Computing Technology

To understand how wireless networking works, you first need to understand the basic elements of computer hardware, software, and networking. A quick review of the basics will help lay the foundation for the concepts in the later chapters. Let's start by examining the fundamental concepts of the computing and networking environment.

NOTE **Those readers who already have a firm grasp of the information in this chapter may choose to skip ahead to Chapter 2.**

The chapter is divided into two sections:

- *Computer architecture.* The hardware/software elements that create a computer system.
- *Network technology.* The internetworking elements that enable computer systems to communicate with each other.

Computer Basics

The fundamental building blocks of a computer describe its architecture. These hardware and software elements combine to create the entire computing *platform*. A computer's architecture has four basic elements:

- The central processing unit (CPU) and its related processes
- Random access memory (RAM), read-only memory (ROM), and other types of memory
- Various input/output (I/O) devices
- The operating system and software

CPU

The basic functions of modern computers haven't really changed much since John von Neumann's "stored program concept" and Alan Turing's "universal machine" propositions of the 1930s. Although the technology functionality has improved exponentially, the process of binary computation (XOR, NAND, and so on) remain basically unchanged, as do the fundamental concepts of the architecture.

The CPU contains an *arithmetic logic unit* (ALU). The ALU performs arithmetic and logical operations on the binary code of the computer. The CPU also contains other processing elements and functions, including program counters, control logic, accumulators, the instruction register, and other general-purpose registers.

Bus

The computer processing elements coordinate their activities by the means of a computer bus. A *computer bus* is a collection of electronic conductors running on a common plane and connecting these different computer functions.

THE VON NEUMANN ARCHITECTURE

An excellent short paper on John von Neumann can be found at: http://ei.cs.vt.edu/~history/VonNeumann.html. His insights into the organization of computing machines came to be known as the "von Neumann architecture." Von Neumann recognized the need for computers to process in parallel but also understood that computers employing sequential processing were much more likely to be constructed.

In contrast to CPU speed, which has been steadily and dramatically increasing for years, it is only recently that bus speed, previously a major limiting factor in the computer's architecture, has been radically altered and improved. Computers may have a bus speed of 33 MHz, 66 MHz, 100 MHz, or higher. A diagram of a computer bus is shown in Figure 1.1.

Memory

The term "memory" often causes confusion because a computer's architecture uses many different types of memory for many different functions. Let's look at the main types of memory:

Random access memory (RAM). RAM is directly addressable and alterable memory. RAM is *volatile*, meaning that data will be lost if the power is removed from the system. RAM is used for primary (sometimes called "real") memory storage. This is the high-speed memory directly addressable by the CPU and used for storage of instructions and data associated with the program being executed.

Cache memory. Cache memory is a very small amount of high-speed RAM used to dynamically store the most recently used data and computer instructions. It improves the performance of the CPU by storing data that is most frequently accessed. Cache memory greatly improves the execution time of various processes.

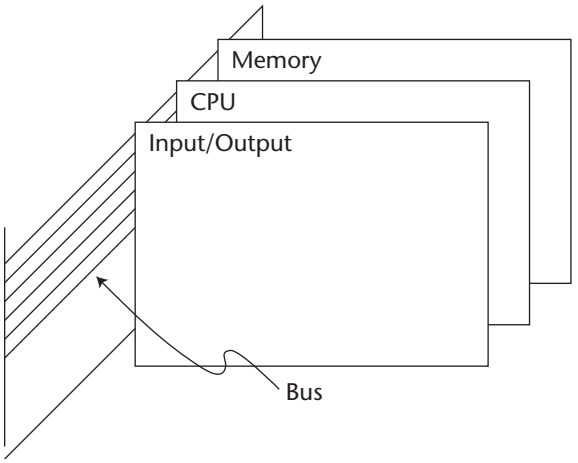

Figure 1.1 Computer bus.

INPUT/OUTPUT SYSTEMS

One of the CPU's primary functions is to interface with other devices such as input/output (I/O) adapters. I/O devices provide data buffering, and have timing and interrupt controls. Also, I/O adapters have addresses on the computer bus that are selected by computer instructions. An I/O adapter may support direct memory access (DMA), whereby data is transferred directly to and from memory without going through the CPU.

Read-only memory (ROM). ROM provides the computer with *nonvolatile* storage, which means the data is (relatively) permanent. Nonvolatile storage retains its information even when the computer loses power. ROM is used to hold programs and data that is rarely changed, such as firmware. The contents of some ROM cannot be altered, whereas other ROM can be upgraded from the flash process, such as an EPROM.

Secondary memory. Secondary memory is a data storage area that, like ROM, is also nonvolatile. It is a larger, slower memory storage area, and consists of the familiar hard drives, floppy-disk drives, zip drives, and tapes. These are referred to as secondary memory.

Virtual memory. Virtual memory is a combination of primary and secondary memory that creates a large addressable memory space. This space allows the processor to access much larger amounts of memory than the RAM alone would be able to address. The Windows swap file is an example of virtual memory.

A typical memory hierarchy is depicted in Figure 1.2.

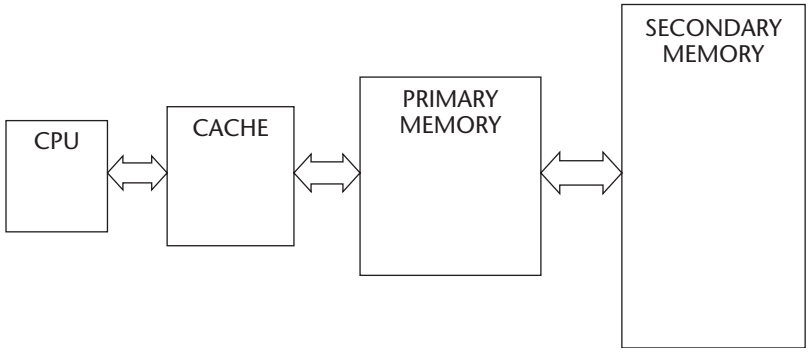

Figure 1.2 Computer memory hierarchy.

OPEN VERSUS CLOSED SYSTEMS

Open systems are vendor-independent and have published specifications that allow interoperability with other vendors' products. Closed systems use vendor-dependent proprietary hardware and/or software that is usually not compatible with other vendors' systems.

Operating Systems and Software

The primary program that controls the operations of the computer is called an operating system (OS). Windows NT, Windows 98, Windows 2000, Linux, and Unix are examples of operating systems. Operating systems manage various processes, such as memory and the file allocation tables.

