Direct Sequence Spread Spectrum

Prepared By:
Bud Robinson
Narellan Inc.

Direct Sequence Spread Spectrum

Contents **2**

Direct Sequence Spread Spectrum

Introduction

Businesses of all sizes across the country have developed a strong need for access to the Internet that is high-speed, secure, and reliable. Companies are aggressively searching for new ways to extend their reach, to forge new connections between locations once considered geographically remote. In fact, in the last 5 years, the rate at which technology has moved towards networking, Intranets and the Internet has accelerated exponentially. The drive to connect these "last mile locations" has brought wireless solutions into focus. Due to rapidly advancing technological know-how, a wireless network can, in fact, be implemented to provide high-speed, secure and reliable access. In the aspect of connectivity, a wireless network has quickly become a front-runner solution for remote locations.

There are a number of approaches to the implementation of wireless networks. This paper will review Direct Sequence Spread Spectrum

In reviewing Direct Sequencethis paper first begins with a general explanation of how wireless transmits without errors and the layer of the OSI Model at which this transmission occurs, before providing a detailed analysis of each approach, including the appropriate purposes each serves in the networking world and supporting articles.

General explanation of how wireless devices decide when to transmit

End-user devices, equipped with radio network cards, use a sensing protocol to share the air medium. Devices transmit data only when they detect that there are no others transmitting. For example, the radio card in a handheld PC that needs to send data first senses the air to determine whether another station is transmitting. If the card detects no activity, it transmits a data packet. If it detects signals from another transmitting station, however, the radio card waits until the other station finishes its transmission.

Note:

RF interference occurs when unwanted signals appear to be coming from a legitimate wireless LAN radio card or access point. When this occurs, the interfering signal blocks transmissions on the wireless LAN until it goes away. Even worse, interference that strikes a packet in transit results in errors and retransmissions. This all leads to unhappy users experiencing network delays.

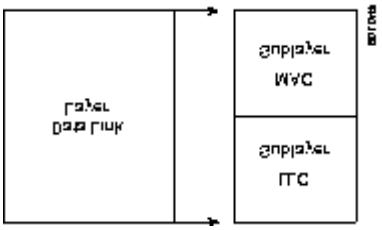
Transmission occurs at the Data-Link Layer in the OSI Model

The data link layer provides reliable transit of data across a local network link.

Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Error notification alerts' upper-layer protocols that a transmission error has occurred*, and the* sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderat*es* the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data-link layer into two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC).

Figure 1-8 illustrates the IEEE sub-layers of the data-link layer.



The Logical Link Control (LLC) sub-layer of the data-link layer manages communications between devices over a single link of a network. IEEE 802.2 defines a number of fields in data-link layer frames that enable multiple higher-layer protocols to share a single physical data link. The Media Access Control (MAC) sub-layer of the data link layer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer. (12).

Defining the Terms:

Spread Spectrum- A modulation technique that spreads a signal's power over a wide band of frequencies. The main reasons for this technique is that the signal becomes much less susceptible to electrical noise and interferes less with other radio-based systems. (16)

Detailed Explanations:

Spread Spectrum Modulation

Modulation, which is a Physical Layer function, is a process in which the radio transceiver prepares the digital signal within the NIC for transmission over the airwaves. *Spread spectrum* "spreads" a signal's power over a wider band of frequencies, sacrificing bandwidth in order to gain signal-to-noise performance (referred to as process gain). This contradicts the desire to conserve frequency bandwidth, but the spreading process makes the data signal much less susceptible to electrical noise than conventional radio modulation techniques. Other transmission and electrical noise, typically narrow in bandwidth, will only interfere with a small portion of the spread spectrum signal, resulting in much less interference and less errors when the receiver demodulates the signal.

In 1985, as an attempt to stimulate the production and use of wireless network products, the FCC modified Part 15 of the radio spectrum regulation, which governs unlicenced devices. The modification authorized wireless network products to operate in the *Industrial, Scientific, and Medical (ISM) bands* using spread spectrum modulation. The ISM frequencies are follows:

- 902-928 MHz
- 2.4-2.4835 GHz
- 5.725-5.850 GHz

The FCC allows users to operate wireless products without obtaining FCC licenses if the products meet certain requirements, such as operation under 1 watt transmitter output power.

This deregulation of the frequency spectrum eliminates the need for user organizations to perform costly and time-consuming frequency planning to coordinate radio installations that will avoid interference with existing radio systems. This is even more advantageous if you plan to move your equipment frequently because you can avoid the paperwork involved in licensing the product again at the new location.

Spread spectrum modulators use one of two methods to spread the signal over a wider area: frequency hopping or direct sequence. We will concentrate on the aspects of direct sequence spread spectrum in the rest of this discussion on Spread Spectrum.

Direct Sequence Spread Spectrum

Direct sequence spread spectrum combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a *chipping code* (also known as *processing gain*). A high processing gain increases the signals resistance to interference. The minimum linear processing gain that the FCC allows is 10, and most commercial products operate under 20. The IEEE 802.11 Working Group has set their minimum processing gain requirements at 11. In comparison to frequency hopping, direct sequence can achieve much higher than 2 Mbps data rates. Direct sequence spread spectrum sends a specific string of bits for each data bit sent.

A chipping code is assigned to represent logic 1 and 0 data bits. As the data stream is transmitted, the corresponding code is actually sent. For example, the transmission of a data bit equal to 1 would result in the sequence 00010011100 being sent.

Characteristics of DSSS:

- Highest potential data rates from individual physical layers
- Smallest number of geographically separate radio cells due to a limited number of channels.
- Direct sequence, has a high potential for data rates, which would be best for bandwidth intensive applications (13)

DSSS basics and operation

A DSSS transmitter operates on an incoming data stream of a certain bit rate (bps). The incoming bit stream is typically converted into a symbol stream where each symbol represents a group of 1, 2, or more bits. Modulation techniques similar to those used in voice-band data modems are used to operate on the symbol stream and generate the transmitted signal. The DSSS transmitter modulates or multiplies each data bit or symbol with a pseudo random noise (PN) sequence that is also called a "chip" sequence. This multiplication provides the spreading phenomena.

To understand the DSSS modulation process consider an example. Lucent's WaveLAN products use DQPSK (differential quadrature phase shift keying) modulation and the draft IEEE 802.11 standard also specifies DQPSK. In a QPSK or DQSP modulator, symbols are differentiated by the phase of a sinusoidal wave. Each symbol can be represented by a point in a symbol constellation plotted on a standard Cartesian graph. The so-called I (in-phase) and Q (quadrature phase) axes of the graph actually represent the cosine and sine of the phase angle respectively.

