Chapter 4: Communication and Network Security Domain 4 Practice Questions

Questions from the following topics are included in this domain:

- Assess secure network design principles.
- Implement secure network design principles.
- Secure network components using network access control devices.
- Implement secure design communication channels.
- Understand data communications and virtualized networks.

Understanding security around network and communications design principles is critical to passing the CISSP exam, and you need to score well because there is a high 13% weighting on this topic.

Practice questions for domain 4 include understanding the OSI layers, the TCP/IP model, IPsec, the details of IPv4, and the basics of IPv6. The successful CISSP will know how to design, secure, and manage wired and wireless networks.

After studying these practice questions, you will be prepared to pass the communication and network security section of the exam, including the important scenarios on networking protocols, wireless networks, and content distribution networks.

Questions

1. James, a network engineer, considers using SCP for copying files from one computer to another. Which connection-oriented protocol will be used?

   A. PAP

   B. TCP

   C. UDP

   D. ICMP

2. Daria, a network engineer, seeks to set up a network that uses CSMA/CA. Which of the following should she select?

   A. Wi-Fi

B. FDDI

C. Ethernet

D. Token Ring

3. Dennis, a systems engineer, is upgrading 10 fax machines. What process should he use to dispose of the old fax machines?

   A. Print the last fax, and then dump in a dumpster.

   B. Use secure destruction methods.

   C. Clear the memory buffer and then discard.

   D. Simply dump in a dumpster.

4. Melanie, a systems administrator, needs a secure, private connection from her home to the office. Which technology makes this possible for her?

   A. IPsec

   B. Encryption

   C. Tunneling

   D. VPN

5. Emil is a network administrator setting up systems so that when users use FQDN, they are converted to IP addresses. Which technology is he configuring? (Choose two.)

   A. HTTPD

   B. NAMED

   C. DHCPD

   D. BIND

6. Danka, a network engineer, desires to add routers that make routing decisions based on hop count only. Which protocol should she select?

   A. EIGRP

   B. RIP

C. OSPF

D. IGRP

7. Camila is a network engineer in charge of the placement of detection systems for her organization. What type of device does she install for this functionality?

   A. Firewall

   B. IDS

   C. IPS

   D. HIPS

8. Sugita is a network engineer installing Network Intrusion Prevention Systems (NIPS) in his organization. What are the two methods he should employ to detect incidents and attacks? (Choose two.)

   A. Host

   B. Network

   C. Heuristic

   D. Pattern matching

9. Uchiyama is a network engineer tasked with explaining to management the differences between fraggle and smurf attacks. Which of the following is his *BEST* explanation?

   A. A fraggle attack is the same as a smurf attack but sends UDP packets instead of ICMP packets.

   B. A fraggle attack is the same as a smurf attack but sends ICMP packets instead of UDP packets.

   C. A fraggle attack is the same as a smurf attack but sends TCP packets instead of UDP packets.

   D. A fraggle attack is the same as a smurf attack but sends half-open packets instead of ICMP packets.

10. Darcey, a network administrator, needs to set up a web server that allows customer access. To do this, the device sits outside of the corporate firewall. In which area should she deploy this system?

A. Intranet

B. DMZ

C. Internet

D. Honeypot

11. IPv4 allows for about 4.3 billion IP addresses to be used on computers, tablets, smartphones, cameras, thermometers, and so on. Since the world ran out of IP addresses, IPv6 is one solution that extends the address space to more than 300 trillion trillion trillion IP addresses. What other systems increase IP address utilization? (Choose two.)

    A. DAT

    B. FAT

    C. NAT

    D. PAT

12. Kirlyam is a security administrator seeking the best way to defend her organization's network against sniffing. What is the *BEST* way for her to accomplish this?

    A. Enable DHCP.

    B. Encryption.

    C. Monitor for rogue access points.

    D. Heuristic firewall.

13. Aya is a network engineer looking to implement a security protocol that operates on the OSI application layer. Which of the following does she select?

    A. S/MIME

    B. RIP

    C. SSL

    D. TLS

14. Which of the following is an attack on web applications that injects client-side scripts into a web page?

A. XSRF

B. XSS

C. SQL injection

D. Input validation

15. Yamir, a network administrator, is asked to install a router to separate two networks within his LAN where there are no web or email services, instead of a firewall. After asking "Why not a firewall?", how does his network manager respond?

    A. Firewalls are less expensive.

    B. Routers are less expensive.

    C. Routers are stateful by default.

    D. Routers are stateless by default.

16. Which VPN protocol operates at layer 2 of the OSI model using 256-bit encryption?

    A. PPTP

    B. L2TP

    C. PPP

    D. IPsec

17. Chelsea is a security engineer completing setups for a single-sign-on system. Which system should she set up for the *MOST* secure authentication?

    A. EAP

    B. PAP

    C. MD5

    D. AES

18. A full-mesh network of four nodes requires how many connections?

    A. 7

    B. 6

C. 5

D. 4

19. Evelin is a network engineer tasked with architecting the network connection from headquarters to a field office 50 miles away. Which solution should she choose for *BEST* security and performance?

    A. 802.11n

    B. CAT5 cable

    C. Coaxial cable

    D. Fiber optic media

20. Brett is a network manager architecting a wired network through *KloutCo*. Part of the cabling will run above drop ceilings and through raised floors. Which of the following is his *BEST* recommendation?

    A. Use standard-grade cables because it is the least expensive.

    B. Use plenum-grade cables because in the case of a fire, standard-grade cables emit deadly gas.

    C. Use standard-grade cables because they are fireproof.

    D. Use plenum-grade cables because of their encryption features.

21. Daya, a network engineer, desires to configure a network using a star-type topology. Which of the following should she select?