The OS communicates with I/O systems through a controller, which is a device that interfaces with the peripherals and runs device drivers to communicate with the device. Examples of this type of controller are a disk controller, a network interface card (NIC), a modem, and a video controller.

Software

The CPU executes sets of instructions that tell the hardware what to do. These sets of instructions are grouped into various hierarchical levels of languages, which range from binary or mnemonic code (called assembly language) to high-level languages, like Java and BASIC.

High-level languages are converted into machine language through either interpreter or compiler programs. An interpreter operates on each high-level language source statement individually and executes the requested operation immediately, whereas a compiler first translates the entire software program into its corresponding machine language then executes them as a unit.

The high-level languages are grouped into five generations of languages (GLs), examples of which are listed in Table 1.1.

Table 1.1 Examples of Language Generations

LEVEL	DESCRIPTION
1 GL	The computer's binary machine language
2 GL	Assembly language
3 GL	BASIC, FORTRAN, C++
4 GL	FOCUS, NATURAL
5 GL	Artificial intelligence (AI) languages like LISP or Prolog

Network Technologies

In this book, the term *network technologies* refers to those hardware and software elements that allow computers to communicate with each other, whether to send email, surf the Web, or share a printer or documents. Since this book is about wireless networking, you should have some background in:

- Local area networks (LANs)
- Wide area networks (WANs)
- Virtual private networks (VPNs)
- Firewalls
- Protocols

Analog versus Digital

As shown in Figure 1.3 and Table 1.2, there are several differences between analog and digital signals. If you access the Internet via a dial-up connection at home, you probably are using a modem to create an analog circuit-switched connection. But analog technologies are more prone to interference; and they are less secure and run at slower speeds than digital technologies.

Digital has other advantages over analog as well. Long circuit-switched session setup and teardown times make analog networks unsuitable for high-speed networking, including wireless LANs. Also, digital communications can be managed by software, making it possible to build sophisticated communications switching products.

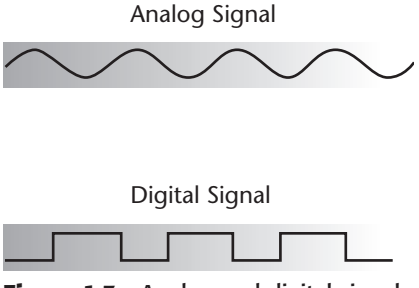

Figure 1.3 Analog and digital signals.

Table 1.2 Analog versus Digital Technologies

ANALOG	DIGITAL
Infinite wave form	Sawtooth wave form
Continuous signal	Pulses
Varied by amplification	On-off only

Local Area Networking

A data network consists of two or more computers connected for the purpose of sharing files, printers, exchanging data, email, and so on. To communicate via the network, every workstation must have a network interface card (NIC); a transmission medium such as copper, fiber, or wireless; and a network operating system (NOS). The networked computer usually connects to a network device of some sort (hub, bridge, router, or switch). Figure 1.4 shows common data networking components.

A local area network (LAN) is designed to operate in a specific limited geographic area. LANs connect workstations with file servers so they can share network resources like printers, email, and files. LAN devices are linked using a type of connection medium (copper wire, fiber optics) and use various LAN protocols and access methods to communicate through LAN devices (bridges, routers, wireless access points). LANs may be connected to a public switched network. Figure 1.5 shows three local area networks.

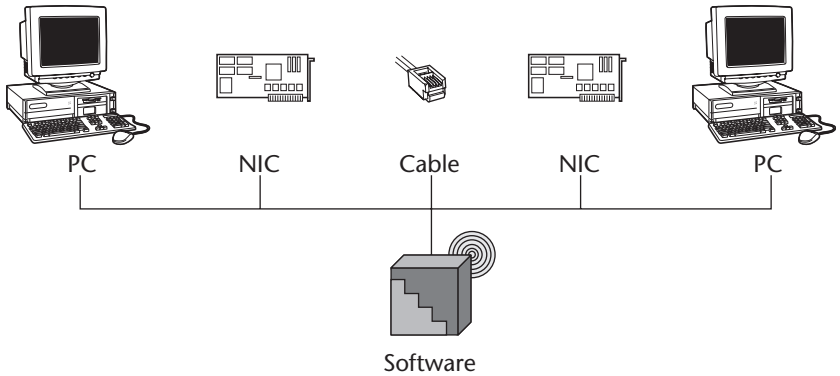

Figure 1.4 Data networking components.

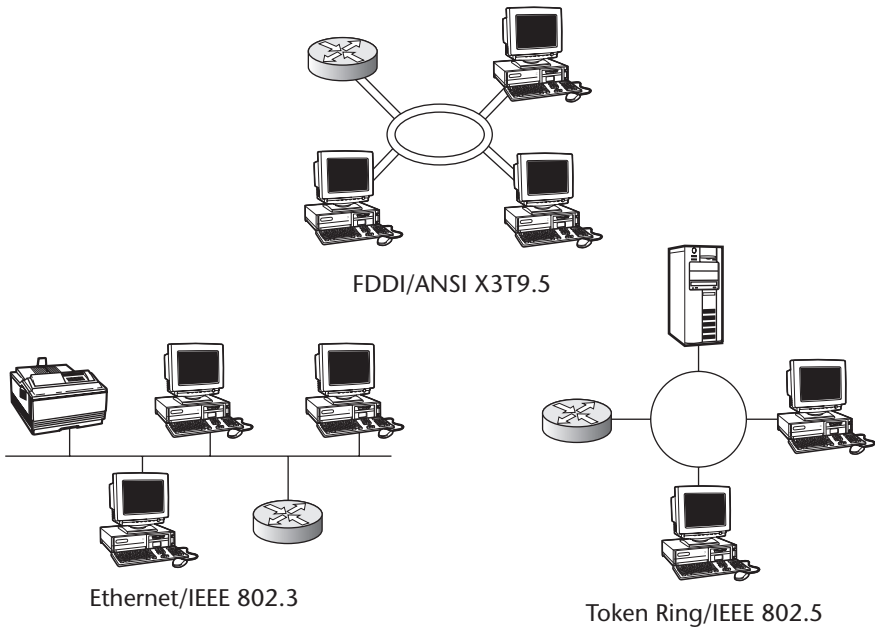

Figure 1.5 Local area networks.