At the receiver, the implementor has the choice of using DQPSK or QPSK detection. In a DQPSK (also called a non-coherent QPSK) design, the receiver uses the

previous phase as a reference to detect the current symbol. Coherent QPSK receivers, meanwhile, include PLL-based, carrier-recovery circuits. A QPSK receiver design is slightly more complex than a DQPSK design and offers a 3-dB advantage in detection efficiency. A typical QPSK implementation such as Lucent's codes two bits in each symbol. The constellation for this implementation consists of four symbols each separated by 90 degrees. The constellation points are actually at 45, 135, 225, 315 degrees -- each at constant amplitude -- and each represents a two-bit symbol (00, 01, 10, 11). The phase spacing also means that each symbol's I and Q Cartesian coordinates are either +1 or -1. A standard QPSK modulator would simply transmit the symbol stream. In this example, the transmitted sinusoid would undergo a phase shift a maximum of once during each symbol period and the symbol rate is half the incoming data rate.

To spread the signal, the DSSS modulator then multiplies each symbol by the chip sequence. The chip sequence is actually a series of +1 and -1 values. You can also think of each symbol as being represented by its I and Q values of +1 or -1. Consider a symbol, represented by the I,Q coordinate (1,1) -- polar or phase coordinate 45 degrees. That symbol is multiplied by each member of the chip sequence. In the case of a +1 chip, the symbol is unchanged. In the case of a -1 chip, the symbol shifts 180 degrees in phase or to coordinates (-1,-1).

Where standard QPSK results in at most one phase change per symbol period, DSSS spreading can result in as many as "n" phase changes per period where n is the number of entries in the chip sequence.

DSSS modulation effectively combines a relatively low-rate Bitstream with a higher-rate chip sequence of n chips per symbol interval. The parameter n is called the spreading ratio. In the case of the DSSS modulated signal, the apparent symbol rate and required bandwidth for transmission are increased by a factor of n.

The WaveLAN system developed by Lucent modulates each symbol with an 11-chip PN sequence. The resulting 11-Mchip/sec transmitted stream requires 11 MHz of bandwidth to yield an actual raw bit rate of 2 Mbps, and Lucent has plans to increase this raw bit rate in the future. To provide a clear, non-interfering channel, WaveLAN actually reserves 22 MHz for each channel.

The DSSS receiver uses the same PN chip sequence as the transmitter to extract data from the spread signal. The incoming signal is first processed by a pass-band RF filter to reject out-of-band noise and interference. This operation isolates the entire band of interest -- for example the entire 83.5-MHz ISM band located at 2.4 GHz. A down converter (or selective filter) then isolates the 22-MHz channel. A decor relator function then removes the chip sequence and restores the original signal.

A measure of the results of the decor relation function is referred to as the processing gain of the receiver. The processing gain actually represents an increase in signal-to-noise ratio with respect to the signal in and out of the decor relator. This gain allows more reliable data communications.

Think of the robustness to noise in terms of the I and Q coordinates of each chip. Because the original symbol is present in each chip, several chips can be corrupted yet the decor relator will still recover good data.

Security and robustness to noise in a DSSS system results from the complexity of the DSSS modulation. A higher spreading ratio adds security and immunity to noise to the system but also limits the amount of data that can be handled in a given band. Engineers designing a DSSS system must choose a spreading ratio that allows both robust and cost-effective data transmissions. For wireless LANs, these parameters will ultimately be determined by the IEEE and governmental bodies. (19)

DSSS

Can be used to expand a network to a building or a mobile user; connecting seamlessly as if the user were hard wired to the network. Today, the computer networking industry is using DSSS in place of the more traditional hard-wired solutions. DSSS can support applications on a network across backbones and to remote users. The transmission rates vary from 256k-100MB depending on the equipment, distance to the number of access points as well as whether the network design is point to point or point to multipoint.

Appendix A

Press Releases: DSSS Wireless Technology

Cisco Acquires aironet

Cisco Systems (San Jose, CA), a leader in networking for the Internet, has acquired publicly owned Aironet Wireless Communications (Akron, OH) for approximately $800 million. According to Cisco, this acquisition will enable its business customers to gain wireless capabilities that act as extensions to existing wired local area networks. The announcement presents a solid indication that major infrastructure players are interested in wireless technology.

Lucent and Qualcomm Join Forces

Lucent Technologies (Murray Hill, NJ) and Qualcomm Inc. (San Diego, CA) have formed an alliance to commercialize a wireless technology that increases the capacity and data capabilities of Lucent's network equipment based on CDMA. Under terms of the co-development agreement, Qualcomm CDMA Technologies will provide the core chip and software to be incorporated into Lucent's CDMA base station equipment. The base stations will be equipped with new channel cards incorporating Qualcomm's CSM5000 Cell Station Modem while preserving existing RF components. Field trials are expected to start during the first half of 2000 using Lucent's Flexent base stations and trial handset terminals.

Telxon Formalizes Relationship with Intelliworxx

Telxon Corp. (Akron, OH) and Intelliworxx Inc. (Sarasota, FL) have entered into a strategic partnership that includes joint product development and technology licensing. Telxon will contribute its experience in the handheld mobile computer marketplace, its knowledge of ergonomics and industrial design and its sales and support infrastructure, while Intelliworxx will contribute its advanced, high-speed Pentium design expertise, for both embedded and handheld product arenas.

The Following Article is an actual site Implemented in 1999, which is up and running more efficiently on FHSS Wireless Technology.

The Spirit of Radio
Spread spectrum radio links township WAN, saves bundles

Spread spectrum radio frequency (SSRF) is a fast-growing alternative for providing data connectivity between locations in a given region. SSRF has been around since the late 1920s, but it was during World War II that its potential was first fully demonstrated. The 1940s movie actress Hedy Lamarr holds the first public patent on the technology. While at a dinner, she and a friend thought up a spread spectrum scheme to safeguard radio communications about the Allies' torpedo attacks without the enemy's detecting them or jamming their transmissions.

Today, the computer networking industry is using SSRF in place of the more traditional hard-wired solutions.

For successful implementation, a line of sight must be available between the antennas, and they must be within the distance limits of the signal strength.

In the Town of Tonawanda in Western New York, the geography worked well for using this "old" technology to advance the town's Wide Area Network (WAN). For the past seven years, the town used the local telephone company (telco) infrastructure to connect its buildings. We had an assortment of connection types, ranging from T1 (1.5Mbps) and 56Kbps leased lines to standard dial-up and Integrated Services Digital Network (ISDN) metered lines.

Thirteen government buildings throughout the town were brought online via the telco lines. As of 1998, we were spending $65,000 per year for this connectivity. The town's technical support department and its consultant, Aurora Consulting Group of East Aurora, New York, brought the spread spectrum project to fruition. Beginning its research in the spring of 1998, the group presented its findings to town officials that

fall.

