APPENDIX A

Online Networking Resources

This appendix offers an array of networking-related resources available on the Web as of this writing. Should you encounter a problem with a URL (such as the dreaded 404: Not Found error message), open your favorite search engine and search for the appropriate terms. You might find an even better source of information!

A.1 General Networking Information and Support

- Microsoft Knowledge Base: *http://www.Microsoft.com/*. Point to Support in the left pane and then select Knowledge Base. You can search for support information on nearly every Microsoft product offered.
- Microsoft TechNet: *http://www.microsoft.com/technet/default.mspx.* An online version of the popular CD/DVD subscription, TechNet offers general support information for Microsoft products, security updates, patches, hotfixes, white papers, and much more.
- Novell: *http://www.novell.com.* Click the Support link to access Novell's knowledge base, patches and fixes, support forums, documentation, and downloads.
- Linux.com: *http://www.linux.com;* LinuxOnline: *http://www.linux.org;* Linux Journal: *http://www.linuxjournal.com.* These preceding

Linux URLs offer general information and support for Linux distributions, such as Red Hat, Caldera, Slackware, Mandrake, Debian, and SuSE.

- Cisco: *http://www.cisco.com.* Click the Technical Support link and choose from several networking-related categories of support that include hardware, software, technology, tools and utilities, and the software center.

A.2 General Protocol Information

- Protocol Directory: *http://www.protocols.com/pbook/toc.htm.* Protocols.com offers information on many types of networking protocols, and pin assignments for physical interfaces. Be sure to check out the TCP/IP Suite link for a list of protocols for each layer of the OSI model, and a protocol route map.
- ASL Protocol Decodes: *http://www.decodes.co.uk/content/chart.htm.* Here you'll find a protocol decode chart that lists the layers of the OSI model with the associated protocols that exist at each layer, along with the layer boundaries. You can view the chart online or download the file (in Microsoft Publisher format).
- Computer Networking and Internet Protocols: A Comprehensive Introduction: *http://www.cis.ohio-state.edu/cs/Services/index.html.* Visit this site for information on GNU, Internet RFCs, and Internet Engineering Notes (EINs).

A.3 Security

A.3.1 Best Practices

Each of the following sites provides information on best practices.

- *http://csrc.nist.gov/fasp/*
- *http://www.cert.org/security-improvement/*

- *http://www.sans.org/rr/*
- *http://www.securityfocus.com*

A.3.2 IP Security

- Computer Security FAQs: *www.faqs.org/faqs/computer-security/*. This is one of the best resources for IP security-related FAQs.
- SysAdmin, Audit, Network, Security (SANS) Institute: *www.sans.org*. SANS provides, by far, some of the best security training and information. It offers a weekly vulnerability digest and weekly news digest, access to the Internet's early warning system (Internet Storm Center), flash security alerts, and research papers.

A.3.3 Certificates and Encryption

- RSA Security: *http://www.rsasecurity.com*. RSA Security owns a digital signature authentication system that uses the Rivest-Shamir-Adleman algorithm. It is often included as part of Web browsers and various other software products.
- VeriSign: *http://www.verisign.com*. This is a popular certificate and registration authority. You can use VeriSign to issue certificates for secure Web site connections.

A.3.4 Password-Revealing Programs

- Openwall Project: *http://www.openwall.com/*. Openwall offers several password-revealing programs, such as WASP and John the Ripper.

A.3.5 Wireless LANS

- Wireless LANS: *http://www.wlana.org/security.htm*. This site offers links to several white papers that focus on WLAN security.

A.4 Requests for Comments (RFCs)

- Internet FAQs Archive: *http://www.faqs.org/rfcs/*. This site offers a search engine for Internet RFCs. We've found it to be an up-to-date depository.
- Internet Engineering Task Force: *http://www.ietf.org*. A must-visit site for all things networking. Be sure to check out the RFC Pages link in addition to the Overview of the IETF link.

A.5 IP Addressing, Subnetting, and Supernetting

- Understanding IP Addressing: Everything You Ever Wanted To Know: *http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf*. Chuck Semeria's paper offers comprehensive information on every part of IP addressing.
- IPv6: *http://www.ipv6.com;* IPv6 Forum: *www.ipv6forum.com/*. Both IPv6 sites offer the latest information on the development and pending deployment of IPv6.

A.6 Binary Arithmetic Overviews

- Binary Arithmetic: *http://www.freesoft.org/CIE/Topics/19.htm*. This article, from the "Connected: An Internet Encyclopedia" site, offers easy-to-understand illustrations that help the reader grasp binary arithmetic.

A.7 DHCP and DNS

- DHCP Resources: *http://www.dhcp.org/*. Ralph Droms offers outstanding DHCP resources and links to additional sources of information.
- DNS Resources Directory: *http://www.dns.net/dnsrd*. Need to brush up on DNS, or just get a handle on what it's really about? András Salamon shares information on nearly every DNS-related topic imagineable.

A.8 Routing and Switching

- Circuit Switching: *http://jhunix.hcf.jhu.edu/~tnaugler/770.512/Common_files/CircuitSwitching/CircuitSwitching.htm.* Thomas Naugler offers a fully illustrated primer on circuit switching, with additional Web references.
- Packet Switching Demo: *http://www.pbs.org/opb/nerds2.0.1/geek_glossary/packet_switching_flash.html.* This PBS Flash tutorial walks you through the basics of packet switching.

A.9 SNMP

- SNMPWorld.com: *www.snmpworld.com/*. You can find links, tools, RFCs, MIBs, and more at this SNMP-focused site.

APPENDIX B

Networking Standards

For networks to function properly, an amazing array of devices and technologies must all work well together. From the networking cables or media, to the hardware necessary to connect computers and other devices to such media, to the protocols and communication formats that give networks shared capabilities to get things done, ingenuity and technology are essential to coordinate all the required components.

A vast collection of networking standards and specifications explains how all of these pieces and parts can be successfully—and easily—assembled into working networks. The key to this is interoperability: the ability of devices of the same kind and capability to work with one another, even if made by different manufacturers in different parts of the world. At each layer of the OSI network reference model, which is covered in Chapter 2, network standards exist to ensure interoperability. From specifying common cable types and connectors (so that plugs fit network interfaces) to establishing common network protocols, such as HTTP for Web access and SMTP for e-mail access, various networking standards make it possible to plug different parts together and get them to work.

Standards help establish common sets of implementation guidelines, connectivity and behavioral specifications, message formats, error-handling requirements, and so forth, that create comprehensive sets of rules that make interoperability possible. Some standards even supply batteries of tests that implementers or manufacturers must use to demonstrate compliance with standards. Likewise, as new technologies are developed, partici-

pants hold regular "bake-offs" to provide ample opportunities to make sure that different implementations can and do indeed work together as required and desired. In the following sections, you'll find information about key networking standards that apply at various levels of the OSI network reference model and links where you can find more information.

B.1 Making Standards Happen

Before we present and examine various key networking standards, it's important to understand the processes whereby standards are made. Virtually all standards emerge from various committees of multiple individuals, such as working groups, special interest groups, and task forces from business, industry, academia, government, and other groups with particular agendas and investments to protect. Creating standards involves considering various points of view and looking for workable compromises and sometimes even alternative implementations that satisfy all parties involved equally.

In general, the process of creating a standard works like this:

- Standards are built by standards organizations, industry or trade associations, consortia, or other groups, which recruit assistance from volunteers and staff to document and maintain individual standards documents. Many such organizations have only a small number of paid staff who oversee ongoing efforts, but rely on support from interested parties to provide the manpower necessary to research, craft, and maintain standards and specifications.
- Oversight committees and/or members of the parent organization generate ideas for potential standards. Often, individuals who represent third parties that share common interests or avocations form groups to deal with specific networking-related technologies or issues to drive activity in specific areas.
- Within communities focused on special interests, working groups form to deal with specific topics, issues, or technologies. Such groups are usually run by a chairperson and staffed by volunteer members who share the workload involved in defining problems and crafting standards to address them.

- Starting with whatever ideas, prototypes, and existing allegiances members may bring to the working group, such groups work to build consensus around the problems a standard seeks to address and how it attempts to resolve them. Given sufficient time (often months to years), numerous proposals are drafted. The proposals are debated and amended until consensus is reached or efforts are abandoned, as sometimes happens when consensus fails to emerge. Internet standards, for example, aim at something called "rough consensus," which means that the majority of the working group backs a proposal and that dissenters are willing to play along.
- Once the working group agrees that its draft standard proposal is ready for outside review, the group turns the proposal over to the parent organization. There it's subjected to wider review and comment within a special interest group or technical team. It is then returned to the working group for further work, as needed. A draft proposal typically goes through several iterations in this phase, which normally takes between three and 12 months to complete.
- Finally, the special interest group turns the draft standard over to a higher-level parent group, often a standards committee, which provides an additional level of review and feedback. Then it is brought to the organization's membership for comment and discussion. If accepted, this final stage results in creation of an official standard. However, the draft may be rejected outright. This step can take from three to six months to complete.
- Once accepted and finalized, official standards are published in printed and/or electronic format. As such, they will often be subjected to formal editing procedures, in much the same way that manuscripts are readied for publication. Depending on length and complexity, this process takes between one and six months to complete.
- After publication, official standards must be reviewed regularly and updated or amended to keep up with changing times and technologie. An official author or technical editor is generally appointed to take stewardship of a standard; this person oversees the post-publication maintenance work. Reviews typically occur once or twice a year, unless the parent organization or its membership calls for an

interim review earlier. Given their frequency, this process seldom takes more than a month or two to complete.

- Standards that are not superceded outright by updated versions are often declared obsolete. The newer version may be a revision of the original standard or an entirely new (but similar) standard taking into account new technology, protocols, or services. In any event, once a standard is made obsolete, another standard is invariably used in its place.

Creating standards, and especially achieving consensus, takes time and involves a lot of effort, discussion, and compromise. This explains why proprietary protocols and technologies so often come and go while related standards may still be under development. This creates an important dynamic between open, standard implementations and specifications and closed, proprietary ones: In many important ways, each of them helps to keep the other honest. Proprietary technologies and protocols help keep pressure on standards groups to finish up before their standards become passé; standards groups help make sure that proprietary solutions meet general market needs by specifying minimal accepted features and functions (which proprietary implementations usually seek to exceed rather than simply to meet).

