APPENDIX

Check Your Understanding and Challenge Questions Answer Key

Chapter 1

Check Your Understanding

1. C. Instant messaging is the only answer that is both text based and real time.
2. B. An extranet provides as-needed access for external vendors and customers to a secure corporate network. An intranet is for internal users.
3. Wikis
4. C. Considering the importance of traffic flow when managing data is a function of a quality of service (QoS) strategy. Network administrators would evaluate the network traffic to determine a QoS strategy.
5. protocols
6. A, B. A quality of service strategy first classifies traffic based on requirements and then assigns priorities to the classifications as needed by the owners of the network. The network administrator can give different priorities to e-mail, web traffic, and movies.
7. media
8. B, D. Two components of a network's architecture are scalability, which is planning for growth, and fault tolerance, which includes redundant links. The other answers describe either users of the network or the product of it (data transfer).
9. icons
10. B, C, and E. Circuit-switched networks did not automatically establish alternative circuits in the event of circuit failure and required that an open circuit between network endpoints be established, even if data was not being actively transferred between locations. Also, the establishment of simultaneous open circuits for fault tolerance is costly.
11. A, B, C. Packet-switched, connectionless data communications technology can rapidly adapt to the loss of data transmission facilities and efficiently utilizes the network infrastructure to transfer data, and data packets can travel multiple paths through the network simultaneously. D and E refer to connections being established, which is not the nature of connectionless data communications.

12. router

13. B. QoS establishes priorities for different communications. It is not required to rate all network communication, just to give priority to what is deemed important.

14. B. Convergence is combining different technologies, such as telephone, video, and text, on one network platform.

15. packets

16. B. Only the cut cable pertains to infrastructure security. The others refer to content security. The unsecured wireless network might be allowed in network plans, but care must be taken to keep sensitive information beyond its reach.

Challenge Questions and Activities

1. B, D. It is possible that music and video downloads could take too much bandwidth and processing, disrupting the conference. Better QoS would give the video session priority over the download and avoid disruption.

2. C. The connection is established and exclusive, so it is privately circuit switched. Circuit-switched connections are connection oriented.

Chapter 2

Check Your Understanding

1. C. IP addressing is a concern of the OSI network layer (Layer 3). Physical addressing happens at OSI Layer 2.

2. channel

3. B, C. A MAC address is the physical address burned on to the OSI Layer 2 network interface card. Logical addressing happens at OSI Layer 3.

4. D. Encapsulating into TCP segments occurs at OSI Layer 4, so the next encapsulation is at OSI Layer 3, which includes adding source and destination IP addresses to the segment headers and converting them into packets. Then the physical addressing is added and the data is converted to bits.

5. B. A protocol describes a specific set of rules for communication, including message formatting and encapsulation.

6. proprietary

7. B. TCP has control features pertaining to OSI Layer 4, FTP is an application (Layer 7), and IP and TFTP are network layer protocols (Layer 3).

8. NIC, or network interface card

9. C. Segmentation, which occurs at OSI Layer 4, is the correct answer.

10. router

11. B. Multiplexing is the correct term.

12. A. IP addressing is an OSI Layer 3 function. All others are OSI Layer 2 functions.

13. B. The correct order is application, presentation, session, transport, network, data link, physical.

14. B. End-to-end message delivery is the concern of OSI Layer 4, the transport layer.

Challenge Questions and Activities

1. B, D, F, G. The OSI presentation and session layers are combined into the application layer of the TCP/IP model. The OSI data link and physical layers are combined into the network access layer of TCP/IP. The transport and network layers have parallel layers in TCP/IP.

2. C, E. LANs are connected by WANs. WANs connect networks through telephone service providers (TSP). Logical addressing is used between networks, and physical addressing, or MAC addresses, are used inside LANs.

Chapter 3

Check Your Understanding

1. D. Layer 7 is the application layer and its components: applications, services, and protocols.

2. B. The functionality of the TCP/IP application layer protocols fits roughly into the framework of the top three layers of the OSI model: application, presentation, and session.

3. C. Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the web pages of the World Wide Web. DNS is used to resolve Internet names to IP addresses, and Telnet is used to provide remote access to servers and networking devices.