The argument for making a capital investment estimated at $115,000 in an SSRF system was simple: We could have a greater-bandwidth WAN that would be more reliable, less complicated and save at least $65,000 per year. The benefits of such a system include:

- resistance to jamming by outsiders
- encoded signals that restrict the communications to legitimate users
- resistance to interference by rain, snow, ice and other environmental factors
- multiple levels of security, both physical and electronic
- easy accessibility for multiple users
- excellent signal resolution
- operation on a segment of the radio spectrum that's exempt from federal licensing.

Another catalyst for the project was the 180-foot-high cellular phone and radio tower that had recently been built at the town's centrally located police station.

Specs for Success

The town then prepared a performance specification for a 3Mbps wireless WAN, the fastest available at the time. The project required line-of-sight analyses for connecting 14 buildings throughout the town (one additional building was to be brought into the network). The WAN was to be a multipoint hub-and-spoke topology, with the tower at the police station as the hub. Distances between sites ranged from just across the street to over three miles at our water treatment plant along the Niagara River. The network had to be Ethernet 802.3 compliant. The equipment to be furnished and installed included a wireless radio bridge, an antenna and cabling between the two for each site.

The town's Internet, e-mail and financial system servers are located at the Municipal Building, about 1.5 miles from the police tower. Most of the network traffic is bound for these servers. Internet access is gained and controlled at one point at the proxy server. Therefore, the network design had to take this traffic pattern into consideration.

Bids for the project were called for in November 1998; by then, Ethernet-speed bridges (10Mbps) were coming onto the market. These faster devices were bid as an alternative to the original 3Mbps system. In December 1998, bids were received

for the project and the 11Mbps wireless bridges offered by Aironet Wireless Communications Inc. through local contractor Trans wave Communication Systems were selected as the system of choice. The project was awarded to Transwave at a cost of $112,500 and it completed the installation by April 1999.

Installation

The contractor began by installing the main omnidirectional antenna near the top of the police station tower. This antenna, about the size of a broom handle, was an omnidirectional type. The bridge was installed on a small shelf near the existing hubs and configured to act as the root device to which all other bridges were directed. The antennas installed at the other sites were directional in function and either Yagi or parabolic in type, depending on the distance and signal strength required.

In most cases, the contractor mounted a galvanized steel pipe (or mast) to a high point on the building. This formed the structure for the antenna. A 45-foot and a 55-foot tripod tower were installed at two sites to create the necessary line of sight, and existing tripods were used at two other sites.

The Aironet ER-500 wireless bridge operates from a standard power source. Antennas are connected to the bridge by coaxial cable and the bridge is then attached to the LAN by Category 5 Ethernet cable. The configuration of the bridge includes a unique site identifier along with the common radio signal identifier. Our contractor configured the bridge through a serial cable from a laptop, but configuration can also be confirmed and the system monitored via Telnet or through a standard Web browser. Configuration was completed at the contractor's shop, then modified as necessary on site.

Bridges operate by providing an origin and destination database for all network TCP packets. The MAC address of every network device is stored in tables on the bridge. When a packet is destined for another device on the network, the bridge determines if it is inside or outside of the LAN and directs it accordingly.

From Wired to Wireless - Managing the Transition

Town personnel and staff from Aurora Consulting completed the conversion of the network by disconnecting all of the telco devices and connecting the new bridges to existing local area networks at each building. Having a new Ethernet connection among all town departments made it possible to deploy several network management strategies. One is the configuration of the file server at the Municipal Building; this is now a Dynamic Host Control Protocol (DHCP) server, which allows for the automatic assignment of IP addresses to all clients on the network. This strategy was implemented at the same time as the conversion.

Another important management tool is virus protection for all servers. The virus software is continually updated from the Web, and these updates are then pushed to

the other servers on the network.

In addition to the town's conversion, the local school district joined the project under a $30,000 shared service grant sponsored by New York State. The school district connected three schools by using the town's contractor and by co-locating an antenna on the tower at the police station.

The school wanted to participate in the RF project because its two telco leased lines were about to expire.

Other strategies being implemented for the network include Microsoft Systems Management Server for network management and system maintenance and intranet enterprise resource applications development. At the same time, the number of calls related to network problems has decreased substantially; the former routers, ISDN modems, CSU/DSUs and telco circuits have been taken out of service and shelved, and users have actually been pleased with Internet access speeds.

Bottom-Line Benefits

The town is saving $65,000 a year in local telco costs, and we've increased our networking speeds from 56K to 10Mbps. The speed increase is a minimum of 10-fold, resulting in much faster file transfer, Internet access and system reliability. In addition, our return on investment for the new RF system is only 18 months.

Another benefit: Our spread spectrum WAN is virtually administration-free and transparent to the user. Once a month we monitor the system to make sure "it's still there." We've had only minor disruptions in performance in our running time thus far. For example, once a severe rainstorm resulted in water leaking inside the jacket of the radio cable, resulting in a degraded RF signal for roughly four hours at one site. Our contractor replaced the cable immediately and solved the problem.

Another time, the town's technical department did a massive deployment of software over the network and bogged it right down. That was a big project we were doing under normal, every-day traffic, and required that we re-boot the Aironet bridge.

Our users enjoy great speeds for surfing the Internet and transferring files of town documents, maps (GIS) and photographs, and doing application sharing such as spreadsheets and financial programs (Munis), and internal and external e-mail. We're also developing a wireless intranet for building permits and complaint tracking.

James B. Jones is project engineer, Town of Tonawanda, New York.

Appendix B

ISO/OSI Network Model

The standard model for networking protocols and distributed applications is the International Standard Organization's Open System Interconnect (ISO/OSI) model. It defines seven network layers.

Layer 1 - Physical

Physical layer defines the cable or physical medium itself, e.g., thinnet, thicknet, unshielded twisted pairs (UTP). All media are functionally equivalent. The main difference is in convenience and cost of installation and maintenance. Converters from one media to another operate at this level.

Layer 2 - Data Link

Data Link layer defines the format of data on the network. A network data frame, aka packet, includes checksum, source and destination address, and data. The largest packet that can be sent through a data link layer defines the Maximum Transmission Unit (MTU). The data link layer handles the physical and logical connections to the packet's destination, using a network interface. A host connected to an Ethernet would have an Ethernet interface to handle connections to the outside world, and a loopback interface to send packets to itself.

Ethernet addresses a host using a unique, 48-bit address called its Ethernet address or Media Access Control (MAC) address. MAC addresses are usually represented as six colon-separated pairs of hex digits, e.g., 8:0:20:11:ac:85. This number is unique and is associated with a particular Ethernet device. Hosts with multiple network interfaces should use the same MAC address on each. The data link layer's protocol-specific header specifies the MAC address of the packet's source and destination. When a packet is sent to all hosts (broadcast), a special MAC address (ff:ff:ff:ff:ff:ff) is used.

