Applications”, *ACM SIGMETRICS Performance Evaluation Review*, Vol. 28, No. 2, pages 29-35, September 2000.
5. Ellen W. Zegura, Mostafa Ammar, Zongming Fei, and Samrat Bhattacharjee. “Application-Layer Anycasting: A Server Selection Architecture and Use in Replicated Web Service”, *Transactions on Networking*, Vol. 8, Issue 4, pages 455-466, August 2000.
6. Suman Banerjee and Samrat Bhattacharjee. “Scalable Secure Group Communications over IP-multicast”, *IEEE Journal of Selected Areas in Communications, JSAC*, Vol. 20, No. 8, pages 1511 - 1527, October 2002.
7. U. Cetintemel, P. J. Keleher, B. Bhattacharjee, and M. J. Franklin. “Deno: A Decentralized, Peer-to-Peer Object-Replication System for Weakly-Connected Environments”, *IEEE Transactions on Computers*, Vol. 52, No. 7, pages 943–959, July 2003.
8. Suman Banerjee, Christopher Kommareddy, and Bobby Bhattacharjee. “Efficient Peer Location on the Internet”, *Computer Networks Journal*, Vol. 5:1, pages 5-17, 2004.
9. Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. “P5: A Protocol for Scalable Anonymous Communications”, *Journal of Computer Security*, Vol 13:6, pages 839-876, 2005.
10. Suman Banerjee, Christopher Kommareddy, Koushik Kar, Bobby Bhattacharjee, and Samir Khuller. “OMNI: An Efficient Overlay Multicast Infrastructure for Real-time Applications”, *Special Issue of Computer Networks on Overlay Distribution Structures and their Applications*, Vol 50:6, pages 826-842, 2005.

11. Rob Sherwood, Seungjoon Lee, and Bobby Bhattacharjee. “Cooperative Peer Groups in NICE”, *Computer Networks Journal, Special Issue on Management in P2P systems: Trust, Reputation and Security*, Vol 50:4, pages 523-544, 2006.
12. Tuna Guven, Chris Kommareddy, Richard J. La, Mark A. Shayman, and Bobby Bhattacharjee. “Measurement-Based Optimal Routing on Overlay Architectures for Unicast Sessions”, *Computer Networks Journal: Special issue on Network Modeling and Simulation*, Vol. 50, No. 12, pages 1938–1951, August 2006.
13. Suman Banerjee, Seungjoon Lee, Bobby Bhattacharjee, and Aravind Srinivasan. “Resilient Multicast using Overlays”, *IEEE/ACM Transactions on Networking*, Vol. 14, No. 2, pages 237–248, April 2006.
14. Ruggero Morselli, Bobby Bhattacharjee, Michael A. Marsh, and Aravind Srinivasan. “Efficient Lookup on Unstructured Topologies”, *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Peer-to-Peer Communications and Applications*, pages 62-72, 2007.
15. Jik-Soo Kim, Beomseok Nam, Peter Keleher, Michael Marsh, Bobby Bhattacharjee, and Alan Sussman. “Trade-offs in Matching Jobs and Balancing Load for Distributed Desktop Grids”, *Future Generation Computer Systems – International Journal of Grid Computing: Theory, Methods & Applications*, Vol. 25, No. 5, pages 415–424, 2008.
16. Seungjoon Lee, Bobby Bhattacharjee, Aravind Srinivasan, and Samir Khuller. “Efficient and Resilient Backbones for Multihop Wireless Networks”, *IEEE Transactions on Mobile Computing*, Vol 7:11, 2008.
17. T. Guven, R. La, M. Shayman, and B. Bhattacharjee. “A Unified Framework for Multipath Routing for Unicast and Multicast”, *IEEE/ACM Transactions on Networking*, Vol. 6:5, 2008.
18. Seungjoon Lee, Bobby Bhattacharjee, Suman Banerjee, Bo Han. “A Generic Framework for Efficient Geographic Routing in Wireless Networks”, *Elsevier Computer Networks*, Vol 54:5, 2010.
19. Bo Han, Lusheng Ji, Seungjoon Lee, Bobby Bhattacharjee, and Robert R. Miller. “Are All Bits Equal? – Experimental Study of IEEE 802.11 Communication Bit Errors”. *IEEE/ACM Transactions on Networking*, Vol. 20, No. 6, 2012.
20. V. Singh, M. Lentz, B. Bhattacharjee, R. J. La and M. A. Shayman. “Dynamic frequency resource allocation in heterogeneous cellular networks”. *IEEE Trans. on Mobile Computing (TMC)*. 2016.
21. Wagner, Justin and Paulson, Joseph N. and Wang, Xiao and Bhattacharjee, Bobby and Bravo, Hector Corrada, Privacy-Preserving Microbiome Analysis Using Secure Computation, *Bioinformatics*, 2016.
22. Suman Banerjee, Bobby Bhattacharjee, and Christopher Kommareddy. “Scalable Application Layer Multicast”, *Transactions on Networking*, Under revision, Submitted in 2002.

## 2.3 Articles in Refereed Conferences and Workshops

1. Ellen W. Zegura, Kenneth L. Calvert, and Bobby Bhattacharjee. “How to Model an Internetwork”, In *Proceedings of INFOCOM’96*, pages 594–602, 1996.
2. Bobby Bhattacharjee, Mostafa Ammar, Ellen Zegura, Viren Shah, and Zongming Fei. “Application-Layer Anycasting”, In *Proceedings of INFOCOM’97*, pages 1388–1396, Kobe, Japan, 1997.
3. Bobby Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “Active Networking and the End-to-End Argument”, In *Proceedings of ICNP’97*, pages 220–228, 1997.
4. Bobby Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “An Architecture for Active Networking”, In *Proceedings of IFIP TC6 Seventh International Conference on High Performance Networking’97*, pages 265–279, 1997.
5. Bobby Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “Self-Organizing Wide Area Network Caches”, In *Proceedings of INFOCOM’98*, pages 600–608, 1998.
6. Bobby Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “Reasoning about Active Networks”, In *Proceedings of ICNP’98*, pages 31–41, 1998.
7. Zongming Fei, Bobby Bhattacharjee, Ellen W. Zegura, and Mostafa Ammar. “A Novel Server Selection Technique for Improving the Response Time of a Replicated Service”, In *Proceedings of INFOCOM’98*, pages 783–791, San Francisco, CA, 1998.
8. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “Congestion Control and Caching in CANEs”, In *Proceedings of ICC’98, Workshop on Active Networks and Programmable Networks*, 1998.
9. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “LIANE — Composition for Active Networks”, *Computer Communications Workshop*, 1998.
10. Gisli Hjálmtýsson and Samrat Bhattacharjee. “Control on Demand”, *Proceedings of International Workshop on Active Networking*, Berlin, pages 315–329, 1999.
11. S. Merugu, S. Bhattacharjee, E. Zegura, and K. Calvert. “Bowman: A Node OS for Active Networks”. *Proceedings of IEEE Infocom*, pages 1127–1136, 2000.
12. Y. Chae, S. Merugu, E. Zegura, and S. Bhattacharjee. “Exposing the Network: Support for Topology Sensitive Applications”, *Proceedings of IEEE OpenArch*, pages 65–74, 2000.
13. Samrat Bhattacharjee, William Cheng, Chen-Fu Chou, Leana Golubchik, and Samir Khuller. “Bistro: A Platform for Building Scalable Wide-Area Upload Applications”, *Proceedings of PAWS Workshop*, 2000.
14. R. Jaegar, S. Bhattacharjee, J. K. Hollingsworth, R. Duncan, T. Lavian, and F. Travostino. “Integrating Active Networking and Commercial-Grade Routing Platforms”, *Usenix 2000 Workshop on Intelligence at the Edge*, 2000.

15. Suman Banerjee and Bobby Bhattacharjee. “Scalable Group Communication over IP Multicast”, In *Proceedings of the International Conference on Network Protocols*, pages 261–271, 2001.
16. Narendar Shankar, Christopher Komareddy, and Bobby Bhattacharjee. “Finding Close Friends over the Internet”, In *Proceedings of the International Conference on Network Protocols*, pages 301–311, 2001.
17. Matt Sanders, Ken Calvert, Bobby Bhattacharjee, Stephen Zabele, Mark Keaton, and Ellen Zegura. “Active Reliable Multicast on CANEs: A Case Study”, *IEEE OpenArch*, pages 49–62, 2001.
18. Suman Banerjee and Samrat Bhattacharjee. “Scalable Application-Layer Multicast for Content Distribution”, *Computer Communications Workshop*, 2001.
19. Suman Banerjee, Bobby Bhattacharjee, and Christopher Komareddy. “Scalable Application-Layer Multicast”, *Proceedings of ACM SIGCOMM*, pages 205–217, 2002.
20. Bobby Bhattacharjee, Matt Sanders, Shashidhar Merugu, Ken Calvert, and Ellen Zegura. “CANEs: An Execution Environment for Composable Services”, In *DARPA Active Networks Conference and Exposition (DANCE 2002)*, pages 255–267, 2002.
21. Laura Bright, Samrat Bhattacharjee, and Louiqa Raschid. “Supporting Diverse Mobile Applications with Client Profiles”, In *Proceedings of ACM Workshop on Wireless Mobile Multimedia (WoWMoM)*, pages 88–95, 2002.
22. Suman Banerjee, Christopher Komareddy, and Bobby Bhattacharjee. “Scalable Peer-Finding on the Internet”, *Proceedings of Globecom 2002*, pages 2217–2221, 2002.
23. Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. “P5: A Protocol for Scalable Anonymous Communications”, In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 58–70, 2002.
24. Pete Keleher, Samrat Bhattacharjee, and Bujor Silaghi. “Are Virtualized Overlay Networks Too Much of a Good Thing?”, *First International Workshop on Peer-to-Peer Systems (IPTPS’02)*, 2002.
25. Bujor Silaghi, Bobby Bhattacharjee, and Pete Keleher. “Routing in the TerraDir Directory Service”, *Proceedings of SPIE/ITCom 2002*, Vol. 4868-30, pages 42–53, 2002.
26. Suman Banerjee, Seungjoon Lee, Bobby Bhattacharjee, and Aravind Srinivasan. “Scalable Resilient Multicast”, *Proceedings of ACM SIGMETRICS*, pages 102–113, 2003.
27. K-T Kuo, S. Phuvoravan, B. Bhattacharjee, R. J. La, M. Shayman, and H. S. Chang. “On the Use of Flow Migration for Handling Short-term Overloads”, *IEEE Globecom*, pages 3108–3112, 2003.
28. Suman Banerjee, Christopher Komareddy, Koushik Kar, Bobby Bhattacharjee, and Samir Khuller. “Construction of an Efficient Overlay Multicast Infrastructure for Real-time Applications”, *Proceedings of IEEE Infocom*, pages 1521–1531, 2003.

29. Seungjoon Lee, Rob Sherwood, and Bobby Bhattacharjee. “Cooperative Peer Groups in NICE”, *Proceedings of IEEE Infocom*, pages 1272–1282, April 2003.
30. K-T Kuo, S. Phuvoravan, T. Guven, L. Sudarsan, H. S. Chang, S. Bhattacharjee, and M. A. Shayman. “Fast Timescale Control for MPLS Traffic Engineering”, *Proceedings of Globecom 2003*, pages 3108–3114, 2003.
31. Bobby Bhattacharjee, Sudarshan Chawathe, Vijay Gopalakrishnan, Pete Keleher, and Bujor Silaghi. “Efficient Peer-To-Peer Searches Using Result-Caching”, *Second International Workshop on Peer-to-Peer Systems (IPTPS’03)*, 2003.
32. Ruggero Morselli, Jonathan Katz, and Bobby Bhattacharjee. “A Game-Theoretic Framework for Analyzing Trust-Inference Protocols”, *In the Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems*, June 2004.
33. Bujor Silaghi, Pete Keleher, and Bobby Bhattacharjee. “Multi-Dimensional Quorum Sets for Read-Few Write-Many Replica Control Protocols”, *In Proceedings of the IEEE/ACM CCGRID, 4th Fourth International Workshop on Global and Peer-to-Peer Computing (GP2PC)*, April 2004.
34. Suman Banerjee, Seungjoon Lee, Ryan Braud, Bobby Bhattacharjee, and Aravind Srinivasan. “Scalable Resilient Media Streaming”, *In Proceedings of ACM NOSSDAV’04*, pages 4–9, 2004.
35. Seungjoon Lee, Suman Banerjee, and Bobby Bhattacharjee. “The Case for a Multi-hop Wireless Local Area Network”, *In Proceedings of IEEE Infocom*, pages 894–905, 2004.
36. T.Guven, C. Kommareddy, R.J. La, M.A. Shayman, and B. Bhattacharjee. “Measurement Based Optimal Multi-path Routing”, *In Proceedings of IEEE Infocom*, pages 187–196, March 2004.
37. Ruggero Morselli, Bobby Bhattacharjee, Jonathan Katz, and Pete Keleher. “Trust-Preserving Set Operations”, *In Proceedings of IEEE Infocom*, pages 2231–2241, March 2004.
38. Rob Sherwood, Ryan Braud, and Bobby Bhattacharjee. “Slurpie: A Cooperative Bulk Data Transfer Protocol”, *In Proceedings of IEEE Infocom*, pages 941–951, March 2004.
39. V. Gopalakrishnan, B. Silaghi, B. Bhattacharjee, and P. Keleher. “Adaptive Replication in Peer-to-Peer Systems”, *In Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 360–369, March 2004.
40. David Hovemeyer, Jeff Hollingsworth, and Bobby Bhattacharjee. “Running on the Bare Metal with GeekOS”, *In Proceedings of the Technical Symposium on Computer Science Education (SIGCSE)*, pages 315–319, March 2004.
41. Bujor Silaghi, Vijay Gopalakrishnan, Bobby Bhattacharjee, and Pete Keleher. “Hierarchical Routing with Soft-State Replicas in TerraDir”, *In Proceedings of the 18th IPDPS Conference*, pages 48–57, April 2004.



42. Rob Sherwood, Bobby Bhattacharjee, and Ryan Braud. “Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse”, *Proceedings of Computer and Communications Security (CCS)*, pages 383–392, 2005.
43. Ruggero Morselli, Bobby Bhattacharjee, Michael A. Marsh, and Aravind Srinivasan. “Efficient Lookup on Unstructured Topologies”, *Principles of Distributed Computing*, pages 77–86, 2005.
44. Seungjoon Lee, Bobby Bhattacharjee, and Suman Banerjee. “Efficient Geographic Routing in Multihop Wireless Networks”, *ACM MobiHoc 2005*, pages 230–241, 2005.
45. T. Guven, R. J. La, M. Shayman, and B. Bhattacharjee. “Measurement-based Multipath Multicast,” *In IEEE Global Internet Symposium*, pages 2803–2808, 2005.
46. Vahid Tabatabaee, Bobby Bhattacharjee, Richard La, and Mark Shayman. “Differentiated Traffic Engineering for QoS Provisioning”, *In the Proceedings of INFOCOM’05*, pages 2349–2359, 2005.
47. J. S. Kim, B. Nam, P. Keleher, M. Marsh, B. Bhattacharjee, and A. Sussman. “Resource Discovery Techniques in Distributed Desktop Grid Environments”, *Proceedings of the 7th IEEE/ACM International Conference on Grid Computing - GRID 2006*, pages 9–16, September 2006. *Best paper award*.
48. Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. “Decentralized Message Ordering for Publish/Subscribe Systems”, *ACM/IFIP/Usenix 7th International Middleware Conference*, 2006.
49. Abhishek Kashyap, Samrat Bhattacharjee, Richard La, Mark Shayman, and Vahid Tabatabaee. “Single-Path Routing of Time-varying Traffic”, *In the Proceedings of Globecom*, 2006.
50. Vasile Gaburici, Peter Keleher, and Bobby Bhattacharjee. “File System Support for Collaboration in the Wide Area”, *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 26–36, 2006.
51. J. H. Li, M. Yu, R. Levy, and B. Bhattacharjee. “A Scalable Key Management and Clustering Scheme for Ad Hoc Networks”, *Proceedings of InfoScale*, pages 28–38, Hong Kong, 2006.
52. Vijay Gopalakrishnan, Bobby Bhattacharjee, and Peter Keleher. “Distributing Google”, *In 2nd IEEE International Workshop on Networking Meets Databases (NetDB’06)*, pages 33–39, April 2006.
53. Dave Levin, Rob Sherwood, and Bobby Bhattacharjee. “Fair File Swarming with FOX”, *Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS’06)*, 2006.
54. Alan Mislove, Massimiliano Marcon, Krishna Gummadi, Peter Druschel, and Bobby Bhattacharjee. “Measurement and Analysis of Online Social Networks”, *In Proceedings of the ACM/Usenix Internet Measurement Conference (IMC 2007)*, pages 29–42, 2007.

55. Jik-Soo Kim, Peter Keleher, Michael Marsh, Bobby Bhattacharjee, and Alan Sussman. “Using Content-Addressable Networks for Load Balancing in Desktop Grids”, *In Sixteenth IEEE International Symposium on High-Performance Distributed Computing (HPDC)*, pages 189–198, 2007.
56. Vijay Gopalakrishnan, Ruggero Morselli, Bobby Bhattacharjee, Peter J. Keleher, and Aravind Srinivasan. “Distributed Ranked Search”, *14th Annual IEEE International Conference on High Performance Computing (HiPC)*, pages 7–20, 2007. *Best paper award*.
57. Animesh Nandi, Aditya Ganjam, Peter Druschel, T. S. Eugene Ng, Ion Stoica, Hui Zhang, and Bobby Bhattacharjee. “A Shared Control Plane for Overlay Multicast”, *Fourth Usenix Symposium on Networked Systems Design and Implementation (NSDI 2007)*, 2007.
58. Seungjoon Lee, Dave Levin, Vijay Gopalakrishnan, and Bobby Bhattacharjee. “Backbone Construction in Selfish Wireless Networks”, *Proceedings of SIGMETRICS*, pages 121–132, 2007.
59. Jik-Soo Kim, Beomseok Nam, Michael A. Marsh, Peter J. Keleher, Bobby Bhattacharjee, Derek Richardson, Dennis Wellnitz, and Alan Sussman. “Creating a Robust Desktop Grid using Peer-to-Peer Services”, *Proceedings of NSF Next Generation Software Workshop (NSFNGS)* (Appears with proceedings of IPDPS 2007), pages 1–7, 2007.
60. Vahid Tabatabaee, Abhishek Kashyap, Bobby Bhattacharjee, Richard La, and M. Shayman. “Robust Routing with Unknown Traffic Matrices”, *IEEE INFOCOM Minisymposiums*, pages 2336–2440, 2007.
61. Adam Bender, Neil Spring, Dave Levin, and Bobby Bhattacharjee. “Accountability as a Service”, *USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, 2007.
62. Dave Levin, Adam Bender, Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. “Boycotting and Extorting Nodes in an Internetwork”, *Workshop on the Economics of Networked Systems and Incentive-Based Computing*, 2007.
63. B. Bhattacharjee, R. Rodrigues, and P. Kouznetsov. “Secure Lookup without (Constrained) Flooding”, *Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS)*, 2007.
64. R. Rodrigues, P. Kouznetsov, and B. Bhattacharjee. “Large-Scale Byzantine Fault Tolerance: Safe but Not Always Live”, *In the Third Workshop on Hot Topics in System Dependability (HotDep’07)*, 2007.
65. Ruggero Morselli, Bobby Bhattacharjee, Jonathan Katz and Michael Marsh. “Exploiting Approximate Transitivity of Trust”, *In Fourth International Conference on Broadband Communications, Networks, and Systems, 2007 (BroadNets 2007)*, pages 515–524, 2007.
66. Jik-Soo Kim, Beomseok Nam, Michael Marsh, Peter Keleher, Bobby Bhattacharjee, and Alan Sussman. “Integrating Categorical Resource Types into a P2P Desktop Grid System”, *In Proceedings of the 9th IEEE/ACM International Conference on Grid Computing (Grid 2008)*, 2008.

67. Dave Levin, Katrina LaCurts, Neil Spring, and Bobby Bhattacharjee. "BitTorrent is an Auction: Analyzing and Improving BitTorrent's Incentives", *In Proceedings of Sigcomm*, 2008.
68. Alan Mislove, Hema Swetha Koppula, Krishna P. Gummadi, Peter Druschel, and Bobby Bhattacharjee. "Growth of the Flickr social network", *In Proceedings of the 1st ACM SIGCOMM Workshop on Social Networks (WOSN'08)*, Seattle, WA, 2008.
69. Dave Levin, Randolph Baden, Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. "Motivating Participation in Internet Routing Overlays", *In NetEcon 2008 (Workshop on the Economics of Networks, Systems, and Computation)*, 2008.
70. Bo Han, Lusheng Ji, Seungjoon Lee, Bobby Bhattacharjee, Robert R. Miller. "All Bits Are Not Equal – A Study of IEEE 802.11 Communication Bit Errors", INFOCOM 2009.
71. Bo Han, Lusheng Ji, Seungjoon Lee, Robert R. Miller, Bobby Bhattacharjee. "Channel Access Throttling for Overlapping BSS Management". IEEE ICC, June 2009.
72. Vijay Gopalakrishnan, Bobby Bhattacharjee, K. K. Ramakrishnan, Rittwik Jana, Divesh Srivastava. "CPM: Adaptive Video-on-Demand with Cooperative Peer Assists and Multicast." IEEE INFOCOM 2009.
73. Bo Han, Lusheng Ji, Seungjoon Lee, Robert Miller, Bobby Bhattacharjee, "Channel Access Throttling for Improving WLAN QoS", IEEE Secon, Rome, Italy, June 2009
74. Cristian Lumezanu and Randy Baden and Dave Levin and Neil Spring and Bobby Bhattacharjee, "Symbiotic Relationships in Internet Routing Overlays", Usenix-NSDI, 2009.
75. Cristian Lumezanu and Randy Baden and Neil Spring and Bobby Bhattacharjee, "Triangle Inequality and Routing Policy Violations in the Internet", Passive and Active Measurement Conference (PAM), 2009.
76. Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, Daniel Starin, "Persona: An Online Social Network with User-Defined Privacy", Proceedings of SIGCOMM, August 2009
77. Cristian Lumezanu, Randolph Baden, Neil Spring, Bobby Bhattacharjee "Triangle Inequality Variations in the Internet", Proceedings of IMC, November 2009
78. Randy Baden, Neil Spring, Bobby Bhattacharjee "Identifying close friends on the Internet", The Workshop on Hot Topics in Networks (ACM Hotnets), 2009
79. Adam Bender, Rob Sherwood, Derek Monner, Nate Goergen, Neil Spring, Bobby Bhattacharjee, "Fighting Spam with the NeighborhoodWatch DHT", Proceedings of IEEE INFOCOM, April 2009
80. Cristian Lumezanu, Randolph Baden, Dave Levin, Neil Spring, Bobby Bhattacharjee, "Symbiotic Relationships in Internet Routing Overlays", Proceedings of USENIX NSDI, April 2009

81. Animesh Nandi, Bobby Bhattacharjee, Peter Druschel, “What a mesh: understanding the design tradeoffs for streaming multicast”, Extended Abstract, ACM SIGMETRICS Performance Evaluation, 2009.
82. Bo Han, Aaron Schulman, Francesco Gringoli, Neil Spring, Bobby Bhattacharjee, Lorenzo Nava, Lusheng Ji, Seungjoon Lee, and Robert Miller, “Maranello: Practical partial packet recovery for 802.11”, Proceedings of USENIX NSDI 2010.
83. Cristian Lumezanu, Dave Levin, Bo Han, Neil Spring, and Bobby Bhattacharjee, “Don’t love thy nearest neighbor”, International Workshop on Peer-to-Peer Systems (IPTPS), April 2010.
84. Cristian Lumezanu, Katherine Guo, Neil Spring, Bobby Bhattacharjee, “The Effect of Packet Loss on Redundancy Elimination in Cellular Wireless Networks”, ACM Sigcomm Internet Measurement Conference (IMC), 2010.
85. Satinder Pal Singh, Randolph Baden, Choon Lee, Bobby Bhattacharjee, Richard J. La, Mark Shayman, “IP Geolocation in Metropolitan Areas”, Extended Abstract, Proceedings of ACM Sigmetrics, 2011.
86. Matthew Lentz, Dave Levin, Jason Castonguay, Neil Spring, Bobby Bhattacharjee, D-mystifying the D-root address change, IMC (International Measurement Conference), 2013.
87. Lentz, Matthew and Erdélyi, Viktor and Aditya, Paarijaat and Shi, Elaine and Druschel, Peter and Bhattacharjee, Bobby, ”SDDR: Light-Weight, Secure Mobile Encounters”, USENIX Security Symposium, 2014.
88. Aditya, Paarijaat and Erdélyi, Viktor and Lentz, Matthew and Shi, Elaine and Bhattacharjee, Bobby and Druschel, Peter, “EnCore: Private, Context-based Communication for Mobile Social Apps”, International Conference on Mobile Systems, Applications, and Services (MobiSys), 2014.
89. Aditya, Paarijaat and Bhattacharjee, Bobby and Druschel, Peter and Erdélyi, Viktor and Lentz, Matthew, Brave New World: Privacy Risks for Mobile Users, Workshop on Security and Privacy Aspects of Mobile Environments (SPME), 2014.
90. Dave Levin, Youndo Lee, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, Bobby Bhattacharjee “Alibi Routing” Proceedigs of ACM SIGCOMM, 2015.
91. Matthew Lentz, James Litton, Bobby Bhattacharjee “Drowsy Power Management” Proceedings of Symposium on Operating Systems Principles (SOSP), 2015.
92. Raul Herbster, Scott DellaTorre, Peter Druschel, Bobby Bhattacharjee. “Privacy Capsules: Preventing Information Leaks by Mobile Apps” Proceedings of Mobisys, 2016.
93. Paarijaat Aditya, Rijurekha Sen, Seong Joon Oh, Rodrigo Benenson, Bobby Bhattacharjee, Peter Druschel, Tongtong Wu, Mario Fritz, Bernt Schiele. “I-Pic: A Platform for Privacy-Compliant Image Capture” Proceedings of Mobisys, 2016.

94. Vaibhav Singh, Matthew Lentz, Bobby Bhattacharjee, Richard La, Mark Shayman.
95. ‘Dynamic Frequency Resource Allocation in Heterogeneous Cellular Networks’
96. roceedings of IEEE TMC 2016 (IEEE Transactions on Mobile Computing)
97. James Litton, Anjo Vahldiek-Oberwagner, Eslam Elnikety, Deepak Garg, Bobby Bhattacharjee, Peter Druschel “Light-weight Contexts: An OS Abstraction for Safety and Performance” Proceedings of OSDI, 2016.
98. Zhihao Li, Dave Levin, Neil Spring, Bobby Bhattacharjee profile imageBobby Bhattacharjee. “Internet anycast: performance, problems, and potential” Proceedings of SIGCOMM, 2018.
99. Matthew Lentz, Rijurekha Sen, Peter Druschel, Bobby Bhattacharjee. “SeCloak: ARM TrustZone-based Mobile Peripheral Control” Proceedings of Mobisys 2018 (Conference on Mobile Systems, Applications, and Services)
100. Viktor Erdelyi, Trung-Kien Le, Bobby Bhattacharjee, Peter Druschel, Nobutaka Ono. “Sonoloc: Scalable positioning of commodity mobile devices.” In Proceedings of the Sixteenth International Conference on Mobile Systems, Applications, and Services (MobiSys 2018).
101. Lillian Tsai, Roberta De Viti, Matthew Lentz, Stefan Saroiu, Peter Druschel, Bobby Bhattacharjee. “enClosure: Group Communication via Encounter Closures” Proceedings of Mobisys 2019
102. Composing Abstractions using the null-Kernel James Litton, Deepak Garg, Peter Druschel, Bobby Bhattacharjee HotOS, 2019
103. Sergi Delgado-Segura, Surya Bakshi, Cristina Perez-Sola, James Litton, Andrew Pachulski Andrew Miller, Bobby Bhattacharjee “TxProbe: Discovering Bitcoin’s Network Topology Using Orphan Transactions” Financial Crypto, 2019
104. Venkat Arun, Aniket Kate, Deepak Garg, Peter Druschel, Bobby Bhattacharjee. “Finding Safety in Numbers with Secure Allegation Escrows” NDSS 2020 (to appear)

## 2.4 Technical Reports and Invited Papers

1. Ellen W. Zegura, Kenneth. L. Calvert, and Samrat Bhattacharjee. “Tera-op networking: Local adaptation to congestion”, In *Gigabit Networking Workshop*, 1996.
2. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. “Network Support for Multicast Video Distribution”, Technical Report GIT-CC-98-16, College of Computing, Georgia Institute of Technology, 1996.
3. Samrat Bhattacharjee. “Self-Organizing Wide-Area Network Caches”, Technical Report GIT-CC-97-31, College of Computing, Georgia Institute of Technology, 1996.

4. Zongming Fei, Samrat Bhattacharjee, Ellen W. Zegura, and Mostafa H. Ammar. "A Novel Server Selection Technique for Improving the Response Time of a Replicated Service", Technical Report GIT-CC-97-24, College of Computing, Georgia Institute of Technology, 1996.
5. Samrat Bhattacharjee, Mostafa Ammar, Ellen Zegura, Viren Shah, and Zongming Fei. "Application-Layer Anycasting", Technical Report GIT-CC-96-25, College of Computing, Georgia Institute of Technology, 1996.
6. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. "An Architecture for Active Networking", Technical Report GIT-CC-96-20, College of Computing, Georgia Institute of Technology, 1996.
7. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. "On Active Networking and Congestion", Technical Report GIT-CC-96-02, College of Computing, Georgia Institute of Technology, 1996.
8. Samrat Bhattacharjee, Ellen W. Zegura, and Kenneth L. Calvert. "High Performance Web: An Application for Wide Area Caching", In *Gigabit Networking Workshop*, 1997.
9. Samrat Bhattacharjee and Gisli Hjalmtysson. "Control-on-Demand: A Flow Oriented Approach towards Active Networking", *AT&T Labs Technical Memorandum*, 1997.
10. Samrat Bhattacharjee, Kenneth L. Calvert, and Ellen W. Zegura. "Improving the Quality of Best Effort Service", Technical Report GIT-CC-98-31, College of Computing, Georgia Institute of Technology, 1998.
11. S. Bhattacharjee and M. W. McKinnon. "Performance of Application-Specific Buffering Schemes for Active Networks", Technical Report GIT-CC-98-17, College of Computing, Georgia Institute of Technology, 1998.
12. S. Merugu, S. Bhattacharjee, Y. Chae, M. Sanders, K. Calvert, and E. Zegura. "Bowman and CANEs: Implementation of an Active Network", *Proceedings of the Thirty-Seventh Annual Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, September 1999 (invited paper).
13. Ugur Cetintemel, Peter J. Keleher, and Bobby Bhattacharjee. "A Security Infrastructure for Mobile Transactional Systems", University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4171, 2000.
14. Peter J. Keleher, Bobby Bhattacharjee, Kuo Kuo-Tung, and Ugur Cetintemel. "A Security Infrastructure for Mobile Transactional Systems", University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4077, 2000.
15. Suman Banerjee and Bobby Bhattacharjee. "Scalable Secure Group Communication over IP Multicast", University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4252, 2001.

16. Suman Banerjee and Samrat Bhattacharjee. “Spatial Clustering for IP Multicast: Algorithms and an Application”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4177, 2001.
17. Suman Banerjee and Bobby Bhattacharjee. “Analysis of the NICE Application Layer Multicast Protocol”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4380, 2002.
18. K-T Kuo, S. Phuvoravan, T. Guven, L. Sudarsan, S. Bhattacharjee, and M. A. Shayman. “Fast Time Scale Control for MPLS Traffic Engineering”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4351, 2002.
19. Suman Banerjee, Bobby Bhattacharjee, and Christopher Kommareddy. “Scalable Application Layer Multicast”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4373, 2002.
20. Bobby Bhattacharjee, Pete Keleher, and Bujor Silaghi. “The Design of TerraDir”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4299, 2002.
21. Suman Banerjee, Bobby Bhattacharjee, and Srinivasan Parthasarathy. “A Protocol for Scalable Application Layer Multicast”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4278, 2002.
22. Vijay Gopalakrishnan, Bujor Silaghi, Bobby Bhattacharjee, and Pete Keleher. “Adaptive Replication in Peer-to-Peer Systems”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4515, 2003.
23. Seungjoon Lee, Suman Banerjee, and Bobby Bhattacharjee. “The Case for a Multi-hop Wireless Local Area Network”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4504, 2003.
24. Christopher Kommareddy, Tuna Guven, Bobby Bhattacharjee, Richard La, and Mark Shayman. “Intradomain Overlays: Architecture and Applications”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4501, 2003.
25. Tuna Guven, Chris Kommareddy, Richard J. La, Mark A. Shayman, and Bobby Bhattacharjee. “Measurement Based Optimal Multi-path Routing”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4500, 2003.
26. Ruggero Morselli, Bobby Bhattacharjee, Jonathan Katz, and Pete Keleher. “Trust-Preserving Set Operations”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4499, 2003.
27. Suman Banerjee, Ryan Braud, Seungjoon Lee, Bobby Bhattacharjee, and Aravind Srinivasan. “Scalable Resilient Media Streaming”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4482, 2003.
28. Bujor Silaghi, Pete Keleher, and Bobby Bhattacharjee. “Multi-dimensional Quorum Sets for Read-Few Write-Many Replica Control Protocols”, University of Maryland, Dept. of Computer Science Technical Report, CS-TR-4440, 2003.

29. Tuna Guven, Richard La, Mark Shayman, and Bobby Bhattacharjee. “Measurement-based Multicast on an Overlay Architecture”, University of Maryland, Dept. of Computer Technical Report, CS-TR-4603, 2004.
30. Vijay Gopalakrishnan, Bobby Bhattacharjee, Sudarshan Chawathe, and Pete Keleher. “Efficient Peer-to-Peer Namespace Searches”, University of Maryland, Dept. of Computer Technical Report, CS-TR-4568, 2004.
31. Rob Sherwood, Bobby Bhattacharjee, and Ryan Braud. “Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4737, 2005.
32. Jik-Soo Kim, Bobby Bhattacharjee, Peter Keleher, and Alan Sussman. “Matching Jobs to Resources in Distributed Desktop Grid Environments”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4791, 2006.
33. Ruggero Morselli, Bobby Bhattacharjee, Jonathan Katz, and Michael Marsh. “Key-Chains: A Decentralized Public-Key Infrastructure”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4788, 2006.
34. Ruggero Morselli, Bobby Bhattacharjee, Michael Marsh, and Aravind Srinivasan. “Efficient Lookup on Unstructured Topologies”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4772, 2006.
35. Seungjoon Lee, Bobby Bhattacharjee, and Suman Banerjee. “Efficient Geographic Routing in Multihop Wireless Networks”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4625, 2006.
36. Vijay Gopalakrishnan, Ruggero Morselli, Bobby Bhattacharjee, Peter Keleher, and Aravind Srinivasan. “Ranking Search Results in Peer-to-Peer Systems”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4779, 2006.
37. Randy Baden, Adam Bender, Dave Levin, Rob Sherwood, Neil Spring, and Bobby Bhattacharjee. “A Secure DHT via the Pigeonhole Principle”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4884, 2007.
38. Jik-Soo Kim, Peter Keleher, Michael Marsh, Bobby Bhattacharjee, and Alan Sussman. “Using Content-Addressable Networks for Load Balancing in Desktop Grids”, University of Maryland, Dept. of Computer Science Technical Report CS-TR-4863, 2007.

## 2.5 Tutorials, Talks, Abstracts, and Other Professional Papers Presented

- *Privacy by Design*, NEC Labs, Princeton, November 2012.
- *Systems without Cooperation*, South China University of Technology, October 2008.
- *Systems without Cooperation*, Sichuan University, October 2008.
- *Systems without Cooperation*, University of Maryland, September 2008.



- *Decentralized Applications on the Internet*, University of Lisbon, Portugal, July 2006.
- *Decentralized Applications on the Internet*, Bell Labs, January 2006, Murray Hill, New Jersey.
- *An Overview of Decentralized Applications*, at the *Algorithms in Networking* Workshop, FSCCTS 2005, Hyderabad, India.
- *Security Architectures for Peer-to-Peer Applications*, at the Marconi Foundation Video P2P Conference, Columbia University, 2004, New York City, NY.
- *Replication and Search in Distributed Namespaces*, at IBM Research, 2004, Hawthorne, NY.
- Invited Panelist, *Network Security: How Good Does it Have to Be?* at IEEE INFOCOM, 2003, San Francisco, CA.
- *P5: A Protocol for Scalable Anonymous Communications*, at IEEE S&P, 2002, Oakland, CA.
- *Cooperative Peer Groups in NICE*, at IEEE INFOCOM, April 2003, San Francisco, CA.
- *Overlay and P2P Systems: Protocols, Applications, and Analysis*, Tutorial (with Dan Rubenstein) at Networking Group Communications (NGC '02), October 2002, Boston, MA.
- *Cooperative Peer Groups in NICE*, Invited talk at BBN Technologies, Cambridge, MA, October 2002.
- *Finding Close Friends over the Internet*, at the International Conference on Network Protocols (ICNP), 2001, Riverside, CA.
- *Adaptive Network Processing*, at the Washington University Gigabit Switch Seminar, Washington University at St. Louis, St. Louis, January, 2001.
- *Active Networks: A Possible Future for the Internet?*, Invited Talk to the Washington DC/Northern VA Chapter for the IEEE/Microwave Theory and Techniques Society, April 2000.
- Invited Panelist at Gigabit Networking Workshop, San Francisco, CA, 1998 and International Communications Conference, Atlanta, GA 1998.
- *LIANE - Composition for Active Networks*, at IEEE Computer Communications Workshop, September 1998, Oxford, MS.
- *Self-Organizing Wide Area Network Caches*, at IEEE INFOCOM 1998, San Francisco, CA.
- *Reasoning about Active Networks*, at ICNP 1998, Austin, TX.
- *Finding the Best Server within the Application-Layer Anycasting Architecture*, at IEEE INFOCOM 98, San Francisco, CA.

- *High Speed Web: An Application for Active Caching*. Presented at Gigabit Networking Workshop '97, March 1997, Kobe, Japan.
- *Application-Layer Anycasting*, at IEEE INFOCOM 1997, Kobe, Japan.
- *Active Networking and the End-to-End Argument*, at IEEE ICNP'97, Atlanta, GA.
- *Tera-Op Networking: Local Adaptation to Congestion*. Presented at Gigabit Networking Workshop '96, March 1996, San Francisco, CA.

## 2.6 Patents

1. *Scalable wide-area upload system and method*, Leana Golubchik, William C. Cheng, Samir Khuller, Samrat Bhattacharjee, and Cheng-Fu Chou. United States Patent # 7,181,623. Granted: February 20, 2007.
2. *Method for encoding frame data*, Lusheng Ji, Samrat Bhattacharjee, Bo Han, Seungjoon Lee, Robert Miller. United States Patent # 7,940,850. Granted: May 10, 2011.
3. *Detection of distributed denial of service attacks in autonomous system domains*, Chris Kommareddy, Samrat Bhattacharjee, Mark Shayman, Richard La. United States Patent # 8,397,284. Granted: March 12, 2013.

## 2.7 Contracts and Grants

1. "EAGER: Decomposing Operating Systems for Better Control over Policy and Privacy", *National Science Foundation*, PI,
2. "LTS - Securing Critical Networking Infrastructure: DNS Root Servers", *Department of Defense*, PI, (Co-PIs: Neil Spring and David Levin), 2014-2015, \$199,799.00
3. "Interference Management in Heterogeneous Networks", *Air Force Research Laboratory*, Co-PI, (PI: Mark Shayman), 2012-2013, \$358,054.
4. "University Partnership with the Laboratory for Telecommunications Science", *Department of Defense*, Co-PI, 2010-2013, (PI: Joseph Jaja) \$896,814.
5. "University Partnership with the Laboratory for Telecommunications Science", *Department of Defense*, Co-PI, 2010-2013, (PI: Joseph Jaja) \$496,228.
6. "Privacy Preserving Social Systems", *National Science Foundation*, PI, Co-PIs: Neil Spring, Jonathan Katz, 2010 – 2013, \$880,000.
7. "Greed Resistant Protocols", *National Science Foundation*, Co-PI, (PI: Neil Spring), 2009 – 2012, \$499,344.
8. "An Integrated Approach to Computing Capacity and Developing Efficient Cross-Layer Protocols for Wireless Networks", *National Science Foundation*, Co-PI, (Principal Investigator: Aravind Srinivasan), September 2006 – September 2009, \$365,000.

9. “A Postmodern Internetwork Architecture”, *National Science Foundation*, Co-PI, Principal Investigator: Neil T. Spring, September 2006 – September 2009, \$400,000.
10. “Robust Grid Computing using Peer-to-Peer Services”, *NASA*, Co-PI. Principal Investigator: Alan Sussman. Other co-PIs: P. Keleher, D. Richardson, February 2006 – February 2009, \$1,008,251.
11. “A Wide-Area Event Notification System for MENTER”, *Laboratory for Telecommunication Sciences, National Security Agency*, January 2001 – August 2008, \$625,000.
12. “Employing Peer-to-Peer Services for Robust Grid Computing”, Co-PI. Principal Investigator: Alan Sussman. Other co-PIs: P. Keleher, D. Richardson, September 2005 – August 2006, \$60,000.
13. “Resilient Storage and Querying in Decentralized Networks”, *National Science Foundation*, Principal Investigator (Co-PI: Aravind Srinivasan, Sudarshan Chawathe, Jonathan Katz, Michael Marsh), Fall 2004 – Fall 2007, \$720,000.
14. Alfred P. Sloan Jr. Fellowship, September 2004 – September 2007, \$40,000.
15. “Distributed Trust Computations for Decentralized Systems”, *National Science Foundation*, Principal Investigator (Co-PI: Jonathan Katz), Fall 2003 – Fall 2006, \$375,000.
16. “CAREER: Adaptive Network Processing”, *National Science Foundation CAREER Award*, Fall 2001 – Spring 2006, \$500,000.
17. “Decentralized Directories for the Internet”, *National Science Foundation*, Principal Investigator (Co-PI: P. Keleher), Fall 2001 – Spring 2004, \$710,000.
18. “Parametric Design of Embedded Real-Time Systems”, *National Science Foundation*, Principal Investigator, Summer 2002 – Summer 2003. (Original PI: Richard Gerber, Fall 1998 – Summer 2002), \$200,154.
19. *Washington University Gigabit Switch Kit*. NSF, Washington University at St. Louis, Fall 1999 (Equipment only).

## 2.8 Fellowships, Prizes and Awards

1. Department of Computer Science Faculty Award for Teaching Excellence, 2012.
2. Department of Computer Science Faculty Award for Teaching Excellence, 2008.
3. Best paper award, 14th Annual IEEE International Conference on High Performance Computing (HiPC), 2007; paper co-authored with Vijay Gopalakrishnan, Ruggero Morselli, Peter J. Keleher, and Aravind Srinivasan.
4. Best paper award, 7th IEEE/ACM Conference on Grid Computing, 2006; paper co-authored with Jiksoo Kim, Byomsuk Nam, Peter Keleher, Michael Marsh, and Alan Sussman.

5. Alfred P. Sloan Jr. Fellowship, 2004.
6. Department of Computer Science Faculty Award for Teaching Excellence, 2004.
7. NSF CAREER award, 2001.
8. Recipient of Distinguished Teaching Assistant award from College of Computing, Georgia Tech, Spring 1997.

## 2.9 Editorial Boards and Reviewing Activities for Learned Publications

Reviewer for

ACM/IEEE Transactions on Networking

IEEE Journal on Selected Areas in Communications

Computer Communications Journal (Special Issue on Network Security)

ACM Transactions on Computer Systems

Performance Evaluation Journal

Computer Communications Review

European Transactions on Telecommunications

IEEE Transactions on Parallel and Distributed Systems

ACM Transactions on Internet Technology

Virtually all conferences in Networking and Systems including SOSP, OSDI, SIGCOMM, Sigmetrics, INFOCOM, SCW, DISC (formerly WDAG), Global Internet Conference, Infocom, IC3N, ICDCS, ICNP, ICPP, ICS, OpenArch, and WWW.

## 2.10 Research Software

1. *Odyssey: An active networking platform.* This distribution includes complete source and documentation for the Bowman Node OS and the CANEs Execution Environment. Released on the Internet, Summer 1999.
2. *NICE protocol simulator.* This distribution includes source for simulators of the NICE multicast protocols and complete implementation of the NICE protocols for video multicast. Released on the Internet, 2002.
3. *Slurpie.* This distribution includes the entire source code for a file-swarming system. Released on the Internet, 2004.
4. *OptAck Random Segment skip patch.* This software fixes a protocol fault (for Linux kernel versions 2.4 and 2.6). The fault exists in all known versions of TCP. Released on the Internet, 2005.
5. *Local Minima Search (LMS).* LMS is a protocol for unstructured search using virtual namespaces in distributed environments. Released on the Internet, 2006.

6. *KeyChains PKI*. KeyChains is a web-of-trust public key distribution/discovery system; it is built based on LMS local minima search algorithm, and uses CODEX libraries (from Cornell). Released on the Internet, 2006.
7. *Distributed Grid Software* The Distributed Grid software implements a complete distributed job matching system. The software suite is currently being field tested by researchers in Astronomy, and is available upon request, 2007.
8. *Cryptographic library for Chit-based access*. Developed cryptographic library for “chit”-based security. Library is used for different chit-based applications, including a filesystem and a distributed calendar application. Code available upon request, 2007.
9. *CPM on-demand video service*. The CPM software includes a novel video server and associated client software (and other supporting code) for implementing Cooperative Peer-Assisted Multicasting. Co-implemented the full software suite at AT&T Research. Code available upon request, 2007.
10. *IBOBSP*. IBOBSP is an in-network platform targeted towards reducing latency in interactive applications (in particular, games). The software distribution includes the in-network server pieces, and several graphical test applications and games. Co-implemented the full IBOBSP suite at AT&T Research. Code available upon request, 2007.

## 3 Teaching

### 3.1 Teaching Awards and Other Special Recognition

1. Teaching Excellence Award for Faculty, Department of Computer Science, Spring 2008.
2. Teaching Excellence Award for Faculty, Department of Computer Science, Spring 2004.
3. Distinguished Teaching Assistant, College of Computing, Georgia Tech, Spring 1997.

### 3.2 Advising: Research Advisor

#### 3.2.1 Undergraduate

- Sebastian Gomez, Fall 2010 – Spring 2011.
- Chris Heistand, Fall 2010 – Spring 2011.
- Robert Kiefer, Spring 2009 – Summer 2010.
- Anika Cartas, Summer 2008 – Spring 2009.
- Katrina LaCurts, Fall 2007 – Summer 200.
- David Renie, Spring – Fall 2004.
- Ryan Evans Braud, Graduated Spring 2004.
- Mentor for Joseph Barrett, Colin Dixon, Tianzhou Duan, Kevin Genson, Bryant McIver, Ben Roseman, as part of the University of Maryland GEMSTONE program. Project title: *Anonymous Communications*, 2002-2005.

#### 3.2.2 Masters

- Randolph Baden, Spring 2008.
- Chunyuan Liao, Fall 2004.
- Vijay Gopalakrishnan, Spring 2003.
- Kuo-Tung Kuo, Spring 2003.
- Dave Hovemeyer, Fall 2001.
- Vaibhav Kumar (ECE), Spring 2001.
- William Shapiro, Spring 2000.

### 3.2.3 Doctoral (completed)

- Suman Banerjee, graduated Summer 2003. Current position: Assistant Professor at University of Wisconsin.
- Laura Bright, graduated Spring 2003 (co-advisor). Current position: Research Associate, Oregon Graduate Institute.
- Vijay Gopalakrishnan, graduated Summer 2006. Current position: MTS, AT&T Research.
- Seungjoon Lee, graduated Summer 2006. Current position: MTS, AT&T Research.
- Ruggero Morselli, graduated Summer 2006. Current position: MTS, Google Inc.
- Christopher Kommareddy, graduated Summer 2006. Current position: Researcher, Amazon, Inc.
- Rob Sherwood, graduated Summer 2008. Current position: MTS, Deutsche Telekom Labs.
- Adam Bender, graduated Fall 2010, Current Position: MTS, Google.
- Dave Levin, graduated Summer 2010, Current Position: Visiting Research Professor, University of Maryland.
- Randolph Baden, graduated Summer 2012, Current Position: MTS, LTS-NSA.

### 3.2.4 Doctoral (current)

- Matthew Lentz
- Yeongsam Park
- Kookjin Lee
- James Litton
- Also advised visiting Ph.D. student Paolo Massa (Univ. of Trento) during Winter 2003-2004

### 3.3 Advising: Ph.D. Committees

- Nikhil Swami, Expected July 2008.
- Arun Vasan, 2008.
- Stephen Birrer (Northwestern University), 2007.
- Tuna Guven (ECE), 2006.
- Wan, Yung Chun, 2005.

- Andrzej Kochut, 2005.
- Yoo Ah Kim, 2005.
- Mehdi Kalantari (ECE), 2005.
- Arunesh Mishra, 2005.
- Surapich Phuvoravan (ECE), 2003.
- Bujor Silaghi, 2003.
- Suman Banerjee, 2003.
- Laura Bright, 2003.
- Kaushik Kar (ECE), 2002.
- Sungjoon Ahn, 2001.
- Ugur Cetintemel, 2001.
- Gabriel Rivera, 2001.
- Cuneyt Akinlar, 2001.
- Jung-Min Kim, 2001.
- Kritchalach Thitikamol, 2000.
- Saswati Sarkar (ECE), 2000.
- Demet Aksoy, 2000.

## 4 Service

### 4.1 Professional

#### 4.1.1 Unpaid Reviewing Activities for Agencies

1. *NSF workshop on Network Testbeds*, attended workshop and co-authored report, 2002. Report basis for new NSF program on research testbeds.
2. NSF Networking Research Panel, Fall 2000, Fall 2001, Spring 2002, Fall 2002, Spring 2003, Spring 2004, Fall 2005, Spring 2008.
3. DoE High Performance Networking Panel, Spring 2001.
4. Evaluator for Intel Science Talent Search, 2001, 2002, 2003, 2004, 2005, 2007.



#### 4.1.2 Other non-University Panels and Positions

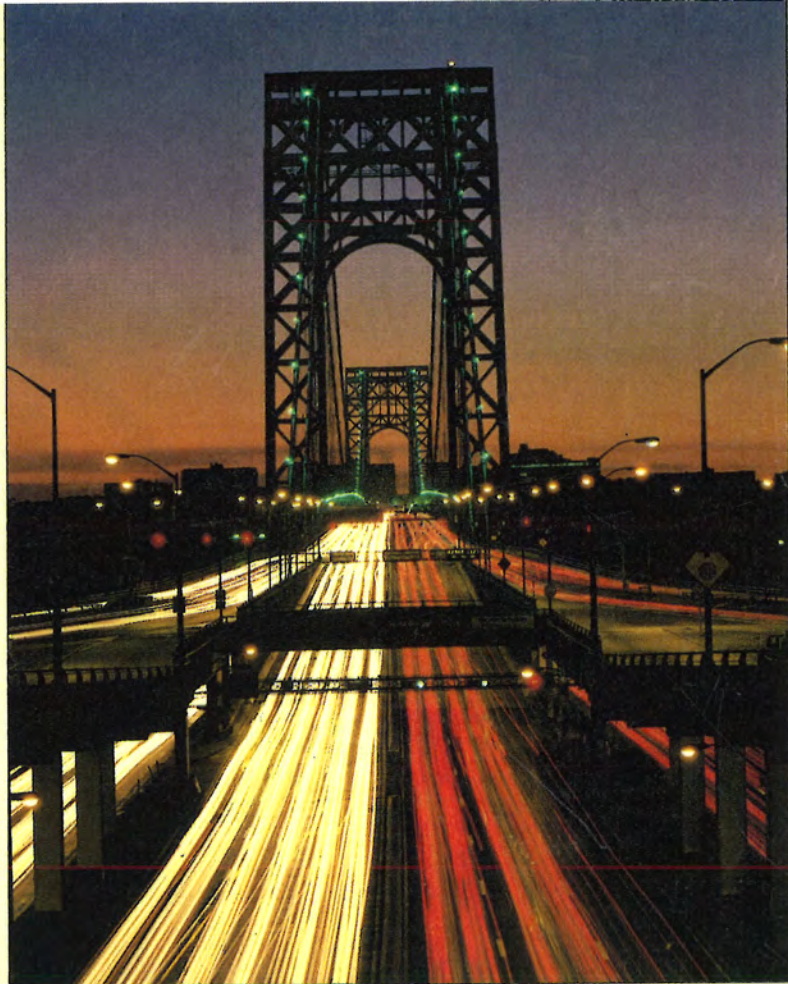
- Program Committee Member, W-PIN+Netecon, 2013.
- Program Committee Member, WWW, 2013.
- Program Co-Chair, IEEE ICNP 2012.
- Program Committee Member, IMC, 2011.
- Co-Chair, Internet Research Task Force (IRTF) Peer-to-Peer Research Group, 2003 – 2009.
- Member, Internet Research Steering Group (IRSG), 2003 – current.
- Co Program Committee Chair, NetEcon 2009 Workshop.
- Program Committee Member, INFOCOM, 2009.
- Program Committee Member, Sigmetrics, 2009.
- Program Committee Member, Area TPC Chair, ICNP, 2008.
- Program Committee Member, INFOCOM, 2008.
- Program Committee Member, LANMAN, 2008.
- Program Committee Member, Sigmetrics, 2008.
- Program Committee Member, Workshop on Social Network Systems, 2008.
- Program Committee Member, ACM SIGCOMM, 2007.
- Program Committee Member, NetDB, 2007.
- Program Committee Member, Sigmetrics, 2007.
- Program Committee Member, ICDCS (P2P track), 2007.
- Program Committee Member, ICNP (P2P track), 2007.
- Program Committee Member, Electronic Commerce (EC), 2007.
- Area Chair (Dependable and Trustworthy Computing), ICPADS, 2007.
- Program Committee Member, IEEE Consumer Communications and Networking Conference - Workshop on Peer-to-Peer Multicasting, 2007.
- Program Committee Member, IEEE INFOCOM, 2006.
- Associate Chair (P2P, Grids Track), Fifteenth International Conference on Computer Communications and Networks (IC3N), 2006.

- Associate Chair (P2P Track), The 26th International Conference on Distributed Computing Systems (ICDCS), 2006.
- Program Committee Member, Global Internet (GI), 2006.
- Program Committee Member, IWAN, 2006.
- Program Committee Member, ICNP, 2006.
- Program Committee Member, IEEE INFOCOM, 2006.
- Program Committee Member, The 25th International Conference on Distributed Computing Systems (ICDCS), 2005.
- Program Committee Member, International Workshop on Active Networking (IWAN), 2005.
- Program Committee Member, IEEE INFOCOM 2005.
- Program Committee Member, IPTPS, 2005.
- Program Committee Member, HICSS, 2005.
- Program Committee Member, ACM SIGCOMM, 2004.
- Program Committee Member, 6th International Workshop on Distributed Computing (IWDC), 2004.
- Program Committee Member, 24th International Conference on Distributed Computing Systems (ICDCS), 2004.
- Program Committee Member, IEEE Global Internet Conference, 2004.
- Program Committee Member, International Workshop on Active Networking (IWAN), 2004.
- Program Committee Co-Chair, OpenArch, 2003.
- Program Committee Member, IEEE International Conference on Network Protocols, 2003.
- Program Committee Member, IEEE OpenSig, 2003.
- Program Committee Member, International Workshop on Networked Group Communications (NGC), 2003.
- Program Committee Member, International Workshop on Active Networking (IWAN), 2003.
- Program Committee Member, IEEE Global Internet Conference, 2003.
- Program Committee Member, IEEE International Conference on Network Protocols, 2002.

- Program Committee Member, International Workshop on Networked Group Communications (NGC), 2002.
- Program Committee Member, IEEE Global Internet Conference, 2002.
- Program Committee Member, International Workshop on Active Networking (IWAN), 2002.
- Program Committee Member, IEEE International Conference on Network Protocols, 2001.
- Program Committee Member, Workshop on Performance and Architecture of Web Servers (PAWS), 2001.
- Publications Chair, Member of Organizing and Program Committee, IEEE/ACM Open-Arch, 2001.
- Program Committee member, IEEE Global Internet Conference, 2001.

# **APPENDIX B**

MACMILLAN NETWORK  
ARCHITECTURE &  
DEVELOPMENT SERIES



# WIRELESS LANs

---

*Implementing Interoperable Networks*

---

*Jim Geier*

ROKU EXH. 1002



# WIRELESS LANs

## *Implementing Interoperable Networks*

**Jim Geier** holds B.S.E. and M.S.E. degrees in electrical engineering, with an emphasis in computer networks. He was an active member of the IEEE 802.11 Working Group, responsible for developing international standards for wireless LANs. Jim has served as chairman of the Institute of Electrical and Electronic Engineers (IEEE) Computer Society, Dayton Section, and chairman of the IEEE International Conference on Wireless LAN Implementation. Jim has 18 years of experience providing information system consultation to companies worldwide, and has instructed many courses internationally on topics such as wireless networking, software development, and project management. He is currently the director of Data Collection Solution Development at Monarch Marking Systems. Jim is also the author of the *Wireless Networking Handbook* (1996, New Riders Publishing) and *Network Reengineering* (1996, McGraw-Hill), as well as numerous articles in leading publications, such as *Byte* and *Network Magazine*.