LAN Topology

Common LAN topologies are *bus*, *ring*, and *star*. In a bus topology, all network node transmissions travel the full length of cable and are received by all other stations. Ethernet uses primarily this topology.

In a ring topology, the network nodes are connected by unidirectional transmission links to form a closed loop. Token ring and Fiber-Distributed Data Interface (FDDI) both use this topology.

In a star topology, the nodes of the network are connected directly to a central LAN device. Figure 1.6 shows a common bus Ethernet topology.

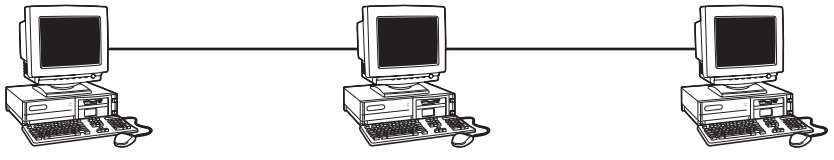

Figure 1.6 Bus topology.

The two most common LAN transmission protocol forms are carrier-sense multiple access with collision detection (CSMA/CD) used by Ethernet, and token passing, used in token ring and FDDI networks. Ethernet, ARCnet, token ring, and FDDI, the most common LAN types, use these transmission protocols.

Institute of Electrical and Electronic Engineers Standards

The Institute of Electrical and Electronic Engineers (IEEE) is a U.S. organization that participates in the development of standards for data transmission systems. IEEE has made significant progress in the establishment of standards for LANs by creating the IEEE 802 series of standards, which govern all LAN transmission methods and media access technology. Table 1.3 lists the various IEEE standards that relate to local area networking.

The LAN types are defined as follows:

Ethernet. Ethernet is a LAN media access method that uses CSMA/CD. Ethernet was originally designed to serve networks with sporadic, occasionally heavy traffic. Ethernet comes in three cabling types: thinnet coax, thicknet coax, and unshielded twisted pair (UTP). UTP is the most common of the three types, and 10BaseT/100BaseT cables and equipment are the most common. Figure 1.7 shows an Ethernet segment. Table 1.4 lists the various Ethernet 10Base standards and the types of cable used. Cable types are described later in this chapter.

Table 1.3 Common IEEE 802 Standards

STANDARD	DESCRIPTION
802.2	Specifies the logical link control (LLC).
802.3	Specifies a bus topology using CSMA/CD at 10 Mbps.
802.4	Specifies a token-passing bus access method
802.5	Specifies a token-passing ring access method.
802.10	Specifies LAN security and privacy access methods.
802.11	Specifies 1 Mbps and 2 Mbps wireless networks.
802.11a	Specifies high-speed wireless networking in the 5 GHz band up to 54 Mbps.
802.11b	Specifies high-speed wireless networking in the 2.4 GHz band up to 11 Mbps.
802.15	Specifies Bluetooth (see Chapter 2) LANs in the 2.4-2.5 GHz band.

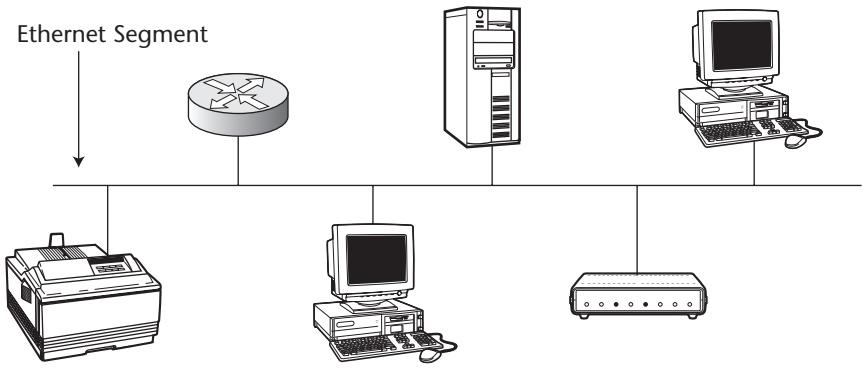

Figure 1.7 Ethernet segment.

ARCnet. ARCnet is one of the earliest LAN technologies. It provides predictable but slow network performance.

Token ring. IBM originally developed token ring in the 1970s. Although it was originally the primary LAN network type, it was eventually surpassed in popularity by Ethernet. The term "token ring" can refer to either IBM's Token Ring network (in which case, it is capitalized to indicate it is a trademarked name) or any IEEE 802.5 network. In a token ring network, all end stations are attached to a device called a multistation access unit (MSAU).

Table 1.4 10Base Ethernet Standards

STANDARD	DESCRIPTION
10Base2	10 Mbps thinnet coax rated to 185 meters
10Base5	10 Mbps thicknet coax rated to 500 meters
10BaseF	10 Mbps baseband optical fiber
10BaseT	10 Mbps UTP rated to 100 meters
10Broad36	10 Mbps broadband rated to 3600 meters
100BaseT	100 Mbps UTP
1000BaseT	1000 Mbps UTP

TOKEN-PASSING BUS NETWORKS

A token-passing bus network uses a logical token-passing access method. Unlike a token-passing ring, permission to transmit is based on the node address rather than the position in the network. It uses a shared single cable with all the data broadcast across the entire LAN.

Fiber Distributed Data Interface (FDDI). Similar to token ring, FDDI is a token-passing media access topology. It consists of dual rings operating at 100 Mbps, commonly over fiber optic cabling, although a version using category 5 copper cable exists, called Copper Distributed Data Interface (CDDI). FDDI employs a token-passing media access with dual counter-rotating rings, with only one ring active at any given time. If a break or outage occurs, the ring will wrap back in the other direction, keeping the ring intact.

LAN Cabling

LAN cabling comes in three common varieties: coaxial (called coax), unshielded twisted pair (called UTP), and fiber optic. Let's briefly look at each type.

Unshielded twisted pair (UTP). UTP wiring consists of four wire pairs (eight connectors) individually insulated and twisted together. UTP comes in several categories based on how tightly the insulated copper strands are twisted together. The tighter the twist, the higher the rating and its resistance against interference and attenuation. Table 1.5 shows the various categories of UTP cabling.

Table 1.5 UTP Cable Categories

CATEGORY	DESCRIPTION
Category 1	Used for early analog telephone communications; not suitable for data.
Category 2	Used in early token ring networks; rated for 4 Mbps.
Category 3	Common in 10BaseT networks; rated for 10 Mbps.
Category 4	Common in later token ring networks; rated for 16 Mbps.
Category 5	Current standard; rated for 100 Mbps.
Category 6	Rated for 155 Mbps.
Category 7	Rated for 1 Gbps.