Layer 3 - Network

NFS uses Internetwork Protocol (IP) as its network layer interface. IP is responsible for routing, directing datagrams from one network to another. The network layer may have to break large datagrams, larger than MTU, into smaller packets and host receiving the packet will have to reassemble the fragmented datagram. The Internetwork Protocol identifies each host with a 32-bit IP address. IP addresses are written as four dot-separated decimal numbers between 0 and 255, e.g., 129.79.16.40. The leading 1-3 bytes of the IP identify the network and the remaining bytes identifies the host on that network. The network portion of the IP is assigned by InterNIC Registration Services, under the contract to the National Science Foundation, and the host portion of the IP is assigned by the local network administrators, locally by noc@indiana.edu. For large sites, usually subnetted like ours, the first two bytes represents the network portion of the IP, and the third and fourth bytes identify the subnet and host respectively.

Even though IP packets are addressed using IP addresses, hardware addresses must be used to actually transport data from one host to another. The Address Resolution Protocol (ARP) is used to map the IP address to it hardware address.

Layer 4 - Transport

Transport layer subdivides user-buffer into network-buffer sized datagrams and enforces desired transmission control. Two transport protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), sits at the transport layer. Reliability and speed are the primary difference between these two protocols. TCP establishes connections between two hosts on the network through 'sockets' which are determined by the IP address and port number. TCP keeps track of the packet delivery order and the packets that must be resent. Maintaining this information for each connection makes TCP a stateful protocol. UDP on the other hand provides a low overhead transmission service, but with less error checking. NFS is built on top of UDP because of its speed and statelessness. Statelessness simplifies the crash recovery.

Layer 5 - Session

The session protocol defines the format of the data sent over the connections. The NFS uses the Remote Procedure Call (RPC) for its session protocol. RPC may be built on either TCP or UDP. Login sessions uses TCP whereas NFS and broadcast use UDP.

Layer 6 - Presentation

External Data Representation (XDR) sits at the presentation level. It converts local representation of data to its canonical form and vice versa. The canonical uses a standard byte ordering and structure packing convention, independent of the host.

Layer 7 - Application

Provides network services to the end-users. Mail, ftp, telnet, DNS, NIS, NFS are examples of network applications. (1).

Appendix C
Bibliography
Web Sites Referenced:

1
2 http://standards.ieee.org/search.html
3 http://www.itp-journals.com/
4 http://www.wilan.com/ofdm/main.html
5 http://www.cetp.ipsl.fr/~porteneu/inet98/6x/6x_1.htm#s3
6 http://www.radiata.com/
7 http://www.homerf.org/
8 http://www.wirelessethernet.org/
9 http://hydra.carleton.ca/info/wlan.html
10 http://wi.pennnet.com/home/search.cfm
11 http://www.sss-mag.com/
12 http://sss-mag.com/destopics.html
13 http://grouper.ieee.org/groups/802/15/pub/TG2.html
14 http://www.uwsg.indiana.edu/usail/network/nfs/network_layers.html
15 http://www.netbeam.net/products/default.htm
16 http://mosquitonet.stanford.edu/mobile/
17 http://www.wireless-nets.com/glossary.htm
18 http://www.wirelessguys.com/shop/index.html
19 http://www.wavelan.com/solutions/outdoor/
20 http://www.wavelan.com/search/index.html
http://www.wireless-nets.com/whitepaper_cdpd.htm

Appendix C

Glossary of Terms

10Base-2 - IEEE standard (known as thin Ethernet) for 10 Mbps baseband Ethernet over coaxial cable at a maximum distance of 185 meters.

100Base-T - IEEE standard for a 100 Mbps baseband Ethernet over twisted-pair wire.

802.2 - IEEE standard that specifies the Logical Link Control (LLC) that is common to all 802 series LANs

802.3 - IEEE standard that specifies a carrier sense medium access control and physical layer specifications for wired LANs.

802.10 - IEEE standard that specifies security and privacy access methods for both wired and wireless LANs.

802.11 - IEEE standard that specifies medium access and physical layer specifications for 1 Mbps and 2 Mbps wireless connectivity between fixed, portable, and moving stations within a local area.

access point (AP) - An interface between the wireless network and a wired network. Access points combined with a distribution system (e.g. Ethernet) support the creation of multiple radio cells (BSSs) that enable roaming throughout a facility.

acknowledged connectionless service - A datagram-style service that includes error-control and flow-control mechanisms.

ad hoc network - A wireless network composed of only stations and no access point.

adaptive routing - A form of network routing whereby the path data packets traverse from a source to a destination node that depends on the current state of the network. Normally with adaptive routing, routing information stored at each node changes according to some algorithm that calculates the best paths through the network.

Address Resolution Protocol (ARP) - A TCP/IP protocol that binds logical (IP) addresses to physical addresses.

analog cellular - A telephone system that uses radio cells to provide connectivity

among cellular phones. The analog cellular telephone system uses FM (Frequency Modulation) radio waves to transmit voice grade signals. To accommodate mobility, this cellular system will switch your radio connection from one cell to another as you move between areas. Every cell within the network has a transmission tower that links mobile callers to a Mobile Telephone Switching Office (MTSO).

analog signal - An electrical signal with an amplitude that varies continuously as time progresses.

appliance - Runs applications and is a visual interface between the user and the network. There are several classes of user appliances—the desktop workstation, laptop, palmtop, pen-based computer, Personal Digital Assistant (PDA), and pager.

application layer - Establishes communications with other users and provides services such as file transfer and electronic mail to the end users of the network.

application process - An entity, either human or software, that uses the services offered by the application layer of the OSI reference model.

application software - Accomplishes the functions users require, such as database access, electronic mail, and menu prompts. Therefore, application software directly satisfies network requirements, particularly user requirements.

ARP - See Address Resolution Protocol.

ARQ - See automatic repeat-request.

association service - An IEEE 802.11 service that an enables the mapping of a wireless station to the distribution system via an access point.

Asynchronous Transfer Mode (ATM) - A cell-based connection-oriented data service offering high speed (up to 2.488 Gbps) data transfer. ATM integrates circuit and packet switching to handle both constant and burst information. Frequently called cell relay.

asynchronous transmission - Type of synchronization where there is no defined time relationship between transmission of frames.

ATM - See Asynchronous Transfer Mode.

attachment unit interface (AUI) - A 15-pin interface between an Ethernet network

interface card and transceiver.

AUI - See attachment unit interface.

automatic repeat-request (ARQ) - A method of error correction where the receiving node detects errors and uses a feedback path to the sender for requesting the retransmission of incorrect frames.

Authentication - The process a station uses to announce its identify to another station. IEEE 802.11 specifies two forms of authentication: open system and shared key.

bandwidth - Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

baseband - A signal that has not undergone any shift in frequency. Normally with LANs, a baseband signal is purely digital.