The *Macmillan Network Architecture and Development Series* is a comprehensive set of guides that provide computing professionals with the unique insight of leading experts in today's networking technologies. Each volume explores a technology or set of technologies that is needed to build and maintain the optimal network environment for any particular organization or situation.



CATEGORY: Networking

Wireless local area networks can provide unique benefits to many organizations, but require specific support and tools for maintaining network integrity. Based on the most recent developments in the field, *Wireless LANs*, gives network engineers, designers, and architects vital information on how to plan, configure, and implement wireless networks, including

- Coverage of the implications of migrating from proprietary solutions to the 802.11 standard
- Explanation of critical issues, such as maximizing interoperability between existing and future system infrastructure
- Authoritative advice on how to address common problems, such as radio frequency interference
- Discussion on how to realize significant cost savings through wireless LAN implementation for data collection systems
- Case studies and implementation notes, which provide real-world insight into the best practices of deploying a wireless LAN

This book provides both a context for understanding how an enterprise can benefit from the application of wireless technology, and the proven tools for efficiently implementing a wireless LAN. Designers and implementors will learn the considerations that must be addressed at each stage of the process, and find authoritative information on

- Primary wireless LAN applications, such as barcode scanners, data collectors, and printers
- The features and functionality of the IEEE 802.11 standard
- The details of upgrading from existing 902MHz to 2.4GHz networks
- Selecting the type of spread spectrum (direct sequence or frequency hopping) that best fits the needs of their particular networking environment

\$40.00 USA / \$57.95 CAN



ISBN 1-57870-081-7



ROKU EXH. 1002

# *Wireless LANs*

---

## *Implementing Interoperable Networks*

---

*Jim Geier*

**M**  
**TP**  
MACMILLAN  
TECHNICAL  
PUBLISHING  
U.S.A.



## Wireless LANs: Implementing Interoperable Networks

Copyright © 1999 by Macmillan Technical Publishing

### FIRST EDITION

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

International Standard Book Number: 1-57870-081-7

Library of Congress Catalog Card Number: 98-85498

2001 00 99 98 4 3 2 1

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit, the number of the book's printing. For example, the printing code 98-1 shows that the first printing of the book occurred in 1998.

*Composed in Bergamo and MCPdigital by Macmillan Computer Publishing*

*Printed in the United States of America*

### Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Macmillan Technical Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

### Warning and Disclaimer

This book is designed to provide information about wireless LAN technology. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an as-is basis. The authors and Macmillan Technical Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

### Feedback Information

At Macmillan Technical Publishing, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us at [networktech@mcp.com](mailto:networktech@mcp.com). Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

#### Publisher

*Jim LeValley*

#### Executive Editor

*Linda Ratts Engelman*

#### Managing Editor

*Caroline Roop*

#### Acquisitions Editor

*Karen Wachs*

#### Development Editor

*Thomas Curtin*

#### Project Editor

*Laura N. Williams*

#### Copy Editor

*Keith Cline*

#### Indexer

*Tim Wright*

#### Proofreader

*Julie Searls*

#### Acquisitions Coordinator

*Amy Lewis*

#### Manufacturing Coordinator

*Brook Farling*

#### Book Designer

*Gary Adair*

#### Cover Designer

*Sandra Schroeder*

#### Production Team Supervisor

*Tricia Flodder*

#### Production

*Eric S. Miller*



Supermarket scanners and most diffused infrared wireless LANs satisfy Class I requirements, where there is no hazard under any circumstance. Class IV specifies devices, such as laser-scalpels, which can cause grave danger if the operator handles them improperly. Most long-range, laser-based wireless networks are rated as Class III devices, whereby someone could damage his eyes if looking directly at the laser beam. Therefore, care should be taken when orienting lasers between buildings.

## The Components of a Wireless Network

Wireless networks perform similar functions as their wired ethernet and token ring counterparts. In general, networks perform the following functions to enable the transfer of information from source to destination:

1. The medium provides a bit pipe (path for data to flow) for the transmission of data.
2. Medium access techniques facilitate the sharing of a common medium.
3. Synchronization and error control mechanisms ensure that each link transfers the data intact.
4. Routing mechanisms move the data from the originating source to the intended destination.
5. Connectivity software interfaces an appliance, such as pen-based computer or bar code scanner, to application software hosted on a server.

A good way to depict these functions is to specify the network's architecture. This architecture describes the protocols, major hardware, and software elements that constitute the network. A network architecture, whether wireless or wired, may be viewed in two ways, physically and logically.

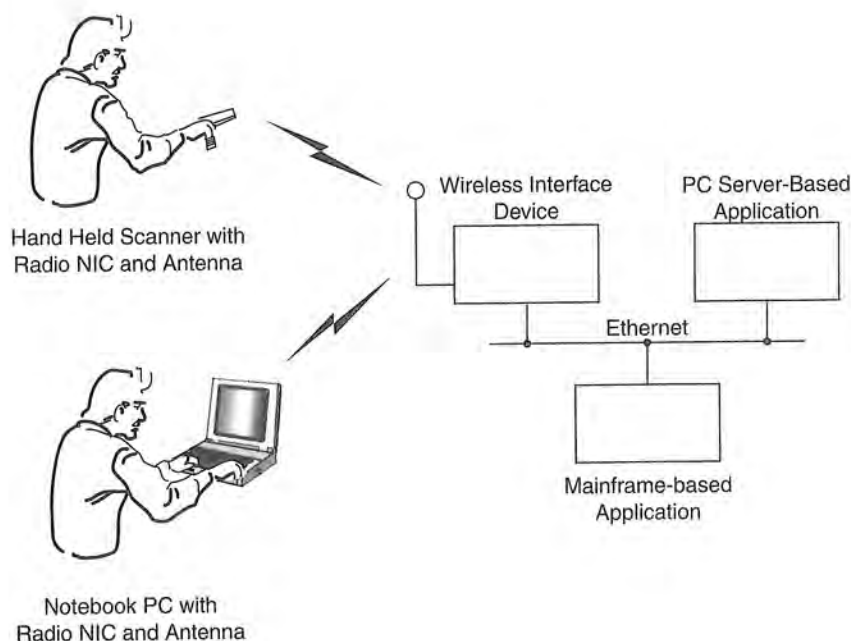
## Physical Architecture of a Wireless Network

The physical components of a wireless network implement the Physical, Data Link, and Network Layer functions (see Figure 1.7) to satisfy the functionality needed within local, metropolitan, and wide areas. The following sections explain the various components of a wireless LAN.

### End-User Appliances

As with any system, there needs to be a way for users to interface with applications and services. Whether the network is wireless or wired, an *end-user appliance* is an interface between the user and the network. Following are the classes of end-user devices that are most effective as appliances for wireless networks:

- Desktop workstations
- Laptop computers



**FIGURE 1.7** *The physical components of a wireless network extend the capability of ethernet and token ring.*

- Palmtop computers
- Handheld PCs
- Pen-based computers
- Personal digital assistants (PDA)
- Handheld scanners and data collectors
- Handheld printers

Today, the handheld PC, introduced by Microsoft (but developed and manufactured by other companies), is the primary hardware platform for Windows CE, which makes an excellent handheld wireless appliance. The main goals in developing the handheld PC include long battery life, affordable price (around \$500), compactness and light weight, familiar interfaces, easy PC connection, and effective keyboard input.

#### Note

*Microsoft, being mostly a software house, signed up seven partners to develop a variety of handheld PCs that provide common functionality and vendor-specific features that support Windows CE. These partners are Casio, Compaq, Hewlett-Packard, Hitachi, Phillips Electronics, NEC, and LG Electronics.*

Common features of handheld PCs include the following:

- Embedded QWERTY keyboard with alphanumeric keys, standard punctuation, a Ctrl key, an Alt key, and two Shift keys. Other vendor-specific keys are optional. A word of warning: If you have large fingers, you may have a difficult time pressing keys. Japanese and Chinese versions do not have keyboards; they have handwriting recognition as input.
- Embedded touch screen with resolutions of 480×240 or 640×240 pixels, four gray scales (2-bit pixel depth).
- Styles that acts like a mouse when tapped on the touch screen.
- Docking cradle to recharge the machine's batteries and connect it to your desktop PC.
- One PC Card (PCMCIA) slot, one serial connector, and one infrared port (IrDA).
- At least 2 MB RAM and 4 MB of ROM.

### **PalmPilot**

As an example of handheld PCs, consider the PalmPilot by 3Com. It is a pocket-size organizer designed to connect seamlessly with a Windows-based or Macintosh computer. This combination of portability and one-touch connectivity provides a practical way to carry personal data anywhere. The PalmPilot fits in a shirt pocket and contains a suite of personal information management (PIM) applications.

A touchscreen and physical buttons provide one-finger data access. The compact Palm Connected Operating System switches screens and launches applications instantly, yet is efficient enough that two AAA batteries can power the device for several months. The organizer contains a memory module that the user can replace to add memory or upgrade the device. In addition, users will be able to attach communications add-on products,

such as modems and pagers as they become available.

The PalmPilot drops into a docking station that is connected to the desktop by a serial cable. Pressing the HotSync button on the cradle automatically backs up and synchronizes data with the desktop. Because the desktop synchronization software runs in the background, the user does not need to manage the process on the desktop and viewer. As a result, synchronizing data requires less user interaction than printing a document.

The PalmPilot includes Microsoft Windows or Macintosh OS companion versions of applications. Desktop software serves as the gateway between PalmPilot and desktop applications. For example, a mail merge between the PalmPilot Address Book and Microsoft

*continues*

*continued*

Word is accomplished with a simple click-and-drag operation.

Because wireless network appliances are often put into the hands of mobile people who work outdoors, the appliance must be tough enough to resist damage resulting from dropping, bumping, moisture, and heat. Some companies offer more durable versions of the portable

computer. Itronix, for example, sells the X-C 6000 Cross Country portable computer. The X-C 6000's case is built from strong, lightweight magnesium and includes a elastomer covering that protects the unit from weather and shock. The unit is impervious to rain, beverage spills, and other work environment hazards.

### Note

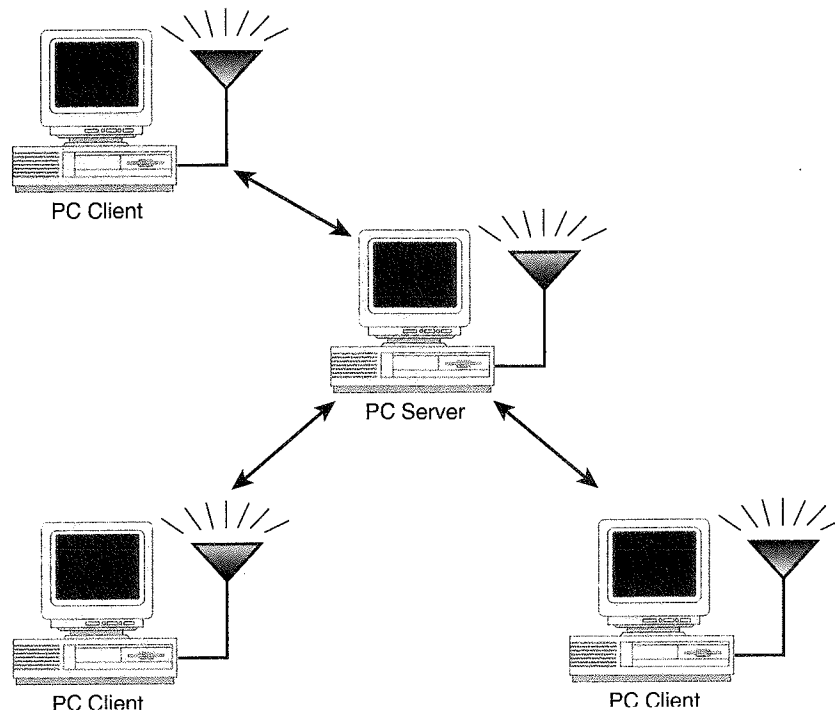
*When evaluating appliances for use with a mobile application, be certain to consider the ergonomics of the unit. You certainly won't be able to realize any of the benefits of a wireless network if users don't use the system because of appliances that weigh too much or are difficult to use.*

### Network Software

A wireless network consists of software that resides on different parts of the network. A network operating system (NOS), such as Microsoft NT Server, hosted on a high-end PC provides file, print, and application services. Many NOS's are server oriented, as shown in Figure 1.8, where the core application software and databases reside. In most cases, the appliances will interface via TCP/IP with application software or a database running on the NOS.

Client software, located on the end-user's appliance, directs the user's commands to the local appliance software, or steers them out through the wireless network. The software residing on a wireless appliance is very similar to software that runs on a wired appliance. The main difference is that it is important to develop the wireless software to optimize the use of the wireless network's relatively small amount of bandwidth.

The software performing application functions can run on a server/host, the appliance, or a combination of both. In some cases, such as with applications running on an IBM mainframe, IBM AS/400, or UNIX-based hosts, the wireless appliances may need to run terminal emulation. This makes the appliance act as a dumb terminal, just interfacing the keyboard, screen, printer, and so on, with the application running on the host. With client/server systems, the software on the appliance may perform part or all of the application's functionality and merely interface with a database located on a server, such as Microsoft NT Server. Chapter 6, "Wireless System Integration," covers this in more detail.



**FIGURE 1.8** The server-based network operating system provides a centralized platform for applications and data storage for mobile users.

#### Note

A wireless network appears transparent to application software and operating systems on the network. As a result, applications written for a wired network can generally run without changes over a wireless network.

In some cases, a gateway running *middleware* is necessary to provide an interface between the appliance and the application software running on the server. The appliances communicate with the host/server through the gateway. The gateway acts as a proxy for the various appliances. The advantages of using the gateway are as follows:

- *Better RF throughput:* With the presence of a transport and application gateway, the appliances communicate with the gateway by using a “lightweight” protocol that is wireless friendly, unlike TCP/IP.
- *Reliability:* Because the gateway proxies all the appliances, any outages in communication due to the appliances roaming out of range are transparent to the host/server.
- *Longer battery life:* When the appliances are idle, the network software does not have to periodically send out keep-alive packets to keep the connection to the host/server open. The gateway does this.



### Wireless Network Interface

Computers process information in digital form, with low direct current (DC) voltages representing data 1s and 0s. These signals are optimum for transmission within the computer, not for transporting data through wired or wireless media. A wireless network interface couples the digital signal from the end-user appliance to the wireless medium, which is air, to enable an efficient transfer of data between sender and receiver. This process includes the modulation and amplification of the digital signal to a form acceptable for propagation to the receiving location.

#### Note

*Modulation is the process of translating the baseband digital signal used in the appliance to an analog form suitable for transmission through the air. This process is very similar to the common telephone modem, which converts a computer's digital data into an analog form within the 4 KHz limitation of the telephone circuit. The wireless modulator translates the digital signal to a frequency that propagates well through the atmosphere. Of course wireless networks employ modulation by using radio waves and infrared light.*

The wireless network interface generally takes the shape of a wireless NIC or an external modem that facilitates the modulator and communications protocols. These components interface with the user appliance via a computer bus, such as ISA (Industry Standard Architecture) or PCMCIA (Personal Computer Memory Card International Association). The ISA bus comes standard in most desktop PCs. Many portable computers have PCMCIA slots that accept credit card-sized NICs. PCMCIA specifies three interface sizes: Type I (3.3 millimeters), Type II (5.0 millimeters), and Type III (10.5 millimeters). Some companies also produce wireless components that connect to the computer via the RS-232 serial port.

The interface between the user's appliance and NIC also includes a software driver that couples the client's application or NOS software to the card. The following driver standards are common:

- *NDIS (Network Driver Interface Specification)*: Driver used with Microsoft network operating systems
- *ODI (Open Datalink Interface)*: Driver used with Novell network operating systems
- *PDS (Packet Driver Specification)*: A generic DOS-based driver developed by FTP Software, Inc. for use with TCP/IP-based implementations

#### Note

*Be sure to investigate the existence of suitable (NDIS, ODI, PACKET) drivers for the wireless NIC, and fully test its functionality with your chosen appliance before making large investments in wireless network hardware.*

Radio cards traditionally come in a two-piece version configuration—that is, a PCMCIA card that inserts into the appliance and an external transceiver box. This setup is okay for some applications, such as forklift-mounted appliances; however, it is not ergonomic for most handheld appliances. Some vendors, especially with their newest radio cards, offer one-piece units having an integrated radio and transceiver assembly that all fits within the PCMCIA form factor.

### Antenna

The antenna radiates the modulated signal through the air so that the destination can receive it. Antennas come in many shapes and sizes and have the following specific electrical characteristics:

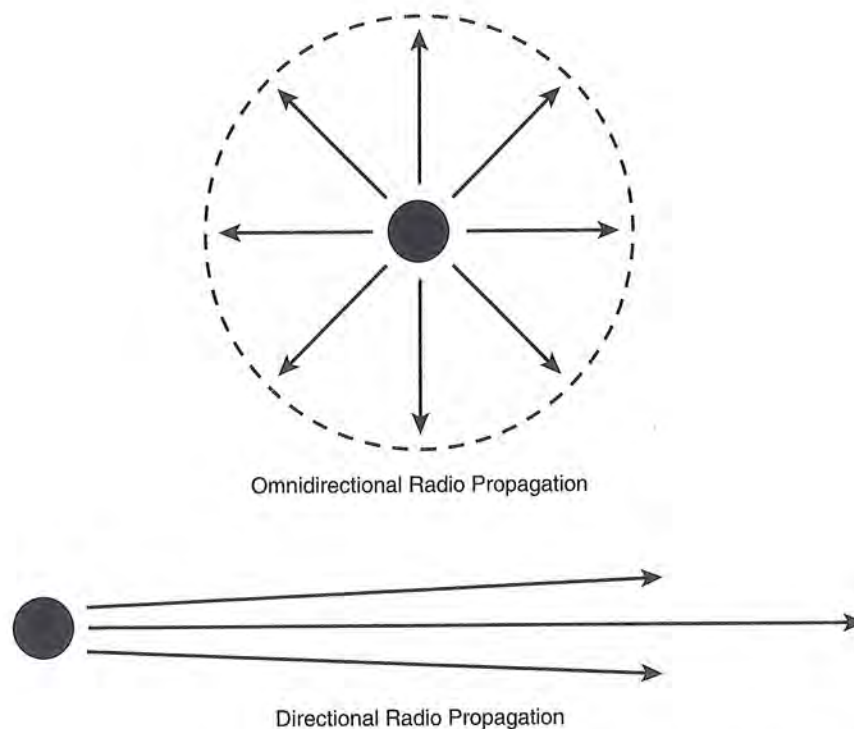
- Propagation pattern
- Gain
- Transmit power
- Bandwidth

The *propagation pattern* of an antenna defines its coverage. A truly omnidirectional antenna transmits its power in all directions; whereas, a directional antenna concentrates most of its power in one direction. Figure 1.9 illustrates the differences.

A directional antenna has more *gain* (degree of amplification) than the omnidirectional type and is capable of propagating the modulated signal farther because it focuses the power in a single direction. The amount of gain depends on the directivity of the antenna. An omnidirectional antenna has a gain equal to one; that is, it doesn't focus the power in any particular direction. Omnidirectional antennas are best for indoor wireless networks because of relatively shorter range requirements and less susceptibility to outward interference.

Directional antennas will best satisfy needs for interconnecting buildings within metropolitan areas because of greater range and the desire to minimize interference with other systems.

The combination of *transmit power* and gain of an antenna defines the distance the signal will propagate. Long-distance transmissions require higher power and directive radiation patterns; whereas, shorter distance transmissions can get by with less power and gain. With wireless networks, the transmit power is relatively low, typically one watt or less.



**FIGURE 1.9** An omnidirectional antenna broadcasts radio waves in all directions; whereas, a directional antenna focuses the power in a particular direction.

#### Note

Most spread spectrum radio vendors sell the following types of antennas:

- Snap-on antenna: Connects directly to the radio card and provides relatively low gain via an omnidirectional radio propagation pattern. This relatively small antenna is best for highly mobile applications when a larger antenna is impractical.
- Dipole antenna: Sits on a desk or table and connects to the radio card via a short antenna cable. This approach provides relatively low gain. This antenna is best for portable applications.
- High gain antenna: Attaches to a wall or antenna pole/tower and connects to the radio card or access point via a relatively long antenna cable. This approach provides relatively high gain and is best for access points and permanent stations.

*Bandwidth* is the effective part of the frequency spectrum that the signal propagates. The telephone system, for example, operates over a bandwidth roughly from 0 to 4 KHz. This is enough bandwidth to accommodate most of the frequency components within our voices. Radio wave systems have greater amounts of bandwidths located at much higher frequencies. Data rates and bandwidth are directly proportional: the higher the data rates, the more bandwidth you will need.



**Note**

*If you're considering integrating a radio NIC into a particular PCMCIA-based appliance, such as a hand-held data collector, you may have to redesign the antenna mounting hardware to accommodate the construction of the appliance.*

---

**The Communications Channel**

All information systems employ a communications channel along which information flows from source to destination. Ethernet networks may utilize twisted-pair or coaxial cable. Wireless networks use air as the medium. At the earth's surface, where most wireless networks operate, pure air contains gases, such as nitrogen and oxygen. This atmosphere provides an effective medium for the propagation of radio waves and infrared light.

**Troubleshooting Tip**

*The communications channel offers unforeseen obstacles to wireless systems. Always perform a site survey to investigate the effects of physical structures and atmospheric conditions on the propagation of wireless signals before finalizing the design and purchase of a wireless system. (See "Identifying the Location of Access Points" in Chapter 8, "Implementing a Wireless LAN," for information on conducting a site survey.)*

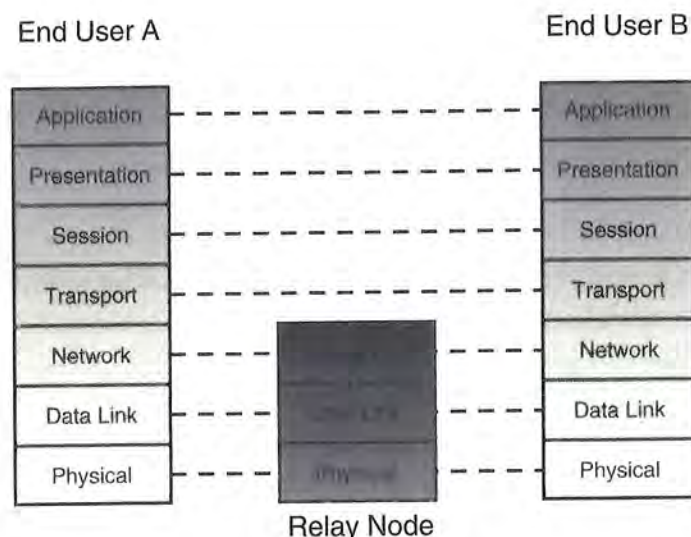
---

Rain, fog, and snow can increase the amount of water molecules in the air, however, and can cause significant *attenuation* to the propagation of modulated wireless signals. Smog clutters the air, adding attenuation to the communications channel as well. Attenuation is the decrease in the amplitude of the signal, and it limits the operating range of the system. The ways to combat attenuation are to either increase the transmit power of the wireless devices, which in most cases is limited by the FCC, or incorporate special amplifiers called *repeaters* that receive attenuated signals, revamp them, and transmit downline to the end station or next repeater.

**Logical Architecture of a Wireless Network**

A *logical architecture* defines the network's protocols, which ensures a well-managed and effective means of communication. PCs, servers, routers, and other active devices must conform to very strict rules to facilitate the proper coordination and transfer of information.

One popular standard logical architecture is the seven-layer Open System Interconnect (OSI) Reference Model, developed by the International Standards Organization (ISO). OSI specifies a complete set of network functions, grouped into layers. Figure 1.10 illustrates the OSI Reference Model.



**FIGURE 1.10** The Open System Interconnect Reference Model illustrates all levels of network functionality.

The OSI layers provide the following network functionality:

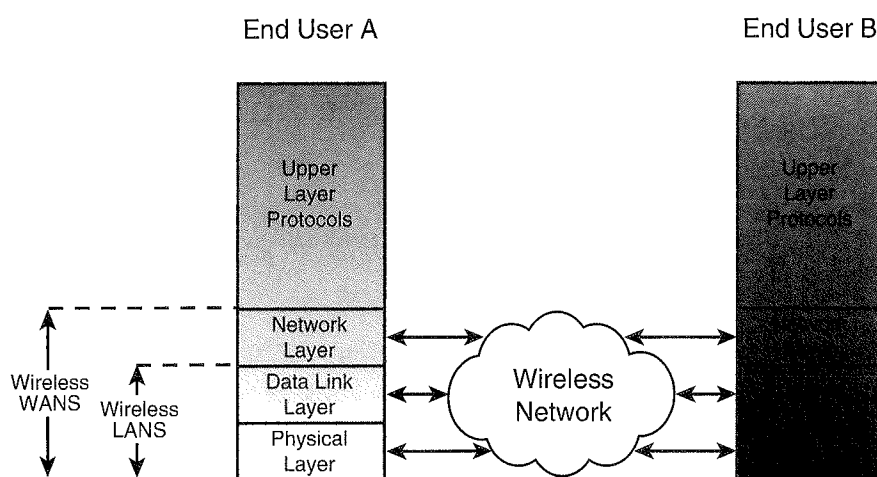
- *Layer 7—Application Layer:* Establishes communications with other users and provides such services as file transfer and email to the end users of the network.
- *Layer 6—Presentation Layer:* Negotiates data transfer syntax for the Application Layer and performs translations between different data types, if necessary.
- *Layer 5—Session Layer:* Establishes, manages, and terminates sessions between applications.
- *Layer 4—Transport Layer:* Provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, while shielding the higher layers from the network implementation details. Such protocols as TCP operate at this layer.
- *Layer 3—Network Layer:* Provides the routing of packets through routers from source to destination. Such protocols as IP operate at this layer.
- *Layer 2—Data Link Layer:* Ensures synchronization and error control between two entities.
- *Layer 1—Physical Layer:* Provides the transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications.

#### Note

Each layer of OSI supports the layers above it.

Does a wireless network offer all OSI functions? No, not in a theoretical sense. As shown in Figure 1.11, wireless networks operate only within the bottom three layers. Only wireless wide area networks, however, perform Network Layer functions.

In addition to the wireless network functions, a complete network architecture needs to include such functions as end-to-end connection establishment and application services to make it useful. Chapter 3, “Overview of the IEEE 802.11 Standard,” provides details on the architecture of 802.11-compliant LANs which only covers the Network and Physical Layers of OSI. Chapter 6, “Wireless System Integration,” explains other components necessary to design and implement a complete system.



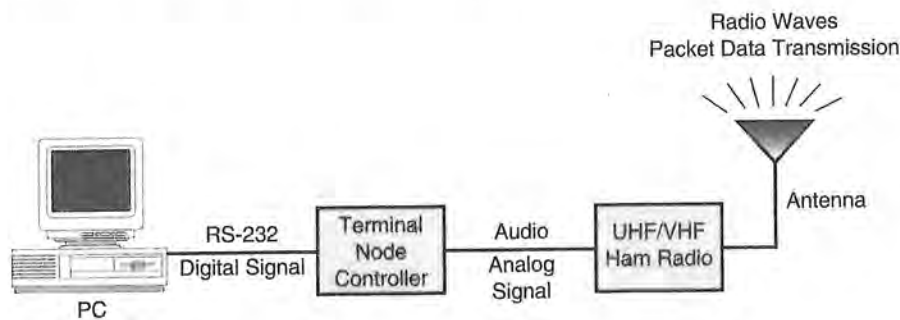
**FIGURE 1.11** *Wireless LANs and MANs fulfill Data Link and Physical Layer functionality; whereas, wireless WANs also include functions at the Network Layer.*

## The History of Wireless Networks

Network technologies and radio communications were brought together for the first time in 1971 at the University of Hawaii as a research project called ALOHANET. The ALOHANET system enabled computer sites at seven campuses spread out over four islands to communicate with the central computer on Oahu without using the existing unreliable and expensive phone lines. ALOHANET offered bidirectional communications, in a star topology, between the central computer and each of the remote stations. The remote stations had to communicate with one another via the centralized computer.

In the 1980s, amateur radio hobbyists, *hams*, kept radio networking alive within the United States and Canada by designing and building *terminal node controllers* (TNCs) to interface their computers through ham radio equipment (see Figure 1.12). TNCs

act much like a telephone modem, converting the computer's digital signal into one that a ham radio can modulate and send over the airwaves by using a packet-switching technique. In fact, the American Radio Relay League (ARRL) and the Canadian Radio Relay League (CRRL) have been sponsoring the Computer Networking Conference since the early 1980s to provide a forum for the development of wireless WANs. Thus, hams have been utilizing wireless networking for years, much earlier than the commercial market.



**FIGURE 1.12** Terminal node controllers enable a PC to interface with a ham radio to form a packet radio network.

In 1985, the Federal Communications Commission (FCC) made the commercial development of radio-based LAN components possible by authorizing the public use of the Industrial, Scientific, and Medical (ISM) bands. This band of frequencies resides between 902 MHz and 5.85 GHz, just above the cellular phone operating frequencies. The ISM band is very attractive to wireless network vendors because it provides a part of the spectrum upon which to base their products, and end users do not have to obtain FCC licenses to operate the products. The ISM band allocation has had a dramatic effect on the wireless industry, prompting the development of wireless LAN components. Without a standard, however, vendors began developing proprietary radios and access points.

In the late 1980s, the Institute for Electrical and Electronic Engineers (IEEE) 802 Working Group, responsible for the development of LAN standards, such as ethernet and token ring, began development of standards for wireless LANs. Under the chairmanship of Vic Hayes, an engineer from NCR, the IEEE 802.11 Working Group developed the Wireless LAN Medium Access Control and Physical Layer specifications.

The IEEE Standards Board approved the standard on June 26, 1997, and the IEEE published the standard on November 18, 1997. The finalizing of this standard is prompting vendors to release 802.11-compliant radio cards and access points throughout 1998. Other vendors new to the wireless market are sure to develop and

release 802.11-compliant products based on the standard blueprint provided by the 802.11 standard.

Another widely accepted wireless network connection, however, has been wireless WAN services, which began surfacing in the early 1990s. Companies such as ARDIS and RAM Mobile Data were first in selling wireless connections between portable computers, corporate networks, and the Internet. Companies then began introducing Cellular Digital Packet Data (CDPD) services, which enable users to send and receive data packets via digital transmission services. These services enable employees to access email and other information services from their personal appliances without using the telephone system when meeting with customers, traveling in the car, or staying in a hotel.

## **The Future of Wireless Networks**

Where is wireless networking going? What will the future bring? Predicting what the state of this technology and its products will be five years from now, or even a year from now, is impossible. The outlook for wireless networks, however, is very good. The maturation of standards should motivate vendors to produce new wireless products and drive the prices down to levels that are much easier to justify.

The presence of standards will motivate smaller companies to manufacture wireless components because they will not need to invest large sums of money in the research and development phases of the product. These investments already will have been made and embodied within the standards, which will be available to anyone interested in building wireless network components.



# CHAPTER 2

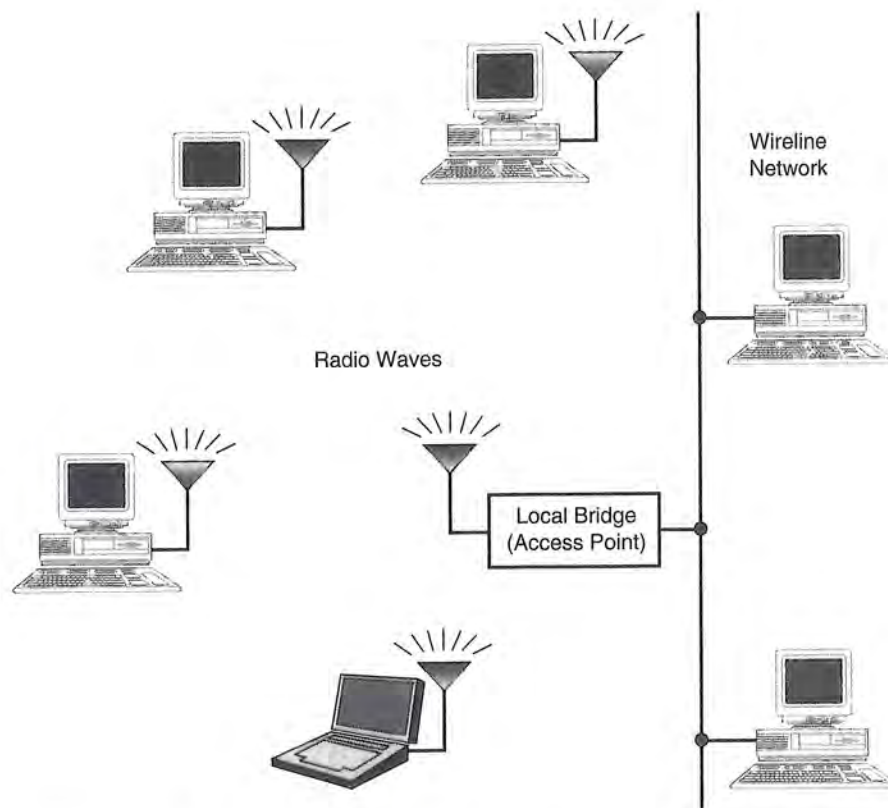
## *Wireless Network Configurations*

---

- **Wireless LANs**  
It is important to understand the various types of wireless LANs to choose the best alternative technology and select the right components for use within a local area. You learn about the different configurations of a wireless LAN and how they operate.
- **Wireless point-to-point networks**  
While providing network connectivity—mostly outdoors—wireless point-to-point networks offer additional challenges that are different from wireless LANs. Understanding how to maximize the use of wireless point-to-point network technologies is crucial to implementing their solutions.
- **Wireless WANs**  
Wireless WANs can solve your wide area mobile network connectivity needs, but you need to use the technology that is going to provide the necessary coverage. You learn to differentiate the choices you have for wireless wide area networks.

### **Wireless LANs**

Most wireless LANs operate over unlicensed frequencies at near-ethernet speeds (10 Mbps) using carrier sense protocols to share a radio wave or infrared light medium. The majority of these devices are capable of transmitting information up to 1,000 feet between computers within an open environment, and their costs per user range from \$150 to \$800. In addition, most wireless LAN products offer Simple Network Management Protocol (SNMP) to support network management through the use of SNMP-based management platforms and applications. Figure 2.1 illustrates the concept of a wireless local area network interfacing with a wired network.



**FIGURE 2.1** A wireless local area network provides connectivity over the airwaves within a local area, such as a building.

The components of a wireless LAN consist of a wireless NIC and a wireless local bridge, which is often referred to as an *access point*. The wireless NIC interfaces the appliance with the wireless network, and the access point interfaces the wireless network with a wired network. Most wireless NICs interface appliances to the wireless network by implementing a carrier sense access protocol and modulating the data signal with a spreading sequence.

The following sections describe three approaches to wireless networking within a local environment. These methods include the following:

- Radio waves
- Infrared light
- Carrier currents

### Radio-Based Wireless LANs

The most widely sold wireless LAN products use radio waves as a medium between computers and peripherals. An advantage of radio waves over other forms of wireless

connectivity is that they can interconnect users without line of sight and propagate through walls and other obstructions with fairly little attenuation, depending on the type of wall construction. Although several walls might separate the user from the server or wireless bridge, users can maintain connections to the network. This supports true mobility. With radio-LAN products, a user with a portable computer can move freely through the facility while accessing data from a server or running an application.

A disadvantage of using radio waves, however, is that an organization must manage them along with other electromagnetic propagation. Medical equipment and industrial components may utilize the same radio frequencies as wireless LANs, which could cause interference. An organization must determine whether potential interference is present before installing a radio-based LAN. Because radio waves penetrate walls, security might also be a problem. Unauthorized people from outside the controlled areas could receive sensitive information; however, vendors often scramble the data signal to protect the information from being understood by inappropriate people.

This section discusses the following topics that explain the operation and configuration of radio-based wireless LANs:

- Medium access control
- Spread spectrum modulation
- Narrowband modulation
- Wireless local bridges
- Single-cell wireless LANs
- Multiple-cell wireless LANs

### **Medium Access Control**

Medium access control, which is a Data Link Layer function in a radio-based wireless LAN, enables multiple appliances to share a common transmission medium via a carrier sense protocol similar to ethernet. This protocol enables a group of wireless computers to share the same frequency and space.

As an analogy, consider a room of people engaged in a single conversation in which each person can hear if someone speaks. This represents a fully connected bus topology (where everyone communicates using the same frequency and space) that ethernet and wireless networks, especially wireless LANs, utilize.

To avoid having two people speak at the same time, you should wait until the other person has finished talking. Also, no one should speak unless the room is silent.



# CHAPTER 3

## *Overview of the IEEE 802.11 Standard*

---

- **The importance of standards**  
This chapter begins with an introduction to the types of LAN standards and the primary organization that makes the standards: the Institute for Electrical and Electronic Engineers (IEEE). You learn the important benefits of using the IEEE 802.11 wireless LAN standard.
- **IEEE 802 LAN standards family**  
It is important to know how the IEEE 802.11 standard fits into other LAN protocols to ensure proper interoperability. An overview of the 802 series of LAN standards describes the operation of the 802.2 Logical Link Control that directly interfaces with 802.11.
- **Introduction to the IEEE 802.11 standard**  
An explanation of the scope and goals of the 802.11 standard provides an understanding of the basic functionality of 802.11. Learn the peculiar wireless network issues that were addressed when developing the standard.
- **IEEE 802.11 topology**  
An overview of the physical structure of 802.11-compliant LANs provides an understanding of 802.11 topology. Understand how basic physical 802.11 elements, such as Basic Service Sets (single-cell wireless LANs) and access points, form integrated, multiple-cell wireless LANs that support a variety of mobility types.
- **IEEE 802.11 logical architecture**  
Coverage of the main elements of the 802.11 protocol stack provides an overview of how the 802.11 protocol works. Learn the main functionality of each of the following 802.11 protocol layers: MAC Layer and individual PHY (Physical) Layers (frequency hopping, direct sequence, and infrared).

- **IEEE 802.11 services**  
802.11-compliant LANs function based on a set of services that relate to stations and distribution systems. Discover how these services offer security equivalent to wired LANs.
- **Implications of the IEEE 802.11 standard**  
Although the long-awaited 802.11 standard offers several benefits over using proprietary-based wireless LANs, the 802.11 standard still has shortcomings that implementors should be aware of. Learn some of the 802.11 implications, such as relatively low data rates and lack of roaming.
- **IEEE 802.11 standard compliance**  
The compliance with 802.11 depends on those having the need for wireless networks. Become aware of how vendors are complying with 802.11, what end users need to do to be compliant, and how different regions of the world comply with 802.11 radio frequencies.
- **IEEE 802.11 Working Group operations**  
Involvement in IEEE 802.11 standards development is open to anyone with a desire to participate, but you need to understand the membership requirements and types of 802.11 members.
- **Future of the IEEE 802.11 standard**  
When making decisions about wireless LANs, be sure to include what the future holds for the 802.11 standard. Discover the projects IEEE 802.11 members are working on to increase the performance of 802.11-compliant wireless LANs.

## The Importance of Standards

Vendors and some end users initially expected markets to dive headfirst into implementing wireless networks. Markets did not respond as predicted, and flat sales growth of wireless networking components prevailed through most of the 1990s. Relatively low data rates, high prices, and especially the lack of standards kept many end users from purchasing the wire-free forms of media.

For those having applications suitable for lower data rates and enough cost savings to warrant purchasing wireless connections, the only choice before 1998 was to install proprietary hardware to satisfy requirements. As a result, many organizations today have proprietary wireless networks for which you have to replace both hardware and software to be compliant with the IEEE 802.11 standard. The lack of standards has been a significant problem with wireless networking, but the first official version of the standard is now available. In response to lacking standards, the Institute for Electrical and Electronic Engineers (IEEE) developed the first internationally recognized wireless LAN standard: IEEE 802.11.

## Types of Standards

There are two main types of standards: official and public. An *official standard* is published and known to the public, but it is controlled by an official standards organization, such as IEEE. Government or industry consortiums normally sponsor official standards groups. Official standards organizations generally ensure coordination at both the international and domestic level.

A *public standard* is similar to an official standard, except it is controlled by a private organization, such as the Wireless LAN Interoperability Forum. Public standards, often called *de facto standards*, are common practices that have not been produced or accepted by an official standards organization. These standards, such as TCP/IP, are the result of widespread proliferation. In some cases, public standards that proliferate, such as the original ethernet, eventually pass through standards organizations and become official standards.

Companies should strive to adopt standards and recommended products within their organizations for all aspects of information systems. What type of standards should you use? For most cases, focus on the use of an official standard if one is available and proliferating. This will help ensure widespread acceptance and longevity of your wireless network implementation. If no official standard is suitable, a public standard would be a good choice. In fact, public standards can often respond faster to changes in market needs because they usually have less organizational overhead for making changes. Be sure to avoid nonstandard or proprietary system components, unless there are no suitable standards available.

### Case Study 3.1: 802.11 Versus Proprietary Standards

A large retail chain based in Sacramento, California, had requirements to implement a wireless network to provide mobility within their 10 warehouses located all over the United States. The application calls for clerks within the warehouse to utilize new handheld wireless data collectors that perform inventory-management functions.

The company, already having one vendor's data collection devices (we'll call these brand X), decides to use that vendor's

brand Y proprietary wireless data collectors and their proprietary wireless network (the vendor doesn't offer an 802.11-compliant solution). This decision eliminates the need to work with additional vendors for the new handheld devices and the wireless network.

A year passes since the installation, and enhancement requirements begin to pour in for additional mobile appliances that are not available from the brand X

*continues*



*continued*

vendor. This forces the company to consider the purchase of new brand Z appliances from a different vendor. The problem, however, is that the brand Z appliances, which are 802.11-compliant, don't interoperate with the installed proprietary brand Y wireless network. Because of the cost associated with replacing their network with one that is 802.11 compliant (the brand Y wireless network has no upgrade path to 802.11), the company can't cost effectively implement the new enhancement.

The company could have eliminated the problem of not being able to implement the new enhancement if it would have implemented the initial system with 802.11-compliant network components, because most vendors offer products that are compatible with 802.11, but not all the proprietary networks. The result would have been the ability to consider multiple vendors for a wider selection of appliances.

### **Institute for Electrical and Electronic Engineers (IEEE)**

The IEEE is a nonprofit professional organization founded by a handful of engineers in 1884 for the purpose of consolidating ideas dealing with electro-technology. In the last 100 plus years, IEEE has maintained a steady growth. Today, the IEEE, which is based in the United States, has over 320,000 members located in 150 countries. The IEEE consists of 35 individual societies, including the Communications Society, Computer Society, and Antennas and Propagation Society.

The IEEE plays a significant role in publishing technical works, sponsoring conferences and seminars, accreditation, and standards development. The IEEE has published nearly 700 active standards publications, half of which relate to power engineering and most others deal with computers. The IEEE standards development process consists of 30,000 volunteers (who are mostly IEEE members) and a Standards Board of 32 people. In terms of LANs, IEEE has produced some very popular and widely used standards. The majority of LANs in the world utilize network interface cards based on the IEEE 802.3 (ethernet) and IEEE 802.5 (token ring) standards, for example.

Before someone can develop an IEEE standard, he must submit a Project Authorization Request (PAR) to the IEEE Standards Board. If the board approves the PAR, IEEE establishes a standards working group to develop the standard. Members of the working groups serve voluntarily and without compensation, and they are not necessarily members of the institute. The working group begins by writing a draft standard, and then solicits the draft to a balloting group of selected IEEE members for review and approval. The ballot group consists of the standard's developers, potential users, and other people having general interest.

Before publication, the IEEE Standards Board performs a review of the Final Draft Standard, and then considers approval of the standard. The resulting standard represents a consensus of broad expertise from within IEEE and other related organizations. All IEEE standards are subjected to review at least once every five years for revision or reaffirmation.

**Note**

*In May 1991, a group of people, led by Victor Hayes, submitted a Project Authorization Request (PAR) to IEEE to initiate the 802.11 Working Group. Victor became Chairman of the working group and led the standards effort to its completion in June 1997.*

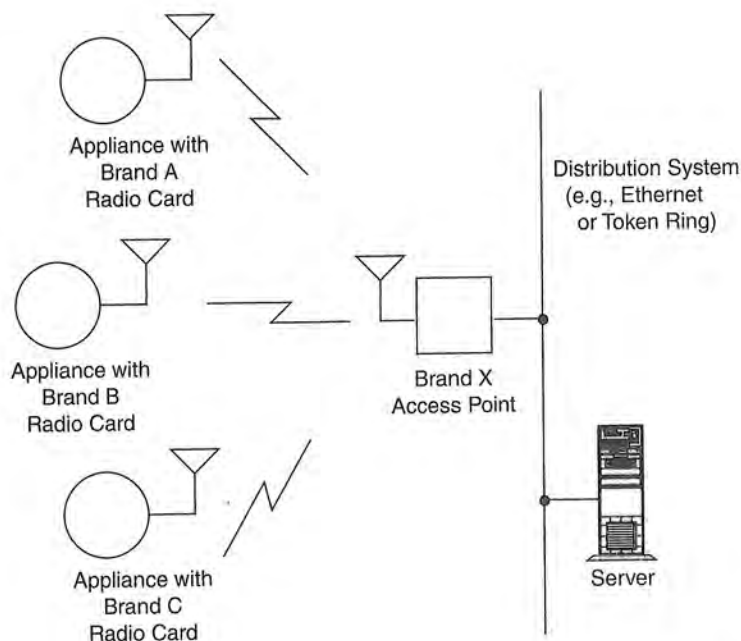
**Benefits of the 802.11 Standard**

The benefits of utilizing standards, such as those published by IEEE, are great. The following sections explain the benefits of complying with standards, especially IEEE 802.11.

**Appliance Interoperability**

Compliance with the IEEE 802.11 standard makes interoperability between multiple-vendor appliances and the chosen wireless network type possible. This means you can purchase an 802.11-compliant PalmPilot from Symbol and Pathfinder Ultra handheld scanner/printer from Monarch Marking Systems, and they will both interoperate within an equivalent 802.11 wireless network, assuming 802.11 configuration parameters are set equally in both devices. Standard compliance increases price competition and enables companies to develop wireless LAN components with lower research and development budgets. This enables a greater number of smaller companies to develop wireless components. As a result, the sales of wireless LAN components should boom over the next few years as the finalization of the IEEE 802.11 standard sinks in.

As shown in Figure 3.1, appliance interoperability avoids the dependence on a single vendor for appliances. Without a standard, for example, a company having a non-standard proprietary Symbol network would be dependent on purchasing only appliances that operate on a Symbol network. This would exclude appliances such as ones from Telxon that only operate on proprietary Aironet networks. With an 802.11-compliant wireless network, you can utilize any equivalent 802.11-compliant appliance. Because most vendors, including Symbol and Telxon, have migrated their products to 802.11, you have a much greater selection of appliances for 802.11 standard networks.



**FIGURE 3.1** *Appliance interoperability ensures that multiple-vendor hardware works within equivalent wireless networks.*

### Fast Product Development

The 802.11 standard is a well-tested blueprint that developers can use to implement wireless devices. The use of standards decreases the learning curve required to understand specific technologies because the standard-forming group has already invested the time to smooth out any wrinkles in the implementation of the applicable technology. This leads to the development of products in much less time.

### Stable Future Migration

Compliance with standards helps protect investments and avoids legacy systems that must be completely replaced in the future as those proprietary products become obsolete. The evolution of wireless LANs should occur in a similar fashion as 802.3, ethernet. Initially, ethernet began as a 10 Mbps standard using coaxial cable media. The IEEE 802.3 Working Group enhanced the standard over the years by adding twisted-pair, optical-fiber cabling, and 100 and 1000 Mbps data rates.

Just as IEEE 802.3 did, the 802.11 Working Group recognizes the investments organizations make in network infrastructure and the importance in providing migration paths that maximize the installed base of hardware. As a result, 802.11 will certainly ensure stable migration from existing wireless LANs as higher performance wireless networking technologies become available.



### Price Reductions

High costs have always plagued the wireless LAN industry; however, prices should drop significantly as more vendors and end users comply with 802.11. One of the reasons for lower prices is that vendors will no longer need to develop and support lower-quantity proprietary subcomponents, cutting design, manufacturing, and support costs. Ethernet went through a similar lowering of prices as more and more companies began complying with the 802.3 standard.

### Avoiding Silos

Over the past couple of decades, MIS organizations have had a difficult time maintaining control of network implementations. The introduction of PCs, LANs, and visual-based development tools has made it much easier for non-MIS organizations, such as finance and manufacturing departments, to deploy their own applications. One part of the company, for example, may purchase a wireless network from one vendor, and then another part of the company may buy a different wireless network. As a result, *silos*—noninteroperable systems—appear within the company, making it very difficult for MIS personnel to plan and support compatible systems. Some people refer to these silos as *stovepipes*.

Acquisitions bring dissimilar systems together as well. One company having a proprietary system may purchase another having a different proprietary system, resulting in noninteroperability. Figure 3.2 illustrates the features of standards that minimize the occurrence of silos.

#### Case Study 3.2:

##### Problems with Mixed Standards

A company located in Barcelona, Spain specializes in the resale of women's clothes. This company, having a MIS group without much control over the implementation of distributed networks in major parts of the company, has projects underway to implement wireless networks for an inventory application and a price-marking application.

Non-MIS project managers located in different parts of the company lead these projects. They have little desire to coordinate their projects with MIS because of past difficulties. As a result, both pro-

ject managers end up implementing noncompatible proprietary wireless networks to satisfy their networking requirements.

The project managers install both systems: one that covers the sales floorspace of their 300 stores (for price marking) and one that encompasses 10 warehouses (for doing inventory functions). Although the systems are noncompatible, all is fine for the users operating the autonomous systems.

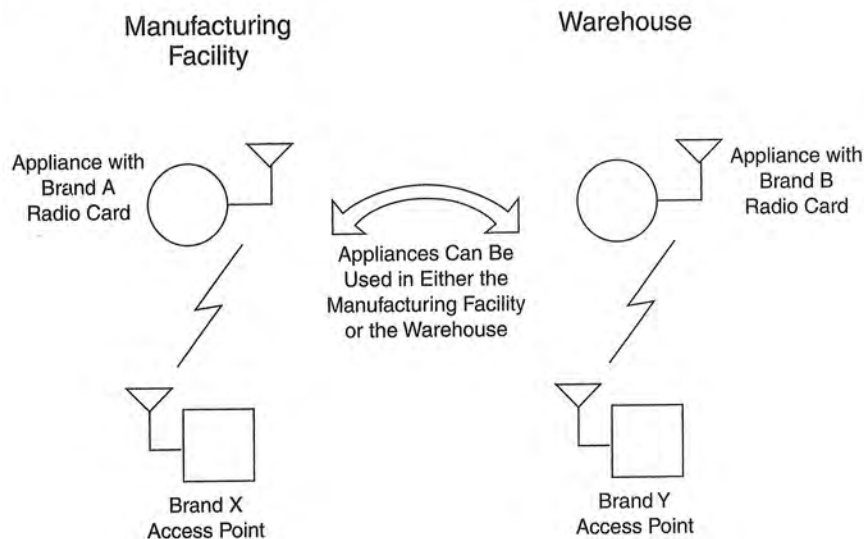
The issues with this system architecture, however, are the difficulty in providing

*continues*

*continued*

operational support and inflexibility. The company must maintain purchasing and warranty contracts with two different wireless network vendors, service personnel need to acquire and maintain an understanding in the operation of two networks, and the company cannot share appliances and wireless network components between the warehouses and the stores.

As a result, the silos in this case make the networks more expensive to support and limit their flexibility in meeting future needs. The implementation of standard 802.11-compliant networks would have avoided these problems.



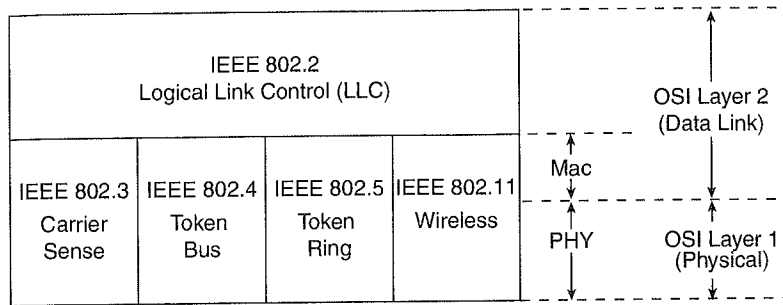
**FIGURE 3.2** Compliance with the IEEE 802.11 standard can minimize the implementation of silos.

## IEEE 802 LAN Standards Family

The IEEE 802 Local and Metropolitan Area Network Standards Committee is a major working group chartered by IEEE to create, maintain, and encourage the use of IEEE and equivalent IEC/ISO standards. IEEE formed the committee in February 1980, and has met at least three times per year as a plenary body since then. IEEE 802 produces the series of standards known as IEEE 802.x, and the JTC 1 series of equivalent standards are known as ISO 8802-nnn.

IEEE 802 includes a family of standards, as depicted in Figure 3.3. The MAC and Physical Layers of the 802 standard were organized into a separate set of standards from the LLC because of the interdependence between medium access control, medium, and topology.





**FIGURE 3.3** The IEEE 802 family of standards falls within the scope of layers 1 and 2 of the OSI Reference Model. The LLC protocol specifies the mechanisms for addressing stations across the medium and for controlling the exchange of data between two stations; whereas, the MAC and PHY Layers provide medium access and transmission functions.

The IEEE 802 family of standards includes the following:

- *IEEE 802.1: Glossary, Network Management, and Internetworking:* These documents, as well as IEEE 802 Overview and Architecture, form the scope of work for the 802 standards.
- *IEEE 802.2: Logical Link Control (LLC):* This standard defines Layer 2 synchronization and error control for all types of 802 LANs, including 802.11. Refer to the next section, "IEEE 802.2 LLC Overview," for more detail on the features and operation of the LLC.
- *IEEE 802.3: CSMA/CD Access Method and Physical Layer Specifications:* This defines the widely accepted 10, 100, and 1000 Mbps ethernet asynchronous protocol for use over twisted-pair wiring, coaxial cable, and optical fiber.
- *IEEE 802.4: Token-Passing Bus Access Method and Physical Layer Specifications:* This offers a token-passing protocol over a bus topology that can be embedded in other systems.
- *IEEE 802.5: Token-Passing Ring Access Method and Physical Layer Specifications:* This defines a 4 and 16 Mbps synchronous protocol that uses a token for access control over a ring topology.
- *IEEE 802.10: Security and Privacy Access Method and Physical Layer Specifications:* Provides security provisions for both wired and wireless LANs.
- *IEEE 802.11: Wireless Access Method and Physical Layer Specification:* Encompasses a variety of physical media, including frequency hopping spread spectrum, direct sequence spread spectrum, and infrared light for data rates up to 2 Mbps.

### IEEE 802.2 LLC Overview

The LLC is the highest layer of the IEEE 802 Reference Model and provides similar functions of the traditional Data Link Control protocol: HDLC (High-Level Data

Link Control). The ANSI/IEEE Standard 802.2 specifies the LLC. The purpose of the LLC is to exchange data between end users across a LAN using a 802-based MAC controlled link. The LLC provides addressing and data link control, and it is independent of the topology, transmission medium, and medium access control technique chosen.

Higher layers, such as TCP/IP, pass user data down to the LLC expecting error-free transmission across the network. The LLC in turn appends a control header, creating an LLC protocol data unit (PDU). The LLC utilizes the control information in the operation of the LLC protocol (see Figure 3.4). Before transmission, the LLC PDU is handed down through the MAC service access point (SAP) to the MAC Layer, which appends control information at the beginning and end of the packet, forming a MAC frame. The control information in the frame is needed for the operation of the MAC protocol.

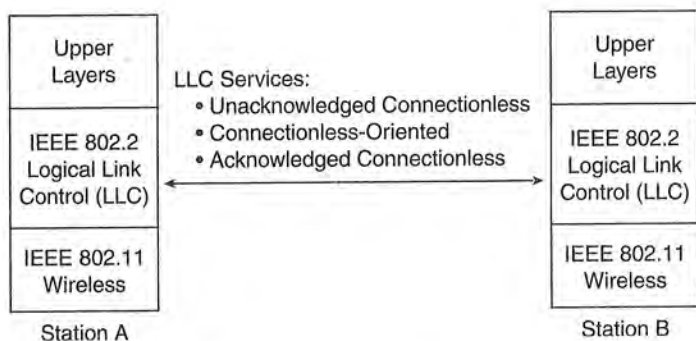


FIGURE 3.4 The LLC provides end-to-end link control over an 802.11-based wireless LAN.

### IEEE 802.2 LLC Services

The LLC provides the following three services for a Network Layer protocol:

- Unacknowledged connectionless service
- Connection-oriented service
- Acknowledged connectionless service

These services apply to the communication between peer LLC Layers—that is, one located on the source station and one located on the destination station. Typically, vendors will provide these services as options that the customer can select when purchasing the equipment.

All three LLC protocols employ the same PDU format that consists of four fields (see Figure 3.5). The Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) fields each contains 7-bit addresses, which specify the destination and

source stations of the peer LLCs. One bit of the DSAP indicates whether the PDU is intended for an individual or group station(s). One bit of the SSAP indicates whether it is a command or response PDU. The format of the LLC Control field is identical to that of HDLC, using extended (7-bit) sequence numbers. The Data field contains the information from higher-layer protocols that the LLC is transporting to the destination.