Within the networking world, thousands of trade groups, professional societies and associations, standards bodies, and industry consortia exert considerable influence. In the following section, we provide a short but select list of those groups and bodies most deeply involved in and responsible for the state of networking as it exists today.

B.2 Key Standards Organizations

Networking standards come in many forms and from many kinds of organizations. Some are specifically international or global in scope (the International Organization for Standardization, or ISO, is a good example). Others focus only on particular countries or regions of the world, such as Underwriters Laboratories, which warrants electrical and electronic equipment for North American markets.

Standards organizations also tend to have specific areas of interest or focus: some concentrate on networking media, others on networking devices and

technologies, and still others on networking protocols, services, and communications. IT professionals or those simply interested in networking should be familiar with the major networking standards organizations. The Computer and Communication Web site at *http://www.cmpcmm.com/cc/standards.html* has one of the best overall lists of general networking-related standards that we've found. Be sure to visit it for a broader view of such organizations than we can cover in this appendix.

Here are our picks for key standards organizations related to networking:

- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)
- Internet Society (ISOC)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- Telecommunications Industry Association (TIA)
- World Wide Web Consortium (W3C)

We'll review the areas of focus and coverage for each of these organizations, followed by information about resources for other networking technology and standards.

B.2.1 American National Standards Institute (ANSI)

Simply put, ANSI is involved in the development of technology standards in the United States. Although ANSI is an American organization, it exerts influence worldwide: the United States has been a technology leader in so many areas that its standards lead the rest of the world. In fact, this organization has created more than 10,000 standards. Also, although its primary areas of focus are networking technologies, programming languages, and communications techniques and methods, ANSI also acts as the American representative to the ISO, the ITU-T, and the IEC, all of which are discussed elsewhere in this appendix.

Well-known ANSI programming languages include C, COBOL, FORTRAN, and ANSI Standard SQL (Structured Query Language), a standard variant of the well-known database query language SQL. ANSI standards for networking technologies include joint efforts with the IEEE on various aspects of the 802 networking standards for Token Ring (802.5) and Ethernet (802.3 and others), as well as on FDDI and SONET. Communication standards include standards for voice and data transmission, encryption and privacy, and numerous types of signaling controls and technologies. To learn more about ANSI, visit the organization's Web site at *http://www.ansi.org*.

B.2.2 Electronic Industries Alliance (EIA)

Based in Arlington, Virginia, the EIA is a national trade organization that represents more than 2,500 members, mostly manufacturers who work in the electronics industry in the United States. The EIA represents its members on issues that are relevant to implementing successful technologies; its current focuses include broadband and Internet security. The EIA also works with other industry groups, including the TIA, to develop various recommended standards for electronics equipment and communications. EIA standard designations take two forms:

- RS-nnn, where RS stands for "recommended standard" and nnn is a three-digit sequence number
- EIA-nnn, where the same number is used but the standard designation is assumed

A well-known EIA standard is the RS-232C standard, which was originally approved in 1987. Although it's still most commonly known as RS-232, this standard was advanced to EIA/TIA-232-E in 1991, and remains the most common standard for serial communications. (The TIA was a joint sponsor for this standard; see the discussion of the TIA elsewhere in this appendix.) The EIA has defined newer standards for serial communications known as RS-422, RS-423, and RS-449 that offer faster data transfer and superior immunity to electrical interference. To learn more about the EIA and related standards, visit *http://www.eia.org*.

B.2.3 International Electrotechnical Commission (IEC)

The IEC is a Swiss-based, global organization that creates and publishes international standards for electronic, electrical, and related technologies. The organization's charter addresses all forms of electronics, including

electronic circuitry and devices, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution. The IEC also addresses related terminology and symbols, compatibility issues, measurement and performance, dependability, design and development topics, as well as safety and the environment.

IEC standards also represent the World Trade Organization's Agreement on Technical Barriers to Trade (WTO TBT), created to help central governments establish and recognize international standards as a way to improve global industrial efficiency and develop world trade. Hundreds of standardization bodies have accepted the IEC's Code of Good Practice for the Preparation, Adoption, and Application of Standards. This body also promotes conformity assessment and product certification schemes that ensure interoperability among components and devices manufactured worldwide. Key networking-related IEC standards govern standard cabling, broadband networking and ISDN, transformers, electrical motors, and other standard electrical components and devices. For information on this organization, visit *http://www.iec.*

B.2.4 International Telecommunication Union-Telecommunication (ITU-T)

The ITU-T was formerly known as the Comite Consultatif Internationale de Telegraphie et Telephonique (CCITT); it is probably still better recognized under its old name than its new one. This group operates as a permanent part of the ITU and under the authority of the United Nations (UN). The ITU itself includes members from more than 160 countries, representing the vast majority of UN member states. Often, delegates to the ITU-T work for national postal, telephone, and telegraph services, commonly known as PTTs.

The ITU-T manages standards that relate to various networking topics and technologies including communications, telecommunications, and outright networking services. The ITU-T works with ISO, which explains why many standards carry both ISO and ITU-T designations. The ITU-T is divided into 15 named topic and study groups, plus two sets of standards designated V (for modems) and X (for various forms of networking protocols and communications), as follows:

- *A, B:* working terms, definitions, procedures, and standards guidelines
- *D, E:* tariffs and fee exchanges

- *F:* telegraph, telemetric, and mobile services
- *G, H:* transmissions
- *I:* ISDN
- *J:* television transmission
- *K, L:* facilities protection
- *M, N:* maintenance
- *P:* telephone transmissions
- *R-U:* terminal and telegraph services
- *V:* telephone-based data communications
- *X:* data communication networks

This nomenclature explains the various V.nn standards (such as V.90 for 56 Kbps modem communications). When a standard is named V.nn *bis* or V.nn *ter*, the italicized terms refer to the second and third standards that share the common two-digit (nn) value. For more information about the ITU-T, visit the parent organization's Web site at *http://www.itu.org*.

B.2.5 Internet Society (ISOC)

The ISOC is a large, member-oriented organization that is deeply involved with all things related to the Internet. Numerous suborganizations within the ISOC are of greatest interest from a standards perspective:

- The Internet Engineering Steering Group (IESG), an oversight group that provides input and guidance over IETF working groups, allocates resources and set priorities. For more information, visit *http://www.iesg.org/iesg.html*.
- The Internet Research Task Force (IRTF) is a forward-looking group that researches Internet protocols, applications, architecture, and technologies that have potential social or technical significance. Some of this research is sent on to the IETF and results in the creation of actual Internet standards. For more information, visit *http://www.irtf.org*.
- The Internet Architecture Board (IAB) governs Internet architecture, services, protocols, and related technologies, and is the parent to many suborganizations responsible for researching, creating,

and maintaining Internet standards. This group's Web site is *http://www.iab.org*.

- The Internet Corporation for Assigned Names and Numbers (ICANN) oversees names and addresses for the Internet, including IP address space allocation, protocol parameter assignments, domain name system management, and root server system management functions for the entire Internet. Although the Internet Network Information Center (InterNIC, *http://www.internic.net*) maintains information about domain name registries—third-party companies and organizations that manage various portions of the overall Internet domain name space—ICANN oversees all other aspects of Internet naming and addressing. Visit *http://www.icann.org* for more information about this organization.
- The Internet Engineering Task Force (IETF) is one body under the IAB that is responsible for proposing, developing, and maintaining Internet standards documents. Such documents, known as Requests for Comment (RFCs), come in numerous forms (draft, experimental, historical, best practices, official, and obsoleted) that reflect their relevance, currency, and importance. Individual standards are the focus of specific working groups, of which more than 100 may be active at any one time. The IETF's Web site is *http://www.ietf.org*.

As of this writing, there are nearly 4,000 RFC documents in the index of RFCs maintained by the IETF—a collection of documents far too large to document in this appendix. RFCs numbers are allocated in strict numerical order and always contains the most recent version of the "Internet Official Protocol Standards" (RFC 3700, at the time of this writing). Thus, the RFC ending in 00 is numerically closest to the highest-numbered current document. Keep this in mind to determine which official standard RFCs are currently in effect, what best current practice (BCP) documents are active, and so forth. You can locate the current document at *http://www.faqs.org/rfcs/rfc3700.html*, or by searching for "RFC 3700" using your favorite search engine. Starting from this document, you can usually find the most important RFCs, except perhaps for those introduced since the last Internet Official Protocol Standards Document was published. Because this document is updated regularly, you'd seldom have to search through more than 18 months of new RFCs.

B.2.6 Institute of Electrical and Electronics Engineers (IEEE)

The IEEE (pronounced "eye-triple-e") is a nonprofit, technical professional association with members from more than 150 countries around the world. Although it's based in the United States, the organization acts as a technical authority on a broad range of topics and technologies than range from computer engineering and telecommunications to biomedical technology. As part of its focus, the IEEE produces and maintains a large body of networking-related specifications and standards. Work that originates in the IEEE is often shared with ANSI, and in turn may be shared with ISO. This explains why many important IEEE networking standards are also ANSI and ISO standards.

The most important IEEE networking project is its collection of standards known as the 802 project. This number indicates that it was the second project begun in 1980, although many additions have been made, and continue to be made, since then. At its inception, 12 working groups were designated for the 802 project, numbered 802.1 through 802.20. Today, there are 9 active working groups (A), eight hibernating groups (H: no longer active, published a standard), and two disbanded working groups (D: no longer active, did not publish a standard) in the 802 family, as shown in Table B.1.

For more information about the IEEE, visit *http://www.ieee.org*. For an excellent overview of the IEEE 802 standards, visit *http://www.ieee802.org*.

B.2.7 International Organization for Standardization (ISO)

The Paris-based ISO is sometimes incorrectly called the International Standards Organization, but "ISO" is not really an acronym. ISO's focus is on defining, maintaining, and promoting global standards for the worldwide community. Member countries may be represented by government officials or by national standards organizations, such as the ANSI in the United States. ISO representatives also include participants from business, research and development, or educational organizations and from other international standards bodies such as the IEC and the ITU-T. Overall, ISO's mission is to create and promote international standards for all manufactured products or goods, and for services as well.