Basic Service Set (BSS) - A set of 802.11-compliant stations that operate as a fully-connected wireless network.Basic Service Set

Identification (BSSID) - A six-byte address that distinguishes a particular access point from others. Also know as a network ID.

baud rate - The number of pulses of a signal that occur in one second. Thus, baud rate is the speed the digital signal pulses travel.

bit rate - The transmission rate of binary symbols (“0” and “1”). Bit rate is equal to the total number of bits transmitted in one second.

bridge - A network component that provides internetworking functionality at the data link or medium access layer of a network’s architecture. Bridges can provide segmentation of data frames.

Broadband - A signal that has undergone a shift in frequency. Normally with LANs, a broadband signal is analog.

BSS - See Basic Service Set.

BSSID - See Basic Service Set Identification.

bus topology - A type of topology where all nodes are connected to a single length

of cabling with a terminator at each end.

carrier current LAN - A LAN that uses power lines within the facility as a medium for the transport of data.

CDPD - See Cellular Digital Packet Data.

cell relay - See Asynchronous Transfer Mode.

Cellular Digital Packet Data (CDPD) - Overlays the conventional analog cellular telephone system, using a channel-hopping technique to transmit data in short bursts during idle times in cellular channels. CDPD operates full duplex in the 800 and 900 Mhz frequency bands, offering data rates up to 19.2 Kbps.

clear channel assessment - A function that determines the state of the wireless medium in an IEEE 802.11 network.

coaxial cable - Type of medium having a solid metallic core with a shielding as a return path for current flow. The shielding within the coaxial cable reduces the amount of electrical noise interference within the core wire; therefore, coaxial cable can extend to much greater lengths than twisted-pair wiring. Commonly called coax and used in older Ethernet (10base2) networks.

connection-oriented service - Establishes a logical connection that provides flow control and error control between two stations needing to exchange data.

connectivity - A path for communications signals to flow through. Connectivity exists between a pair of nodes if the destination node can correctly receive data from the source node at a specified minimum data rate.

connectivity software - A wireless system component that provides an interface between the user's appliance and the database or application software located on the network.

Copper Data Distributed Interface (CDDI) - A version of FDDI specifying the use of unshielded twisted-pair wiring (Category 5).

CRC - See Cyclic Redundancy Check.

Cyclic Redundancy Check (CRC) - An error detection process that (at the transmitting station) divides the data being sent by a particular polynomial and

appends the resulting remainder to the transmitted data. Then (at the receiving station) the process divides the received data by the same polynomial and compares the resulting remainder to the remainder appended to the data at the transmitting station. If the remainders are equal, there is very high probability that no errors are present in the data. If the don't match, then errors are present.

Data Encryption Standard (DES) - A cryptographic algorithm that protects unclassified computer data. DES is a National Institute of Standards and Technology (NIST) standard and is available for both public and government use.

data service unit/channel service unit (DSU/CSU) - A set of network components that reshape data signals into a form that can be effectively transmitted over a digital transmission medium, typically a leased 56 Kbps or T1 line.

datagram service - A connectionless form of packet switching whereby the source does not need to establish a connection with the destination before sending data packets.

DES - See Data Encryption Standard.

DHCP - See Dynamic Host Configuration Protocol.

direct sequence spread spectrum (DSSS) - Combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a chip sequence (also known as processing gain). A high processing gain increases the signal's resistance to interference. The minimum processing gain that the FCC allows is 10, and most products operate under 20.

disassociation service - An IEEE 802.11 term that defines the process a station or access point uses to notify that it is terminating an existing association.

distributed routing - A form of routing where each node (router) in the network periodically identifies neighboring nodes, updates its routing table, and, with this information, then sends its routing table to all of its neighbors. Because each node follows the same process, complete network topology information propagates through the network and eventually reaches each node.

distribution service - An IEEE 802.11 station uses the distribution service to send MAC frames across a distribution system.

distribution system - An element of a wireless system that interconnects Basic Service Sets via access points to form an Extended Service Set.

DQDB - See Distributed Queue Dual Bus.

DSSS - See direct sequence spread spectrum.

DSU/CSU - See Data Service Unit/Channel Service Unit.

Dynamic Host Configuration Protocol (DHCP) - Issues IP addresses automatically within a specified range to devices such as PCs when they are first powered on. The device retains the use of the IP address for a specific license period that the system administrator can define. DHCP is available as part of the many operating systems including Microsoft Windows NT Server and UNIX.

EDI - See electronic data interchange.

EIA - See Electronics Industry Association.

electronic data interchange (EDI) - A service that provides standardized inter-company computer communications for business transactions. ANSI standard X.12 defines the data format for business transactions for EDI.

Electronics Industry Association (EIA) - A domestic standards-forming organization that represents a vast number of United States electronics firms.

ethernet - A 10 Mbps LAN medium-access method that uses CSMA to allow the sharing of a bus-type network. IEEE 802.3 is a standard that specifies Ethernet.

ethernet repeater - Refers to a component that provides ethernet connections among multiple stations sharing a common collision domain. Also referred to as a shared ethernet hub.

ethernet switch - More intelligent than a hub, having the ability to connect the sending station directly to the receiving station.

Extended Service Set (ESS) - A collection of Basic Service Sets tied together via a distribution system.

FDDI - See Fiber Distributed Data Interface.

FEC - See forward error correction.

FHSS - See frequency hopping spread spectrum.

Fiber Distributed Data Interface (FDDI) - An ANSI standard for token-passing

networks. FDDI uses optical fiber and operates at 100 Mbps.

File Transfer Protocol (FTP) - A TCP/IP protocol for file transfer.

firewall - A device that interfaces the network to the outside world and shields the network from unauthorized users. The firewall does this by blocking certain types of traffic. For example, some firewalls permit only electronic mail traffic to enter the network from elsewhere. This helps protect the network against attacks made to other network resources, such as sensitive files, databases, and applications.

forward error correction (FEC) - A method of error control where the receiving node automatically corrects as many channel errors as it can without referring to the sending node.

fractional T-1 - A 64 Kbps increment of a T1 frame.

frame relay - A packet-switching interface that operates at data rates of 56 Kbps to 2 Mbps. Actually, frame relay is similar to X.25, minus the transmission error control overhead. Thus, frame relay assumes that a higher layer, end-to-end protocol will check for transmission errors. Carriers offer frame relay as permanent connection-oriented (virtual circuit) service.

frequency hopping spread spectrum (FHSS) - Takes the data signal and modulates it with a carrier signal that hops from frequency to frequency as a function of time over a wide band of frequencies. For example, a frequency-hopping radio will hop the carrier frequency over the 2.4 GHz frequency band between 2.4 GHz and 2.483 GHz. A hopping code determines the frequencies it will transmit and in which order. To properly receive the signal, the receiver must be set to the same hopping code and “listen” to the incoming signal at the right time at the correct frequency.

