

## Chapter 4 Review Questions: A Small Ethernet PC Network

1. What are the elements of a small PC network?  
Client PCs, NICs, Ethernet hub or switch, UTP, servers  
For Internet connectivity, an access router and broadband modem connected to a broadband Internet access line.
2. a) Why do we discuss Ethernet in this chapter? b) Who standardizes Ethernet?  
a) Ethernet is the dominant LAN technology.  
b) 802.3 Working Group of the IEEE 802 LAN/MAN standards committee
3. Explain 10/100 Ethernet 100Base-TX technology.  
100Base-TX is designed to operate at 100 Mbps over UTP. Both the switch and the router, however, can autosense the speed of the other device. If the other device is a 10Base-T device, its partner will slow to 10 Mbps.
4. What does the “T” stand for in 10Base-T and 100Base-TX?  
Twisted pair or telephone
5. a) “Category 5e” is a measure of a cord’s \_\_\_\_\_. b) Who creates wiring quality standards? c) What wiring quality standard is now recommended for LANs? d) What wiring quality standards can be used with 10Base-T? e) With 100Base-TX? f) With gigabit Ethernet (1000Base-T)? g) Describe the emerging Category 6 standard and its potential usefulness. h) (Added question) What category is currently recommended for new LANs?  
a) quality  
b) TIA and EIA  
c) TIA/EIA-568  
d) Category 3 or higher  
e) Category 5 or higher  
f) Category 5 or higher  
g) Higher quality but not needed for Gigabit Ethernet. Really only needed for 155 Mbps ATM, which is not popular. However, Cat 6 may come to dominate retail products, making it the normal UTP wiring.

- h) Cat 5e (Category 5 enhanced)
6. a) What is the technical difference between regular wiring and plenum wiring?  
b) Where must you use plenum wiring? c) Why must you use it there?
- a) Regular UTP wiring gives off toxic fumes when burned. Plenum wiring gives off fewer toxic fumes.
- b) You must use plenum wiring in airways—air conditioning ducts, false floors, and false ceilings.
- c) Toxic fumes in airways are extremely dangerous.
7. a) What are the advantages of patch cords? b) Where would you use bulk UTP cabling?
- a) There is no need to cut, connectorize, and test them. You use them in the runs between the wall jack and the client PC.
- b) You would use bulk UTP for long cords that must be cut to specific distances.
8. a) Describe hub operation, including the pins on which the NIC and hub transmit.  
b) What is broadcasting called? c) How does a NIC know that an arriving frame is intended for it?
- a) The NIC transmits a bit on Pins 1 and 2 to the hub. The hub broadcasts the bit out all ports, on Pins 3 and 6.
- b) Broadcast is referred to as having a bus topology.
- c) The NIC assembles the frame, reads the destination address, and discards frames not intended for it.
- However, NICs can be put in promiscuous mode to read all traffic. Hub operation offers no security at all.*
9. a) What happens if two stations connected to a hub wish to transmit at the same time? b) What does it mean that hub speed is “shared?” c) What problem does sharing cause? d) What are the market prospects for hubs?
- a) If one station is transmitting the other must wait.
- b) The rated speed (usually 100 Mbps) is the total available to all devices.
- c) Sharing causes latency (delay).
- d) They are dying in the marketplace.
10. a) Describe basic switch operation. b) Is speed shared on a switch? c) What problem does this reduce?
- a) The source station sends a frame to a switch. The switch sends the frame out a single port—the one that leads to the destination station.
- b) Speed is not shared on a switch. Stations can always transmit.

*If two stations transmit to the same destination station at once, by the way, the switch will hold one frame in a buffer while delivering the other.*