ISO's focus in the networking arena is to establish global standards for information exchange, e-commerce, data communications, and network-

TABLE B.1 Working Groups in the IEEE 802 Project

Number	Status	Title
802.1	A	High Level Interface (HILI) Working Group
802.2	H	Logical Link Control (LLC) Working Group
802.3	A	CSMA/CD Working Group
802.4	H	Token Bus Working Group
802.5	H	Token Ring Working Group
802.6	H	Metropolitan Area Network (MAN) Working Group
802.7	H	BroadBand Technical Advisory Group (BBTAG)
802.8	D	Fiber Optics Technical Advisory Group (FOTAG)
802.9	H	Integrated Services LAN (ISLAN) Working Group
802.10	H	Standard for Interoperable LAN Security (SILS) Working Group
802.11	A	Wireless LAN (WLAN) Working Group
802.12	H	Demand Priority Working Group
802.14	D	Cable-TV Based Broadband Communication Network Working Group
802.15	A	Wireless Personal Area Network (WPAN) Working Group
802.16	A	Broadband Wireless Access (BBWA) Working Group
802.17	A	Resilient Packet Ring (RPR) Working Group
802.18	A	Radio Regulatory Technical Advisory Group
802.19	A	Coexistence Technical Advisory Group
802.20	A	Mobile Wireless Access Working Group

ing protocols. These standards are intended to permit interoperability among products and services on a global level, so that components and systems from around the world can be easily integrated. ISO's major efforts in this area are known collectively as the Open Systems Interconnection (OSI, or ISO/OSI). Although most such standards now serve primarily as teaching models, some components continue to exert real market influence today. For more information about ISO, visit *http://www.iso.ch*.

B.2.8 Telecommunications Industry Association (TIA)

The TIA is a leading, U.S.-based nonprofit trade association that serves communications and information technology industries. Its missions include market development, sponsoring of trade shows, and industry awareness promotion and advocacy, as well as standards development. Although based in the United States, the organization takes a global focus, primarily because its member companies serve the global community.

Although it can trace its roots back to trade show planning for independent telephone vendors in 1924, the TIA did not form under its present name until 1988 after a merger of the United States Telecommunications Suppliers Association (USTSA) and the Information and Telecommunications Technologies group of the EIA (covered elsewhere in this appendix). Between 1924 and 1988 the organization focused almost exclusively on telephony topics, as a committee of the United States Independent Telephone Association and, after 1979, as the USTSA.

With a dual focus on communications and information technology, the TIA has been involved in formulating standards across a number of broad technology areas, including fiber optics, user premises equipment (primarily telephone switches and systems), network equipment, wireless communications, and satellite communications. As such, it affects networking technology in all of these groups, especially in light of continuing convergence of voice and data networks and technologies. From wireless networking of many kinds to the cables that make wired networking possible, the TIA is likely to be involved in related standards. For more information, visit the organization's Web site at *http://www.tiaonline.org*.

B.2.9 World Wide Web Consortium (W3C)

A relatively new standards body, the W3C (pronounced "double-you-three-see"), formed in 1994 when the underlying technologies that support the Web were first introduced. The initial effort originated at the research labs at CERN (Conseil Européen pour la Recherche Nucléaire; European Laboratory for Particle Physics) in Geneva, Switzerland. This group decided to release its work on the Web markup language HyperText Markup Language (HTML) and the protocol and service environment known as HyperText Transfer Protocol (HTTP) to the world community,

which led directly to the formation of W3C. In the United States, W3C makes its home on the campus of the Massachusetts Institute of Technology (MIT). W3C is also involved with INRIA (Institut National de Recherche en Informatique et en Atomatique, the French National Institute for Research in Computer Science and Control). Both organizations help to staff and house W3C as well.

Although the relationship between the Web and networking may not be immediately obvious, so much Internet access focuses on the Web and related services and capabilities that we'd be remiss in omitting it from this collection. IT professionals in general, including those who specialize in networking, regularly turn to the Web for news, information, updates, patches, fixes, and more. With a Web presence at nearly every organization, many network professionals are also responsible for or involved in Web sites.

Important W3C standards include:

- **Cascading Style Sheets (CSS):** A document markup language used to manage how pages are displayed within Web browsers (or other viewing software)
- **HyperText Markup Language (HTML):** The basic markup language for representing simple content and information in Web pages
- **HyperText Transfer Protocol (HTTP):** The collection of message formats used to request Web pages to be downloaded from a Web server and delivered to a client for access (and, usually, viewed within a Web browser)
- **eXtensible Markup Language (XML):** A sophisticated markup language designed to replace HTML with more abstract and powerful content representation, management, and presentation controls
- **XML vocabularies:** Any of a number of standard or named collections of markup built using XML; hundreds of standard XML vocabularies have been defined for content ranging from anatomy to zoology

The W3C operates an extensive Web site with complete documentation for its hundreds of standards at *http://www.w3c.org*. Robin Cover's "Cover Pages" at *http://xml.coverpages.org* is another great, comprehensive source of information about XML and XML vocabularies that includes news,

information and overviews, as well as W3C pointers and third-party documents about XML and XML vocabularies.

B.3 Other Valuable Networking Technology and Standard Resources

In addition to the organizations mentioned in the preceding sections, a plethora of sites and information about networking topics and technologies is available online. When researching a specific standard, visit your favorite search engine and look for tutorial or overview documents on the subject by concatenating the subject name with the terms "standard tutorial" or "standard overview" in your search string. Also see Appendix A for more general pointers on sources of networking information online.

APPENDIX C

Binary Arithmetic and IP Address Calculation

Understanding TCP/IP means understanding IP addresses, those strange dotted-quad numbers such as 172.16.1.24 or 192.25.1.1. You'll sometimes see the numbers when surfing the Web, and you'll deal with them any time you must install or configure networking software or devices. Understanding IP addresses and learning how to subdivide or combine IP address ranges—sometimes called subnetting and supernetting, respectively—makes more sense if you understand the binary or Base 2 notation that computers use and see when they work with addresses.

Having some basic knowledge of binary numbers is extremely helpful; knowing how to convert from decimal to binary and binary to decimal is also quite helpful. (We "slow" humans understand numbers much better in decimal form, whereas our fast computers understand numbers much better in binary form.) This is not a terribly complex job, and can be accomplished by mastering several simple tasks:

- Learning how to convert binary numbers into decimal equivalents, and vice versa
- Understanding the concept of a mask, and how mask bits translate into specific decimal and binary numbers
- Learning to recognize specific bit patterns in 8-bit numbers and how they convert to decimal
- Understanding how to concatenate multiple 8-bit numbers and convert them into decimal

You should understand one more subtlety about numbers before we tackle the subjects outlined above—namely, the distinction between distance and the number of positions on a number line. This can be best summed up by asking the question: "How many numbers fall in the range from 1 to 6?" Subtracting 1 from 6, you get 5, but this is the distance (or difference, in arithmetic terms) between 1 and 6. If you count the number of values in this sequence—1, 2, 3, 4, 5, 6—you'll quickly see that there are 6 numbers in this range. The general formula that answers the question "How many numbers fall in the range from *a* to *b*?" is best expressed as $a - b + 1$ (to add back the starting value that the difference ignores). Please keep this notion in mind when dealing with address ranges, subnetting, and supernetting, because the maximum number of addresses needed is important when making such calculations.

C.1 Converting Between Binary and Decimal

C.1.1 About Binary Numbers

Binary numbers (Base 2) are either 0 or 1 for any possible power of 2, where all binary numbers may be expressed using exponential notation as follows:

$$c_1*2^n+c_2*2^{n-1}+c_3*2^{n-2}+...+c_k*2^3 +c_{k+1}*2^2+c_{k+2}*2^1+c_{k+3}*2^0$$

The c^i values are constants and, because of the way binary arithmetic works, must be either zeros (0s) or ones (1s). The 2^n values represent some power of 2, or the number of 2 raised to a specific exponent value. (Note that $2^1 = 2$ and $2^0 = 1$ by mathematical convention; this trick of notation is what makes it possible to represent any number in binary form.) Binary numbers aren't compact or easy for humans to read once those numbers get large, but they can represent any integer or whole number imaginable.

C.1.2 Converting Binary to Decimal

If you count the number of values in a binary number starting from right to left, each position you count specifies the exponent for the power of 2 associated with the specific value you're counting in the number at any given moment, as long as you start counting with 0 (zero).

Let's use the number 10010011 as an example. If you count the number of positions in this number you get 8, which means the highest power of 2 in this string of binary digits is 7 (counting from 0 to 7 gives you a total of 8

TABLE C.1 Decimal Values for Powers of 2

Power	Exp Value	Decimal
0	2^0	1
1	2^1	2
2	2^2	4
3	2^3	8
4	2^4	16
5	2^5	32
6	2^6	64
7	2^7	128
8	2^8	256

numbers, as explained earlier in this appendix). Thus, this number may be expressed in exponential notation, as follows:

$1*2^7 + 0*2^6 + 0*2^5 + 1*2^4 + 0*2^3 + 0*2^2 + 1*2^1 + 1*2^0$

As a quick check on your work, list only the constants that precede the values of 2 in this sum, and you get 10010011, which matches the original number exactly—as it must, to be correct.

Now, calculating the decimal value of the number means that you need only to add the decimal values for the powers of 2 that have a coefficient of 1 so that this number could be more compactly expressed by omitting all zero coefficient values, as follows:

$1*2^7 + 1*2^4 + 1*2^1 + 1*2^0$

Note that this transformation breaks the symmetry with the original binary number, but it also provides only those numbers you care about. By using a calculator or the values in Table C.1, you can determine that $2^7 = 128$, $2^4 = 16$, $2^1 = 2$, and $2^0 = 1$, so the decimal value of the binary number 10010011 is 128 + 16 + 2 + 1, or 147. This same approach works for all binary numbers, but gets tedious as numbers get large. (Hint: The Microsoft Calculator has a special button that converts from binary to decimal, and another that converts from decimal to binary!)

C.1.3 Converting Decimal to Binary

There are two traditional approaches to converting decimal numbers to binary—a brute force technique that is extremely easy to calculate but may be difficult to understand, and a value-fitting technique that depends on knowing the powers of 2 to fit decimal numbers to them. Each method depends on dividing or subtracting specific numbers and working on what's left over (the remainder, in mathematical terms).