FTP - See File Transfer Protocol.

gateway - A network component that provides interconnectivity at higher network layers. For example, electronic mail gateways can interconnect dissimilar electronic mail systems.

Gaussian frequency shift keying - A frequency modulation technique that filters the baseband signal with a Gaussian filter before performing the modulation.

Global Positioning System (GPS) - A worldwide, satellite-based radio navigation system providing three-dimensional position, velocity and time information to users having GPS receivers anywhere on or near the surface of the Earth.

HDLC - See High-level Data Link Control.

hierarchical topology - A topology where nodes in the same geographical area are joined together, then tied to the remaining network as groups. The idea of a hierarchical topology is to install more links within high density areas and fewer links between these populations.

High-level Data Link Control (HDLC)- An ISO protocol for link synchronization and error control.

Hypertext Markup Language (HTML)- A standard used on the Internet World Wide Web for defining hypertext links between documents.

IBSS Network- See Independent Basic Service Set Network.

IEEE- See Institute of Electrical and Electronic Engineers.

Independent Basic Service Set Network (IBSS Network)- An IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an ad hoc network because it can be constructed quickly without much planning.

industrial, scientific, and medicine bands (ISM bands)- Radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz.

infrared light- Light waves having wavelengths ranging from about 0.75 to 1,000 microns, which is longer (lower in frequency) than the spectral colors but much shorter (higher in frequency) than radio waves. Therefore, under most lighting conditions, infrared light is invisible to the naked eye.

Institute of Electrical and Electronic Engineers (IEEE)- A United States-based standards organization participating in the development of standards for data transmission systems. IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE 802 series of standards.

Integrated Services Digital Network (ISDN)- A collection of CCITT standards specifying WAN digital transmission service. The overall goal of ISDN is to provide a single physical network outlet and transport mechanism for the transmission of all types of information, including data, video, and voice.

integration service- enables the delivery of MAC frames through a portal between an IEEE 802.11 distribution system and a non-802.11 LAN.

integration testing- Type of testing that verifies the interfaces between network components as the components are installed. The installation crew should integrate components into the network one-by-one and perform integration testing when necessary to ensure proper gradual integration of components.

interframe space- Defines spacing between different aspects of the IEEE 802.11 MAC access protocol to enable different transmission priorities.

Intermediate System-to-Intermediate System Protocol- An OSI protocol for intermediate systems exchange routing information.

International Standards Organization (ISO)- A non-treaty standards organization active in the development of international standards such as the Open System Interconnection (OSI) network architecture.

International Telecommunications Union (ITU)- An agency of the United States providing coordination for the development of international standards.

International Telegraph and Telephone Consultative Committee (CCITT)- An international standards organization that is part of the ITU and dedicated to establishing effective and compatible telecommunications among members of the United Nations. CCITT develops the widely used V-series and X-series standards and protocols.

internetwork- A collection of interconnected networks. Often it is necessary to connect networks together, and an internetwork provides the connection between different networks. One organization having a network may want to share information with another organization having a different network. The internetwork provides functionality needed to share information between these two networks.

inward interference- Interference coming from other devices, such as microwave ovens and other wireless network devices, that will result in delay to the user by either blocking transmissions from stations on the LAN, or by causing bit errors to occur in data being sent.

ISDN- See Integrated Services Digital Network.

ISM Bands- See industrial, scientific, and medicine bands.

ISO- See International Standards Organization.

isochronous transmission- Type of synchronization where information frames are sent at specific times.

ITU- See International Telecommunications Union.

joint application design (JAD)- A parallel process simultaneously defining requirements in the eyes of the customer, users, sales people, marketing staff, project managers, analysts, and engineers. You can use the members of this team to define requirements.

LAP- See Link Access Procedure.

laser- Is a common term for Light Amplification by Stimulated Emission of Radiation, a device containing a substance where the majority of its atoms or molecules are put into an excited energy state. As a result, the laser emits coherent light of a precise wavelength in a narrow beam. Most laser MANs use lasers that produce infrared light.

light emitting diode (LED)- Used in conjunction with optical fiber, it emits incoherent light when current is passed through it. Advantages to LEDs include low cost and long lifetime, and they are capable of operating in the Mbps range.

Link Access Procedure (LAP)- An ITU error correction protocol derived from the HDLC standard.

local bridge- A bridge that connects two LANs within close proximity.

Logical Link Control Layer (LLC)- The highest layer of the IEEE 802 Reference Model and provides similar functions of a traditional data link control protocol.

MAC Layer- See Medium Access Control Layer.

MAC protocol data unit (MPDU)- The unit of data in an IEEE 802 network that two peer MAC entities exchange across a physical layer.

mail gateway- A type of gateway that interconnects dissimilar electronic mail systems.

management information base (MIB)- A collection of managed objects residing in a virtual information store.

MAU- See multi-station access unit.

medium- A physical link that provides a basic building block to support the transmission of information signals. Most media are composed of either metal,

glass, plastic, or air.

medium access- A data link function that controls the use of a common network medium.

Medium Access Control Layer (MAC Layer)- Provides medium access services for IEEE 802 LANs.

meteor burst communications- A communications system that directs a radio wave, modulated with a data signal, at the iono-
sphere. The radio signal reflects off the ionized gas left by the burning of meteors entering the atmosphere and is directed back to Earth in the form of a large footprint, enabling long distance operation.

MIB- See management information base.

middleware- An intermediate software component located on the wired network between the wireless appliance and the application or data residing on the wired network. Middleware provides appropriate interfaces between the appliance and the host application or server database.

MIDI- See Musical Instrument Digital Interface.

Mobile IP- A protocol developed by the Internet Engineering Task Force to enable users to roam to parts of the network associated with a different IP address than what's loaded in the user's appliance.

mobility- Ability to continually move from one location to another.

mobility requirements- Describe the movement of the users when performing their tasks. Mobility requirements should distinguish whether the degree of movement is continuous or periodic.

modulation- The process of translating the baseband digital signal to a suitable analog form.

MPDU- See MAC protocol data unit.

multi-station access unit (MAU)- A multiport wiring hub for token-ring networks.

multiplexer- A network component that combines multiple signals into one composite signal in a form suitable for transmission over a long-haul connection, such as leased 56 Kbps or T1 circuits.

Musical Instrument Digital Interface (MIDI)- A standard protocol for the interchange of musical information between musical instruments and computers.

narrowband system- A wireless system that uses dedicated frequencies assigned by the FCC licenses. The advantage of narrowband systems is that if interference occurs, the FCC will intervene and issue an order for the interfering source to cease operations. This is especially important when operating wireless MANs in areas having a great deal of other operating radio-based systems.