    A. Partial mesh

    B. Wi-Fi

    C. Token ring

    D. Bus

22. Which of the following *BEST* describes the Media Access Control (MAC) address burned into a Network Interface Card (NIC)?

    A. A MAC address is 24 bits, and the whole thing is a manufacturer code.

    B. A MAC address is 24 bits, and the whole thing defines a unique address.

C. A MAC address is 48 bits, and 24 bits define the manufacturer.

D. A MAC address is 96 bits, and 48 bits define the manufacturer.

23. Cassia is an ethical hacker who cannot penetrate the network due to an advanced firewall. Which of the following should be her next step?

    A. Conclude the test and inform the client that their security levels will stop all attacks.

    B. Conduct reconnaissance.

    C. Attempt war dialing.

    D. Collect data using OSINT.

24. What is the primary purpose of an attacker launching an ARP poisoning attack?

    A. As a man-in-the-middle exploit

    B. To change the network's ARP table

    C. To modify IP addresses

    D. To decrease the acceptable resource pool

25. Jason, an ethical hacker, is working with *Jefferson Bank* to perform a penetration test. Which of the following is the *MOST* important step for him to complete?

    A. Reconnaissance.

    B. Confirm management buy-in by having them sign the working agreement.

    C. Network mapping and scanning for open ports and other vulnerabilities.

    D. Running the exploit.

26. Wireless access points and wireless systems use which technology?

    A. CSMA/CD

    B. Polling controls

    C. Token passing

    D. CSMA/CA

27. Which of these is *NOT* an attribute of a packet filter firewall?

    A. Makes use of access control lists

    B. Runs at the application layer

    C. Is a first-generation firewall type

    D. Inspects the source and destination addresses

28. TACACS and TACACS+ systems have which of the following two features? (Choose two.)

    A. Allows password changes

    B. Communicates via UDP protocols

    C. Encrypts passwords but not data

    D. Two-factor authentication

29. Which of the following *BEST* describes UTP cables?

    A. UTP cables have two conductors in concentric circles.

    B. UTP cables have two insulated twisted wires.

    C. UTP cables transfer data using laser signals.

    D. UTP cables have a range of 1 km before data signal loss.

30. Alexei is a marketing representative for *GL Food Bars* and maintains a mailing list for 5,000 customers. His ISP alerts him that his email server is sending spam to millions of users at 100 messages per minute. What is *MOST LIKELY* the problem?

    A. The most recent update to the email server was buggy.

    B. Millions of new clients have signed up for GL Food Bars information

    C. Hackers have compromised his email list.

    D. He has an open relay SMTP server.

31. Loren runs the networking department and desires to architect a system for her website customers that will simplify scalability, improve security, and ease implementation on

various devices, such as smartphones, smartwatches, and laptops. Which model should she select?

A. Demilitarized zone

B. N-tier architecture

C. Split DNS

D. Split tunneling

32. Benvele is a hacker launching attacks on smartphones to gain access and download photos and contacts. What type of attack is this?

A. Bluesnarfing

B. Bluejacking

C. Bluebugging

D. BlueBorne

33. Kyle is a secretary working fast to get work done for his boss. During a short break, he visits social media and clicks a link for cheap Ray-Ban glasses. Unbeknownst to Kyle, a hacker has downloaded his browser's cookies. What is the name of this attack?

A. XSRF

B. XSS

C. Cookie stealing

D. Cookie monster

34. Fernando is a salesperson visiting one of his corporate field locations. He has the Wi-Fi password but still cannot access the internet because his browser requests another username and password. What is *MOST LIKELY* to be the trouble?

A. The RADIUS server is not granting him a ticket.

B. The SAML system has an incorrect password.

C. Improper user ID for extensible authentication protocol.

D. Port authentication is required through 802.1x.

35. Two popular networking models include OSI and TCP/IP. The TCP/IP application layer represents which layer(s) of the OSI model?

    A. Transport, session, presentation, application

    B. Session, presentation, application

    C. Presentation, application

    D. Application

36. Graphical imagery, whether it is JPEG, TIFF, or GIF, is generally processed in which layer of the OSI model?

    A. Application

    B. Presentation

    C. Session

    D. Transport

37. Mikoopst is a hacker seeking vulnerabilities to attack a bank and steal money electronically. Which network device is likely to be the weakest vulnerability?

    A. The bank website

    B. The firewall

    C. Fish tank thermometer

    D. The internal corporate website

38. Which protocol uses sequence and acknowledgment numbers to keep track of communications?

    A. ICMP

    B. UDP

    C. TCP

    D. IP

39. Sandor is a hacker attacking a user's online banking experience. While the user is logged in to their banking account, the user clicks an enticing email for free check-printing from

their bank and allows the attacker to transfer money from the user's bank account. Which of the following *BEST* describes this attack?

A. TCP hijacking

B. XSRF

C. XSS

D. SQL injection

40. Which of the following is an example of protocols that would operate at the session layer of the OSI model?

A. RPC and FTP

B. PAP and PPTP

C. TCP and UDP

D. ICMP and RIP

41. Aleksandra is an ethical hacker manipulating TTL values to determine where firewalls are located. What technique is she using?

A. Ping-of-death

B. TTL trace

C. Tracerouting

D. Firewalking

42. The networking system designed to guarantee good performance of data flow and prioritize applications is known as what?

A. Prioritization

B. QoS

C. Service quality

D. Guaranflo

43. Jorge is starting a new CBD business and desires to set up his online shopping cart. He wants users to trust his store, so he registers a digital certificate with which role for the PKI?