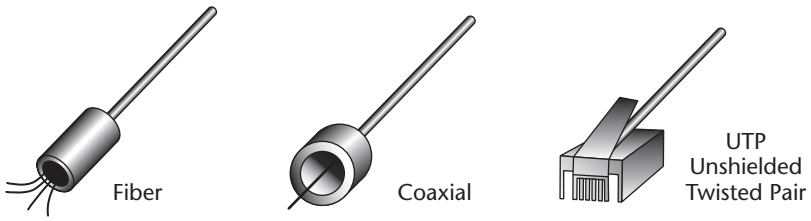

Figure 1.8 LAN cable types.

Coaxial cable. Coaxial cable (commonly called coax) consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor. Coax comes in two common types: thinnet (RG58), and thicknet (RG8 or RG11). Because the shielding reduces the amount of electrical noise interference, coax can extend to much greater lengths than twisted pair wiring.

Fiber optic. Fiber optic cable is a physical medium capable of conducting modulated light transmission, thereby creating higher transmission speeds and greater distances. It is the most resistant to electromagnetic interference. Fiber optic cable is a very reliable cable type but is very expensive to install and terminate.

Figure 1.8 shows the three different LAN cable types.

LAN Network Devices

LANs are connected by communication devices, such as hubs, bridges, routers, switches, or gateways. Let's take a look at these.

Hubs. Hubs amplify the data signals to extend the length of the network segment and help compensate for signal deterioration due to attenuation. They don't add any intelligence to the process; that is, they don't filter packets, examine addressing, or alter anything in the data packet. Hubs are used to connect LAN devices into a concentrator. Figure 1.9 shows a hub or repeater.

Bridges and switches. Bridges are like hubs, but they add some intelligence. A bridge forwards the data to all other network segments if the media access control (MAC) or hardware address of the destination computer isn't on the local network segment. If the destination computer is on the local network segment, it doesn't forward the data. Figure 1.10 shows a bridged network. A switch is similar to a bridge or a hub, except that a switch will send the data packet only to the specific port where the destination MAC address is located, rather than to all ports attached to the hub or bridge. This improves performance.

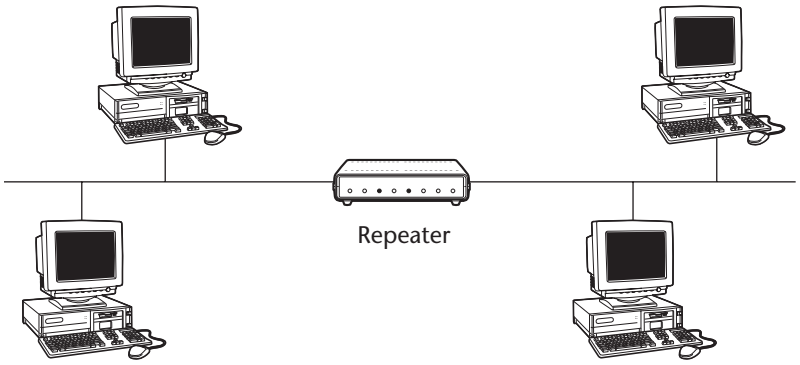

Figure 1.9 Hub or repeater.

Routers. Routers add even more intelligence to the process of forwarding data packets. A router opens up the data packet and reads either the hardware or network address (IP address) before forwarding it, then forwards the packet only to the network to which the packet was destined. This prevents unnecessary network traffic from being sent over the network by blocking broadcast information and blocking traffic to unknown addresses. Figure 1.11 is an example of a routed network.

Gateways. Gateways are primarily software products that can be run on computers or other network devices. They can be multiprotocol (link different protocols) and can examine the entire packet.

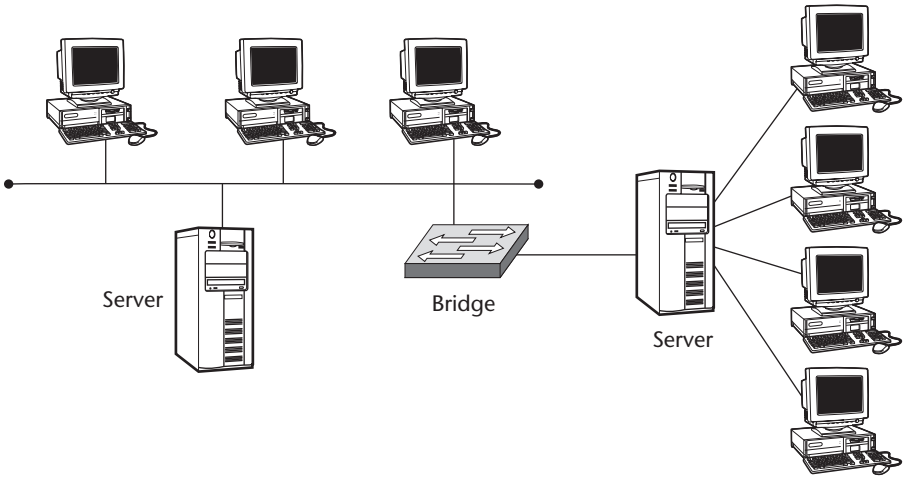

Figure 1.10 Bridged network.

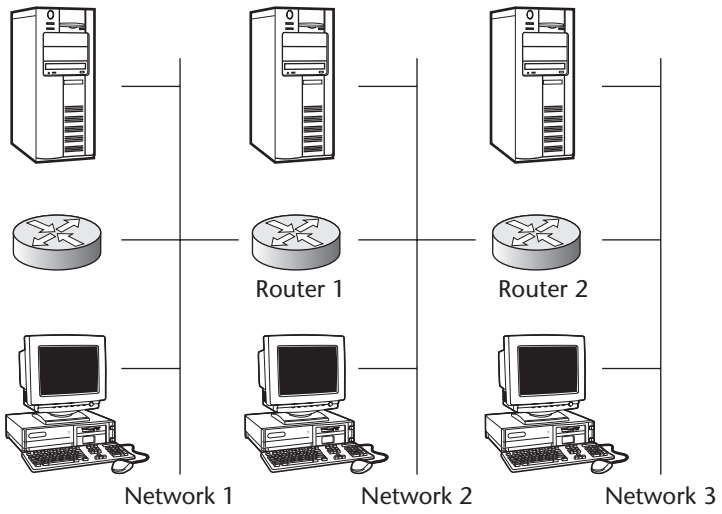

Figure 1.11 Routed network.