4. D. Post Office Protocol (POP) uses UDP port 110.

5. A. GET is a client request for data.

6. D. E-mail, the most popular network service, has revolutionized how people communicate through its simplicity and speed. Choice A. is incorrect, because HTTP is a protocol, not a service.
7. B. To successfully transfer files, FTP requires two connections between the client and the server: one for commands and replies and another for the actual file transfer.
8. C. The Dynamic Host Configuration Protocol (DHCP) enables clients on a network to obtain IP addresses and other information from a DHCP server.
9. A. The Linux and UNIX operating systems provide a method of sharing resources with Microsoft networks using a version of SMB called SAMBA.
10. C. A connection using Telnet is called a VTY session, or connection.
11. eBay is a client/server application. eBay is implemented as a web server that responds to web client (browser) requests using HTTP.
12. client. Even though a device can serve as a client and a server at times, the device requesting a service is defined as the client and the device providing the service is defined as the server.
13. GET, PUT, and POST. GET is a request; PUT and POST provide uploading.
14. Assignment of IP addresses, subnet masks, and default gateway. The protocol automates the assignment of IP addresses, subnet masks, gateway, and other IP networking parameters.
15. FTP stands for File Transfer Protocol. It is used to move files on the network. FTP was developed to allow file transfers between a client and a server. An FTP client is an application that runs on a computer that is used to push and pull files from a server.

Challenge Questions and Activities

1. 1. The user inputs data using a hardware interface.

   2. The application layer prepares human communication for transmission over the data network.

   3. Software and hardware convert data to a digital format.

   4. Application services initiate the data transfer.

   5. Each layer plays its role, and the OSI layers encapsulate data down the stack. Encapsulated data travels across the media to the destination. OSI layers at the destination decapsulate the data up the stack.

   6. Data is ready to be processed by the end device.

2. Application software has two forms: applications and services:

   - Applications are designed to interact with us. Application is software for the user. If the device is a computer, the application is typically initiated by the user. Although there can be many layers of support underneath, application software provides an interface between humans and the hardware. The application will initiate the data transfer process when the user clicks the Send button or performs a similar action.

   - Services are background programs that perform a particular function in the data network. Services are invoked by a device connecting to the network or by an application. For example, a network service can provide functions that transmit data or provide conversion of data in a network. In general, services are not directly accessible or seen by the end user. They provide the connection between an application and the network.

3. The source end of data communication is referred to as the *server*, and the receiving end is called the *client*. The client and server processes are application layer services that provide the foundation for data network connectivity.

   In some cases, the servers and clients are devices that perform that role specifically and exclusively. For example:

   - A central file server can contain an organization's business data files that employees access using their client-only workstation.

   - Internet-based examples include web servers and mail servers, where many users access a centrally provided service.

   - In other situations, such as file sharing over a home network, individual devices can perform both server and client roles at different times.

     Servers are both a repository and a source of information such as text files, databases, pictures, video, or audio files that have been previously recorded.

     Client processes at the other end of the communication across the data network allow the user to make requests to obtain the data from a server. The client software typically uses a program initiated by a user. The client initiates communication data flow from the server by sending requests for the data to the server. The server responds by starting to send one or more streams of data to the client. In addition to the actual data transfer, this exchange can include user authentication and identification of the data file to be transferred.

   Examples of common client/server services include the following:

   - DNS (Domain Name Service)

   - FTP

- HTTP
- Telnet (Teletype Network Service)

4. Client/server data transfer specifically refers to the centralized source end of data communication as the server and the receiving end as the client.

   With peer-to-peer data transfer, both client and server services are used within the same conversation. Either end of the communication can initiate the exchange, and both devices are considered equal in the communication process. The devices on either end of the communication are called peers.

   In contrast to a client/server model, where a server is typically a centralized repository and responds to requests from many clients, peer-to-peer networking has distributed data. Furthermore, after the communication is established, the peers communicated directly; the data is not processed at the application layer by a third device on the network.

5. Functions specified by application layer protocols include

   - The processes that are to occur at either end of the communication. This includes what has to happen to the data and how the data is to be structured.
   - The types of messages. These can include requests, acknowledgments, data messages, status messages, and error messages.
   - The syntax of the message. This gives the expected order of information (fields) in a message.
   - The meaning of the fields within specific message types. The meaning has to be constant so that the services can correctly act in accordance with the information.
   - The message dialogs. This determines which messages elicit which responses so that the correct services are invoked and the data transfer occurs.

6. DNS, HTTP, SMB, and SMTP/POP use a client/server process.

   - Domain Name System (DNS) provides users with an automated service that matches or resolves resource names and e-mail domains with the required numeric device network addresses. This service is available to any user connected to the Internet and running an application layer application such as a web browser or e-mail client program.
   - HTTP was originally developed to publish and retrieve HTML pages and is now used for distributed, collaborative, hypermedia information systems. HTTP is used by the World Wide Web (WWW) to transfer data from web servers to web clients.