8 Bits	8 Bits	8 Bits	Variable
Destination SAP	Service SAP	Control	Data

**FIGURE 3.5** The LLC PDU consists of data fields that provide the LLC functionality.

The Control field has bits that indicate whether the frame is one of the following types:

- *Information:* Used to carry user data
- *Supervisory:* Used for flow control and error control
- *Unnumbered:* Various protocol control PDUs

### Unacknowledged Connectionless Service

The *unacknowledged connectionless service* is a datagram-style service that does not involve any error-control or flow-control mechanisms. This service does not involve the establishment of a Data Link Layer connection (that is, a connection between peer LLCs). This service supports individual, multicast, and broadcast addressing. This service just sends and receives LLC PDUs, with no acknowledgment of delivery. Because the delivery of data is not guaranteed, a higher layer, such as TCP, must deal with reliability issues.

The unacknowledged connectionless service offers advantages in the following situations:

- If higher layers of the protocol stack provide the necessary reliability and flow-control mechanisms, it would be inefficient to duplicate them in the LLC. In this case, the unacknowledged connectionless service would be appropriate. TCP and the ISO transport protocol, for example, already provide the mechanisms necessary for reliable delivery.
- It is not always necessary to provide feedback pertaining to successful delivery of information. The overhead of connection establishment and maintenance can be inefficient—as an example, for applications involving the periodic sampling of data sources, such as monitoring sensors. The unacknowledged connectionless service would best satisfy these requirements.



**Case Study 3.3:  
Using Unacknowledged  
Connectionless Service to  
Minimize Overhead**

The executive office building of a high-rent advertising agency in Southern California has 20 sensors to monitor temperatures throughout its building as an input to the heating and air conditioning system. These sensors send short information packets every minute to an application on a centralized server that updates a temperature table in a database. The heating and air conditioning system uses this information to control the temperature in different parts of the building.

For this application, the server does not need to acknowledge the reception of

every sensor transmission because the information updates are not critical. The system can maintain a comfortable temperature throughout the building even if the system misses temperature updates from time to time.

Additionally, it is not feasible to require the sensors to establish connections with the server to send the short information packets. As a result, designers of the system chose to use the LLC unacknowledged connectionless service to minimize overhead on the network, making the limited wireless network bandwidth available to other applications.

**Connection-Oriented Service**

The *connection-oriented service* establishes a logical connection that provides flow control and error control between two stations needing to exchange data. This service does involve the establishment of a connection between peer LLCs by performing connection establishment, data transfer, and connection termination functions. The service can only connect two stations; therefore, it does not support multicast or broadcast modes. The connection-oriented service offers advantages mainly if higher layers of the protocol stack do not provide the necessary reliability and flow-control mechanisms, which is generally the case with terminal controllers.

Flow control is a protocol feature that ensures a transmitting station does not overwhelm a receiving station with data. With flow control, each station allocates a finite amount of memory and buffer resources to store sent and received PDUs.

Networks, especially wireless networks, suffer from induced noise in the links between network stations that can cause transmission errors. If the noise is high enough in amplitude, it causes errors in digital transmission in the form of altered bits. This will lead to inaccuracy of the transmitted data, and the receiving network device may misinterpret the meaning of the information.

The noise that causes most problems with networks is usually Gaussian and impulse noise. Theoretically, the amplitude of Gaussian noise is uniform across the frequency spectrum, and it normally triggers random single-bit independent errors.

Impulse noise, the most disastrous, is characterized by long quiet intervals of time followed by high-amplitude bursts. This noise results from lightning and switching transients. Impulse noise is responsible for most errors in digital communication systems and generally provokes errors to occur in bursts.

To guard against transmission errors, the connection-oriented and acknowledged-connectionless LLCs use error-control mechanisms that detect and correct errors that occur in the transmission of PDUs. The LLC ARQ mechanism recognizes the possibility of the following two types of errors:

- *Lost PDU*: A PDU fails to arrive at the other end or is damaged beyond recognition.
- *Damaged PDU*: A PDU has arrived, but some bits are altered.

When a frame arrives at a receiving station, the station checks whether there are any errors present by using a *Cyclic Redundancy Check* (CRC) error detection algorithm. In general, the receiving station will send back a positive or negative acknowledgment depending on the outcome of the error detection process. In case the acknowledgment is lost en route to the sending station, the sending station will retransmit the frame after a certain period of time. This process is often referred to as *Automatic Repeat-Request* (ARQ).

Overall, ARQ is best for the correction of burst errors because this type of impairment occurs in a small percentage of frames, thus not invoking many retransmissions. Because of the feedback inherent in ARQ protocols, the transmission links must accommodate half-duplex or full-duplex transmissions. If only simplex links are available due to feasibility, it is impossible to use the ARQ technique because the receiver would not be able to notify the transmitter of bad data frames.

#### Note

*In cases for which single bit errors predominate or when only a simplex link is available, forward error correction (FEC) can provide error correction. FEC algorithms provide enough redundancy in data transmissions to enable the receiving station to correct errors without needing the sending station to retransmit the data.*

*FEC is effective for correcting single-bit errors, but it requires a great deal of overhead in the transmissions to protect against multiple errors, such as burst errors. The IEEE LLC, however, specifies only the use of ARQ-based protocols for controlling errors.*

The following are two approaches for retransmitting unsatisfactory blocks of data using ARQ.

#### **Continuous ARQ**

With continuous ARQ, often called a *sliding window protocol*, the sending station transmits frames continuously until the receiving station detects an error. The



sending station is usually capable of transmitting a specific number of frames and maintains a table indicating which frames have been sent.

The system implementor can set the number of frames sent before stopping via configuration parameters of the network device. If a receiver detects a bad frame, it will send a negative acknowledgment back to the sending station requesting that the bad frame be sent over again. When the transmitting station gets the signal to retransmit the frame, several subsequent frames may have already been sent (due to propagation delays between the sender and receiver); therefore, the transmitter must “go back” and retransmit the erred data frame.

There are a couple ways the transmitting station can send frames again using continuous ARQ. One method is for the source to retrieve the erred frame from the transmit buffer and send the bad frame and all frames following it. This is called the *go-back-n technique*. A problem, however, is when  $n$  (the number of frames the transmitter sent after the erred frame plus one) becomes large, the method becomes inefficient. This is because the retransmission of just one frame means that a large number of possibly “good” frames will also be resent, thus decreasing throughput.

The go-back- $n$  technique is useful in applications for which receiver buffer space is limited because all that is needed is a receiver window size of one (assuming frames are to be delivered in order). When the receive node rejects an erred frame (sends a negative acknowledgment), it does not need to buffer any subsequent frames for possible reordering while it is waiting for the retransmission because all subsequent frames will also be sent.

An alternative to the continuous go-back- $n$  technique is a method that selectively retransmits only the erred frame, and then resumes normal transmission at the point just before getting the notification of a bad data frame. This approach is called *selective repeat*. It is obviously better than continuous go-back- $n$  in terms of throughput because only the erred frame needs retransmission. With this technique, however, the receiver must be capable of storing a number of frames if they are to be processed in order. The receiver needs to buffer data that have been received after an erred frame was requested for retransmission because only the damaged frame will be sent again.

### **Stop-and-Wait ARQ**

With stop-and-wait ARQ, the sending station transmits a frame and then stops and waits for some type of acknowledgment from the receiver on whether a particular frame was acceptable or not. If the receiving station sends a negative acknowledgment, the frame will be sent again. The transmitter will send the next frame only after it receives a positive acknowledgment from the receiver.

An advantage of stop-and-wait ARQ is that it does not require much buffer space at the sending or receiving station. The sending station needs to store only the current transmitted frame. However, stop-and-wait ARQ becomes inefficient as the propagation delay between source and destination becomes large. For example, data sent on satellite links normally experience a round-trip delay of several hundred milliseconds; therefore, long block lengths are necessary to maintain a reasonably effective data rate. The trouble is that with longer frames, the probability of an error occurring in a particular block is greater. Therefore, retransmission will occur often, and the resulting throughput will be lower.

**Case Study 3.4:**  
**Using Automatic Repeat-Request (ARQ) to Reduce Errors**

A mobile home manufacturer in Florida uses robots on the assembly line to perform welding. Designers of the robot control system had to decide whether to use ARQ or FEC for controlling transmission errors between the server and the robots. The company experiences a great deal of impulse noise from arc welders and other heavy machinery.

In the midst of this somewhat hostile environment, the robots require error-free information updates to ensure that they function correctly. Designers of the system quickly ruled out the use of FEC because of the likely presence of burst errors due to impulse noise. ARQ, with its capability to detect and correct frames having a lot of bit errors, was obviously the better choice.

**Acknowledged Connectionless Service**

As with the unacknowledged connectionless service, the *acknowledged connectionless service* does not involve the establishment of a logical connection with the distant station. But the receiving stations with the acknowledged version do confirm successful delivery of datagrams. Flow and error control is handled through use of the stop-and-wait ARQ method.

The acknowledged connectionless service is useful in several applications. The connection-oriented service must maintain a table for each active connection for tracking the status of the connection. If the application calls for guaranteed delivery, but there are a large number of destinations needing to receive the data, the connection-oriented service may be impractical because of the large number of tables required. Examples that fit this scenario include process control and automated factory environments that require a central site to communicate with a large number of processors and programmable controllers. In addition, the handling of important and time-critical alarm or emergency control signals in a factory would also fit this



case. In all these examples, the sending stations need an acknowledgment to ensure successful delivery of the data; however, the urgency of transmission cannot wait for a connection establishment.

#### Note

*A company having a requirement to send information to multiple devices needing positive acknowledgment of the data transfer can make use of the acknowledged connectionless LLC service. A marina may find it beneficial to control the power to different parts of the boat dock via a wireless network, for example. Of course, the expense of a wireless network may not be justifiable for this application alone.*

*Other applications, such as supporting data transfers back and forth to the cash register at the gas pump and the use of data-collection equipment for inventorying rental equipment, can share the wireless network to make a more positive business case. For shutting off the power on the boat dock, the application would need to send a message to the multiple power controllers, and then expect an acknowledgment to ensure the controller receives the notification and that the power is shut off. For this case, the connectionless transfer, versus connection-oriented, makes most sense because it would not be feasible to make connections to the controllers to support such a short message.*

### LLC/MAC Layer Service Primitives

Layers within the 802 architecture communicate with each other via service primitives having the following forms:

- *Request:* A layer uses this type of primitive to request that another layer perform a specific service.
- *Confirm:* A layer uses this type of primitive to convey the results of a previous service request primitive.
- *Indication:* A layer uses this type of primitive to indicate to another layer that a significant event has occurred. This primitive could result from a service request or from some internally generated event.
- *Response:* A layer uses this type of primitive to complete a procedure initiated by an indication primitive.

These primitives are an abstract way of defining the protocol, and they *do not* imply a specific physical implementation method. Each layer within the 802 model uses specific primitives. The LLC communicates with its associated MAC Layer through the following specific set of service primitives:

- **MA-UNITDATA.request:** The LLC sends this primitive to the MAC Layer to request the transfer of a data frame from a local LLC entity to a specific peer LLC entity or group of peer entities on different stations. The data frame could be an information frame containing data from a higher layer or a control frame (for example, a supervisory or unnumbered frame) that the LLC generates internally to communicate with its peer LLC.
- **MA-UNITDATA.indication:** The MAC Layer sends this primitive to the LLC to transfer a data frame from the MAC Layer to the LLC. This occurs only if the



MAC has found that a frame it receives from the Physical Layer is valid, has no errors, and that the destination address indicates the correct MAC address of the station.

- *MA-UNITDATA-STATUS.indication*: The MAC Layer sends this primitive to the LLC Layer to provide status information about the service provided for a previous *MA-UNITDATA.request* primitive.

#### Note

*The current ANSI/IEEE 802.2 standard (dated May 7, 1998) states that the 802.2 Working Group is developing a single-service specification of primitives that is common to all MAC Layers. IEEE will refer to this change in the 802.2 standard, not the individual MAC Layer standards (for example, 802.3, 802.5, 802.11).*

---

## Introduction to the IEEE 802.11 Standard

The initial 802.11 PAR states, "...the scope of the proposed [wireless LAN] standard is to develop a specification for wireless connectivity for fixed, portable, and moving stations within a local area." The PAR further says that the "purpose of the standard is to provide wireless connectivity to automatic machinery and equipment or stations that require rapid deployment, which may be portable, handheld, or which may be mounted on moving vehicles within a local area."

The resulting standard, which is officially called *IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications*, defines over-the-air protocols necessary to support networking in a local area. As with other IEEE 802-based standards (for example, 802.3 and 802.5), the primary service of the 802.11 standard is to deliver MSDUs (MAC Service Data Units) between peer LLCs. Typically, a radio card and access point provide functions of the 802.11 standard.

#### Note

*To order a copy of the IEEE 802.11 standard, contact the IEEE 802 Document Order Service at 800-678-4333. You can also order the standard via IEEE's Web site at [www.ieee.org](http://www.ieee.org).*

---

The 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable, and moving stations moving at pedestrian and vehicular speeds within a local area. Specific features of the 802.11 standard include the following:

- Support of asynchronous and time-bounded delivery service
- Continuity of service within extended areas via a distribution system, such as ethernet
- Accommodation of transmission rates of 1 and 2 Mbps
- Support of most market applications

- Multicast (including broadcast) services
- Network management services
- Registration and authentication services

Target environments for use of the standard include the following:

- Inside buildings, such as offices, banks, shops, malls, hospitals, manufacturing plants, and residences
- Outdoor areas, such as parking lots, campuses, building complexes, and outdoor plants

The 802.11 standard takes into account the following significant differences between wireless and wired LANs:

- *Power management:* Because most wireless LAN NICs are available in PCMCIA Type II format, obviously you can outfit portable and mobile handheld computing equipment with wireless LAN connectivity. The problem, however, is these devices must rely on batteries to power the electronics within them. The addition of a wireless LAN NIC to a portable computer can quickly drain batteries.

The 802.11 Working Group struggled with finding solutions to conserve battery power; however, they found techniques enabling wireless NICs to switch to lower-power standby modes periodically when not transmitting, reducing the drain on the battery. The MAC Layer implements power-management functions by putting the radio to sleep (that is, lowering the power drain) when no transmission activity occurs for some specific or user-definable time period. The problem, however, is that a sleeping station can miss critical data transmissions. 802.11 solves this problem by incorporating buffers to queue messages. The standard calls for sleeping stations to awaken periodically and retrieve any applicable messages.

- *Bandwidth:* The ISM spread spectrum bands do not offer a great deal of bandwidth, keeping data rates lower than desired for some applications. The 802.11 Working Group, however, dealt with methods to compress data, making the best use of available bandwidth. Efforts are also underway to increase the data rate of 802.11 to accommodate the growing need for exchanging larger and larger files (see the section titled “Future of the IEEE 802.11 Standard” at the end of this chapter).
- *Security:* As mentioned in Chapter 1, “Introduction to Wireless Networks,” in the “Network Security” section, wireless LANs transmit signals over much larger areas than that of wired media, such as twisted-pair, coaxial, and optical fiber cable. In terms of privacy, therefore, wireless LANs have a much larger area to protect. To employ security, the 802.11 Working Group coordinated their work with the IEEE 802.10 Standards Committee responsible for developing security mechanisms for all 802 series LANs.

- *Addressing:* The topology of a wireless network is dynamic; therefore, the destination address does not always correspond to the destination's location. This raises a problem when routing packets through the network to the intended destination. Therefore, you may need to utilize a TCP/IP-based protocol, such as MobileIP, to accommodate mobile stations. Chapter 6, "Wireless System Integration," provides details on the MobileIP protocol.

To ensure interoperability with existing standards, the 802.11 Working Group developed the standard to be compatible with other existing 802 standards, such as the following:

- *IEEE 802:* Functional Requirements
- *IEEE 802.2:* MAC Service Definition
- *IEEE 802.1-A:* Overview and Architecture
- *IEEE 802.1-B:* LAN/MAN Management
- *IEEE 802.1-D:* Transparent Bridges
- *IEEE 802.1-F:* Guidelines for the Development of Layer Management Standards
- *IEEE 802.10:* Secure Data Exchange

### Note

*At the time of this writing, key participants of the IEEE 802.11 standard effort included the following:*

*Victor Hayes, Chair*

*Stuart Kerry and Chris Zegelin, Vice Chairs*

*Bob O'Hara and Greg Ennis, Chief Technical Editors*

*George Fishel and Carolyn Heide, Secretaries*

*David Bagby, MAC Group Chair*

*Jan Boer, Direct Sequence Chair*

*Dean Kawaguchi, PHY Group and Frequency Hopping Chair*

*C. Thoman Baumgartner, Infrared Chair*

### HIPERLAN

High Performance Radio Local Area Network (HIPERLAN) is a European family of standards that specify high-speed digital wireless communication in the 5.15–5.3

GHz and the 17.1–17.3 GHz spectrum. These standards specify the Physical and Data Link Layers of network architecture, similar in scope to 802.11. However,

*continues*



*continued*

HIPERLAN operates using different protocols and is not compatible with other IEEE standards, such as IEEE 802.2 Logical Link Control.

Two stations in a HIPERLAN can exchange data directly, without any interaction from a wired network infrastructure. The simplest HIPERLAN consists of two stations. If two HIPERLAN stations are out of range with each other, a third station can relay the messages. HIPERLAN networks have the following specifications:

- Short range, approximately 150 feet (50 meters)
- Support of asynchronous and isochronous traffic
- Support of audio at 32 Kbps
- Support of video at 2 Mbps
- Support of data at 10 Mbps

HIPERLAN is unlikely to be a serious competitor to 802.11-based LANs, especially outside of Europe.

## IEEE 802.11 Topology

The IEEE 802.11 topology consists of components, interacting to provide a wireless LAN that enables station mobility transparent to higher protocol layers, such as the LLC. A station is any device that contains functionality of the 802.11 protocol (that is, MAC Layer, PHY Layer, and interface to a wireless medium). The functions of the 802.11 standard reside physically in a radio NIC, the software interface that drives the NIC, and access point. The 802.11 standard supports the following two topologies:

- Independent Basic Service Set (IBSS) networks
- Extended Service Set (ESS) networks

These networks utilize a basic building block the 802.11 standard refers to as a BSS, providing a coverage area whereby stations of the BSS remain fully connected. A station is free to move within the BSS, but it can no longer communicate directly with other stations if it leaves the BSS.

### Note

*Harris Semiconductor was the first company to offer a complete radio chip set (called PRISM) for direct sequence spread spectrum that is fully compliant with IEEE 802.11. The PRISM chip set includes six integrated microcircuits that handle all signal processing requirements of 802.11.*

## Independent Basic Service Set (IBSS) Networks

An IBSS is a stand-alone BSS that has no backbone infrastructure and consists of at least two wireless stations (see Figure 3.6). This type of network is often referred to as an *ad hoc network* because it can be constructed quickly without much planning.

The ad hoc wireless network will satisfy most needs of users occupying a smaller area, such as a single room, a sales floor, or a hospital wing.

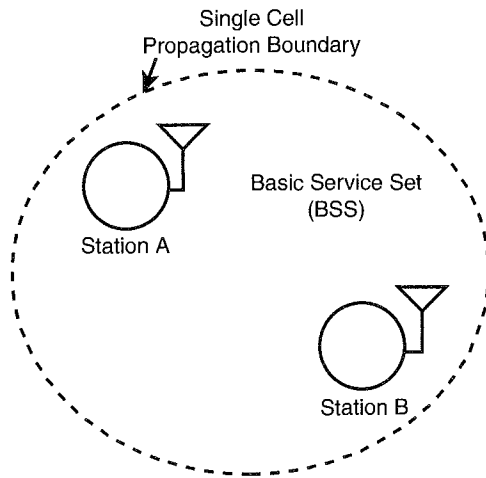


FIGURE 3.6 An independent BSS (IBSS) is the most basic type of 802.11 wireless LAN.

### Extended Service Set (ESS) Networks

For requirements exceeding the range limitations of an independent BSS, 802.11 defines an Extended Service Set (ESS) LAN, as illustrated in Figure 3.7. This type of configuration satisfies the needs of large-coverage networks of arbitrary size and complexity.

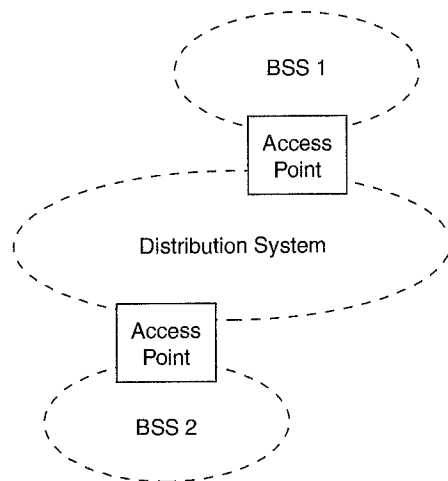


FIGURE 3.7 An Extended Service Set (ESS) 802.11 wireless LAN consists of multiple cells interconnected by access points and a distribution system, such as ethernet.

The 802.11 standard recognizes the following mobility types:

- *No-transition*: This type of mobility refers to stations that do not move and those that are moving within a local BSS.
- *BSS-transition*: This type of mobility refers to stations that move from one BSS in one ESS to another BSS within the same ESS.
- *ESS-transition*: This type of mobility refers to stations that move from a BSS in one ESS to a BSS in a different ESS.

The 802.11 standard clearly supports the no-transition and BSS-transition mobility types. The standard, however, does not guarantee that a connection will continue when making an ESS-transition.

The 802.11 standard defines the *distribution system* as an element that interconnects BSSs within the ESS via access points. The distribution system supports the 802.11 mobility types by providing logical services necessary to handle address-to-destination mapping and seamless integration of multiple BSSs. An *access point* is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC Layer.

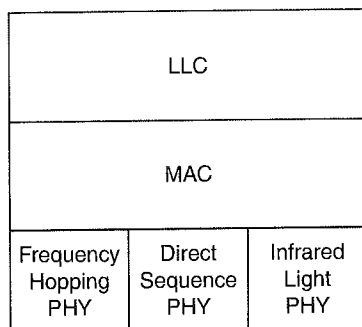
Within the ESS, the 802.11 standard accommodates the following physical configuration of BSSs:

- *BSSs that partially overlap*: This type of configuration provides contiguous coverage within a defined area, which is best if the application cannot tolerate a disruption of network service.
- *BSSs that are physically disjointed*: For this case, the configuration does not provide contiguous coverage. 802.11 does not specify a limit to the distance between BSSs.
- *BSSs that are physically collocated*: This may be necessary to provide a redundant or higher-performing network.

The 802.11 standard does not constrain the composition of the distribution system; therefore, it may be 802-compliant or some nonstandard network. If data frames need transmission to and from a non-IEEE 802.11 LAN, these frames, as defined by the 802.11 standard, enter and exit through a logical point called a *portal*. The portal provides logical integration between existing wired LANs and 802.11 LANs. When the distribution system is constructed with 802-type components, such as 802.3 (ethernet) or 802.5 (token ring), the portal and the access point become one and the same.

## IEEE 802.11 Logical Architecture

A topology provides a means of explaining necessary physical components of a network, but the *logical architecture* defines the network's operation. As Figure 3.8 illustrates, the logical architecture of the 802.11 standard that applies to each station consists of a single MAC and one of multiple PHYs.



**FIGURE 3.8** A single 802.11 MAC Layer supports three separate PHYs: frequency hopping spread spectrum, direct sequence spread spectrum, and infrared light.

## IEEE 802.11 MAC Layer

The goal of the MAC Layer is to provide access control functions (such as addressing, access coordination, frame check sequence generation and checking, and LLC PDU delimiting) for shared-medium PHYs in support of the LLC Layer. The MAC Layer performs the addressing and recognition of frames in support of the LLC. The 802.11 standard uses CSMA/CA (carrier sense multiple access with collision avoidance); whereas, standard ethernet uses CSMA/CD (carrier sense multiple access with collision detection). It is not possible to both transmit and receive on the same channel using radio transceivers; therefore, an 802.11 wireless LAN takes measures only to avoid collisions, not to detect them.

## IEEE 802.11 Physical Layers

The working group decided in July 1992 to concentrate its radio frequency studies and standardization efforts on the 2.4 GHz spread spectrum ISM bands for both the direct sequence and frequency hopping PHYs. The final standard specifies 2.4 GHz because this band is available license free in most parts of the world. The FCC Part 15 in the United States governs the radiated RF power in the ISM bands. Part 15 limits antenna gain to 6 dBi maximum and radiated power to one watt within the United States. European and Japanese regulatory groups limit radiated power to 10 milliwatts per 1 MHz. The actual frequencies authorized for use in the United States, Europe, and Japan differ slightly.



In March 1993, the 802.11 committee began receiving proposals for a direct sequence Physical Layer standard. After much discussion and debate, the committee agreed to include a chapter in the standard specifying the use of direct sequence. The direct sequence Physical Layer specifies two data rates:

- 2 Mbps using Differential Quaternary Phase Shift Keying (DQPSK) modulation
- 1 Mbps using Differential Binary Phase Shift Keying (DBPSK)

The standard defines seven direct sequence channels. One channel is exclusively available for Japan. Three channel pairs are defined for the United States and Europe. Channels in a pair can work without interference. In addition, the channels of all three pairs can be used simultaneously for redundancy or higher performance by developing a frequency plan that avoids signal conflicts.

In contrast to direct sequence, the 802.11-based frequency hopping PHY uses radios to send data signals by hopping from one frequency to another, transmitting a few bits on each frequency before shifting to a different one. Frequency hopping systems hop in a pattern that appears to be random, but really has a known sequence. A particular hop sequence is commonly referred to as a *frequency hopping channel*. Frequency hopping systems tend to be less costly to implement and do not consume as much power as their direct sequence counterpart, making them more suitable for portable applications. However, frequency hopping is much less tolerant of multiple-path and other interference sources. The system must retransmit data if it becomes corrupted on one of the hop sequence frequencies.

The 802.11 committee defined the frequency hopping Physical Layer to have a 1 Mbps data rate using 2-level Gaussian frequency shift keying (GFSK). This specification describes 79 channel center frequencies identified for the United States, from which there are three sets of 22 hopping sequences defined.

The infrared Physical Layer describes a modulation type that operates in the 850 to 950 nM band for small equipment and low-speed applications. The basic data rate of this infrared medium is 1 Mbps using 16-PPM (pulse position modulation) and an enhanced rate of 2 Mbps using 4-PPM. Peak power of infrared-based devices are limited to a peak power of 2 watts.

As with the IEEE 802.3 standard, the 802.11 Working Group is considering additional PHYs as applicable technologies become available.

For an inside look of each layer of the 802.11 standard, refer to Chapter 4, "Medium Access Control (MAC) Layer," and Chapter 5, "Physical (PHY) Layer."



## IEEE 802.11 Services

The 802.11 standard defines *services* that provide the functions that the LLC Layer requires for sending MSDUs (MAC service data units) between two entities on the network. These services, which the MAC Layer implements, fall into two categories:

- Station services
  - Authentication
  - Deauthentication
  - Privacy
  - MSDU delivery
- Distribution system services
  - Association
  - Disassociation
  - Distribution
  - Integration
  - Reassociation

The following sections define the station and distribution system services.

### Station Services

The 802.11 standard defines services for providing functions among stations. A station may be within any wireless element on the network, such as a handheld PC or handheld scanner. In addition, all access points implement station services. To provide necessary functionality, these stations need to send and receive MSDUs and implement adequate levels of security.

#### Authentication

Because wireless LANs have limited physical security to prevent unauthorized access, 802.11 defines authentication services to control LAN access to a level equal to a wired link. All 802.11 stations, whether they are part of an independent BSS or ESS network, must use the authentication service prior to establishing a connection (referred to as an association in 802.11 terms) with another station with which they will communicate. Stations performing authentication send a unicast management authentication frame to the corresponding station.

The IEEE 802.11 standard defines the following two authentication services:

- *Open system authentication*: This is the 802.11 default authentication method, which is a very simple, two-step process. First the station wanting to

authenticate with another station sends an authentication management frame containing the sending station's identity. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.

- *Shared key authentication:* This type of authentication assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of shared key authentication requires implementation of the Wireless Equivalent Privacy algorithm.

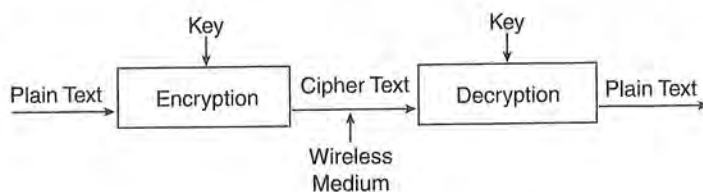
### Deauthentication

When a station wishes to *disassociate* with another station, it invokes the *deauthentication* service. Deauthentication is a notification, and cannot be refused. Stations perform deauthentication by sending an authentication management frame (or group of frames to multiple stations) to *advise* the termination of authentication.

### Privacy

With a wireless network, all stations and other devices can “hear” data traffic taking place within range on the network, seriously impacting the security level of a wireless link. IEEE 802.11 counters this problem by offering a privacy service option that raises the security level of the 802.11 network to that of a wired network.

The privacy service, applying to all data frames and some authentication management frames, is based on the 802.11 *Wired Equivalent Privacy (WEP)* algorithm that significantly reduces risks if someone eavesdrops on the network. This algorithm performs encryption of messages, as shown in Figure 3.9. With WEP, all stations initially start “in the clear”—that is, unencrypted. Refer to Chapter 4, in the section titled “Private Frame Transmissions,” for a description of how WEP works.



**FIGURE 3.9** The Wired Equivalent Privacy (WEP) algorithm produces ciphertext, keeping eavesdroppers from “listening in” on data transmissions.

### Note

The WEP protects RF data transmissions using a 64-bit seed key and the RC4 encryption algorithm. When enabled, WEC only protects the data packet information. Physical Layer headers are left unencrypted so that all stations can properly receive control information for managing the network.

## Distribution System Services

Distribution system services, as defined by 802.11, provide functionality across a distribution system. Access points provide distribution system services. The following sections provide an overview of the services that distribution systems need to provide proper transfer of MSDUs.

### Association

Each station must initially invoke the *association service* with an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point. Each station can associate with only a single access point, but each access point can associate with multiple stations. Association is also a first step to providing the capability for a station to be mobile between BSSs.

### Disassociation

A station or access point may invoke the *disassociation service* to terminate an existing association. This service is a notification; therefore, neither party may refuse termination. Stations should disassociate when leaving the network. An access point, for example, may disassociate all its stations if being removed for maintenance.

### Distribution

A station uses the *distribution service* every time it sends MAC frames across a distribution system. The 802.11 standard does not specify how the distribution system delivers the data. The distribution service provides the distribution system with only enough information to determine the proper destination BSS.

### Integration

The *integration service* enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN. The integration function performs all required media or address space translations. The details of an integration function depends on the distribution system implementation and are beyond the scope of the 802.11 standard.

### Reassociation

The *reassociation service* enables a station to change its current state of association. Reassociation provides additional functionality to support BSS-transition mobility for associated stations. The reassociation service enables a station to transition its association from one access point to another. This keeps the distribution system informed of the current mapping between access point and station as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the station remains associated with the same access point. The mobile station always initiates the reassociation service.

**Note**

IEEE 802.11 allows a client to roam among multiple access points that may be operating on the same or separate channels. To support the roaming function, each access point typically transmits a beacon signal every 100 milliseconds. Roaming stations use the beacon to gauge the strength of their existing access point connection. If the station senses a weak signal, the roaming station can implement the reassociation service to connect to an access point emitting a stronger signal.

**Case Study 3.5:  
Reassociation Provides Roaming**

A grocery store in Gulfport, Mississippi, has a bar code-based shelf inventory system that helps the owners of the store keep track of what to stock, order, and so on. Several of the store clerks use handheld scanners during the store's closed hours to perform inventory functions. The store has a multiple cell 802.11-compliant wireless LAN (that is, ESS) consisting of access points A and B interconnected by an ethernet network. These two access points are sufficient to cover the store's entire floorspace and backroom.

At one end of the store in the frozen meat section, a clerk using a handheld device may associate with access point A. As the person walks with the device to the beer-and-wine section on the other end of the store, the mobile scanner (that is, the 802.11 station within the scanner) will begin sensing a signal from access point B. As the signal from B becomes stronger, the station will then *reassociate* with access point B, offering a much better signal for transmitting MSDUs.

**Station States and Corresponding Frame Types**

The state existing between a source and destination station (see Figure 3.10) governs which IEEE 802.11 frame types the two stations can exchange.

The following types of functions can occur within each class of frame:

- Class 1 Frames
  - Control Frames
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgment (ACK)
    - Contention-free (CF)
  - Management Frames
    - Probe request/response
    - Beacon
    - Authentication



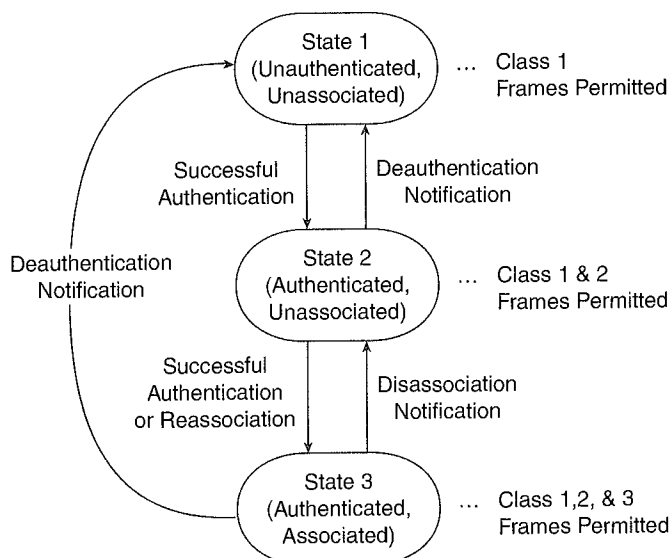


FIGURE 3.10 The operation of a station depends on its particular state.

Deauthentication

Announcement traffic indication message (ATIM)

- Data Frames
- Class 2 Frames
  - Management Frames
    - Association request/response
    - Reassociation request/response
    - Disassociation
- Class 3 Frames
  - Data Frames
  - Management Frames
    - Deauthentication
  - Control Frames
    - Power Save Poll

To keep track of station state, each station maintains the following two state variables:

- *Authentication state*: Has values of either unauthenticated and authenticated
- *Association state*: Has values of either unassociated and associated

## Implications of the IEEE 802.11 Standard

As with any technologies and standards, one must be aware of the implications surrounding the implementation of wireless networks based on the IEEE 802.11 standard. Chapter 1, in the section “Wireless Network Concerns,” discusses the general issues of implementing wireless networks. In addition to these problems, the following are a couple of implications specifically related to the IEEE 802.11 standard:

- *Relatively low data rates:* As mentioned before, the 802.11 standard currently supports data rates up to 2 Mbps. Some end users and vendors claim this data rate is too low. In some cases, this is true; but in other cases, it is not true. Video transmissions, for example, may require higher data rates if applications need frame rates, pixel depth, and resolutions that require greater amounts of bandwidth. Large data block transmissions may also require higher data rates to keep transmission delays tolerable.

On the other hand, bar code applications, such as receiving, inventory, and price marking, generally work well under the 2 Mbps limitation of the current 802.11 standard.

- *Lack of standard roaming across multiple-vendor access points:* The 802.11 standard does not define the protocols necessary to move 802.11 frames within the distribution system because it falls outside the scope of 802-type LANs. The Network and Transport Layers are left to address distribution system protocols. As a result, the 802.11 standard does not define communications *between* access points.

Currently, it is up to the access point vendors to define the protocols necessary to support roaming from one access point to another. To be safe, you should consider purchasing access points from a single vendor, although you can mix-and-match radio cards in the appliances. Chapter 6, “Wireless System Integration,” discusses industry standards, such as the Inter Access Point Protocol (IAPP) specification, that are beginning to define multiple-vendor roaming protocols.

## IEEE 802.11 Standard Compliance

No standard is worthwhile unless vendors and end users comply with it. The following sections describe activities taking place to ensure compliance with 802.11.

### Vendor Compliance

Most wireless LAN vendors (that is, manufacturers of the hardware) are releasing initial radio cards and access points throughout 1998 and 1999 that comply with the official 802.11 standard. Before deeming their devices as 802.11 compliant, they must follow the protocol implementation compliance procedures that the 802.11 standard specifies in its appendix. The procedures state that the vendor shall

complete a Protocol Implementation Conformance Statement (PICS) proforma. The structure of the PICS proforma mainly includes a list of fixed questions that the vendor responds to with yes or no answers, indicating adherence to the standard. The PICS can have the following uses:

- A checklist that helps the vendor reduce the risk of failure to conform to the standard
- For the vendor and system implementor to better understand what 802.11-compliance means
- As a basis for designing an interface between the 802.11 device and another network or system
- As the basis for developing protocol conformance tests and simulations

To ensure proper compliance, vendors test their products at the InterOperability Laboratory located at the Leavitt Center on the campus of The University of New Hampshire. In March 1997, for example, Aironet Wireless Communications, Inc.; Breezecom Wireless Communications; Netwave Technologies, Inc.; Proxim Inc.; Raytheon Electronics; and Symbol Technologies performed joint interoperability testing to advance customer adoption of wireless technology. In some cases, users can upgrade their existing proprietary radio cards to be 802.11 compliant by just reinstalling NIC interface software on their appliances.

#### Note

*Vendors are easing the transition to 802.11-compliant radio networks by offering relatively simple ways to upgrade existing radio LAN devices. Symbol, Inc., for example, offers a firmware upgrade to your existing Symbol 2.4 GHz (Spectrum 24) networks, avoiding the purchase of new network adapters.*

---

The InterOperability Laboratory, founded in 1988, performs research and development work and is used by more than 100 vendors to verify the interoperability and conformance of their computer communications products. The University of New Hampshire encourages vendors to conduct interoperability testing by providing facilities for a multiple-vendor test environment. The goal of the laboratory is to provide complete testing for all networking products, including ethernet, ADSL, ATM, fast ethernet, FDDI, FDSE, Fibre Channel, gigabit ethernet, IP/Routing, Network Management, and Wireless.

#### Note

*Be aware that in 1997 some vendors released "802.11-compliant" wireless LAN radio cards and access points that were not certified as compliant with the final 802.11 standard. These products may or may not operate within the final official standard.*

---



**WLI Forum**

The Wireless LAN Interoperability Forum (WLI Forum), a not-for-profit corporation founded in March 1996, promotes the growth of the wireless LAN market by delivering interoperable products and services. The Forum consists primarily of appliance suppliers/vendors (such as Hewlett-Packard, Fujitsu, Monarch Marking Systems, and Handheld Products) having products that operate on the WLI Forum's OpenAir™ wireless network. The Forum provides certification via an independent third-party test lab to ensure proper compliance.

The OpenAir™ specification describes a MAC and radio frequency Physical Layer, similar in scope to the 802.11 specification. The OpenAir™ network is based on Proxim's RangeLAN2 protocol, employing frequency hopping spread spectrum technology in the unlicensed 2.4 GHz ISM band. The OpenAir™ operates at a data rate of 1.6 Mbps per channel, with 15 independent channels (hopping patterns) available. This architecture enables up to 15 wireless LANs to overlap independently in the same physical space,

providing up to 24 Mbps of aggregate network bandwidth.

The WLI Forum wrote the OpenAir™ specification to motivate third-party development of compatible products. At the time, with no official IEEE standard on wireless networking, the Forum decided to base its specification on Proxim's product. Soon after the release of the 802.11 specification in June 1997, the WLI Forum announced its support for the adoption of the IEEE 802.11 standard and urged the supplier community to move toward conformance. As a result, the WLI Forum is likely to establish conformity to the IEEE 802.11 standard as well.

The WLI Forum is a worldwide organization, and is completely self funded through membership dues and fees. Membership is open to all companies that develop, manufacture, or sell wireless LAN products or services. For more information on the WLI Forum, visit their Web site located at <http://www.wlif.com>.

**End-User Compliance**

Throughout 1999 and beyond, end users should begin widespread implementations of 802.11-compliant LANs. As an end user, do you need to purchase and use products that comply with the 802.11 standard? Of course the answer is no, but you should carefully consider the advantages and disadvantages of implementing 802.11-compliant networks. Most likely, complying with 802.11 will be favored over the use of proprietary networks unless extenuating circumstances prevail. If the decision is to go with 802.11, you will be starting with one of the following scenarios:

- No existing implementation of wireless LANs
- Existing implementation of proprietary wireless LANs

If you are an end user with no existing installation of wireless networking components, compliance with the 802.11 standard is easy. Right? Actually, it is not as sim-



ple as it seems. The 802.11 standard is not as Plug and Play as the 802.3 ethernet standard. With 802.11, you must first decide which version of 802.11 best satisfies your needs. You might consider the following questions:

- *What type of modulation do I need?* Do I have radio interference implications that lean toward using the infrared PHY? Does the application require wider area coverage that may depend on the longer range capability of one of the spread spectrum PHYs? If the choice is spread spectrum, should I use direct sequence or frequency hopping?
- *Will the application require roaming across BSS cells interconnected by access points of different vendors?* If yes, you will need to think about how to provide roaming between access points.
- *Does the network require the optional WEP security?* If the answer is yes, be sure to choose wireless devices having WEP available.
- *Do the appliances I need to comply with have the 802.11 options I have chosen?* If not, you need to choose options that comply with the appliance, or you must choose different appliances.

Answers to the preceding questions define the options you need to consider when planning to purchase radio cards and access points complying with 802.11.

If proprietary wireless LANs already exist, you will need to either upgrade or replace the existing network to make it compliant with 802.11. Many of the vendors offer free upgrades to make your existing wireless LANs (if they are of a recent enough version) compliant with 802.11. BreezeCOM, for example, guarantees software upgrades to the IEEE 802.11 standard for its BreezeNET PRO product line.

If it is not possible or feasible to upgrade your existing wireless LAN, then of course you must perform a complete replacement if benefits outweigh the expenses. The replacement of the network will be difficult to cost-justify; however, it may become necessary as proprietary wireless components become obsolete.

### **International Electromagnetic Compliance**

The 802.11 standard specifies operation in the 2.4 GHz band; however, electromagnetic compatibility requirements vary from one country to another. Operating frequencies, power levels, and spurious levels differ throughout the world.

Regional and national regulatory administrations of each individual country demand certification of wireless equipment. The 802.11 standard, however, identifies the minimum technical requirements for interoperability and compliance based on established regulations for Europe, Japan, and the North America. Therefore, wireless LAN vendors must be aware of all current regulatory requirements prior to releasing a product for sale in a particular country. The following agencies and

documents specify the current regulatory requirements for various geographical areas:

Canada

- *Approval standards:* Industry Canada (IC)
- *Documents:* GL36
- *Approval authority:* Industry Canada

Europe

- *Approval standards:* European Telecommunications Standards Institute
- *Documents:* ETS 300-328, ETS 300-339
- *Approval authority:* National Type Approval Authorities

France

- *Approval standards:* La Reglementation en France por les Equipements fonctionnant dans la bande de frequences 2,4 GHz "RLAN-Radio Local Area Network"
- *Documents:* SP/DGPT/ATAS/23, ETS 300-328, ETS 300-339
- *Approval authority:* Direction Generale des Postes et Telecommunications

Japan

- *Approval standards:* Research and Development Center for Radio Communications (RCR)
- *Documents:* RCR STD-33A
- *Approval authority:* Ministry of Telecommunications (MKK)

Spain

- *Approval standards:* Suplemento del Numero 164 del Boletin Oficial del Estado (published 10 July 91; revised 25 June 93)
- *Documents:* ETS 300-328, ETS 300-339
- *Approval authority:* Cuadro Nacional De Atribucion De Frecuencias

The United States of America

- *Approval standards:* Federal Communications Commission (FCC)
- *Documents:* CFR47, Part 15, Sections 15.205, 15.209, 15.247
- *Approval authority:* FCC

Operation in countries within Europe and other areas outside Japan or North America may be subject to additional regulations.

## IEEE 802.11 Working Group Operations

The 802.11 Working Group is a part of the IEEE LAN MAN Standards Committee (LMSC), which reports to the Standards Activity Board (SAB) of the IEEE Computer Society. IEEE 802.11 meetings are open to anyone. The only requirement to attend is to pay dues, which offset meeting expenses. Most of the active participants are representatives from companies developing wireless LAN components. The IEEE bylaws explain that to vote on standards activities, however, you must become a member by participating in at least two out of four consecutive plenary meetings. Then, you must continue to attend meetings to maintain voting status. The 802.11 Working Group meets three times a year during the plenary sessions of the IEEE 802 and three times a year between plenary sessions.

The IEEE 802.11 Working Group consists of about 200 members; membership falls into the following categories:

- *Voting members:* Those who have maintained voting status.
- *Nearly members:* Those who have participated in two sessions of meetings, one of which being a plenary session. Nearly members become voting members in the first session they attend following their qualification for nearly membership.
- *Aspirant members:* Those who have participated in one plenary or interim session meeting.
- *Sleeping voting members:* Those who were once voting members, but have chosen to discontinue.

## Future of the IEEE 802.11 Standard

What is the future of IEEE 802.11? Will end users eventually fully comply with the standard? Will the 802.11 Working Group solve implications revolving around the standard? Only time will tell for certain. It is known today, however, that all major wireless LAN vendors are releasing 802.11-compliant wireless LANs throughout 1998, and these vendors are making it fairly easy for end users to upgrade their existing systems. This, combined with the advantages of standardization, should proliferate the use of 802.11-compliant networks.

To solve implications of the current release of the standard, the IEEE 802.11 Working Group is actively working on the following projects that will aid the widespread acceptance of the standard:

- *802.11rev: Revision of IEEE Standard 802.11-1997:* This project was charted to rectify a number of errors in the current standard and to accommodate input from the JTC1 review to result in a single JTC1/IEEE standard.

- *802.11a: Extension of the IEEE Standard 802.11-1997 with a higher data rate PHY in the 5 GHz band:* This project was initiated to develop a high speed (about 20 Mbps) wireless PHY suitable for data, voice, and image information services in fixed, moving, or portable wireless local area networks. The project concentrates on improving spectrum efficiency and will review the existing 802.11 MAC to ensure its capability to operate at the higher speeds.

The IEEE 802.11 Working Group will actively correspond with regulatory bodies worldwide to encourage spectrum allocations that match these frequencies.

- *802.11b: Extension of the IEEE Standard 802.11-1997 with a higher data rate PHY in the 2.4 GHz band:* The purpose of this project is to extend the performance and the range of applications of the existing 802.11 standard. The header of the two existing radio-based PHYs can support data rates up to 4.5 Mbps for frequency hopping and up to 25.5 Mbps for direct sequence. This project will investigate ways to exploit these data rate capabilities and analyze the capability of the existing 802.11 MAC to support higher data rates.

The actual data rates targeted by this project are at least 3 Mbps for the frequency hopping PHY and at least 8 Mbps for the direct sequence PHY. As with project 802.11a, IEEE 802.11 will correspond with regulatory bodies worldwide to ensure that the proposed extension will be applicable as widely as possible.

In addition to the preceding official projects, the 802.11 Working Group is actively studying the needs for standardization of wireless communications of wearable computing devices. The study is examining the requirements for Wireless Personal Area Networking (WPAN) of devices that are worn or carried by individuals. The objectives of the study group are as follows:

- Review WPAN requirements.
- Determine the need for a standard.
- If a standard is necessary, draft a PAR for submittal.
- Seek appropriate sponsorship within 802.

The study group is soliciting industry input on market requirements and technical solutions for a WPAN with 0-to-30-foot range, data rates of less than 1 Mbps, low power consumption, small size (less than 0.5 cubic inches), and low cost relative to target device.

As mentioned in this chapter, the 802.11 wireless LAN standard certainly has benefits that an organization should consider when selecting components that provide LAN mobility. IEEE 802 is a solid family of standards that will provide much greater multiple-level interoperability than proprietary systems.



Wireless LANs conforming to 802.11 provide interoperability between radio cards and access points. The 802.11 standard has the backing of IEEE, having an excellent track record of developing long-lasting standards, such as IEEE 802.3 (ethernet) and IEEE 802.5 (token ring). When designing a wireless LAN, definitely consider the use of 802.11-compliant products, but ensure that the data rates of 802.11 will support your application and that the chosen components support roaming between access points.

With 802.11, system implementors have several choices. You will need to choose the type of physical medium, for example: frequency hopping spread spectrum, direct sequence spread spectrum, or infrared light. This concept is similar to choosing between twisted-pair, optical-fiber, and coaxial cable in an ethernet LAN. You will also need to determine how to interface wireless devices with server operating systems and applications. In defining these elements, be sure the resulting network supports all requirements.

# APPENDIX C

# *New Economy; Airborne and grass roots. By popular acclaim, a wireless format with a name only a geek could love is taking hold.*

By John Markoff

Oct. 30, 2000

See the article in its original context from  
October 30, 2000, Section C, Page 5    [Buy Reprints](#)

[VIEW ON TIMESMACHINE](#)

TimesMachine is an exclusive benefit for home  
delivery and digital subscribers.

AT the recent Agenda 2001 computer conference in Phoenix earlier this month, there was validation and a touch of irony for the conference organizer, Robert Metcalfe, co-inventor of the Ethernet office networking standard.

Hundreds of those attending the conference sat in a huge auditorium with their portable computers wirelessly linked to the Internet via tiny PC cards plugged in to their machines.

It was tacit validation of a theorem Mr. Metcalfe set forth years ago, now widely known as Metcalfe's Law, which states that "the usefulness, or utility, of a network equals the square of the number of users."

The irony, of course, was that while many of the conference participants were using a technology that essentially provides wireless connections at Ethernet speeds, they were using it to read their e-mail and surf the Web rather than pay much attention to Mr. Metcalfe's conference.

There is no doubt, however, that "wireless Ethernet"-- formally known as the 802.11b wireless technical standard as specified by the Institute of Electrical and Electronics Engineers -- is finally taking off.

The Ethernet standard for wiring computers into local networks caught on two decades ago because it was "open" -- owned by no single company and available for many to adopt and improve. Those same characteristics could propel wireless Ethernet as embodied in the 802.11b standard, which allows data to be transmitted at 11 megabits -- 11 million bits a second.

The 802.11b format is catching on so quickly that it is displacing alternative wireless competitors that include Bluetooth and HomeRF. The cost of 802.11b technology continues to plummet; chip sets that cost as little as \$10 or less may arrive in the next two years. So it should become cheaper and easier to set up an office network wirelessly than with traditional Ethernet wires.

To be sure, there are some clouds ahead. The 802.11b wireless transmitters operate on the 2.4 gigahertz radio band, which does not require a license to use. Some technical experts worry that this band may soon grow so congested that it will create the world's first wireless data gridlock.

The standard, first popularized by Apple Computer in its Airport line of wireless products last year, is now being embraced so quickly that it is touching off a wireless "air rush" as start-up companies and telecommunication vendors vie to lock up valuable sites at airports, hotels and other public hot spots. Such companies operate the Internet server computers by which wireless users actually connect to the global network.

The appearance of the wireless standard in public spaces is following on the heels of installations on university campuses and corporate office parks. And some community 802.11b wireless networks have been set up, including SFlan in San Francisco.

As part of SFlan, some Internet hobbyists have set up inexpensive 802.11b networks on their rooftops and are distributing Internet service throughout their neighborhoods. One user, Tim Pozar, said his local network reached a half-mile radius around his home.

Brewster Kahle, a computer network expert who has led the SFlan project, said, "It's possible that a grass-roots broadband network could be built organically."

But for now, commercial efforts seem to be gathering steam most quickly. There have been a series of announcements in recent weeks by wireless companies including Aerzone , Mobilstar and Wayport, that have struck deals with airports and hotels to install 802.11b.

Just last Friday, United Airlines said it was teaming with Aerzone, a San Francisco-based subsidiary of Softnet Systems, to deploy 802.11b in Red Carpet Club airport lounges, gate areas and terminals in as many as 50 airports served by the airline.



"This is potentially a huge business because we offer the two things people want most: relatively unlimited bandwidth and mobility," said Lawrence B. Brilliant, chief executive of Aerzone.

Just two days earlier Wayport, based in Austin, Tex., announced it was installing 802.11b in the lobbies of 15 hotels in the Los Angeles area. Wayport has already started its service at the Dallas-Fort Worth International Airport and the Austin Bergstrom airport.

And while so far Apple and I.B.M. are the only two computer makers to offer portable systems with built-in 802.11b capability, by early next year the standard is expected to become a common built-in feature on all makes of portable computers.

Meanwhile, a number of sports stadium deals have been announced and several of the wireless start-up companies say they have been in talks with Starbucks to offer wireless Internet service in the company's nationwide chain of coffee shops.

Indeed the possibility of Starbucks's encouraging customers to spend time sipping coffee in its stores while they read their e-mail has created a new technology buzz-phrase: the "high-loiter retail" marketplace, in the words of Brett Stewart, Wayport's president and founder.

The wireless networks based on 802.11b are also becoming popular as a convenient and low-cost way to create a network within homes already connected to the Internet through D.S.L. or cable modems.

All this activity raises the possibility that 802.11b might upset the plans of some of the big telecommunications giants that are planning to spend millions of dollars building third-generation data and voice cellular networks. If millions of computer users and companies effectively build their own high-speed data network from the ground up, the telecommunications carriers might think twice about putting money into third-generation systems.

The 802.11b standards offer far greater speed than the proposed third-generation network standards, which generally offer two megabits that must be shared by all the users of a single cell. And the industry is finishing a standard called 802.11a, which will allow even higher speed -- 54 megabits a second -- on the 5 gigahertz radio band.

In fact, a top Microsoft executive, Craig Mundie, said his company was trying to rally the computer and telecommunications industries to agree upon that standard for the future of wireless data networking.

If the largely spontaneous 802.11 wave does swamp the various other wireless data networking standards, it might be fitting. After all, it was as an anarchic self-assembling world of isolated networks that the Internet originally came into being.

3/16/2021

New Economy; Airborne and grass roots. By popular acclaim, a wireless format with a name only a geek could love is taking hold. - The ...

A version of this article appears in print on , Section C, Page 5 of the National edition with the headline: New Economy; Airborne and grass roots.  
By popular acclaim, a wireless format with a name only a geek could love is taking hold.

# APPENDIX D

## Abstract

A few years ago it was recognized that the vision of a truly low-cost, low-power radio-based cable replacement was feasible. Such a ubiquitous link would provide the basis for portable devices to communicate together in an ad hoc fashion by creating personal area networks which have similar advantages to their office environment counterpart, the local area network. Bluetooth™ is an effort by a consortium of companies to design a royalty-free technology specification enabling this vision. This article describes the radio system behind the Bluetooth concept. Designing an ad hoc radio system for worldwide usage poses several challenges. The article describes the critical system characteristics and motivates the design choices that have been made.

# The Bluetooth Radio System

Jaap C. Haartsen, Ericsson Radio Systems B.V.

In the last decades, progress in microelectronics and very large scale integration (VLSI) technology has fostered the widespread use of computing and communication devices for commercial usage. The success of consumer products like PCs, laptops, personal digital assistants (PDAs), cell phones, cordless phones, and their peripherals has been based on continuous cost and size reduction. Information transfer between these devices has been cumbersome, mainly relying on cables. Recently, a new universal radio interface has been developed enabling electronic devices to communicate wirelessly via short-range ad hoc radio connections. The Bluetooth technology — which has gained the support of leading manufacturers like Ericsson, Nokia, IBM, Toshiba, Intel, and many others — eliminates the need for wires, cables, and the corresponding connectors between cordless or mobile phones, modems, headsets, PDAs, computers, printers, projectors, and so on, and paves the way for new and completely different devices and applications. The technology enables the design of low-power, small-sized, low-cost radios that can be embedded in existing (portable) devices. Eventually, these embedded radios will lead toward ubiquitous connectivity and truly connect everything to everything. Radio technology will allow this connectivity to occur without any explicit user interaction.

This article describes the basic design and technology trade-offs which have led to the Bluetooth radio system. We describe some fundamental issues regarding ad hoc radio systems. We give an overview of the Bluetooth system itself with the emphasis on the radio architecture. It explains how the system has been optimized to support ad hoc connectivity. We also describe the Bluetooth specification effort.

## Ad Hoc Radio Connectivity

The majority of radio systems in commercial use today are based on a cellular radio architecture. A mobile network established on a wired backbone infrastructure uses one or more base stations placed at strategic positions to provide local cell coverage; users apply portable phones, or more generic mobile terminals, to access the mobile network; the terminals maintain a connection to the network via a radio link to the base stations. There is a strict separation between the base stations and the terminals. Once registered to the network, the terminals remain locked to the control channels in the network, and connections can be established and released according to the control channel protocols. Channel access, channel allocation, traffic control, and interference minimization are neatly con-

trolled by the base stations. Examples of these conventional radio systems are the public cellular phone systems like Global System for Mobile Communications (GSM), D-AMPS, and IS-95 [1–3], but also private systems like wireless local area network (WLAN) systems based on 802.11 or HIPERLAN I and HIPERLAN II [4–6], and cordless systems like Digital Enhanced Cordless Telecommunications (DECT) and Personal Handyphone System (PHS) [7, 8].