    A. RA

    B. CA

    C. CRL

    D. Root

44. What is the primary difference between baseband and broadband technologies?

    A. Baseband is for cable TV only.

    B. Baseband transmits over a single channel, and broadband over multiple channels simultaneously.

    C. Broadband is for cable TV only.

    D. Broadband transmits over a single channel, and baseband over multiple channels simultaneously.

45. Anfisa, a network engineer is asked to inspect a network and determine whether it should be upgraded to fiber optic. Building-to-building connections are connected using coaxial cables, and privacy information is showing up on PASTEBIN. What is her recommendation for *BEST* security?

    A. Save money and make no changes because fiber optic cable is expensive.

    B. Save money and enable encryption for business-to-business communications.

    C. Upgrade the network to fiber because it is less expensive than STP.

    D. Upgrade the network to fiber because EMI transmissions are being intercepted.

46. Philyuk is a sales manager who is ready to get to work. He opens his laptop, connects to the Wi-Fi, but cannot access the internet. He notices that he has an IP address of **169.254.3.4** but still cannot access his online bank. What is *MOST LIKELY* to be the problem?

    A. The internet is down.

    B. The DHCP server is down.

C. The bank's web server is down.

D. His network card is disabled.

47. Azan is part of the network security team and they are setting up a Wi-Fi system that allows any member of the company to connect to the network when at the office. Which feature should he recommend to help secure access to the network?

A. DHCP snooping

B. Flood guards

C. Integrity checking

D. Encryption

48. Marcgerm is an overseas hacker conducting reconnaissance on the victim's network at *EB Inc*. What safeguards can the security team put in place to mitigate the attack?

A. Install an NIDS to block network threats.

B. Close ports 161 and 162 on the firewall and enable SNMPv3.

C. Upgrade the network from SNMPv1 to SNMPv2.

D. Attacks using SNMP are impossible to mitigate.

49. Nicole, a systems administrator, is seeking methods to defend her public DNS server from hackers. Which of these is her *BEST* solution?

A. Enable encryption.

B. Deny access to everyone except staff.

C. Install an HIDS.

D. Enable DNSSEC.

50. Matt is a salesperson for *Wilco* and plans to use the Wi-Fi offered at his local restaurant. He enters the Wi-Fi password but cannot access the internet like others there. The computer works fine at home on the VPN and at work. What is *MOST LIKELY* to be the problem?

A. He cannot access the DHCP server in the restaurant.

B. He has a static IP address set.

C. The DHCP server is down within the restaurant.

D. A hacker is altering the restaurant's network.

51. Luis is a systems administrator at *East School*, and the board is requesting a network that allows students to reach Google but disallows access to X-rated websites. Which system is *BEST* for him to install?

    A. Switch

    B. Proxy

    C. Repeater

    D. Router

52. Which of the following is a difference between an application-level firewall over a circuit-level firewall?

    A. Circuit-level firewalls are, in general, slower than application-level firewalls.

    B. Application-level firewalls do not require a proxy for each protocol monitored.

    C. An application-level firewall can perform deep packet inspection.

    D. A circuit-level firewall performs deep packet inspection.

53. What are the port numbers for these services, respectively?

    HTTP, FTP, SSH, SMTP, IMAP

    A. **443**, **21**, **23**, **25**, **123**

    B. **80**, **21**, **23**, **53**, **143**

    C. **80**, **21**, **22**, **25**, **143**

    D. **443**, **20**, **22**, **25**, **110**

54. Molly is a network engineer tasked with reducing interference on VoIP phones within the network. Which of the following is her *BEST* solution?

    A. Place all SIP- and RTP-related traffic into a separate VLAN.

    B. Place VoIP phones onto their own switch within the subnet.

C. Reduce the thresholds on the NIDS devices.

D. Develop corporate policies to limit phone use.

55. Alla, a network engineer, needs to extend a network so that computers 100 meters away from each other are on the same subnet. Which technology should she use to extend the network?

    A. Router

    B. Bridge

    C. Gateway

    D. Firewall

56. RIP is a distance-vector routing protocol. Distance-vector routing protocols make routing decisions based on what?

    A. Physical distance measured in centimeters and kilometers if preferred

    B. A combination of physical distance and number of hops

    C. Number of hops, network load, and packet size

    D. Minimum number of hops to reach the destination

57. Narkyia is an email administrator and her email server is being used to send forged emails. What technology can she install to mitigate this issue?

    A. SSL

    B. SPF

    C. SASL

    D. SMTP

58. Difata is new to hacking and has discovered a new attack. The instructions state that to best breach the victim server, you should launch the attack on IP address **127.0.0.1**. What type of individual is Difata?

    A. Script kiddie

    B. Skilled hacker

C. Ethical hacker

D. White hat hacker

59. Olulowo is a network engineer asked to install an internal DNS server for staff and a separate DNS server on the internet for the public. He decides to install which type of setup?

A. Split-network

B. Split-DNS

C. Split-VPN

D. Split-IP

60. Alice is a network engineer being consulted as to why network transmissions have slowly degraded over time. The small company has grown and installed microwave ovens in the break rooms, and the 100 new staff are using cell phones. What is her recommendation?

A. Create new policies not allowing the use of cell phones at work, and remove the microwave ovens.

B. After researching the environment, there is really nothing more that can be done.

C. Upgrade the STP cabling to UTP cabling.

D. Upgrade the UTP cabling to STP cabling.

61. Technologies such as Fiber Channel over Ethernet, Multiprotocol Label Switching, VoIP, and Internet Small Computer System Interface are examples of which protocol?

A. Fiber optics

B. IP convergence

C. Ethernet

D. Storage

62. Translating a set of public addresses to private addresses is accomplished with what method?

A. NAT

B. TCP

C. RFC

D. Teredo

63. Mattrich uses a VPN to work from his Apple computer. While connected, he clicks a link from his personal email account. Days later, corporate offices are down because of a massive ransomware attack. What *MOST LIKELY* occurred?