- Server Message Block (SMB) describes the structure of sharing network resources, such as directories, files, printers, and serial ports, between computers.
- Simple Mail Transport Protocol (SMTP) transfers outbound e-mails from the e-mail client to the e-mail server and transports e-mail between e-mail servers and so enables e-mail to be exchanged over the Internet.
- POP, or POP3 (Post Office Protocol version 3), delivers e-mail from the e-mail server to the client.

7. DNS includes standard queries, responses, and data formats. DNS protocol communications are carried in a single format called a message. This message format is used for all types of client queries and server responses, for error messages, and for the transfer of resource record information between servers.

   HTTP is a request/response protocol:

   - A client application layer application, typically a web browser, sends a request message to the server.
   - The server responds with the appropriate message.

   HTTP also includes messages to upload data to the server, such as when completing an online form.

   SMB messages use a common format to

   - Start, authenticate, and terminate sessions
   - Control file and printer access
   - Allow an application to send or receive messages to or from another device

   SMTP specifies commands and replies that relate to session initiation, mail transaction, forwarding mail, verifying mailbox names, expanding mailing lists, and the opening and closing exchanges.

   POP is a typical client/server protocol, with the server listening for client connections and the client initiating the connection to the server. The server can then transfer the e-mail.

   DNS, HTTP, SMB, and SMTP/POP use client/server, request/response messages. Whereas users see the applications that use HTTP (a web browser), SMB (file manager), and SMTP/POP (e-mail client), a DNS operation underlies these applications and is truly transparent to the user.

Chapter 4

Check Your Understanding

1. B. Port 80 is the standard port number used with HTTP. Port 23 is Telnet, port 20 is FTP, and port 110 is POP3.
2. C. Port number 25 is used for SMTP.
3. A, D. TCP is a reliable, connection-oriented protocol.
4. C. TCP uses flow control to avoid buffer overflows.
5. D. Port numbers 0 to 1023 are the well-known () ports. Port numbers 1024 to 49151 are the registered ports and are used by the host for dynamic port allocation. Port numbers 49152 to 65535 are the private and dynamic ports.
6. D, E. The receiving host has to acknowledge receipt of the packets and then reassemble them in the right order.
7. Answers could vary and could include (a) keeping track of the individual conversations taking place between applications on the source and destination hosts, (b) segmenting data and adding a header to identify and manage each segment, (c) using the header information to reassemble the segments into application data, and (d) passing the assembled data to the correct application.
8. A. Sequence numbers are used in the TCP headers because segments could arrive at their destination in a different order than when they were sent. The numbers allow the receiving host to reassemble them in the proper order.
9. D. In TCP, window size is used to manage flow control.
10. D. Port numbers allow you to track multiple conversations generated by the same host using the same IP address.
11. Segmentation of the data, in accordance with transport layer protocols, provides the means to both send and receive data when running multiple applications concurrently on a computer.
12. Reliability means ensuring that each segment that the source sends arrives at the destination.
13. Web browsing, e-mail, file transfer.
14. DNS, video streaming, Voice over IP (VoIP).
15. The source and destination port number.
16. A sequence number allows the transport layer function on the destination host to reassemble segments in the order in which they were transmitted.

Challenge Questions and Activities

1. 7. The acknowledgment number is always one more than the last segment received.
2. D. A flag is set in the segment header. If this flag actually reads 17, it is identified as a UDP header.
3. B. Port 53 is used for DNS.
4. Netstat lists the protocol in use, the local address and port number, the foreign address and port number, and the state of the connection. Netstat also displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for IP, ICMP, TCP, and UDP), and IPv6 statistics (for IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6). Used without parameters, the **netstat** command displays active TCP connections.
5. TCP uses the acknowledgment number in segments sent back to the source to indicate the next byte in this session that the receiver expects to receive.