In contrast, in truly ad hoc systems, there is no difference between radio units; that is, there are no distinctive base stations or terminals. Ad hoc connectivity is based on peer communications. There is no wired infrastructure to support connectivity between portable units; there is no central controller for the units to rely on for making interconnections; nor is there support for coordination of communications. In addition, there is no intervention of operators. For the scenarios envisioned by Bluetooth, it is highly likely that a large number of ad hoc connections will coexist in the same area without any mutual coordination; that is, tens of ad hoc links must share the same medium at the same location in an uncoordinated fashion. This is different from ad hoc scenarios considered in the past, where ad hoc connectivity focused on providing a single (or very few) network(s) between the units in range [4, 5]. For the Bluetooth applications, typically many independent networks overlap in the same area. This will be indicated as a scatter ad hoc environment. Scatter ad hoc environments consist of multiple networks, each containing only a limited number of units. The difference between a conventional cellular environment, a conventional ad hoc environment, and a scatter ad hoc environment is illustrated in Fig. 1. The environmental characteristics the ad hoc radio system has to operate in have a major impact on the following fundamental issues:

- Applied radio spectrum
- Determining which units are available to connect to
- Connection establishment
- Multiple access scheme
- Channel allocation
- Medium access control
- Service prioritization (i.e., voice before data)
- (Mutual) interference
- Power consumption

Ad hoc radio system have been in use for some time, for example, walky-talky systems used by the military, police, fire departments, and rescue teams in general. However, the Bluetooth system is the first commercial ad hoc radio system envisioned to be used on a large scale and widely available to the public.

## Bluetooth Radio System Architecture

In this section the technical background of the Bluetooth radio system is presented. It describes the design trade-offs made in order to optimize the ad hoc functionality and addresses the issues listed above.

### Radio Spectrum

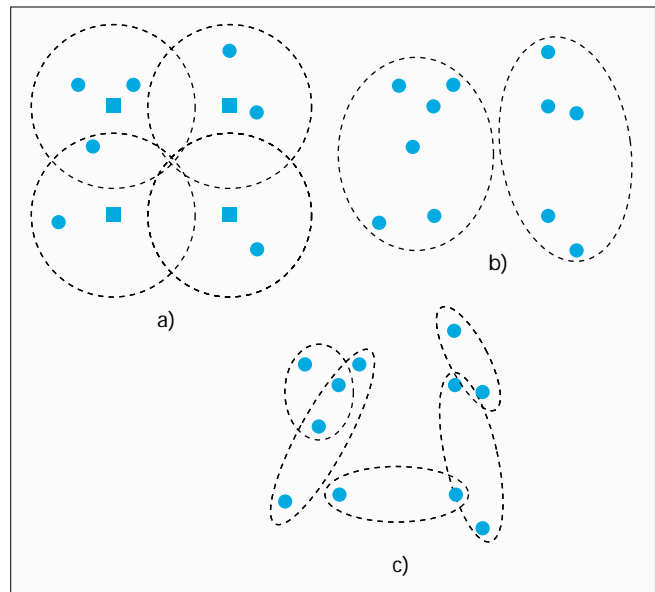
The choice of radio spectrum is first determined by the lack of operator interaction. The spectrum must be open to the public without the need for licenses. Second, the spectrum must be available worldwide. The first Bluetooth applications are targeted at the traveling businessperson who connects his/her portable devices wherever he/she goes. Fortunately, there is an unlicensed radio band that is globally available. This band, the Industrial, Scientific, Medical (ISM) band, is centered around 2.45 GHz and was formerly reserved for some professional user groups but has recently been opened worldwide for commercial use. In the United States, the band ranges from 2400 to 2483.5 MHz, and the FCC Part 15 regulations apply. In most parts of Europe,<sup>1</sup> the same band is available under the ETS-300328 regulations. In Japan, recently the band from 2400 to 2500 MHz has been allowed for commercial applications and has been harmonized with the rest of the world. Summarizing, in most countries of the world, free spectrum is available from 2400 MHz to 2483.5 MHz, and harmonization efforts are ongoing to have this radio band available truly worldwide.

The regulations in different parts of the world differ. However, their scope is to enable fair access to the radio band by an arbitrary user. The regulations generally specify the spreading of transmitted signal energy and maximum allowable transmit power. For a system to operate globally, a radio concept has to be found that satisfies all regulations simultaneously. The result will therefore be the minimum denominator of all the requirements.

### Interference Immunity

Since the radio band is free to be accessed by any radio transmitter as long as it satisfies the regulations, interference immunity is an important issue. The extent and nature of the interference in the 2.45 GHz ISM band cannot be predicted. Radio transmitters may range, for example, from 10 dBm baby monitors to 30 dBm WLAN access points. With high probability, the different systems sharing the same band will not be able to communicate. Coordination is therefore not possible. More of a problem are the high-power transmitters covered by the FCC part 18 rules which include, for example, microwave ovens and lighting devices. These devices fall outside the power and spreading regulations of part 15, but still coexist in the 2.45 GHz ISM band. In addition to interference from external sources, co-user interference must be taken into account, which results from other Bluetooth users.

Interference immunity can be obtained by interference suppression or avoidance. Suppression can be obtained by coding or direct-sequence spreading. However, the dynamic range of the interfering and intended signals in an ad hoc, uncoordinated radio environment can be huge. Taking into account the distance ratios and power differences of uncoordinated transmitters, near-far ratios in excess of 50 dB are no exception. With desired user rates on the order of 1 Mb/s and beyond, practically attained coding and processing gains are inadequate. Instead, interference avoidance is more attractive



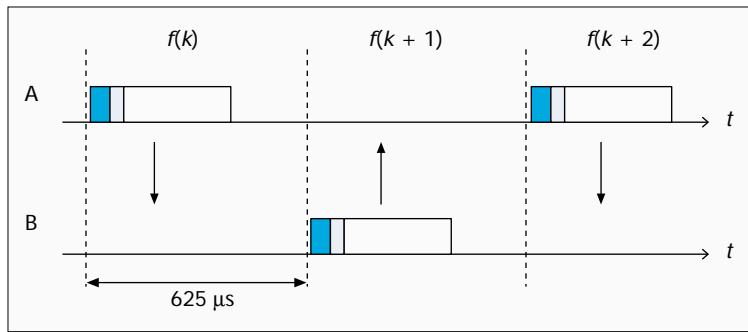
■ **Figure 1.** Topologies for: a) cellular radio systems with squares representing stationary base stations; b) conventional ad hoc systems; and c) scatter ad hoc systems.

since the desired signal is transmitted at points in frequency and/or time where interference is low or absent. Avoidance in time can be an alternative if the interference concerns a pulsed jammer and the desired signal can be interrupted. Avoidance in frequency is more practical. Since the 2.45 GHz band provides about 80 MHz of bandwidth and most radio systems are band-limited, with high probability a part of the radio spectrum can be found where there is no dominant interference. Filtering in the frequency domain provides the suppression of the interferers at other parts of the radio band. The filter suppression can easily arrive at 50 dB or more.

### Multiple Access Scheme

The selection of the multiple access scheme for ad hoc radio systems is driven by the lack of coordination and the regulations in the ISM band. Frequency-division multiple access (FDMA) is attractive for ad hoc systems since channel orthogonality only relies on the accuracy of the crystal oscillators in the radio units. Combined with an adaptive or dynamic channel allocation scheme, interference can be avoided. Unfortunately, pure FDMA does not fulfill the spreading requirements set in the ISM band. Time-division multiple access (TDMA) requires strict time synchronization for channel orthogonality. For multiple collocated ad hoc connections, maintaining a common timing reference becomes rather cumbersome. Code-division multiple access (CDMA) offers the best properties for ad hoc radio systems since it provides spreading and can deal with uncoordinated systems. Direct sequence (DS)-CDMA is less attractive because of the near-far problem which requires coordinated power control or excessive processing gain. In addition, as in TDMA, DS-CDMA channel orthogonality requires a common timing reference. Finally, for higher user rates, rather high chip rates are required, which is less attractive because of the wide bandwidth (interference immunity) and higher current consumption. Frequency-hopping (FH)-CDMA combines a number of properties which make it the best choice for ad hoc radio systems. On average the signal can be spread over a large frequency range, but instantaneously only a small bandwidth is occupied, avoiding most of the potential interference in the ISM band. The hop carriers are orthogonal, and the interference on adjacent hops can effectively be suppressed by filter-

<sup>1</sup> In France and Spain the exact location of the band differs, and the band is smaller.



■ **Figure 2.** An illustration of the FH/TDD channel applied in Bluetooth.

ing. The hop sequences will not be orthogonal (coordination of hop sequences is not allowed by the FCC rules anyway), but narrowband and co-user interference is experienced as short interruptions in the communications, which can be overcome with measures at higher-layer protocols.

Bluetooth is based on FH-CDMA. In the 2.45 GHz ISM band, a set of 79 hop carriers have been defined at a 1 MHz spacing.<sup>2</sup> The channel is a hopping channel with a nominal hop dwell time of 625  $\mu$ s. A large number of pseudo-random hopping sequences have been defined. The particular sequence is determined by the unit that controls the FH channel, which is called the *master*. The native clock of the master unit also defines the phase in the hopping sequence. All other participants on the hopping channel are *slaves*; they use the master identity to select the same hopping sequence and add time offsets to their respective native clocks to synchronize to the frequency hopping. In the time domain, the channel is divided into slots. The minimum dwell time of 625  $\mu$ s corresponds to a single slot. To simplify implementation, full-duplex communications is achieved by applying time-division duplex (TDD). This means that a unit alternately transmits and receives. Separation of transmission and reception in time effectively prevents crosstalk between the transmit and receive operations in the radio transceiver, which is essential if a one-chip implementation is desired. Since transmission and reception take place at different time slots, transmission and reception also take place at different hop carriers. Figure 2 illustrates the FH/TDD channel applied in Bluetooth. Note that multiple ad hoc links will make use of different hopping channels with different hopping sequences and have misaligned slot timing.

### The Modulation Scheme

In the ISM band, the signal bandwidth of FH systems is limited to 1 MHz. For robustness, a binary modulation scheme was chosen. With the above-mentioned bandwidth restriction, the data rates are limited to about 1 Mb/s. For FH systems and support for bursty data traffic, a noncoherent detection scheme is most appropriate. Bluetooth uses Gaussian-shaped frequency shift keying (FSK) modulation with a nominal modulation index of  $k = 0.3$ . Logical ones are sent as positive frequency deviations, logical zeroes as negative frequency deviations. Demodulation can simply be accomplished by a limiting FM discriminator. This modulation scheme allows the implementation of low-cost radio units.

### Medium Access Control

Bluetooth has been optimized to allow a large number of uncoordinated communications to take place in the same area. Unlike other ad hoc solutions where all units in range share the same channel, Bluetooth has been designed to allow

a large number of independent channels, each channel serving only a limited number of participants. With the considered modulation scheme, a single FH channel in the ISM band only supports a gross bit rate of 1 Mb/s. This capacity has to be shared by all participants on the channel. Theoretically, the spectrum with 79 carriers can support 79 Mb/s. In the user scenarios targeted by Bluetooth, it is highly unlikely that all units in range need to share information among all of them. By using a large number of independent 1 Mb/s channels to which only the units are connected that really want to exchange information, the 80 MHz is exploited much more effectively. Due to nonorthogonality of the hop sequences, the theoretical capacity of 79 Mb/s cannot be reached, but is at least much larger than 1 Mb/s.

An FH Bluetooth channel is associated with a piconet. As mentioned earlier, the piconet channel is defined by the identity (providing the hop sequence) and system clock (providing the hop phase) of a master unit. All other units participating in the piconet are slaves. Each Bluetooth radio unit has a free-running system or native clock. There is not a common timing reference, but when a piconet is established, the slaves add offsets to their native clocks to synchronize to the master. These offsets are released again when the piconet is cancelled, but can be stored for later use. Different channels have different masters and therefore also different hopping sequences and phases. The number of units that can participate on a common channel is deliberately limited to eight (one master and seven slaves) in order to keep a high-capacity link between all the units. It also limits the overhead required for addressing. Bluetooth is based on peer communications. The master/slave role is only attributed to a unit for the duration of the piconet. When the piconet is cancelled, the master and slave roles are cancelled. Each unit can become a master or slave. By definition, the unit that establishes the piconet becomes the master.

In addition to defining the piconet, the master also controls the traffic on the piconet and takes care of access control. Access is completely contention free. The short dwell time of 625  $\mu$ s only allows the transmission of a single packet. A contention-based access scheme would provide too much overhead and is not efficient in the short dwell time Bluetooth applies. In Bluetooth, the master implements centralized control; only communication between the master and one or more slaves is possible. The time slots are alternately used for master transmission and slave transmission. In master transmission, the master includes a slave address of the unit for which the information is intended. In order to prevent collisions on the channel due to multiple slave transmissions, the master applies a polling technique: for each slave-to-master slot, the master decides which slave is allowed to transmit. This decision is performed on a per-slot basis: only the slave addressed in the master-to-slave slot directly preceding the slave-to-master slot is allowed to transmit in the slave-to-master slot. If the master has information to send to a specific slave, this slave is polled implicitly and can return information. If the master has no information to send, it has to poll the slave explicitly with a short poll packet. Since the master schedules the traffic in both the uplink and downlink, intelligent scheduling algorithms have to be used that take into account the slave characteristics. The master control effectively prevents collisions between the participants on the piconet channel. Independent collocated piconets may interfere when they occasionally use the same hop carrier. A type of ALOHA is applied: information is transmitted without checking for a clear carrier (listen-before-talk). If the information is received incorrectly, it is retransmitted at

<sup>2</sup> Currently, for France and Spain a reduced set of 23 hop carriers has been defined at a 1 MHz carrier spacing.

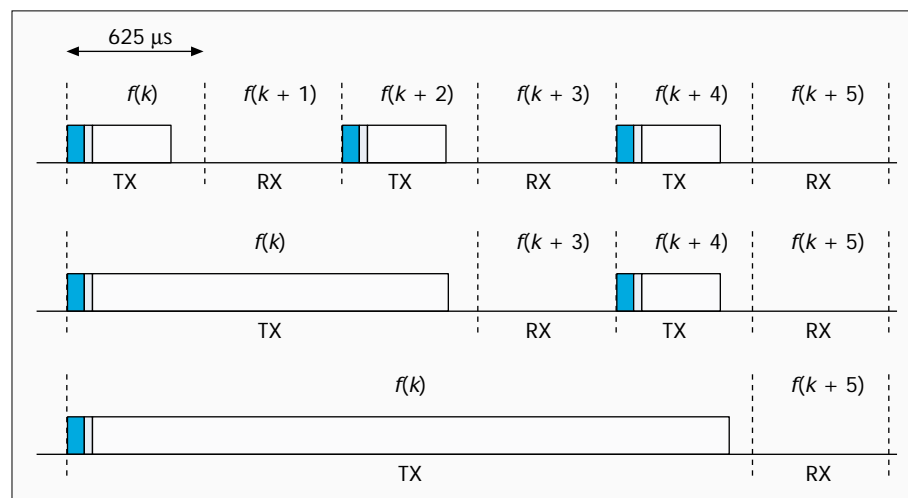
the next transmission opportunity (for data only). Due to the short dwell time, collision avoidance schemes are less appropriate for FH radio. For each hop, different contenders are encountered. Backoff mechanisms are therefore less efficient.

### Packet-Based Communications

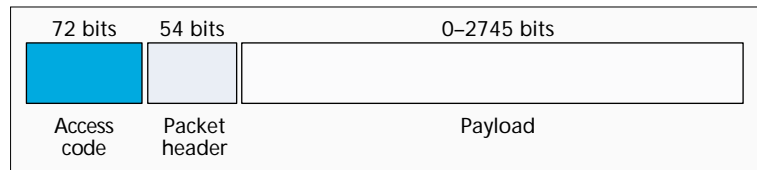
The Bluetooth system uses packet-based transmission: the information stream is fragmented into packets. In each slot, only a single packet can be sent. All packets have the same format, starting with an access code, followed by a packet header, and ending with the user payload (Fig. 3).

The access code has pseudo-random properties and is used as a direct-sequence code in certain access operations. The access code includes the identity of the piconet master. All packets exchanged on the channel are identified by this master identity. Only if the access code matches the access code corresponding to the piconet master will the packet be accepted by the recipient. This prevents packets sent in one piconet falsely being accepted by units of another piconet that happens to land on the same hop carrier. In the receiver, the access code is matched against the anticipated code in a sliding correlator. This correlator provides the direct-sequence processing gain. The packet header contains link control information: a 3-bit slave address to separate the slaves on the piconet, a 1-bit acknowledgment/negative acknowledgment (ACK/NACK) for the automatic repeat request (ARQ) scheme, a 4-bit packet type code to define 16 different payload types, and an 8-bit header error check (HEC) code which is a cyclic redundancy check (CRC) code to detect errors in the header. The packet header is limited to 18 information bits in order to restrict the overhead. The header is further protected by 1/3 rate forward error correction (FEC) coding. Bluetooth defines four control packets:

- The ID or identification packet: Only consists of the access code; used for signaling
- The NULL packet: Only has an access code and a packet header; used if link control information carried by the packet header has to be conveyed
- The POLL packet: Similar to the NULL packet; used by the master to force slaves to return a response
- The FHS packet: An FH-synchronization packet; used to exchange real-time clock and identity information between the units; contains all the information to get two units hop synchronized



■ **Figure 4.** The frequency and timing characteristics of single-slot, three-slot, and five-slot packets.



■ **Figure 3.** The format of packets applied in Bluetooth.

The remaining 12 type codes are used to define packets for synchronous and asynchronous services. These 12 types are divided into three segments. Segment 1 specifies packets that fit into a single slot, segment 2 specifies 3-slot packets, and segment 3 specifies 5-slot packets. Multislot packets are sent on a single-hop carrier. The hop carrier which is valid in the first slot is used for the remainder of the packet; therefore, there is no frequency switch in the middle of a packet. After the packet has been sent, the hop carrier as specified by the current master clock value is used (Fig. 4). Note that only an odd number of multislot packets have been defined, which guarantees that the TX/RX timing is maintained.

On the slotted channel, synchronous and asynchronous links have been defined, as will be further explained later. The interpretation of packet type is different for synchronous and asynchronous links. Currently, asynchronous links support payloads with or without a 2/3-rate FEC coding scheme. In addition, on these links single-slot, three-slot, and five-slot packets are available. The maximum user rate that can be obtained over the asynchronous link is 723.2 kb/s. In that case, a return link of 57.6 kb/s can still be supported. Link adaptation can be applied on the asynchronous link by changing the packet length and FEC coding depending on link conditions. The payload length is variable and depends on the available user data. However, the maximum length is limited by the minimum switching time between RX and TX, which is specified at 200 μs. This switching time seems large, but allows the use of open-loop voltage controlled oscillators (VCOs) for direct modulation and provides time for packet processing between RX and TX; this is also discussed later. For synchronous links, only single-slot packets have been defined. The payload length is fixed. Payloads with 1/3-rate FEC, 2/3-rate, or no FEC are supported. The synchronous link supports a full-duplex link with a user rate of 64 kb/s in both directions.

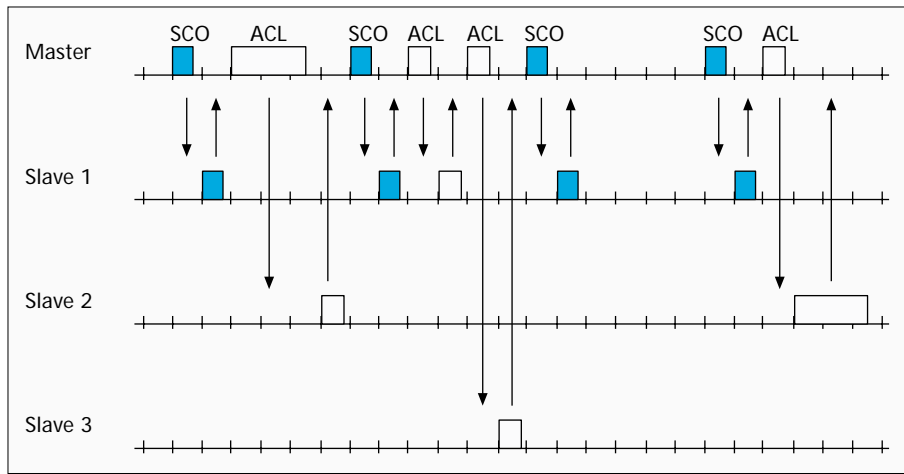
### Physical Link Definition

The Bluetooth link supports both synchronous services such as voice traffic, and asynchronous services such as bursty data traffic. Two physical link types have been defined:

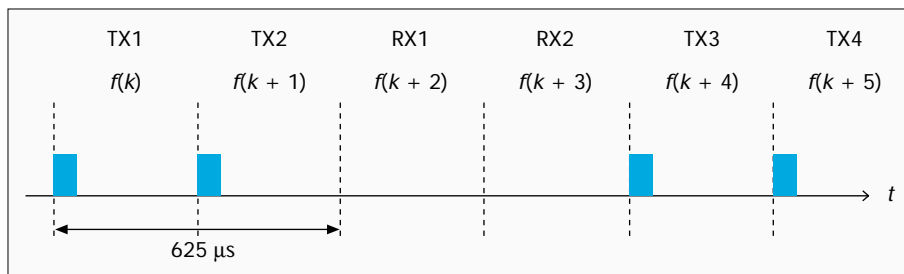
- The synchronous connection-oriented (SCO) link
- The asynchronous connectionless (ACL) link

The SCO link is a point-to-point link between the master and a single slave. The link is established by reservation of duplex slots at regular intervals. The ACL link is a point-to-multipoint link between the master and all the slaves on the piconet. The ACL link can use all of the remaining slots on the channel not used for SCO links. The traffic over the ACL link is scheduled by the master. The slotted structure of the piconet channel allows effective mixing of the synchronous and asynchronous links. An example of a channel with SCO and ACL links is





■ **Figure 5.** An example of mixing synchronous SCO links and asynchronous ACL links on a single piconet channel.



■ **Figure 6.** Frequency and timing behavior for a Bluetooth paging unit.

illustrated in Fig. 5. For the SCO link and ACL link, different packet types have been defined.

### Connection Establishment

A critical design issue in ad hoc radio systems is connection establishment. How do units find each other, and how do they make connections? In Bluetooth, three elements have been defined to support connection establishment: scan, page, and inquiry. A unit in idle mode wants to sleep most of the time to save power. However, in order to allow connections to be made, the unit frequently has to listen whether other units want to connect. In truly ad hoc systems, there is no common control channel a unit can lock to in order to listen for page messages, as is common in conventional (cellular) radio systems. In Bluetooth, a unit periodically wakes up to listen for its identity. However, the explicit identity is not used, but the access code derived from this identity. When a Bluetooth unit wakes up to scan, it opens its sliding correlator which is matched to the access code derived from its own identity. The scan window is a little longer than 10 ms. Every time the unit wakes up, it scans at a different hop carrier. This is required by the regulations, which do not permit a fixed wake-up frequency, and also provides the necessary interference immunity. The Bluetooth wake-up hop sequence is only 32 hops in length and is cyclic. All 32 hops in the wake-up sequence are unique, and they span at least 64 MHz of the 80 MHz available. The sequence is pseudo-random and unique for each Bluetooth device. The sequence is derived from the unit identity. The phase in the sequence is determined by the free-running native clock in the unit. Thus, during idle mode, the native clock is used to schedule wake-up operations. It will be understood that a trade-off has to be made between idle mode power consumption and response time: increasing the sleep time will reduce power consumption, but will prolong the time before an access can be made. The unit that wants to

connect has to solve the frequency-time uncertainty: it does not know when the idle unit will wake up and on which frequency. The burden of solving this uncertainty is deliberately placed at the paging unit because this will require power consumption. Since a radio unit will be in idle mode most of the time, the paging unit should take the power burden. We first assume that the paging unit knows the identity of the unit to which it wants to connect. Then it knows the wake-up sequence and can also generate the access code which serves as the page message. The paging unit then transmits the access code repeatedly at different frequencies: every 1.25 ms; the paging unit transmits two access codes and listens twice for a response (Fig. 6).

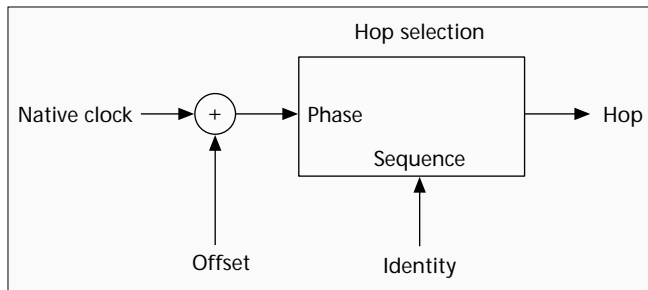
Consecutive access codes are transmitted on different hops selected from the wake-up sequence. In a 10 ms period 16 different hop carriers are visited, which represent half of the wake-up sequence. The paging unit transmits the access code on these 16 frequencies cyclically for the duration of the sleep period of the idle unit. If the idle unit wakes up in any of these 16 frequencies, it will

receive the access code and a connection setup procedure follows. However, since the paging unit does not know the phase the idle unit is using, the idle unit can equally well wake up in any of the 16 remaining frequencies in the 32-hop wake-up sequence. Therefore, if the paging unit does not receive a response from the idle unit after a time corresponding to the sleep time, it will transmit the access code repeatedly on the hop carriers in the remaining half of the sequence.<sup>3</sup> The maximum access delay therefore amounts to twice the sleep time. When the idle unit receives the page message, it notifies the paging unit by returning a message, which again is the access code derived from the idle unit's identity. Thereafter the paging unit transmits an FHS packet which contains all of the pager's information (e.g., identity and clock). This information is then used by both the paging unit and the idle unit to establish a piconet; that is, the paging unit becomes the master using its identity and clock to define the FH channel, and the idle unit becomes the slave.

The above-described paging process assumes that the paging unit has no knowledge at all of the clock in the idle unit. However, if the units have met before, the paging unit will have an estimate of the clock in the idle unit. When units connect, they exchange their clock information, and the time offsets between their free-running native clocks are stored. This offset is only accurate during the connection; when the connection is released, the offset information becomes less reliable due to clock drifts. The reliability of the offsets is inversely proportional to the time elapsed since the last connection. However, the paging unit can exploit the offset infor-

<sup>3</sup> In determining the hop carriers of the second half of the sequence, the paging unit takes into account that the clock in the idle unit also progresses. The remaining half will therefore have one carrier in common with the first half.





■ **Figure 7.** The basic concept of hop selection in Bluetooth.

mation to estimate the phase of the idle unit. Suppose the clock estimate of the idle unit in the paging unit is  $K$ . If  $f(m)$  is the hop in the wake-up sequence at time  $m$ , the paging unit will assume that the idle unit will wake up in  $f(K)$ . But since in 10 ms it can cover 16 different frequencies, it will also transmit the access code  $a$  hop frequencies before and after  $f(K)$  or  $f(K-8), f(K-7), \dots, f(K), f(K+1), \dots, f(K+7)$ . As a result, the phase estimate in the paging unit can be off by  $-8$  or  $+7$  while it still covers the wake-up frequency of the unit in idle mode. With a free-running clock accuracy of  $\pm 250$  ppm, the clock estimate  $K$  is still useful at least 5 hr after the last connection. In this case, the average response time is reduced to half the sleep time.

To establish a connection, the identity of the recipient is required to determine the page message and wake-up sequence. If this information is not known, a unit that desires to make a connection may broadcast an inquiry message that induces recipients to return their address and clock information. With the inquiry procedure, the inquirer can determine which units are in range and what their characteristics are. The inquiry message is again an access code, but derived from a reserved identity (the inquiry address). Idle units also listen to the inquiry message according to a 32-hop inquiry sequence. Units that receive the inquiry message return an FHS packet which includes, among other things, their identity and clock information. For the return of the FHS packet a random backoff mechanism is used to prevent multiple recipients transmitting simultaneously.

During the page and inquiry procedures, 32 hop carriers are used. For pure hopping systems, at least 75 hop carriers must be used. However, during the page and inquiry procedures, only an access code is used for signaling. This access code is used as a direct-sequence code. The processing gain obtained from this direct-sequence code combined with the processing gain obtained from the 32-hop sequence provides sufficient processing gain to satisfy the regulations for hybrid DS/FH systems. Thus, during the page and inquiry procedures the Bluetooth system acts like a hybrid DS/FH system, whereas during the connection it acts as a pure FH system.

### Hop Selection Mechanism

Bluetooth applies a special hop selection mechanism. The hop selection mechanism can be considered a black box with an identity and clock in, and a hop carrier out (Fig. 7). The mechanism satisfies the following requirements:

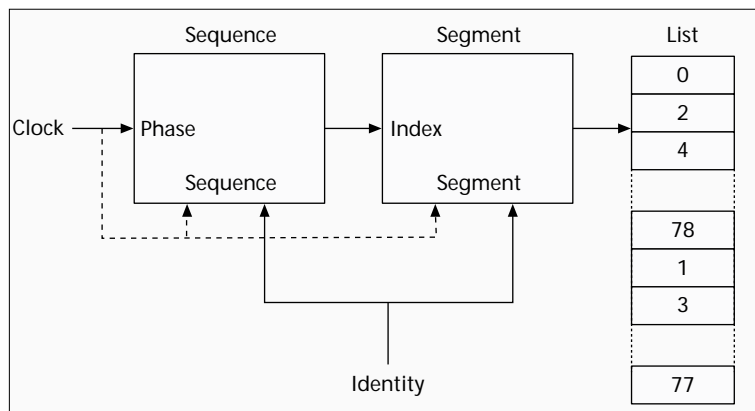
- The sequence is selected by the unit identity, the phase by the unit clock.
- The sequence cycle covers about 23 hours.
- 32 consecutive hops span about 64 MHz of spectrum.
- On average, all frequencies are visited with equal probability.

<sup>4</sup> For 23-hop systems, a corresponding scheme is constructed with 16-hop segments and a 23-hop list.

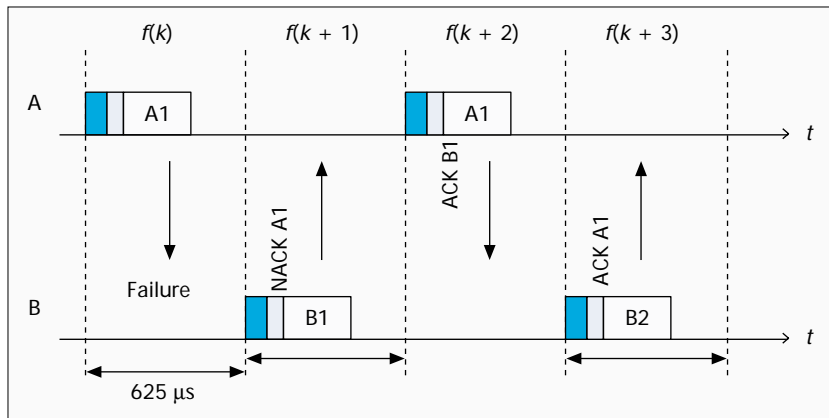
- The number of hop sequences is very large.
- By changing the clock and/or identity, the selected hop changes instantaneously.

Note that no extra effort has been taken to make the sequences orthogonal. With only 79 hop carriers, the number of orthogonal sequences is rather limited. The first requirement supports the piconet concept where the master unit defines the hop channel by its identity and clock. The second requirement prevents repetitions in the interference pattern when several piconets are collocated. Repetitive interference is detrimental for synchronous services such as voice. The spanning requirement provides maximal interference immunity by spreading as much as possible over a short time interval. Again, this is most important for voice services. It also provides the desired features for the wake-up and inquiry sequences which are 32 hops in length. Over a larger interval, regulations require that all carriers are visited with equal probability. Since many piconets can coexist in the same area, many hop patterns must be available. This excludes the use of prestored sequences: the sequences are generated on the fly by logic circuitry. Finally, the last requirement provides flexibility to run backward and forward in the sequence by running the clock backward or forward, which is attractive in the page and inquiry procedures. In addition, it supports jumping between piconets: a unit can jump from one piconet to another by merely changing the master parameters (i.e., identity and clock). The latter requirement excludes the use of a memory in the algorithm: only combinatorial logic circuitry is used.

The selection mechanism is illustrated in Fig. 8.<sup>4</sup> In the first block, the identity selects a 32-hop subsequence with pseudo-random properties. The least significant part of the clock hops through this sequence according to the slot rate (1600 slots/s). The first block thus provides an index in a 32-hop segment. The segments are mapped on the 79-hop carrier list. The carrier list is constructed in such a fashion that even-numbered hops are listed in the first half of the list, odd-numbered hops in the second half of the list. An arbitrary segment of 32 consecutive list elements spans about 64 MHz. For the paging and inquiry procedures, the mapping of the 32-hop segment on the carrier list is fixed. When the clock runs, the same 32-hop sequence and 32 hop carriers will be used. However, different identities will map to different segments and different sequences, so the wake-up hop sequences of different units are well randomized. During the connection, the more significant part of the clock affects both sequence selection and segment mapping: after 32 hops (one segment) the sequence is altered, and the segment is shifted in the forward direction by half its size (16 hops). Segments, each 32 hops in



■ **Figure 8.** The hop selection mechanism; the dashed line for the more significant clock part is used in connection mode only.



■ Figure 9. An example of retransmission operation in Bluetooth.

length, are concatenated, and the random selection of the index changes for each new segment; the segments slide through the carrier list, and on average all carriers are visited with equal probability. Changing the clock and/or identity will directly change the sequence and segment mapping.

### Error Correction

Bluetooth includes both FEC and packet retransmission schemes. For FEC, a 1/3-rate code and a 2/3-rate FEC code are supported. The 1/3-rate code merely uses a 3-bit repeat coding with majority decision at the recipient. With the repeat coding, extra gain is obtained due to the reduction of instantaneous bandwidth. As a result, intersymbol interference (ISI) introduced by the receive filtering is decreased. The 1/3-rate code is used for the packet header, and can additionally be applied on the payload of the synchronous packets on the SCO link. For the 2/3-rate FEC code, a shortened Hamming code is used. Error trapping can be applied for decoding. This code can be applied on both the payload of the synchronous packets on the SCO link and the payload of the asynchronous packets on the ACL link. The applied FEC codes are very simple and fast in encoding and decoding operations, which is a requirement because of the limited processing time between RX and TX. This will be further apparent in the next paragraph.

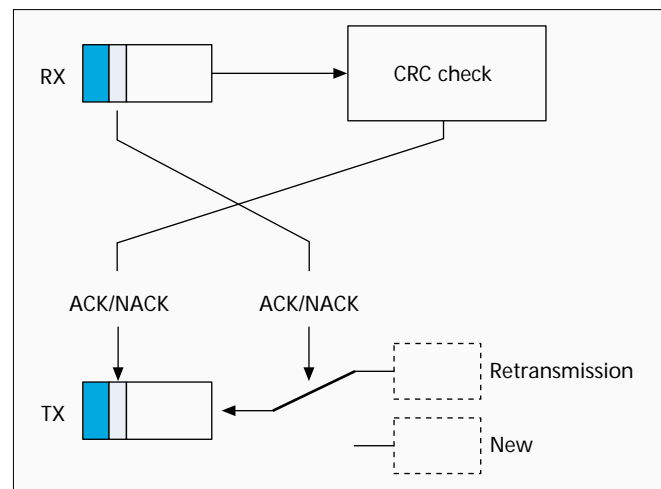
On the ACL link, an ARQ scheme can be applied. In this scheme, a packet retransmission is carried out if the reception of the packet is not acknowledged. Each payload contains a CRC to check for errors. Several ARQ schemes have been considered like stop-and-wait ARQ, go-back- $N$  ARQ, and selective-repeat ARQ [9]. Also, hybrid schemes have been analyzed. However, to minimize complexity, overhead, and wasteful retransmissions, Bluetooth has implemented a fast-ARQ scheme where the sender is notified of the packet reception in the RX slot directly following the TX slot in which the packet was sent (Fig. 9). If the 2/3-rate FEC code is added, a type I hybrid ARQ scheme results. The ACK/NACK information is piggybacked in the packet header of the return packet. There is only the RX/TX switching time for the recipient to determine the correctness of the received packet and creating the ACK/NACK field in the header of the return packet. In addition, the ACK/NACK field in the header of the packet received indicates whether the previously sent payload was correctly received, and thus determines whether a retransmission is required or the next packet can be sent. This process is illustrated in Fig. 10. Due to the short processing time, decoding is preferably carried out on the fly while the packet is received. In addition, the simplicity of the FEC coding schemes speed up the processing. The fast-ARQ scheme is similar to the stop-and-wait ARQ scheme, but the delay has been minimized; in fact, there is no additional delay caused by the ARQ scheme. The scheme is more efficient than go-back- $N$ , since only

failed packets are retransmitted. This is the same efficiency obtained with selective-repeat ARQ, but with reduced overhead: only a 1-bit sequencing number suffices in the fast-ARQ scheme (in order to filter out packets that are correctly received twice due to an error in the ACK/NACK field).

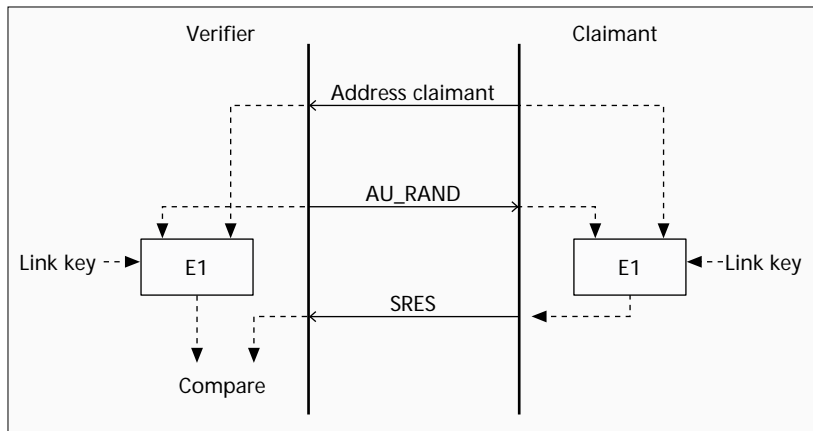
### Power Management

In the Bluetooth design, special attention has been paid to reduction of current consumption. In the idle mode, the unit only scans a little over 10 ms every  $T_s$  where  $T_s$  can range from 1.28 to 3.84 s. Thus, the duty cycle is well below 1 percent. Additionally, a PARK mode has been defined where the duty cycle can be reduced even more. However, the PARK mode can only be applied after the piconet has been established. The slave can then be parked; that is, it only listens to the channel at a very low duty cycle. The slave only has to listen to the access code and the packet header (126  $\mu$ s excluding guard time to account for drift) to resynchronize its clock and decide whether it can return to sleep. Since there is no uncertainty in time and frequency (the parked slave is locked to the master, similar to how cordless and cellular phones are locked to their base stations), a much lower duty cycle is achievable. Another low-power mode during connection is the SNIFF mode, in which the slave does not scan at every master-to-slave slot, but has a larger interval between scans.

In the connection state, current consumption is minimized, and only transmitting when information is available prevents wasteful interference. If no useful information needs to be exchanged, no transmission takes place. If only link control information needs to be transferred (e.g., ACK/NACK), a NULL packet without payload is sent. Since NACK is implicit, a NULL packet with NACK does not have to be sent. In longer periods of silence, the master once in a while needs to send a packet on the channel such that all slaves can resynchronize their clocks and compensate for drift. The accuracy of the clocks and the scan window length applied in the slave determines the period of this resynchronization. During continuous TX/RX operations, a unit starts to scan for the access code at the beginning of the RX slot. If in a certain window this access code is not found, the unit returns to sleep until



■ Figure 10. ARQ mechanisms where received ACK/NAK information decides on retransmission and received payload determines transmitted ACK/NAK information.



■ **Figure 11.** *The Bluetooth authentication procedure.*

the next TX slot (for the master) or RX slot (for the slave). If the access code is received (which means the received signal matches the expected access code), the header is decoded. If the 3-bit slave address does not match the recipient, further reception is stopped. The header indicates what type of packet it is and how long the packet will last; therefore, the nonaddressed recipients can determine how long they can sleep.

The nominal transmit power used by most Bluetooth applications for short-range connectivity is 0 dBm. This both restricts current consumption and keeps interference to other systems to a minimum. However, the Bluetooth radio specifications allow TX power up to 20 dBm. Above 0 dBm, closed-loop received signal strength indication (RSSI)-based power control is mandatory. This power control only compensates for propagation losses and slow fading. In the uncoordinated environment where ad hoc systems operate, interference-based power control is to say the least doubtful, especially since different types of systems with different power characteristics share the same band. Since power control cannot be coordinated among different systems, it cannot be prevented that certain systems always try to overpower their contenders, and the strongest transmitter will prevail.

### Security

Although Bluetooth is mainly intended for short-range connectivity between personal devices, some basic security elements are included to prevent unauthorized usage and eavesdropping. At connection establishment, an authentication process is carried out to verify the identities of the units involved. The authentication process uses a conventional challenge-response routine illustrated in Fig. 11. The claimant (right) transmits its claimed 48-bit address to the verifier (left). The verifier returns a challenge in the form of a 128-bit random number (AU RAND). The AU RAND, the claimant address, and a 128-bit common secret link key form the inputs to a computational secure hash function *E1* based on SAFER+, which produces a 32-bit signed response (SRES). The SRES produced by the claimant is sent to the verifier, which compares this result with its own SRES. Only if the two calculated SRES numbers are the same will the challenger continue with connection establishment. The authentication can be uni- or bidirectional.

In addition to the 32-bit SRES, the *E1* algorithm produces a 96-bit authenticated cipher offset (ACO). This offset is used in the encryption procedure. To prevent eavesdropping on the link, which is a danger inherent to radio communications even if the intended recipient is only at short range, the payload of each packet is encrypted. Encryption is based on stream-ciphering; the payload bits are modulo-2 added to a binary keystream. The binary keystream is generated by a second

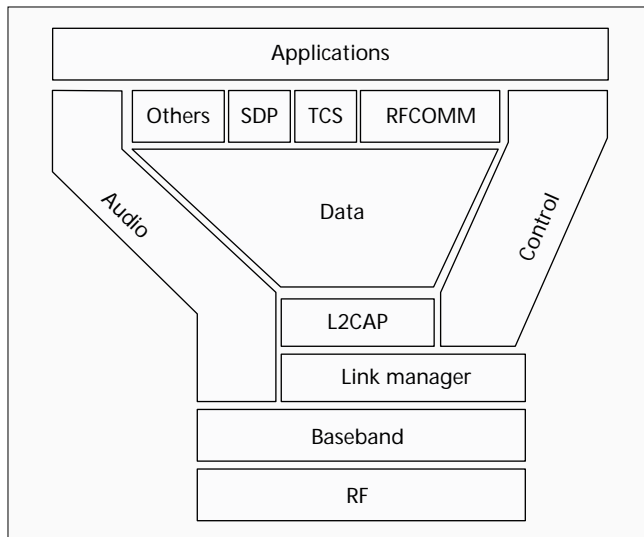
hash function *E0* which is based on linear feedback shift registers (LFSRs). When encryption is enabled, the master sends a random number EN RAND to the slave. Before the transmission of each packet, the LFSR is initialized by a combination of this EN RAND, the master identity, an encryption key, and the slot number. Since the slot number changes for each new packet, the initialization is new for each packet. The encryption key is derived from the secret link key, the EN RAND, and the ACO.

The central element in the security process is the 128-bit link key. This link key is a secret key residing in the Bluetooth hardware and is not accessible by the user. The link key is generated during an initialization phase. Two units that want to authenticate each other and establish secure links in the future have to be associated (i.e., provided with the same secret link key). An initialization phase initiated by the user is required to associate two devices. To authorize initialization, the user has to enter an identical PIN in both devices. For devices without a user interface (e.g., headsets), initialization is only possible during a short time window (e.g., after the user has pressed an initialization key). Once the initialization has been carried out, the 128-bit link keys reside in the devices and can from then on be used for automatic authentication without user interaction. In principle, the link key provides an agreement between two units. Thus, to provide security in  $N$  units,  $N \times (N - 1)/2$  link keys are required. Bluetooth provides methods to reduce the number of keys in certain applications. If a single unit is used by many users (e.g., a printer shared by several users), a single key is used by all users for secure communications to this single unit. In addition, methods are available to use the same encryption key for all slaves in a single piconet.

Bluetooth provides a limited number of security elements at the lowest level. More advanced security procedures (e.g., public keys, certificates) can be implemented at higher layers.

### Interpiconet Communications

The Bluetooth system has been optimized to have tens of piconets operate in the same area without noticeable performance degradation. Multiple piconets in the same area are referred to as a *scatternet*. Due to the fact that Bluetooth uses packet-based communication over slotted links, it is possible to interconnect different piconets. This means that units can participate in different piconets. However, since the radio can tune to a single hop carrier only, at any instant in time a unit can communicate in one piconet only. However, the unit can jump from one piconet to another by adjusting the piconet channel parameters (i.e., the master identity and master clock). A unit can also change role when jumping from one piconet to another. For example, a unit can be the master in one piconet at one instant in time, and be a slave in a different piconet at another instant in time. A unit can also be a slave in different piconets. However, by definition, a unit cannot be the master in different piconets, since the master parameters specify the piconet FH channel. The hop selection mechanism has been designed to allow for interpiconet communications: by changing the identity and clock input to the selection mechanism, instantaneously a new hop for the new piconet is selected. In order to make jumps between different piconets feasible, guard time has to be included in the traffic scheduling to account for the slot misalignment of different piconets. In Bluetooth, a HOLD mode has been introduced to allow a unit to temporarily leave one piconet and visit another



■ Figure 12. The Bluetooth protocol stack.

(HOLD can also be used as an additional low-power mode when no new piconet is visited during the leave). Traffic scheduling and routing in a scatternet with interpiconet communications is a challenge and still a subject for future study.

## Bluetooth Standardization

In the beginning of 1998, a Bluetooth Special Interest Group (SIG) was formed to further expand and promote the Bluetooth concept and establish an industry standard. The SIG promoters are formed by leading manufacturers of the mobile communication industry, portable computer industry, and chip integration industry: Ericsson, Nokia, IBM, Toshiba, and Intel. Version 1.0 of the specification was published in July 1999. Over 1000 companies have signed as adopters of the technology. The Bluetooth technology is royalty-free. A special certification program, including logos, is under development to guarantee Bluetooth interoperability.

The specified protocol stack of Bluetooth is shown in Fig. 12. This article has dealt mainly with the three lower layers:

- The RF layer, specifying the radio parameters
- The baseband layer, specifying the lower-level operations at the bit and packet levels (FEC operations, encryption, CRC calculations, ARQ protocol)
- The link manager (LM) layer, specifying connection establishment and release, authentication, connection and release of SCO and ACL channels, traffic scheduling, link supervision, and power management tasks

The Logical Link Control and Adaptation Protocol (L2CAP) layer has been introduced to form an interface between standard data transport protocols and the Bluetooth protocol. It handles multiplexing of higher-layer protocols, and segmentation/reassembly of large packets. The data stream crosses the LM layer, where packet scheduling on the ACL channel takes place. The audio stream is directly mapped on an SCO channel and bypasses the LM layer. The LM layer, though, is involved in the establishment of the SCO link. Between the LM layer and the application, control messages are exchanged in order to configure the Bluetooth transceiver for the considered application. Above the L2CAP layer, RFCOMM, transmission convergence sublayer (TCS), and other network protocols (e.g., TCP/IP, PPP, OBEX, Wireless Application Protocol) may reside. RFCOMM and TCS are also specified in Bluetooth and provide serial cable emulation and a cordless telephony protocol, respectively. SDP is a service discovery protocol which enables a Bluetooth unit to find the capabilities of other Bluetooth units in range. It discovers which services are available

and the characteristics of these services. This can involve common services like printing, faxing, and so on, as well as more advanced services like teleconferencing, network bridging and access points, e-commerce facilities, and so on. SDP specifically addresses the Bluetooth environment; it does not specify the methods for accessing the service, for which other (non-Bluetooth) protocols can be used.

In addition to protocols which guarantee that two units speak the same language, profiles are defined. Profiles are associated with applications. The profiles specify which protocol elements are mandatory in certain applications. This concept prevents devices with little memory and processing power implementing the entire Bluetooth stack when they only require a small fraction of it. Simple devices like a headset or mouse can thus be implemented with a strongly reduced protocol stack. Profiles are dynamic in the sense that for new applications, new profiles can be added to the Bluetooth specification.

## Conclusions

In this article the Bluetooth radio system is presented. The focus is on its capabilities to provide ad hoc radio connectivity. With the restrictions set by regulations, power consumption, lack of coordination, and interference immunity, a robust radio system has evolved which provides a universal wireless interface to a large range of low-cost, portable devices. The article has also described the motivation of the various design choices.

## References

- [1] M. Mouly and M.-B. Pautet, *The GSM System for Mobile Communications*, 1992.
- [2] TIA/EIA/IS-136.2, "800 MHz TDMA Cellular-Radio Interface-Mobile Station-Base Station Compatibility — Traffic Channels and FSK Control Channel," Dec. 1994.
- [3] TIA/EIA IS-95B, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular Systems," 1998.
- [4] IEEE 802.11, "Wireless LAN MAC and Physical Layer Specification," June 1997.
- [5] ETSI RES, "High Performance Radio Local Area Network (HIPERLAN) Type 1, Functional Specifications," ETS 300 652, 1996.
- [6] ETSI BRAN, "HIPERLAN Type 2, Functional Specifications," preliminary.
- [7] ETSI RES, "Digital European Cordless Telecommunications (DECT), Common interface Part 1: Overview," ETS 300 175-1, 1996.
- [8] "Personal Handy Phone Standard (PHS)," CRC STD-28, 1993.
- [9] S. Lin and D. J. Costello, *Error Control Coding*, Prentice-Hall, 1983.

## Biography

JAAP C. HAARTSEN (jaap.haartsen@erh.ericsson.se) joined Ericsson Mobile Communications in 1991 and has since worked at sites in RTP, the United States, and Lund, Sweden in the area of wireless technology. In Sweden he worked on the foundations of the Bluetooth radio concept. Currently, he is located in Emmen, the Netherlands, where he is working with the Bluetooth system for both current and future applications. Jaap is chair of the Bluetooth air protocol group. He earned M.Sc. and Ph.D. degrees (both with honors) in electrical engineering from Delft University of Technology, the Netherlands. He holds over 25 patents.

# **APPENDIX E**



# Service Advertisement and Discovery:

## *Enabling Universal Device Cooperation*

**GOLDEN G. RICHARD III**  
University of New Orleans

Service advertisement and discovery technologies enable device cooperation and reduce configuration hassles, a necessity in today's increasingly mobile computing environments. This article surveys five competing but similar "service discovery suites" and looks at efforts to bridge the technologies.

Computer users increasingly face the management of many computing devices. One reason is the expansion of computing environments in the home and office, as printers, scanners, digital cameras, and other peripherals are integrated into networked environments. Another reason is the proliferation of mobile devices such as laptop and palm-sized computers, cellular phones, and pagers. Because these devices trade functionality for suitable form factors and low power consumption, they are necessarily "peripheral-poor" and must therefore establish connections to neighboring devices for storage, faxing, high-speed network access, and printing.

It is easy to become frustrated when dealing with the configuration and interaction of such a multitude of devices. Service discovery technologies were developed to reduce this frustration and to simplify the use of mobile devices in a network by allowing them to be "discovered," configured, and used by other devices with a minimum of manual effort.

This article briefly surveys five of the leading technologies in this area. Table 1 lists the features of each technology. Although most of these "service discovery suites" promise similar functionality—namely, reduced configuration hassles, improved device cooperation, and automated discovery of required services—they come at the problem from different philosophical and technical approaches. Since none of these technologies is a superset of the others and none is mature enough to dominate the market, interoperability among them will require bridging mechanisms. The survey concludes with a review of some developments in this area.

### **BLUETOOTH: PICONETS FOR WIRELESS DEVICES**

Bluetooth is a low-power, short-range, wireless radio system being developed by the Bluetooth Special Interest Group, an industry consortium whose member companies include Ericsson, Nokia, and IBM. The radio has a range of 10 meters and provides up to seven 1-megabit-per-second links to other Bluetooth devices. Bluetooth operates in the 2.4-GHz indus-

trial scientific and medical (ISM) band to maximize international acceptance and employs a frequency-hopping system to minimize interference. The low-level communications are detailed in the Bluetooth specification.<sup>1</sup>

Bluetooth has a small form factor; complete systems can be as small as 2-cm square. The technology supports both isochronous and asynchronous services. A simple isochronous application might link a cellular phone and wireless headset, where the headset and base are both Bluetooth devices. More complicated applications include automatic discovery of wireless network connections and automatic synchronization of data between several Bluetooth devices.

Figure 1 shows the Bluetooth protocol stack. At the bottom, the radio and baseband layers provide the short-range, frequency-hopping radio platform. The link manager protocol (LMP) handles data link setup and provides authentication and encryption services. The logical link control and adaptation protocol (L2CAP) supports multiplexed connectionless and connection-oriented communication over the LMP layer. L2CAP is proprietary, but other network protocols, such as IP, can be built on top of it. L2CAP is also used by higher level protocols. For example, Figure 1 shows links to the Hayes-compatible AT (ATtention) protocol, which provides a standard interface for controlling remote cellular phones and modems; RFComm, which emulates an RS-232 serial interface; a simple object exchange protocol (OBEX), which enhances Bluetooth's interoperability with IrDA; and Bluetooth's service discovery protocol (SDP).

Groups of up to eight Bluetooth devices can form ad hoc networks called *piconets* to communicate, share services, and synchronize data. In each piconet, a master device coordinates the other Bluetooth devices (including setting the 1,600-hops-per-second frequency-hopping pattern). Individual devices can participate in more than one piconet at a time and can be in one of several states:

- *Standby*—the device is conserving power and waiting to connect to another Bluetooth device.
- *Inquire*—the device is searching for nearby Bluetooth devices.
- *Page*—the device is connecting to another Bluetooth device.

Table 1. Features of the five leading service discovery suites.

Feature	Bluetooth	Jini	Salutation	UPnP	SLP
Service discovery	✓	✓	✓	✓	✓
Service announcement		✓	✓	✓	✓
Service registry		✓	✓		✓
Interoperability	✓	✓	✓		✓
Security	✓	✓			✓

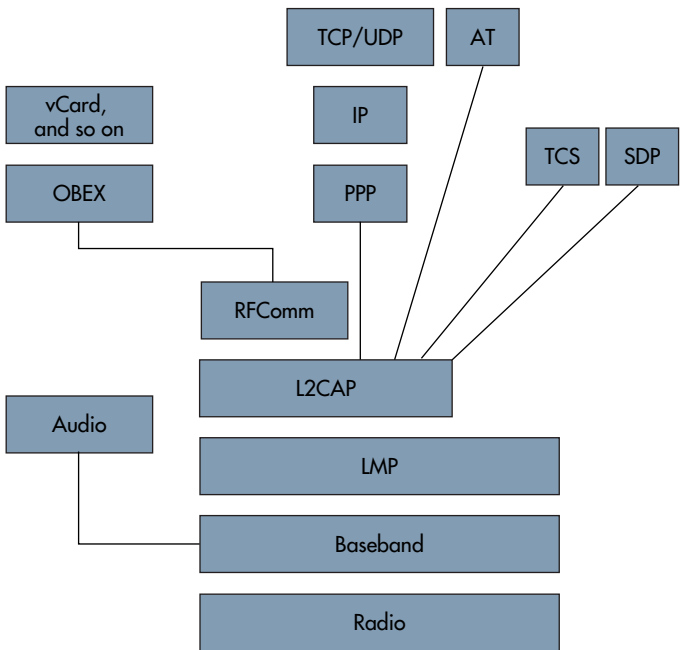
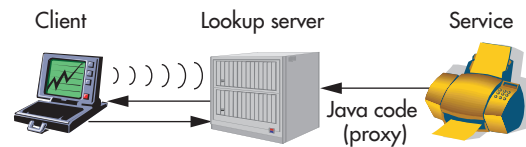


Figure 1. Bluetooth protocol stack. The link manager protocol (LMP) controls link setup and provides encryption and authentication services. The proprietary logical link control and adaptation protocol (L2CAP) provides multiplexed communication over LMP to higher level layers.

- *Connected*—the device is connected to another Bluetooth device.
- *Hold and park*—the device is participating in a piconet with varying degrees of power savings.

The Bluetooth SDP provides a simple API for enumerating the devices in range and browsing available services. It also supports *stop rules* that limit the duration of searches or the number of devices returned. Client applications use the API to search for available services either by service



**Figure 2. Jini service discovery entities: clients, lookup servers, and services. In this example, a printer service registers a proxy object with a lookup server, which will serve as a remote control for clients that use the service.**

classes, which uniquely identify types of devices (such as printers or storage devices), or by matching attributes (such as a model number or supported protocol). Attributes that describe the services offered by a Bluetooth device are stored as a service record and are maintained by the device's SDP server.

## Jini requires each device either to run a Java virtual machine or to associate itself with a device that can execute a JVM on its behalf.

The distinction between service classes and descriptive attributes is not well defined, but service classes generally define broad device categories, such as Printer, ColorPrinter, and PostScriptPrinter, while attributes allow a finer level of description. Manufacturers must eventually standardize these service classes for maximal interoperability between Bluetooth devices.

Unlike higher level service discovery technologies such as Jini, Bluetooth's SDP does not provide a mechanism for using discovered services—specific actions required to use a service must be provided by a higher level protocol. However, it does define a standard attribute `ProtocolDescriptorList`, which enumerates appropriate protocols for communicating with a service.