Network Basic Input Output System (NetBIOS)- A standard interface between networks and PCs that allows applications on different computers to communicate within a LAN. It was created by IBM for its early PC Network, was adopted by Microsoft, and has since become a de facto industry standard. It is not routable across a WAN.

network file system (NFS)- A distributed file system enabling a set of dissimilar computers to access each other's files in a transparent manner.

network interface card (NIC)- A network adapter inserted into a computer so the computer can be connected to a network. It is responsible for converting data from the form stored in the computer to the form transmitted or received.

network layer- Provides the routing of packets from source to destination.

network management- Consists of a variety of elements that protect the network from disruption and provide proactive control of the configuration of the network.

network management station- Executes management applications that monitor and control network elements.

network monitoring- A form of operational support enabling network management to view the inner-workings of the network. Most network monitoring equipment is non-obtrusive and can determine the network's utilization and locate faults.

network re-engineering- A structured process that can help an organization proactively control the evolution of its network. Network re-engineering consists of continually identifying factors influencing network changes, analyzing network modification feasibility, and performing network modifications as necessary.

network service access point (NSAP)- A point in the network where OSI network services are available to a transport entity.

NFS- See network file system.

NIC- See network interface card.

node- Any network-addressable device on the network, such as a router or network interface card.

NSAP- See network service access point.

ODI- See Open Data-Link Interface.

ODBC- See Open Database Connectivity.

Open Database Connectivity (ODBC)- A standard database interface enabling interoperability between application software and multi-vendor ODBC-compliant databases.

Open Data-Link Interface (ODI)- Novell's specification for network interface card device drivers, allowing simultaneous operation of multiple protocol stacks.

Open Shortest Path First (OSPF)- Routing protocol for TCP/IP routers that bases routing decisions on the least number of hops from source to destination.

open system authentication- The IEEE 802.11 default authentication method, which is a very simple, two-step process. First the station wanting to authenticate with another station sends an authentication management frame containing the sending station's identify. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.

Open System Interconnection (OSI)- An ISO standard specifying an open system capable of enabling the communications between diverse systems. OSI has the following seven layers of distinction: physical, data link, network, transport, session, presentation, and application. These layers provide the functions necessary to allow standardized communications between two application processes.

OSPF- See Open Shortest Path First.

packet radio- Uses packet switching to move data from one location to another across radio links.

PCF- See point coordination function.

PCM- See pulse code modulation.

PCMCIA form factor- See Personal Computer Memory Card International Association form factor.

PCS- See Personal Communications Services.

peer-to-peer network- A network where there are communications between a group of equal devices. A peer-to-peer LAN does not depend upon a dedicated server, but allows any node to be installed as a non-dedicated server and share its files and peripherals across the network. Peer-to-peer LANs are normally less expensive because they do not require a dedicated computer to store applications and data. They do not perform well, however, for larger networks.

performance modeling- The use of simulation software to predict network behavior, allowing you to perform capacity planning. Simulation allows you to model the network and impose varying levels of utilization to observe the effects. Performance Monitoring Addresses performance of a network during normal operations. Performance monitoring includes real-time monitoring, where metrics are collected and compared against thresholds that can set off alarms; recent-past monitoring, where metrics are collected and analyzed for trends that may lead to performance problems; and historical data analysis, where metrics are collected and stored for later analysis.

Personal Communications Services (PCS)- A spectrum allocation located at 1.9 GHz, a new wireless communications technology offering wireless access to the World Wide Web, wireless e-mail, wireless voice mail, and cellular telephone service.

Personal Computer Memory Card International Association form factor (PCMCIA form factor)- A standard set of physical interfaces for portable computers. PCMCIA specifies three interface sizes—Type I (3.3 millimeters), Type II (5.0 millimeters), and Type III (10.5 milli-meters).

physical layer- Provides the transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications.

physical layer convergence procedure sublayer (PLCP)- Prepares MAC protocol data units (MPDUs) as instructed by the MAC Layer for transmission and delivers incoming frames to the MAC Layer.

physical medium dependent sublayer (PMD)- Provides the actual transmission and reception of Physical Layer entities between two stations via the wireless

medium.

plain old telephone system (POTS)- The original common analog telephone system, which is still in wide use today.

PLCP- See Physical layer convergence procedure sublayer.

PMD- See Physical medium dependent sublayer.

point coordination function (PCF)- An IEEE 802.11 mode that enables contention-free frame transfer based on a priority mechanism. Enables time-bounded services that support the transmission of voice and video.

Point-to-Point Protocol (PPP)- A protocol that provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. PPP is the successor to SLIP.

portability- Defines network connectivity that can be easily established, used, then dismantled.

portal- A logical point where MSDUs from a non-IEEE 802.11 LAN enter the distribution system of an extended service set wireless network.

POTS- See plain old telephone system.

PPP- See Point-to-Point Protocol.

presentation layer- Negotiates data transfer syntax for the application layer and performs translations between different data types, if necessary.

processing gain- Equal to the data rate of the spread direct sequence signal divided by the data rate of the actual data.

project charter- Formally recognizes the existence of the project, identifies the business need that the project is addressing, and gives a general description of the resulting product.

project management- Overseers needed to make sure actions are planned and executed in a structured manner.

prototyping- A method of determining or verifying requirements and design specifications. The prototype normally consists of network hardware and software that support a proposed solution. The approach to prototyping is typically a

trial-and-error experimental process.

pseudo-noise- An actual signal having a long pattern that resembles noise.

pulse code modulation (PCM)- A common method for converting analog voice signals into a digital bit stream.

pulse position modulation- The varying of the position of a pulse to represent different binary symbols. The changes in pulse positions maintain the information content of the signal.

reassociation service- enables an IEEE 802.11 station to change its association with different access points as the station moves throughout the facility.

Red Book- A document of the United States National Security Agency (NSA) defining criteria for secure networks.

relay node- Implements a routing protocol that maintains the optimum routes for the routing tables, forwarding packets closer to the destination.

remote bridge- A bridge that connects networks separated by longer distances. Organizations use leased 56 Kbps circuits, T1 digital circuits, and radio waves to provide long distance connections between remote bridges.

repeater- A network component that provides internetworking functionality at the physical layer of a network's architecture. A repeater amplifies network signals, extending the distance they can travel.

requirements analysis- A process of defining what the network is supposed to do, providing a basis for the network design.

ring topology- A topology where a set of nodes are joined in a closed loop.

RIP- See Routing Information Protocol.

router- A network component that provides internetworking at the network layer of a network's architecture by allowing individual networks to become part of a WAN. It routes using logical and physical addresses to connect two or more separate networks. It determines the best path by which to send a packet of information.