- c) The ability of stations to always transmit reduces delay (latency).
11. a) What types of information do switching tables hold? b) How are switching tables used in switching decisions?
- a) Switching tables have two columns: Station (NIC) addresses and ports.
  - b) When a frame arrives, the switch looks up the destination address, reads the corresponding port, and sends the frame out that port.
12. a) What OSI layer did the 802 Committee split? b) What are the two layers into which it split the data link layer? c) Does the LLC layer have practical significance to network administrators? Explain.
- a) They split the data link layer.
  - b) They split it into the logical link control layer (upper) and the media access control layer (lower).
  - c) No, the LLC layer has no practical significance for network administrators. While it is capable of doing error correction, this capability is rarely used (or useful).
13. a) How many MAC layer standards does Ethernet have? b) What is its name?
- a) Only one
  - b) 802.3 Media Access Control Layer Standard
14. a) What is an octet?
- An octet is a collection of eight bits. This is the same as a byte.
16. a) How long are MAC addresses? b) When are MAC layer addresses set on NICs? c) Do computers work with them in hex representation? d) Do people tend to work with them in hex representation?.
- a) MAC addresses are 48 bits long.
  - b) MAC addresses are set at the factory.
  - c) No, computers do NOT work with hex representation.
  - d) Yes. Hex if for human use.
17. a) How long is the Ethernet length field? b) It tells the length of what?
- a) The Ethernet length field is 2 octets long.
  - b) It tells the length of the data field.
20. Describe the three main phases in CSMA/CD.

1) If there is no traffic, a station may transmit; if there is traffic, the station must wait until there is no traffic.

2) If two stations transmit at the same time, their signals will collide. The stations will stop and wait a random amount of time. The first one to finish may transmit—but only if there is no traffic.

3) If there are multiple collisions, the NICs will increase their random waits each time; if there are 16 failures, the sending NIC discards the frame.

21. a) If CSMA/CD is implemented, is it implemented on NICs, hubs, switches, or all three?

CSMA/CD is only implemented on NICs—NOT on hubs or switches.

23. To turn a typical PC you buy from the store into a client PC, what else may you have to purchase?

a) Only a NIC, and most PCs come with that now. (*This is still rare with notebooks.*)

24. a) Distinguish between manual configuration and autoconfiguration. b) Why is autoconfiguration good? c) Explain how the DHCP autoconfiguration protocol works. d) Why is DHCP so popular?

a) In manual configuration, you must type in all TCP/IP configuration values. In autoconfiguration, the PC gets TCP/IP configuration information from a DHCP server.

b) Autoconfiguration is easier (less work) for configuration, and it automatically is up-to-date.

c) A station sends a request to a DHCP server. The DHCP server sends back an IP address for the station and other autoconfiguration information as well.

*Actually, the client first broadcasts a request to DHCP configuration servers. Several may respond with offers of data and lengths of time these data can be used before reconfiguration is needed. The client picks the best offer and sends an acceptance to that DHCP server, which sends back the data.*

d) DHCP is popular because it is built into Microsoft Windows clients, which are by far the most common clients in corporations.

## Chapter 5 Review Questions

### Other LAN Technologies

1. In a single-switch LAN, the switch reads the address of an incoming frame, looks up an output port in the switching table, and sends the frame out that port. Do individual switches work differently in multi-switch LANs? Explain.

Switches in multi-switch LANs work the same as in single-switch LANs. When a frame arrives, the switch looks up the destination address in the switching table and then sends the frame out the indicated port.

2. a) How are switches in an Ethernet LAN organized? b) Therefore, how many possible paths can there be between two stations? c) In Figure 5-2, what is the single possible path between Client PC 1 and Server Y? d) Between Client PC 1 and Server X? e) What is the benefit of having a single possible path? f) Why is having a single possible path between any two stations dangerous?

a) They are arranged in a hierarchy.

b) Only one

c) Switch D – Switch B – Switch A – Switch C – Switch F

d) Switch D – Switch B – Switch E

e) If there is only a single possible path, there will only be one row in the switching table for each address. This allows a simple and fast lookup.

f) If there is a line break or switch failure, there is no way to get around it.

3. a) Distinguish between workgroup switches and core switches in terms of what devices they connect. b) How do they compare in terms of input port speed?

a) Workgroup switches connect stations to core switches. Core switches connect other core switches.

b) Core switches need faster port speeds than workgroup switches because each core switch port may have to carry the traffic of many stations, while most workgroup switch ports are for access links to individual stations.

4. a) What problem do VLANs address? b) How do they address it? c) Describe VLAN interoperability. d) Describe the VLAN tagging standard. e) When a server on a VLAN broadcasts, what stations receive its message? f) Do VLANs increase security?

a) VLANs address the problem of congestion and latency due to broadcasting.

b) Broadcasts are only allowed to go to stations within the sender's same VLAN.

c) VLAN interoperability is still poor, although the 802.1Q standard is improving the situation.

d) There are two fields added between the source address and length field. The first is a two-octet Tag Protocol ID with the value 81-00 hex to indicate that the frame is tagged (length fields always have values below 1500), followed by a Tag Control Information field that contains a 12-bit VLAN value to indicate the VLAN to which the transmission belongs. *There also is a 3-bit priority field to indicate the frame's priority. If frames with different priorities arrive at a switch at the same time, the switch sends the frame with higher priority out first.*

e) Only stations on its VLAN receive its message.

f) VLANs increase security only slightly because stations not on a VLAN do not receive messages sent among stations in the VLAN. However, it is so easy to circumvent this that even the U.S. Federal Aviation Administration would call this security inadequate.

