

Chapter 1 Review Questions:

Core Network Concepts

Test Your Understanding - Questions for Chapter 1

1. Distinguish between telecommunications and data networking.

Telecommunications is a broad concept that embraces voice and video communication as well as the transmission of **data** (words, numbers, still images, and so forth).

In **data networking**, at least one of the parties is a computer (later in the chapter).

Follow-up questions: classify telephony, television, World Wide Web access, and e-mail. (E-mail is considered data communications, indicating how this distinction is blurring.)
2. a) What is a network? b) What are the six main elements of a typical network?

a) A **network** is a system of hardware, software, and transmission components that collectively allow two application programs on two different stations connected to the network to communicate well.

b) The six major hardware, software, and transmission elements found in networks are messages, applications, stations, switches, access links, and trunk links.
3. What is a client/server architecture?

In a **client/server architecture**, client computers receive service from server computers.
4. a) In this book, what systems are considered to be PCs? b) What is a Wintel PC? c) Give examples of some mobile client stations. d) What is a NIC?

a) Wintel PCs and Macintoshes are both considered PCs. Note: LINUX PCs should have been included, but they are quite rare.

b) **Wintel** PCs run client versions of the Microsoft Windows operating system and use a standard Intel Pentium microprocessor or a compatible microprocessor from one of Intel's competitors.

c) Some examples of mobile client stations are notebook computers, cellular telephones (cell phones), personal digital assistants, and tablet PCs.

d) A **network interface card (NIC)** is a printed circuit board that allows a computer to communicate over a network.

5. a) What are the three types of servers? b) What is a NOS? c) What are the popular NOSs for PC servers? d) Distinguish between PC servers and workstation servers in terms of hardware and software. e) Distinguish between PC servers and workstation servers in terms of ability to handle large processing loads.

a) The three types of servers are PC servers, workstation servers, and mainframes.

b) A network operating system (NOS) is an operating system designed to run on a server.

c) Popular NOSs for PC servers include Windows, UNIX (including LINUX), and NetWare.

d) PC servers use mass-production Intel and Intel-compatible microprocessors, while workstation servers use fast and expensive custom-designed microprocessors.

PC servers run PC-oriented network operating systems, while workstation servers run UNIX (including LINUX).

e) Single UNIX workstation servers can handle much greater processing loads than can single PC servers.

6. a) What is scalability? b) Why is scalability important in networking?

a) **Scalability** is the ability to grow as demand grows.

b) If you have a solution that is not scalable, you may not be able to meet rising demand at all or may only be able to meet it by switching to a new system, which is very difficult and expensive.

7. What are the purposes of directory servers?

Directory servers store policies and important information about the firm's people and computers in a centralized location.

8. From the box Increasing Server Scalability. a) What are the three ways to increase server scalability once you have selected a basic platform (PC server, workstation server, or mainframe server)? b) Which of these increases reliability?

a) The three basic ways to increase server capacity within a platform family are multiprocessing single computers, clusters of computers, and load balancing.

Multiprocessing means having the server operate multiple microprocessors to share the work load.

Clustering means that a small number of servers can be linked together to act as a single large server.

In **load balancing**, a load balancer such as a router assigns tasks to servers in a server farm.

b) Clustering and load balancing increase reliability. Multiprocessing does not.

9. a) What are the two basic types of transmission links? b) Which connects a client to a switch? c) Which connects a switch to another switch?

a) The two basic types of transmission links are access links and trunk links.

b) Access links connect a station to a switch.

c) Trunk links connect a switch to another switch.

Note: In an internet, trunk links also connect switches and routers to one another.

10. a) What is a switching decision? b) What is packet switching? c) What is a packet? d) How does packet switching save money for data traffic? e) What are the three main parts of a message? f) The header and trailer are further subdivided into sections called what? g) Explain the importance of the address field. h) What is a message in a single network called?

a) In a **switching decision**, the switch accepts a message in one port, selects another port to send the message back out, and transmits the message out that port.

b) In packet switching, messages are sent through a switched network in a series of short messages called packets.