Chapter 5

Check Your Understanding

1. A. IP provides connectionless network layer services. TCP is connection oriented. UDP is connectionless, but it works at the transport layer.
2. **netstat -r** and **route print**.
3. A, C, D. A routing table contains the next-hop, metric, and destination network address. Routers do not need the source address, last hop, or default gateway to find a path to a network.
4. A, B, D. Reduced network bandwidth, increased overhead, and reduced host functions are three potential results of excessive broadcasts. The other answers can be part of a solution to the problem of excessive broadcasts.
5. Purpose, ownership, and geographic location are three key ways to divide a network.
6. C, D. Delivery reliability is a transport layer concern. Application data analysis is a concern of the presentation layer. Routing, addressing packets with an IP address, encapsulation, and decapsulation are functions of the network layer.
7. B, E. IP stands for the Internet Protocol, which operates at OSI Layer 3 (the network layer). IP encapsulates transport layer segments. IP does not look inside the upper-level PDU, so it has no knowledge of the presentation layer data.

8. Decapsulation.

9. C. Routers and hosts use IP. B is incorrect because IP uses addressing information in the header to determine the best path for a packet. D is incorrect because IP is a “best effort” unreliable protocol.

10. A, D. Network layer encapsulation adds a header to a segment and adds both source and destination IP addresses. Network layer encapsulation happens only on the original host; other devices can read the data, but they do not remove or alter it until the destination network is reached. The network layer converts transport layer segments into packets.

11. B, C. TCP is reliable and connection oriented. IP is unreliable and connectionless. IP operates at the network layer.

12. B. IP encapsulates OSI Layer 4 data. IP can carry voice, video, and other types of data, but “media independent” refers to the OSI Layer 1 medium that carries the data across the networks. IP, or any other communication, can occur without a physical (OSI Layer 1) medium.

13. transport

14. 32. There are four octets (8 bits each) in an IPv4 address.

15. C, E. Dynamic routing adds packet-processing overhead, and routers can use static and dynamic routing simultaneously. Static routing does not require a routing protocol. A default route is an example of a static route. Because static routes must be manually configured and updated, they add to administrative overhead.

Challenge Questions and Activities

1. A, C. When the TTL is 1, it has one hop remaining to be either delivered or discarded. IP does not provide return notification of dropped packets. TCP controls at the destination will request a packet retransmission, but the TCP PDU is never accessed en route.

2. D. The destination host will send a request if the packet does not arrive. IP is connectionless, so there is no reliability built into the protocol. Previous packets with TCP information have arrived at the destination host with “expectational” information. Routing protocols, such as RIP, are used by routers to share route information; they are not involved in TCP/IP reliability.

Chapter 6

Check Your Understanding

1. B, D. 192.168.12.64 /26 and 198.18.12.16 /28 are network addresses.

2. B. 172.31.255.128 /27

3. C. 255.255.252.0

4. B. The four networks are .224, .228, .232, and .236.

5. Hosts with the same network portion of their IPv4 address.

6. The three types of IPv4 addresses are

   - **Network address:** The address by which you refer to the network
   - **Broadcast address:** A special address used to send data to all hosts in the network
   - **Host addresses:** The addresses assigned to the end devices in the network

7. C. 255.255.255.224 provides the 16 addresses required. .224 will provide 30. .240 will provide only 14.

8. The three types of IPv4 addresses are

   - **Network address:** Lowest address in the network 0 for each host bit in the host portion of the address.
   - **Host address:** Host bits are a unique mix of 1s and 0s within a network.
   - **Broadcast address:** Uses the highest address in the network range. The host portion is all 1s.

9. Following are the three forms of IPv4 communication:

   - **Unicast:** The process of sending a packet from one host to an individual host
   - **Broadcast:** The process of sending a packet from one host to all hosts in the network
   - **Multicast:** The process of sending a packet from one host to a selected group of hosts

10. Specified private addresses allow network administrators to allocate addresses to those hosts that do not need to access the Internet.

11. A. The host is using a link-local address. Link-local addresses should not be routed.

12. The allocation of addresses inside the networks should be planned and documented for the following purposes:

    - Preventing duplication of addresses
    - Providing and controlling access
    - Monitoring security and performance

13. Administrators should statically assign addresses to servers, printers, LAN gateway addresses on routers, management addresses on network devices such as switches, and wireless access points.

14. Running out of IPv4 addresses is the primary motivation for developing IPv6.

15. Network devices use the subnet mask to determine the network or subnet address of an IP address that the device is processing.

16. Networks are subnetted to overcome issues with location, size, and control. In designing the addressing, consider these factors for grouping the hosts:

    - Grouping based on common geographic location
    - Grouping hosts used for specific purposes
    - Grouping based on ownership

17. Three tests that use the ping utility are

    - Ping 127.0.0.1: Loopback test to test IP operation
    - Ping the host gateway address or another host on the same network: To determine communication over the local network
    - Ping a host on a remote network: Test device default gateway and beyond

Challenge Questions and Activities

1. The reserved and special IPv4 addresses are

    - **Multicast addresses:** Reserved for special purposes is the IPv4 multicast address range 224.0.0.0 to 239.255.255.255.
    - **Private addresses:** The private address blocks are
        - 10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
        - 172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
        - 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

      Private space address blocks are set aside for use in private networks. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses.