Wireless Access Protocol (WAP) gateway. A gateway device, called a WAP gateway, is used to serve HTML-style content to WAP-enabled devices, such as Internet-enabled cell phones. WAP gateways are discussed in more detail in Chapter 3.

Wireless access points (APs). An AP functions like a bridge or router, but is made for wireless, 802.11 communications. The most common APs on the market today are 802.11b Ethernet-compatible, but a new Ethernet format with a faster transmission speed, 802.11a, is becoming available for the home and office market. However, 802.11b will continue to dominate the market for some time. A more complete description of wireless access points is given in Chapter 2. Figure 1.12 shows a common home networking 802.11b AP by GigaFast Ethernet[1]. Some APs made for use in the home or small office/home office (SOHO) often have several additional functions, for example:

- Broadband routing, to allow sharing of a single high-speed cable modem or DSL Internet line.
- Dynamic Host Configuration Protocol (DHCP) service, which provides the workstation with a usable IP address, and provides network address translation (NAT); see the NAT sidebar.
- Printer sharing through a printer server.
- Redundant dial-up access, in case of failure of the broadband line.

[1] www.gigafast.com

Figure 1.12 GigaFast 802.11b wireless access point.
(Courtesy of GigaFast Ethernet USA)

Figure 1.13 shows the GigaFast USB 802.11b network interface adapter. It is designed to operate with the Gigafast access point shown earlier, but like most 802.11b USB adapters, can operate with any WLAN-compliant network.

Figure 1.13 GigaFast 802.11b USB adapter.
(Courtesy of GigaFast Ethernet USA)

DOMAIN NAME SERVICE (DNS)

The Domain Name Service matches Internet URL (Uniform Resource Locator) requests with the actual address or location of the server providing that URL. DNS is a distributed database system used to map host names to IP addresses. The Domain Name Service is not to be confused with the Domain Name System (also abbreviated as DNS), which is a global network of servers that provide these domain name services.

Figure 1.14 shows an 802.11b AP manufactured by SMC Networks[2] with these additional routing features. Features of this kind were unheard of in the home or SOHO environment just a couple of years ago. SMC's most recent product introduction, the Barricade Plus Cable/DSL Broadband Router, offers integrated stateful packet inspection (SPI) and a VPN tunneling feature, which supports up to five VPN tunnels.

Another recent vendor with an entry into the 802.11b home or SOHO market is Belkin Components[3], more well known as a maker of cables and PC accessories. Like Gigafast and SMC, they offer several WLAN products, including a wireless Cable/DSL gateway router (shown in Figure 1.15), and a wireless USB network adapter (shown in Figure 1.16.)

Figure 1.14 SMC Barricade wireless broadband router.
(Courtesy of SMC Networks)

[2] www.smc.com
[3] www.belkin.com

Figure 1.15 Belkin Wireless Cable/DSL gateway router.
(Courtesy of Belkin Components)

Wide Area Networking

A wide area network (WAN) is a network of subnetworks that physically or logically interconnects LANs over a large geographic area. Basically, the WAN is everything outside of the LAN. It may be privately operated for a specific user community, it may support multiple communication protocols, or it may provide network connectivity and services via an interconnected public packet data network, like the Internet.

Circuit-Switched versus Packet-Switched Networks

Circuit-switching technology uses a dedicated physical circuit path between the sender and receiver for the duration of the connection, and consists of a physical, permanent data connection. Though this technology predates packet-switching, it is the preferred choice for communications that need to be continuously on and that have a limited distribution scope (one transmission path only). Modems and analog voice phone calls are circuit-switched.

NETWORK ADDRESS TRANSLATION

Network address translation (NAT) is the process of preventing a "real" IP address from being seen from outside the network. The Internet Assigned Numbers Authority (IANA) reserved three blocks of IP addresses for private networks: 10.0.0.0(10.255.255.255; 172.16.0.0(172.31.255.255; and 192.168.0.0(192.168.255.255. NAT masks the host's true IP address by translating it into a private, internal address.

Figure 1.16 Belkin USB network adapter.
(Courtesy of Belkin Components)

In contrast, packet-switching is a network communications technology that lets nodes share bandwidth with each other by sending packets. A packet-switched network (PSN) or packet-switched data network (PSDN) uses packet-switching technology for data transfer. Unlike circuit-switched networks, the data in packet-switched networks is broken up into relatively small units of data, called *packets*, and is then sent to the next destination based on the destination address contained within each packet. At that destination the packets are reassembled based on the originally assigned sequence numbers. Though the data is manhandled a lot in this process, it results in a network that is very resilient to error.

It's important to note that this type of communication between sender and receiver is known as connectionless communication, as opposed to connection-oriented dedicated communications. Dividing communications into packets allows the same data path to be shared. Packet-switched networks are more cost-effective than dedicated circuits because they generate virtual circuits that are created and discarded dynamically, in contrast to a static continuous dedicated circuit.

A couple of analogies might help to clarify the difference between dedicated and connectionless networks. Calling someone on the phone creates a dedicated circuit, because you've established a direct connection with the party at the other end. That party may or may not be the person you want to speak to, nevertheless, you know you made contact. A connectionless network can be likened to sending a letter: You write your message, address it, and mail it. If,

however, you divide the message into several parts, address each of them separately to the same person, then mail them, you have no way of confirming they will get there in the same order—or at all.

Packet-Switched Technologies

Examples of packet-switching networks are X.25, link access procedure balanced (LAPB), frame relay, Switched Multimegabit Data Services (SMDS), Asynchronous Transfer Mode (ATM), and voice over IP (VoIP). Most traffic over the Internet uses packet switching, and the Internet is basically a connectionless network.

X.25. A terminal interface standard for a packet-switching network. X.25 was developed by the Comité Consultatif International Télégraphique et Téléphonique (CCITT; in English, the International Telegraph and Telephone Consultative Committee) as the first public packet switching technology during the 1970s and is still available. It offers connection-oriented virtual circuits at 64 Kbps. It was designed to operate effectively regardless of the type of systems connected to the network. It has become an international standard and is now much more prevalent overseas than in the United States.