Many short messages flow through a network more easily than fewer long messages, much as sand flows more easily through an hour glass than do pebbles.

c) Packets are short messages sent through a packet-switched network.

d) Packet switching saves money in networks by allowing trunk lines to be multiplexed. Each conversation only has to pay for its share of the trunk line's capacity.

e) The three main parts of a message are the header, the data field, and the trailer.

f) The header and trailer are further subdivided into sections called fields.

g) Switches look at the destination address field to make switching decisions to move a message closer to its destination, just as post offices use destination addresses on envelopes to deliver letters.

h) A message in a single network is called a frame.

11. a) List and briefly describe the major service quality parameters listed in the text.
b) What is an SLA? c) What happens if SLA guarantees are not met?
- a) The following are the major service quality parameters listed in the text:
- Speed, measured in bits per second, describes the throughput of a network.
- Latency is a measure of delay (usually in milliseconds) caused by congestion.
- Availability is the percentage of time the network will accept and deliver messages.
- 24x7x365 is the ultimate goal.
- In the telephone network, the standard is 99.999% (the five nines)
- The **error rate** is the percentage of bits or messages that are damaged or lost during transmission.
- b) An SLA (service level agreement) is a set of written guarantees for such matters as speed, latency, availability, and error rates.
- c) If guaranteed goals are not met, the network provider will have to pay **performance penalties**.
12. a) Distinguish between LANs and WANs in terms of geographical scope. b) In terms of who provides service. c) How do LANs and WANs typically differ in price and speed?
- a) Geographical scope:
- A **local area network (LAN)** may consist of a few computers in a small office, all of the computers in a building, or all of the computers in a university campus or industrial park.
- Wide area networks (WANs)** transmit data *between* customer premises.
- b) In LANs, the organization itself provides service; for WANs, a carrier must provide service.
- This is because LANs operate on the customer premises, so the customer is responsible for everything.
- c) LANs generally have a lower price-per-bit-transmitted than WANs and also are faster.
- WAN speeds, by the way, are lower precisely because organizations cannot afford as much WAN traffic because of higher costs.
13. Distinguish between WANs and MANs.
- A **metropolitan area network (MAN)** is a carrier network covering a single urban area. It is a special type of WAN.

14. a) Distinguish between networks and internets. b) What device connects two or more networks in internets? c) Distinguish between internets and the Internet. d) What do we call the path a packet takes through an internet from the source host to the destination host?
- a) An **internet** is a group of networks linked together with routers in a way that allows an application program on any station *on any network* in the internet to be able to communicate with an application program on another station *on any other network*.
 - b) A router connects networks in internets.
 - c) An internet is any network of networks, while the Internet is the global Internet that most people use for e-mail, access to the World Wide Web, and other services.
 - d) The path a packet takes through an internet from the source host to the destination host is called its route.
15. The source host and the destination host are separated by seven routers. How many packets are sent along the route? How many frames?
- One packet is sent.
 - Eight frames are sent (one per network).
- Note: N-R-N-R-N, where Ns are networks and Rs are routers. There is always one more network than routers along a route.
16. a) Do you think the router changes the packet as it forwards it? b) The destination address in a packet in Figure 1-20 is the destination address of the what device?
- a) The router generally does not change packets (really, it makes a few minor changes) but merely forwards them closer to their destinations.
 - b) The destination address in a packet is the address of the destination host. In Figure 1-20, this is Host B.
17. a) Do you think switches change frames when they switch them? b) In the frame in Figure 1-20, the destination address is the address of what device?
- a) Switches generally do not change frames but merely forward frames closer to their destinations.
 - b) The address field is the address of a station or router to which the frame will be delivered within the specific network. In Figure 1-20, this is Router R1.
18. a) On the Internet, what is a host computer? b) When you connect to the Internet with a PC in your home or a laboratory, is your PC a host computer? c) What are the two types of host addresses on the Internet? d) Which is a host's official address? e) How long is an IP address? f) What happens if you know a target host's host name but not its IP address? g) Who uses dotted decimal notation to represent IP addresses: humans or computers? h) What do computers use?