The brute force technique takes the initial decimal number and keeps dividing it by 2 until the result is 0, while recording the results of those operations in a special way. The recipe is to divide the number by 2, and to write a 1 if the first number is odd or write a 0 if the first number is even. Repeat the technique on the result of the division until that result is a 0. The following is an example, using the number 147 for which we already know the binary value:

147 divided by 2 is 73 with a remainder of 1

73 divided by 2 is 36 with a remainder of 1

36 divided by 2 is 18 with a remainder of 0

18 divided by 2 is 9 with a remainder of 0

9 divided by 1 is 4 with a remainder of 1

4 divided by 2 is 2 with a remainder of 0

2 divided by 2 is 1 with a remainder of 0

1 divided by 2 is 0 with a remainder of 1

If you write the digits that result from this recipe, starting from the bottom of the list, you get the binary number 10010011 (which we already know is correct). This formula works for any binary number.

The other approach relies on knowledge of the powers of 2. Small decimal numbers—such as those that appear in IP addresses—can be readily obtained from Table C.1. In each case, we look for the power of 2 that is closest to and less than the value we're working on:

147 is between 256 and 128, 128 is less; record 2^7 for 128, then subtract 128 from 147 to get 19

19 is between 32 and 16, 16 is less; record 2^4 for 16, then subtract 16 from 19 to get 3

3 is between 4 and 2, 2 is less, record 2^1 for 2, then subtract 2 from 3 to get 1

1 is precisely 2^0, so record 2^0

Note that this formula indicates that $147 = 2^7 + 2^4 + 2^1 + 2^0$, which precisely matches our earlier calculation after dropping the numbers with zero coefficients.

C.2 Understanding Bit Masks

In computer terms, a bit mask is a pattern of zeros and ones in which the ones in the pattern "block off" bit positions in related binary numbers in a special way. The position of the ones in the mask is called high-order if it runs from left to right, and low-order if it runs from right to left. For example, a 3-bit high-order mask for an 8-bit number is expressed in binary terms as 11100000 (the three leftmost bits are set to 1); a 3-bit low-order mask for an 8-bit number is expressed as 00000111 (the three rightmost bits are set to 1). Converting the first number to decimal, we get $2^7 + 2^6 + 2^5 = 128 + 64 + 32 = 224$; converting the second number to decimal we get $2^2 + 2^1 + 2^0 = 4 + 2 + 1 = 7$. Tables C.2 and C.3 list the values of high- and low-order bit masks for 8-bit binary numbers, respectively. Each table explains a way to calculate the value of such a mask based on its size or value.

TABLE C.2 High-order Bit Masks and Decimal Values

Binary	Decimal	Calculation
10000000	128	2^7
11000000	192	$2^7 + 2^6$
11100000	224	$2^7 + 2^6 + 2^5$
11110000	240	$2^7 + 2^6 + 2^5 + 2^4$
11111000	248	$2^7 + 2^6 + 2^5 + 2^4 + 2^3$
11111100	252	$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2$
11111110	254	$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1$
11111111	255	$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

TABLE C.3 Low-order Bit Masks and Decimal Values

Binary	Decimal	Calculation
00000001	1	$2^1 - 1$
00000011	3	$2^2 - 1$
00000111	7	$2^3 - 1$
00001111	15	$2^4 - 1$
00011111	31	$2^5 - 1$
00111111	63	$2^6 - 1$
01111111	127	$2^7 - 1$
11111111	255	$2^8 - 1$

A general formula for low-order bit masks is $2^n - 1$, where *n* is the number of bits set in the mask.

By becoming familiar with the values in Tables C.2 and C.3, you'll be well-equipped to handle most ordinary IP address calculations, including various forms of address masks often called subnets and supernets. These are discussed in the following two sections.

C.3 Working with Subnet Masks

As discussed in Chapter 7, a subnet permits you to divide an IP address range into a collection of distinct networks, all of which function together as a single routing domain. You use a higher-order bit mask called a subnet mask to steal bits from the host portion of an IP address, which you can then use to create subnetworks within an existing network address.

Here's what's involved in creating a subnet mask, in recipe form:

1. Calculate how many subnets are needed and add 2 to that number: one for the underlying network address, the other for a broadcast address.
2. Jump to the next highest power of 2. For example, if you need four subnet masks, adding 2 creates a value of 6. The nearest next highest power of 2 is 8, or 2^3, where the 3 tells you how many bits you need for your subnet mask.

3. Use a high-order bit mask to block off space for these subnetworks. The mask that meets a need for four subnetworks is therefore 11100000, or 224.
4. Check your work. Analyze the number of bits in the host portion of the address to make sure enough host addresses remain usable (if *h* is the number of bits in the host portion, $2^h - 2$ defines the number of usable host addresses). For a 3-bit subnet mask, the number of hosts on each subnet is $2^5 - 2 = 30$.
5. If n is the number of bits in the subnet mask, remember that $2^n - 2$ represents the number of usable subnets that result from this mask (here again, the all-zeros version of this address is needed to address all subnets as a whole, and the all-ones version to broadcast to them as a group). For a 3-bit subnet mask, that number is $2^3 - 2 = 6$.

Here is another example that will help you understand this process:

1. MegaInc needs nine subnets for a Class C address of 196.24.24.0, and each subnet must be able to accommodate 12 host addresses.
2. Add 2 to the number of subnets (9) to get 11. The nearest power of 2 is 16 or 2^4, which dictates a 4-bit mask. Four bits are left over for the host portion, which equates to 14 hosts per subnet. That number meets MegaInc's host addressing requirements.
3. Adding to the default Class C mask address of 255.255.255.0, we use the 4-bit high-order decimal value to extend that mask. Because a 4-bit mask produces a value of 240, this makes the complete subnet mask 255.255.255.240.

A more complex example that partitions a bigger address helps to show the power of subnet masking. Let's apply this example to Picture This!, a company with multiple locations around the world that uses a Class B address:

1. Picture This! wants 240 subnets for its Class B address of 168.32.10.0. No subnet needs more than 200 host addresses.
2. Add 2 to the host and subnet portions of the address to get 242 subnets and 202 hosts. The nearest higher power of 2 for 242 is 256, or 8 bits. This leaves 8 bits for the host portion, which meets the company's host addressing requirements.

3. Reserving 8 bits in the final 16 bits of the IP address creates a subnet mask of 11111111 00000000. In decimal terms, this is 255.0, so the default Class B subnet mask of 255.255.0.0 turns into 255.255.255.0 to meet requirements as stated. In fact, this basically breaks a single Class B address into 253 Class C addresses.

To learn more about this fascinating subject, visit your favorite search engine and searching for "IP subnetting tutorial". A recent visit to Google turned up more than 150 hits on this query.

C.4 Working with Supernet Masks

Subnets steal bits from the host portion of an IP address to subdivide that address space into logical subnetworks. Supernets go the other way. By concatenating multiple IP network addresses (which must be in sequence and fit the dictates of the bit patterns they'll attempt to use), they permit host address space to be extended so that bits "stolen" from the network portion of the address are "given" to the host portion of the address. This has the nice side effect of modestly increasing the total number of hosts that may be addressed, because the number of all-zeros network addresses and all-ones broadcast addresses that must be preserved is reduced as host address size increases. (It works out to about 1% of overall address space.)

When combining addresses to create supernets, the number of addresses required corresponds to the low-order bit mask patterns shown in Table C.3. The caveat is that the number of addresses required is the value of 2^n, where n is the number of bits to be used. (Two bits' worth of supernet mask requires $2^2 = 4$ sequential addresses.) Calculating supernets is similar to calculating subnets, except that bits come from the low end of the mask rather than the high end. Here's what this means:

- To use 3 bits of network address for host addressing, you need to reserve the 3 low-order bits in an address range. Because $2^3 = 8$, you need eight contiguous addresses to do this.
- If you're extending a Class C address, the resulting host address now covers 11 bits rather than 8. The resulting subnet mask (it's still called that, even though you're supernetting) is 255.255.248.0 instead of 255.255.255.0 because you've reduced the number of bits in the network portion of the third octet by 3 bits.

- You can calculate supernet masks in one of two ways:
  - You can work from the bit pattern. For the preceding example this produces 11111000, which translates to 248.
  - You can recognize that $2^3 - 1 = 7$ and subtract that value from 255 to get 248. (This only works because it's a low-order bit mask that borrows from the bottom up, as it were.)

  Note that each of the eight Class C addresses that you're combining can address 254 hosts ($2^8 - 2$), for a total of 2,032 hosts. By combining them into a single address range, it can address $2^{11} - 2 = 2{,}046$ hosts. This produces a modest increase of 16 hosts overall.

C.5 Modern IP Addressing

Although it's still helpful to describe IP addresses as Class A, B, or C, modern Internet addressing uses a different type of notation called CIDR addressing. In CIDR addressing, an IP address is followed by notation that looks like /n, where n is typically a number between 4 and 20. This notation simply identifies the number of bits in the network (leftmost) portion of the address, so that you can calculate the number of bits in the host portion by subtracting that value from 32 (or 5, for the /27 example just stated).

Everything explained about subnetting and supernetting works for CIDR addresses, except that network and host portions seldom fall on octet boundaries. This requires a bit more mathematical sophistication and practice to master, but works according to all the rules explained herein.

APPENDIX D

IP Tools and Software

This appendix includes several IP-related tools, utilities, and software. They should become an essential part of your networking toolkit.

D.1 Command Prompt IP Utilities

D.1.1 Ipconfig

Ipconfig displays the MAC address of your computer (the physical address of your NIC), and displays your IP address, subnet mask, and default gateway or the DNS server address.

Syntax

ipconfig /? | /all | /release [*adapter*] | /renew [*adapter*] | /flushdns | /registerdns | /showclassid *adapter*

| /setclassid *adapter* [classidtoset]

For more information about Ipconfig and an explanation of the parameters, type **ipconfig /help** at a command prompt.

D.1.2 Tracert

Tracert (aka Traceroute) tracks the path a packet takes to get to its destination, measuring how long it takes to travel through each hop to get to its target. Tracert uses an ICMP echo request packet to find the path.

Syntax

tracert [-d] [-h *maximum_hops*] [-j *host_list*] [-w *timeout*] *target_name*

For more information about Tracert and an explanation of the parameters, type **tracert** at a command prompt.

D.1.3 Ping

Ping uses the ICMP echo function. A small packet containing an ICMP echo message is sent through the network to a particular IP address. The computer that sent the packet then waits for a return packet. If the connections are good and the target computer is up, the echo message return packet will be received. It is one of the most useful network tools available because it tests the most basic function of an IP network. It also shows the TTL value and the amount of time it takes for a packet to make the complete trip, also known as round trip time (RTT).