Link access procedure balanced (LAPB). Created for use with X.25, LAPB defines frame types and is capable of retransmitting, exchanging, and acknowledging frames, as well as detecting out-of-sequence or missing frames.

Frame relay. Frame Relay is an upgrade from X.25 and LAPB. It's a packet-switching interface that operates at data rates of 56 Kbps to 2 Mbps and utilizes no error correction. Carriers offer frame relay as permanent connection-oriented virtual circuit service.

Asynchronous Transfer Mode (ATM). ATM is a very high-bandwidth, low-delay technology that uses both switching and multiplexing. It uses 53-byte fixed-size cells instead of frames, like Ethernet. It can allocate bandwidth on demand, making it a good solution for bursty applications, that is, applications that require intensive bandwidth for short periods of time, rather than steady, constant bandwidth. It requires a high-speed, high-bandwidth medium such as fiber optics.

Switched Multimegabit Data Services (SMDS). SMDS is a high-speed technology used over public-switched networks. It helps companies exchange large amounts of data with other companies over WANs on a bursty, or noncontinuous, basis by providing connectionless bandwidth on demand.

Private Circuit Technologies

Private circuits evolved before packet-switching networks. A private circuit network is composed of a dedicated analog or digital point-to-point connection that joins geographically diverse networks. The following defines the types of private circuit technologies:

Dedicated and leased lines. A dedicated line is defined as a communications line that is indefinitely and continuously reserved for communication. A leased line is a type of dedicated line reserved by a communications carrier for the private use of a customer.

Serial Line Internet Protocol (SLIP). SLIP supports TCP/IP over low-speed serial interfaces. Windows NT computers can use TCP/IP and SLIP to communicate with remote hosts using Window's Remote Access Server (RAS) service. This is an older technology but still in use.

Point-to-Point Protocol (PPP). PPP is a specification used by data communications equipment for communicating over dial-up and dedicated links. It was built to replace the Serial Line Internet Protocol (SLIP), which only supported IP. PPP has built-in security mechanisms such as Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

Integrated Services Digital Network (ISDN). ISDN is combination of digital telephony and data-transport services offered by telecommunications carriers. It supports voice and other digital services (data, music, video) over existing telephone wires. It has recently been replaced by Digital Subscriber Line (DSL), described next.

Digital Subscriber Line (DSL). DSL is a broadband technology that uses existing twisted pair telephone lines to move high bandwidth data to remote subscribers, with download speeds commonly faster than upload speeds. The installation must be within 15,000 feet of a provider's central office (CO). Some types of DSL are: Asymmetric Digital Subscriber Line (ADSL), Single-Line Digital Subscriber Line (SDSL), High-Rate Digital Subscriber Line (HDSL), and Very-High-Data-Rate Digital Subscriber Line (VDSL).

Virtual Private Networking (VPNs)

A virtual private network (VPN) is created by building (often dynamically) a secure communications link between two nodes, using a secret encapsulation method. This link is commonly called a secure encrypted tunnel, although it's more accurately defined as an encapsulated tunnel, as encryption may or may not be used.

CABLE MODEMS

A cable modem is a broadband technology that is used like DSL, but with some differences. A cable modem is a shared connection, whereas DSL is a direct, unshared connection; therefore, speed can degrade during peak usage times. Also, a cable modem commonly has a larger starting bandwidth than DSL, which may offset the shared usage degradation.

VPN Communications Standards

The three most common VPN communications protocol standards are:

Point-to-Point Tunneling Protocol (PPTP). PPTP works at the data link layer of the Open Systems Interconnect (OSI) model, which is described shortly. It is designed for individual client-to-server connections as it allows only a single point-to-point connection per session. PPTP is commonly used by Windows clients for asynchronous communications. PPTP uses the native PPP authentication and encryption services.

Layer 2 Tunneling Protocol (L2TP). L2TP is a combination of PPTP and the earlier Layer 2 Forwarding Protocol (L2F); it, too, works at the data link layer. L2TP is an accepted tunneling standard for VPNs, as dial-up VPNs use this standard frequently. Like PPTP, it was designed for single point-to-point client-to-server connections. Multiple protocols can be encapsulated within the L2TP tunnel.

Internet Protocol Security (IPSec). IPSec operates at the network layer and allows multiple simultaneous tunnels. IPSec contains the functionality to encrypt and authenticate IP data. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec also encompasses network-to-network connectivity.

Firewalls

Let's look at three different types of firewall architectures. This will help when we discuss WAP gateways and security methodologies later. A firewall is a set of programs residing on a device on the perimeter of the network that protects the resources of a private network from users from other networks. An organization commonly installs a firewall to prevent outsiders from accessing its own private data resources and for controlling to what outside resources its own users have access.

Packet-Filtering Firewall

The simplest form of firewall is the packet-filtering firewall, also called a *screening router*. This type of firewall examines both the source and destination address of the incoming data packet and either blocks the packet or passes the packet to its intended destination network, usually the local network segment upon which it resides. The firewall can deny access to specific applications and/or services based on access control lists (ACLs), port numbers, or service numbers.

The packet-filtering firewall uses the information of the source and destination addresses of the incoming packet, the session's communications protocol, and the source and destination application port for the desired service. A packet-filtering router sits between the private trusted network and the untrusted network. Figure 1.17 illustrates a simple packet filtering firewall.

Application-Level Firewalls

An application-level firewall, or application layer gateway, is commonly implemented as a proxy server. The firewall transfers a copy of each authorized data packet from one network to another, thereby masking the origin of the data. This controls which services are allowed to be used by the workstation and aids in protecting the network from outsiders who may be trying to get information about the design of the network.

Stateful Inspection Firewall

In a stateful inspection firewall, data packets are captured by an inspection engine operating at the faster network layer; they are then queued and analyzed at higher OSI layers. This type of firewall is commonly faster than an application-level firewall while providing a thorough inspection of the data. The stateful inspection firewall examines the state and context of the incoming data packets and helps track connectionless protocols, like UDP.

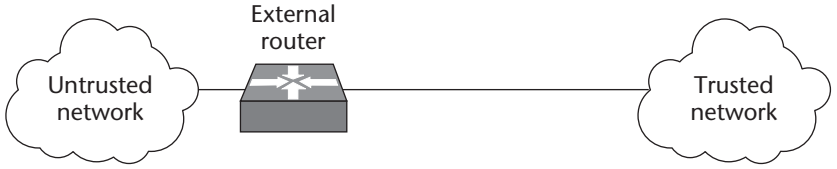

Figure 1.17 Packet-filtering firewall.