5. a) What is the relationship between wavelength and distance of propagation in optical fiber? b) What is the drawback to using longer wavelengths?

a) The longer the wavelength, the longer the signal will travel without mode problems causing problems.

b) The electronics to send longer-frequency signals cost more.

6. a) What are the advantages of wireless LANs? b) What is the average cost to wire an RJ-45 LAN outlet? c) What are the disadvantages of wireless LANs?

a) Wireless LANs eliminate wiring cost and allow devices to be fully mobile.

b) The average cost to wire an RJ-45 outlet is about \$1,000. *\$500 for smaller LANs, but this is still high.*

7. a) Which 802 Working Group creates wireless LAN standards? b) What is the speed of most 802.11 installations today?

a) 802.11 Working Group

b) Most installations today use 802.11b, which run at 11 Mbps (actually about 3-4 Mbps.)

8. a) Describe the elements in a typical 802.11 LAN today. b) Why is a wired LAN still needed? c) What do access points do? d) What is handoff?

a) The station needs a wireless NIC.

There must be an access point in the area.

There normally is a wired LAN—see b)

- b) Servers normally are on the wired LAN, so the access point connects wireless stations to the access point.
- c) The access point receives frames from a wireless station and sends them out to a server on the wired LAN, doing frame conversion in the process (802.11 uses a different frame structure than 802.3). The access point reverses this process when the server responds.

*The access point also can connect two wireless stations if the server is wireless.*

Access points control wireless NIC transmission power.

- d) Handoff occurs when a station moves between access points—much as a cellular telephone user travels between cells. The new access point will take over service automatically. Unfortunately, this is now vendor-specific.

## Chapter 6 Review Questions:

# Telephony: Internal and External

1. a) Explain why it is important for data networking professionals to understand telephony. b) Explain why it is important for telephone specialists to understand data networking.
  - a) Networking and technology often are managed by the same group; LAN building wiring is derived from telephone technology, and WAN technology uses telephone service and is affected by telephone regulation.
  - b) Telephony is likely to be converged with data networking in the future.
2. a) What is the function of a PBX? b) What type of wiring is used in building telephone wiring?
  - a) A private branch exchange is an internal switching office for a corporate site. It handles all intra-site communication and links to the external public switched telephone network.
  - b) 4-pair UTP was created for building telephone wiring and is used almost universally in building telephone wiring.
3. Explain the following concepts in building wiring. a) Entrance facility. b) Termination equipment. c) Equipment room. d) Riser. e) Backbone wiring. f) Telecommunications closet. g) Cross-connect block. h) Horizontal cabling. i) Wall jack. j) In Figure 6.2, how many UTP pairs will run from the PBX through the vertical riser space if there are 25 telephones on each floor (and no telephones in the equipment room)?
  - a) The entrance facility is where lines from carriers come into the firm's building (or site).
  - b) Termination equipment sits between incoming lines from carriers and the company's internal network. The purpose of termination equipment is to prevent the company from sending incorrect signals into the telephone network.
  - c) The equipment room, usually in a basement, terminates connections to outside carriers, runs them through a PBX, and sends wires up through the floors.
  - d) A riser is a space between floors through which UTP cables can be run.
  - e) Backbone wiring is vertical wiring going from the telecommunications room to upper floors.

- f) The telecommunications closet on each floor is where pairs coming up through the vertical riser are terminated and sent up to the next floor or are used for horizontal distribution on the closet's floor.
- g) A cross-connect block terminates many UTP pairs coming up the vertical riser and connects them to cords running horizontally on the floor.
- h) Horizontal cabling is cabling on a floor. A 4-pair UTP connection runs from the wiring closet to the wall jack and then the telephone (or computer).
- i) A wall jack is the outlet for the internal telephone network. A 4-pair UTP cord runs from the telephone (or computer) to the RJ45 wall jack.
- j) There are three floors and 25 telephones per floor. Each telephone requires 4 pairs. Therefore, 300 UTP pairs must be run up through the vertical riser.