- a) All stations attached to the Internet are called **hosts**.
 - b) Yes, your home or laboratory PC is a host.
 - c) The two types of addresses on the Internet are IP addresses and host names.
 - d) A host's official address is its IP address.
 - e) An IP address is 32 bits long.
 - f) If you know a target host's host name but not its IP address, your computer must call a DNS host and ask for the IP address based on the host name.
 - g) Only humans use dotted decimal notation to represent IP addresses. (Added since the book was printed.)
 - h) Computers use 32-bit binary numbers. (Added since the book was printed.)
19. a) What are the two types of carriers on the Internet? b) What is the technical function of an ISP? c) What is its economic function? d) Describe the Internet backbone.
- a) The two types of carriers on the Internet are Internet service providers (ISPs) and the backbone carriers that connect ISPs to one another.
Some companies are both ISPs and backbone carriers.
 - b) An ISP's technical function is to connect users to the main part of the Internet, called the Internet backbone.
 - c) The ISP's economic function is to fund the Internet.
20. a) What is the community of the Internet? b) What is an intranet? c) What is an extranet? d) What is the role of a firewall?
- a) The intended community of the Internet is the entire world.
 - b) In an **intranet**, a firm uses Internet technology, including transmission standards (discussed in Chapter 2) and Internet applications (e-mail, the World Wide Web, etc.) for *internal* communication. The firm is its own limited community. The intranet may have links to the outside world, usually via the Internet; but these are outside the intranet.
 - c) In an **extranet**, the community is a group of suppliers and purchasers who agree to communicate with one another under a certain set of rules.
 - d) **Firewalls** separate allowed and non-allowed traffic, permitting allowed traffic to pass and discarding non-allowed traffic.

Chapter 2 Review Questions: Standards

Test Your Understanding Questions

1. a) What are standards? b) What are the benefits of standards?
 - a) **Standards** are rules of operation that govern communication between two (or more) hardware or software processes on different machines.
 - b) Standards allow hardware and software processes from different vendors to **interoperate**. Interoperability creates competition, which lowers prices and speeds technological advancement. If our vendor fails, we can still buy compatible products from other vendors.

2. a) How long is an IP header if there are no options? b) What bit number in the header marks the start of the destination address field? (*Note: The first bit in binary counting is the zeroth bit.*)
 - a) 20 bytes (160 bits)
 - b) 128 (four times 32)

3. a) What are protocols? b) What are the five standards layers shown in Figure 2.3? c) Define the purpose of each layer.
 - a) **Protocols** are standards that govern communication between peer processes on different machines but at the same layer (horizontal communication).

Note that not all standards are protocols. A protocol is a particular type of standard. However, all protocols are standards.
 - b) Application, transport, internet, data link, and physical.
 - c) The following are the purposes of the individual layers:

The purpose of the **application layer** is to allow two application programs on different hosts to work together. *Note: HTTP should not be mentioned in the answer. It is not part of the application layer's purpose. HTTP is not always used at the application layer.*

The purpose of the **transport layer**, in turn, is to allow two host computers to talk to one another even if they have very different internal designs, such as a PC and a workstation server. *Note: it is NOT part of the definition to say that HTTP requires TCP at the transport layer.*

The purpose of the **internet layer** is to route packets from the source host to the destination host across one or more routers. *Note: IP should NOT be mentioned in the definition.*

The purpose of the **data link layer** is to govern the movement of messages from a source station to a destination station or router across a single network containing switches. *Note: Ethernet should NOT be mentioned in the definition.*

The purpose of the **physical layer** is to govern the transmission of bits one at a time over a wire, radio, or other connection between a station and a switch, between pairs of switches, or between a switch and a router. *Note: Ethernet should NOT be mentioned in the definition.*

4. In layered communication, is HTTP always used at the application layer? Explain.

HTTP is only the application standard in interactions with a webserver. E-mail, FTP, and other applications use different application layer standards.