Protocols

A protocol describes the format that a message must be in when computers communicate; that is, protocols enable different types of computers to communicate despite their differences. They do this by describing a standard format and method for communications by adhering to a layered architecture model. A layered architecture divides communications processes into logical groups called *layers*.

Open Systems Interconnect (OSI) Model

The Open Systems Interconnection (OSI) model was created in the early 1980s by the International Standards Organization (ISO) to help vendors develop interoperable network devices. The OSI model describes how data and network information is communicated from one computer to another computer through the network media. This model breaks this information into seven distinct layers, each with a unique set of properties. Each layer directly interacts with its adjacent layers. The seven OSI layers are shown in Figure 1.18.

Application layer (layer 7). The application layer is the highest level of the OSI model and is the direct interface to the user. It supports the processes that deal with the communication aspects of an application. The application layer is responsible for identifying and establishing the availability of the intended communication partner. This layer is also responsible for determining whether sufficient resources for the intended communication exists.

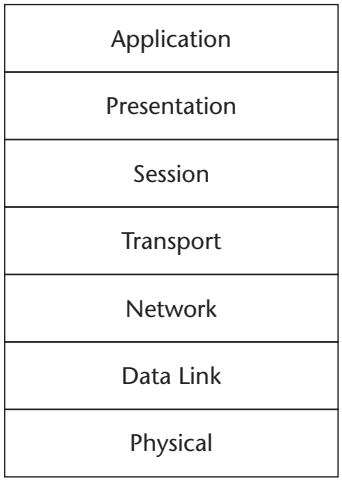

Figure 1.18 The OSI seven-layer reference model.

Presentation layer (layer 6). The presentation layer presents data to the application layer. It's essentially a translator. Tasks like data compression, decompression, encryption, and decryption are associated with this layer. The presentation layer defines how applications can enter the network.

Session layer (layer 5). The session layer makes the initial contact with other computers and sets up lines of communication. It formats the data for transfer between end nodes, provides session restart and recovery, and performs general maintenance of the session from end to end. It also splits up a communication session into three different phases: connection establishment, data transfer, and connection release.

Transport layer (layer 4). The transport layer is responsible for maintaining the end-to-end integrity and control of the session. It defines how to address the physical locations and/or devices on the network, makes connections between nodes, and handles the internetworking of messages. Services located in the transport layer both segment and reassemble the data from upper-layer applications and unite it onto the same data stream, provide end-to-end data transport services, and establish a logical connection between the sending host and destination host on a network.

Network layer (layer 3). The network layer defines how the small packets of data are routed and relayed between end systems on the same network or on interconnected networks. At this layer, message routing, error detection, and control of node data traffic are managed. Sending packets from the source network to the destination network is the network layer's primary function. The IP protocol operates at this layer.

Data link layer (layer 2). The data link layer defines the protocol that computers must follow to access the network for transmitting and receiving messages. Token ring and Ethernet operate within this layer, which establishes the communications link between individual devices over a physical link or channel. The data link layer ensures that messages are delivered to the proper device, and translates messages from above into bits for the physical layer (layer 1) to transmit. The data link layer formats the message into data frames and adds a customized header that contains the hardware destination and source address. It also contains the logical link control and the media access control (MAC) sublayers.

Physical layer (layer 1). The physical layer has only two responsibilities: to send and receive bits. The physical layer defines the physical connection between the computer and the network and converts the bits into voltages or light impulses for transmission. It defines the electrical and mechanical aspects of the interface of the device to a physical transmission medium, such as twisted pair, coax, or fiber.

Transmission Control Protocol/Internet Protocol (TCP/IP) Model

Transmission Control Protocol/Internet Protocol (TCP/IP) is the common name for the suite of protocols developed by the Department of Defense in the 1970s to support the construction of worldwide networks. The Internet is based on TCP/IP, which are the two best-known protocols in the suite.

As shown in Figure 1.19, TCP/IP adheres roughly to the bottom four layers of the OSI model. This figure reflects the original Department of Defense (DoD) concept of the TCP/IP model.

Application layer. This layer isn't really in TCP/IP, it's made up of whatever application is trying to communicate using TCP/IP. TCP/IP views everything above the three bottom layers as the responsibility of the application, so that the Application, Presentation, and Session layers of the OSI model are considered folded into this top layer. Therefore, the TCP/IP suite primarily operates in the Transport and Network layers of the OSI model.

Host-to-host layer. The host-to-host layer is comparable to the OSI transport layer. It defines protocols for setting up the level of transmission service. It provides for reliable end-to-end communications, ensures the error-free delivery of the data, handles packet sequencing of the data, and maintains the integrity of the data.

Internet layer. The Internet layer corresponds to the OSI network layer. It designates the protocols relating to the logical transmission of packets over the network. It gives network nodes an IP address and handles the routing of packets among multiple networks. It also controls the communication flow between hosts.

Network access layer. At the bottom of the TCP/IP model, the network access layer monitors the data exchange between the host and the network. The equivalent of the data-link and physical layers of the OSI model, it oversees hardware addressing and defines protocols for the physical transmission of data.

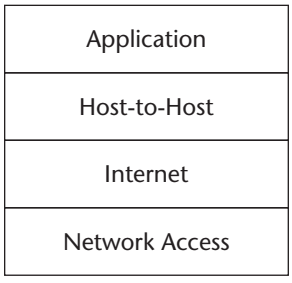

Figure 1.19 The DoD layered model for TCP/IP.

Table 1.6 TCP/IP Protocols

LAYER	PROTOCOL
Host-to-host	Transmission Control Protocol (TCP)
Host-to-host	User Datagram Protocol (UDP)
Internet	Internet Protocol (IP)
Internet	Address Resolution Protocol (ARP) l
Internet	Reverse Address Resolution Protocol (RARP)
Internet	Internet Control Message Protocol (ICMP)

TCP/IP Protocols

Let's look at the various protocols that populate the TCP/IP model. Table 1.6 lists some important TCP/IP protocols, and their related layers.

Transmission Control Protocol (TCP). TCP provides a full-duplex, connection-oriented, reliable connection. Incoming TCP packets are sequenced to match the original transmission sequence numbers. Any lost or damaged packets are retransmitted.