4. a) Compare how data cabling and telephone cabling are different for vertical runs. b) Compare how data cabling and telephone cabling are similar for horizontal runs. c) In Figure 6.3, how many 4-pair UTP cords will run from the core switch through the vertical riser space if there are 25 computers on each floor (and no computers in the equipment room), and if UTP is used for vertical communication? d) If optical fiber is used in place of UTP, how many optical fiber cords will run through the vertical riser?

a) For vertical runs, data cabling only runs a single UTP cord or a pair of optical fiber cords from the basement to the workgroup switch on each floor.

For vertical runs, telephone cabling must run four UTP pairs for each telephone on the floor.

b) They are the same for horizontal runs, running a 4-pair UTP cord to each wall jack.

c) 25 4-pair UTP cords (really, a bundle of 100 UTP pairs) would have to be run up to each floor.

d) One fiber pair is run from the basement to each floor.

5. a) What is a structured cabling plan, and why is it important? b) Why is documentation critical?

a) Cabling has many options. A structured cabling plan specifies what options a company will use. Without it, wiring will become chaotic.

b) Without documentation, you will lose track of which cable goes where.

6. a) What is a central office? b) How are switches organized in the telephone network? c) What are the classes of switches? d) Which class of switches is highest in the hierarchy?

a) A central office is a telephone building that contains a switch.

b) Switches are organized hierarchically in the telephone network.

c) Classes 1 through 5

d) Class 1 is at the top of the hierarchy. Subscribers connect to Class 5 end office switches.

7. a) What are the designations and speeds of the two fastest trunk lines in the North American Digital Hierarchy? b) Are they designed for point-to-point service? c) What transmission medium do 56 kbps and T1 trunk lines use? d) What are the designations and speeds of the two fastest trunk lines in the CEPT Multiplexing Hierarchy? e) What trunk line technology do carriers use for SONET and SDH? f) Are SONET and SDH designed for point-to-point service? g) Explain why your answer to the previous part of this question (f) is important.

a) T1 (1.544 Mbps) and T3 (44.7 Mbps)

b) Yes. Both are for point-to-point service.

c) 56 kbps and T1 lines normally use two pairs of data grade UTP wire.

d) E1 (2.048 Mbps) and E3 (34.4 Mbps)

e) Carriers use optical fiber for SONET and SDH.

f) SONET and SDH are designed for ring topologies rather than point-to-point topologies.

g) The use of a dual ring means that the ring can be wrapped if a link between two switches in the ring is broken, and transmission will be able to continue after a tiny delay. *Fixing a point-to-point connection, in contrast, may take hours or days. Broken trunk lines due to accidental dig-ups by construction back hoes is the most common cause of telephone service failure.*

8. a) What is a circuit? b) Why are circuits good? c) Why is circuit switching bad for data transmission?

a) A circuit is an end-to-end connection between two subscribers. Although it will pass through multiple switches and trunk lines, it will look like a direct connection to the subscribers.

b) Capacity is dedicated during a call, so that service cannot “slow down.”

c) Data transmission is bursty. If you have a circuit, you will only use it a small percentage of the time if you send data. Yet, you will pay for the capacity whether you use it or not. *For data transmission, multiplexing on trunk links using a packet switched network is much more efficient, saving money.*

9. a) What parts of the telephone system are largely digital today? b) What parts of the telephone system are largely analog today? c) What are the roles of the codec in the end office switch? d) Explain why the ADC generates 64 kbps of data for voice calls. e) Why do we need DACs? f) How do they work?

a) Switches and trunk lines are digital in the telephone system today. Even the access link to business customers may be digital today.

b) Only the access link is analog today, and that is mostly to residential subscribers.

- c) The codec converts from analog subscriber signals to digital signals for the switch (coding) and converts from digital switch signals to analog signals for the subscriber line (decoding).
- d) The ADC samples the signal 8,000 times per second, generating an 8-bit sample each time. This gives 64 kbps of data.
- e) We need DACs to convert digital switch signals to analog signals for transmission to the subscriber.
- f) The DAC takes each 8 bit sample's data and generates a corresponding level of 1/8000 of a second.