5. a) What two devices do routers connect at the internet layer? b) What two devices do data links connect at the data link layer? c) What two devices do physical links connect at the physical layer?

a) Routers connect the source host to the destination host across an internet.

b) Switches connect a source station to a destination station across a single network. *Note: a router can be a station in a single network.*

c) Physical links connect two devices: a source station to a switch, a switch to another switch, or a switch to a router.

6. a) What are messages called at the internet layer? b) At the data link layer? c) At the physical layer? (Trick question.)

a) Messages at the internet layer are called packets.

b) Messages at the data link layer are called frames.

c) There are no messages at the physical layer: signals are sent bit-by-bit. In a sense, however, individual bits are the messages at the physical layer.

7. a) A station's MAC address is its address on its _____. b) A station's IP address is the station's address on its _____.

a) single network. Some will say on its NIC.

b) entire internet

8. a) What type of connecting device is a Layer 3 device? b) A Layer 2 device? c) A Layer 1 device?

- a) router
 - b) switch
 - c) repeater or hub
9. a) Switches convert between different _____ formats. b) Routers convert between different _____ formats.
- a) physical media
 - b) physical and data link layer (network)
10. a) All switches in a single network must follow the same _____ layer standard. b) All routers in an internet must follow the same _____ layer standard.
- a) data link layer
 - b) internet layer
11. a) What do the application, transport, internet, and data link layer processes on the source host do as soon as they create a message for their peer on another machine? b) What is encapsulation? c) When the Layer *N* process passes the message down to the Layer *N-1* process, which layer performs encapsulation?
- a) They immediately pass the message down to the next-lower layer. *Note: They do not do encapsulation; that is done at the next-lower layer.*
 - b) Encapsulation is the placing of a message in the data field of another message.
 - c) Layer *N-1* performs the encapsulation.
12. a) What layers are involved in switching? b) What does the switch look at to make its switching decision? c) What does the switch decide to do in making a switching decision? d) Do switches modify frames when they switch them? e) In a frame, the destination address is the destination of what device? f) Does the switch look at the contents of the internet layer packet?
- a) The physical and data link layers are involved in switching.
 - b) The switch looks at the destination address in the frame header. *This is the network address of the destination station on the network.*
 - c) The switch decides what port to use to send the frame out.
 - d) Switches normally do NOT modify frames. They just pass them out.
 - e) The destination address is the address of the destination station on the single network. *It is NOT the destination address of the switch receiving it.*
 - f) The switch does not look at the contents of the internet layer packet.
13. a) What layers are involved in routing? b) What does the router look at to make its routing decision? c) What does the router decide to do in making a routing decision? d) What layers do router ports implement? e) Do routers encapsulate first or decapsulate

first? f) Does the router change the IP packet as it forwards it? g) The destination address in a packet header is the destination address of what device?

- a) The physical, data link, and internet layers are involved in routing.
- b) The router looks at the internet layer address in the internet layer packet header.
- c) The router decides what port to use to send the packet out.
- d) Router ports implement the physical and data link layers.
- e) Routers first decapsulate when they receive a frame and then encapsulate when they send a frame back out.
- f) The router makes only small changes on the packet as it forwards it.
- g) The destination address in the packet header is the address of the destination host on the internet.

14. a) Does the data link process on the destination host encapsulate or decapsulate?
b) What does it do after that?

- a) The data link process on the destination host decapsulates.
- b) After it decapsulates the internet layer packet, the data link process passes the internet layer packet up to the internet layer process.

15. a) What is a reliable protocol? b) What is an unreliable protocol? c) Why are the data link and internet layers generally unreliable? d) Why is the transport layer generally made reliable?

- a) A reliable protocol is one that corrects errors.
- b) An unreliable protocol does not correct errors, although it may detect them and discard incorrect messages.
- c) The data link layer has to be implemented on multiple hops among switches, and the internet layer has to be implemented on multiple hops between routers. Doing error correction on each hop would be extremely expensive.
- d) The transport layer generally is made reliable because it can correct errors at the transport layer and at all lower layers as well, giving clean data to the application layer process. Only the two hosts are involved, so error correction only has to be done once, not at each switch or router hop.