Routing Information Protocol (RIP)- A common type of routing protocol. RIP bases its routing path on the distance (number of hops) to the destination. RIP maintains optimum routing paths by sending out routing update messages if the

network topology changes. For example, if a router finds that a particular link is faulty, it will update its routing table, then send a copy of the modified table to each of its neighbors.

RS-232- An EIA standard that specifies up to 20 Kbps, 50 foot, serial transmission between computers and peripheral devices.

RS-422- An EIA standard specifying electrical characteristics for balanced circuits (i.e. both transmit and return wires are at the same voltage above ground). RS-422 is used in conjunction with RS-449.

RS-423- An EIA standard specifying electrical characteristics for unbalanced circuits (i.e. the return wire is tied to ground). RS-423 is used in conjunction with RS-449.

RS-449- An EIA standard specifying a 37-pin connector for high-speed transmission.

RS-485- An EIA standard for multipoint communications lines.

SAP- See Service Access Point.

Serial Line Internet Protocol (SLIP)- An Internet protocol used to run IP over serial lines and dial-up connections.

server-oriented network- A network architecture where the network software is split into two pieces, one each for the client and the server. The server component provides services for the client software; the client part interacts with the user. The client and server components run on different computers, and the server is usually more powerful than the client. The main advantages of a server-oriented network is less network traffic. Therefore, networks having a large number of users will normally perform better with server-oriented networks.

service access point (SAP)- A point at which the services of an OSI layer are made available to the next higher layer.

service primitive- A communications element for sending information between network architectural layers.

session layer- Establishes, manages, and terminates sessions between applications.

shared key authentication- A type of authentication that assumes each station

has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of Shared Key authentication requires implementation of the 802.11 Wireless Equivalent Privacy algorithm.

Simple Mail Transfer Protocol (SMTP)- The Internet electronic mail protocol.

Simple Network Monitoring Protocol (SNMP)- A network management protocol that defines the transfer of information between Management Information Bases (MIBs). Most high-end network monitoring stations require the implementation of SNMP on each of the components the organization wishes to monitor.

SLIP- See Serial Line Internet Protocol.

SMDS- See Switched Multimegabit Digital Service.

SMTP- See Simple Mail Transfer Protocol.

SNA- See Systems Network Architecture.

SNMP- See Simple Network Monitoring Protocol.

SONET- See Synchronous Optical NETwork.

spectrum analyzer- An instrument that identifies the amplitude of signals at various frequencies.

spread spectrum- A modulation technique that spreads a signal's power over a wide band of frequencies. The main reasons for this technique is that the signal becomes much less susceptible to electrical noise and interferes less with other radio-based systems.

SQL- See Structured Query Language.

ST connector- An optical fiber connector that uses a bayonet plug and socket.

star topology- A topology where each node is connected to a common central switch or hub.

station- In IEEE 802.11 networks, any device that contains an IEEE 802.11-compliant medium access control and physical layers.

Structured Query Language (SQL)- An international standard for defining and

accessing relational databases.

Switched Multimegabit Digital Service (SMDS)- A packet switching connectionless data service for WANs.

Synchronous Optical NETwork (SONET)- A fiber optic transmission system for high-speed digital traffic. SONET is part of the B-ISDN standard.

synchronous transmission- Type of synchronization where information frames are sent within certain time periods. It uses a clock to control the timing of bits being sent.

system testing- Type of testing that verifies the installation of the entire network. Testers normally complete system testing in a simulated production environment, simulating actual users in order to ensure the network meets all stated requirements.

Systems Network Architecture (SNA)- IBM's proprietary network architecture.

T1- A standard specifying a time division multiplexing scheme for point-to-point transmission of digital signals at 1.544 Mbps.

TCP- See Transmission Control Protocol.

TDR- See time-domain reflectometer.

Technical Service Bulletin 67 (TSB 67)- Describes how to test Category 5 twisted-pair cable. TSB 67 was published by the Link Performance Task Group, a subcommittee of the Telecommunications Industry Association's TR41 Standards Committee.

technology comparison matrix- A documentation method that compares similar technologies based on attributes such as functionality, performance, cost, and maturity.

telecommuting- The concept of electronically stretching an office to a person's home.

Telnet- A virtual terminal protocol used in the Internet, enabling users to log into a remote host.

terminal node controller (TNC)- Interfaces computers to ham radio equipment. TNCs act much like a telephone modem, converting the computer's digital signal

into one that a ham radio can modulate and send over the airwaves using a packet switching technique.

test case- An executable test with a specific set of input values and a corresponding expected result.

time-domain reflectometer (TDR)- Tests the effectiveness of network cabling.

TNC- See terminal node controller.

token ring- A medium access method that provides multiple access to a ring type network through the use of a token. FDDI and IEEE 802.5 are token-ring standards.

top-down design- First defines high-level specifications directly satisfying network requirements, then defines the remaining elements in an order that satisfies the most specifications already determined.

topography- A description of the network's physical surface spots. Topography specifies the type and location of nodes with respect to one another.

topology- A description of the network's geographical layout of nodes and links.

TP0- OSI Transport Protocol Class 0 (Simple Class), useful only with very reliable networks.

TP4- OSI Transport Protocol Class 4 (Error Detection and Recovery Class), useful with any type of network. The functionality of TP4 is similar to TCP.

transceiver- A device for transmitting and receiving packets between the computer and the medium.

Transmission Control Protocol (TCP)- A commonly used protocol for establishing and maintaining communications between applications on different computers. TCP provides full-duplex, acknowledged, and flow-controlled service to upper-layer protocols and applications.

transport layer- Provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, while shielding the higher layers from the network implementation details.

TSB 67- See Technical Service Bulletin 67.

twisted-pair wire- Type of medium using metallic type conductors twisted together

to provide a path for current flow. The wire in this medium is twisted in pairs to minimize the electromagnetic interference between one pair and another.

UDP- See User Data Protocol.

unacknowledged connectionless service- A datagram-style service that does not involve any error-control or flow-control mechanisms.

unit testing- Type of testing that verifies the accuracy of each network component, such as servers, cables, hubs, and bridges. The goal of unit testing is to make certain the component works properly by running tests that fully exercise the internal workings of the component.

User Data Protocol (UDP)- A connetionless protocol that works at the OSI transport layer. UDP transports datagrams but does not acknowledge their receipt.

user profile requirements- Identify the attributes of each person who will be using the system, providing human factors that designers can use to select or develop applications.

WBS- See work breakdown structure.

WEP- See Wired Equivalent Privacy.

Wired Equivalent Privacy (WEP)- An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

wireless metropolitan area network- Provides communications links between buildings, avoiding the costly installation of cabling or leasing fees and the down time associated with system failures.

wireless network interface- Couples the digital signal from the end-user appliance to the wireless medium, which is air.