    - **Default route:** The IPv4 default route is 0.0.0.0. The use of this address reserves all addresses in the 0.0.0.0 to 0.255.255.255 (0.0.0.0 /8) address block.

- **Loopback:** The IPv4 loopback address 127.0.0.1 is a reserved address. Addresses 127.0.0.0 to 127.255.255.255 are reserved for loopback, where hosts direct traffic to themselves.
- **Link-local addresses:** IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.
- **Test-net addresses:** The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples. Unlike the experimental addresses, network devices will accept these addresses in their configurations.

2. IPv4 is an unreliable best-effort protocol. ICMPv4 provides a means for network problems such as dropped packets or congestion to be reported to the source network or host. Messages include
   - Host Conformation
   - Unreachable Destination or Service
   - Time Exceeded
   - Route Redirection
   - Source Quench

Chapter 7

Check Your Understanding

1. The data link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer to create a frame.
2. MAC methods for shared media are as follows:
   - **Controlled:** Each node has its own time to use the medium, a ring topology
   - **Contention-based:** All nodes compete for the use of the medium, a bus topology

   Media access control in point-to-point connections can be one of the following:
   - **Half duplex:** A node can only transmit or receive at one time.
   - **Full duplex:** A node can both transmit and receive at the same time.

3. In a logical ring topology, each node in turn receives a frame. If the frame is not addressed to a node, the frame is passed to the next node. If there is no data being transmitted, a signal (known as a token) can be placed on the media. A node can place a frame on the media only when it has the token. This is a controlled media access control technique called token passing.

4. Layer 2 protocols include

   - Ethernet
   - PPP
   - High-Level Data Link Control (HDLC)
   - Frame Relay
   - ATM

5. Typical frame header fields include

   - **Start Frame field:** Indicates the beginning of the frame
   - **Source and Destination address fields:** Indicate the source and destination nodes on the media
   - **Priority/Quality of Service field:** Indicates a particular type of communication service for processing
   - **Type field:** Indicates the upper-layer service contained in the frame
   - **Logical connection control field:** Used to establish a logical connection between nodes
   - **Physical link control field:** Used to establish the media link
   - **Flow control field:** Used to start and stop traffic over the media
   - **Congestion control field:** Indicates congestion in the media

6. A. The node drops the frame. The CRC provides error detection, not error correction, so B is incorrect. C is incorrect because the frame is not forwarded. The interface is not disabled, so D is incorrect.

7. C, D. PPP and HDLC are designed as WAN protocols. 802.11 and Ethernet are LAN protocols, so A and B are incorrect.

8. B. The network layer PDU is encapsulated in the frame. The number of bytes in the payload is variable, so A is incorrect. C is incorrect because the Layer 2 source address is in the address field of the frame header. The data from the application undergoes encapsulation before being passed down to the data link layer, so D is incorrect.

9. B. Nodes compete for the media. Option A is incorrect because contention-based is used on shared media. C is incorrect because one of the primary purposes of Layer 2 is MAC. D is incorrect because taking turns is a function of controlled access.

10. B, C. LLC is the upper sublayer, and MAC is the lower sublayer.

11. D. Virtual circuits establish a logical connection between two devices to provide a logical point-to-point topology. Option A is incorrect because CRC is an error-detection technique. Virtual circuits do not provide an encapsulation technique, so B is incorrect. C is incorrect because virtual circuits can be used over multiple types of physical topologies.

12. Header, data, and trailer.

13. C. The data link layer provides the connection between hardware and software. A is incorrect; this is a role of the application layer. B is incorrect; this is a function of the network layer. D is incorrect; this is a function of the transport layer.

14. D. The logical topology influences MAC. The logical topology can be many types of MAC, so A is incorrect. The MAC sublayer provides the physical address, so B is incorrect. The logical and physical topologies are not always the same, so C is incorrect.

Challenge Questions and Activities

1. The media is a potentially unsafe environment for data. The signals on the media could be subject to interference, distortion, or loss that would substantially change the bit values that those signals represent. To ensure that the content of the received frame at the destination matches that of the frame that left the source node, a transmitting node creates a logical summary of the contents of the frame. This is known as the Frame Check Sequence (FCS) and is placed in the trailer to represent the contents of the frame.