16. If the transport layer sets up a connection between two computers, why do we need an application layer standard?

Computers are multitasking computers, so just getting the message to the computer is not enough; it must get to the right application program. Also, each application program has special needs. The application standard that works for e-mail would not work for FTP.

17. a) Is there more than one application layer standard? Explain. b) Are there many application layer standards?

a) Yes, there is more than one application layer standard because different applications need different application layer standards.

b) Yes, there are many application layer standards because there are many applications. There are far more application standards than any other type of standard because there are so many applications.

18. a) When an application layer process creates a message, what does it do immediately afterward? b) When a transport layer process receives a message from the application layer process, what does the transport layer process do?

a) It immediately passes the message down to the transport layer.

b) The transport layer encapsulates the application layer message in the data field of a transport layer message.

19. a) In terms of headers and trailers for all involved layers, describe the final frame coming from the source host if the frame is delivering a Simple Mail Transfer Protocol (SMTP) e-mail message. b) Repeat the question if the frame is delivering a TCP supervisory message to control the delivery of the e-mail message.

a) data link layer header
IP packet header
TCP segment header
SMTP message
Data link layer trailer

b) data link layer header
IP packet header
TCP segment header
Data link layer trailer

20. a) What is a standards architecture? b) What are the two dominant standards architectures?

a) **Standards architectures** are families of related standards that collectively allow an application program on one machine on an internet to communicate with another application program on another machine on the internet.

b) The two dominant standards architectures are TCP/IP and OSI.

21. a) What standards agencies are responsible for the OSI standards architecture? b) At what layers are OSI standards dominant? c) Describe the functions of the top three OSI layers.

a) The International Organization for Standardization (ISO) and the International Telecommunications Union-Telecommunications Standards Sector (ITU-T) are responsible for the OSI standards architectures.

b) OSI standards are dominant at the physical and data link layers.

c) The **session layer (OSI Layer 5)** initiates and maintains a connection between application programs on different computers.

The **presentation layer (OSI Layer 6)** is designed to handle data formatting differences between the two computers.

Application-specific communication is governed by the OSI **application layer (OSI Layer 7)**.

22. a) What standards agency manages TCP/IP? b) What are most of its documents called? c) Are all, some, or none of these documents standards? d) At what layers is TCP/IP dominant?

a) The Internet Engineering Task Force (IETF) is responsible for TCP/IP.

b) Most of its documents are called Requests for Comments (RFCs).

c) Some RFCs are standards, but not all are.

d) TCP/IP is dominant at the internet, transport, and application layers.

23. a) What layers of the hybrid TCP/IP-OSI standards architecture use OSI standards? b) TCP/IP standards?

a) Physical and data link layers use OSI standards.

b) Internet, transport, and application layers use TCP/IP standards.

24. a) When are you likely to encounter IPX/SPX standards? b) SNA standards? c) AppleTalk standards? d) NetBEUI standards?

a) You are likely to encounter IPX/SPX standards when the network uses Novell NetWare servers, especially older Novell NetWare servers.

b) You are likely to encounter SNA standards when your network carries mainframe data.

c) You are likely to encounter AppleTalk standards when your network carries Macintosh data.

d) You are likely to encounter NetBEUI standards if you have a very small LAN that runs Microsoft clients and servers. *Note: Even then, NetBEUI is not likely to be used because it is obsolete.*

Chapter 3 Review Questions: Physical Layer Propagation

Test Your Understanding Questions for Chapter 3

1. a) What is propagation? b) What are propagation effects? c) Why are propagation effects bad?
 - a) Propagation occurs when a signal travels through a medium.
 - b) Propagation effects are changes that take place to a signal as it travels through a medium.
 - c) Propagation effects are bad because if they are too extensive, the receiver may not be able to read the signal correctly.

2. a) Distinguish between analog and binary data. b) Which type of network usually carries analog data? c) Binary data?
 - a) **Analog data** rises and falls among an infinite number of levels (loudness levels, voltage levels, and so forth). **Binary data** consists of a string of ones and zeros.
 - b) The telephone network normally carries analog data.
 - c) Data networks normally carry binary data.