    A. Mattrich infected the company because he read his personal email.

    B. Mattrich infected the company because he was using VPN split tunneling.

    C. Mattrich infected the company because he disabled VPN encryption.

    D. Mattrich infected the company because they mostly use Microsoft computers.

64. Josh, a networking intern, is connecting two computers in a LAN. System A has IP address **192.168.4.7/24**, and system B has IP address **192.168.5.8/24**. He tests the connections using ping but gets the error message **host unreachable**. They are both properly plugged in to the switch. What is *MOST LIKELY* the problem?

    A. One of the cables is broken.

    B. The systems are improperly connected.

    C. Josh needs to use a hub instead of a switch.

    D. The systems are on separate subnets.

65. Which ports are considered the *MOST* well-known ports?

    A. 1-1024

    B. 0-1023

    C. 0-1024

    D. 1-1023

66. In the OSI model, which layer converts voltages to bits?

    A. Bitwise

    B. Physical

    C. V2Bit

D. Data link

67. Carolina is a network engineer and notices that network traffic has degraded to 50% of normal. After investigating, she discovers the problem. What did she determine?

    A. A new employee was streaming online music.

    B. The firewall was blocking the ports to access the web server.

    C. The manufacturer of the routers reported several zero-days that affected performance.

    D. Degradation only occurs in the evening when the users shut down their computers.

68. Noon, a network engineer, has been tasked with setting up a Wi-Fi network by upgrading the firmware of older-generation WAPs currently using WEP security. She is asked to improve the security without replacing the WAPs. Which level of security should she choose?

    A. Open authentication

    B. WEP

    C. WPA

    D. WPA2

69. This technology logically groups networked computers by function or department and enhances security by segregating data traffic, for example, by separating VoIP traffic. What is this technology called?

    A. VLAN

    B. VPN

    C. DNS

    D. DMZ

70. The TCP and UDP protocols are common in that they transfer data. What is the key difference between the two protocols?

    A. TCP is unreliable and transmits data faster than UDP.

    B. UDP is connectionless and has greater potential for data loss.

    C. UDP utilizes a three-way handshake.

D. TCP is great for digital video and audio applications.

71. VPNs have which of these characteristics? (Choose two.)

    A. VPN connections occur through software applications only.

    B. VPN connections can occur through hardware or software utilities.

    C. VPN connections must utilize IPsec.

    D. VPN implementations can be accomplished through certificate or key exchange.

72. Peter is a security analyst reviewing network logs and notices that from 10 PM-4 AM, the server reports attempted connections on ports **0**, **1**, **2**, **3**…, and **1023** from an unknown system on the internet. What type of attack is occurring?

    A. NMAP

    B. Port scanning

    C. HPING

    D. DDOS

73. Serena is a hacker, exfiltrating corporate files to her partner, Janine. What is the *BEST* way for Serena to launch the upload without getting caught?

    A. Janine builds an SSH server so that Serena can launch a covert channel and tunnel HTTP over SSH.

    B. Janine builds an SSH server so that Serena can launch a covert channel using SSH.

    C. Janine builds an FTP server so that Serena can launch a covert channel using FTP.

    D. Janine builds a Telnet server so that Serena can launch a covert channel using Telnet.

74. Simone-Jeannelle is a chemical engineer transferring work-from-home data to her office. As she transfers files from her house, she notices the transfer is taking much longer than expected. The network administrator states the network is functioning normally. What is the *MOST LIKELY* issue?

    A. She needs to upgrade her home-based SDSL modem to ADSL.

    B. Her home-based ADSL modem downloads faster than it uploads.

    C. The office firewall is doing deep packet inspection.

D. The office server is under a DOS attack.

75. Which of these are characteristics of a bridged network? (Choose two.)

    A. Layer 3 network device

    B. Connects two disparate networks

    C. Layer 2 network device

    D. Extends the current network

76. Bryce is a network engineer reviewing an RFP that states they require systems that work with CSMA/CD technologies. Which solution should he suggest?

    A. Wireless access points throughout the environment

    B. Ethernet connections because of the cabling

    C. Fiber optics because of its performance

    D. DVD/CD technology because it will work with CDs

77. Lai is a security engineer working with the networking department. During an audit, she notices the use of several old hubs in secure, networked environments. What is *MOST LIKELY* to be her recommendation?

    A. Replace the hubs with switches.

    B. Update the firmware on the hubs.

    C. Upgrade the hubs to the latest hub technology.

    D. Divide hubs with eight connections to make two hubs with four connections each.

78. Barry is a network engineer seeking to directly network two nearby buildings. Which option should he choose since the empty land between the two buildings is owned by his competitor?

    A. Connect the buildings via fiber channels.

    B. Install a Yagi antenna.

    C. Connect the buildings using CAT5 ethernet.

    D. Install building-to-building Bluetooth.

79. Avril is a systems administrator setting up email for her users. They are able to send email but not receive it. What is the *MOST LIKELY* problem?

    A. No email client is installed.

    B. No email server is installed.

    C. Port 25 needs to be opened on the firewall.

    D. Port 110 needs to be opened in the firewall.

80. Which protocols operate at the application, presentation, network, and data link layers, respectively?

    A. Pretty Good Privacy, routing information protocol, address resolution protocol, IPsec

    B. Routing information protocol, Pretty Good Privacy, IPsec, address resolution protocol

    C. Address resolution protocol, IPsec, Pretty Good Privacy, routing information protocol

    D. IPsec, Pretty Good Privacy, routing information protocol, address resolution protocol

81. Huisha is a security engineer deploying several honeypots. Her manager suggests that once a hacker is identified, the system should automatically attack the hacker's system and wipe the hacker's hard drive. Why does she tell the manager this is not recommended?