Bluetooth devices provide data security through unique 48-bit identifiers, 128-bit authentication keys, and 8- to 128-bit encryption keys. Strong authentication is possible because no international restrictions prevent it, but Bluetooth devices

must negotiate encryption strength to comply with laws restricting encryption. Note that Bluetooth devices must be paired to provide them with matching secret keys that will support authentication. Once paired, Bluetooth devices can authenticate each other and protect sensitive data from snooping. Regardless of encryption strength, Bluetooth's fast frequency-hopping scheme makes snooping difficult.

## JINI: MOBILE JAVA CODE

Jini is a service discovery and advertisement system that relies on mobile code and leverages the platform independence of the Java language.<sup>2</sup> The current Jini implementation is based on TCP and UDP, but implementations based on other network protocols are certainly possible. The major requirements are reliable, stream-oriented communication and a multicast facility. Jini's language-centric approach allows a flexible definition of service; for example, a service can be implemented entirely in software and, after discovery, can be downloaded and executed entirely on the client. Examples of such algorithmic services might include an implementation of a proprietary algorithm for shading a polygon or formatting a document to meet an organizational standard. On the other hand, Jini also requires each device either to run a Java virtual machine or to associate itself with a device that can execute a JVM on its behalf. For example, a Jini "device chassis" might Jini-enable a number of "dumb" devices, making their services available to Jini clients.

Jini entities consist of *services*, *lookup servers* that catalog available services, and *clients* that require services. A service can also be a client; for example, a telescope might provide pictures to a PDA as a service and look for printing services as a client. All service advertisements and requests go through a lookup server. Figure 2 illustrates the discovery and registration process for Jini clients and services.

To register service availability or to discover services, a service or client must first locate one or more lookup servers by using a *multicast request protocol*. This request protocol terminates with the invocation of a *unicast discovery protocol*, which clients and services use to communicate with a specific lookup server. The unicast protocol culmi-



nates in the transfer of an instance of the `ServiceRegistrar` class, a “remote control” for the lookup server. A lookup server can use the *multicast announcement protocol* to announce its presence on the network. When a lookup server invokes this protocol, clients and services that have registered interest in receiving announcements of new lookup services are notified.

These three protocols are encapsulated in a set of Jini classes. For example, to find lookup services, a client or service need only create an instance of `LookupDiscovery`.

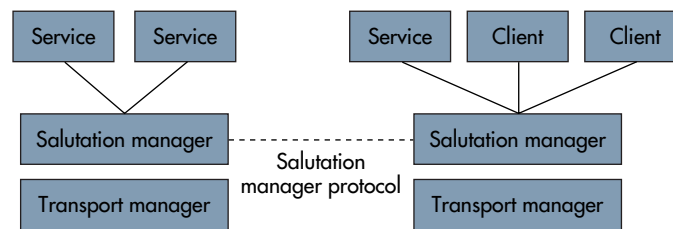
Jini uses Java’s remote method invocation (RMI) facility for all interactions between either a client or a service and the lookup server (after the initial discovery of the lookup server). Once a lookup server has been discovered and an instance of `ServiceRegistrar` is available, services can register their availability, and clients can search for needed services by invoking `ServiceRegistrar` methods.

Jini associates a proxy, or *remote control object*, with each service instance. A service advertises its availability by registering its object in one or more lookup servers via the `register()` method. This method takes several arguments, including an instance of `ServiceItem`, which contains a universally unique identifier for the service, its attribute set, and its remote control object. This object may either implement the service entirely (in the case of an algorithmic service such as the implementation of a polygon-shading algorithm), or provide methods for accessing the service over the network. The `leaseduration` parameter of `register()` specifies the service’s intended lifetime. The service is responsible for renewing the lease within the time specified to maintain its listing. The lookup server is free to adjust the lease time, which is returned in a `ServiceRegistration` object.

When a service first contacts a lookup server, the server generates a unique identifier for it; the service uses this ID in all future registrations. The service identifier lets clients request a specific service explicitly and recognize when services reported by different lookup servers are identical.

To use a service, a device must first secure an instance of the proxy object for it. From a client point of view, the location of the service proxied by this remote control object is unimportant, because the object encapsulates the location of the service and the protocol necessary to operate it.

Clients use the `lookup()` method in `ServiceRegistrar` to discover services. This method takes a single argument, an instance of `ServiceTemplate`. The



**Figure 3. Salutation architecture.** Salutation managers are service brokers, isolated by transport managers from the details of specific network transport protocols.

`ServiceTemplate` constructor takes several arguments. The first is the service identifier. If the service identifier is null, then arrays of types (Java classes, typically interfaces) and attributes (attribute objects) are used to match services. A service matches if its class matches one of the classes in the types array and if, for each of the attribute objects, all non-null members match one of the service’s registered attributes. The return value from `lookup()` is an instance of `ServiceMatches`, which contains an array of remote control objects for the services that match. Finally, the `notify()` method allows a client to request an asynchronous notification when services matching a `ServiceTemplate` instance become available. This method uses Jini’s distributed events mechanism, which extends Java’s infrastructure for eventing across JVMs.

Jini depends on Java’s security model, which provides tools like digital certificates, encryption, and control over mobile code activities such as opening and accepting socket connections, reading and writing to specific files, and using native methods. Systems administrators can establish different policies depending on where the Java code originated (for example, the local file system or a remote machine).

## SALUTATION: A NETWORK-INDEPENDENT ARCHITECTURE

Salutation is an architecture for service discovery under development by the Salutation Consortium, which includes members from both industry and academia.<sup>3</sup> The consortium’s goal is to build a royalty-free architecture for service advertisement and discovery that is independent of a particular network transport.

Figure 3 shows the three fundamental components in the Salutation architecture: *functional units*,

*salutation managers*, and *transport managers*. From a client's point of view, a functional unit defines a service. Functional units already specified or under consideration by the Salutation Consortium include printing, faxing, and document storage. There is also work on a functional unit specification to allow discovery of Hewlett-Packard JetSend-enabled devices. The specifications define attributes that

## Salutation requires a network transport protocol that supports reliable, stream-oriented communication.

characterize a service (for example, in the case of a printer, double-sided capability, color, and so on).

The functional unit Doc Storage defines file attributes that can be used to find information in temporary or long-term storage. For example, a client can search for operating system-specific drivers or software necessary to interact with a newly discovered device. The client simply queries a Salutation manager for the necessary Doc Storage functional unit, extracts the application or device driver, and installs it, thus providing limited code mobility.

Salutation managers function as service brokers; they help clients find needed services and let services register their availability. Services can register and unregister functional units with the local Salutation manager by using the API calls `slmRegisterCapabilities()` and `slmUnregisterCapabilities()`, respectively. A client can use the `slmSearchCapability()` call to determine if Salutation managers have registered specific functional units. Under the current version of the architecture, applications can query only the local Salutation manager. Future versions will allow remote Salutation managers to be specified. Once a functional unit is discovered, `slmQueryCapability()` can be used to verify that a functional unit has certain capabilities. The API also includes calls for initialization/version checking, availability checking, and communication between clients and services. (An API simulator is available at <http://www.salutation.org/simulate.htm>.)

Salutation managers fill a role similar to lookup servers in Jini, but they can also manage the connections between clients and services. A Salutation manager can operate in one of three "personalities":

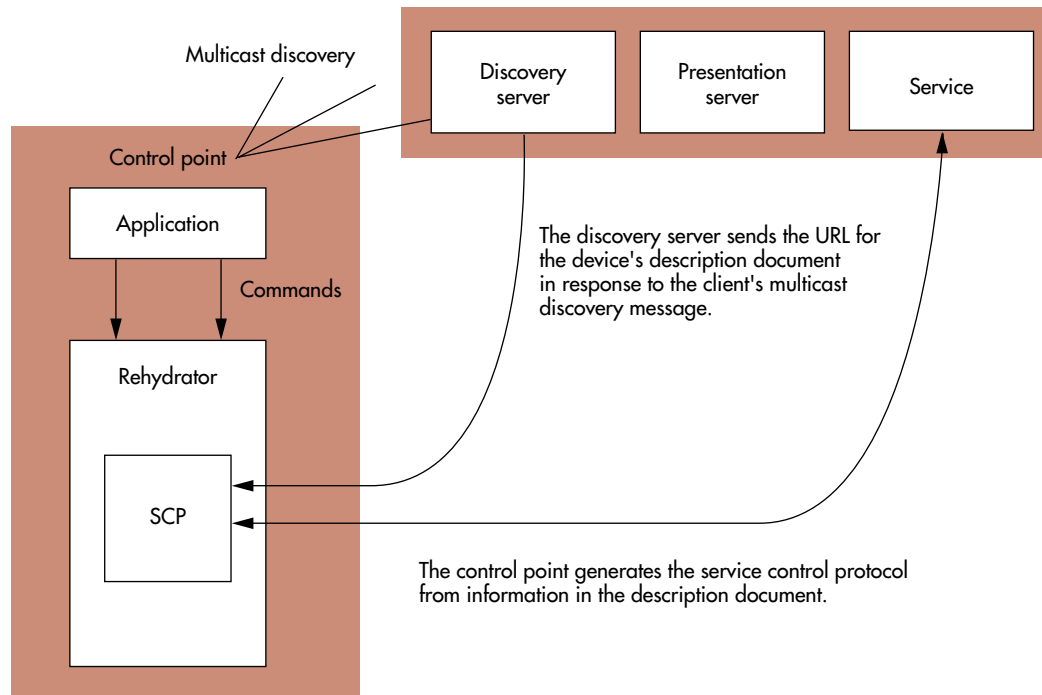
- In *native* personality, Salutation managers are used only for discovery. They establish a connection between a client and service but perform no further operations on the data stream.
- The *emulated* personality is similar to the native personality in that Salutation managers set up the connection, but in this case they transfer native data packets encapsulated in Salutation manager protocol format, providing a bridge when no common message protocol exists between client and service. The Salutation manager is ignorant of the semantic content of the data stream between client and service.
- In *Salutation* personality, Salutation managers establish the connection between client and service, and they also mandate the specific format of the data transferred. The Salutation architecture defines the data formats.

A transport manager isolates the implementation of the Salutation manager from particular transport-layer protocols and thereby gives Salutation network transport independence. To support a new network transport requires a new transport manager to be written, but does not require modifications to the Salutation manager. Like Jini (and UPnP), Salutation requires a network transport protocol that supports reliable, stream-oriented communication. Initial implementations are based on IP and IrDA because of their widespread use.

Transport managers also locate the Salutation managers on their respective network segments via either multicast, static configuration, or reference to a centralized directory. Discovery of other Salutation managers allows a particular Salutation manager to determine which functional units have been registered and to allow clients access to these remote services. Communication between Salutation managers is based on remote procedure call (RPC). This interaction between remote Salutation managers contrasts with other registry-based service discovery mechanisms (for example, Jini and Service Location Protocol), where clients would be responsible for locating remote registries.

The Salutation specification currently does not address security issues.

A lightweight version of Salutation, called Salutation-Lite, has been developed for resource-limited devices. It is based primarily on IrDA to leverage the large number of infrared-capable devices. Salutation-Lite focuses primarily on service discovery. It uses the functional units OpEnvironment and Display to describe the operating system, processor



**Figure 4. Interaction between a client (control point) and a service in UPnP.** The control point discovers the device by sending a multicast message. The device responds with a URL pointing to its description document, which the control point can download for pertinent information, including a URL to which control messages can be sent and the protocol for interacting with the device through this control URL. The “rehydrator” converts generic commands into device-specific control messages.

class, amount of memory, and display characteristics of palm-sized devices. By noting the particular characteristics of the device, servers can provide appropriate drivers and software wirelessly.

Salutation-Lite implementations can be downloaded free from the Salutation website at <http://www.salutation.org>.

## UPnP: XML FOR A WEB-BASED ARCHITECTURE

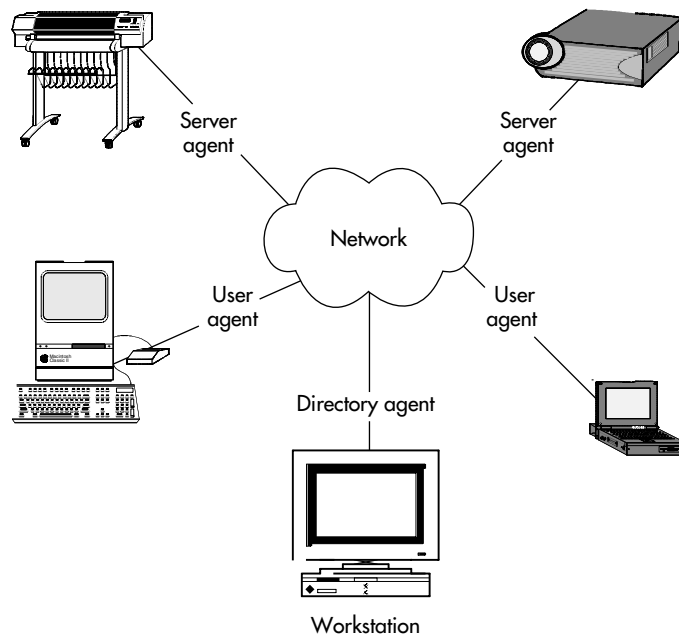
UPnP is a proposed architecture for service advertisement and discovery supported by the UPnP Forum, headed by Microsoft. Unlike Jini, which depends on mobile code, UPnP aims to standardize the protocols used by devices to communicate, using XML. The UPnP specification<sup>4</sup> is still in a preliminary stage; major issues like security have not yet been addressed.

UPnP’s device model is hierarchical. In a compound device (for example, a VCR/TV combo), the *root device* is discoverable, and a client (called a *control point*) can address the individual subdevices (for example, a tuner) independently. Virtual Web servers

in the device act as entry points for interacting with and controlling it. Devices that don’t speak UPnP directly are called *bridged devices*. They can be integrated into a UPnP network in a manner similar to the integration in a Jini device chassis: A bridge maps between UPnP and device-native protocols.

The UPnP specification describes device addressing, service advertisement and discovery, device control, eventing, and presentation. The eventing facility allows clients to watch for significant changes in the state of a discovered service. It functions similarly to Jini’s distributed event facility. Presentation allows a client to obtain a GUI for a discovered device through one of the device’s virtual Web servers. Several protocols support these functions:

- AutoIP,<sup>5</sup> a simple protocol that allows devices to dynamically claim IP addresses in the absence of a DHCP server;
- Simple service discovery protocol (SSDP), the UPnP mechanism for service discovery and advertisement;



**Figure 5. SLP entities: user agents, directory agents, and service agents. UAs discover services on behalf of applications, either via a DA or directly through an SA. In this example, a laptop and desktop are clients seeking services. A plotter and LCD projection system are services advertising their availability.**

- Simple object access protocol (SOAP),<sup>6</sup> a protocol for remote procedure calls based on XML and HTTP that is used for device control after discovery; and
- Generic Event Notification Architecture (GENA), a UPnP subscription-based event notification service based on HTTP.

When devices are introduced into a network, they multicast “alive” messages to control points. When they wish to cancel availability of their services, they send “byebye” messages. In SSDP, each service has three associated IDs—service type, service name, and location—which are multicast when services are advertised. Any of these IDs can also be used to search for services.

To search, a control point sends a UDP multicast request to the network, as shown in Figure 4. Matching services send unicast responses to the client. These responses contain URLs, each pointing to an XML *description document* that describes a service. A description document contains several important items:

- A *presentation URL* allows entry to a device’s root page, which provides a GUI for device control.

- A *control URL* is the entry point to the device’s control server, which accepts device-specific commands to control the device.
- An *event subscription URL* can be used by clients to subscribe to the device’s event service. The client provides an *event sink URL* in the subscription request. Significant state changes in the device result in a notification to the client’s event sink URL.
- A *service control protocol definition* describes the protocol for interacting with the device.

The service control protocol (SCP) definition allows APIs to be converted to device-specific commands, shielding the application level from details of particular devices. After retrieving the description document, a UPnP component on the control point called the *rehydrator* is “plumbed” with a definition of the device’s SCP. This component then sends device-specific commands via the device’s control URL. SOAP is used for this interaction.

SSDP is similar to the Internet Engineering Task Force’s service location protocol, but it lacks a query facility that can search for services by attributes. Further, SLP incorporates security measures and can interact with the IETF standards-track dynamic host configuration protocol (DHCP)<sup>7</sup> and the lightweight directory protocol (LDAP).<sup>8</sup> Finally, SSDP specifications currently limit discovery to a single subnet. Since UPnP does not use a registry, it is also likely to generate significantly more network traffic than SLP.

## SLP: A PROPOSED IETF STANDARD

Service location protocol is an IETF protocol for service discovery and advertisement.<sup>9</sup> It is currently at the “proposed standard” stage along the IETF standards track. Unlike Jini, Salutation, and UPnP, which all aspire to some degree of transport-level independence, SLP is designed solely for IP-based networks. It provides a set of C and Java bindings that provide service discovery and advertisement functions to application software.

SLP comprises three entities: *service agents* (SAs), *user agents* (UAs), and *directory agents* (DAs). SAs advertise the location and attributes of available services, while UAs discover the location and attributes of services needed by client software. UAs can discover services by issuing a directory-like query to the network. DAs cache information about available services. Unlike Jini, SLP can operate without directory servers. The presence of one or more DAs can substantially improve perfor-

mance, however, by reducing the number of multicast messages and the amount of network bandwidth used. In fact, if DHCP is used to configure SLP agents with the location of DAs, then multicast is completely unnecessary. SLP also interoperates with LDAP, so services registered with an SLP DA can be automatically registered in an LDAP directory. This eliminates the need to reconfigure clients that already discover services using LDAP.

SLP has several mechanisms for discovering DAs:

- In passive discovery, SAs and UAs listen for multicast announcements from DAs, which periodically repeat these advertisements.
- In active discovery, SAs and UAs multicast SLP requests or use DHCP to discover DAs. When a DA is present, SAs and UAs use unicast communication to, respectively, register their services and find appropriate services.

In the absence of DAs, UAs multicast requests for service and receive unicast responses directly from the SAs that control matching services. This tends to increase bandwidth consumption, but provides a simpler model, appropriate for small networks (such as a home LAN).

SLP services are advertised through a service URL, which contains all information necessary to contact a service. Clients use the service URL to connect to the service. The protocol used between the client and server is outside the scope of the SLP specification. This separation is similar to Bluetooth, where the SDP does not specifically address how devices will communicate.

Service templates define an attribute set for each service type (a printer, for example).<sup>10</sup> The attributes include a specification of the attribute types and information about default and allowed values; they are used to differentiate between services of the same type and to communicate configuration information to UAs.

SLP doesn't define the protocols for communication between clients and services, and so its security model concentrates on preventing the malicious propagation of false information about service locations. SAs can include digital signatures when registering so DAs and UAs can verify their identity. Digital signatures can also be required when DAs advertise their availability, allowing UAs and SAs to avoid rogue DAs (that is, those without a proper signature). As with Jini, setting up the security features of SLP requires some configura-

tion effort, but the effort can be well worth it, particularly in open environments.

## BRIDGING THE TECHNOLOGIES

For service discovery to become pervasive, either a single service discovery technology must dominate or the most commonly used technologies must be made interoperable. Currently, bridging seems to be the most promising prospect for interoperability.

### Implementations of certain low-level functions of service discovery (such as discovering registries) are interchangeable.

Implementations of certain low-level functions of service discovery (such as discovering registries) are interchangeable. For example, the Salutation Consortium uses SLP for service discovery beyond the local subnet. This lets the Salutation Manager search for SLP DAs, and then use SLP to register functional units and search for requested services.

A Jini-SLP bridge has also been developed, which allows services lacking a JVM to participate in Jini systems.<sup>11</sup> The heart of the Jini-SLP bridge is a special SLP UA that registers the availability of "Jini-capable" SLP SAs. To do this, Jini-capable SLP services advertise the availability of a Jini driver factory. The UA discovers all SAs with driver factories and registers them with one or more Jini lookup services. When a Jini client needs one of the registered SAs, it downloads the driver factory from the lookup server and uses it to instantiate a Java object to drive the service. Note that the SLP SAs are *not* required to host a Java virtual machine—the Java code installed on the SAs is static. Similar schemes are possible for the other technologies; for example, it should be possible to Jini-enable UPnP services in this way.

Miller and Pascoe<sup>12</sup> describe mapping Salutation to Bluetooth SDP to take advantage of Bluetooth's wireless capability. Two approaches are considered: The first maps the Salutation APIs to Bluetooth SDP by implementing Salutation on top of Bluetooth; the second uses a Bluetooth transport manager and essentially replaces Bluetooth SDP with Salutation. This approach will also



work with other schemes, like Jini. Bluetooth is a particularly attractive target for interoperability, primarily because of its wireless capability. Because of this, additional interoperability efforts between Bluetooth and other service discovery technologies seem inevitable.

Each service discovery technology has advantages and disadvantages. Currently, interoperability efforts are perhaps the most important force in service discovery, since it is very unlikely that device manufacturers will embrace multiple service discovery technologies on low-cost devices. ■

### ACKNOWLEDGMENTS

Thanks to Sumi Helal of the University of Florida for sparking my interest in this area. Much of the material in this article is derived from a tutorial he invited me to create for IPCCC 2000 in Phoenix. Many thanks to Erik Guttman of Sun Microsystems for clarifying the differences between SLP and SSDP and going way beyond the call of duty in critiquing early versions of this article. David La Motta and Kirk Perilloux were kind enough to read early versions and offer suggestions. Finally, my personal editor (and mate) Christine Ciarmello-Richard was gracious enough to lend her critical eye, as always.

### REFERENCES

1. *Specification of the Bluetooth System*; available at <http://www.bluetooth.com/developer/specification/specification.asp>.
2. K. Arnold et al., *The Jini Specification*, Addison-Wesley Longman, Reading, Mass., 1999.
3. *Salutation Architecture Specification*; available online at <http://www.salutation.org/specordr.htm>.
4. *Universal Plug and Play specification v1.0*; available online at <http://www.upnp.org/>.
5. R. Troll, "Automatically Choosing an IP Address in an Ad-Hoc IPv4 Network," IETF Internet draft, work in progress, Mar. 2000.
6. Simple Object Access Protocol (SOAP) 1.1, W3C Note; available online at <http://www.w3.org/TR/SOAP>.
7. R. Droms, "Dynamic Host Configuration Protocol," IETF RFC 2131, Mar. 1997; available online at <http://www.dhcp.org/rfc2131.html>.
8. M. Wahl, T. Howes, and S. Kille, "Lightweight Directory Access Protocol, version 3," IETF RFC 2251, Dec. 1997; available online at <http://www.rfc-editor.org/rfc/rfc2251.txt>.
9. E. Guttman, "Service Location Protocol: Automatic Discovery of IP Network Services," *IEEE Internet Computing*, vol. 3, no. 4, July/Aug. 1999, pp. 71-80.
10. E. Guttman, C. Perkins, and J. Kempf, "Service Templates and Service: Schemes," IETF RFC 2609, June 1999; available online at <http://www.rfc-editor.org/rfc/rfc2609.txt>.
11. E. Guttman and J. Kempf, "Automatic Discovery of Thin Servers: SLP, Jini and the SLP-Jini Bridge," *Proc. 25th Ann. Conf. IEEE Industrial Electronics Soc. (IECON 99)*, IEEE Press, Piscataway, N.J., 1999.
12. B. Miller and R. Pascoe, "Mapping Salutation Architecture APIs to the Bluetooth Service Discovery Layer," white paper; available online at <http://www.salutation.org/whitepaper/BtoothMapping.pdf>.

Golden G. Richard III is an assistant professor of computer science at the University of New Orleans in Louisiana. His research interests include mobile computing, wireless networking, operating systems, and fault tolerance. He is on the executive committee of the IEEE Technical Committee on the Internet, a member of the IEEE and the ACM, and liaison to the University of New Orleans for Usenix's Educational Outreach Program.

Readers may contact the author at [golden@cs.uno.edu](mailto:golden@cs.uno.edu).

## How to Reach IC

### Writers

We welcome submissions about Internet application technologies. For detailed instructions and information on peer review, *IEEE Internet Computing's* author guidelines are available online at <http://computer.org/internet/edguide.htm>.

### Letters to the Editor

Please send letters via e-mail to [internet-computing@computer.org](mailto:internet-computing@computer.org).

### Reuse Permission


For permission to reprint an article published in *IC*, contact William J. Hagen, IEEE Copyrights and Trademarks Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331; [w.hagen@ieee.org](mailto:w.hagen@ieee.org). Complete information is available at <http://computer.org/permission.htm>. To purchase reprints, visit <http://computer.org/author/reprint.htm>.

# **APPENDIX F**

**Mc  
Graw  
Hill**

**[ Thoroughly Explains More Than  
1,400 Networking Concepts ]**

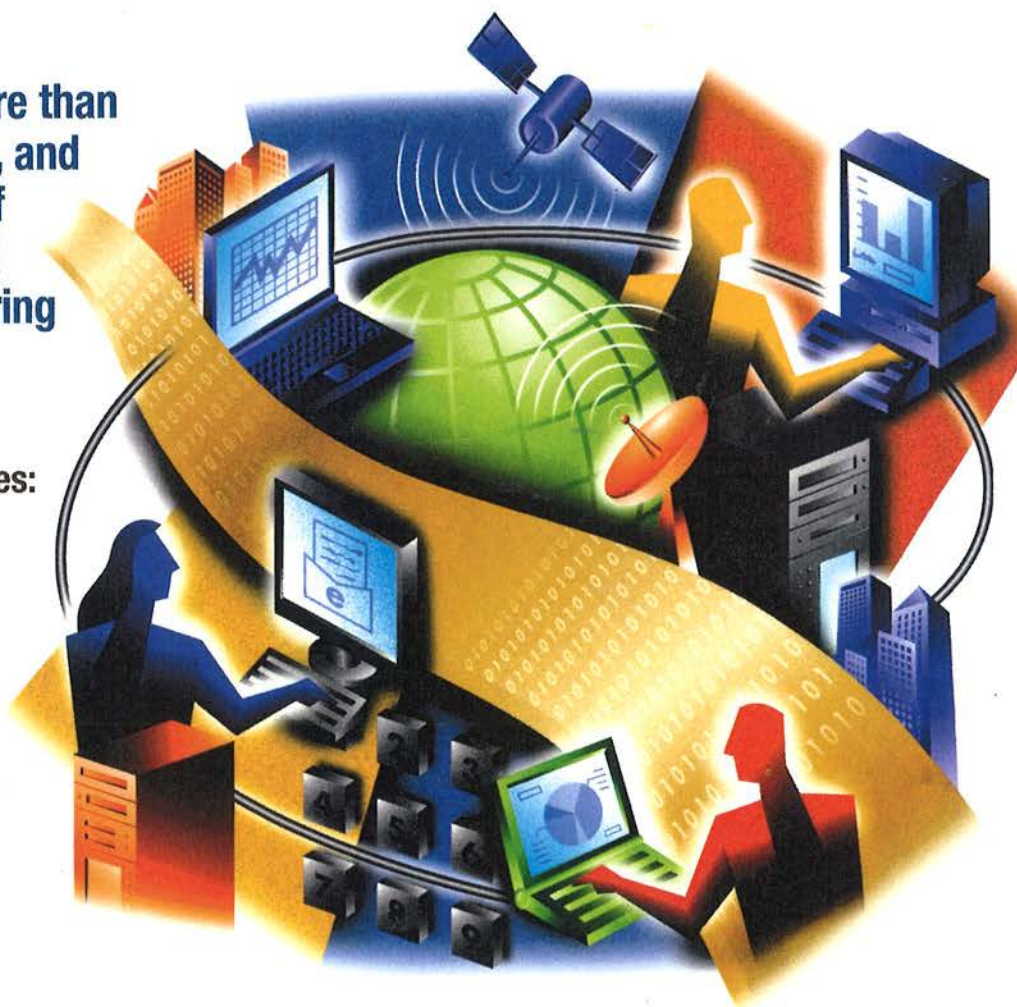
# Encyclopedia of Networking & Telecommunications



**CD contains more than  
5,000 hyperlinks, and  
a complete set of  
cross-referenced  
Internet engineering  
documents**

**Covers emerging technologies:  
all-optical networks,  
broadband access,  
wireless computing, QoS,  
.NET, and more**

**Addresses vendor-specific  
technologies: Microsoft®,  
Cisco®, IBM®, Juniper®,  
Nortel®, Sun®, and others**



**Tom Sheldon**

Certified Network Engineer and author of the best-selling  
*Encyclopedia of Networking, Electronic Edition*

**OSBORNE**   
ROKU EXH. 1002





McGraw  
Hill

# Encyclopedia

of Networking & Telecommunications

## The Most Complete Volume of Networking Technologies Available

### TOPICS COVERED:

ASP (Application Service Provider)  
Bluetooth  
Cryptography  
Distributed Computer Networks  
Embedded Systems  
Hacking and Hackers  
InfiniBand  
Java  
Linux  
Load Balancing  
Mobile Computing  
NAS (Network Attached Storage)  
Network Processors  
Optical Networks  
Outsourcing  
PKI (Public Key Infrastructure)  
QoS (Quality of Service)  
SAN (Storage Area Network)  
Switching Fabrics  
Transaction Processing  
UNIX  
Webcasting  
XML



*Authoritative and up-to-date,* this all-encompassing book and CD-ROM package is filled with thousands of explanations and analyses of core and cutting-edge networking and telecommunications topics—from Abilene to QoS to ZAWS. Extensive cross-referencing throughout helps you understand the relationship among the technologies.

This is a must-have resource for every network professional, as well as technology investors, marketing managers, head hunters, technology writers, and anyone interested in networking.

The book also includes the most comprehensive guide to Internet engineering documents (RFCs) available today. *The McGraw-Hill Encyclopedia of Networking & Telecommunications* reflects the latest in networking and Internet technologies.



### On the value-packed CD-ROM

- Complete, fully searchable version of the book with thousands of hyperlinks to related topics in the book
- External hyperlinks to author-selected Web sites for further information
- Illustrations of complex networking topics

Praise for the previous edition:

**"In the rapidly converging disciplines of voice and data networks, I haven't found any other source that provides the coverage that [this book] provides."**

—Randy Johnson,  
Applications Engineer,  
Nokia IP Telephony  
Business Unit

**"The best reference I could find as a student learning about networks."**

—Joe Higgins,  
Southwest Memorial  
Hospital, Director of  
Education/Telemedicine

**"I interface daily with network engineers. This encyclopedia has helped me 'keep pace' with the engineering units."**

—Steve Goldman,  
Chief Technical Specialist,  
Empire Blue Cross and  
Blue Shield

### ABOUT THE AUTHOR:

Tom Sheldon is a Certified Network Engineer and has been building networks for nearly three decades. In that time, he has operated a network testing lab and constructed networks for Lockheed Space Operations. He is the author of more than 30 highly-acclaimed technical books, including *Encyclopedia of Networking*, *Electronic Edition*, *Windows NT Security Handbook*, and *Microsoft Internet Information Server*. Tom maintains the Linktionary.com Web site.

OSBORNE

REQUIRED READING for the Information Age

A Division of The McGraw-Hill Companies

\$69.99 USA

£51.99 UK

NETWORKING



www.osborne.com

Book P/N 0-07-212270-6 of  
ISBN 0-07-212005-3



90000



# **McGraw-Hill**

# **Encyclopedia of Networking & Telecommunications**

Tom Sheldon

**Osborne/McGraw-Hill**

New York Chicago San Francisco  
Lisbon London Madrid Mexico City  
Milan New Delhi San Juan  
Seoul Singapore Sydney Toronto



Osborne/McGraw-Hill  
2600 Tenth Street  
Berkeley, California 94710  
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact Osborne/McGraw-Hill at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

### **McGraw-Hill Encyclopedia of Networking & Telecommunications**

Copyright © 2001 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

1234567890 DOC DOC 01987654321

Book p/n 0-07-212005-3 and CD p/n 0-07-212005-3  
parts of  
ISBN 0-07-212005-3

#### **Publisher**

Brandon A. Nordin

#### **Vice President & Associate Publisher**

Scott Rogers

#### **Acquisitions Editors**

Wendy Rinaldi and Ann Sellers

#### **Project Editor**

Lisa Wolters-Broder

#### **Acquisitions Coordinator**

Timothy Madrid

#### **Technical Editor**

Dan Logan

#### **Copy Editor**

Dennis Weaver

#### **Proofreaders**

Linda and Paul Medoff

#### **Indexer**

Jack Lewis

#### **Computer Designers**

Michelle Galicia

Tara A. Davis

#### **Illustrator**

Michael Mueller

#### **Series Design**

Peter F. Hancik

#### **Cover Design**

Amparo del Rio

This book was composed with Corel VENTURA™ Publisher.

Information has been obtained by Osborne/McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, Osborne/McGraw-Hill, or others, Osborne/McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from use of such information.

## Service Advertising and Discovery

Services on networks can be advertised so that users can discover them. A number of protocols and schemes are available to support service advertising and discovery. For example, service advertising and discovery is important as mobile devices and mobile wireless devices proliferate on networks. These devices may connect to networks at varying locations. A service discovery and advertising protocol is an important tool to help these devices find services on the network wherever they connect, and to let other network users know about the services they are offering.

Keep in mind that as networks evolve, a variety of services will be offered. For example, network services such as file, print, and applications services can be advertised to “foreign” mobile users who temporarily connect to a network. But other possibilities exist, especially in the wireless realm. For example, an airport could have numerous small wireless networks that are limited in range to about 10 or 20 feet. As you walk into the range of one of these networks, various service advertisements appear on your portable device. These may be advertisements for peripherals like printers that you can use, but they could also be commercial advertisements.

If you are familiar with instant messaging, you are familiar with service advertising protocols. When a person in your “buddy list” signs on to the network, you receive an alert and you can start chatting with them over the network via special chat software, Internet phone, or videoconferencing software. In the case of the airport wireless networks mentioned previously, advertising protocols can alert you to friends who are located in the general vicinity. Their wireless device is advertising their personal ID and your wireless device listens for IDs and looks them up in your personal address book. If a friend is nearby, your device gets excited and starts beeping.

Two earlier advertising services that were developed for LAN environments include SAP (Service Advertising Protocol) and NetBIOS (Network Basic Input/Output System). These are discussed under their own heading.

A number of new approaches have been developed to provide enhanced service advertising and discovery in dynamic network environments such as the wireless and mobile computing networks, where devices frequently connect and disconnect from the network. When a device comes online, it advertises its services or listens for advertisements of available services.

One technique a device may use to locate a service on the network is to send out a multicast packet that contains a service request. Network devices that are providing services listen for multicast packets and then determine whether they can satisfy the request for services being made by the client. If so, the service will respond to the client with a positive message.

Here are some architectures and schemes related to service discovery, advertising, and acquisition:

- **Salutation** The Salutation architecture is a royalty-free service discovery and service management product from the Salutation Consortium, a nonprofit corporation. Salutation is an open standard, independent of operating system, communications protocol, hardware platform, or vendor-imposed limitations. It was created to provide service

discovery for a broad range of network appliances and equipment in a platform-, OS-, and network-independent environment. Devices can use it to advertise and describe their capabilities and discover the capabilities of other devices by using search features.

- **SLP (Service Location Protocol)** SLP is an IETF standard designed to make it easy for network clients to discover the available services on a network and learn information about the configuration of those services. Many vendors support SLP in their operating systems, including Apple, IBM, Novell, and Sun Microsystems. The IETF Service Location Working Group is developing SLP and similar services. See "SLP (Service Location Protocol)."
- **Microsoft.NET** The Microsoft.NET platform for Web Services is a development environment based on building applications with "Web Services." The technique is similar to building distributed objects, but is based on HTTP and XML. Data is represented with XML and delivered in SOAP (Simple Object Access Protocol) messages via HTTP. A language called WSDL (Web Services Description Language) is used to describe services. An XML-based protocol called Disco is used to discover services at a site and a mechanism called UDDI (Universal Description, Discovery, and Integration) defines how to advertise services and how Web Service consumers can find services. See Microsoft.NET.
- **SSDP (Simple Service Discovery Protocol)** SSDP is a Microsoft service location protocol that is part of Microsoft's Universal Plug and Play (UpnP) initiative. It is oriented toward home networks. Like SLP, it enables devices to request information about services on a network and to advertise their presence and the services they offer.
- **Bluetooth** This is a wireless connectivity specification that enables electronic devices to talk spontaneously and allows instant wireless connectivity between computers, mobile phones, and portable devices. Bluetooth includes its own service discovery protocol that locates services offered by devices within the vicinity of a user's Bluetooth device. Currently, Bluetooth's service discovery protocol is being mapped to the Salutation architecture. See "Bluetooth."
- **Jini** This is a Java-based technology defined by Sun Microsystems. When Jini-enabled devices connect to networks, they establish impromptu Java-oriented networks that let users immediately access network resources and services. The technology is designed to support any device that "passes digital information in or out" according to Sun. Devices register with the network when they connect, which makes them available to other devices. For example, when a printer is attached and gets registered, it makes its driver available on the network and this driver gets downloaded to clients when they need to use the printer.
- **JetSend (Hewlett-Packard)** JetSend is code that is embedded in devices to allow them to directly exchange information. Devices become either senders or receivers. JetSend gives devices the intelligence to know their own capabilities and negotiate the best way to exchange information with other devices. No external operating systems need to get involved. No special drivers are needed to connect with other devices. All JetSend devices can immediately communicate. JetSend is a transport-independent protocol that

works across any bidirectional transport, including TCP/IP, IR, IEEE 1394, and others. It is ideal for PDAs, digital cameras, copiers, network-attached printers and scanners, fax machines, and other devices.

- **Inferno by Lucent Technologies** A real-time network operating system that provides a software infrastructure for creating distributed network applications. Inferno is more like a file system that operates over a variety of transport protocols. It is designed to provide connectivity over the Internet, public telephone networks, cable television, and satellite broadcast networks. Inferno includes network and security protocols. It has a very small memory footprint and can be used as a stand-alone OS on information appliances.

A lot of the work being done in this area is for home networking and network appliance configuration. In particular, Jini and Microsoft's UPnP are designed to help devices connect and cooperate.

The IETF Resource Capabilities Discovery (rescap) Working Group is developing services that distribute information about resources or services to the global Internet. The IETF Service Location Protocol (svrloc) Working Group has developed procedures for discovering services.

**Related Entries** Bluetooth; Directory Services; Embedded Systems; Home Networking; Instant Messaging; Java; Microsoft.NET; Mobile Computing; Network Appliances; Search and Discovery Services; *and* SLP (Service Location Protocol)

Linktionary!—Tom Sheldon's Encyclopedia of Networking updates	<a href="http://www.linktionary.com/s/service_advertising.html">http://www.linktionary.com/s/service_advertising.html</a>
Salutation Consortium	<a href="http://www.salutation.org">http://www.salutation.org</a>
IETF Working Group: Service Location Protocol (svrloc)	<a href="http://www.ietf.org/html.charters/svrloc-charter.html">http://www.ietf.org/html.charters/svrloc-charter.html</a>
IETF Working Group: Resource Capabilities Discovery (rescap)	<a href="http://www.ietf.org/html.charters/rescap-charter.html">http://www.ietf.org/html.charters/rescap-charter.html</a>
Microsoft (search for SSDP)	<a href="http://www.microsoft.com/">http://www.microsoft.com/</a>
Sun Microsystems JINI network technology	<a href="http://www.sun.com/jini/">http://www.sun.com/jini/</a>
The Official Bluetooth Web site	<a href="http://www.bluetooth.com/">http://www.bluetooth.com/</a>
Jetsend home page	<a href="http://www.jetsend.com">http://www.jetsend.com</a>

## Service Providers and Carriers

Anyone with an Internet access account and a telephone is familiar with service providers and carriers. You pay them money every month. However, "service providers" and "carriers" are broad categories. This section describes the different types of service providers and carriers and the service they offer.

In the beginning, at least in the United States, there was one phone company: AT&T. The ILECs (*incumbent local exchange carriers*) are the result of the breakup of AT&T in 1984. That breakup created seven independent RBOCs (Regional Bell Operating Companies). These included Pacific Bell, NYNEX, GTE, and others, but mergers and consolidations have changed

# APPENDIX G



Designed for  
  
Microsoft®  
Windows NT®  
Windows 95

**One-Stop Reference**

*The Essential Guide for Administrators,  
Systems Engineers, and IS Professionals*



# Running Microsoft® **Windows NT Server 4.0**

Charlie Russel and  
Sharon Crawford

**Microsoft® Press**

**RUNNING**

# Microsoft® Windows NT® Server 4.0

The Essential Guide  
for Administrators,  
Systems Engineers,  
and IS Professionals

*Charlie Russel and  
Sharon Crawford*

**Microsoft® Press**

PUBLISHED BY  
Microsoft Press  
A Division of Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052-6399

Copyright © 1997 by Charlie Russel and Sharon Crawford

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data pending.

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QMQM 2 1 0 9 8 7

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office. Or contact Microsoft Press International directly at fax (206) 936-7329.

Macintosh is a registered trademark of Apple Computer, Inc. Intel is a registered trademark of Intel Corporation. Microsoft, Microsoft Press, MS-DOS, Windows, Windows NT, Windows NT Server, and Windows NT Workstation are registered trademarks, and ActiveX, BackOffice, and FrontPage are trademarks of Microsoft Corporation. Java is a trademark of Sun Microsystems, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

**Acquisitions Editor:** David J. Clark  
**Project Editor:** Sigrid Anne Strom  
**Technical Editor:** Jim Fuchs

# CHAPTER 11

## Printers and Other Resources

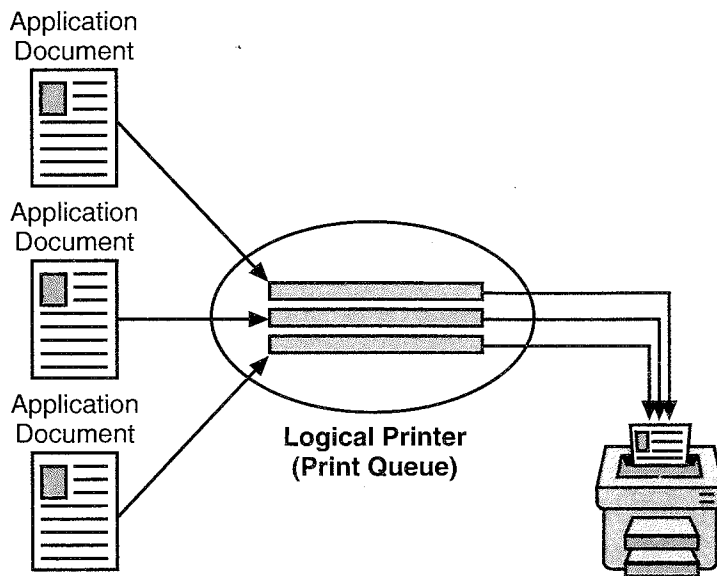
Hardware is expensive and companies don't like to invest in it until they absolutely have to. And as hard as it is to get permission to buy new equipment, it's even harder to get permission to buy equipment that is used only infrequently. From an economics point of view, the investment in equipment pays off only to the extent that the equipment is used. One of the great advantages of a network—although far from being the only one—is the ability to share equipment that otherwise would stand idle much of the time. Printers are a perfect example of this, and they are an obvious item to share. One could, certainly, consider providing an inexpensive dot matrix or ink jet printer for most users, but it's unlikely that many people would consider putting an expensive, high-end color printer or even a good, fast laser printer on everyone's desk. And you don't really need to. By putting one high-end printer on the network, you spread the cost and machine use across all of your users, which makes the investment in the equipment much easier to justify.

### NOTE

*Microsoft Windows NT version 4 uses some special and sometimes confusing terms when referring to printers. First it's important to differentiate between a print device, which is the actual machine that does the printing, and a printer, which in Microsoft terminology is the software interface between the application and the actual print device. Therefore, a printer in Microsoft terminology is actually a logical entity.*

## Printer Setup Options

To keep confusion to a minimum, we will refer to the print device simply as the “printer.” We will refer to the software interface as the “logical printer.” You should be aware, however, that the Windows NT documentation either doesn't use these terms or doesn't use them in this way. In a Novell NetWare or OS/2 networking environment, the term *print queue* is used instead of printer (meaning the logical printer), but the net effect is the same. Windows NT Server supports a broad range of printers. Figure 11.1 shows the simplest possible arrangement—a print job in Windows NT going to a logical printer, from which the job is spooled to a printer.



**FIGURE 11.1**

*Example of jobs routing through a logical printer to a printer*

You can have one logical printer associated with a single printer, which is the arrangement shown in Figure 11.1. Or you can have several logical printers associated with a single printer. In this arrangement, logical printers can be configured at different priority levels, so that one is for normal printing and the others are for jobs that can wait to be printed later. For a printer that uses both Postscript and PCL, having two logical printers allows users to choose either type of printing.

You also can have a single logical printer associated with multiple printers. If all of the printers use the same printer driver—an arrangement called a *printer pool*—a single logical printer will send jobs to the first available printer. The advantage of a printer pool is that the administrator can add or remove printers without affecting user configurations because the printers are interchangeable. The disadvantage of a printer pool is that there's no way to predict which printer will receive which job. So don't pool printers when they are physically far apart!

## Planning Network Printing

As for everything you do on a network, you need to actually *plan* where and how your printers will be set up, configured, shared, and managed—a nuisance, but a necessary nuisance if you want to keep your trouble and your support calls down. You need to think about how your users really use printers, where the heaviest users are physically located, where to physically locate highly specialized printers such as plotters and color laser printers, and how you're going to physically connect all of the printers to the network.

Let's look at the last of these questions for a moment. To the average PC user, printers are always attached to a parallel port. But that doesn't work well for a network or for a server. Parallel ports require a fair amount of CPU attention to do their thing, which is the last thing you want on a server. You're also usually limited to three parallel ports. The other two choices are a serial connection (preferably using a "smart," multiport serial card) or a network connection. Either works well, but, in most cases these days, your best bet is a direct network connection.

How you choose to connect your printers will be influenced by several factors. You'll need to consider your physical layout. Are your users all in central physical locations? If so, you might find it easiest to simply recycle an older PC as a print server by installing a multiport serial card in it and using it to drive the printers. Or are your users (and their associated print needs) located in separate offices spread over several floors? If so, you'll probably want to use network connections, either external connections or connections built into the printers, to connect printers that are conveniently located for each group of offices.

There are two basic methods for connecting your printers directly to the network. You can use a high-end printer that comes with a network card that is either built in or available as an option. Or you can use a stand-alone network print server—the Hewlett-Packard JetDirect EX is a good example—that supports a variety of protocols and usually comes with drivers to support many network operating systems, including Windows NT Server. This is useful in a typical organizational environment, where your network might well consist of multiple operating systems—all of which require access to that expensive color laser printer.

In any case, once you've decided where and how to physically locate and connect the printers, you'll need to create and manage the logical printers that your users will actually see.

## **Managing Printers**

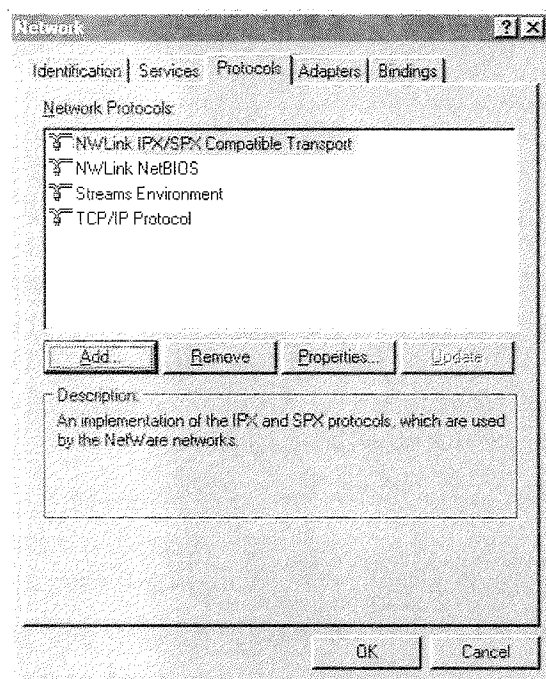
Managing printers is not about the printers themselves but about how they are connected to and managed as part of your overall Windows NT Server network. You'll have to choose which networking protocol to use if the printers are network printers, decide which server you will use to manage them, and decide what functions you will allow your users to have access to.

### **Installing the DLC Protocol**

If you have a Hewlett-Packard (HP) network printer, you have several options for controlling it; the simplest option is probably to use the DLC protocol. Another option is to use TCP/IP, which is probably the better option in the long run; but we'll

save the discussion of TCP/IP printing installation for Chapter 17, where we discuss the TCP/IP protocol in detail. For the moment, let's stick with DLC. It has the advantage of being simple and straightforward, so we can focus on the printer side of what we're doing and not get bogged down in the intricacies of TCP/IP. If you will be managing HP printers and if you haven't already installed DLC, now is a good time to install it. Remember, installing any protocol will require a reboot of the server, so plan the installation for a time when there will be minimal disruption to your users. To install the DLC protocol, follow these steps:

1. Open Control Panel, and double-click the Network icon to bring up the Network dialog box.
2. Click the Protocols tab (shown in Figure 11.2).

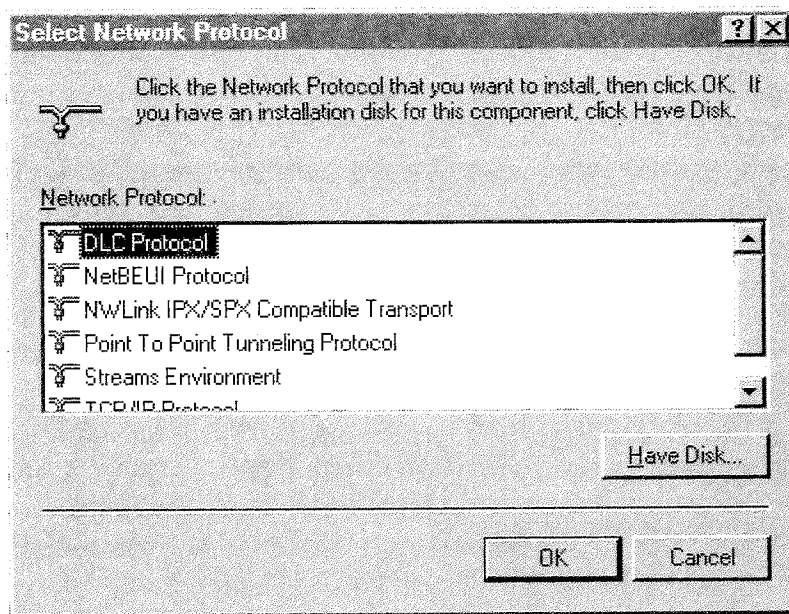


**FIGURE 11.2**

*The Protocols page in the Network dialog box*

3. Click Add, and select the DLC protocol from the list, as shown on the following page in Figure 11.3.
4. The system will prompt you for your Windows NT Server version 4 CD-ROM, of course, so that the necessary files can be loaded. If Windows NT Server is looking in the wrong place, you can browse for the correct location.

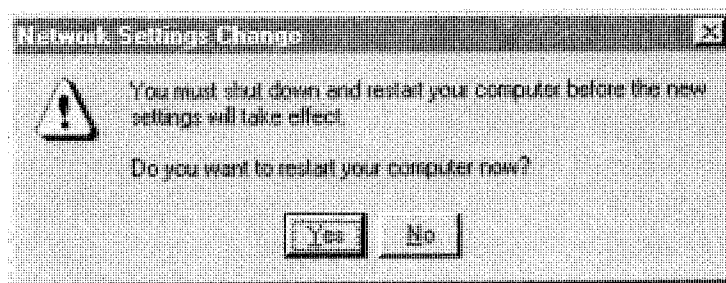




**FIGURE 11.3**

*The Select Network Protocol dialog box showing the selected protocol*

5. After the necessary files are loaded, go ahead and close the Network properties dialog box; Windows NT Server will make the necessary changes to network bindings. When it's finished, it will prompt you to reboot your server, as shown in Figure 11.4. Click Yes. When the rebooting is complete, the new protocol will be in place.



**FIGURE 11.4**

*Network Settings Change confirmation message*

Now that you have the DLC protocol installed, you will be able to manipulate the HP network printers and JetDirect print servers directly, just as if they were physically attached to the server.

## Adding a New Printer

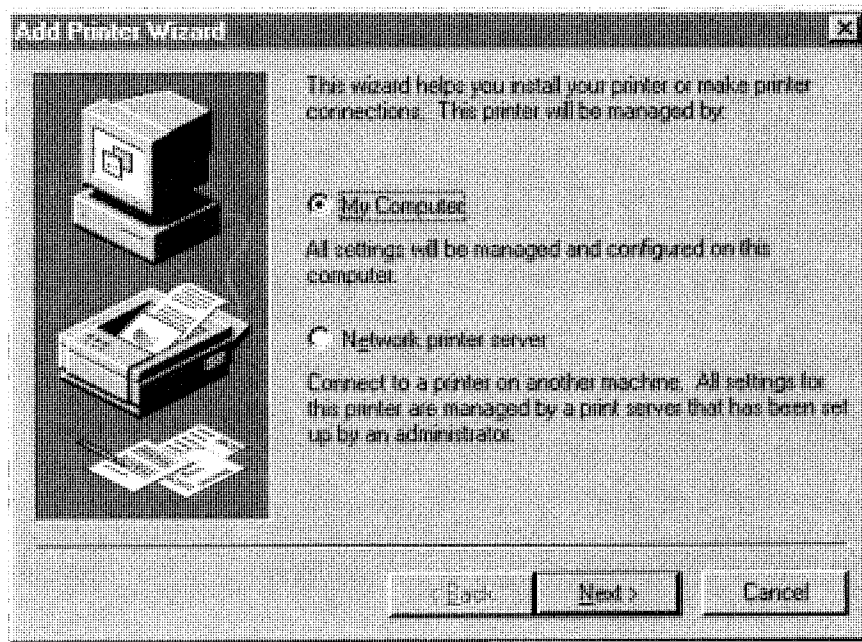
Before you can make a printer available to the rest of your network, you must add it to the server that will control it. Try to centralize the control of your printers to make managing them simpler. But whenever possible, you also should have at least two different servers sharing the same network printer. This allows the users access to a printer pool that consists of two logical printers that point to the same printer. Now if you need to take down one of the servers for some reason, users will still have access to the printer.

Adding a new printer to the network involves several actions:

- ◆ Adding the printer port, if it doesn't already exist
- ◆ Logically connecting the printer to the port
- ◆ Setting the device-specific options for the printer
- ◆ Loading the necessary drivers for Windows clients who will be using the printer
- ◆ Sharing the printer to the rest of the network, and then setting permissions for who can control the printer and manage the documents that are printed on it
- ◆ Testing the new logical printer
- ◆ Adding the printer to the network clients and testing the connections

The Add Printer Wizard will take you through the process of adding a new logical printer to a server—creating the logical printer, connecting it to the print device, and testing the result. To add a printer to the server, follow these steps:

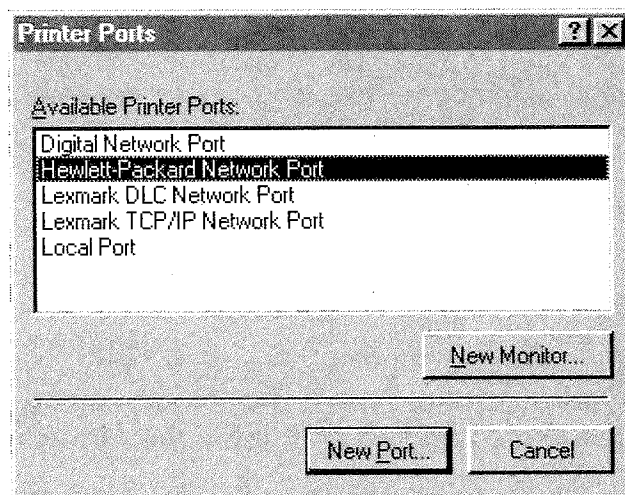
1. Click Start. Choose Settings and then Printers from the submenus that open from the Start menu.
2. Double-click Add Printer to start the Add Printer Wizard (Figure 11.5 on the following page).
3. Click the My Computer option button, even if the printer you are adding is physically connected to the network and not to the server. Then click Next.



**FIGURE 11.5**

*Add Printer Wizard opening window*

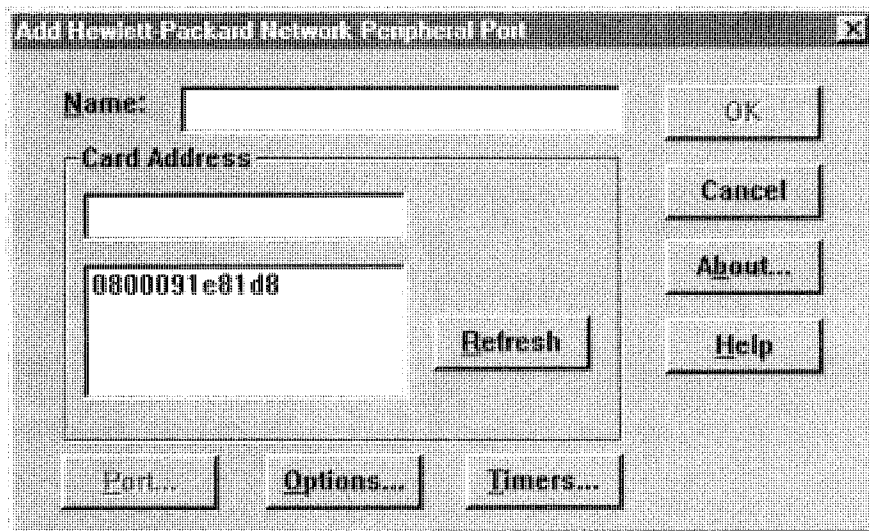
4. If the port to which the printer is physically attached is present on the list that is displayed, check that box and jump to step 7. Otherwise, click Add Port to bring up the Printer Ports dialog box shown in Figure 11.6.