Syntax

ping [-t] [-a] [-n *count*] [-l *size*] [-f] [-i *TTL*] [-v *TOS*] [-r *count*] [-s *count*] {[-j *host-list*] | [-k *host-list*]}

[-w *timeout*] *destination-list*

For more information about Ping and an explanation of the parameters, type **ping** at a command prompt.

D.2 Networking Tools and Utilities

- Advanced Checksum Verifier: *http://www.irnis.net/soft/acsv*
- Download a free error-checking utility that verifies the integrity of your files via the CRC32 or MD5 algorithms.
- Whois: *http://www.whois.com*

Search for a domain name before you register.

D.2.1 Antivirus Software

- Symantec: *http://www.symantec.com/avcenter/index.html*
- McAfee Security: *http://us.mcafee.com/*

- Sophos: *http://www.sophos.com/*
- F-Prot: *http://www.f-prot.com*

The preceding list offers both shareware and retail versions of popular, downloadable antivirus software packages.

- McAfee FreeScan: *http://www.McAfee.com*

Click the Scan Now link to run a thorough check of your computer for viruses.

D.2.2 Synchronized Time Services

- U.S. Naval Observatory Time Service Department: *http://tycho.usno.navy.mil/frtime.html*
- NIST Internet Time Service: *http://www.boulder.nist.gov/timefreq/service/its.htm*

Both of these URLs offer synchronized time services to help you maintain accurate global time across your network.

D.2.3 Hardware Addresses

- IEEE OUI and Company ID assignments: *http://standards.ieee.org/regauth/oui/index.shtml*. IEEE offers a downloadable list of organizationally unique identifiers (OUIs) and an OUI search engine.
- Vendor/Ethernet MAC Address Lookup and Search: *http://www.coffer.com/mac_find/*. Jason Coffer provides a search engine for looking up vendors of Ethernet hardware.

D.3 Analyzers

D.3.1 Computer and Network Analyzers

- Microsoft Baseline Security Analyzer (MBSA): *http://www.microsoft.com/technet/security/tools/mb5ahome.mspx*. This Microsoft tool scans your computer for missing security updates and service packs.
- Microsoft Network Monitor: *http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_NETMNintro.htm*

- Novell LANalyzer: *http://www.novell.com*

Microsoft Network Monitor and Novell LANalyzer are a combination of network monitors and network analyzers. The URLs listed provide information about their features and functions.

- SLAC Network Monitoring Tools: *http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#nmp*
- Monitoring Software: *http://www.monitoring-software.net/network-monitoring-software.htm*

Both SLAC and Monitoring Software provide links to shareware and commercial versions of tools for network monitoring, Internet monitoring, intrusion detection, and more.

D.3.2 Protocol Analyzers

- Wildpackets EtherPeek: *http://www.wildpackets.com*
- Ethereal: *http://www.ethereal.com/*

Both WildPackets and Ethereal offer free, downloadable protocol analyzers.

APPENDIX E

Glossary

4B/5B encoding: A scheme that takes data in 4-bit codes and maps it to corresponding 5-bit codes.

4D-PAM5 encoding: Stands for 4-dimensional, 5-level pulse amplitude modulation. This is a way of encoding bits on copper wires to get a 1 GB per second transfer rate by employing a five-level signal called pulse amplitude modulation 5.

802.1x: A standard that governs internet working and link security. It governs authentication mechanisms for both wired and wireless technologies.

8B/6T encoding: An encoding scheme in which the value of the data byte is compared to the values in the 8B/6T table. The remapping table has nine symbols used for starting and ending delimiters and control characters.

8B/10B encoding: An encoding scheme in which 8-bit binary data values are represented by 10-bit symbols. The data octet is split up into the three most-significant bits and the five least-significant bits.

A

acceptable use: Defines the proper use of an information system and the data it contains.

ad hoc: A wireless network setup between clients without using a WAP.

addressing: A method of identifying network-connected equipment with a unique value.

Address Resolution Protocol (ARP): A protocol used by IP Network layer protocols to map IP network addresses to the hardware addresses used by a Data Link protocol.

all routes explorer (ARE): A frame used to discover the best path to a client in source route bridging networks.

ALOHA: One of the earliest multiple access schemes. It allows network stations to access the channel whenever they have data to transmit, but each station must add a checksum at the end of its transmission to allow the receiver to recognize whether the frame was properly received.

amplitude modulation (AM): The encoding of a carrier wave by the changes of its amplitude along with the changes in input signal.

analog signal: Adds information or encodes information to an AC base signal by modifying the frequency or signal strength.

ANDing: The process of adding the subnet mask to an IP address to determine the network ID.

AppleTalk: The protocol suite used to interconnect Macintosh computers. It is designed to be a flexible, simple, and inexpensive network means for connecting computers, peripherals, and servers.

Application Configuration Access Protocol (ACAP): A protocol to store and retrieve client-specific configurations from a server for mobile clients.

Application layer: Layer 7 of the OSI reference model. This layer provides services to application processes to ensure that effective communication with other application programs is possible.

application-specific integrated circuit (ASIC): A hardware circuit with embedded code used in switching.

arbitrated loop (AL): A Fibre Channel configuration that creates a multipoint configuration between a maximum of 127 nodes.

area border router (ABR): An OSPF-configured router that borders more than one area.

ARP cache: A small portion of memory used on a client to store the ARP table.

ARP table: A table that maintains the association between an IP address and a corresponding MAC address.

asynchronous communication: Communication that is not synchronized or kept in check with a clocking mechanism between communication devices.

Asynchronous Transfer Mode (ATM): A communications services technology that provides a common format for services with high bandwidth requirements, such as video conferencing and video on demand. ATM supports transmission rates up to 9953 Mbps.

attachment unit interface (AUI): A transceiver cable between the medium access unit (MAU) and the data terminal equipment.

auditing: The process of tracking users and then actions, and other events, on a network.

autonomous system (AS): A collection of routers under common administrative authority or control.

autonomous system border router (ASBR): A router that borders an area not in the same autonomous system (usually the Internet).

B

backbone: A single cable segment used in a bus topology to connect computers in a straight line.

backbone router: An OSPF router with at least one interface in the backbone (Area 0).

back door: A program that allows access to a computer without the user's knowledge or authorization.

backleveling: The process used to roll back or reverse an upgrade or change.

bandwidth: A measurement of how much information can be transmitted over a medium over a prescribed period of time.

base station (BS): A special fixed node on a network. It is located in a central location for use on a wireless or cellular network.

baseline: A measure of normal network activity.

benchmarking: The process of determining how much load the server can handle by comparing two or more systems or components of a system.

binding: The process of linking network components on different levels to enable communication between the components.

blackouts: Caused by faults on the utility power system, they are a complete loss of utility power.

blocking: A state on a bridge or a switch where traffic is not passed to or from the port.

Bluetooth: An open standard of wireless communications that allows communications between devices from different vendors.

Boot Protocol (BootP): A protocol used to assign IP address and IP configuration information to IP hosts.

Border Gateway Protocol (BGP): An industry-standard EGP used to maintain routing tables for the Internet.

borrowing: The process of extending the subnet mask into the host portion of a network address.

bottleneck: Occurs when too much data is pushed into a narrow opening, causing it to jam.

bridge: A device that connects two or more segments of a network to make them one.

bridge ID: A two-part ID consisting of bridge priority and MAC address.

bridge priority: A 2-byte user-configurable field that provides administrators control over which bridge becomes the root.

broadcast: A frame that has a Layer 2 MAC address of all Fs.

broadcast address: The last available address for a given network address range. This address can be identified when all host bits set to 1.

broadcast domain: A group of network devices that are capable of receiving each other's broadcast packets.

brute force: Term used that describes a way of cracking a cryptographic key or password by trying every conceivable combination until a password is found, or until all possible combinations have been exhausted.

buffering: The act of temporarily storing data in memory while waiting for access to the media for further processing.

buffer overflow: Condition that occurs when the data presented to an application or service exceeds the storage space allocation that has been reserved in memory for that application or service.

bus: A major network topology in which the computers connect to a backbone cable segment to form a straight line.

business continuity plan (BCP): A plan that takes a long-term look at recovery in the case of a complete loss of facilities.

busy-tone multiple access (BTMA): An access method designed for station-based networks, it divides a channel into a message channel and a busy-tone channel.

C

cable checker: Device that determines whether your cabling can provide physical connectivity.

cable tester: A device that determines whether your cabling can provide physical connectivity. It operates at higher layers of the OSI model and provides more detailed information than a cable checker.

capture-division packetized access (CDPA): An alternative to systems based on bandwidth subdivision methods such as TDMA, FDMA, and CDMA. In CDPA there is no subdivision of bandwidth.

carrier sense multiple access (CSMA): A fundamental advance in network access, it checks whether the medium is active before sending a packet; that is, it listens before it transmits.

carrier sense multiple access with collision avoidance (CSMA/CA): Designed to prevent collisions at the moment they are most likely to occur. All nodes are forced to wait for a random number of timeslots and then check the medium again before starting a transmission.

Carrier sense multiple access with collision detection (CSMA/CD): A method used in Ethernet that allows clients to access to the medium. Clients must listen for a carrier signal before transmitting and must then listen for collisions.

certificate: A digital document that attests to the truth that you are who you say you are. Besides providing authentication, a certificate also secures the exchange of information.

certification authority (CA): An organization or service that issues and manages security certificates.

checksum: A simple error-detection scheme whereby each message is accompanied by a value based on the number of bits in the message.

cipher: The process of replacing letters or numbers with different characters. The letters can also be rearranged without changing their identities to form an enciphered message.

classful routing: The process of routing using the default mask based on the class of the address rather than the actual network mask.

classless inter-domain routing (CIDR): A function of network devices where routing takes place using the full network ID and not the classful address boundary.

client: A computer on a network that requests resources or services from some other computer.

code division multiple access (CDMA): An access method that combines spread-spectrum technology with analog-to-digital conversion. After the data is digitized, it is spread out over the entire bandwidth available.

collision: Refers to when two network stations attempt to communicate at the same time and the signals crossover each other on the wire.

collision domain: All networking clients with the potential to send signals and have them collide are said to be in the same collision domain.

converged: The state at which all routers have a complete set of entries for the network.

convergence: The process of routing updates involved when a change occurs in the routing environment. Convergence can refer to the process or the time it takes to reach a converged state.

cooperative multitasking: A form of multitasking in which the operating system has no control over the processes. The operating system transfers control to the application. Once an application process has control of the CPU, it cannot be interrupted.

crossbar switch: A device that directly switches data between any input and any output port, without sharing a bus with other data.

crossover cable: Cable that looks like an ordinary twisted-pair cable, but with two wires crossed, making the cable able to directly connect two computers without using additional equipment.

cut-through switching: A type of switching method where the switch forwards packets as soon as the 6-byte destination MAC address is received.

cyclic redundancy checking (CRC): A sophisticated method of error-checking that is based on algebra. It is substantially reliable in detecting transmission errors and is commonly used in modems.