10. a) What is a cell? b) What is a cellsite? c) What is the function of the MTSO?  
d) Distinguish between handoffs and roaming.
- a) A city is divided into 20 to 200 areas called cells.
  - b) In each cell, there is a cellsite, which is a transceiver that communicates with the cellphones in its cell.
  - c) The MTSO coordinates the cellsites and connects the cellular network to the wired Public Switched Telephone Network.
  - d) Handoffs occur when a cellphone moves from one cell to another cell in the same cellular system. The customer is transferred from the current cell's cellsite to the new cell's cellsite.
- Roaming occurs when a subscriber leaves their cellular system and goes to a cellular system in another city.
11. a) Why does cellular telephony use cells? b) If I use Channel 3 in a cell, can I reuse the channel in an adjacent cell? Explain.
- a) Cells allow channels to be reused, allowing the system to serve more customers.
  - b) I cannot use Channel 3 in an adjacent cell because the signals will be too strong and will interfere. However, if I use a cell at least one cell away, there will be no interference.
12. a) Which generation of cellular technology is analog? b) What are the two service bands for 2G systems? c) How do they differ in bandwidth? d) How do they differ in cell size? e) How do 2G systems serve more customers than first-generation systems? (There are several parts to this answer.) f) What is SMS? g) What is wireless Web access? h) What is the international standard for wireless Web access? i) Why do we need 3G service? j) What speeds will 3G service bring? k) What is 2.5G service? l) Why is it attractive?
- a) 1G was analog.
  - b) 2G systems use both the 800/900 MHz band and the 1.8/1.9 GHz band.

- c) The 800/900 MHz band has 50 MHz of bandwidth. The 1.8/1.9 GHz band has 150 MHz of capacity.
- d) Compared to 1G systems, 2G systems have more bandwidth, use smaller cells, and compress the signal.
- e) Short message service allows cellphone users to type brief messages and send them to another user.
- f) Wireless Web access is a wireless MAN service for mobile devices.
- g) The international standard for wireless Web access is the wireless access protocol (WAP).
- h) We need 3G service for high-speed data transmission to move larger files.
- i) 3G will bring up to 2 MHz for motionless stations, 384 kbps for modestly moving devices.
- j) 2.5G service uses existing 2G spectrum to bring speeds of 20 kbs up to about 384 kbps.
- k) 2.5G systems will be an interim step to full 3G service. 2.5G will give relatively good speeds in the near future. *A few 2.5G systems have already appeared. Some are called 3G systems.*

## Chapter 7 Review Questions:

### Wide Area Networks

1. a) How are telephony and wide area networking related? b) What are the three main reasons to use a WAN? c) What are the four technologies for WANs? d) What is the main speed range for WAN communication? Why?
  - a) WAN often uses PSTN transmission services.  
*Also, WANs are affected by PSTN regulations we see in this chapter.*
  - b) Remote access for individuals  
Site-to-site transmission  
Internet access
  - c) Telephone modem  
Network of leased lines  
Public switched data network (PSDN)  
Virtual private network (VPN)
  - d) 56 kbps to a few megabits per second.
2. a) In telephone modem communication, does the home user use a modem?  
b) Does the ISP or a corporate site use a modem?
  - a) Yes. Duh.
  - b) May or may not. Under 33.6 kbps, ISP may use a modem. For higher download speeds, ISP must have a digital connection to the Internet.
4. a) How are leased lines like dial-up telephone circuits? b) How are they different in terms of operation? c) How are they different in terms of speed and cost?
  - a) Both provide end-to-end connections between customers.
  - b) Dial-up circuits only exist during a call. Leased line circuits are always on.
  - c) Leased lines are faster and more expensive.
5. a) What is the difference between trunk lines and trunk line-based leased lines?  
b) What is provisioning? c) If a trunk line-based leased line uses UTP, what type of UTP will it use? d) What are fractional T1 lines, and why are they desirable?

- a) A trunk line only runs between two switches within the telephone network. Trunk-line based leased lines extend trunk line speeds to end-to-end circuits between subscribers.
- b) Provisioning is a carrier's setting up capacity. *This can take a long time.*
- c) A trunk-line based leased line requires expensive data-grade UTP. *Usually two pairs—one for transmission in each direction.*
- d) Fractional T1 lines have speeds between 56 kbps and 1.544 Mbps, offering lower prices for companies that do not need full T1 service.