**FIGURE 11.6**

*Printer Ports dialog box*

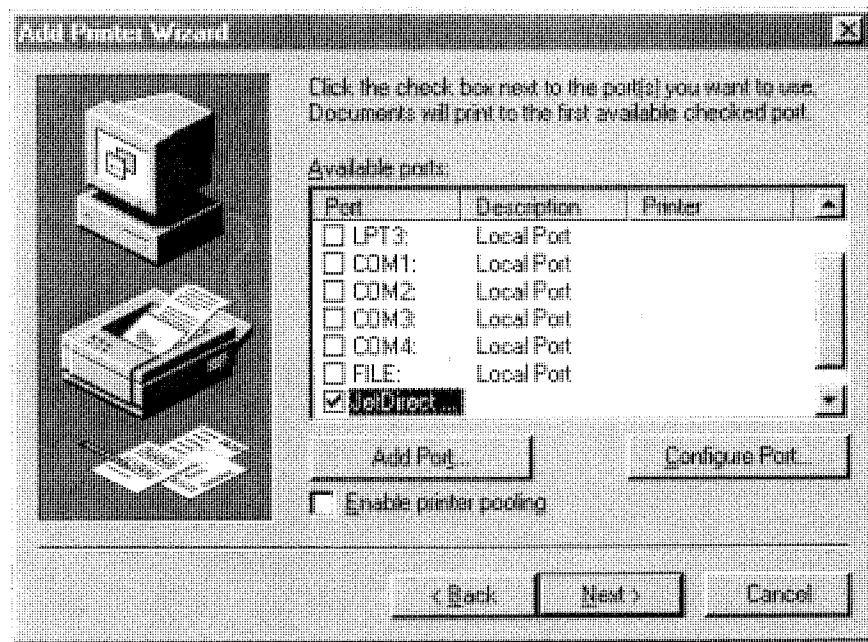
5. Select the kind of port you want to add, and click New Port. If the necessary files are not yet on the server, the Add Printer Wizard will prompt for your Windows NT Server version 4 CD-ROM to install them. Then it will prompt you to specify the name and network card address for the type of port you are adding. To add an HP DLC printer, for example, select Hewlett-Packard Network Port and click New Port. You'll see the dialog box shown in Figure 11.7.



**FIGURE 11.7**

*Example of an Add Network Peripheral Port dialog box*

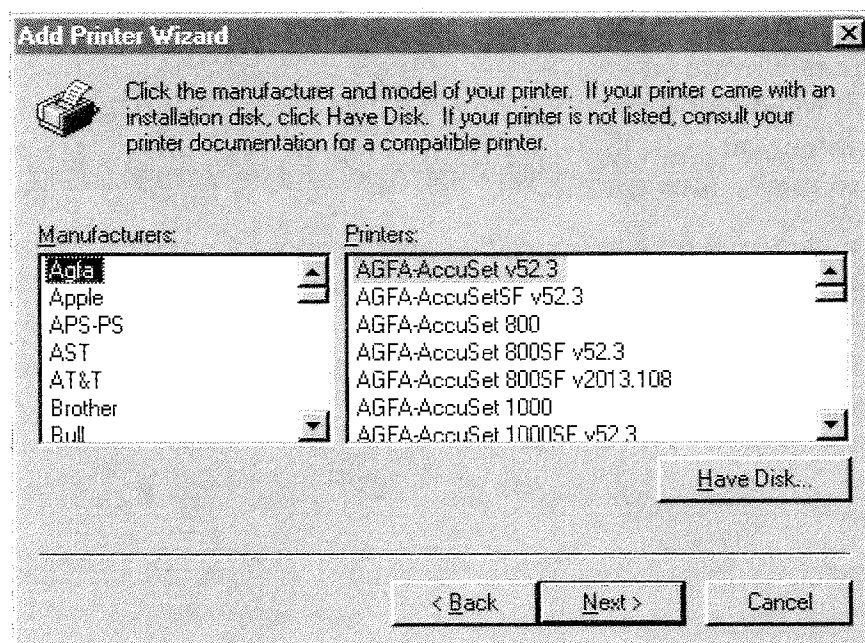
6. Select the hardware address of the printer or print server network card you want to add, and then double-click it. If you are adding an HP network printer, you must know the hardware MAC address for the printer or print server's network card.
7. Choose a name for the new port. Be sure to choose a name that describes the printer or printer port clearly because you won't be able to change it later. Type the name in the Name text box. Click OK. The main Add Printer Wizard screen will return with the new port checked, as shown in Figure 11.8 on the following page.



**FIGURE 11.8**

*Example of Add Printer Wizard dialog box showing a new port*

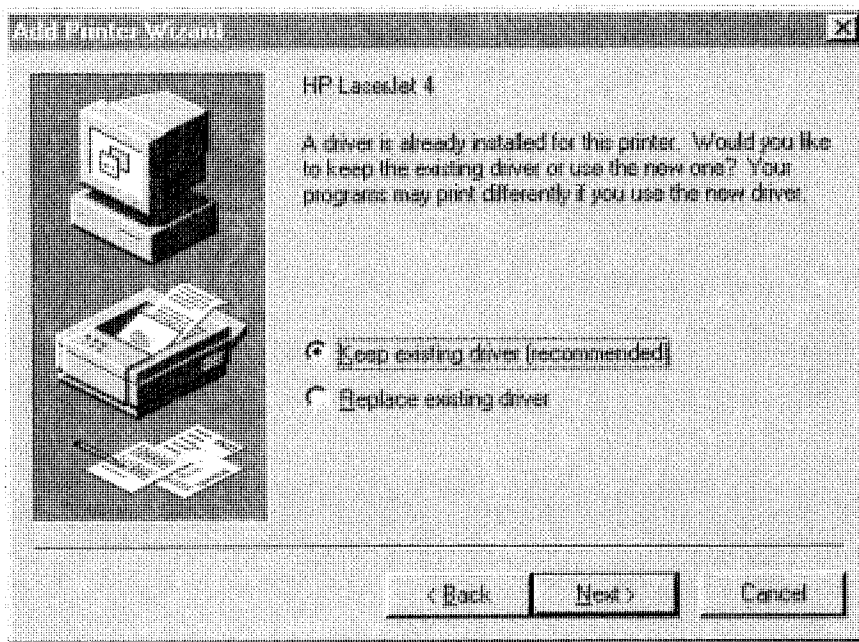
8. Click Next to choose the type of printer you are attaching to the port, as shown in the example in Figure 11.9. Select the printer manufacturer in the left-hand pane of the window, and then select the model of printer from the list in the right-hand pane.



**FIGURE 11.9**

*Add Printer Wizard showing list of printers and manufacturers*

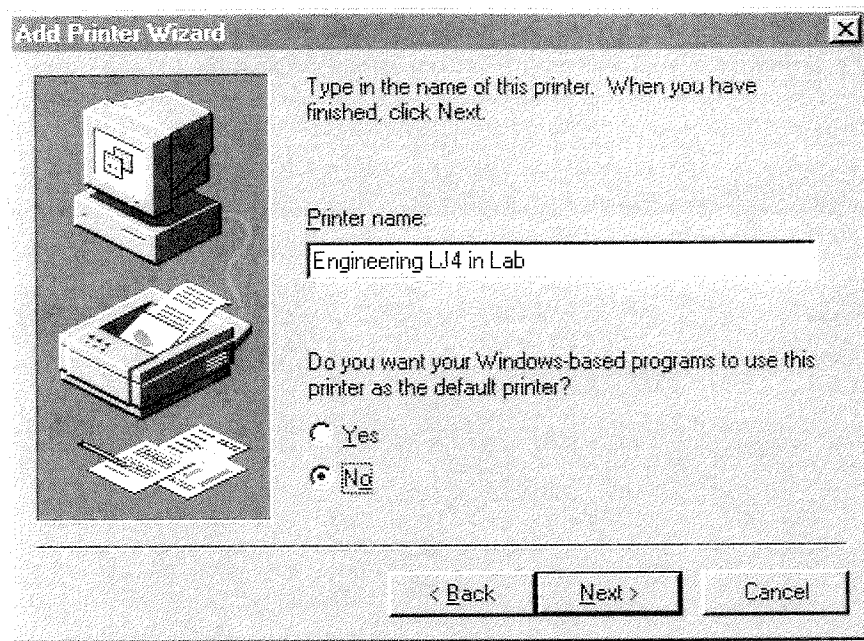
9. If your printer manufacturer has provided a special driver disk for Windows NT version 4, click Have Disk to manually add this driver.
10. After you've chosen the type of printer you are adding, click Next. If there is already a driver for this type of printer loaded, you'll get a message like the one shown in Figure 11.10. You can use that driver or replace it with a new driver. Click the appropriate option button, and then click Next.



**FIGURE 11.10**

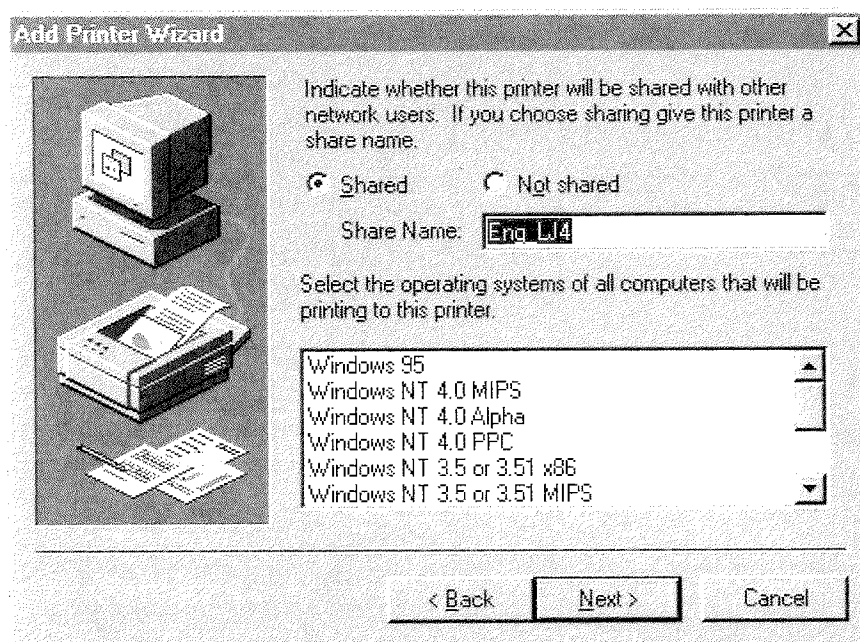
*Add Printer Wizard showing existing driver message*

11. Give the new printer a name that describes its function or its location clearly. Type the name in the Printer Name text box, as shown on the following page in Figure 11.11. Click the Yes or the No option button to specify whether this printer will be the default Windows NT Server printer. Then click Next.
12. If you're sharing this printer on the network, click the Shared option button. Choose a share name for the printer, and type the name in the Share Name text box, as shown on the following page in Figure 11.12. If the printer will be shared with MS-DOS or Microsoft Windows 3.x clients, make sure you stick to a maximum of eight characters for the name and don't use spaces or weird characters in the name.



**FIGURE 11.11**

*Add Printer Wizard showing Printer Name text box*

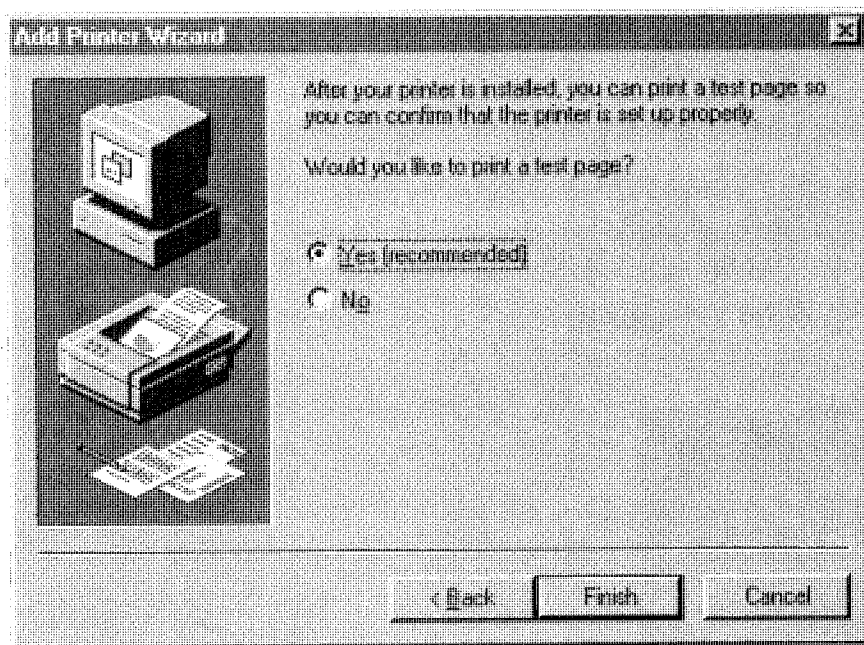


**FIGURE 11.12**

*Add Printer Wizard showing shared printer dialog box*



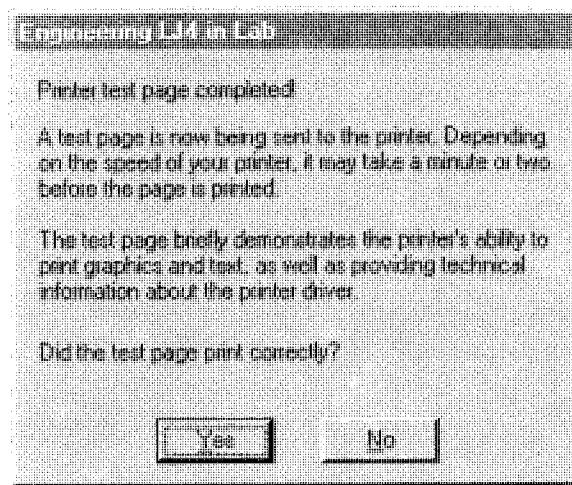
13. Windows NT Server can load printer drivers for other 32-bit Microsoft operating systems in addition to the current version of Windows NT, including drivers for previous versions of Windows NT and Microsoft Windows 95. Select all operating systems on the network that will be using this printer, and click Next.
14. The Add Printer Wizard will now prompt you for a variety of disks, CD-ROMs, and source directories for the various operating systems you selected. Just browse to the proper places in the dialog boxes, and you'll eventually get to the last screen in this process, which is shown in Figure 11.13.



**FIGURE 11.13**

*Add Printer Wizard showing print test message*

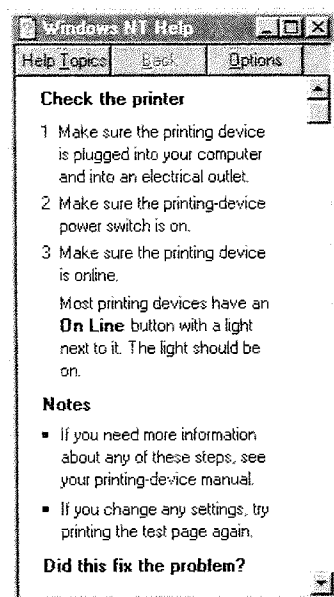
15. Always choose to print a test page to make sure everything works as it should from the server. You'll also want to test each client machine as you add this printer to them, but first things first. The printer should work from the server before it's added to the network clients. Click Finish, and you're almost done.
16. When it has finished printing the test page, Windows NT Server will give you a chance to confirm that all went as expected. (See Figure 11.14 on the following page.)



**FIGURE 11.14**

*Add Printer Wizard test page confirmation message*

17. If the test page printed correctly, you're done. If it did not print correctly, click No to start up the Windows NT Help system (Figure 11.15). The Windows NT Help application will walk you through the steps to troubleshoot and fix your printer.



**FIGURE 11.15**

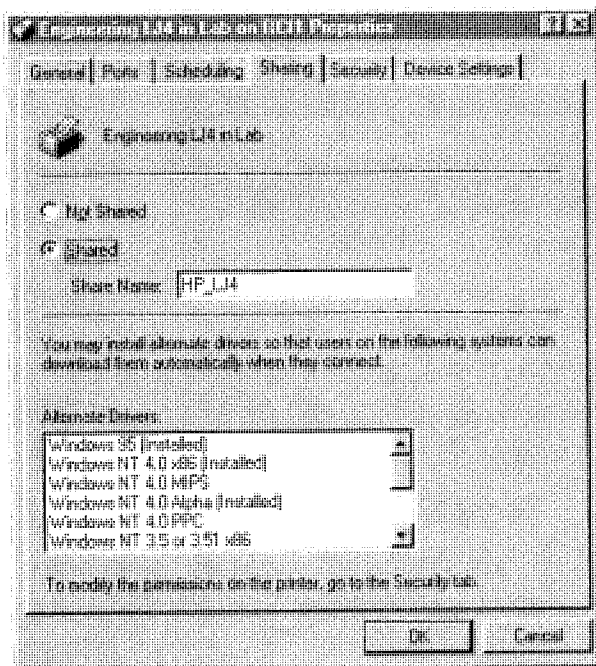
*Windows NT Help window*

Whew! We've now added a new printer to the system and shared it to the network. You'll use an essentially similar series of steps to add a printer to the system no matter what kind of connection you have to the printer, although the particular options obviously will differ for each type of connection.

## Sharing a Printer

Sharing a printer in Windows NT Server is easy. As you have seen in the preceding section, the normal printer installation process allows you to share the printer during installation. But you also can choose to share a printer on the network later, after installation, as a separate step. Perhaps you're experimenting with the printer locally before making it available to the network. Or perhaps something about the printer has changed, and you want to change the share name. Or maybe you have a printer with multiple personalities, and you want to share it with a different name for each personality. Whatever the reason, the steps to share a printer are the same.

1. Choose Settings and then Printers from the submenus that open from the Start menu.
2. Right-click the printer you want to share. Choose Sharing from the menu that appears, which brings up the Properties dialog box for the printer with the Sharing page in front, as shown in Figure 11.16. Now click the Shared option button.

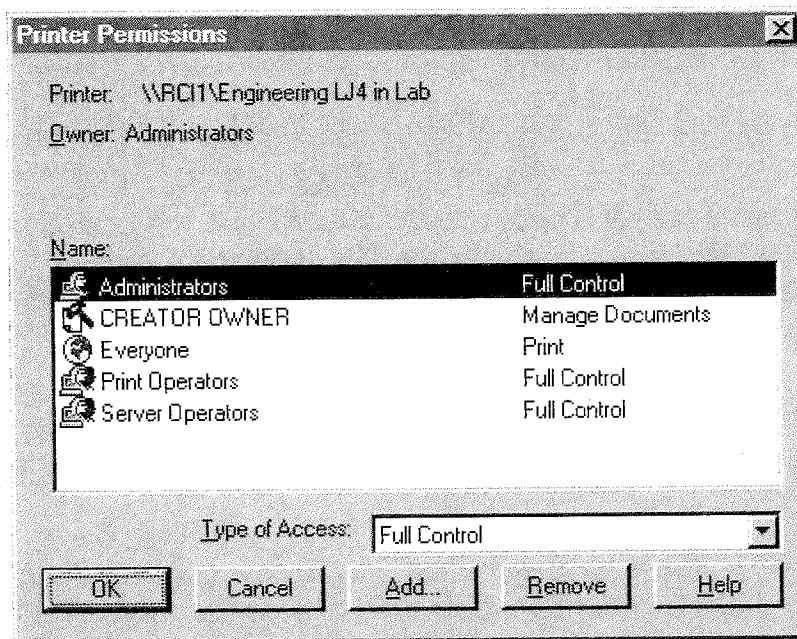


**FIGURE 11.16**

*Printer Properties dialog box showing Sharing page*

3. If your printer will be used by other operating systems, such as earlier versions of Windows NT or Windows 95, you can choose to have the printer drivers for these operating systems loaded on the server, which further reduces the overhead to the clients. Select the drivers you want to support in the Alternate Drivers list box.

4. Click the Security tab to establish the permissions for the printer. From here you can control who has access to a printer and who manages the printer queue. The default settings are shown in Figure 11.17, but you can change them easily to, for example, allow only a special group to use the printer. See “Configuring Printer Security” on page 240 for instructions on printer security specifications.



**FIGURE 11.17**

*Printer Permissions dialog box*

5. After you’ve made your changes (if any) to the security settings for the printer, click OK and the printer will be shared to the network.

That’s it. Pretty straightforward. You should now add the printer to at least one client of each operating system type that you expect to support and print a test page, just to make sure that everything works as you expect.

## Deleting a Printer

If you change your network’s printer configuration, you might have to delete a printer from the list of currently available printers stored in the system. This is one procedure that is a bit awkward in Windows NT Server. There is no simple way to remove a printer and change all of the workstation references to it.

You can remove the printer easily enough, of course. That’s not hard. Simply select the printer in the Printers folder, and press Delete. ZAP! It’s gone. But this does nothing to remove the printer reference from workstations that may have been

using the printer. They're going to end up with a reference that points to a non-existent printer. This isn't generally a polite way to run your network. Now you could, and obviously *should*, send around an E-mail message to all users on your system who might be using the printer and let them know the printer is going to be removed—preferably with a bit of advance notice, although one doesn't always have a lot of choice in this matter.

However, there's a better choice than simply removing the printer—replace it. In most cases, there will be a functionally equivalent printer available somewhere in your system, maybe one in the same geographical area as the printer you are removing. Perhaps it's the printer you bought to replace that aged and infirm printer you now want to remove. Or maybe it's another printer in the same general vicinity as the one you want to remove. Whatever it is, you'll do your users a favor by sharing the replacement printer with the same name as the name of the printer you're removing. Or create a second name for an existing printer that matches the name of the one you're removing. But however you make the change, notify your users. It cuts down on the noise level substantially.

## **Changing a Printer**

Changing a printer—that is, replacing one printer with another—requires little if any change to your user configurations if the printers are close relatives. Just swap the two printers and keep the printers' shared name the same, even if some of the underlying configuration has changed. As long as there is no real difference in the overall capabilities of the two printers, this will work. This is one advantage in the way Windows NT Server version 4 handles printers. Because printer drivers are maintained at the server level instead of at the workstation level, even fairly significant changes in the printer will be transparent to the user. When you physically change the printer out, however, don't forget to change the printer driver that is associated with the printer.

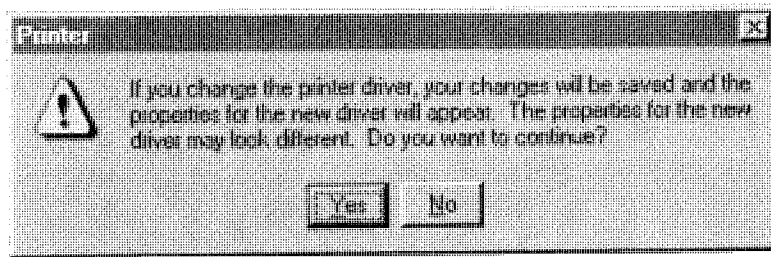
### ***Changing the printer driver***

One of the tasks you inevitably will have to do is change a printer driver. The reason—whether it's because you've physically changed a printer or because the manufacturer of the printer has provided an updated driver—doesn't really matter. This is a nuisance, but at least now you only have to do it in one place, although you will need drivers for all of the operating systems you're supporting. Be aware that changing a printer driver can change the available features of the printer.

To change the printer driver for a printer, follow these steps:

1. Choose Settings and then Printers from the submenus that open from the Start menu.
2. Right-click the printer for which you are changing the driver, and choose Properties to bring up the Properties dialog box for the printer.

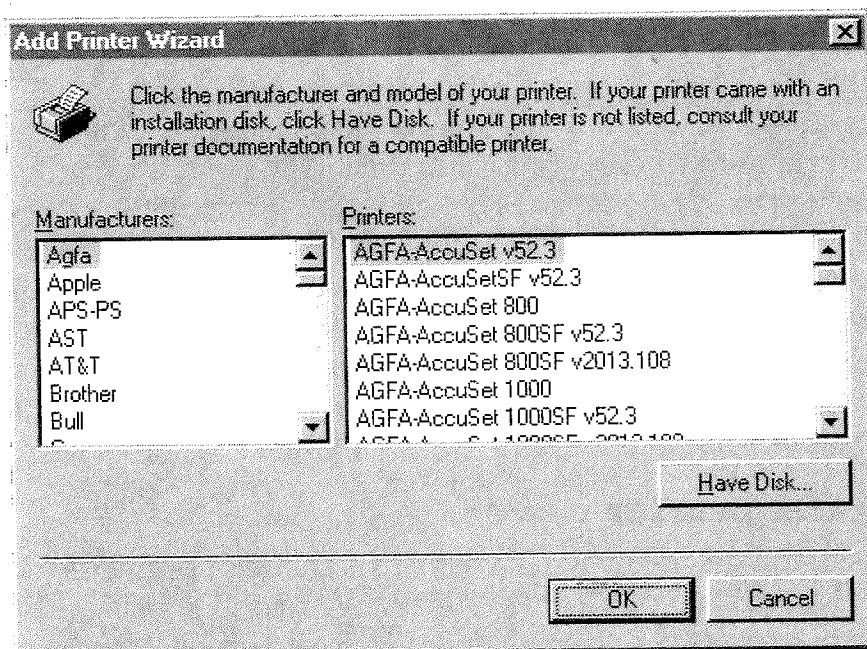
3. Click New Driver. You'll get a warning message like the one shown in Figure 11.18. Click Yes to continue.



**FIGURE 11.18**

*Printer change driver warning message*

4. A list of printers like the one shown in Figure 11.19 will appear. Select your printer from this list of available printer drivers; click OK. Or select Have Disk to use an updated driver from the manufacturer.

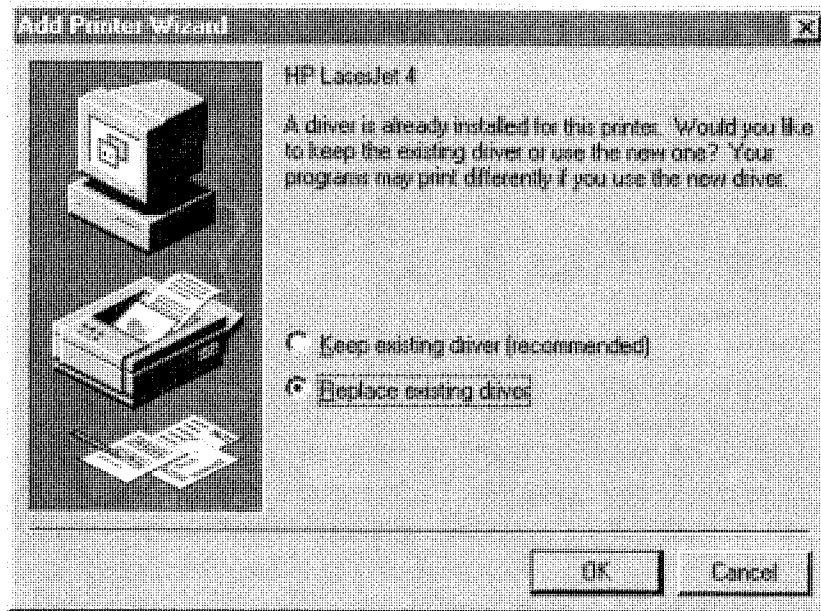


**FIGURE 11.19**

*Add Printer Wizard showing available printer drivers*

5. If you select Have Disk, browse to the location of the new driver's .INF file. Or select the correct printer manufacturer and correct model of your printer from the list. Click OK.
6. If you already have a driver for the selected printer on the system, you will see a warning message like the one in Figure 11.20. If you're updat-

ing the printer driver, you'll generally want to overwrite the existing driver. Otherwise, you can keep the existing driver. Click the appropriate option button, and then click OK.



**FIGURE 11.20**

*Existing driver warning message*

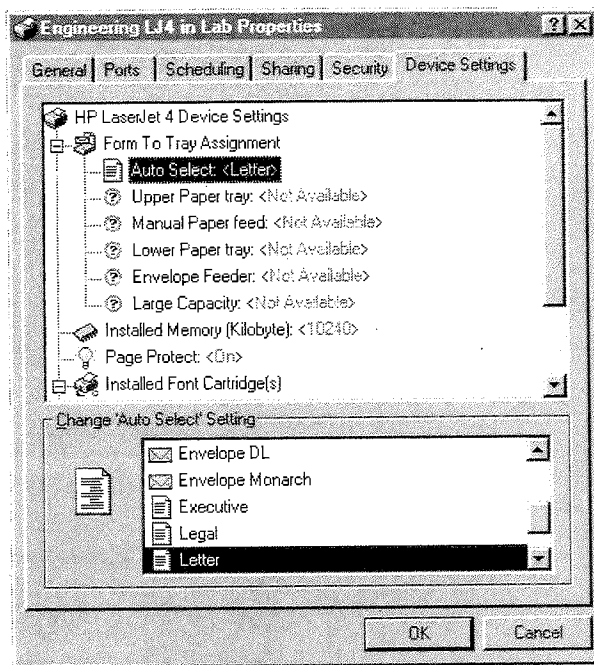
7. After you've updated the driver, also update all versions of the driver that you have on the system to support other operating systems. Click the Sharing tab of the Properties dialog box for the printer. In the Alternate Drivers list box, click the operating systems you'll be updating, and then click OK. You might have to browse to the correct location for the necessary files.
8. When the files have been updated, the new drivers are in place.

## **Modifying printer properties**

Each printer has its own unique set of device-specific settings, which you can modify to match your needs. We won't attempt to tell you what all the possibilities are but will point you in the direction of where to go to change them.

The printer's device-specific properties are a tab in the printer's Properties dialog box that we've been working with in the preceding sections. Right-click the printer icon, and choose Properties. Now click the Device Settings tab. You'll see a long list of device-specific settings that you can change, assuming you have the permission to do so. A typical example is the list of settings for an HP LaserJet 4 printer shown in Figure 11.21 on the following page.





**FIGURE 11.21**

*A Device Settings dialog box showing the settings for a specific printer*

If you have anything other than the default amount of memory installed on the printer, the value for Installed Memory is often incorrect. Change this if you've added extra memory. If you have added print cartridges to the printer since the device settings were last updated, also add them here.

## Logical Printer or Print Queue

In addition to managing your printer and the drivers that are associated with it, you'll also need to manage the print jobs that are sent to the logical printer (print queue). Generally, you can do the following things:

- ◆ Attach a device name to a logical printer (necessary for many legacy MS-DOS programs).
- ◆ Change the times when a printer is available.
- ◆ Pause a printer. (Jobs can continue to be sent to the printer, but nothing comes out.)
- ◆ Pause a specific document in the queue.
- ◆ Resume printing a paused document.
- ◆ Restart a specific document in the queue.
- ◆ Change the priority of the documents in the queue.

- ◆ Cancel (delete) a print job from the queue.
- ◆ Schedule a specific time to print a particular job in the queue.
- ◆ Change which user gets notified when a job is done printing.

The way you do the things in the bulleted list is pretty straightforward and can be performed from the printer's window. However, redirecting a logical printer to a print device is specific to each workstation and is done at the workstation. It's not something that is done at the server. But because Windows NT Server can do this for legacy MS-DOS applications only by using a command line, we'll show you the specifics of how to do that.

## Attaching a Device Name to a Logical Printer

Many legacy MS-DOS programs don't really "understand" network logical printers. They understand good old-fashioned device names such as LPT1 and LPT2. So you have to fool them into thinking they're printing to one of those devices, even though you are actually redirecting their output to one of the logical printers. You have to do it at each workstation or server that will have programs printing to the specific device in question. Unfortunately, there's no cute GUI way to do this in Windows NT Server. The only way you can do it is to use a command line that reassigns a device name to the logical printer. For example, you might want to assign the device name LPT1 to a network printer. The command line to accomplish this task is this:

```
net use lpt1 \\<servername>\<sharename>
```

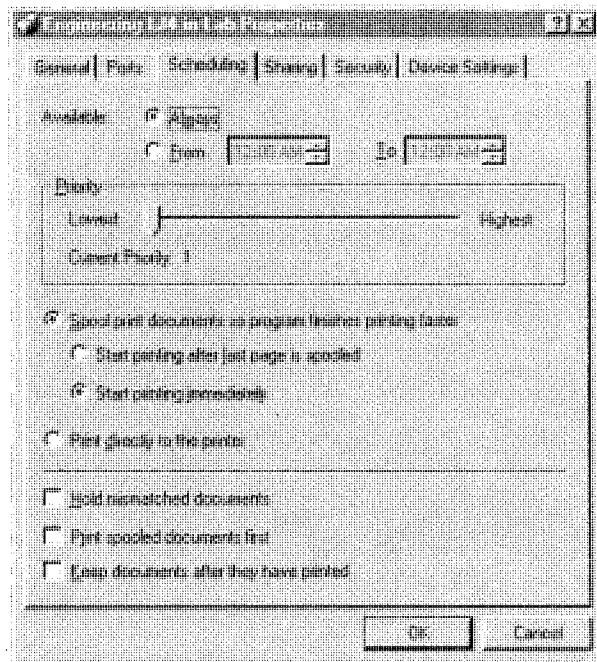
You can add this command easily to the users' logon script to make this happen automatically. Or you can let your users know about the command, and they can run the command manually as needed. Normally, the connection will not be remembered between logon sessions, but you can change that by changing the command line to read:

```
net use lpt1 \\<servername>\<sharename> /persistent:yes
```

## Changing the Times a Printer Is Available

By default, printers are available on the network at all times of the day. But if you have an expensive printer, you might want to restrict access to the printer to a particular time of the day. You can change the schedule for the printer. Right-click the printer icon, and choose Properties. Then click the Scheduling tab in the dialog box that appears (Figure 11.22 on the following page). Click the option button next to From, and choose the begin and end times from the From and To list boxes.

You also can change a number of other options on this page, but, in general, you'll find that the default settings for these other options are perfectly adequate.

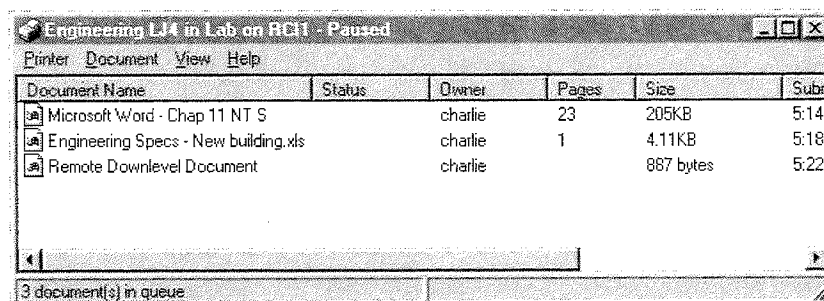


**FIGURE 11.22**

*Printer Properties dialog box showing Scheduling tab*

## Managing Documents in a Logical Printer

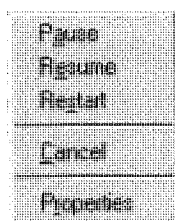
You can manipulate the documents in a logical printer by opening the printer window on your screen and then selecting which document you want to manipulate. Open the printer by double-clicking its icon. A window will open, the one shown in Figure 11.23, which shows a printer that has been directed to pause with three documents waiting in the queue to print.



**FIGURE 11.23**

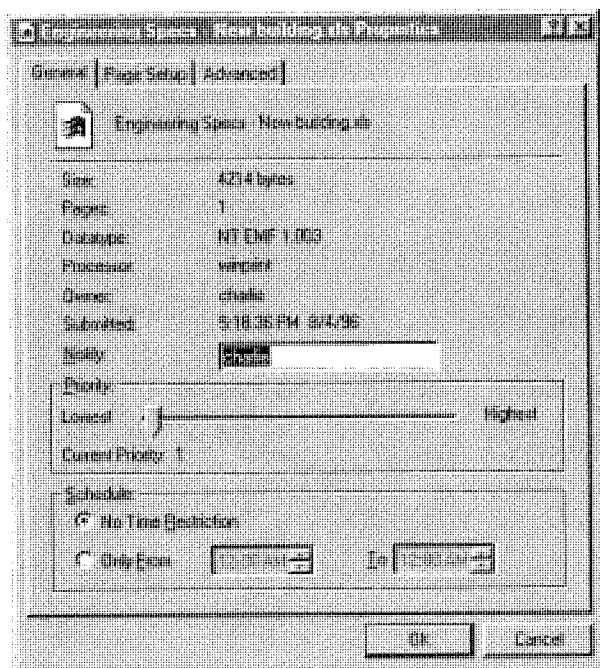
*Printer Properties dialog box showing documents paused in print queue*

Right-click a document to bring up the menu shown here:



From this menu, you can pause the printing of a document in the queue, resume printing a document that is paused in the queue, restart a document from the beginning, or select Cancel to delete it from the queue entirely. Pause is a useful option when you have a problem with a printer and you need to stop any jobs that are being sent to it while you fix the problem.

You also can use this menu to change the properties of a print job on the fly. Perhaps you realize that your 400-page document is going to tie up the printer for a while and your boss really needs that shopping list printed out before he goes home. Or you want to notify the administrative assistant that you've printed out a stack of new hardware requisitions, which now need to be entered into the system. No problem. Right-click the document, and choose Properties. You'll get the dialog box shown in Figure 11.24.



**FIGURE 11.24**

*Example of a document Properties dialog box*

In the document Properties dialog box, you can change or view the properties of the documents in the queue for printing. You can change the document's priority in the queue—making sure that a specific document is the next one printed, for example, by giving it the highest priority of any of the documents currently in the queue. You also can change the time when the document is scheduled to print and who will be notified when the document is finished printing. So you can take that 400-page document and schedule it to print after everyone else has gone home; you then can change the Notify field so that the system notifies your administrative assistant when the requisitions are finished. All you have left to do is crank up the priority on your boss's shopping list. You look like a genius. We wish administrative tasks were all that easy.

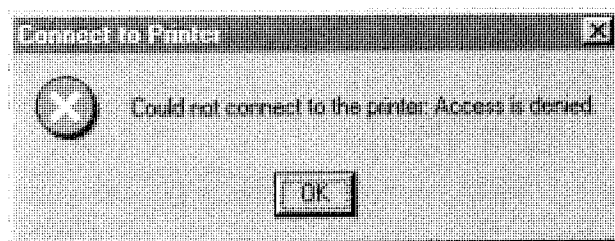
## Configuring Printer Security

When a printer is to be shared on the network, one of the decisions you will have to make is which users will be allowed access to the printer. As for all security features of Windows NT Server, you, as the system administrator, have a great deal of control over who can use the printer and what level of control each individual can have over the printer and the print jobs on it. Windows NT Server is definite about defining levels of individual access to a printer.

There are four basic levels of user access to a printer:

### ◆ No Access

The printer is not available to users who have this level of access. They can see the printer when browsing, but if they attempt to add the printer, the result is the rather rude message shown in Figure 11.25.



**FIGURE 11.25**

*No-access-to-printer message*

### ◆ Print

The user can print to the printer but has no control over the printer queue or the documents in it unless he or she created the print job.

### ◆ **Manage Documents**

The user can pause print jobs that are scheduled to print on the printer, change their priority, or even delete them.

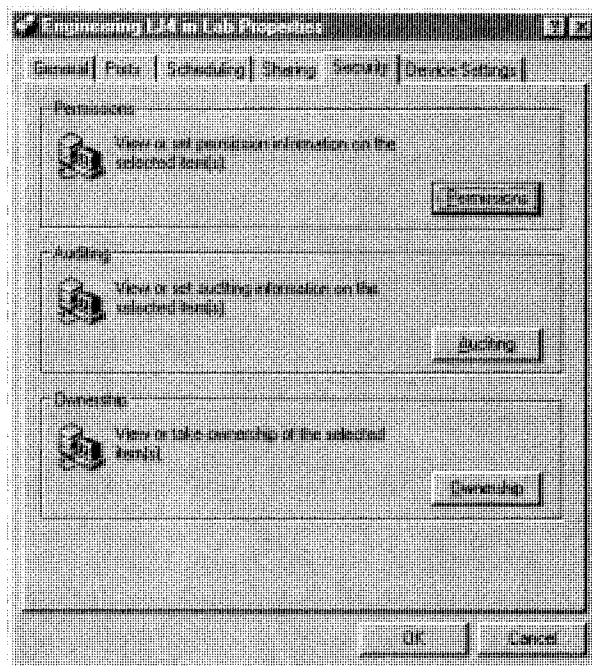
### ◆ **Full Control**

The user can make all changes to the printer, including taking ownership of the printer.

## **Viewing or Changing Printer Permissions**

The default printer security settings for Windows NT Server are designed to give everyone the ability to print, to give the owner of a print job the ability to manage that specific print job, and to allow Administrators, Print Operators, and Server Operators to set or change security settings for a printer. To set or change the printer security settings, follow these steps:

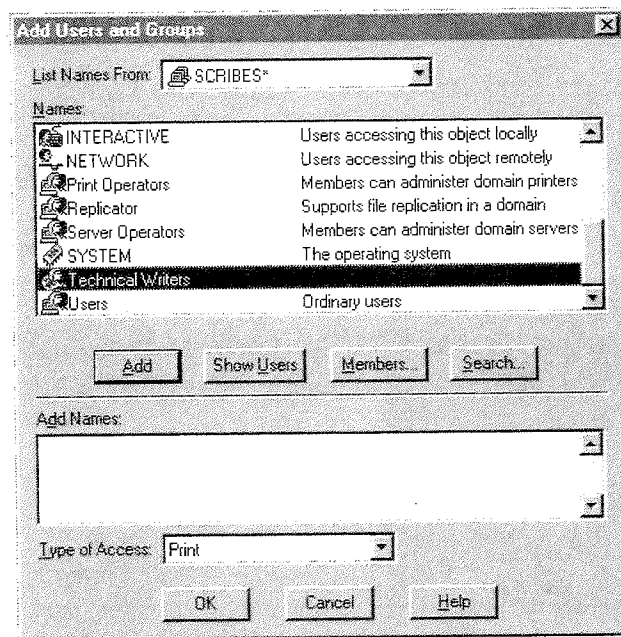
1. Choose Settings and then Printers from the submenus that open from the Start menu.
2. Right-click the printer for which you want to change the security settings. Choose Properties from the menu to bring up the printer's Properties dialog box. Click the Security tab to bring the Security page to the top, as shown in Figure 11.26.



**FIGURE 11.26**

*Printer Properties dialog box showing Security page*

3. Click Permissions to view or to modify user permissions. You'll see a dialog box like the one shown in Figure 11.17 on page 232.
4. To change printer access permission for one of the users or groups listed, select the user or group. Then select the type of access from the Type Of Access drop-down list box. Click OK, and the user or group access is changed.
5. To add a new user or group to the set of permissions, click Add. The familiar Add Users And Groups dialog box will appear (Figure 11.27). The dialog box lets you assign specific users and groups a permission level to an object. Select the user or group you want to add. (Click Show Users to include individual users in the list.) Select the type of access you want to grant to the user or group, and then click Add. When you are finished adding the users or groups you want for that permission level, click OK.



**FIGURE 11.27**

*Add Users And Groups dialog box*

## NOTE

*You can only add one type of permission at a time from the Add Users And Groups dialog box. You'll have to make repeated trips here if you want to set more than one type of permission.*



6. If you want to delete the permissions setting for a particular user or group, select the user or group and click Remove in the Printer Permissions dialog box.
7. When you are finished viewing or modifying the permissions for the printer, click OK in the Printer Permissions dialog box.

## Auditing Printer Operations

Another important aspect of printer security and administration is being able to see who has been using and, more to the point, abusing the system. Printer auditing allows you to keep track of whether a user or a group is successfully using a particular printer option.

Do you want to make sure you always know if your boss is having any difficulty using the printer? No problem; set up an audit log to record any failures from his account. Do you have a hunch that some of your users are abusing their privileges to jump their printing jobs ahead of others? Set up an audit log for the event.

What events can you audit? Pretty much what you'd expect. You can keep track of either the success or failure (or both) of the following events:

- ◆ **Print** Monitors the changes to print status, priority, and so forth
- ◆ **Full Control** Monitors the changes to the print spooler status, priority, and so forth
- ◆ **Delete** Monitors the deletions of print jobs
- ◆ **Change Permissions** Monitors the changes to permissions
- ◆ **Take Ownership** Monitors the changes to ownership of the printer

### WARNING!

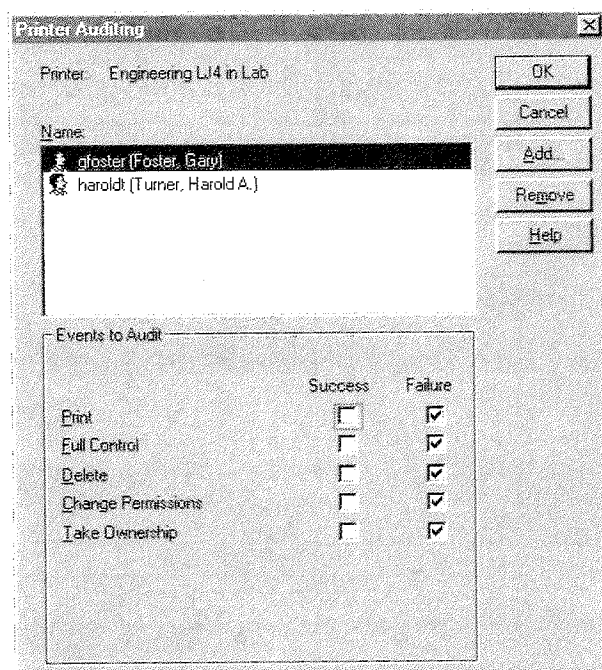
*Event logs can get very large, very quickly, on a busy system. Use printer auditing sparingly. It increases the overhead on any actions being audited because it requires the events to be written to the event log—and the logs can grow very rapidly. For more on auditing and security, see Chapter 21.*

## NOTE

*To enable logging of the events for a particular printer, you must enable auditing for the domain as a whole. You can set up the log, but nothing will actually get written to the log unless you have the auditing function enabled. See Chapter 21 for more on auditing.*

To view or change the auditing on a print queue, follow these steps:

1. Choose Settings and then Printers from the submenus that open from the Start menu.
2. Right-click the printer you want to audit or for the audit record to view. Choose Properties from the menu to bring up the printer's Properties dialog box. Click the Security tab.
3. Click Auditing to view the current auditing status of the printer. If the audit function is enabled on this printer, the window will look like the one in Figure 11.28. The default setting for printer auditing is disabled.

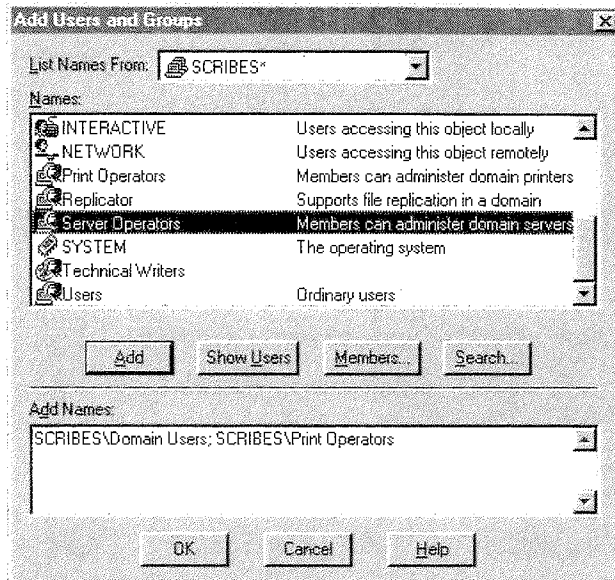


**FIGURE 11.28**

*Printer Auditing dialog box showing auditing enabled*

4. To audit an event for a user or group, click Add to bring up the standard Add Users And Groups dialog box used throughout Windows NT (Figure 11.29).

Type the name of the individual users or groups whose use of the printer you want to monitor in the Add Names text box. Click OK to return to the Printer Auditing dialog box.

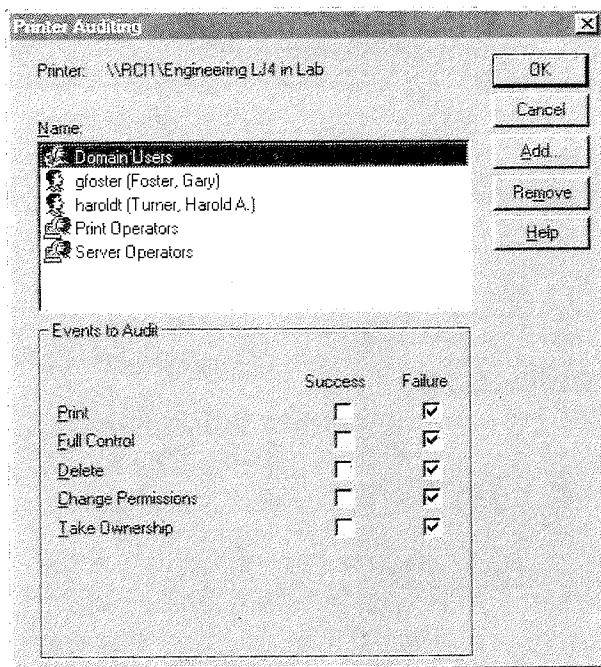


**FIGURE 11.29**

*Add Users And Groups dialog box showing group to be added to audit list*

5. The Printer Auditing dialog box will display the users or groups you have chosen to audit and also the kinds of printing events you can audit as shown in Figure 11.30 on the following page.
6. Select the user or group name, and then click the check boxes for the events you want to audit for that user or group of users. You can choose to audit both the success and the failure of any event.
7. If you decide to stop auditing a particular user or group, select the user or group name and click Remove.
8. When you're done viewing or modifying the events being audited for this printer, click OK. Then click OK again to exit the printer's Properties dialog box.

Auditing print operations can be an effective and useful tool for troubleshooting, but we find that it's a management tool best used judiciously. It's easy to get buried in so much detail that it's hard to find the root problem.



**FIGURE 11.30**

*Printer Auditing dialog box showing users and groups added to audit log*

## POINTS TO REMEMBER

- ◆ Choose your printer locations on the basis of the projected use (and users) of the printer.
- ◆ Use network or serial connections rather than parallel connections to the printer; it reduces the load on the server and increases your flexibility in being able to move printers from one location to another.
- ◆ The *physical* printer and the *logical* printer are managed separately.
- ◆ Use auditing as a troubleshooting tool, but use it sparingly.

## WHAT'S NEXT?

In Chapter 12, we'll talk about managing your disk resources—the files, the folders, and the sharing of these resources on the network.

# Microsoft Windows NT<sup>®</sup> Server 4.0

## If You Design Networks with Windows NT Server 4.0, Think of This as Your Most Important Component.

In this practical, one-volume handbook and reference, system administrators and managers will find powerful help with the networking challenges they face most often. It's all here—planning the right network design; installing, tuning, and maintaining the system; and recovering from disaster.

And unlike books that are little more than presentations of system capabilities, *RUNNING MICROSOFT WINDOWS NT SERVER 4.0* is a comprehensive road map. The emphasis is always on planning, strategy, and the needs of your organization—so you always know where you're going and why.

If you work with Windows NT Server 4.0, this book is for you. It's complete enough for the technically advanced, yet it's friendly and accessible. A quick introduction to basic concepts helps you if you're developing a Windows NT network from scratch. And hundreds of pages of practical, hands-on guidance from these experienced professionals help you implement a system that's tailored to your organization. You'll also learn how to work with Microsoft Exchange and with Internet server tools such as Microsoft Internet Information Server.

Get *RUNNING MICROSOFT WINDOWS NT SERVER 4.0*. It fits perfectly between Microsoft Windows NT Server Resource Kit and Microsoft's official multivolume training materials. And that makes *RUNNING MICROSOFT WINDOWS NT SERVER 4.0* the perfect handbook to use every day.

Windows NT/Networking



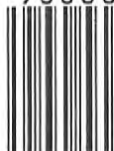
7 90145 13331 1

ISBN 1-57231-333-1



9 781572 313330

9 0000 >



U.S.A. \$39.95  
U.K. £36.99  
Canada \$54.95  
[Recommended]

[www.microsoft.com/mspress/](http://www.microsoft.com/mspress/)



**Start Faster and Go Farther with Help from Microsoft Press.**

*Whether you're a beginner, a veteran, or a power user, Microsoft Press has books to fit your needs and your style.*



### Select Editions—

*Comprehensive information in one volume*



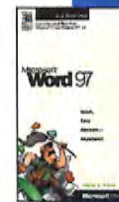
### At a Glance series—

*Easy, visual information, just when you need it*



### Step by Step series—

*Microsoft's self-paced training kits*



### Field Guides—

*Compact quick references*



### Starts Here™ CD-ROM series—

*Interactive training*

**Microsoft® Press**

# APPENDIX H



**Microsoft®**

**"The gospel of home LANs..."**

David Wall, *Amazon.com Editorial Reviews*, [www.amazon.com](http://www.amazon.com)

# **This Wired** **Home**

**SECOND EDITION**

The Microsoft® Guide to Home Networking

- Build a simple network for your home or home-based business
- Work smarter by sharing programs, printers, and an Internet account
- Play multiplayer interactive games—and take on challengers over the Net!

**Alan Neibauer**



ROKU EXH. 1002



**"A simple, understandable, and well-illustrated primer to the labyrinthine charms of home networking."**

Paul Andrews, *The Seattle Times*

## **If you can plug in a PC, you can build your own home network!**

Are there two or more computers in your house—but only one printer? Do your kids want to play games on the Internet at the same time you want to check your e-mail? Is your entire household competing for the same dial tone?

If you're running more than one PC under your roof, **THIS WIRED HOME** can show you how to build a simple network—and quickly multiply the computing power for your family or home office.

Just follow the easy step-by-step instructions for creating a secure and reliable network that can grow as your family or business grows. This how-to guide is written in plain, nontechnical language so you can put the information to work right away. You'll learn how to:

- Save time—save *money*—by sharing files, programs, printers, and other resources
- Match a networking solution to your needs—from direct PC-to-PC connections to DSL, wireless systems, and networks that run on your home electrical or phone lines
- Find the best free and low-cost connection software—including using the built-in capabilities in the Microsoft® Windows® Me, Windows 2000 Professional, Windows 98, and Windows 95 operating systems
- Hook up PCs and Macs on the same network
- Share a single phone line and Internet account
- Use your private network to send electronic sticky notes, maintain a central calendar, play multiplayer interactive games, and dial in from the road
- See what's ahead for home networking technologies and how to make wiring and setup decisions now that can evolve with the times

Like any home improvement project, all you need to build your own network is some guidance and the right tools. And with **THIS WIRED HOME**, you get the tips, tricks, and know-how to do it yourself!



### **About the Author:**

Alan Neibauer has written several best-selling computer books, including *Running Microsoft Outlook® 2000* and *Small Business Solutions for Networking*. With a master's degree from Wharton, Alan has helped organizations of all sizes network their business information systems. He's also served as chairperson for an innovative computer MIS program at the university level.

Net

THIS WIRED HOME-002

NEIBAUER A3841 Netuk Gen G010  
6309792 QP 1 10/16/01 MIGT  
703-19H 000167963

2580

90000

U.S.A. \$29.99  
U.K. £20.99  
Canada \$43.99  
[Recommended]

To learn more about  
Microsoft Press® products, visit:  
[mspress.microsoft.com](http://mspress.microsoft.com)

**Microsoft®**  
ROKU EXH. 1002

# This Wired Home

**SECOND EDITION**

The Microsoft® Guide to Home Networking

**Alan Neibauer**

**PUBLISHED BY**

Microsoft Press  
A Division of Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052-6399

Copyright © 2000 by Alan R. Neibauer

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

**Library of Congress Cataloging-in-Publication Data**

Neibauer, Alan R.

This Wired Home : The Microsoft Guide to Home Networking / Alan Neibauer.-- 2nd ed.

p. cm.

Includes index.

ISBN 0-7356-1158-0

1. Home computer networks--Amateurs' manuals. I. Title.

TK5105.75.N45 2000

004.6'8--dc21

00-057856

Printed and bound in the United States of America.

2 3 4 5 6 7 8 9 QWTQWT 5 4 3 2 1 0

Distributed in Canada by Penguin Books Canada Limited.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at [mspress.microsoft.com](http://mspress.microsoft.com). Send comments to [mspinput@microsoft.com](mailto:mspinput@microsoft.com).

FrontPage, Microsoft, Microsoft Press, MSN, NetMeeting, Outlook, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

**For Microsoft Press**

**Acquisitions Editor:** Christey Bahn

**Project Editor:** Sally Stickney

**For nSight**

**Project Manager:** Susan H. McClung

**Copy Editor:** Chrisa Hotchkiss

**Technical Editors:** Don Lesser, Mannie White,  
Doug Slaughter, Eric Brewer, Timothy Upton

You can also drag a document onto a printer icon that you've placed on the Windows desktop. To place a printer icon on the desktop, follow these steps in all versions of Windows:

1. On the Start menu, point to Settings, and then click Printers.
2. In the Printers window, right-click a printer and choose Create Shortcut from the shortcut menu.
3. When a message tells you that you can't place a shortcut in the Printers folder and asks whether you want to place the shortcut on the desktop instead, click Yes.