D

Data Encryption Standard (DES): A block cipher using a 56-bit key on each 64-bit chunk of data used to encrypt data.

datagram: A packet that consists of a header, data, and a trailer.

Datagram Delivery Protocol (DDP): An AppleTalk Network layer protocol used to connect more than one network.

Data Link Connection Identifier (DLCI): A method of identifying multiple virtual circuits in a Frame Relay network.

Data Link layer: Layer 2 of the OSI reference model. This layer packages raw bits from the Physical layer into logical, structured data packets.

DECnet: A proprietary network protocol designed by Digital Equipment Corporation.

decryption: The act of converting a message from code into plaintext.

default gateway: An entry on a host or in a route table used when a destination address is unknown. Frames not matching any entries in the route table are forwarded to the default gateway.

default route: A routing table entry used when a destination address is unknown. Frames not matching any entries in the route table are forwarded to the next hop identified by the default route.

delay: *See* latency.

denial of service (DoS) attack: A type of attack that disrupts the resources or services to which a user expects to have access.

designated port: In a looped bridge or switch environment, this is the port that is designated to forward traffic for a given segment. All other switches on that segment will filter all client traffic.

designator: Exchanges a locally mapped drive letter with the correct network address of a directory share.

Digital Network Architecture (DNA): A layered network architecture that supports standard and proprietary protocols.

digital signal: Uses steps to represent information in binary format as zeros (0s) or ones (1s).

directory service: A database of service names and addresses that exists on a network.

disaster recovery plan (DRP): A plan that aims to restore essential computer and network functions shortly after a disaster strikes.

distance vector: A simple routing protocol where the best route decision is based on hop count.

distributed denial of service (DDoS) attack: Attacks that come in the form of the standard DoS attack but the effects of which are multiplied by the total number of computers under the control of the attacker.

Domain Name System (DNS): Used to resolve the names typed into a Web browser and match them to a proper network address.

driver: A program that interacts with either a particular device or type of software. It contains specific information about a device or a software interface that programs using the driver do not.

Dual-Attached Concentrator (DAC): A network node in FDDI that is attached to both rings and can wrap the ring in case of a primary ring failure. It is also responsible for connecting end-nodes to the FDDI ring.

Dual-Attached Station (DAS): A network node in FDDI that is attached to both rings and can wrap the ring in case of a primary ring failure.

dual-homed: A network node in an FDDI network that is attached to two DACs.

due care: The knowledge and actions that a reasonable and prudent person would possess or act upon.

duplexing: Refers to the transmission of packets. Half-duplexing transmits packets in one direction only. Full duplexing transmits packets in two directions simultaneously.

Dynamic Host Configuration Protocol (DHCP): Enables individual computers to automatically obtain their network configurations from a server rather than be manually configured.

E

egress port: The designated outbound port for a given frame.

encapsulation: The process of packaging upper-layer protocol information and data into a frame.

encoding: The process of putting electronic data into a standard format.

encryption: Transformation of data into a form that cannot be read without the appropriate key to decipher it.

error checking and correcting (ECC): A more sophisticated form of checking where errors are corrected when they are detected. Also known as error-correction code.

Ethernet: A Layer 2 networking protocol used for delivering frames between two network interface cards. Network access is achieved through CSMA/CD.

Ethernet II: A modification of the original Ethernet standard. Ethernet II uses a Type field instead of an LLC field.

Ethernet raw: A Novell proprietary implementation of the original Ethernet I standard. It does not use an LLC field.

Ethernet SNAP: An extension of the Ethernet I specification that allows for more service access points.

Event Viewer: A Windows-based tool that maintains log files and allows you to audit certain events.

Extensible Markup Language (XML): A markup language for documents containing structured information.

Exterior Gateway Protocol (EGP): An early industry-standard exterior protocol replaced by BGP.

exterior gateway protocols (EGPs): A classification of protocols used to create and maintain routing tables and routing policy on the Internet.

F

fabric: A Fibre Channel configuration that creates a multipoint configuration between an infinite number of nodes. It requires a special switch.

Fiber Distributed Data Interface (FDDI): A Layer 2 protocol similar to Token Ring. It uses token passing for media access and a dual-ring topology for redundancy.

Fibre Channel: A Layer 2 networking protocol used to create a channel between communicating nodes.

File Allocation Table (FAT): A file system used by DOS and supported by all other DOS- and Windows-based operating systems. It is simple, reliable, and uses little storage.

file system: Describes the operating system's method of organizing, managing, and accessing of files through logical structuring of the hard disk.

File Transfer Protocol (FTP): Allows a person to transfer files between two computers.

filtering: The process of reading information in a packet, such as the destination address, and either forwarding or dropping the packet based on that information.

firewall: A component placed between computers and networks to help eliminate undesired access by the outside world.

flooding: When a bridge receives a broadcast, multicast, or a packet with an unknown destination and copies the packet to all ports except the port of entry.

flow control: A method by which the data flow between devices is managed so that the data can be handled at an efficient pace.

forwarding: The process that a bridge uses when copying a frame from one port to another using a known destination MAC address.

fragment-free switching: A form of switching used instead of cut-through to eliminate forwarding collision fragments. The packet is forwarded after the 64th byte of data is received.

Frame Relay: A packet-switched WAN technology whereby bandwidth is shared among subscribers.

frequency division duplex (FDD): Uses different frequency bands for uplink and downlink.

frequency division multiple access (FDMA): Provides multiple and simultaneous transmissions to a single transponder.

frequency division multiplexing (FDM): A method of transmission in which numerous signals are combined on a single communications line or channel.

frequency modulation (FM): The method of encoding data onto an AC wave by changing the instantaneous frequency of the wave.

full-duplex: A transmission method whereby data can be transmitted in both directions on a signal carrier at the same time. Full-duplex transmission implies a bidirectional communications (one that can move data in both directions).

G

giant: A frame that is larger than the defined current protocol and media.

group: Contains users who share a common need for access to a particular resource.

group-based access control: A type of access control in which permissions are assigned to groups, and user accounts become members of the groups. Each user account has access based on the combined permissions inherited from its group memberships.

Group Policy object (GPO): A virtual storage location for Group Policy settings used to apply Group Policy to users and computers.

H

half-duplex: A transmission method whereby data can be transmitted in both directions on a cable, but not at the same time.

hand-off point (hop): The next Layer 2 destination in an end-to-end Layer 3 communications path or route.

Hardware Compatibility List (HCL): A manufacturer list that details compatible hardware for operating systems.

hashing: The process of transforming a string of characters into a shorter fixed-length value or key that represents the original string. Hashing is used in many encryption algorithms.

hello packet: Also known as a heartbeat, a special message (packet) that a router sends out periodically to determine network adjacency relationships.

High-level Data Link Control (HDLC): A Layer 2 WAN protocol used on point-to-point serial links.

High-Performance File System (HPFS): Designed for the OS/2 operating system to allow for greater access to larger hard drives.

hold-down timer: A routing loop prevention mechanism that requires a router to disregard all route advertisements about an offline network until the hold-down timer expires.

home RF: A wireless technology being developed for use with home appliances.

hop: *See* hand-off point.

host: Any system configured with a TCP/IP address, which can include routers, switches, hubs, personal computers, mainframes, Unix systems, or any network-enabled device.

hub: A multiport repeater that retransmits a signal on all ports.

Hypertext Markup Language (HTML): The language used to format pages on the Web.

Hypertext Transfer Protocol (HTTP): A protocol that Web clients and servers use to communicate with each other.

I

Institute of Electrical and Electronic's Engineers (IEEE): A professional engineering organization that defines standards for networking devices, which include network interfaces, cabling, and connectors.

Integrated Services Digital Network (ISDN): A packet-switched digital connection method similar to phone service.

inter-frame gap: The 9.6-microsecond required wait time between the receipt of the last signal and the start of a new signal on an Ethernet network.

interior gateway protocols (IGPs): A family of protocols used to create and maintain routing tables and routing policy inside a company's network infrastructure.

International Organization for Standardization (ISO): An international standards organization responsible for developing a wide range of standards, including many that are relevant to networking, such as the OSI reference model and the OSI protocol suite.

International Telecommunication Union-Telecommunication Standardization Sector (ITU-T): An international organization that develops communication standards. The ITU-T developed X.25 and other communications standards.

Internet Control Message Protocol (ICMP): A part of the Internet layer that uses IP datagram delivery to send messages notifying the sender if something has gone wrong in the transmission process.

Internet Message Access Protocol (IMAP): Allows the client e-mail program to access remote message stored as if they were local.

Internet Protocol (IP): The Network layer protocol that's part of the TCP/IP suite.

Internet service provider (ISP): An organization that provides Internet access to customers, primarily as a paid service.

Internetwork Packet Exchange (IPX): A connectionless datagram-based Layer 3 (Network) protocol of the IPX/SPX suite that is used to route packets through networks.

interworking function (IWF): Provides the necessary protocol conversions so that wireless data users can continue to access existing network-wired applications without requiring modifications to the applications.

IP Security (IPSec): A set of protocols operating at the Transport layer that support the secure exchange of packets.

IP version 4 (IPv4): An abbreviation for Internet Protocol version 4. A widely deployed suite of protocols used in network communications. IPv4 is the most commonly deployed network communications protocol in the world today.

IP version 6 (IPv6): An abbreviation for Internet Protocol version 6. The newest version of the IP protocol that uses expanded features and addressing to overcome the limitations of version 4.

J

jitter control: A process that ensures that traffic travels through a network smoothly.

K

kernel: The core program component of an operating system.