    A. It is technically impossible to launch a counter-attack.

    B. Hackback is against the law.

    C. There are not enough staff to conduct the remote hard-drive wipes.

    D. Hackback is too difficult to automate.

82. Of the following options, which provides the least protection to data in motion?

    A. WEP

    B. WPA

    C. L2TP

    D. PPTP

83. Which of these is a type of prevention system that performs IOC pattern matching, such as comparing instruction sequences of known malware or correlating known file hashes?

    A. Heuristic-based

    B. Network-based

    C. Signature-based

    D. IDS

84. What is another term for a pharming attack where victims get diverted to an attacker's fake website?

    A. DNS poisoning

    B. Flooding

    C. IP forwarding

    D. Phishing

85. Which setting does traceroute manipulate in the TCP/IP model?

    A. UDP

    B. TTL

    C. Data link

    D. Frame header

86. Hackers look for soft, vulnerable targets to attack, as they make it easier to upload exploits. Security engineers harden these systems by disabling which features? (Choose two.)

    A. FTP

    B. SSH

    C. HTTPS

    D. Telnet

87. Justin is a senior security officer asked for his opinion on installing wireless access points in a secure area. What does he recommend as security levels for the implementation?

A. WPA

B. WPA2

C. WEP

D. Open system

88. Of the following, which two are *NOT* VPN protocols? (Choose two)

A. RADIUS

B. Kerberos

C. L2TP

D. PPTP

89. Aziza is a network administrator setting up a private network with non-routable IP addresses. Which network block should she use?

A. **169.254.0.0/16**

B. **192.168.0.0/8**

C. **127.0.0.0/8**

D. **192.16.0.0/8**

90. Louis, a security engineer, is testing methods to defeat the firewall. Which method would he find *MOST* effective?

A. Fragmentation

B. Firewalking

C. Changing static IP address

D. Encryption

91. Alan is a network engineer tasked with writing firewall rules that allow SYN-ACK-SYN communications. Which protocol should he set to permit?

A. UDP

B. TCP

C. ICMP

D. IP

92. What are the *BEST* examples of IPv6 addresses here? (Choose two.)

A. **::1**

B. **a:b:c:d:d:c:b:a**

C. **:::1**

D. **a:b:c:d:e:f:g:h**

93. A system that encrypts a symmetric key so that two users can use this key for secret messages is known as what?

A. DSS

B. Diffie-Hellman

C. AES

D. MD5

94. At which layer does IPsec operate within the OSI model?

A. Application

B. Physical

C. Data Link

D. Network

95. Devar is a systems administrator who manages 1,000 users and their email usage. What is his number one security issue with email?

A. Poor passwords

B. Phishing attacks

C. Use of Thunderbird and other open source email clients

D. Disk space utilization

96. The network interface layer of the TCP/IP model is equivalent to which layer of the OSI model?

A. Application

B. Data link

C. Session

D. Network

97. Which device operates at the data link layer of the OSI model?

A. Firewall

B. Hub

C. Switch

D. Router

98. Which of these protocols operate at the transport layer of the OSI model? (Choose two.)

A. TCP

B. ICMP

C. UDP

D. RARP

99. The ARP command (address resolution protocol) notifies the user of which MAC address a computer uses by providing the IP address of that system. ARP collects data from which layers of the OSI model?

A. Network and data link

B. Physical and data link

C. Network and transport

D. Presentation and application

100. Irina, a systems engineer, is in the process of installing fax machines on a corporate network. Where is the *BEST* place for her to install these for the best security?

A. Break room

B. SOC

C. Computer room

D. Utility closet

Quick Answer Key

1. B	16. B	31. B	46. B	61. B	76. B	91. B
2. A	17. A	32. A	47. A	62. A	77. A	92. A, B
3. B	18. B	33. B	48. B	63. B	78. B	93. B
4. D	19. D	34. D	49. D	64. D	79. D	94. D
5. B, D	20. B	35. B	50. B	65. A	80. B	95. B
6. B	21. B	36. B	51. B	66. B	81. B	96. B
7. B	22. C	37. C	52. C	67. C	82. C	97. C
8. C, D	23. C	38. C	53. C	68. C	83. C	98. A, C
9. A	24. A	39. B	54. A	69. A	84. A	99. A
10. B	25. B	40. B	55. B	70. B	85. B	100. B
11. C, D	26. D	41. D	56. D	71. B, D	86. A, D	
12. B	27. B	42. B	57. B	72. B	87. B	
13. A	28. A, D	43. A	58. A	73. A	88. A, B	
14. B	29. B	44. B	59. B	74. B	89. B	
15. D	30. D	45. D	60. D	75. C, D	90. D	

Answers with explanations

1. **Answer: B Password Authentication Protocol** (**PAP**) is an authentication system used for verifying users. SCP does not use PAP because it does not encrypt like **Extensible Authentication Protocol** (**EAP**) will. The **Transmission Control Protocol** (**TCP**) verifies that each packet has reached its destination. The **User Datagram Protocol** (**UDP**) does not verify that a packet has reached its destination. The **Internet Control**

Message Protocol (**ICMP**) is a protocol that sends error messages based on whether a packet can reach a router or node.