6. a) How do trunk line-based leased lines and DSL lines differ in terms of transmission media? b) Describe ADSL speeds and technology. c) Does ADSL disable your telephone line when you are using the Internet? d) Describe HDSL and HDSL2 in terms of speed. e) Describe SHDSL in terms of speed and distance. f) Can you always get a DSL to your premises? g) What is the biggest determining factor for whether you can? h) Which DSL services usually offer performance guarantees for speed?

- a) Trunk line-based leased lines use data grade copper—usually two pairs. DSL uses ordinary voice-grade wiring, usually a single pair. *Typically, they use the voice-grade pair already going to the home or small business.*
- b) ADSL offers high download speeds (256 kbps to over 1.5 Mbps) but limited upload speeds (typically 64 kbps to 256 kbps).
- c) ADSL does NOT disable your ordinary voice telephone service.
- d) HDSL offers half-T1 speeds on a single voice-grade wire pair. HDSL2 offers full T1 speeds on a single voice-grade wire pair.
- e) SHDSL offers variable symmetrical speed (384 kbps to 2.3 Mbps). It offers longer distances than HDSL and HDSL2 as well.
- f) No, DSL service depends on the quality of the wiring to your home or business and how far you are from the end office switch.
- g) The biggest determining factor is your distance from the end office switch.
- h) Symmetric speed DSL service is designed for business and offers QoS guarantees. ADSL is a consumer-oriented service and does not offer guarantees.

9. a) Describe how corporate WANs use meshes of leased lines to create their WANs. b) Describe PSDN technology. c) Describe how PSDNs ~~use~~ [still require (added)] leased lines. d) Do these two types of WANs use the same number of leased lines for a given number of sites? Explain. e) Do their leased lines have about the same average distance? Explain. f) How do PSDNs reduce labor costs?

- a) Companies lease lines between their sites in a mesh. They then add switching and manage the network.
- b) PSDN technology requires firms to have a single leased line to a point of presence (POP). From the POP, the PSDN handles all switching between sites.

- c) PSDNs require a single leased line from each site to the PSDN.
  - d) PSDNs require fewer leased lines—only one per site. Meshes of leased lines require many leased lines between sites.
  - e) Leased line networks require longer leased lines on average—all the way between sites. PSDNs only require leased lines from a site to the nearest POP.
  - f) PSDNs manage the WAN actively, freeing companies of the burden of managing their WANs (as is required in meshes of leased lines).
18. a) What is a VPN? b) Why are VPNs attractive? c) What problems do they face? d) How can latency be controlled for intranets?
- a) a virtual private network is the use of the Internet (sometimes, PSDNs) with added security.
  - b) VPNs should be cheaper than PSDNs (or meshes of leased lines).
  - c) VPNs raise the issues of security, latency, and availability.
  - d) Latency can be controlled in intranets by connecting all sites to a single ISP, thus avoiding the Internet backbone.
19. a) What is a remote access VPN? b) Why is it attractive?
- a) A remote access VPN allows a single user to connect to a corporate site.
  - b) Remote access VPNs are attractive because they save the cost of long-distance telephone calls and can offer faster-than-modem speeds.
20. a) What is PPTP? b) Where is it likely to be used? c) Can ISPs provide the PPTP access concentrator? d) Describe the components of a PPTP system that uses a RADIUS server. e) What is a tunnel? f) Why is PPTP attractive? (Give two reasons.) g) Describe PPTP's two security limitations. h) Why do remote access servers usually check with RADIUS servers before accepting a user connection?
- a) PPTP is the Point-to-Point Transport Protocol. It supports remote access securely.
  - b) It is likely to be used in remote access VPNs.
  - c) Yes, ISPs usually do provide the PPTP access concentrators.
  - d) The user dials into an ISP and connects to the PPTP access concentrator at the ISP's dial-in site. The access concentrator sets up a secure connection to the PPTP remote access server at the corporate site. The PPTP remote access server checks with the RADIUS server to authenticate the user when the user logs in.
  - e) A tunnel is a secure connection between two sites.
  - f) PPTP is attractive because it is built into all recent Windows clients.
  - g) PPTP offers no security between the user and the ISP's PPTP access concentrator.

PPTP does not offer message-by-message authentication, such as a digital signature.

h) RASs usually check with a RADIUS server for authentication so that authentication information can be maintained in a single location for uniformity of authentication across RASs.

21. Why are site-to-site VPNs likely to become the most important corporate use for VPNs?

There is a great deal more potential site-to-site transmission volume than remote access volume.