## Connecting Printers Directly to the Network

Because a printer that's connected to a computer on the network works only when the computer is on, you might want to use an alternative: connecting the printer directly to the network. Connecting a printer directly to the network also frees up a computer's printer port so that you can hook up an external Zip drive, scanner, or other parallel device without a conflict.

In a twisted-pair network, you use twisted-pair cable to connect a printer to the hub. In a thin Ethernet network, you use coaxial cable to connect the printer to the network interface card (NIC) of the nearest networked device. Because the printer isn't connected to the printer port of a computer, anyone on the network can access it directly as long as the printer is turned on.

The disadvantage of connecting printers directly to the network is expense. Most printers are designed only for standard parallel connections. To connect them directly to the network, you'll need to purchase either a network-ready printer or a *print server*, a device that makes your printer network-ready.

Network-ready printers have a NIC built in. They cost more than standard printers and can be a little harder to find. The print server is equipped with an Ethernet connection on one side and a parallel, or possibly serial, connection on the other.

The least expensive print servers are called *pocket servers*. About the size of a pack of cigarettes, a pocket server plugs directly into a printer's parallel port. The twisted-pair cable from the network hub or the coaxial cable from another networked device plugs into the other end of the server.

Another type of print server connects to a printer with a cable. These external servers are usually more expensive than pocket servers, but they might include additional features. Some models, for example, have more than one parallel port, allowing them to connect several printers to the network at the same time.



**Note**

For some HP LaserJet printers, you can purchase an internal print server that fits inside the printer, much the way some NICs fit inside a computer.

When selecting a print server, make sure it matches your cable type—either twisted pair or coaxial. Some print servers, but not all, can accommodate both types.

The print server must also support the protocol you're using on your network. Some print servers support only IPX/SPX; others require either TCP/IP or NetBEUI.

Finally, while most printers have a standard-sized parallel port, called a *Centronics* port, some models, such as the LaserJet 1100, have a smaller mini-Centronics port. The standard-sized connection on a pocket print server won't fit a mini-Centronics port. If you're using such a printer, you'll need an adapter for the print server.

**Note**

To install an external print server, just connect the cable that came with the printer to the server's parallel connection. Connect the network cable to the server's network connection.

**Setting Up a Pocket Print Server**

Many different models of pocket print servers exist. Although they all operate in about the same way, their setup procedures vary. Most servers are sold with software that helps them connect to the network, but the process really depends on the type of protocol the server supports.

A TCP/IP server needs to be assigned an IP address. With a Windows peer-to-peer network, you'll probably have to assign the server a static IP address that isn't used by any computer on the network. Consequently, you might have to assign static IP addresses to every computer on the network as well, rather than have Windows assign them for you. Check the literature that came with your server for step-by-step directions for assigning it an IP address.

Most manufacturers provide programs to help you through the process. The Microplex Ethernet Pocket Print Server, for example, offers two programs for configuring the print server—IPAssign and Waldo. The IPAssign program, whose main dialog box is shown in Figure 11-5, accesses the print server through the Ethernet address and assigns it an IP address of your choosing.



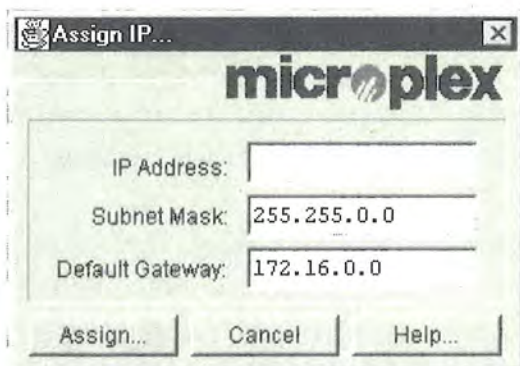
**Figure 11-5.**

*The IPAssign program for a Microplex print server assigns an IP address to the server.*

The Waldo program is Java based, so you must have the Java runtime files installed on your computer. When you run Waldo, it searches for a Microplex print server on the network and displays its Ethernet address.

Device List						
Status	Ethernet Address	IP Address	Model	Serial	Version	Location
	00:80:72:03:21:ae		M205	08622	5.7	

You can then click the Assign button in the Waldo window to associate an IP address and subnet to the Ethernet address.



Once you assign an IP address to your server, you configure Windows to communicate with the printer. You first have to associate the server with a printer port. The default port most printers use is called LPT1, the parallel connector that the printer cable plugs into. When you configured your printer, as you learned in “Installing a Printer” earlier in

this chapter, you associated the printer with the port so Windows knows where to send the information to be printed—to the LPT1 port and then out to the printer.

When you connect a print server to the network, you need to create a port with which the IP address is linked. When you associate a printer to that port, Windows sends the information to be printed through the network and the Ethernet address of the print server.

How you associate a printer port to the print server depends on the print server itself. With Microplex servers, for example, the server appears as a device in Network Neighborhood or My Network Places and has four ports associated with it. When you configure the printer, you browse to the port you want to use in the same way you would browse to a workstation, as explained in the section “Accessing a Shared Printer,” earlier in this chapter.

Other manufacturers handle port assignments differently. The pocket print servers from Axis Communications, for instance, don’t appear in Network Neighborhood or My Network Places. Instead, you use the NetPilot program to associate the server with a port, and then you use a program called Axis Print System to add the printer to Windows.

Microplex and Axis certainly aren’t the only makers of pocket print servers. Table 11-1, later in this chapter, lists other print server makes and models.

## Setting Up an External Print Server

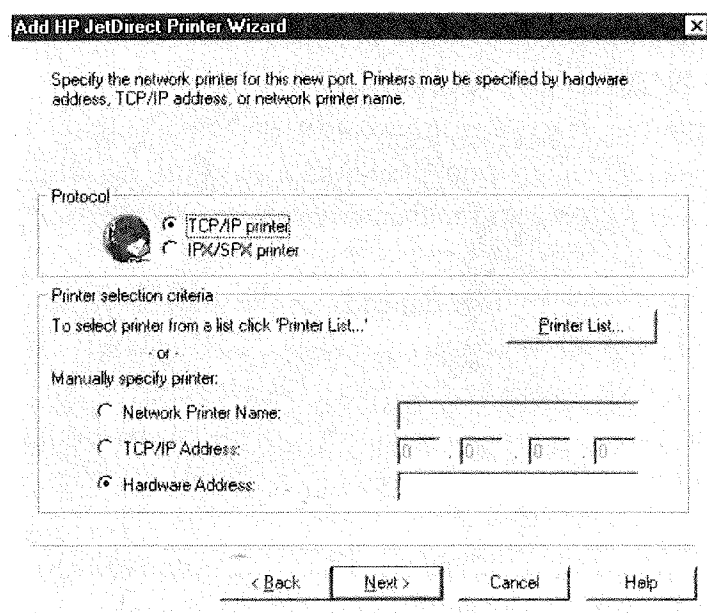
External print servers, an alternative to pocket print servers, connect to a printer by cable rather than plug directly into the printer itself. External servers work in the same way and are set up the same way as pocket print servers, although they’re more expensive than pocket print servers. Many models also come with two or more parallel connections that allow you to place multiple printers on the network so that you can use different printers for different documents.

Hewlett-Packard’s JetDirect print servers, for example, work with virtually any printer equipped with a parallel port—not just HP’s own brand. The line includes two models that have three parallel connections and a one-printer model, the 170X, that’s more suitable for home networks.

Setting up an HP print server is easy. After you connect the server both to the printer and to your network hub, you press a small button on the back of the server to print out a page of configuration information, including the electronic hardware address that is built into the device.

You then install the JetAdmin program supplied with the server and use the HP JetDirect Printer Wizard to configure the device. Figure 11-6 shows the wizard page in which you select a protocol and enter the unit’s hardware address.

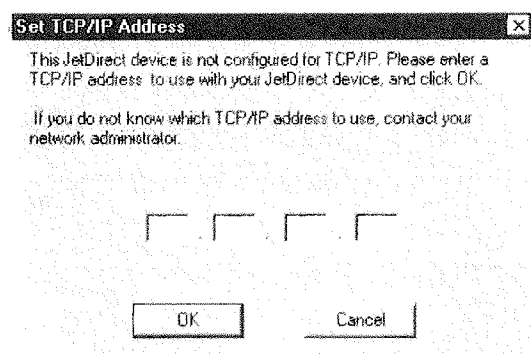




**Figure 11-6.**

*The HP JetDirect Printer Wizard prompts you to select a protocol and enter the server's hardware address.*

Using the address, JetAdmin locates the printer and displays a dialog box in which you can specify an IP address if you're using the TCP/IP protocol. After a few additional steps, JetAdmin starts the Add Printer Wizard in Windows, which opens a dialog box that prompts you to assign an IP address.



After the JetAdmin setup, you can send documents to the printer from your computer, and other network users can select the printer as their network printer and print documents even when your computer isn't on.

Many manufacturers of print servers exist, so you have plenty of choices. Table 11-1 lists print server makes and models and each manufacturer's Web address.

Table 11-1. Print Server Manufacturers and Models

Manufacturer	Models	Web site
Axis Communications	Pocket, and one-port and two-port models, some with both parallel and serial ports	<a href="http://www.axis.com/">http://www.axis.com/</a>
NETGEAR	One- and two-port models, some with built-in four-port hub	<a href="http://www.netgear.com/">http://www.netgear.com/</a>
Emulex	Pocket, and two-port and three-port models	<a href="http://www.emulex.com/">http://www.emulex.com/</a>
Extended Systems	Pocket, and one-port and two-port models, some with both parallel and serial ports	<a href="http://www.extendedsystems.com/">http://www.extendedsystems.com/</a>
Hewlett-Packard JetDirect	One-port and three-port models, external and internal, and one model for sharing over home telephone lines	<a href="http://www.hp.com/">http://www.hp.com/</a>
Intel NetPort Express	One-port and three-port models	<a href="http://www.intel.com/">http://www.intel.com/</a>
Lantronix	Pocket and external print servers, up to six-port models (four parallel and two serial)	<a href="http://www.lantronix.com/">http://www.lantronix.com/</a>
Linksys EtherFast	One-port and three-port models	<a href="http://www.linksys.com/">http://www.linksys.com/</a>
MicroPlex	Pocket, and a four-port model (two parallel and two serial)	<a href="http://www.microplex.com/">http://www.microplex.com/</a>

Sharing printers on a network can be a great time-saver and step-saver. You'll no longer need to carry a disk to another computer to print a document or carry a printer to another computer. With Windows, you don't have to purchase any additional software or hardware unless you want to connect your printer directly to the network.

Sharing files and printers isn't the only benefit of connecting computers on a network, however. You'll learn in the next chapter that you can use your network to create a family e-mail system for sending and receiving messages between family members.

# APPENDIX I

ZIFF-DAVIS  
A SOFTBANK  
company

# PC MAGAZINE

## PC Labs Tests 20 Digital Cameras Plus: 18 Digital Imaging Packages



- After Hours: 6 Encyclopedias on Disk
- 11 Servers to Let You Share Printers
- More Jim Seymour Win 98 Survival Tips



### FIRST LOOKS:

- Exclusive: 250MB Iomega Zip Drive
- 19" Flat-Screen Monitors
- Diamond Rio PMP300
- Deneba Canvas 6
- Sun's Solaris 7.0
- Intel eMail Station

WWW.PCMAG.COM

THE INDEPENDENT GUIDE TO PERSONAL COMPUTING VOL. 18 NO. 2 JANUARY 19, 1999

# FREE SOFTWARE

## ON THE WEB

THE BEST  
DOWNLOAD SITES  
FOR WORD PROCESSING,  
WEB BROWSING,  
E-MAIL, AND  
MORE

**PLUS**

Tips and  
Tricks for  
Downloading

Digitized by Google

ID\*\*\*CAR-RT SORT\*\*C006  
00093 9#451472 1Q  
LIBRARY NOV 30 99  
NAZARENE CLG BALB  
M AV #1467  
MA 02170-2905

University of Michigan--Dearborn  
Mardigian Library  
PC magazine : the independent  
guide to IBM-standard personal  
computing  
18:2  
January 1999  
Received from  
UNIVERSITY OF MICHIGAN





January 19, 1999  
Volume 18  
Number 2

## UP FRONT

From the Editor-in-Chief.....4

Pipeline.....9

Letters.....21

Trends.....28

- More choices in wireless and phone-line home networking
- What's in an Oracle appliance?
- Tuning into desktop TV
- On-screen reading that's easy on the eyes
- Roam the planet
- Chips change their spots
- The Palm goes wireless

Inside PC Labs.....29

- USB speaker technology



First Looks.....41

- 250MB Iomega Zip Drive
- 19" flat-screen monitors
- Diamond Rio PMP300
- Daneba's Canvas 6
- PC radios from ICOM, Sony, and Ten-Tec
- O'Reilly Utilities for Windows 98 Annoyances
- Microtek ImageDeck
- Painter 5.5 Web Edition
- FoneCam
- L&H iTranslator Professional Service
- ALPS MD-5000
- LMSoft Presenter 3.0
- Systat 8.0

Networking First Looks.....75

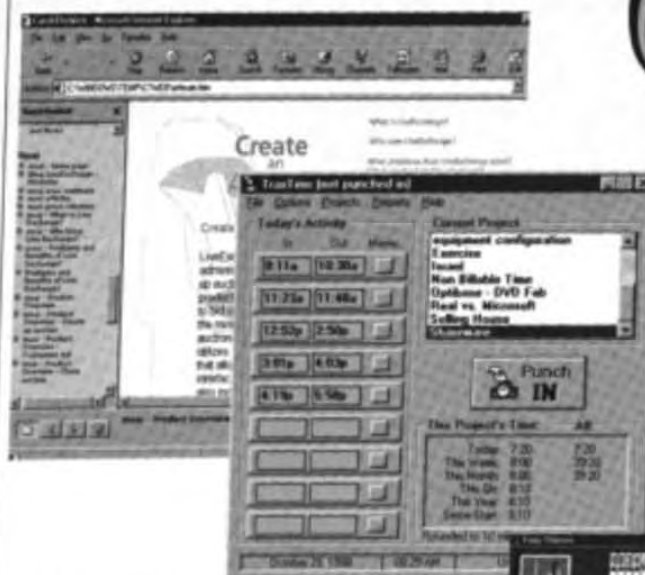
- Sun's Solaris 7.0
- Intel InBusiness eMail Station

Second Looks.....80

- Norton AntiVirus 5.0
- Dragon NaturallySpeaking

## COVER STORY

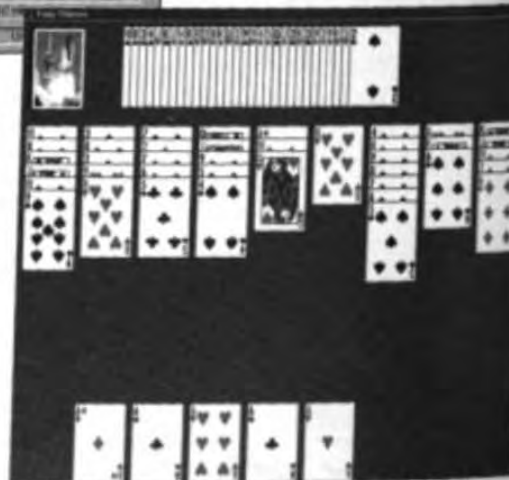
# Free Software On the Web



System Utilities.....	100
Microsoft Office Add-Ons.....	102
Internet Tools.....	102
Communications Tools.....	104
Organizational Tools.....	104
Web Development Tools.....	114
Games.....	114
Tips on Web Downloading and Storage.....	101
Where To Get It: The Sites.....	103
Essentials.....	104

BY GAIL SHAFFER

Downloading software. Besides sending e-mail, it's still our favorite thing to do online—especially if it's free or almost free! We scoured the Web and found a bunch of great programs for you that do all sorts of things. And we surveyed the best download sites so you can save some time the next time you're looking for something.....100



## NETWORKING Sharing Printers

BY STEVE RIGNEY

Still useful after all these years, print servers give you great flexibility in placing your shared printers right where you need them. They're inexpensive and easy to set up.....179



Axis Communications Inc.....	185
Castelle Inc.....	185
D-Link Systems Inc.....	186
Emulex Corp.....	186
Extended Systems Inc.....	186
Hewlett-Packard Co.....	186
Intel Corp.....	186
Lexmark International Inc.....	186
Linksys Inc.....	187
Microplex Systems Ltd.....	187
Oricom Technologies Inc.....	187
Two Ways to Print.....	187
Editors' Choice.....	185
Single-Printer Sharing.....	186
Summary of Features.....	188
Performance Tests.....	181



## FEATURES

### CONSUMER IMAGE EDITING

# Point-and-Shoot Software

BY SALLY WIENER GROTTA AND DANIEL GROTTA

You'll fall in love with your PC all over again once you start playing with digital images using one of these packages. Fix red-eye, adjust contrast and brightness—all with a click or two of the mouse—then move on to even more fun things, including making your own cards and calendars.....154



Adobe PhotoDeluxe Home Edition 3.0	156
Corel Print House Magic Deluxe 3.0	164
LivePix 2.0	167
MGI PhotoSuite II	167
Microsoft Picture It! 99	173
Ulead Photo Express 2.0	174
Editors' Choice	156
Suitability to Task	164
The Digital ShoeBox	166
Other Image Editors	174

## PERIPHERALS

# Digital Cameras

BY DANIEL GROTTA AND SALLY WIENER GROTTA

They've come a long way (in a short time), baby. The latest generation of digital cameras delivers near-35-mm quality photos in larger sizes. Models range from \$300 to \$1,200 and vary in features, so we've awarded Editors' Choices in three market segments. For all that digital cameras offer, they're worth the price.....116



Agfa ePhoto 780, ePhoto 1680	125
Casio QV-7000SX	125
Eastman Kodak DC210 Plus, DC260	125
Epson PhotoPC 700	128
Fujifilm MX-500, MX-700	128
HP PhotoSmart C30	131
Konica Q-M100V	131
Leica digilux	128
Nikon Coolpix 900s	148
Olympus D400 Zoom, D-620L	149
Ricoh RDC-4200, RDC-4300	149
Sanyo VPC-X300	150
Sony MVC-FD71, MVC-FD81	152
Toshiba PDR-M1	152
Editors' Choice	118
Performance Tests and Output Samples	133
Hitachi M2: Video, Too	148
Image Transfer: Easier than Ever	150
Summary of Features	151

Get more online at [www.pcmag.com](http://www.pcmag.com)

### Online Exclusive:

#### Photo Samples

How good do the photos taken by the digital cameras tested for this issue's story look? See for yourself at our Web site.

Plus: The Daily Download! A fresh new pick from the ZDNet Software Library every day.

### Also Currently Online:

#### 100 Desktop Fixes

Windows doesn't have to look that way. Customize it to your heart's content with this collection of hints and free utilities.

Plus:  
▶ Test your PC for Y2K compliance live online! Are you ready?

### Multimedia Extra: CD plus Web Site

#### Top Software

- ▶ 30 utilities ready to install
- ▶ Searchable back-issue database
- ▶ Web site link to more free utilities and the best downloads

Visit Extra at [www.pcmagextra.com](http://www.pcmagextra.com). To order, call 800-335-1195 in the U.S. or 303-665-8930 elsewhere.



See this issue's free utility in action at [www.pcmag.com/download](http://www.pcmag.com/download)

## COLUMNISTS

JAKE KIRCHNER	30
BILL MACHRONE	85
JOHN C. DVORAK	87
INSIDE TRACK	89
JIM SEYMOUR	93
BILL HOWARD	99

## SOLUTIONS

<b>Tutor</b>	194
Expansion buses provide vital connection to peripherals.	
<b>User to User</b>	197
Use Word to create presentations, automate Windows log-on, transpose Excel images easily, and more.	
<b>Utilities</b>	206
InCtrl4 makes keeping track of program installation easy.	
<b>Internet User</b>	212
You can get DHTML to work in both IE and Navigator.	
<b>PC Tech</b>	215
Microsoft Visual C++ 6.0 is both easier and more powerful.	

## AFTER HOURS

<b>A World View</b>	247
Disk-based encyclopedias provide useful, up-to-date information.	



<b>Shogo</b>	252
A first-person shooting game that's in a league of its own.	



### Also in This Issue:

PC Magazine Marketplace	226
Coming Up	254
Editorial Product Index	256
Advertisers' Index: Companies	257
Advertisers' Index: Products	260
Abort, Retry, Fail?	262



# Get a DOWN LOAD of this.

W  
W  
W  
.  
P  
C  
M  
A  
G  
.  
C  
O  
M

250 FREE DOWNLOADS  
(to be precise)



**EDITOR-IN-CHIEF** Michael J. Miller  
**EDITOR** Jake Kirchner  
**SENIOR EXECUTIVE EDITOR** Bill Howard  
**EXECUTIVE EDITORS** Leon Erlanger, Peter McKie, Gail Shaffer, Don Willmet  
**DIRECTOR, PC LABS** Steve Buehler  
**ART DIRECTOR** Laura Baer  
**SENIOR NETWORKING EDITOR** Frank J. Darfler, Jr.  
**SENIOR ONLINE EDITOR** John Clyman **SENIOR EDITORS** Carol Venezia (First Looks), Sebastian Rupley (West Coast)  
**MANAGING EDITOR** Paul B. Ross

**SENIOR ASSOCIATE EDITORS** Jamie M. Bales (Hardware), Carol Levin (Trends), Sharon Terdeman (Technical Columns) **ASSOCIATE EDITORS** Eileen Bien (First Looks Networking), David Lidsky (Internet), John Morris (Software), Tom Ponzo (First Looks Online), Jennifer Triverio (After Hours), Anush Yeghazarian (PCs) **ASSISTANT MANAGING EDITOR** Kim Schueler **PRODUCTION EDITOR** Monica Sirignano **COPY CHIEF** Glen Boisseau Becker **STAFF EDITORS** Mary E. Bahr, Doug Belzer, Paul Dwyer, Matthew Graven, Nancy E. Hirsch, Josh Levy, Carol A. Mangis, Michael W. Muchmore **SENIOR WRITER** Cade Metz **STAFF WRITER** Angela Hickman **SENIOR COPY EDITORS** Jennifer Gollub, Joseph N. Levine **COPY EDITORS** Michael Feist, Jeremy A. Kaplan, Barbara McGeoch, Ann Ovodow **ASSISTANT COPY EDITOR** Sarah Pike **PRODUCTION MANAGER** Patricia Perkowski **SENIOR LAYOUT EDITOR** Lillian Gaffney **LAYOUT EDITOR** Michel Ologinski **PRODUCTION SYSTEM SUPPORT ANALYST** Nancy Goodman-Slayback **LIBRARIAN** Nancy Sirapyan **LIBRARY ASSISTANT** Dolores Williams **EDITORIAL RESEARCHERS** Adam Asch, Roderick A. Beltran, Richard Brown, Sharon Nash, Angela Tuka **DIRECTOR, IS TECHNOLOGY** Craig Ellison **NETWORK SUPPORT ANALYST** Melvin Acevedo **COMMUNICATIONS MANAGER** Anita Anthony **ASSISTANT TO THE EDITOR-IN-CHIEF** Christine Curti **ASSISTANT TO THE EDITOR** Rita Aghamian **ADMINISTRATIVE ASSISTANT** Christine Okang **SYSOP, PC MAGNET** Ken Hipple

**CONTRIBUTING TECHNICAL EDITOR** Neil J. Rubenking **CONTRIBUTING EDITORS** Bill Machrone (Vice President, Technology), Greg Alwang, Douglas Boling, Padraic Boyle, Bruce Brown, Sheryl Carter, John C. Dvork, Les Freed, Daniel Grotta, Sally Wiener Grotta, David Linthicum, Edward Mendelson, Jan Ozer, Charles Petzold, Stephen W. Plain, Alfred Poor, Jeff Prosser, John R. Quain, Neil Randall, Sal Ricciardi, Steve Rigney, Winn L. Rosch, Jim Seymour, Barry Simon, Luise Simone, Craig Stinson, M. David Stone

**SENIOR ASSOCIATE ART DIRECTOR** Lisa Kocurek **ASSOCIATE ART DIRECTORS** Eileen Hanley, Michael Scowden **ASSISTANT ART DIRECTOR** Lore Morgenstern **GRAPHICS DIRECTOR** David Foster **GRAPHIC ARTIST** Mark Tynor **ART PRODUCTION MANAGER** Talor Min **CONTRIBUTING PHOTOGRAPHER** Thom O'Connor **ASSISTANT TO THE ART DIRECTOR** Frieda T. Smallwood

**TECHNICAL DIRECTORS** Ben Z. Gottasman (Software), Nick Stam (Hardware), Jeffrey G. Witt (Networking and Communications) **DIRECTOR, OPERATIONS** John R. Delaney **SENIOR PROJECT LEADERS** Richard Fisco (PCs), Jay Munro (Internet, PC Tech) **PROJECT LEADERS** Laura Cox (First Looks), Russ Iwanchuk (Networking and Communications), Diane Jecker (Software), S. Jae Yang (Hardware), Kevin Young (Networking and Communications) **PROGRAMMERS** Richard V. Dragan, Win Swarr **PRODUCT TESTING MANAGER** Charles Rodriguez **TECHNICAL ANALYSTS** Oliver Kaven, Melanio Lopez, Jacqueline Paredes, Mark Valentine, Brad Walden, Martin Wong **SUPPORT TECHNICIANS** David Carela, William Pagan, Miriam Sampson, Sunita Sawh, Jeffrey Spada **INVENTORY CONTROL MANAGER** Tom Kennedy **INVENTORY CONTROL COORDINATORS** Richard P. Bifone, Bryan Hughes **ADMINISTRATIVE ASSISTANTS** Christina M. Evelyn, Leslie Sorich

**PC MAGAZINE ONLINE**  
**MANAGING EDITOR** Tin Albano **SENIOR EDITOR** Josh Taylor **SENIOR TECHNICAL EDITOR** Thomas W. Giesel **TECHNICAL EDITOR** Webster T. Mudge **PROGRAMMER** Brian D. Buck **ASSOCIATE EDITOR** Edward Grossman **DESIGNER** Marcie Gandell **STAFF EDITORS** Jennifer L. Anderson, Troy Dreier, Richard Egan **PRODUCTION EDITOR** Matthew Slaybaugh

**PUBLISHING DIRECTOR** Nancy Newman

**NATIONAL SALES DIRECTOR** Vickie Pinsky **GROUP BUSINESS DIRECTOR** Bret Violette **ASSOCIATE BUSINESS MANAGER** Christine Holsten  
**RESEARCH DIRECTOR** Gordon Plutsky **MARKETING MANAGER** Dawn Gudelis

**SENIOR ADVERTISING PRODUCTION MANAGER** Ivis Fundichay **ADVERTISING PRODUCTION COORDINATORS** Milena Kotrch, Simone Oliver-Weekes  
**EDITORIAL PRODUCTION MANAGER** Pamela J. Berkowitz **MULTIMEDIA PRODUCTION MANAGER** Louise LaBerge

**ADVERTISING OFFICE:** One Park Ave., New York, NY 10016-5802; 800 33 MAG AD, 212-503-5100

## THE INDEPENDENT GUIDE

PC Magazine is the Independent Guide to Personal Computing. Our mission is to test and review products and report fairly and objectively on the results. Our editors do not invest in firms whose products we review, nor do we accept travel tickets or other gifts of value from such firms. Except where noted, PC Magazine reviews are of currently available products. We review products without regard to advertising or business relationships with any vendor. Softbank, the majority holder of ZD Inc., has made a number of strategic investments in high-technology companies. A list of those companies is available online at [www.pcmag.com/tag](http://www.pcmag.com/tag), and we will alert our readers to such investments whenever pertinent.

## HOW TO CONTACT THE EDITORS

We welcome comments from readers. Send them to Internet address [pcmag@zd.com](mailto:pcmag@zd.com) or to PC Magazine, One Park Ave., New York, NY 10016-5802. Please include a daytime telephone number. PC Magazine's general number is 212-503-5255. The West Coast Operations number is 850-513-8000. We cannot look up stories from past issues, recommend products, or diagnose problems with your PC by phone. For an index of past issues and a list of upcoming stories, browse [www.pcmag.com](http://www.pcmag.com).

If you are dissatisfied with a product advertised in PC Magazine and cannot resolve the problem with the vendor, write (do not call) Ellen Askin, Advertising Department, at the above address. Please include copies of your correspondence with the vendor.

## SUBSCRIPTION SERVICES

Internet: <http://subscribe.pcmag.com/service>  
U.S. and Canada: telephone, 303-665-8930; fax, 303-604-7455  
Elsewhere: telephone, 303-604-7445; fax, 303-664-0540  
Mail: PC Magazine, P.O. Box 54853, Boulder, CO 80322-4093

**Subscription rates.** The one-year rate (22 issues) is \$49.97 in the U.S., \$85.97 elsewhere. Make checks payable to PC Magazine; U.S. currency only.

**Back issues** are \$8 each in the U.S., \$10 elsewhere (subject to availability). Prepayment is required. Make checks payable to PC Magazine; U.S. currency only. Mail your requests to Back Issues, ZD Inc., P.O. Box 53131, Boulder, CO 80322-3131.

**Mailing lists.** We sometimes make lists of our customers available to makers of goods and services that may interest you. If you do not wish to receive their mailings, please write to us. Include your mailing label with any correspondence; it contains information about your subscription that will facilitate processing. Please allow 6 to 8 weeks for your first issue to arrive or for any changes in your subscription to take place.

Additional information on advertised products can be requested online at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

## PC MAGAZINE EXTRA

PC Magazine Extra, the interactive CD-ROM companion to PC Magazine, is available quarterly. To order (\$49.95 per year in the U.S., \$72 in Canada, \$99 elsewhere), please call 303-665-8930 in the U.S. or 303-604-7445 elsewhere. Or write to PC Magazine Extra, P.O. Box 54494, Boulder, CO 80322-9494.



## PC MAGAZINE ONLINE

PC Magazine is on the World Wide Web ([www.pcmag.com](http://www.pcmag.com)) and The Microsoft Network (Go to [pcmagazine](http://pcmagazine)). We operate PC MagNet, an on-line service of ZDNet, hosted by CompuServe. (For details, see the Utilities column.) PC Magazine subscribers receive free access to our online archives.



## PERMISSIONS, REPRINTS

Material in this publication may not be reproduced in any form without permission. If you want to quote from an article or use PC Magazine's logo in conjunction with an Editors' Choice designation, write Chantal Tucker or fax her at 212-503-5475; for information on reprints, please contact ZD Reprints at 800-825-4237.

The following are registered trademarks of ZD Inc.: DOSMark, NetBench, PC, PC DIRECT, PC Labs, PC MAGAZINE, PC MAGAZINE AWARD FOR TECHNICAL EXCELLENCE, PC MagNet, ServerBench, WinBench, Winstone, and ZD.

The following are trademarks of ZD Inc.: Abort, Retry, Fail?, After Hours, BusinessCard, Corporate Developer, CPUmark, EasyComputing, Extending Your Apps, Features Plus, First Looks, First Looks Plus, Lab Notes, New & Improved, OFF THE STACK, PC Bench, PC Magazine At Home, PC Magazine CD, PC MAGAZINE EDITORS' CHOICE, PC Magazine Extra, PC Magazine Marketplace, PC Solutions, PC Tech, Pipeline, Power Programming, Quick Clips, Read Only, ScreenDemos, Tech Notes, Tutor, User-to-User, WinDraw, ZDNet, and ZiffNet.

(Other trademarks and trade names used throughout the publication are the property of their respective owners.)

Copyright (c) 1998 ZD Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.



## Networking

BY  
STEVE  
RIGNEY



Most departmental and enterprise printers come with their own network connections. If your printer doesn't come ready to share, however, you're not out of luck. One solution is to connect it to the departmental file server via a standard parallel cable. But since parallel cables become unreliable after some 25 feet, you may not be able to place the printer where it is most convenient to users. You can also connect your printers to client PCs in a peer-to-peer scenario, but in order to use those printers, you'll have to make sure the PCs are turned on. And the users of those client systems may suffer mysterious pauses while the PC routes print jobs.

The best way to connect network printers is through a print server, which is a small hardware device with a network connection, par-

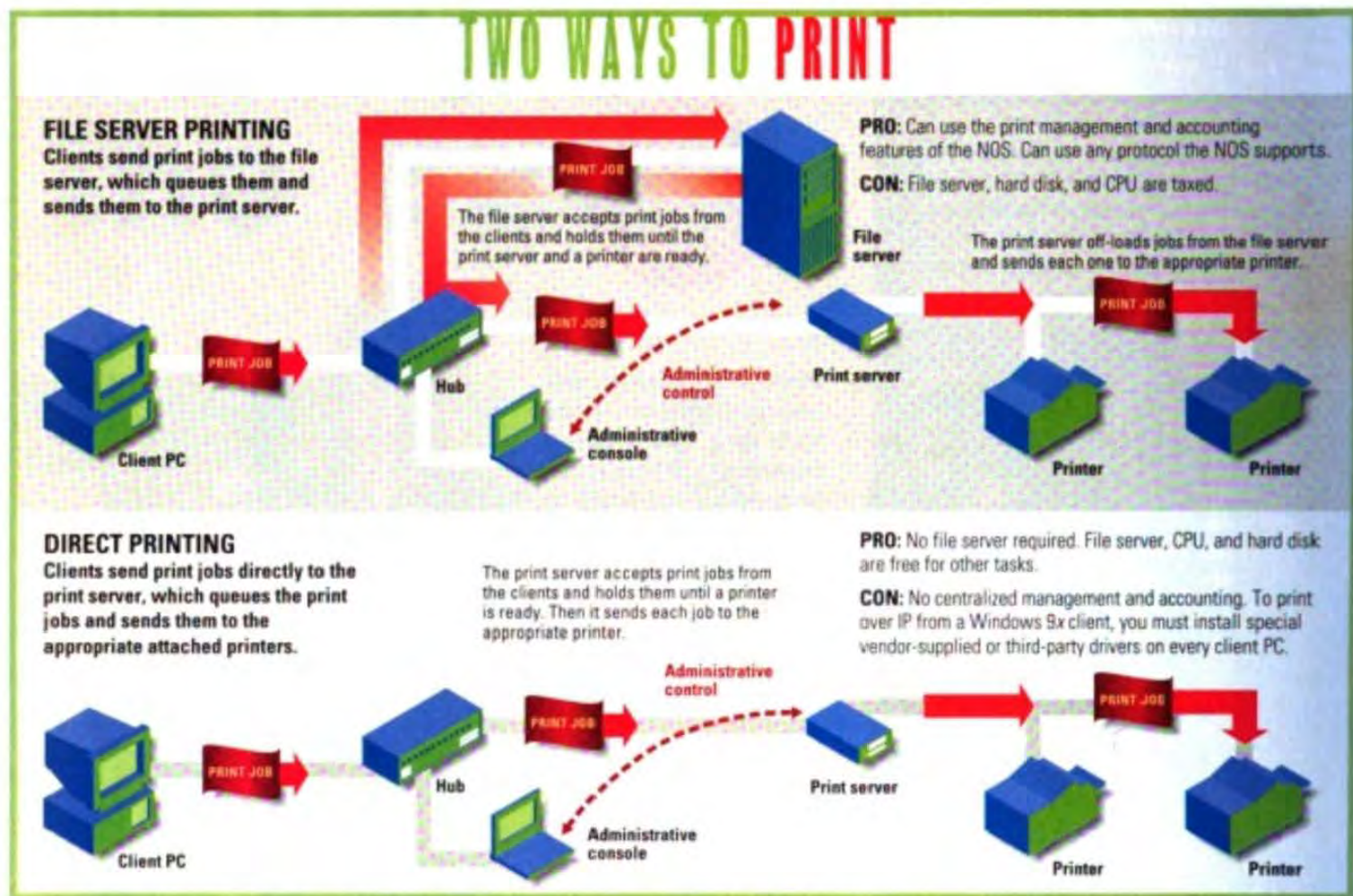
Today's print servers make sharing printers on the LAN easier and less expensive than ever before.

Axis Communications Inc. ....	185	Intel Corp. ....	189
Castelle Inc. ....	185	Lexmark International Inc. ....	189
D-Link Systems Inc. ....	186	Linksys Inc. ....	193
Emulex Corp. ....	188	Microplex Systems Ltd. ....	193
Extended Systems Inc. ....	188	Osicom Technologies Inc. ....	193
Hewlett-Packard Co. ....	189	Summary of Features ....	188

Digitized by Google

Original from  
JANUARY 1999 PC MAGAZINE 179  
UNIVERSITY OF MICHIGAN





allel and serial ports, and software that takes print jobs from clients or a server and routes them to the connected printers one at a time. Best of all, since print servers connect directly to the network, they let you place your printers just about anywhere you want.

#### PLAYERS AND PRICE

In this roundup, we look at 11 network print servers: the Axis PrintPoint 560/100 3P, Castle LANpress 3P/100, D-Link DP-300, Emulex NETQue PRO2, Extended Systems ExtendNet 100x, HP JetDirect 500X, Intel Netport-Express 10/100, Lexmark MarkNet Pro 3, Linksys EtherFast 3-Port 10/100, Microplex M202 Plus, and the Osicom NETPrint 1000 10/100.

The good news for small businesses and workgroups is that print servers have steadily come down in price since we

looked at them last year. For example, the dual-parallel-port D-Link DP-300 has a rock-bottom price of \$199.

The other good news is that we found these devices easier to set up than ever before. And most of them can be managed remotely either via Microsoft Windows software or over the Web with a standard browser.

#### WHAT TO BUY

All of the print servers we tested performed well. In fact, we found that the bottleneck in the printing process was not the print server but the printers to which they were connected. The differences among these devices lie in price, the number of printer ports they provide, whether they have Fast Ethernet or just Ethernet connections, and which operating systems and

protocols they support.

Another important difference lies in the type of remote management offered. All offer some kind of Windows-based management utility. Most now also come with Web servers and permit management over the Internet or company network via any standard Web browser. We especially liked the management packages from Extended Systems, HP, and Intel, which were thorough, well organized, and easy to use. HP's excellent JetAdmin

software lets you manage several types of SNMP devices and organize and map them logically by department, group, or capabilities.

Using HP's JetAdmin with HP printers, you also get monitoring capabilities that go beyond the typical basic errors and online/off-line notification to inform you graphically of paper jams, paper out, and the status of toner and other consumables. The same is true when you use the Lexmark print server management soft-

[www.pcmag.com](http://www.pcmag.com)

To check out this feature story and our online archive of networking coverage, visit our Web site.

**Our Contributors:** STEVE RIGNEY is a contributing editor of *PC Magazine*. JEFFREY G. WITT is the technical director for networking and communications, and RYAN SNEDEGAR is a technical analyst at PC Magazine Labs. KEVIN YOUNG was the project leader and executive editor. LEON ERLANGER was in charge of this story.



## NETWORKING Print Servers

ware with Lexmark printers. Interesting to note, the Axis and Extended Systems print servers also work with the HP Web JetAdmin utility.

The Axis PrintPoint 560/100 3P can work as a Novell Distributed Print System (NDPS) device, which lets NetWare clients search for printers on the LAN by location and capabilities (color, paper size, and so forth), as well as automatically install appropriate printer drivers.

All of the servers come with at least two parallel ports, which should be enough for most installations. If you want to connect a third or fourth printer in the same location, the Castelle, Extended Systems, HP, and Linksys products provide a third port. Most also provide serial ports, but these are no longer widely used.

Many of the units also provide 10/100 connections for both Ethernet and Fast Ethernet networks. Only the Emulex and Microplex products were limited to 10-Mbps Ethernet.

And most of the print servers will work over just about any network protocol you have, including AppleTalk, IPX, NetBEUI, and TCP/IP. But make sure you can use the network protocol you want with your NOS. For example, the D-Link DP-300 can print only over NetBEUI under Windows 95 and over IPX under NetWare. The LinkSys product works only over IPX with NetWare and doesn't work with any protocol besides IPX and TCP/IP. This may require you to reconfigure all your Windows 95 clients if they're presently configured for TCP/IP.

### PRINTING WITH A NET

A new standard in the works from the Printer Working Group of the Internet Engineering Task Force will let you print to any compliant printer on the Internet, if you have rights to it. Called the Internet Printing Protocol, it will let printers on the Internet serve a similar function that fax machines serve today. Final approval is scheduled for mid-December 1998. Only the HP JetDirect 500X supports the IPP standard today, but HP did not have a client ready for review. IBM currently

## EDITORS' CHOICE

### • HP JetDirect 500X



*All of the print servers we tested performed well and were reasonably easy to set up and configure, but the HP JetDirect 500X represents the best combination*

of functionality, management, and price.

For a list price of only \$399, you get a print server with three parallel ports, as well as support for the emerging Internet Printing Protocol and HP's networked all-in-one devices that let you scan directly to print. You also get HP's excellent JetAdmin software which goes a step beyond most print server management packages. JetAdmin lets you manage many different types of SNMP-compliant printers and other HP devices and also organize and map

them graphically by department, location, or capabilities. Combine the JetDirect with some market-leading HP printers and you get detailed information and alerts on consumables such as paper and toner.

We also liked the Intel NetPort-Express 10/100, which also has excellent setup and management software, as well as the Axis PrintPoint 560/100 3P and the Extended Systems Extend-Net 100x, which were easy to use, and can be configured with HP's JetAdmin software in addition to their own Web-based management packages.

offers an IPP prototype client driver as a free download from its Web site ([www.printers.ibm.com/ipp/ipp.html](http://www.printers.ibm.com/ipp/ipp.html)). Expect to see printer URLs on business cards in the near future.

### Axis PrintPoint 560/100 3P

\$499 list. Woburn, MA; 800-444-2947, 781-938-1188; [www.axis.com](http://www.axis.com); 900 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● Last year, we liked the PrintPoint 560/100 3P's small footprint, good per-

formance, and easy setup. This year, Axis has added a TCP/IP driver for Windows 9x-based clients and the ability to serve as a Novell Distributed Print System device.

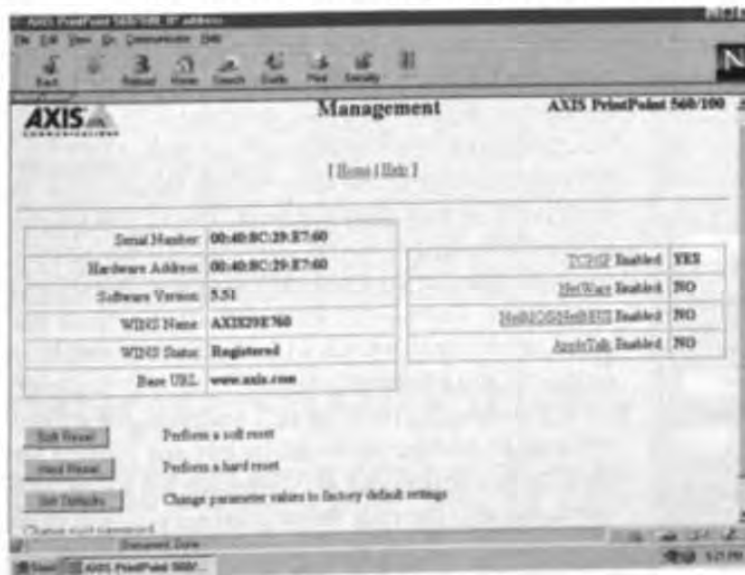
If you already have HP print servers on your network, you can use HP's popular JetAdmin software, which HP packages with its own print servers, to configure and monitor the Axis PrintPoint 560/100 3P. Axis also bundles its excellent

Windows-based NetPilot utility, which automatically looks for Axis print servers and guides you through setup. You can then use any browser to connect to the built-in HTTP server and manage the device.—Steve Rigney

### Castelle LANpress 3P/100

\$429 list. Santa Clara, CA; 800-289-7555, 408-496-0474; [www.castelle.com](http://www.castelle.com); 901 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● The most exciting feature of the Castelle LANpress 3P/100 is its Internet Printing package, which lets you produce output by sending e-mail



The Axis PrintPoint 560/100 3P has one of the better Web-based management packages we tested.

Digitized by Google

Original from  
JANUARY 19, 1999 PC MAGAZINE 105  
UNIVERSITY OF MICHIGAN

NETWORKING  
Print Servers

# SINGLE PRINTER SHOOTING

The products in our main roundup offer ports for attaching multiple printers to a network. If you have only one printer to attach, you can go with a less expensive single-port server, but otherwise, the buying criteria are the same. You want a product that accommodates your operating systems and network protocols and that is simple to set up and manage. And if you're tight on space, you'll want one with a small footprint. We looked at four of these diminutive devices from Extended Systems, I-Data, Intel, and Linksys. All provide a single parallel port and work in Windows NT and NetWare networking environments. Any of these products will do the job. Your choice comes down to features and price.

## EXTENDED SYSTEMS POCKETPRO

Though not much larger than the end of a printer cable, the Extended Systems PocketPro (\$190 street) packs plenty of features, including very good Web-based management. The parallel port of the product can attach directly to the back of your printer, and there's an RJ-45 connector for twisted pair wiring to your 10-Mbps network (but not 100 Mbps). The ExtendView software makes installation and management amazingly simple; printer-condition alerts were the easiest to set up of any product here.

(Extended Systems Inc.; 800-235-7576, 208-322-7576; [www.extendsystems.com](http://www.extendsystems.com); 904 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).)

## I-DATA EASYCOM ETH 100

Slightly smaller than a cigarette pack, the I-Data EasyCom Eth 100 (\$300 street) takes Web management to the hilt, shunning any additional software. After you plug the unit into the printer, it prints out installation instructions. As with the other



products reviewed here, you can assign IP addresses manually or via DHCP. You can set up e-mail alerts, but the instructions for doing so are sparse. (I-Data Inc.; 516-243-6600; [www.i-data.com](http://www.i-data.com); 911 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).)

## INTEL NETPORT EXPRESS 10/100

We found the installation software of the Intel NetPortExpress (\$260 street) to be

the best of the lot. The Netport, about the size of a paperback book, offers 10- and 100-Mbps connectivity, as well as the obligatory Web server for anywhere management. Besides the RJ-45 and parallel connections, the unit has a test button for troubleshooting and DIP switches if you wish to force the auto-sensing networking to either speed. For additional management, the Netport Manager software offers a drop-down menu that lets you configure alerts to work in conjunction with Intel's LANDesk Management Suite. (Intel Corp.; 800-538-3373, 503-264-7354; [www.intel.com](http://www.intel.com); 906 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).)

## LINKSYS POCKETPRINT SERVER PPS1

The least expensive product we tested, the Linksys PocketPrint Server PPS1 (\$170 street), fits in your palm and accommodates 10-Mbps networks via a RJ-45 connector, plus a BNC connector for older, thin net coaxial cabling systems. The software is Windows only; there's no Web management. A Wizard-style setup covers the monitoring bases. One minor nit: to configure the unit for peer-to-peer networking, you'll need to install proprietary software on each client. (Linksys Inc.; 800-546-5797, 949-261-1288; [www.linksys.com](http://www.linksys.com); 908 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).)—Jeffrey Witt

Castelle Internet Printing Driver Configuration (v1.1)

Internet Printing Port Name:

Internet Printer:

E-mail address of the Internet Printer:

Your E-mail information:

Mail Server Name or IP Address:

Your Internet E-mail address (e.g. username@company.com):

Retry Interval:  sec

☐ Page Notifications E-mail

Castelle's LANpress 3P/100 lets you print over the Internet via e-mail.

over the Internet to the print server, thereby providing a capability similar to a fax machine. But though you can use this feature to print over the Internet, the LANpress is not compliant with the Internet Printing Protocol, as is the HP product. Otherwise, the LANpress is a competent three-port Fast Ethernet print server that works with multiple protocols and performs well.

We liked the LANpress's bundled MPAdmin configuration utility but not that it works only over IPX. The LANpress was also the only other print server besides the D-Link DP-300 that does not include Web-based management capability.—SR

## D-Link DP-300

\$199 list. Irvine, CA; 800-326-1688, 949-455-1688; [www.dlink.com](http://www.dlink.com); 902 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● The D-Link DP-300 is the least expensive multiport print server we tested. It comes with three ports and can work with most major protocols and OSs. Unfortunately, you don't get the same protocol flexibility as with most of the products we tested. Windows 9x clients can print only using NetBEUI, and NetWare clients are limited to IPX. Only Windows NT clients can print over TCP/IP. Most of the other products in this roundup provide print redirectors that let the client OS print

Original scanned by almost any protocol the print server.



# **NETWORKING** *Print Servers*

SUMMARY OF FEATURES								
Print Servers								
	Axis PrintPoint 568/100 3P	Castelle LANpress 3P/100	D-Link DP-300	Emulex NETQue PRO2	Extended Systems ExtendNet 100x	PC MAGAZINE EDITOR'S CHOICE HP JetDirect 560X	Intel NetportExpress 10/100	Lexmark MarkNet Pro 3
List price	\$499	\$429	\$199	\$449	\$479	Ethernet 10/100TX version, \$399; Token-Ring version, \$619	\$399	\$409
Street price	\$300	\$340	\$180	\$280	\$320	Ethernet 10/100TX version, \$320; Token-Ring version, \$500	\$330	\$330
Processor type	Axis 32-bit RISC controller	Intel 186	AMD 80186	Intel 186	Intel 386EX	Custom HP ASIC	Intel 486	Hitachi SH2 27MHz
Total memory	2MB	768K	640K	1MB	2MB	4MB	3MB	2MB
Flash memory/Buffer memory	512K / 256K	512K / 256K	512K / 128K	1MB / 64K	1MB / 1MB	2MB / 2MB	1 MB / 2MB	1MB / 256K
Parallel/serial/other ports	2/1/1	3/0/0	2/1/0	2/1/0	2/1/1	3/0/1	2/1/0	2/1/0
Dimensions (HWD, in inches)	1.0 x 2.2 x 4.7	1.0 x 9.1 x 5.2	1.0 x 7.4 x 4.5	2.3 x 9.5 x 5.4	2.0 x 8.0 x 6.5	1.2 x 11.0 x 5.0	1.3 x 6.6 x 4.4	1.5 x 10.5 x 5.4
10/100 auto-sensing Ethernet connection	■	■	■	■	■	■	■	■
BootP / DHCP / DNS	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■
WINS	■	■	■	■	■	■	■	■
LPD support	■	■	■	■	■	■	■	■
<b>Network Operating Systems</b>								
Windows NT, 98, 95, and 3.x	■	■	■	■	■	■	■	■
NetWare/Unix/Macintosh	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■
<b>Network Communications Protocols</b>								
TCP/IP / IPX / NetBEUI	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■
AppleTalk	■	■	■	■	■	■	■	■
<b>Management Software</b>								
Windows NT, 98, 95, and 3.x	■	■	■	■	■	■	■	■
DOS/Unix	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■
Embedded Web server	■	■	■	■	■	■	■	■
E-mail notification of errors	■	■	■	■	■	■	■	■
Allows remote resetting of server	■	■	■	■	■	■	■	■
Includes an SNMP agent	■	■	■	■	■	■	■	■
Can be configured through a browser	■	■	■	■	■	■	■	■
<b>Service and Support</b>								
Warranty	3 years	2 years	Lifetime	2 years	5 years	3 years	3 years	3 years
Technical-support hours (eastern time)	9:00-5:15 M-F	9:00-8:00 M-F	9:00-9:00 M-F	24 hours, 7 days	7:00-6:00 M-F	24 hours, 7 days	10:00-8:00 M-F	9:00-9:00 M-F, noon-6:00 Sat.
N/A—Not applicable. The product does not have this feature.								

er can recognize. We would also like to see D-Link incorporate Web-based management into the DP-300. Still, we found this product easy to install and configure, and its performance was perfectly acceptable, though not top of the line.—SR

## **Emulex NETQue PRO2**

\$449 list. Costa Mesa, CA; 800-368-5391, 714-662-5600; [www.emulex.com](http://www.emulex.com); 903 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● The Emulex NETQue PRO2 performs reasonably well, but it's one of only two products (Microplex is the other) that can print only over a 10-Mbps connection. The box also contains a BNC connector in case you happen to need the older interface.

There's no quick-start guide; all documentation is on the bundled CD or Emulex's Web site. Luckily for us, the unit was fairly easy to install. The NETQue PRO2 includes a built-in Web server for management and configuration, but we had to download a new version of the firmware to use this feature. And documentation for the Web server interface is online only; the company plans to add this information to the CD.—SR

## **Extended Systems ExtendNet 100x**

\$479 list. Boise, ID; 800-235-7576, 208-322-7575; [www.extendsystems.com](http://www.extendsystems.com); 904 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).













● The Extended Systems ExtendNet 100x is one of the most flexible and easily

installed units we reviewed. The small device has ports for four external printers, along with an auto-sensing 10/100-Mbps Ethernet connector. Note that you can use only three of the parallel ports out of the box. The fourth can work as a serial or parallel port but only with a special cable you buy from the vendor.

We liked the ExtendNet 100x's many configuration options. You can use the bundled ExtendWeb HTML utility or the Windows-based ExtendView for NetWare and TCP/IP. We were even able to use HP's popular JetAdmin and Web JetAdmin to set up print server options. The ExtendNet 100x was also the top performer under both NetWare and Windows NT.—SR



## Print Servers

Linksys EtherFast 3-Port 10/100	Microplex M202 Plus	Osicom NETPrint 1000 10/100
\$299	\$795	\$369
\$190	N/A	\$335
AMD 156	Motorola 68340	ARM Risc Processor
896K	3MB	2MB
512K / 128K	1MB / 16K	1 MB / N/A
3/0/1	2/2/0	2/1/0
10x90x55	1.3x8.6x5.4	2.0x7.0x4.0
		
		
		
		
1 year 10:00-8:00 M-F, noon-4:00 Sat	5 years 10:30-7:30 M-F	6 years 8:30-7:00 M-F

## HP JetDirect 500X

\$399 list. Palo Alto, CA; 800-333-1917, 208-323-2551; [www.hp.com](http://www.hp.com); 905 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).



**PC**  
**MAGAZINE**  
**EDITORS' CHOICE**

Our Editors' Choice, the HP JetDirect 500X, comes with Hewlett-Packard's excellent Windows-based JetAdmin and Web-based Web JetAdmin management utilities. JetAdmin and Web JetAdmin automatically detected all of our print servers. Web JetAdmin can be used to monitor any HP or non-HP print server with its own Web server, and both utilities let you arrange and graphically map printers and other SNMP devices in logical groups by department, location, or

Digitized by Google



HP's Web JetAdmin lets you manage several SNMP devices from a single console.

capabilities. You also get some extra monitoring features when you use JetAdmin with certain HP printers, including paper and toner status.

We were impressed with the product's ability to work with HP's networked all-in-one devices, which let you scan documents directly to the print server across the network. You can also use JetAdmin to configure print servers from Axis and Extended Systems and to manage HP CD-ROM servers.

The JetDirect is also the only print server we reviewed that claimed to comply with the Internet Printing Protocol draft. HP hadn't released its IPP client software in time for testing, however. —SR

**Intel NetportExpress 10/100**

\$399 list. Hillsboro, OR; 800-538-3373, 503-264-7354; [www.intel.com](http://www.intel.com); 906 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● The Intel NetPortExpress 10/100 is inexpensive, but it offers only two parallel ports and one serial port versus three parallel ports for the similarly priced HP and Linksys products. We especially liked the NetPortExpress's compact size (1.3 by 6.6 by 4.4 inches) and thorough management options. The package comes with excellent bundled Windows software or an SNMP management package and has

all you need for configuring and monitoring the unit using a browser.

Similar to HP's JetAdmin, Intel's management software lets you monitor and group multiple print servers. Its management capabilities, however, do not extend to other Intel and non-Intel devices.

Intel claims that with a 486 processor and 2MB buffer, the Net-portExpress is the fastest print server on the market. It wasn't the top per-

former on our tests, which found printers to be the performance bottlenecks in a real-world environment, but it performed very well.—SR

## Lexmark MarkNet Pro 3

\$409 list. Lexington, KY; 800-539-6275, 606-232-2000; [www.lexmark.com](http://www.lexmark.com); 907 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink)

- This is the only product in this roundup that lets you attach a fax modem to its serial port and receive incoming faxes (you can't send a fax). Used together with Lexmark printers and the included management utilities, you can also receive detailed alerts via graphical representations of the connected printers, making the MarkNet a must in networked Lexmark printer environments. Otherwise, the Lexmark is typical of the products reviewed here, with two parallel ports and good protocol support.

We liked the detailed, multilingual documentation, but we found the bundled



The Lexmark MarkNet Pro 3 lets you receive faxes via a fax modem attached to the serial port.

Original from  
JANUARY 19, 1990 PC MAGAZINE 180  
UNIVERSITY OF MICHIGAN

NETWORKING  
Print Servers

BENCHMARK TESTS

## Print Servers



All the products we tested performed well. The printer, not the print server, typically is the performance bottleneck.

We used the fastest printers we could find—a 34-ppm Lexmark Optra S 3455 with 8MB of RAM and a 17-ppm HP LaserJet 4000 with 24MB of RAM—in order to make the print server work as hard as possible. Still, we found only a 20 percent variation between the fastest and slowest products. Buffer size, processor speed, and the Ethernet port speed had no significant effect on performance. For example, the Intel NetportExpress 10/100 featured an Intel 486 chip, and the Extended Systems ExtendNet 100x had a 386; yet they had similar output times.