2. **Answer: A** FDDI and Token Ring networks use tokens to pass messages from one node (computer) to another. Ethernet uses **Carrier Sense Multiple Access with Collision Detection** (**CSMA/CD**), where systems listen for the absence of data transmission before sending packets. **Carrier Sense Multiple Access with Collision Avoidance** (**CSMA/CA**) includes systems that transmit a ready-to-send signal to determine whether it is okay to send data.
3. **Answer: B** Secure destruction means removing and destroying the hard drive because it contains records of fax messages sent and received. The other options can leak users' private records.
4. **Answer: D Virtual Private Networks** (**VPNs**) use tunneling protocols, including IPsec and encryption, to allow private, secure networks from home to office or office to office.
5. **Answer: B and D** On Linux systems, the **Domain Name Service** (**DNS**) feature is either called NAMED or BIND, which resolves frequently used domain names (FQDNs) to IP addresses. HTTPD is used to run a web server on the computer. DHCPD allows the computer to run as a DHCP server and supply IP addresses to new clients that join the network.
6. **Answer: B Routing Information Protocol** (**RIP**) is a distance routing protocol that uses hop count metrics to transfer packets from a client to a server. **Open Shortest Path First** (**OSPF**) uses link states such as congestion or lag to determine the best path for packets. **Enhanced Interior Gateway Routing Protocol** (**EIGRP**) is an upgrade of **Interior Gateway Routing Protocol** (**IGRP**), which relearns the best paths for packets, always using the better-performing paths for packets to travel by.
7. **Answer: B** An **Intrusion Detection System** (**IDS**) will report and log, but not block, an incident. Firewalls, **Intrusion Prevention Systems** (**IPSes**), and **Host-Based Intrusion Prevention Systems** (**HIPSes**) all report and block the exploit.
8. **Answer: C and D** Heuristic prevention systems look for anomalies outside of a baseline to detect attacks. Pattern-matching systems look for signatures of known attacks, leaving them vulnerable to zero-day attacks since there is no known solution. **Host-Based Intrusion Detection Systems** (**HIDSes**) and **Network-Based Intrusion Prevention Systems** (**NIPS**) are programmed to employ pattern matching and heuristics to detect attacks.
9. **Answer: A** A fraggle attack sends UDP packets to the local broadcast address and spoofs the source address, which is the target server the attacker wants to disrupt with a **Denial of Service** (**DOS**) attack. Smurf and fraggle attacks can be mitigated by disabling echo requests. Half-open packets are TCP packets that do not respond to ACK requests, thereby not completing the handshake.
10. **Answer: B** The **Demilitarized Zone** (**DMZ**) allows organizations to provide customer access to servers and still provide some level of security. The intranet is a protected area for employees only. A honeypot is a system designed to distract hackers so that researchers can gain intelligence on new attacks.
11. **Answer: C and D Digital Audio Tape** (**DAT**) is used to record audio, video, and data. **File Allocation Table** (**FAT**) is a Windows-based filesystem. Network address translation and port address translation allow organizations to use a common set of internal addresses behind some unique internet address.

12. **Answer: B** Sniffing allows an attacker to monitor a network and collect information such as login names, passwords, emails, files, and more. The best mitigation is encryption. The other options do nothing to protect data on the network.
13. **Answer: A** RIP is an application layer protocol but contains no security features. The Secure Sockets Layer and Transport Layer Security provide encryption at the presentation layer.
14. **Answer: B** Input validation is one of the mitigations of **Cross-Site Scripting** (**XSS**) and SQL injection. XSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. SQL injection is an attack where an attacker injects SQL commands via a web application to extract unauthorized information from a backend database. Reference: https://owasp.org/www-community/attacks/csrf

    https://owasp.org/www-community/attacks/SQL_Injection.

15. **Answer: D** Since the users are operating within LANs that have no web or email services, there is no requirement for stateful services, so a stateless system is most desired in this case.
16. **Answer: B Layer 2 Tunneling Protocol** (**L2TP**) does not encrypt by default, so combined with IPsec, it provides better security compared to PPTP because of the higher-grade encryption but runs slower. PPP and IPsec are not VPN protocols.
17. **Answer: A** PAP sends login and password information in clear text, making it insecure. MD5 is a hashing algorithm, and AES an encryption algorithm. EAP not only encrypts authentication but also can manage certificates, tokens, and other authentication devices.
18. **Answer: B** The formula used to determine the number of connections in a full-mesh network is *N(N-1)/2*. In this case, *N=4*. Substituting the value into the formula *4(4-1)/2* equals *4x3/2*, which becomes *12/2*, and the result of that is *6*. So, six total connections for a four-node full-mesh network.
19. **Answer: D** The key point in this question has to do with range, where fiber optic media can travel around 200 kilometers before significant signal loss. Coaxial cable can travel about 500 meters before significant signal loss. The range for CAT5 is about 100 meters, and **802.11n** Wi-Fi gets about 30 meters before significant signal loss.
20. **Answer: B** Plenum-grade cables are coated with fire retardant so that they emit less smoke when they ignite. Plenum is used for **Heating, Ventilation, and Air Conditioning** (**HVAC**) systems and for circulating oxygen throughout entire buildings. The high oxygen content increases fire risk, so the cabling choice is critical for human safety.
21. **Answer: B** A partial-mesh topology connects all systems together. For example, if there are four nodes, there will be six connections, whereas if the star type was used, the four nodes would connect to a single switch. For a Token Ring topology, the four systems would be connected in a ring, and a token would move counterclockwise and receive and transmit data for that node. A bus network would simply daisy chain the four nodes, and resistors would be installed at each end to signal the end of the bus.
22. **Answer: C** The MAC address burned into a NIC is 48 bits, where the first 24 bits define the manufacturer and the last 24 bits are the card's unique identifier. Ideally, there will be no duplicate MAC addresses in the entire world.