   When the frame arrives at the destination node, the receiving node calculates its own logical summary, or FCS, of the frame. The receiving node compares the two FCS values. If the two values are the same, the frame is considered to have arrived as transmitted. If the FCS values differ, the frame is discarded.

   There is always the small possibility that a frame with a good FCS result is actually corrupt. Errors in bits can cancel each other out when the FCS is calculated. Upper-layer protocols would then be required to detect and correct this data loss.

2. Unlike Layer 3 logical addresses that are hierarchical, physical addresses do not indicate on what network the device is located. If the device is moved to another network or subnet, it will still function with the same Layer 2 physical address.

   Because the frame is only used to transport data between nodes across the local media, the data link layer address is only used for local delivery. Addresses at this layer have no meaning beyond the local network. Compare this to Layer 3, where addresses in the packet header are carried from source host to destination host, regardless of the number of network hops along the route.

3. A logical point-to-point topology connects two nodes directly. In data networks with point-to-point topologies, the MAC protocol can be very simple. All frames on the media can only travel to or from the two nodes. The frames are placed on the media by the node at one end and taken off the media by the node at the other end. In point-to-point networks, if data can only flow in one direction at a time, it is operating as a half-duplex link. If data can successfully flow across the link from each node simultaneously, it is a full-duplex service.

   A logical multiaccess topology enables a number of nodes to communicate by using the same shared media. Data from only one node can be placed on the medium at any one time. Every node sees all the frames that are on the medium, but only the node to which the frame is addressed processes the contents of the frame. Having many nodes share access to the medium requires a data link MAC method to regulate the transmission of data and thereby reduce collisions between different signals.

4. If a router is interfacing media of different speeds, the router will have to buffer the frames for transmission. If not enough buffers are available, the packets can be lost.

5. The source addresses are used to identify the source node. In most cases, Layer 2 source addresses are not used. The most common use of source addresses is for security or by switches learning where the host exists. The source address is also used in the creation of dynamic maps such as ARP.

   Both ATM and Frame Relay use a single address in the frame header. These technologies use a single number that represents a connection.

6. The full-duplex communication between the two nodes could have twice the throughput of half-duplex and more than twice the throughput of multiaccess. If the underlying physical media can support it, the two nodes might be able to transmit and receive at full media bandwidth at the same time. This would be twice that of half duplex. Because multiaccess has overhead to control media access, the throughput is less than the bandwidth and, in many cases, much less. This would allow full duplex to have more than twice the throughput of multiaccess.

7. As the router receives a frame on one interface, it decapsulates the frame down to a packet. It then refers to the routing table to determine out which interface the packet should be forwarded. The router then will encapsulate the packet into a frame of the appropriate size for the segment connected to the outbound interface.

Chapter 8

Check Your Understanding

1. physical media

2. D. Encoding represents the data bits by using different voltages, light patterns, or electromagnetic waves as they are placed onto the physical media.

3. NRZ (nonreturn to zero) and Manchester

4. D. The chief purpose of the physical layer is to define the functional specifications for links between end systems and the electrical, optical, and radio signals that carry data. Reliability, path selection, and media access are the tasks of other layers.

5. RJ-45

6. B. Crosstalk is reduced by the twisting of cables in the UTP (unshielded twisted-pair) cable. UTP has no cladding, shielding, or grounding points.

7. pinout

8. B, D, F. The advantages of using fiber-optic cabling include immunity to electromagnetic interference, longer maximum cable length, greater bandwidth reception and decoding requirements, and antenna design.

9. wireless. Because wireless is open to anyone with a wireless receiver, it is more susceptible to security breaches than copper or fiber-optic media.

10. C. Cladding helps prevent light loss. No other listed functions pertain to fiber-optic cable.

11. B, C. Rollovers work in Cisco console ports, and crossovers would connect two switches.

12. rollover cable

13. C. Throughput measures actual data rates. Bandwidth is the line capacity, and goodput measures only the rate of usable application layer data bits that arrive.

14. C. 1 Mbps = 1,000,000 (10^6) bps

15. B. Synchronization between devices allows them to know when frames begin and end.

16. B. Bit time changes depending on the speed of the NIC. The time it takes a bit to traverse the network is slot time (which counts bits, not bytes).