L

LANalyzer: A complete monitoring and analysis tool for troubleshooting Novell networks. It monitors the network for anomalous events and can decode and support various protocols.

late collision: A collision that occurs after the first 64 bytes of data have been transmitted.

latency: Delay associated with the transmission, retransmission, or processing of network frames.

learning: When a bridge or switch adds an address to its forwarding table.

link state: Complex type of routing protocol that uses advanced logic to determine the best path to a given network.

listening: A phase used on a bridge or switch port that allows it to send BPDU traffic.

load shedding: Process of systematically reducing the system demand by temporarily decreasing the load in response to transmission or capacity shortages.

Local Access and Transport Area (LATA): A geographic zone supported by a single telephone service provider.

local area network (LAN): A group of devices under common administrative control, connected at high speed, and located close together.

Logical Link Control (LLC): A Layer 2 protocol defined by IEEE 802.2 and used in other protocols such as Ethernet and Token Ring.

Logical Link Control (LLC) layer: Sublayer of the Data Link layer that manages communications between devices over a single link. This layer includes error checking and flow control.

loopback adapter: A way to test the ports on a system without having to connect to an external device.

M

MAC address: The unique hardware or physical address of a hardware device. Manufacturers assign MAC addresses to hardware devices.

malware: A shortened version of the words "malicious software." It is software designed with the intent to damage or disrupt a system.

Manchester encoding: A synchronous clock encoding technique used to encode the clock and data of a synchronous bit stream. It uses the rising or falling edge in the middle of each bit time to indicate a zero (0) or one (1).

man-in-the-middle attack: An attack that takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

maximum transmission unit (MTU): The maximum frame size allowed to travel through a network, using a given protocol and media type.

Media Access Control (MAC) address: A unique physical address, also called a hardware address, that all NICs have.

Media Access Control (MAC) layer: A sublayer of the Data Link layer that manages protocol access to the physical network medium.

mesh: A hybrid network topology used for fault tolerance in which all computers connect to each other.

metric: The method or measurement used by a routing protocol that determines the best path to a given network.

metropolitan area network (MAN): A group of LANs connected using WAN and LAN technologies but limited in distance to a metropolitan area or LATA.

middleware: Software that connects applications, allowing them to exchange data.

Multi-Level Transition-3 encoding (MLT-3): A three-level form of data encoding used to concentrate the signal power below 30 MHz.

multiple access: Allows more than one device to communicate.

multiple access collision avoidance (MACA): A multiple access method that attempts to detect collisions at the receiver by establishing a request-response channel of communication between the sender and receiver.

multiplexing: Refers to sharing a communications line. It combines several connections into one larger channel.

multipoint: A network configuration that involves multiple network nodes or end points.

Multipurpose Internet Mail Extensions (MIME): The standard that defines the format of text messages.

Multistation Access Unit (MAU): A device used to attach clients to a Token Ring network.

N

naming convention: The process by which names are created for the workstations and servers on a network.

NetBIOS Extended User Interface (NetBEUI): Specifies the way that upper-level software sends and receives messages over the NetBIOS Frames Protocol (NBF). It has become an industry standard.

NetWare Core Protocol (NCP): One of the core protocols of the IPX/SPX suite. NCP handles requests for services, such as printing and file access, between clients and servers.

network: A group of computers that can communicate with each other to share information and resources.

network address translation (NAT): The process of replacing the source or destination network address in a frame with a valid address.

network analyzer: Also called a protocol analyzer, a hardware-based tool that a network administrator connects to the network expressly to determine the nature of more complex network problems.

Network Basic Input/Output System (NetBIOS): Developed in 1983 for International Business Machines Corporation (IBM) to allow applications on different computers to communicate within a local area network.

Network Device Interface System (NDIS): A communication interface between the MAC sublayer and the network interface driver that allows Windows operating systems to communicate multiple protocols to the NIC.

network ID: The number of bits (determined by the subnet mask) of an IP address that identify a client's network address.

Network layer: Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two systems. This is the layer at which routing occurs.

network medium: Refers to the cable (metallic or fiber-optic) that links computers on a network. Because wireless networking is possible, it can also describe the type of wireless communications used to permit computers to exchange data via some wireless transmission frequency.

Network Monitor: A protocol-analysis tool that captures network traffic and generates statistics for creating reports.

network operating system (NOS): Acts as a director to keep a network running smoothly, and is a complete operating system in addition to managing communication across a LAN.

Network Services Protocol (NSP): A connection-oriented protocol developed by Digital to manage flow control, segmentation, and reassembly functions.

New Technology File System (NTFS): Developed expressly for versions of Windows NT and Windows 2000 as a platform for added functionality, reliability, and security features.

noise: Also referred to as EMI and RFI, it can be caused by lightning, load switching, generators, radio transmitters, and industrial equipment.

Non-Return to Zero (NRZ) encoding: Uses two levels of signaling or is bipolar. The two levels or states can be expressed as either on or off, or high or low.

O

Open Data-Link Interface (ODI): Similar to NDIS except that it supports Novell and Apple operating systems. It allows these operating systems to communicate multiple protocols to the NIC.

Open Shortest Path First (OSPF): An industry-standard link state protocol.

Open Systems Interconnection (OSI) reference model: A hierarchical, seven-layer abstract structure of communications between application processes running in computer systems.

optical time domain reflectometer (OTDR): An advanced diagnostic tool for optical fibers that allows you to take a snapshot of a fiber link and accurately measure various statistics.

oscilloscope: An instrument that can detect shorts, crimps, or attenuation in a cable. It displays its output in a graphical format.

over-subscription: A condition that exists when a network device is too slow or has too little memory for the current traffic load. The result is dropped packets.

P

packet: A small segment of a data stream message transmitted over a packet-switched network. A packet contains the destination address in addition to the data.

parity check: Ensures that when data is transmitted from one device to another or stored locally, there is a means to recover lost transactions.

path cost: The cost of a link between two bridges or switches. It is determined by dividing 1,000 Mbps by the speed of the link.

peer-to-peer: A type of networking in which each computer can be a client to other computers and act as a server as well.

Performance console: A Windows-based tool used for properly monitoring the physical disks, memory, and processor along with other services.

permanent virtual circuit (PVC): A circuit path defined in software for the delivery of packets between two end points. The circuit is up even when no data is being sent.

phase-shift modulation (PSM): Conveys digital signals by shifting phases.

Physical layer: Layer 1 of the OSI reference model. It defines mechanical, functional, procedural, and electrical aspects of networking. It includes connectors, circuits, voltage levels, and grounding.

PING: An ICMP echo function used to test network connectivity.

plain old telephone system (POTS): The public telephone system, also known as public switched telephone network (PSTN).

point-to-point: A network configuration involving only two nodes.

Point-to-Point Protocol (PPP): A newer protocol that does essentially the same thing as SLIP but has extra features, such as error detection and IP address negotiation.

poisoning: A routing loop prevention technique where the route metric is set above the allowed maximum in the route advertisement.

polling: A process in which the master broadcasts a query to every node on the network, asking each node in turn whether it has anything to communicate.

port address translation (PAT): The process of replacing the source or destination network and port address in a frame with a valid address and port number.

Post Office Protocol 3 (POP3): The current version of a protocol used to retrieve e-mail from a mail server.

preemptive multitasking: The process whereby the operating system assigns CPU time slices to processes. After each time slice expires, the process is halted and the next process gets computing time.

Presentation layer: Layer 6 of the OSI reference model. It translates data from the Application layer into an intermediary format, provides services such as data encryption, and data compression.

Pretty Good Privacy (PGP): Encrypts and decrypts e-mail messages based on public-key encryption and provides for digital signatures.

Privacy-Enhanced Mail (PEM): One of the first standards for securing e-mail messages by encrypting 7-bit text messages, it specifies a PKI for key exchange over large networks.

private IP addresses: A set of three ranges of IP addresses defined by RFC 1918 that allows companies to use TCP/IP addressing and configuration without having valid public addresses. The ranges are defined as 10.0.0.0 /8, 172.16.0.0 /20, and 192.168.0.0 /16.

propagation delay: The delay an electronic signal experiences when transmitted between two end points.

protocol data unit (PDU): A defined amount of data that can be transmitted using the current protocol and media.

protocol: A set of rules and conventions that specifically governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.

proxy aware: Software applications that can be configured to use a proxy server.

public-key cryptography: Uses different keys to encrypt and decrypt data. The public key is readily available whereas the private key is kept confidential.

Public Key Infrastructure (PKI): A set of standards and protocols that allows data to be transported with strong authentication and privacy on the Internet.

public switched telephone network (PSTN): *See* plain old telephone system (POTS).

pulse code modulation (PCM): Transmits analog data using a digital scheme.

pure ALOHA: A multiple-access scheme that allows stations access to a communications channel whenever the stations have data to transmit, but each station must add a checksum to the end of its transmission to allow the receiver to determine whether the frame was properly received.

Q

quality of service (QoS): A standard that specifies the time frame in which data will be delivered after transmission. QoS helps control jitter, latency, and loss for long-distance, high-bandwidth applications.

quantization: Stage that allocates a level to a sample signal. The sampled analog signal can take any value, but the quantized signal can have a value only from a set of half voltages.

R

redirector: Operating at the Presentation layer of the OSI model, its function is to accept requests from applications and determine whether network access is needed.

Redundant Array of Inexpensive Disks (RAID): Organizes multiple disks into a large, high-performance logical disk.

Remote Procedure Call (RPC): A protocol that a program can use to request a service from a program located on another computer on a network without understanding network details.

repeater: A device that regenerates electronic signals so that they can travel a greater distance or accommodate additional computers on a network segment.

reservation ALOHA: A combination of a slot reservation design with slotted ALOHA. This channel allocation scheme divides the channel bandwidth into slot sizes equal to the transmission time of a single packet, assuming that the packet sizes are of constant length.

resources: The files, applications, and hardware that are shared by a server for clients to access.

Reverse Address Resolution Protocol (RARP): A network protocol belonging to the OSI Data Link layer used to resolve a Data Link layer address to the corresponding Network layer address.

ring: Topology consisting of computers connected in a circle, forming a closed ring.

risk assessment: Determines how likely it is that certain scenarios might actually occur.