23. **Answer: C Open Source Intelligence** (**OSINT**) is a reconnaissance technique to learn more about the victim using Google, Netcraft, and other public sources. After scanning for network vulnerabilities, hackers test for modems using war dialing because these are not often forgotten when securing the environment. *Answer A* is wrong because there is no such thing as perfect security.
24. **Answer: A** The key part of this question is the *primary purpose*. Changing the ARP table is how the attack is exploited, but the *purpose* of the attack is to listen to packets passing through the network, so *A* is the better answer here. Options *C* and *D* are false answers.
25. **Answer: B** An important key in understanding the CISSP exam is that it is more of a management exam than a technical exam. More often, the candidate should choose the management answer over technical answers because they define how and what technologies to use.
26. **Answer: D** Wireless technologies use **Carrier Sense Multiple Access/Collision Avoidance** (**CSMA/CA**) instead of **CSMA/Collision Detection** (**CSMA/CD**). Token Ring networks use token passing to send and receive messages. Polling networks are used within SCADA technologies.
27. **Answer: B** Packet filtering firewalls work at the network and transport layers. Also, these firewalls are stateless, which means internal requests must be approved by an administrator. The network administrator will create a rule in the firewall to allow the user to communicate with the specific remote site.
28. **Answer: A and D** TACACS (pronounced "takaks") and TACACS+ (pronounced "tak plus") communicate via TCP for better reliability and encrypt all packets. RADIUS communicates via UDP and encrypts passwords only as a AAA (authentication, authorization, and accounting) server.
29. **Answer: B Unshielded Twisted Pair** (**UTP**) has a range of about 100 meters before signal loss, whereas fiber optics can run about 1 kilometer before data loss. Conductors in concentric circles form a coaxial cable.
30. **Answer: D** Most likely, Alexei is running an unsecured SMTP server. Recent updates to the server are not under the control of Alexei and are tested by the cloud provider. Hackers are sending spam to millions of accounts, not his 5,000 users, so the email list is of no concern to the hackers.
31. **Answer: B** An N-tier architecture decouples services into multiple tiers, the most common being the three-tier model. The presentation layer resides at the top and displays differently depending on the device. Below that sits the logic area, where coding is done, for example, HTML. The bottom layer is data where images, videos, customer information, and so on are stored. Split DNS provides a DNS server for the intranet and internet. Split tunneling allows an employee to use a VPN for work resources and not use the VPN for non-work activities. A DMZ is where the public-facing website resides.
32. **Answer: A** Bluejacking allows an attacker to send spam to the victim's phone. Bluebugging allows hackers to eavesdrop on phone calls. When the hacker infects the victim's device with malware and then takes control, this is considered a BlueBorne attack.
33. **Answer: B** CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. XSS attacks occur when an attacker uses a web application to send a malicious script to a different end user that can access any cookies, session tokens, or other sensitive information and can even rewrite

the content of an HTML page. Cookie stealing and cookie monster are false answers. Learn more here: https://owasp.org/www-community/attacks/csrf

https://owasp.org/www-community/attacks/xss/

34. **Answer: D** Kerberos authenticates with tickets, not RADIUS. SAML is used to authenticate a user to another service provider, for example, a bank partnered with check printers, which is not happening here. EAP is a communication protocol, not an authentication protocol.
35. **Answer: B** The OSI transport layer matches the TCP/IP host-to-host layer, and the OSI network layer matches the TCP/IP internet layer, and the OSI data link and physical layers match the TCP/IP network access layer.
36. **Answer: B** The application layer is where programs reside. The presentation layer processes data on how it should appear or sound to the user. The session layer manages communications between applications. The transport layer manages communications between nodes (such as computers, laptops, and smartphones).
37. **Answer: C Internet of Things** (**IoT**) devices are attacked more frequently because security is often overlooked for these devices. This also includes thermometers, IP cameras, refrigerators, televisions, multi-function printers, and others (the question states they are all *network devices*).
38. **Answer: C** TCP provides a guaranteed connection from host to host. To do this, it tracks data receipts through acknowledgment numbers. UDP is connectionless and makes the greatest effort to ensure that data reaches its destination. If a packet is lost, it does not know. The IP header tracks data fragments, and ICMP is used to verify nodes exist and are running.
39. **Answer: B** The attacker uses the session information to strengthen the spoofing details of the victim and performs session hijacking using the victim's already-approved credentials with the bank. The user thinks they were simply disconnected. XSS allows the attacker to run a script on the user's computer. SQL injection is an attack on a web server to send SQL commands and download credit card numbers and so on. Learn more here: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery
40. **Answer: B** Although RPC operates at the session layer, FTP operates at the application layer. TCP and UDP operate at the transport layer, and ICMP operates at the network layer. RIP operates at the application layer.
41. **Answer: D** Firewalking uses traceroute and TTL values to find firewalls, determine which services the firewall allows, and map networks. Ping-of-death is a DOS attack that spoofs the source address, and all requests head to the victim machine.
42. **Answer: B Quality of Service** (**QoS**) prioritizes applications such as VoIP systems to guarantee a level of quality. The other options are false answers.
43. **Answer: A** The **Registration Authority** (**RA**) verifies and validates the user. The **Certificate Authority** (**CA**) signs the certificate and returns it to the user (Jorge, in this case). The **Certificate Revocation List** (**CRL**) is a list of expired and revoked certificates. The root CA maintains all of the certificates it has signed; this system is very secure; for example, it is air-gapped.