22. a) At what layer does IPsec operate? b) Describe IPsec tunnel mode. c) What is the main advantage of tunnel mode? d) What is the main limitation of tunnel mode?

a) IPsec operates at the internet layer.

b) In IPsec tunnel mode, protected information usually takes place between IPsec servers at two sites. The original packet is encapsulated (tunneled) within the data field of another packet.

c) Tunnel mode protects the whole original packet, hiding the source and destination IP address.

d) The main limitation is that IPsec tunnel mode does not protect packet transmission within the site LANs.

## Chapter 9 Review Questions

# Security

## Chapter 9a Review Questions

### **Not Hands-On: How Attackers Hack Servers**

Due Date: \_\_\_\_\_

Last name (family name): \_\_\_\_\_

First name (given name): \_\_\_\_\_

#### **Test Your Understanding Questions for Chapter 9**

1.
  - a) Distinguish between skilled hackers and amateurs using kiddie scripts.
  - b) Describe the three types of criminal attackers. c) What are information warfare and cyberterrorism? d) Why are amateur cyberterrorists dangerous? e) Why are attacks by internal employees especially dangerous?
    - a) Skilled hackers have deep knowledge and skills, while amateurs using kiddie scripts often use these automated attack tools with little skill or understanding.
    - b) The three types of criminal attackers are individual criminals, organized crime, and espionage spies.
    - c) Information war is the use of computers instead of bombs to destroy an enemy's economic infrastructure. Cyberterrorism is using computers rather than bombs and other forms of destruction to attack a target country.
    - d) Amateur cyberterrorists are dangerous because recent major attacks have shown how much damage an individual amateur attacker can do. A small group of attackers can do even more.
    - e) Attacks by employees are especially dangerous because these employees have knowledge of the network and access permissions.

3. a) What is hacking? b) Why are servers attractive to hackers? c) Why are clients attractive to hackers?
- a) Hacking a computer is logging into it illegally. (In U.S. Federal law, it is illegal to intentionally access a protected computer without authorization or in excess of authorization and then doing damage even if unintentional.)
  - b) Servers are attractive because of all the data they contain.
  - c) Clients are attractive because they usually are relatively easy to take over. *After that, they can be used in attacks on other computers.*
4. a) Distinguish between single-message, message stream, and distributed denial-of-service attacks. b) How do distributed denial-of-service attacks work?
- a) In single-message attacks, a single packet causes the target computer to crash.  
  
In message stream DoS attacks, a stream of messages overwhelms the target host or network.  
  
In distributed denial-of-service attacks, the victim is attacked from many zombie computers.
  - b) In distributed DoS attacks, the attacker takes over many PCs. Some become handlers, others zombies. The attacker directs the handlers to attack. The handlers, in turn, direct the zombies to attack.
5. a) Briefly describe the various types of malicious content attacks. b) Describe snakes.
- a) **Viruses** infect files on a single system.  
**Worms** propagate across systems by themselves.  
**Trojan horses** are programs that appear to be one thing, such as a game, but really execute unwanted instructions on the victim host.  
Pornography and e-mail that is sexually or racially harassing, and **spam** is unsolicited commercial e-mail.
  - b) Snakes are blended attacks that combine two or more single attacks.
6. What are scanning attacks?
- In scanning attacks, the attacker sends packets and studies the responses to learn about the victim network or host to determine how to attack it.
7. a) What do firewalls do? b) What is their goal in doing this?
- a) Firewalls scan each incoming message.

- b) Their goal is to detect attack packets and drop them before they can enter the intended victim network.
8. a) What headers and messages do packet filter firewalls examine? b) What are ACLs? c) Why are access control lists difficult to configure?
- a) Packet filter firewalls examine IP headers, TCP headers, UDP headers, and ICMP messages.
  - b) Access control lists are rules for packets to permit or drop.
  - c) ACLs are difficult to configure because they are complex and executed in order, so if there is an ordering error, a packet may be permitted to pass before the firewall gets to a rule requiring it to be dropped.
9. a) What part of a packet do application firewalls examine? b) What do they look for? c) Must there be a separate application proxy program for each application being examined?
- a) Application firewalls examine the application message within a packet.
  - b) They look for illegal content. *They also ensure that an application is not using a well-known port to hide itself. If the application does not match the expected protocol behavior of the application program that should use that port, the packet is dropped.*
  - c) Yes, there must be a separate application proxy for each application being examined because different application programs have different characteristics to examine.