Rivest-Shamir-Adleman (RSA): Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, this is an encryption and digital signature authentication system that uses an algorithm based on the multiplication of prime numbers.

role-based access control: A type of access control that determines what job functions each employee performs and then assigns access to a system or network based on those functions.

root bridge: The bridge with the lowest bridge ID in the Spanning Tree Algorithm. All traffic forwards along the best path toward the root bridge.

root port: The port with the lowest cost path to the root bridge.

router: A device that passes data among networks.

route summarization: The process of representing a block of networks using a single route advertisement.

routing: The process of forwarding frames from one interface to another based on a Layer 3 network address.

routing information field (RIF): A field used in source route bridging that maintains the correct path that a frame used to traverse a series of Token Ring networks. Token Ring bridges or switches populate this field.

routing information indicator (RII): A field used in source route bridging that identifies the packet as a local frame if set to 0, or a source route frame if set to 1.

Routing Information Protocol (RIP): An industry-standard distance vector routing protocol.

routing loop: A condition that occurs when routers get confused during update operations and cause frames to bounce back and forth between a set of interfaces.

routing table: A table stored in the memory of a router that associates a given destination network with an outbound interface.

runt: A frame that is smaller than the defined minimum size for the protocol and media.

S

sags: Short-term decreases in voltage levels that commonly occur when motors are started up or by faults on the utility power system.

security policy: A set of security controls that dictate the company rules for providing a safe and secure working environment.

self-interference: A process by which a large fraction of the signal energy leaks into the receive path when a node is transmitting data.

separation of duties: The concept that the completion of a task should require more than one person.

Sequenced Packet Exchange (SPX): Resides on top of IPX and is a reliable, connection-oriented protocol that supplements the datagram service provided by IPX. SPX works with IPX to ensure that data is received whole, in sequence, and error-free.

Serial Line Interface Protocol (SLIP): An extremely simple framing scheme for putting IP packets on a serial line.

server: A computer whose job is to respond to requests for services or resources from clients elsewhere on a network.

Service Advertising Protocol (SAP): A protocol in the IPX/SPX suite through which network resources, such as file servers and print servers, advertise their addresses and the services they provide.

service pack: An update to an existing release of an operating system that includes solutions to known problems and other product enhancements.

session hijacking: An attack that takes control of a session between a server and a client.

Session layer: Layer 5 of the OSI reference model. It allows two applications on different computers to establish dialog control, regulates which side transmits, and determines the time and length of the transmission

signaling: Communication of information between network nodes by initiation, transmission, control, and termination of telecommunications signals.

Simple Mail Transfer Protocol (SMTP): A transport protocol for sending e-mail from server to server.

Simple Network Management Protocol (SNMP): An Application layer protocol used to exchange management information between network devices.

Single-Attached Station (SAS): A network node in FDDI attached only to the primary ring.

sliding window: A method of flow control for data transfers. The window is the maximum amount of data that can be sent without having to wait for acknowledgments.

slotted ALOHA: Doubles the efficiency of the ALOHA protocol by completely overlapping packets when they collide so that each packet is retransmitted in a future slot until the transmission is successful.

social engineering: Method of attack that plays on human behavior to obtain private information.

Source Route Bridging (SRB): A type of bridging used on Token Ring networks where the client sends out a special frame used to determine the best path to a given destination.

space-division switching: Single transmission-path routing accomplished using a switch to physically separate a set of matrix contacts or cross-points. Space-division is closely related to the concept of the crossbar switch.

Spanning Tree Algorithm (STA): An algorithm that prevents bridging and switching loops.

spikes: Instantaneous, dramatic increases in voltage that result from lightning strikes or when electrical loads are switched on or off.

split horizon: A routing loop prevention technique that requires a router to disregard route advertisements about routes locally propagated routes.

spoofing: Method of making data appear to come from somewhere other than where it really originated.

stack: A set of network protocol layers that work together. The set of TCP/IP protocols that define communication over the Internet is the most commonly used stack.

Standard Generalized Markup Language (SGML): An international markup standard independent of any software applications, devices, and operating systems.

star: A network topology in which computers connect via a central connecting point, usually a hub.

star bus: A network topology that combines the star and bus topologies.

star ring: A network topology wired like a star that handles traffic like a ring.

stealing: The process of extending the subnet mask into the host portion of a network address.

store-and-forward switching: A standard type of bridging and switching process where the entire frame is received before a forwarding decision is made.

subnet mask: A numeric value that is configured in networking software that gives an IP client the ability to determine the network ID.

subnetting: The process of extending the subnet mask to create multiple networks from one master network ID.

summarization: The process of removing network bits from the subnet mask until a collection of individual networks looks like one large network block (in binary format).

surges: Short-term increases in voltage that are commonly caused by large electrical load changes and from utility power line switching.

switch: A special networking device that manages networked connections between any pair of star-wired devices on a network.

Switched Multimegabit Data Service (SMDS): A subscriber WAN service for connecting networks together over high-speed links.

switched virtual circuit (SVC): A circuit path defined in software for the delivery of packets between two end points. The circuit is up only when there is data ready to be sent.

switching fabric: The combination of hardware and software that transfers data coming into a network node to the appropriate output port on the next node on the network. Switching fabric includes the switches in a node, the hardware that they contain, and the software programs that control switching paths.

synchronous communication: Communication whereby a clocking mechanism keeps events in sync to manage flow of information.

Synchronous Optical Network (SONET): A subscriber WAN service that aggregates multiple signaling types into a single large pipe.

T

Task Manager: A Windows-based tool that can be used to end processes or applications that get hung up or cause the operating system to become unstable.

Telecommunications Network (Telnet): A protocol that provides a way for a client to create a connection and to send commands and instructions interactively to the remote computer.

terminator: A device used to absorb signals as they reach the end of a bus, thus freeing the network for new communications.

threat: In terms of network security, anything that endangers the safety of the network.

time-division duplex (TDD): Multiplexing of the transmission in different time periods but in the same frequency band.

time-division multiple access (TDMA): A digital transmission technology that allows users to access a single radio-frequency (RF) channel without interference by dividing the channel into time slots for each user.

time-division multiplexing (TDM): The process by which multiple data streams are combined in a single signal and transmitted over the same link by allocating a different time slot for the transmission of each channel.

time domain reflectometer (TDR): A device that bounces a signal off the end of a cable and measures the signal's travel time to detect faults in the cable.

time-division switching: Switching of TDM channels by shifting bits between time slots in a TDM frame.

time-slot interchange (TSI): In time-division switching, the process of coordinating time slots between the transmitting station and the receiving station.

time-space switching: A combination of space-division and time-division switching. Time-space switching precedes each input trunk in a crossbar with a TSI, and delays samples so that they arrive at the right time for the space-division switch's schedule.

time-to-live (TTL): A number, assigned to a frame, that is decremented to prevent the frame from circulating through the network infinitely.

token: A packet used in some ring topology networks to ensure fair communications between all computers.

Token Bus: An early definition of a token-passing environment in which systems were wired in a physical bus.

token passing: A method of passing data around a ring network.

Token Ring: A Layer 2 networking protocol used for delivering frames between two network interfaces. Network access is achieved by possessing an electronic token.

tone generator: A device used to perform tests on phone and network lines to help aid in the identification of wires during the wire-tracing process.

topology: The basic physical layout of a network.

Traceroute: An ICMP function used to track the path a packet takes to arrive at its destination. Traceroute was originally developed for the Unix platform.

Tracert: The Windows version of Traceroute.

traffic shaping: Regulates the flow of data across a network by changing bursts of traffic to uniform, regular traffic.

translational bridging: A form of bridging that allows bridging between Ethernet and Token Ring networks.

Transmission Control Protocol (TCP): The Transport layer protocol that's part of the TCP/IP suite.

Transmission Control Protocol/Internet Protocol (TCP/IP): The language of the Internet. This is a suite of protocols that enable packets to be routed across many networks to arrive at their destination.

Transport layer: Layer 4 of the OSI reference model. It helps provide a virtual error-free, point-to-point connection between two hosts so that communication between the hosts arrives uncorrupted and in the correct order.

Trivial File Transfer Protocol (TFTP): A simple form of the File Transfer Protocol, often used for booting or loading programs on diskless workstations.

Trojan horse: A program that disguises itself as a useful application but performs malicious actions, such as deleting data files, when launched.

Truncated Binary Exponential Backoff Algorithm: A mathematical formula used by Ethernet clients after a collision has occurred. It insures that clients do not attempt to communicate at the same time again.

tunneling: Uses one network to send its data through the connection of another network.

U

unicast: A frame addressed directly to a destination host.

Uniform Resource Locator (URL): An electronic address that allows a browser to locate pages.

uninterruptible power supply (UPS): A battery-operated power source that sits between the wall electrical outlet and the computer. In the event of a power failure, it takes over and provides power to the computer.

user account: Holds information about a specific user. It can contain basic information such as name, password, and the user's level of permission.

User Datagram Protocol (UDP): A connectionless datagram service in the TCP/IP suite that does not guarantee delivery and does not maintain an end-to-end connection. It merely pushes the datagrams out and accepts incoming datagrams.

V

variable-length subnet masking (VLSM): The process of creating multiple subnetted networks by using subnet masks that vary in length.

virtual FAT (VFAT): An enhanced version of the FAT file system, this file system is also called FAT32.

virtual local area network (VLAN): A configuration on a switch that groups ports into a single broadcast domain.

virtual private network (VPN): A network connection that allows access via a secure tunnel built on top of a publicly accessible infrastructure, such as the Internet or the public telephone network.

virus: A program or piece of code that is loaded onto your computer without your knowledge.

volt-ohm meter or **voltmeter:** A device used to check physical connectivity or to determine whether a cable is intact by measuring AC and DC voltage, current, resistance, capacity, and cable continuity.

W

wave-division multiplexing (WDM): A form of frequency-division multiplexing specifically for combining many optical carrier signals into a single optical fiber.

Web browser: The client software that allows a user to access and view any document on the Web.

wide area network (WAN): A group of LANs connected over a wide geographic area, at slower speeds than a LAN, and under shared administrative control.

Win32 Driver model (WDM): Architecture that divides drivers into various classes by function. It is a complete card interface that enables generic class drivers to handle bus and device functions.

wire address: The first available address of a given network address range. The address is identified when all host bits are set to 0.

wireless: The ability to transmit data without using wires.

wireless access point (WAP): A device used to connect wireless cards into a managed network.

wireless network: A type of LAN that uses high-frequency radio waves rather than physical connections, such as cables or wires, to communicate between devices.

worm: Generic term for a self-replicating virus, Trojan horse, or logic bomb.

X

Xerox Network Systems (XNS): A suite of protocols created by Xerox in the late 1970s and early 1980s to be used with Ethernet networks.