User Datagram Protocol (UDP). UDP is similar to TCP but gives only a "best effort" delivery, which means it offers no error correction, does not sequence the packet segments, and does not care in which order the packet segments arrive at their destination. Consequently, it's referred to as an *unreliable protocol*. It's also considered a connectionless protocol. Table 1.7 points out the differences between the TCP and the UDP protocols.

Internet Protocol (IP). IP provides an *unreliable datagram service*, meaning that it does not guarantee that the packet will be delivered at all, that it will be delivered only once, or that it will be delivered in the order in which it was sent.

On the Internet, and in networks using the IP protocol, each data packet is assigned the IP address of the sender and the IP address of the recipient. Each device then receives the packet and makes routing decisions based upon the packet's destination IP address.

Address Resolution Protocol (ARP). IP needs to know the hardware address of the destination of the packet so it can send it. ARP is used to match an IP address to an Ethernet address. An Ethernet address is a 48-bit address that is hard-wired into the NIC of the network node. ARP is used to match up the 32-bit IP address with this hardware address, technically referred to as the media access control (MAC) address or physical address.

Table 1.7 TCP versus UDP Protocol

TCP	UDP
Sequenced	Unsequenced
Connection-oriented	Connectionless
Reliable	Unreliable
High overhead	Low overhead
Slower	Faster

Reverse Address Resolution Protocol (RARP). In some cases, the reverse of the preceding is required: the MAC address is known but the IP address needs to be discovered. This is sometimes the case when diskless machines are booted onto the network. The RARP protocol sends out a packet that includes its MAC address along with a request to be informed of which IP address should be assigned to that MAC address. A RARP server responds with the answer.

Internet Control Message Protocol (ICMP). ICMP's primary function is to send messages between network devices regarding the health of the network. It can inform hosts of a better route to a destination if there is trouble with an existing route, and help identify the problem with a route. The Packet INternet Groper utility (PING) uses ICMP messages to check the physical connectivity of machines on a network.

Figure 1.20 shows how TCP/IP protocols correspond to the OSI model layers.

The Wireless Application Protocol

Chapter 2 addresses the Wireless Application Protocol (WAP) in more detail, but it's described briefly here to enable a comparison with the previous two protocol models, OSI and TCP/IP.

The WAP architecture is loosely based on the OSI model, and was created from the following layers (top to bottom):

Application layer. The WAP application layer is the direct interface to the user, and contains the wireless application environment (WAE), This top layer consists of several elements, including a microbrowser specification for Internet access, the Wireless Markup Language (WML), WMLScript, and wireless telephony applications (WTA).

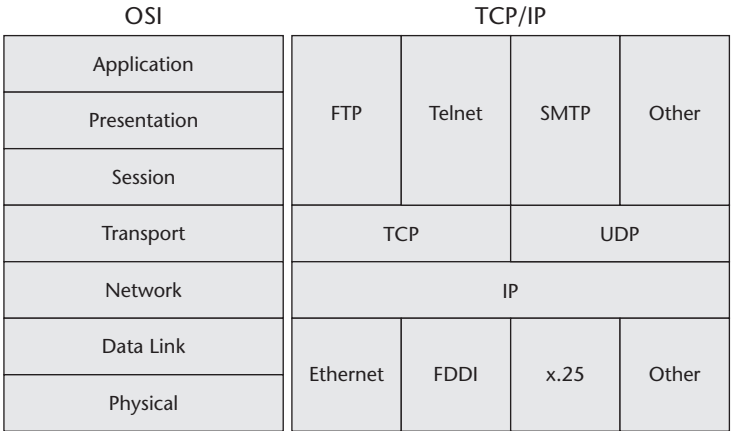

Figure 1.20 OSI model layers mapped to TCP/IP protocols.

Session layer. The WAP session layer contains the Wireless Session Protocol (WSP), which is similar to the Hypertext Transfer Protocol (HTTP), as it is designed for low-bandwidth, high-latency wireless networks. As explained in Chapter 3, WSP facilitates the transfer of content between WAP clients and WAP gateways in a binary format. Additional functionalities include content push and suspension/resumption of connections.

Transaction layer. The WAP transaction layer provides the Wireless Transactional Protocol (WTP), which provides the functionality similar to TCP/IP in the Internet model. WTP is a lightweight transactional protocol that allows for reliable request and response transactions and supports unguaranteed and guaranteed push.

Security layer. The security layer contains Wireless Transport Layer Security (WTLS). WTLS is based on Transport Layer Security (TLS, similar to the Secure Sockets Layer, or SSL). It provides data integrity, privacy, authentication, and denial-of-service (DoS) protection mechanisms.

Transport layer. The bottom WAP layer, the transport layer, supports the Wireless Datagram Protocol (WDP), which provides an interface to the bearers of transportation. It supports the CDPD, GSM, Integrated Digital Enhanced Network (iDEN), CDMA, TDMA, SMS, and FLEX protocols.

Figure 1.21 diagrams the layers of the Wireless Application Protocol.

Since you've immersed yourself in this chapter, you now have a good understanding of computing and network fundamentals. Now you're ready to take this knowledge into the next chapter, "Wireless Theory." Here you will begin to see the building blocks of wireless protocols and concepts.

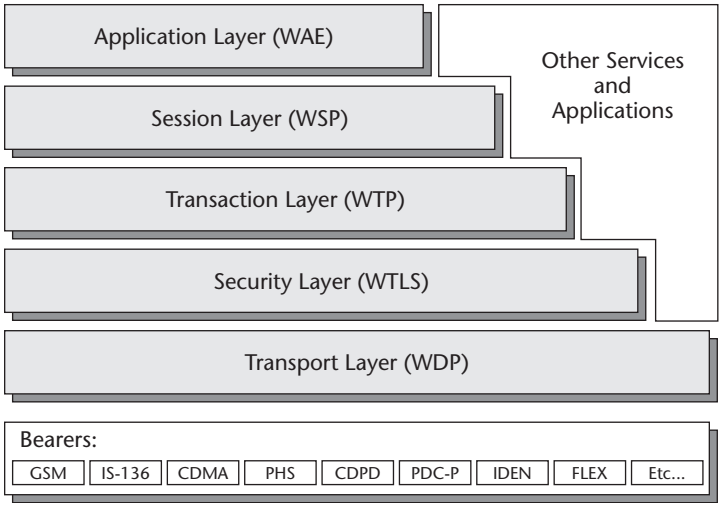

Figure 1.21 The Wireless Application Protocol.