Challenge Questions and Activities

1. B. The two hosts with straight-through cables will link to the hub. The third host is using the original cable, which is a crossover cable appropriate for peer-to-peer connections, but will not link to a hub from a host.
2. A, C, E. A: The A wing, having the most connected workers, can have too much traffic on the cable and packets can be getting dropped. C: Refrigerator compressors and microwave ovens can cause interference on a network. E: Because orders are up, the wing's proximity to the manufacturing shed could be because of electromagnetic interference from the machines on the production line.

   Incorrect answers: B: The janitor's actions are intermittent, and the network problems are consistent. D and F: These differences should provide more reliability, not less.

Chapter 9

Check Your Understanding

1. The two data link sublayers are as follows:

- **Logical Link Control (LLC):** Handles the communication between the upper layers and the lower layers, typically hardware.
- **MAC:** The Ethernet MAC sublayer has the following responsibilities:
  - Data encapsulation
  - Media access control
  - Addressing

2. A. Poor scalability
3. C. Frame Check Sequence. The FCS (4 bytes in length) field is used to detect errors in a frame.
4. C. An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
5. An Ethernet MAC address is used to transport the frame across the local media.
6. C. The Ethernet broadcast MAC address is FF-FF-FF-FF-FF-FF. Frames with this destination address are delivered to and processed by all the devices on that LAN segment.
7. B. The jam signal in CSMA/CD makes sure that all sending nodes see the collision.

8. The group of connected devices that can cause collisions to occur with each other is known as a collision domain. Collision domains occur at Layer 1 of the networking reference model.

9. C. Historic Ethernet and legacy Ethernet both use logical bus topology.

10. B. Is a separate collision domain

11. D. Learning. When a frame of data is received from a node, the switch reads the source MAC address and saves the address to the lookup table against the incoming interface. The switch now knows out which interface to forward frames with this address.

12. D. Learning. When a frame of data is received from a node, the switch reads the source MAC address and saves the address to the lookup table against the incoming interface. The switch now knows out which interface to forward frames with this address.

13. When a host has a packet to send to an IP address that does not have a map in the ARP cache.

14. C. Flooding. When the switch does not have a destination MAC address in its lookup table, it sends (floods) the frame out all interfaces except the one on which the frame arrived.

15. B. Timing can be more easily distorted with the shorter bit times.

Challenge Questions and Activities

1. (Can vary.) With the same frame format, different implementations of Ethernet (PHY) maintain compatibility. Changing the frame format would have resulted in different “Ethernets” that were not compatible.

2. (Can vary.) The primary reason is that the frames are not sent to every device. If a device receives a frame, it can be examined to obtain the sensitive information.

Chapter 10

Check Your Understanding

1. C. One of the primary responsibilities of a DCE device is to provide clocking to the routers for synchronization.

2. A. To have at least 100 hosts, your networks must go up by 128. So, you would have to subnet 178.5.0.0/16 to 178.5.0.0/25. This would make your first network 178.5.0.0, your second network 178.5.0.128, your third network 178.5.1.0, your fourth network 178.5.1.128, your fifth network 178.5.2.0, and so on.

3. D. If you increment your network by 32, you lose two (the network and broadcast address), so you must jump up to 64, which equals 128 + 64 = 192.

4. B. A 248 means that you are incrementing your network in steps of 8 (128 + 64 = 192 + 32 = 224 + 16 = 240 + 8 = 248). If you increment in steps of 8, your networks would be 154.65.128.0 to 154.65.136.0, the next network. That would mean 154.65.128.0 would be the network address, 154.65.128.1 to 154.65.128.254 would be the hosts, and 154.65.128.255 would be the broadcast address.

5. D. 100BASE-FX uses fiber cabling and supports full duplex up to a distance of 2000 meters.

6. True.

7. A straight-through UTP cable would be used to connect these devices:

   - Switch to router
   - PC to switch
   - PC to hub (if used)

8. A crossover UTP cable would be used to connect these devices:

   - Switch to switch
   - Switch to hub (if used)
   - Hub to hub (if used)
   - PC to PC
   - PC to router

9. The terms DCE and DTE are described as follows:

   - **Data communication equipment (DCE):** A device that supplies the clocking to another device. It is typically a device at the WAN access provider end of the link.
   - **Data terminal equipment (DTE):** A device that receives clocking from another device and adjusts accordingly. Typically this device is at the WAN customer or user end of the link.

   In a lab environment, generally connect two routers with a serial cable, providing a point-to-point WAN link. In this case, decide which router is going to be the one in control of the clocking. Cisco routers are DTE devices by default but can be configured to act as DCE devices.