4. a) Distinguish between binary and digital transmission. b) Is binary transmission digital? c) What is good about having multiple states instead of just two? d) What is bad about having multiple states?
 - a) In digital transmission, there are a few states. In binary transmission, there are exactly two states.
 - b) Binary transmission is a special case of digital transmission.
 - c) Having multiple states allows the sender to transmit multiple bits in each clock cycle.
 - d) If there are multiple states, relatively small propagation effects may result in errors.

5. a) Distinguish between the bit rate and the baud rate. b) When are the two equal?
 - a) The bit rate is the number of information bits transmitted per second. The baud rate is the number of clock cycles per second.
 - b) The two are only equal for binary transmission.

6. a) In sending binary data over an analog transmission line, what kind of device does the conversion? b) Describe amplitude modulation.
- a) Modem
 - b) The amplitude (intensity) of the signal is kept at one level to send a zero, at another level to send a one.
9. a) In 4-pair UTP, how many wires are there in a cord? b) What surrounds each wire? c) How are the wires of each pair arranged? d) What is the outer covering called?
- a) 8 wires
 - b) insulation
 - c) The two wires in each pair are twisted around one another.
 - d) The outer covering is called the jacket.
10. Why is 4-pair UTP dominant in LANs for the access line between a NIC and the switch that serves the NIC?
- Four-pair UTP is easy to install and rugged enough to withstand normal office abuse.
11. a) Describe the attenuation problem and why it is important. b) Describe the noise problem and why it is important. c) As a signal propagates down a UTP cord, the noise level is constant. Will greater propagation distance result in fewer noise errors, the same number of noise errors, or more noise errors? Explain.
- a) Signals attenuate (get weaker) as they travel. If the signal becomes too weak, it will not be readable by the receiver.
 - b) Noise is random energy in a transmission medium. Noise energy adds to the signal energy. If there is a noise spike, the combined energy may not be readable by the receiver as the original signal.
 - c) Even if the noise level is constant, the signal will attenuate, so the number of noise errors will increase.
12. How are UTP attenuation and noise errors kept to an acceptable level? Explain.
- UTP attenuation and noise errors are kept to an acceptable level by limiting cord length to 100 meters.
13. a) Distinguish between electromagnetic interference (EMI), crosstalk interference, and terminal crosstalk interference. b) How is interference controlled? Explain. c) How is terminal crosstalk interference controlled? Explain.
- a) There is a hierarchy of concerns. EMI is any electromagnetic interference from an external source.

Crosstalk interference is a specific type of EMI that takes place between adjacent pairs of wires (not between the two wires in a pair but between pairs).

Terminal crosstalk interference is crosstalk interference at the end of a cord, where the wires have been untwisted to put into an RJ-45 connector. In UTP, terminal crosstalk interference usually is the dominant form of EMI.

- b) Interference in general is controlled by twisting the wires in a pair around one another. This creates immunity to general EMI and crosstalk interference
- c) Terminal crosstalk interference is controlled by not unwrapping the wires in a pair more than 1.25 cm (half an inch).

19. a) What are the three characteristics of radio signals? d) What is a hertz? e) When would you use frequency to describe propagation? f) When would you use wavelength?

- a) Wavelength, frequency, and amplitude
- d) Hertz is a measure of frequency; one hertz is one cycle per second.
- e) We normally use frequency to describe radio propagation.
- f) We normally use wavelength to describe light propagation.

20. Distinguish between the a) frequency spectrum, b) service bands, and c) channels. d) How can multiple signals be sent without interference?

- a) The frequency spectrum is the range of all possible frequencies, from 0 Hz to infinity.
- b) A service band is a range of the frequency spectrum in which a particular service is authorized. (AM radio, FM radio, television, etc.)
- c) A channel is a range of frequencies used to send a single signal (e.g., channels on television).
- d) Multiple signals can be sent without interference by sending them in different channels. *Note: there is always a little interference between adjacent channels.*