Pooling the printers together in a single queue let Windows NT and NetWare send most of the print jobs to the Lexmark Optra, the faster printer. This resulted in faster printer performance than when we divided the print jobs into two queues, which used the slower printer, the HP LaserJet 4000, more often. We were forced to print results from two queues in Windows NT, however, because single-queued results varied significantly from one test to another. The Microplex M202 Plus in particular had problems handling Windows NT, at first taking over an hour to print using two print queues. Microplex suggested we abandon its driver and try the generic Windows LPR ports instead, which remedied the problem.—*Analysis written by Martin Wong*

### How We Tested

We tested the print servers using a variety of test files, including 6-page Excel, 5-page Word, 35-page Word, 5-page PDF, and 10MB TIFF files. We tested under Novell's IntranetWare 4.11 with Support Pack 5B, and Windows NT with Service Pack 3. We installed the NOSs on identical Compaq 1600R servers with dual 266-MHz Pentium II CPUs and 512MB of RAM. Our clients were eight Dell OptiPlex GXas with Pentium II/233-MHz processors and

### PRINT SERVER THROUGHPUT

Low scores are best. Minutes: seconds.  
Bold type denotes first place within each category.  
PC denotes Editors' Choice.

NETWARE 4.11	
Axis PrintPoint 560/100 3P	5:05
Castelle LANpress 3P/100	5:34
D-Link DP-300	4:51
Emulex NETQue PRO2	5:53
Extended Systems ExtendNet 100x	4:42
HP JetDirect 500X	5:00
Intel NetportExpress 10/100	5:05
Lexmark MarkNet Pro 3	4:58
Linksys EtherFast 3-Port 10/100	5:35
Microplex M202 Plus	5:14
Osicom NETPrint 1000 10/100	4:50

WINDOWS NT SERVER 4.0	
Axis PrintPoint 560/100 3P	6:47
Castelle LANpress 3P/100	6:44
D-Link DP-300	6:36
Emulex NETQue PRO2	6:40
Extended Systems ExtendNet 100x	6:19
HP JetDirect 500X	6:37
Intel NetportExpress 10/100	6:43
Lexmark MarkNet Pro 3	6:35
Linksys EtherFast 3-Port 10/100	6:48
Microplex M202 Plus	6:41
Osicom NETPrint 1000 10/100	6:44

32MB of RAM, eight Dell Dimension XPS Pro200ns with Pentium Pro/200 processors and 32MB of RAM, and eight Dell Dimension XPS P166s with Pentium/166 processors and 32MB of RAM, each running Windows 95. The PCs were connected by SynOptics 28115 Fast Ethernet switches. A connection through a 3Com Superstack II Hub 100TX let us capture network data.

For NetWare, we printed using NDS in Pconsole mode. We used TCP/IP native drivers if available; otherwise, we used LPR. The printers on the test-bed were a 34-ppm Lexmark Optra S 3455 with 8MB of RAM and a 17-ppm HP LaserJet 4000 with 24MB of RAM.

When we printed to two queues, we used each printer's proprietary driver, but when we pooled the printers into one queue, we used the standard HP PCL 5 driver. In Windows NT, we were able to pause the queue and load up all of the print jobs. We measured the time it took from removing the print-queue pause to finishing the final output page on the last printer finished. For NetWare, we started timing when the clients clicked the Print button and ended with the completion of the last page. For all of the tests, we used a protocol analyzer to capture the network traffic between the print server and the NOS client.

No Monthly  
Payments

freewwwweb

ONE  
TIME  
FEE  
\$99.95

Internet Access

E-Mail/NewsGroups

Nationwide Access

Freewwwweb is the

Internet Access

provider who doesn't

make you pay

month after month!

Call or Download Now

1.888.970.FREE

www.freewwwweb.net

Original from

Digitized by Google

UNIVERSITY OF MICHIGAN



**NETWORKING**  
*Print Servers*

Windows- and Web-based management software a little less easy to use than HP's JetAdmin.—SR

### Linksys EtherFast 3-Port 10/100

\$299 list. Irvine, CA; 800-546-5797, 949-261-1288; [www.linksys.com](http://www.linksys.com); 908 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● At \$299 list (\$190 street), the Linksys EtherFast 3-Port 10/100 is the least expensive print server we tested that offers three parallel ports and a 10/100-Mbps connection. Unfortunately, the EtherFast works only over IPX and TCP/IP, and it lacks browser-based management. Unless you're looking to save a quick \$100, you'll find better flexibility in products from HP, Intel, or Extended Systems.

The bundled Bi-Admin program is not as detailed as those of other packages, but it let us monitor multiple devices and configure our EtherFast as both a NetWare and a Windows NT-based print server. Bi-Admin also automatically detects any EtherFast devices on your network without any prior configuration. Like the D-Link DP-300, the EtherFast works only

with IPX for NetWare clients, but unlike its competitor, the EtherFast lets you print from Windows 9x using TCP/IP.—SR

### Microplex M202 Plus

\$795 list. Burnaby, B.C., Canada; 604-444-4232, 800-665-7798; [www.microplex.com](http://www.microplex.com); 909 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● The Microplex M202 Plus is the only product that shipped with fiber-optic connectors, yet it's also one of only two products that can only connect to the network at 10-Mbps Ethernet. And if you opt for an AUI connector instead of fiber, the price is still a whopping \$575 (list)—far higher than any other unit in this roundup. Unfortunately, the price is not justified by features.

We ran into some performance problems when using the bundled Windows NT driver. Microplex recommended that we use the LPR printer driver with Windows NT, which brought performance in line with the other products we tested. The included configuration utility is easy to use but not on a par with that of the HP or Intel products.—Ryan Snedegar

### Osicom NETPrint 1000 10/100

\$369 list. Waltham, MA; 800-243-2333, 781-647-1234; [www.osicom.com](http://www.osicom.com); 910 at [www.pcmag.com/infolink](http://www.pcmag.com/infolink).

● Though not a standout, the Osicom NETPrint 1000 10/100 works as advertised. The setup utility doesn't automate NetWare configuration as much as most of the other products we tested, but setup is not overly complicated. The Osicom is the only product here with no buffer, so you need to print via a file server.

Osicom comes with browser-based management and includes an IPX-based browser for networks that don't use IP. At 100 Mps, the NETPrint unit we received could not use DHCP or BootP for an IP address assignment, but Osicom claims the problem will be fixed by the time you read this. The product comes with only a single LED to display status; we prefer the multiple LEDs you get with the Lexmark and Microplex products.

The NETPrint performed well, particularly with NetWare.—RS

## The End of Networking As We Know It...

DUAL-SPEED HUBS 8 AND 16 PORTS  
WITH BUILT-IN SWITCH PORTS

UNICOM has developed hubs that combine either an 8 or 16 port dual-speed hub with either a 1, or 2 port switch for half or full duplex operation.


The bottom line...  
**YOU SAVE BIG!**

Now you don't have to buy an extra switch to expand your network. With UNICOM's dual-speed hubs, you can enjoy the benefits of an 8 or 16 port hub with built-in switching capabilities for 10Base-T and 100Base-TX networking. The 16-port hub has a built-in module bay for greater flexibility allowing the installation of an additional 10Base-T/100Base-TX or 100Base-FX switch module. These dual-speed hubs from UNICOM also allow you to extend the distance between hub connections by up to 100 meters (using the extra switch ports).

UNICOM is dedicated to bringing premium quality network hardware at down-to-earth prices.

Ask your dealer for this convenient new product. Or call  
**1-800-346-6668**  
Ask for Operator 106

**UNICOM**  
City of Industry, CA  
[WWW.UNICOMLINK.COM](http://WWW.UNICOMLINK.COM)



# APPENDIX J



# 100%

ONE HUNDRED PERCENT  
COMPREHENSIVE  
AUTHORITATIVE  
WHAT YOU NEED  
ONE HUNDRED PERCENT

**Create** your own  
Windows network

**Set up** client  
services, protocols,  
and security

**Troubleshoot**  
and fix network  
problems quickly



# Home Networking Bible

Your Complete  
Resource —  
Planning, Set Up,  
Troubleshooting and More

**Sue Plumley**

ROKU EXH. 1002



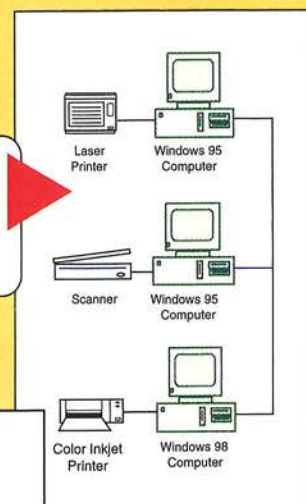
# If network administrators can do it, you can do it too . . .

Whether you're connecting two computers at home or ten PCs at a small office, this all-in-one reference covers the hardware, software, and other resources you'll need to create and manage your own peer-to-peer or client/server network. In straightforward, real-world language, expert consultant and author Sue Plumley explains the fundamentals of networking — and then shows you how to optimize performance, share files, manage your print queue, make backups, and more. *Home Networking Bible* is all you need to get connected and keep everything up and running!

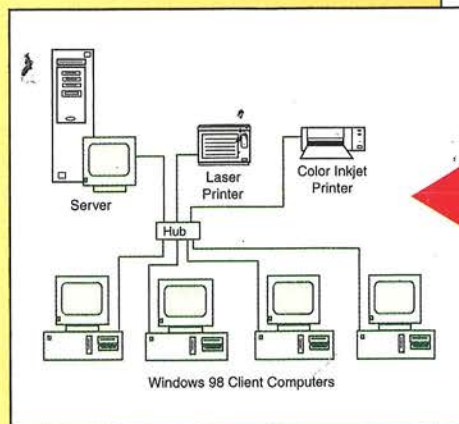
## Inside, you'll find complete coverage of home networking

- Get up to speed on your networking hardware and software options
- Learn about cabling and network connections, including new developments using existing phone wiring
- Plan and set up directory structure and file naming policies for your network
- Install network printers, scanners, CD-ROM drives, Zip drives, and more
- Share files, disk drives, printers, and other resources
- Connect multiple users to the Internet using one Internet account
- Send e-mail over your network or the Internet
- Add a Mac to your PC network
- Educate other users on the proper use of the network
- Troubleshoot problems — from connections, printing, and speed to passwords and user IDs

Set up a simple peer-to-peer network quickly and easily



Also learn about more complicated client/server networks . . . perfect for a small home office



Register to win!

[my2cents.idgbooks.com](http://my2cents.idgbooks.com)



[www.idgbooks.com](http://www.idgbooks.com)

### Reader Level:

Beginning to Advanced

**\$34.99** USA

**\$52.99** Canada

**£33.99** UK

### Shelving Category:

PCs/Home Networking



7 85555 01213 4

The IDG Books Worldwide logo is a registered trademark under exclusive license to IDG Books Worldwide, Inc., from International Data Group, Inc. All other trademarks are the property of their respective owners.

IDG Books Worldwide, Inc.  
An International Data Group Company  
Foster City, CA 94404

Printed in the USA

ISBN 0-7645-3399-1

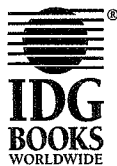


9 780764 533990

ROKU EXH 1002

# **Home Networking Bible**

**Sue Plumley**



IDG Books Worldwide, Inc.  
An International Data Group Company

Foster City, CA ♦ Chicago, IL ♦ Indianapolis, IN ♦ New York, NY

## Home Networking Bible

Published by

**IDG Books Worldwide, Inc.**

An International Data Group Company

919 E. Hillsdale Blvd., Suite 400

Foster City, CA 94404

[www.idgbooks.com](http://www.idgbooks.com) (IDG Books Worldwide Web site)

Copyright © 1999 IDG Books Worldwide, Inc. All rights reserved. No part of this book, including interior design, cover design, and icons, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording, or otherwise) without the prior written permission of the publisher.

Library of Congress Card Number: 99-066522

ISBN: 0-7645-3399-1

Printed in the United States of America

10 9 8 7 6 5 4 3

1B/RU/RQ/ZZ/FC

Distributed in the United States by IDG Books Worldwide, Inc.

Distributed by CDG Books Canada Inc. for Canada; by Transworld Publishers Limited in the United Kingdom; by IDG Norge Books for Norway; by IDG Sweden Books for Sweden; by IDG Books Australia Publishing Corporation Pty. Ltd. for Australia and New Zealand; by TransQuest Publishers Pte Ltd. for Singapore, Malaysia, Thailand, Indonesia, and Hong Kong; by Gotop Information Inc. for Taiwan; by ICG Muse, Inc. for Japan; by Intersoft for South Africa; by Eyrolles for France; by International Thomson Publishing for Germany, Austria and Switzerland; by Distribuidora Cuspidé for Argentina; by LR International for Brazil; by Galileo Libros for Chile; by Ediciones ZETA S.C.R. Ltda. for Peru; by WS Computer Publishing Corporation, Inc., for the Philippines; by Contemporanea de Ediciones for Venezuela; by Express Computer Distributors for the Caribbean and West Indies; by Micronesia Media Distributor, Inc. for Micronesia; by Chips

Computadoras S.A. de C.V. for Mexico; by Editorial Norma de Panama S.A. for Panama; by American Bookshops for Finland.

For general information on IDG Books Worldwide's books in the U.S., please call our Consumer Customer Service department at 800-762-2974. For reseller information, including discounts and premium sales, please call our Reseller Customer Service department at 800-434-3422.

For information on where to purchase IDG Books Worldwide's books outside the U.S., please contact our International Sales department at 317-596-5530 or fax 317-596-5692.

For consumer information on foreign language translations, please contact our Customer Service department at 800-434-3422, fax 317-596-5692, or e-mail [rights@idgbooks.com](mailto:rights@idgbooks.com).

For information on licensing foreign or domestic rights, please phone +1-650-655-3109.

For sales inquiries and special prices for bulk quantities, please contact our Sales department at 650-655-3200 or write to the address above.

For information on using IDG Books Worldwide's books in the classroom or for ordering examination copies, please contact our Educational Sales department at 800-434-2086 or fax 317-596-5499.

For press review copies, author interviews, or other publicity information, please contact our Public Relations department at 650-655-3000 or fax 650-655-3299.

For authorization to photocopy items for corporate, personal, or educational use, please contact Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, or fax 978-750-4470.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND AUTHOR HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK. THE PUBLISHER AND AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS BOOK AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THE DESCRIPTIONS CONTAINED IN THIS PARAGRAPH. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. THE ACCURACY AND COMPLETENESS OF THE INFORMATION PROVIDED HEREIN AND THE OPINIONS STATED HEREIN ARE NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULTS, AND THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY INDIVIDUAL. NEITHER THE PUBLISHER NOR AUTHOR SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.**

**Trademarks:** All brand names and product names used in this book are trade names, service marks, trademarks, or registered trademarks of their respective owners. IDG Books Worldwide is not associated with any product or vendor mentioned in this book.



is a registered trademark or trademark under exclusive license to IDG Books Worldwide, Inc. from International Data Group, Inc. in the United States and/or other countries.



## Sharing Printers and Other Peripherals

You can share many peripherals on both peer-to-peer and client/server networks. Peripherals include printers, scanners, modems, and other devices. Some peripherals require special software to make them work over a network; other peripherals require special hardware or features to make them networkable. Some peripherals require nothing but the share designation.

Sharing peripherals over a peer-to-peer network is different from sharing them over a client/server network. In a client/server network, the network operating system usually has tools and features that enable and manage the shared device. When you're sharing printers with NT Server, for example, the network operating system acts as a print server. The print server distributes the various print jobs to the appropriate printers and enables the network administrator to manage the print jobs that clients send to the server.

In a peer-to-peer network, you may not need extra tools to manage the sharing of peripherals, but if you do, you need to purchase a third-party program to enable sharing and device management.

### Sharing printers

In Windows 95 and 98, you can easily share any printer attached to a computer on the network. Sharing a printer is similar to sharing a drive or folder. You designate the printer as shared and assign it a share name. You also can set a password on the shared device, if you want. Only someone who knows the password can use the printer. In general, however, you'll share all printers on the network with everyone else.

**Tip**



You may want to limit sharing a printer that is especially expensive or difficult to use, such as a color laser printer or color inkjet printer. To limit sharing, either you cannot share the printer or you can share it with a password.

In addition to designating a printer as shared, other users on the network must install your printer's driver to their computers before they can access the printer. The printer's driver is a program that enables the computer to communicate with the printer.

**Cross-Reference**

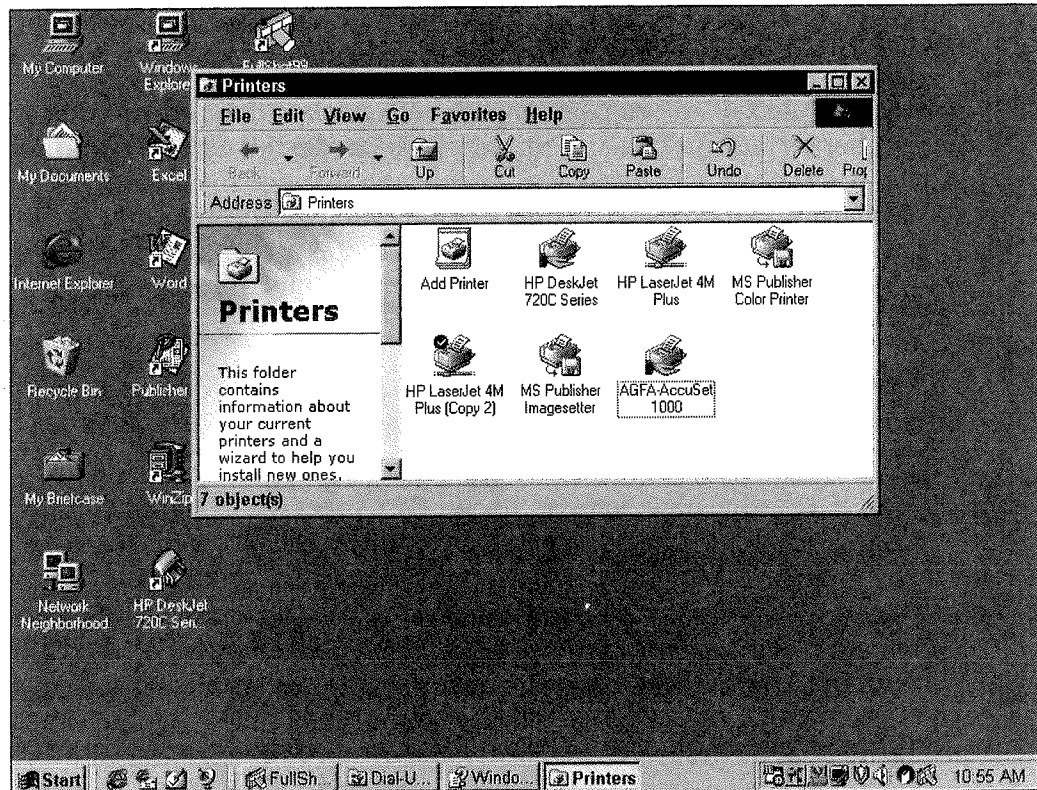
For more information about network printing, see Chapter 14, "Printing on a Network."

### Designating a printer as shared

Before designating your printer as shared, you must install it on your computer. You install the printer as a local printer, just as you would if you planned to use it exclusively with your computer.

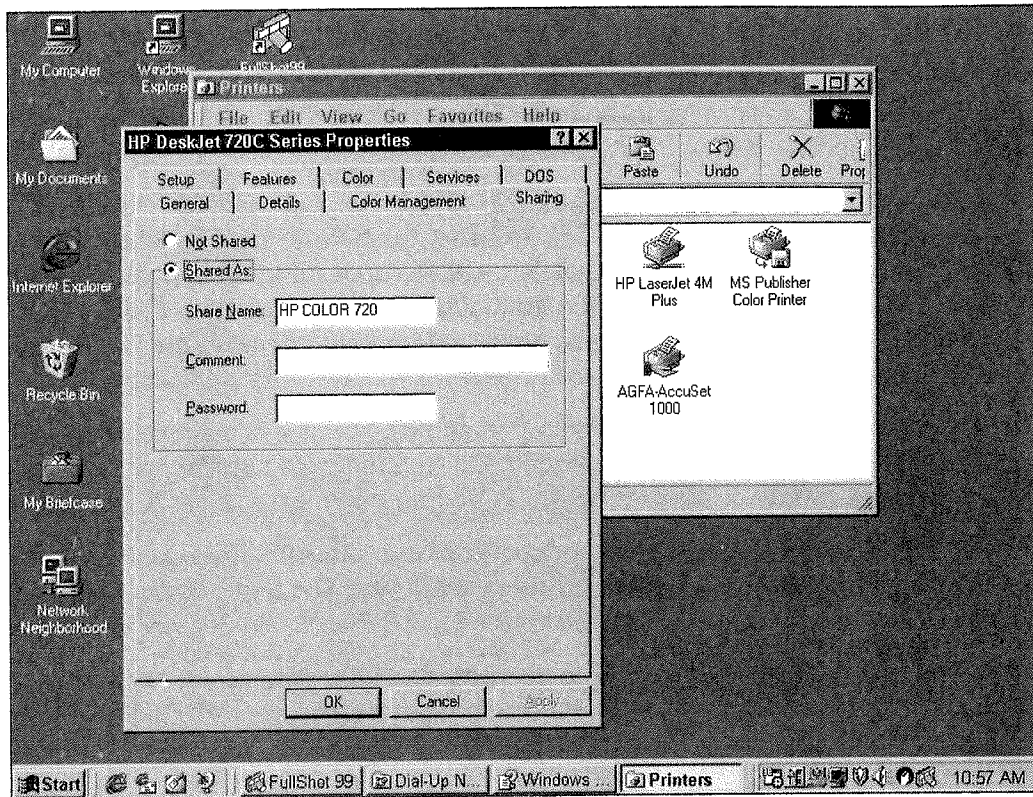
Next, you designate the printer as shared by following these steps:

1. Choose Start ⇨ Settings ⇨ Printers. The Printers dialog box appears, as shown in Figure 11-11.



**Figure 11-11:** Locate the printer to be shared.

2. Right-click the printer's icon and then choose Sharing from the quick menu. The printer's Properties dialog box appears with the Sharing tab displayed.
3. Choose the Shared As option to display the share options, as shown in Figure 11-12.
4. You can either accept the suggested share name or enter a new one. The share name is the name that appears in the Network Neighborhood.
5. Optionally, you can enter a comment about the printer. The comment also appears in the Network Neighborhood.
6. If you want to control the use of the printer, enter a password in the appropriate text box.
7. Click OK to accept the changes and close the printer's Properties dialog box.



**Figure 11-12:** Share the printer by assigning it a share name.

You can view a printer on the network via the Network Neighborhood, the Windows Explorer, or My Computer. For information about finding a printer on the network and installing the driver, see Chapter 14.

### Other methods of sharing printers

When you share a printer that's directly attached to a PC, that PC must remain on for others to print to the printer. Using a device called a print server, you can save the hassle of turning the computer on and going to that printer each time you print a page.

A *print server* manages the printing for all users on a network. It receives all requests for print jobs sent by the networked PCs, places the jobs in a queue to wait their turn, and then routes the job to available printers attached to the server.

#### Tip



A print server is an excellent idea for small networks. If you only have one printer and not many people who need to print, you probably don't need one. If several users print most of the day, however, a print server can help divide the print load and speed the jobs along.

Several types of devices are available that you can purchase, such as an Axis 540+ or the Castle LANpress 1P/10BT, that can handle the job on a small network. Prices range from \$130 to \$250. For more information about print servers, see Chapter 14.

## HP JetDirect and JetSend

Hewlett-Packard (HP) offers many tools and utilities for sharing peripherals over a network. JetDirect and JetSend are two of those tools.

The JetDirect switch box is perfect for the small network. HP calls the JetDirect Auto Switches *intelligent* switch boxes that enable users to share a parallel-based peripheral, such as a scanner or printer. A *switch box* is a set of circuits into which you plug two or more devices. A simple switch knob on the front of the box enables you to change back and forth between computers; other switch boxes automatically make the switches. The JetDirect Auto Switch works without a hub or network management software.

The JetDirect Auto Switch 2:1 connects two PCs and one printer or scanner, or one PC to both a printer and scanner. The price is around \$90. The JetDirect Auto Switch 4:1 connects four PCs to a single printer or scanner or one PC to four peripherals. It costs around \$100.

HP also has come up with the JetSend communication protocol. JetSend enables the user to enter the address of a JetSend-enabled receiving device. The two devices then connect and communicate automatically, sending information back and forth.

HP's Network ScanJet 5 scanners and HP's new LaserJet 4000 printers are JetSend-enabled. The ScanJet scanner, for example, can send information directly to any JetSend-enabled receiving device anywhere in the world. The scanner communicates with the receiving device, and the information is sent to the device, which then prints or displays the information.

HP's plan for JetSend is to integrate it into many HP- and non-HP-manufactured devices, such as PCs, CD-ROM or DVD discs, TVs, cameras, projectors, handheld computers, fax machines, white boards (electronic bulletin boards on which you can write and take notes), and so on. Although the technology is expensive at this time (\$2,999 to \$3,999 for the scanner), HP hopes to lower prices and extend availability in the near future.

## Sharing a modem

You probably want to share an Internet connection over your network. You also might want to share faxing capability. To share either an Internet connection or fax services, you need to share a modem. Modem-sharing software is relatively inexpensive, but you need to remember that the PC with the modem is going to take a dive in performance whenever the Internet connection is active.

You can share modems whether your network is of the peer-to-peer or client/server variety. For a peer-to-peer network, use inexpensive modem-sharing software. For a client/server network, use the more complex and expensive *modem pool* (a device that attaches multiple modems and then designates which call uses which modem) or other devices. Other devices include cable modems and ISDN modems, which are too expensive for normal home use. A *cable modem* is a device that enables you attach to the Internet through your television cable; *ISDN* (short for *Integrated Services Digital Network*) is a digital data transmission device connected to an ISDN line.

2. Click the Capture Printer Port button. The Capture Printer Port dialog box appears, as shown in Figure 14-13.

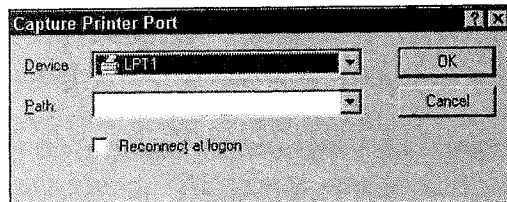


Figure 14-13: Capture a printer port.

3. In the Device drop-down list, choose the LPT port you want to assign to the capture.
4. In the Path text box, type the network path to the printer.
5. If the program is one you use often and you want to reconnect this capture each time you log on to the network, check the Reconnect at logon check box.
6. Click OK and then click OK again to close the printer's Properties dialog box.

## Managing Peer-to-Peer Network Printing

When you have a *local* printer attached to your computer, you control the printing. You can pause the printing of all documents or pause the printing of only one document. You can rearrange the order in which the documents print. You also can cancel the printing of a document completely.

When you print to a *network* printer, you cannot control any of these elements. All you can do is send your job to the printer and relinquish complete control.

To open the print queue (a temporary list of documents waiting to be printed by the network printer), open the Printers folder window and double-click the print icon. The queue appears.

### Note

If you use a client/server network with Windows 95 or 98 as your server, you can attach the printer to the server computer for complete control over the printing process. If you use a client/server network operating system, you need to read the NOS documentation for information about controlling the printer and print queues.

## Understanding the print queue

The *print queue* is an area in which all print jobs for a specific printer wait to be printed. The print queue holds the jobs so that you can get on with your work in Windows. As the printer becomes available to print a job, the queue sends them along, one by one.



## Print Servers

A print server can be the software included with a network operating system to control printers, printer drivers, and the print queue. NT Server, for example, includes a print server applet that enables you to control the printers attached to the server. A print server also can be a device that attaches to the network. This device provides shared network access to the printers.

You attach the latter kind of print server (usually a small box with ports for plugging in printers) to the network and then attach multiple printers to the device. When a user sends a print job to the printer, the job stops first at the print server, which manages the printers attached to it so that no one printer becomes overwhelmed or overworked.

Most of the advantages to using a print server are to businesses and corporations. Home networks usually don't need to use a print server. If you have a small business that you expect to grow, however, you might consider attaching one to your network.

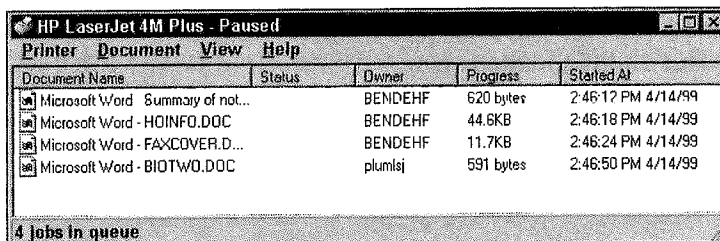
Generally, printers attached to a print server are in a central location for easy retrieval of print jobs. Printers attached to a print server can process jobs on many different operating systems or networks. Also, print servers are easier to administer than the print server software in a network operating system.

Usually, the print queue passes documents quickly to the printer. If several jobs are waiting in the queue, or if there's a problem with the printer (out of paper, paper jam, or such), the jobs wait in the queue until they can print. You also can pause the print queue to hold jobs, such as when you want to load special paper in the printer.

### Note

The print queue is the list of jobs waiting to be printed, but it is the *print spooler* (Simultaneous Peripheral Operation On Line) that receives, processes, and schedules the jobs in the queue. Each print job is saved in a separate file and printed in turn when the printer becomes free.

Figure 14-14 illustrates a print queue that is paused so that you can see the jobs waiting to be printed. Note that three print jobs belong to one user and one job belongs to a second user.



Document Name	Status	Owner	Progress	Started At
Microsoft Word - Summary of not...	Paused	BENDEHF	620 bytes	2:46:12 PM 4/14/99
Microsoft Word - HOINFO.DOC	Paused	BENDEHF	44.6KB	2:46:18 PM 4/14/99
Microsoft Word - FAXCOVER.D...	Paused	BENDEHF	11.7KB	2:46:24 PM 4/14/99
Microsoft Word - BIOTWQ.DOC	Paused	plumlj	591 bytes	2:46:50 PM 4/14/99

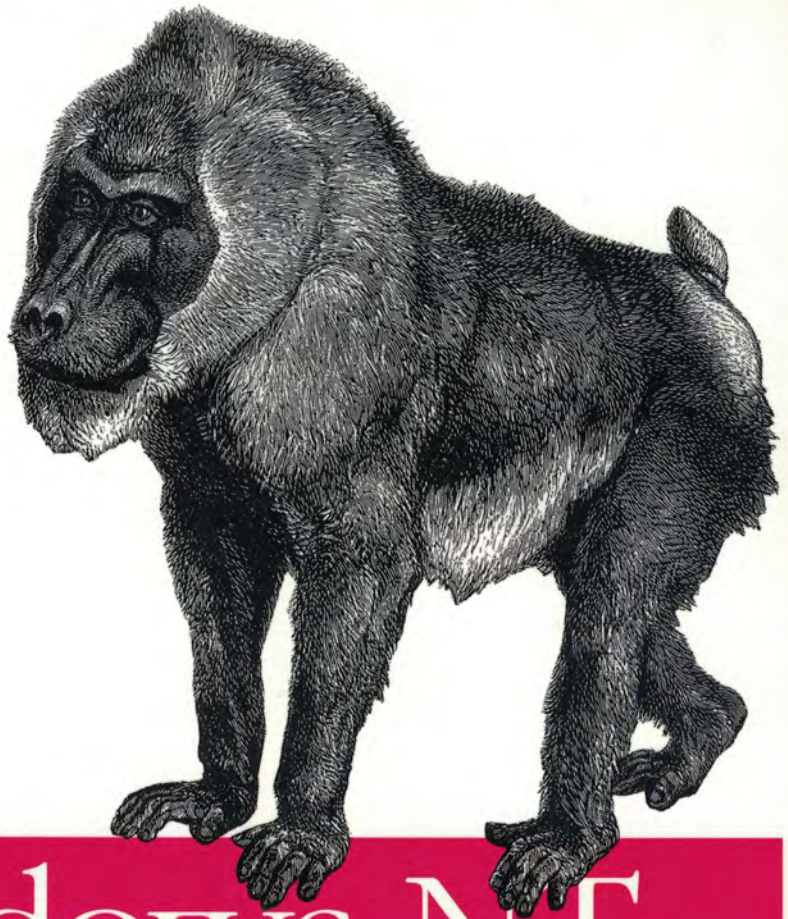
4 jobs in queue

**Figure 14-14:** Print jobs wait in queue until the printer is ready.



# **APPENDIX K**

*Effective and Painless NT Management*



*Essential*

# Windows NT System Administration

**O'REILLY®**

*Eleen Frisch*  
ROKU EXH. 1002

## ***Essential Windows NT System Administration***

by Eileen Frisch

Copyright © 1998 O'Reilly & Associates, Inc. All rights reserved.  
Printed in the United States of America.

Published by O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472.

**Editor:** Mike Loukides

**Production Editor:** Mary Anne Weeks Mayo

### ***Printing History:***

January 1998: First Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks and The Java™ Series is a trademark of O'Reilly & Associates, Inc. The association between the image of a mandrill and the topic Essential Windows NT System Administration is a trademark of O'Reilly & Associates, Inc.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly & Associates, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



This book is printed on acid-free paper with 85% recycled content, 15% post-consumer waste. O'Reilly & Associates is committed to using paper with the highest recycled content available consistent with high quality.

ISBN: 1-56592-274-3

[12/98]

ROKU EXH. 1002



# 9

*In this chapter:*

- *Adding a Printer*
- *Manipulating Print Jobs*
- *Advanced Printer Configuration*

## *Print Services*

Printers are system resources that are typically shared among the various systems and users within a network. We'll begin our consideration of them by looking at what happens when a user prints a document on a local printer (the process of sending a print job to a printer is sometimes referred to as *spooling*).

Suppose user *Chavez* decides to print a short letter from a word processing program. The following events must occur before the printed page appears at the printer:

- The information in the word processing document is translated into a form (language) that is understood by the printer. This is typically handled by the printer driver, possibly in conjunction with the application software.
- A print *job* is created for the page and handed off to the printing subsystem. If *Chavez* is allowed to print to the printer she has specified, the job goes into a print *queue* corresponding to the particular printer (or printer type) that *Chavez* has chosen, where it waits its turn to print.
- When the job reaches the top of the queue, the printing subsystem sends it to an actual printer device. The printer may be physically connected to the same computer as the one where *Chavez* originated the job, to a different computer on the network, or to the network itself.
- The printer receives the print job and produces a printed page based upon the data within it.

The system administration tasks associated with the printing subsystem include adding and configuring new printers and print queues, and monitoring and manipulating print queues and the pending jobs within them. We begin this chapter by considering the basic process of adding a printer to a Windows NT system, then

go on to consider managing print queues, and conclude by considering the setup and configuration of printers in several special sets of circumstances.

## Adding a Printer

The following steps are required to add a new printer to a Windows NT system:

1. Connect the printer to the computer and configure the port to which it is attached (if necessary). If you are using a parallel printer (the most common type), it might be necessary to enable support for bidirectional communication for the corresponding parallel port via the computer's setup program. This option might be labeled "Bidirectional" or "ECP mode" or "ECP/EPP" mode; you should usually select ECP if ECP and EPP are separate choices. Make sure that you are using a bidirectional-capable cable (IEEE 1284-compliant).
2. Windows NT provides an Add Printer wizard, which is easy to use (start it using the **My Computer**►**Printers**►**Add Printer** icon). This tool allows you to specify printers and to create print queues for use with them. We will consider each of its dialog boxes in turn.
3. The first dialog box (illustrated in Figure 9-1) asks you whether the new printer is to be administered locally or remotely (**My Computer** vs. **Network**, respectively). For a local printer, we select **My Computer**.

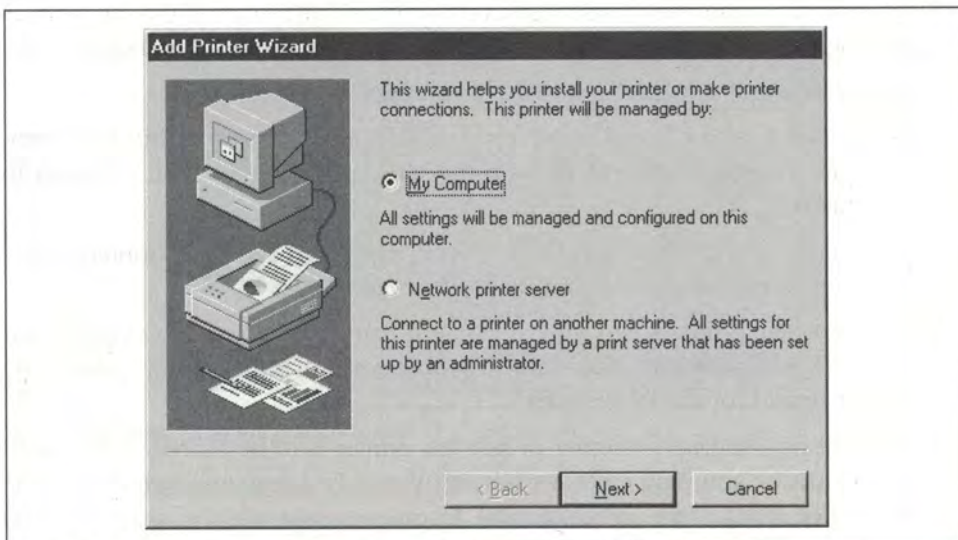


Figure 9-1. Specifying whether a printer is local or remote



4. Next, you are asked to identify the port to which the printer is attached. The example in Figure 9-2 indicates a printer attached to the second parallel port on the local system.

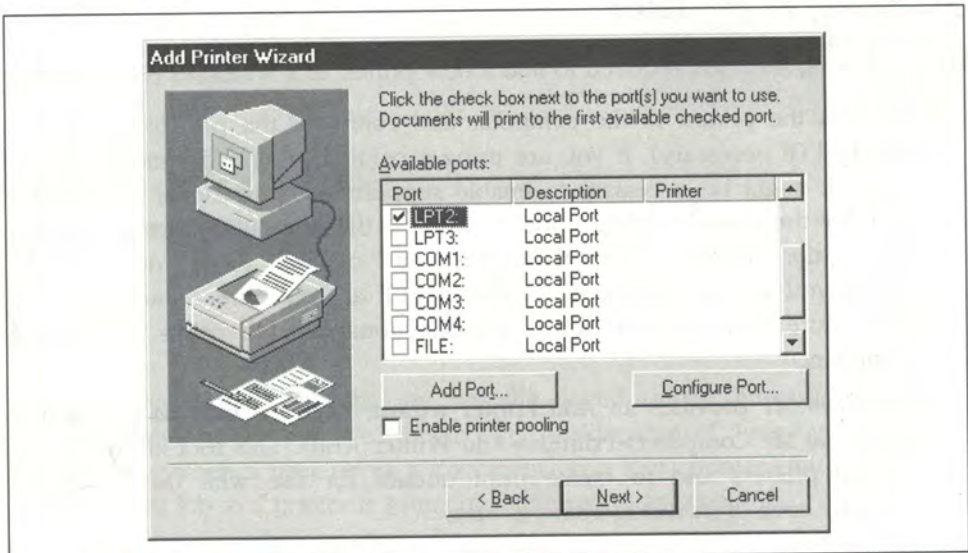


Figure 9-2. Specifying the printer port

5. The next dialog box requires you to specify the manufacturer and model of the specific printer being added. Select the manufacturer from the left list box and then select the appropriate model from the right list box (see Figure 9-3).

If your printer is not listed, you have two options:

- Obtain a driver from the printer manufacturer (often available for download from the Internet) and use this dialog box's **Have Disk...** button to load it.
- Specify a type closely related to and supported by your printer (many printers can emulate several standard printer types).

6. The next dialog box allows you to assign a name to the printer (*Degas* in our example in Figure 9-4). You can also optionally make the new printer the default printer for the local system.

7. You will now indicate whether or not this printer is to be shared. If you indicate that it is, you may enter a name for the shared resource (which defaults to the first word of the printer name). In our example, we will share the new printer, also under the name *Degas* (see Figure 9-5).

The lower portion of this dialog box is used to install printer drivers for other operating systems that may be downloaded to such systems as needed (print



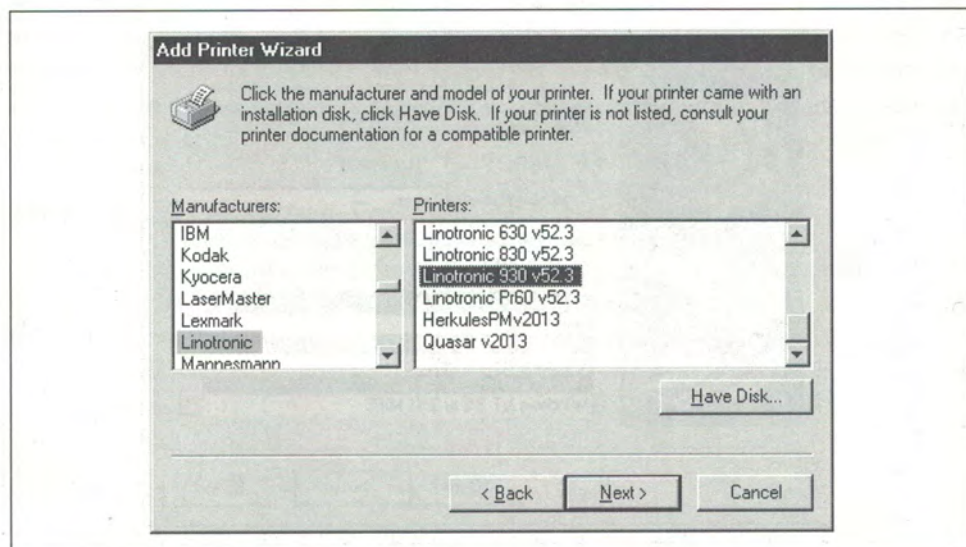


Figure 9-3. Specifying the printer model

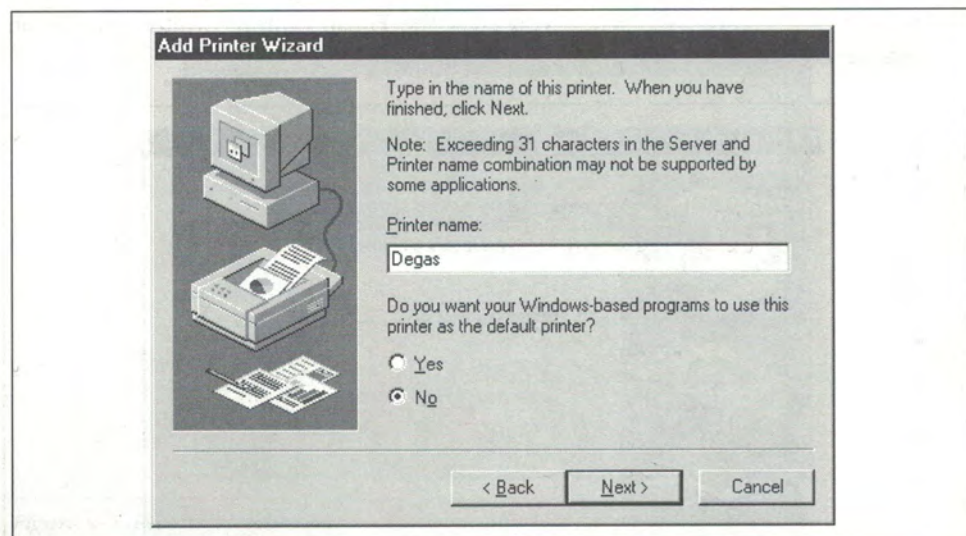


Figure 9-4. Specifying the printer name

clients must determine whether their system has the latest driver when initiating a print job). If you select any items from the list, you will be prompted to insert the distribution CD for each one.

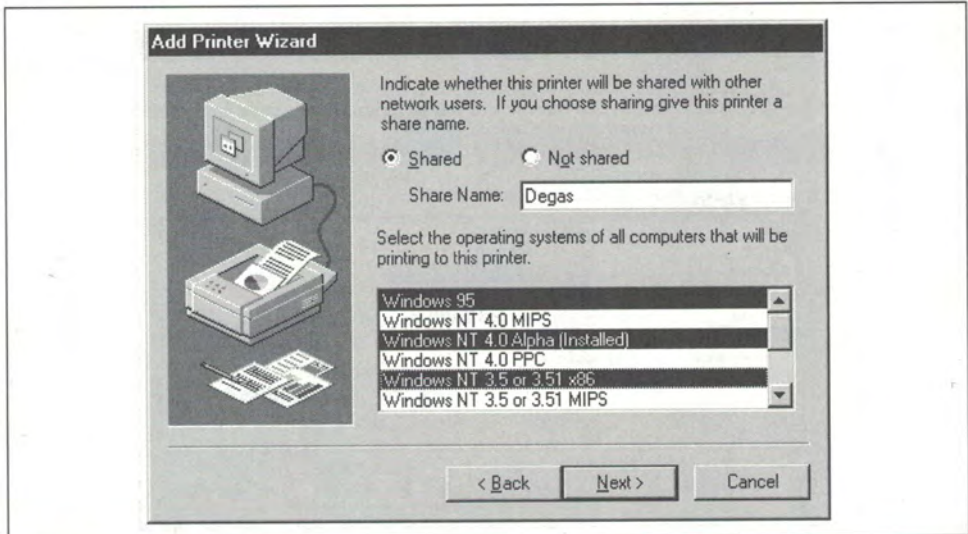


Figure 9-5. Sharing a printer with other operating systems

8. The final dialog box gives you the option of printing a test page to the new printer (see Figure 9-6). When you click the **Finish** button, printer installation will be complete.

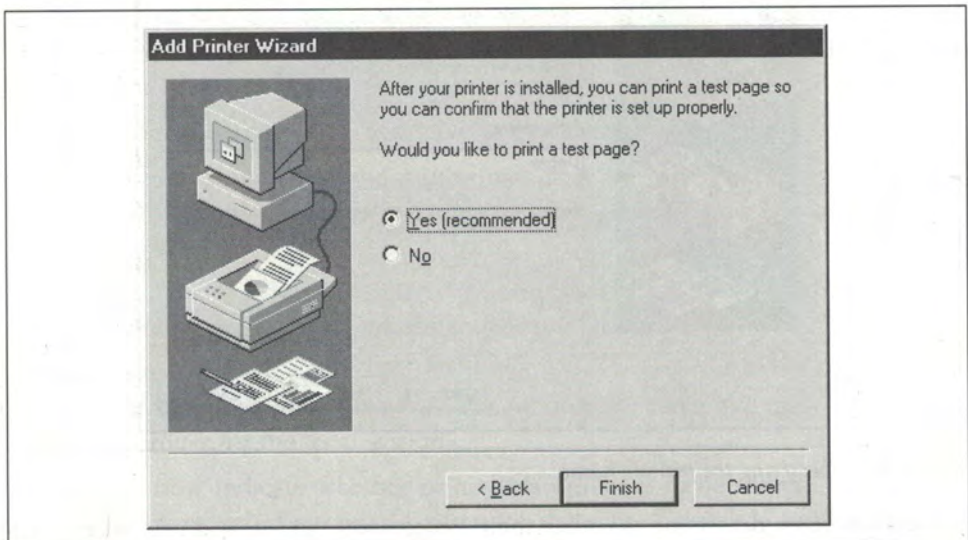


Figure 9-6. Printing a test page

As you might expect, you can change the settings for an existing printer via its **Properties**.



What this process has done is to identify the location of a printer device to the system and create a queue for it. There is no reason that the process can't be repeated in order to create another queue for the same printer (the only item that must change is the printer name). The two queues can then be given different properties.

### Sharing an Existing Printer

The **Sharing...** item on the printer's shortcut (right click) menu allows you to change the sharing status of an existing printer. The resulting dialog box is similar to the corresponding one from the **Add Printer** wizard (Figure 9-5). Using this item, you may later designate a printer as shared or remove network access to a shared printer.

### Setting Printer Permissions

Printers have permissions lists similar to those for filesystem shares. They may be viewed and modified via the **Permissions** button on the **Security** tab of the printer's **Properties**. Figure 9-7 shows the resulting dialog box.

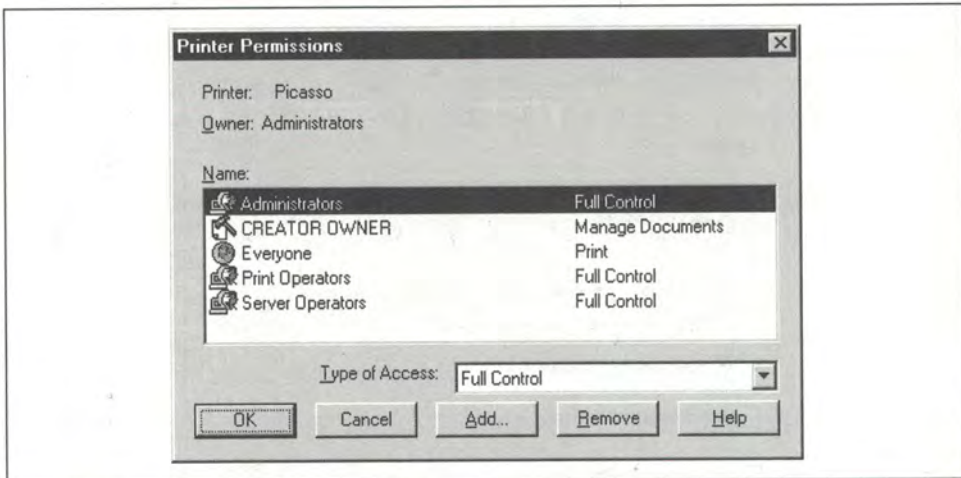


Figure 9-7. Printer permissions

The permissions defined for printers are listed in Table 9-1. They may be assigned to users and groups using the same process as for files and shares.

Table 9-1. Printer Permissions

Permission	Meaning
Full Control	Perform any printer configuration or management function (including printing documents).

Table 9-1. Printer Permissions (continued)

Permission	Meaning
Print	Send documents to this printer and control one's own print jobs.
Manage documents	Manipulate print jobs belonging to any user (this permission doesn't include printing to the device or printer configuration).
No Access	The user/group may not use the printer or affect any print job or the printer configuration.

Figure 9-7 lists the default permissions for a new printer: anyone can submit a print job to it, system administrators and two operator groups have full control of it, and the user who created it can manage print jobs in this queue.

### Printer Scheduling Properties

The Scheduling tab of a printer's Properties may be used to specify how and when jobs may be added to that queue and are sent from the queue to the printer. Its dialog box is illustrated in Figure 9-8.

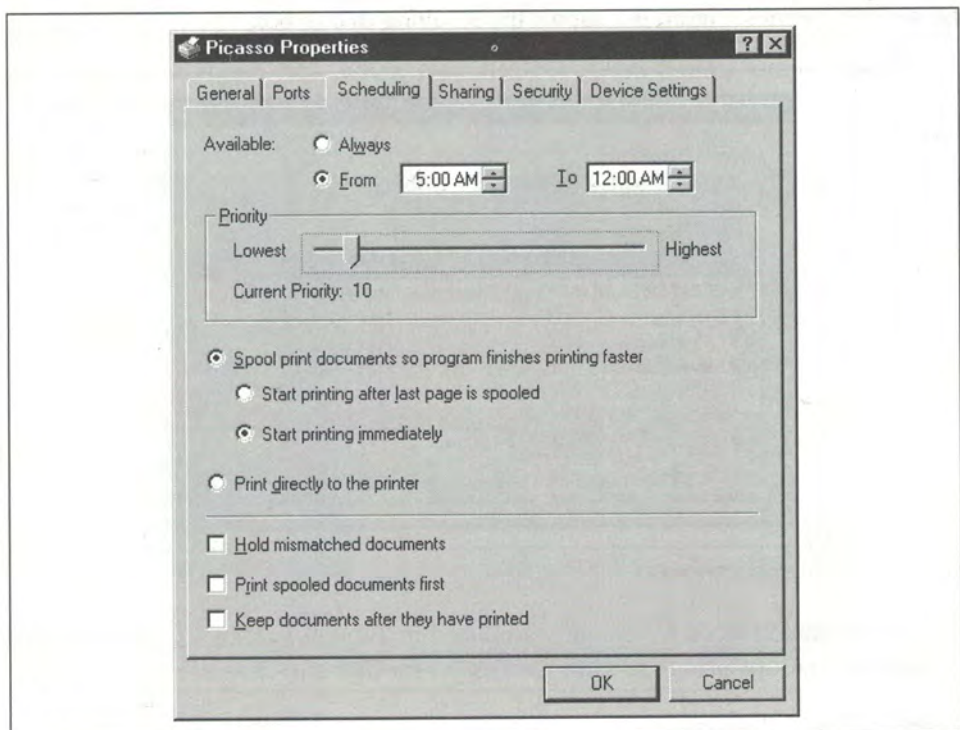


Figure 9-8. Printer scheduling properties

The following items may be specified in this dialog box:

# **APPENDIX L**

































































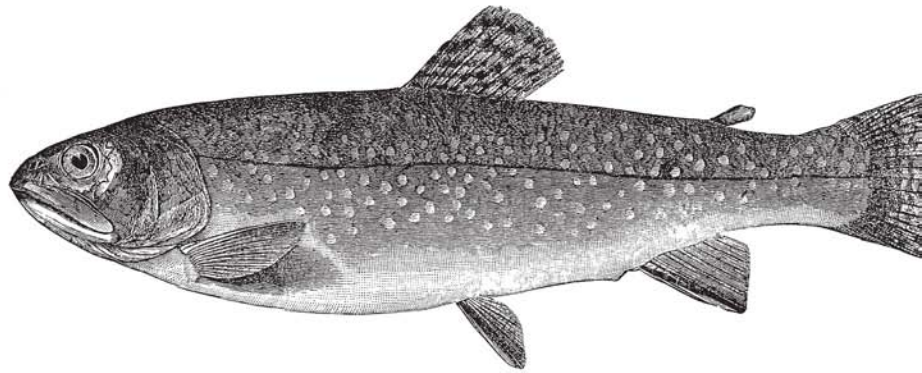
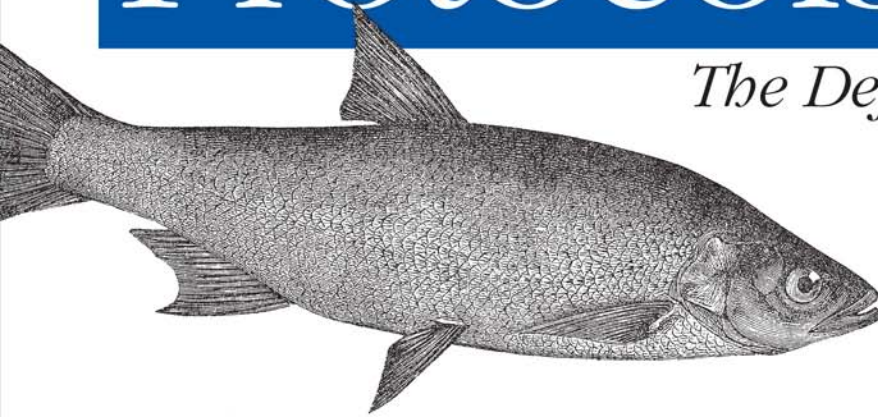
# APPENDIX M

*An Owner's Manual for the Internet*

**Includes  
CD-ROM**

# Internet Core Protocols

*The Definitive Guide*



**O'REILLY®**

*Eric A. Hall*  
*Foreword by Vint Cerf*  
ROKU EXH. 1002

# Internet Core Protocols: The Definitive Guide

Foreword by Vint Cerf.



We're all tired of hearing about the Internet's phenomenal growth, especially since the Internet's growth has landed squarely on our own backs. We're supporting more users, providing more services, and using more protocols (to say nothing of more complex versions of older protocols). There are more things to break, more ways for things to break, and more users to break them. The problems are more critical: network outages don't just inconvenience a few engineers, they cripple your entire business. And if that isn't enough, relative to the number of users (and problems), there are fewer real experts to turn to—and they're just as overworked.

So, when your network goes down in the middle of the night, and you have to get it back online before morning, where do you turn? Network trouble-shooting requires expertise in many unrelated areas, and until now, no single work has assembled all the information you need in one place.

*Internet Core Protocols* is the "TCP/IP owner's manual" you wish you had. It is the first in a series of books that discuss the Internet protocols from the standpoint of a network administrator. **Eric Hall** goes into detail about how each protocol works, what can go wrong, and what problems you typically face. He shows detailed examples of the protocols in action, including many complete packet traces. If you spend your days (and nights) working on real networks, you'll want this book at your side.

This book covers the core protocols that provide the underpinnings of any IP network: IP, TCP, UDP, ARP, ICMP, and IGMP. It also covers the standardization process and IP addressing. The accompanying CD includes Shomiti's Surveyor Lite, and the complete text of all the RFCs. Future books in the series will cover application protocols and other topics. Together, you'll have everything you need to understand your network, figure out what's going on, and get it running again. The only thing we don't provide is the coffee.



This book includes **Surveyor Lite**, a part of Shomiti Systems' high-performance suite of analysis, monitoring, and management tools for Fast Ethernet, Switched Ethernet, Gigabit Ethernet, and other high-speed local area networks. For more information on Shomiti's product line, call 1-888-SHOMITI or check out [www.shomiti.com](http://www.shomiti.com).

[www.oreilly.com](http://www.oreilly.com)

US \$39.95

CAN \$58.95

ISBN: 978-1-56592-572-4



---

# Internet Core Protocols

## *The Definitive Guide*