10. The following criteria should be considered:
    - Cost
    - Cable/wireless
    - Speed
    - Ports
    - Expandability
    - Manageability
    - Features
11. End devices requiring IP addresses include
    - User computers
    - Servers
    - Other end devices such as printers, IP phones, and IP cameras

    Network devices requiring IP addresses include
    - Router LAN gateway interfaces
    - Router WAN (serial) interfaces
12. Reasons for subnetting a network include
    - Manage broadcast traffic
    - Similar network requirements
    - Security
13. The five factors to consider are as follows:
    - Cable length
    - Cost
    - Bandwidth
    - Ease of installation
    - Susceptibility to EMI/RFI

Challenge Questions and Activities

1. C, D, F. A 255.255.255.248 mask would mean that the networks would increment in steps of 8. In other words, the network addresses would be 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192 , 200, 208, 216, 224, 232, 240, and 248. Hence:

   A. would not be correct. 192.168.200.87 would be the broadcast address for the network 192.168.200.80.

   B. would not be correct. 194.10.10.104 would be a network address.

   C. 223.168.210.100 is correct, a host on the 223.168.210.96 network.

   D. 220.100.100.154 is correct, a host on the 220.100.100.152 network.

   E. 200.152.2.160 is not correct. It is a network address.

   F. 196.123.142.190 is correct, a host on the 196.123.142.184 network.

2. E. A /20 would yield 4096 possible IP addresses, minus 1 for the network address, minus 1 for the broadcast address, and minus 1 for the host address already used. That would provide you with 4093 IP addresses left for network devices.

3. A. Using the fact that a /27 would increment the networks by 32, you have the following networks, per Figure 10-27: 192.168.102.0, 192.168.102.32, 192.168.102.64, 192.168.102.96, 192.168.102.128, 192.168.102.160, 192.168.102.192, and 192.168.102.224. Option A is correct because the server address of 192.168.102.147 falls out of the 192.168.102.96 network.

4. E. The only option is to use fiber-optic cable. Thinnet and Thicknet would provide EMI protection but could not provide the bandwidth.

5. B, D. Initial configuration of a Cisco router must be accomplished through the console port, and that requires a rollover cable and terminal emulation software.

6. The four types of interfaces are as follows:

   - **Ethernet:** This interface is used for connection of the LAN device, which includes computers and switches. This interface can also be used to connect routers.

   - **Serial:** This interface is used for connection of the WAN devices to the CSU/DSU. Clock rate and addressing are assigned to these interfaces.

   - **Console:** This is the primary interface for gaining initial access to and configuration of a Cisco router or switch and is the primary means of troubleshooting. It is important to note that through physical access to the console interface router, an unauthorized person can interrupt or compromise network traffic. Physical security is extremely important.

   - **Auxiliary (AUX):** This interface is used for remote, out-of-band management of the router. Typically a modem is connected to the AUX interface for dialup access. From a security standpoint, having the ability to remotely dial in to a network device also requires vigilant management.

Chapter 11

Check Your Understanding

1. E. The **no shutdown** command, given at the interface prompt, will bring the interface up. The **enable** command moves you from operating at the user mode to the privileged mode. **S0 active** and **interface up** are not legal IOS commands.

2. D. The **enable secret** command allows you to input a password that will be used to get you from the user to the privilege mode. This password will be encrypted.

3. B. The **show interfaces** command will display statistics for all interfaces configured on a router. It is the only legal command listed.

4. C. The **show** command will provide you with numerous commands that can be used for viewing router status. The **?** will list those commands.

5. D. The administrator should issue the following commands, which are presented in the correct sequence, and the proper format:

   SanJose(config)#**line con 0**

   SanJose(config-line)#**login**

   SanJose(config-line)#**password CISCO**

6. A rollover cable connected to the serial port of a computer is used.

7. A, B, D. The console port is used strictly to access the configuration of the router; it cannot be used for data routing or for connecting one router to another.

8. C. Routers store routing tables that basically match network addresses to the best exit interface.

9. Setup mode allows you to configure a router by answering a series of questions posed to you.

Challenge Questions and Activities

1. B, C, D. Bits per second would have to be set to 9600 to be correct, and Flow control would have to be set to None to be correct.

2. The router stores the running-configuration file in RAM. The router stores the start-up configuration file, the file created when you save the running-configuration file, in NVRAM.

3. B. The IOS is stored in flash and then run and/or uncompressed in RAM. All other choices are stored either in RAM or NVRAM.