44. **Answer: B** Baseband is usually used for Ethernet networks over coaxial, fiber optic, or twisted pair. Broadband can transmit data, audio, and video at the same time as radio waves, coaxial, or fiber optic.
45. **Answer: D** Encryption can be broken, so the best option is fiber optic cable because it emits no **Electro-Magnetic Interference** (**EMI**). Shielded twisted pair is much lower in cost than fiber optic.
46. **Answer: B.** IP addresses in the form of **169.254.xxx.xxx** have autoconfiguration enabled, which provides a system with an IP address until the DHCP server recovers. Use is very limited, and the user will not be able to access the internet with this IP address.
47. **Answer: A** DHCP snooping assigns IP addresses only to systems assigned by network administrators. Flood guards would help with DOS attacks. Integrity checking and encryption would not secure the network connections.
48. **Answer: B** An NIDS will only report threats, not block them. An NIPS would be more appropriate. Only SNMPv3 encrypts community strings, which carry passwords to routers and switches.
49. **Answer: D** Since this is a *public* **Domain Name Service** (**DNS**) server, restricting traffic to staff would make it useless to the public, and the encryption of zone information would make it useless as well. An HIDS would not protect the server, nor would **Domain Name System Security Extensions** (**DNSSEC**), which ensures that zone transfers are authenticated and robust.
50. **Answer: B** Since other customers are not complaining, the DHCP server is functioning fine, and a hacker would kick everyone off the network, not only Matt.
51. **Answer: B** Basic routers are not designed to block internal website requests, but advanced multi-layer routers can. Proxies are designed to protect the LAN and can be configured to block websites users are attempting to access.
52. **Answer: C** Application-level firewalls not only consider ports, IP addresses, sources, and destinations but can perform deep packet inspection. This further inspection hurts performance as compared to other firewalls, and encryption can mitigate the useful purpose of an application-level firewall.
53. **Answer: C** HTTPS = **443**, FTP-DATA=**20**, FTP-AUTHENTICATION=**21**, Telnet=**23**, DNS=**53**, POP3=**110**, NTP=**123**
54. **Answer: A** SIP is used to initiate phone calls on VoIP systems, and **Real-Time Transport Protocol** (**RTP**) carries the conversation. Placing VoIP phones within their own VLAN assures that only VoIP traffic is allowed in this subnet.
55. **Answer: B** Routers and gateways can extend a network, but computers will reside on different subnets. A firewall is an NIPS designed to block threats from attackers.
56. **Answer: D** Link-state routing protocols are more accurate than distance-vector protocols such as RIP, because they look at the number of hops, network load, packet size, and more to determine the best routes for packets. OSPF is a link-state routing protocol.
57. **Answer: B Sender Policy Framework** (**SPF**) verifies that emails are coming from where they say they are coming from. **Simple Authentication and Security Layer** (**SASL**) is used to authenticate users so they can read their emails. **Secure Sockets Layer** (**SSL**) protects communications through encryption; TLS replaced SSL because of its vulnerabilities. SMTP manages sending email to people.
58. **Answer: A** Script kiddies are new to hacking and therefore very unskilled. In this case, the hacker has launched the attack on himself because **127.0.0.1** is the localhost address

of his computer (and every computer). A white-hat hacker and ethical hacker are the same, and they are paid to audit the security of a business.

59. **Answer: B** Split-DNS provides a secured internal DNS server for internal requests, and the internet-based DNS server provides basic DNS servers for the public, and some access to corporate sites, such as other websites and mail servers.
60. **Answer: D Unshielded Twisted Pair** (**UTP**) cables can be vulnerable to crosstalk. **Shielded Twisted Pair** (**STP**) greatly reduces issues related to crosstalk and other interference.
61. **Answer: B** IP convergence entails utilizing internet protocols to provide other services not initially intended, such as phone services with VoIP or data transfers to storage devices with iSCSI.
62. **Answer: A Network Address Translation** (**NAT**) maps external addresses, such as **1.2.3.4**, to internal addresses, such as **10.0.0.4**. **Transmission Control Protocol** (**TCP**) provides connection-oriented communications. **Request for Comment** (**RFC**) is a set of standards provided by the Internet Engineering Task Force. Teredo provides IPv6 functionality within IPv4 networks.
63. **Answer: B** VPN split tunneling allows a user to connect with a secured corporate network for work-related activities and an unsecured public tunnel for personal work. In cases like this, it is possible for malware to transfer from the public to the private network. For best security, disable split tunneling.
64. **Answer: D** System A is on the **192.168.4.0** subnet, and system B is on the **192.168.5.0** subnet. One way to fix this is to switch system B's address to **192.168.4.8**. Replacing cables and checking connections would result in the same issue. Hubs are inherently insecure because all traffic can be monitored.
65. **Answer: B** Well-known ports include FTP (port **21**), SSH (port **22**), HTTP (port **80**), and others. Ports **1024**-**49151** are called the *registered ports*, which vendors specify for their proprietary applications. The *dynamic ports* start at **49152**-**65535** and are available as needed for applications.
66. **Answer: B** Bitwise and V2Bit are false answers because they are not layers in the OSI model. The data link layer converts bits into frames.
67. **Answer: C** The impact of digital music would introduce negligible performance issues, and if a firewall is blocking ports to a web server, degradation would be 100% for just that service only, not the entire network. Shutting down computers reduces network load, so the most likely cause is malware on the network routers.
68. **Answer: C** Open authentication provides no security at all because no password is required to access the network. WEP is relatively easy to crack. WPA2 would be the very best to use, but older-generation devices do not have that capability. WPA is much more difficult to crack than WEP.
69. **Answer: A Virtual LANs** (**VLANs**) allow administrators to group systems together based on function or need. VPNs allow direct connections from a single machine to home or office. DNS performs IP address lookups when a user provides a domain name. The DMZ is where companies position customer-accessible websites just outside of their LAN on the internet.
70. **Answer: B** UDP is connectionless, so is better for digital video and audio applications because it does not require packet-receipt verification, like TCP, because TCP utilizes a three-way handshake.

71. **Answer: B and D** VPN connections can encrypt data in other manners, not with IPsec only; but IPsec is supported worldwide.
72. **Answer: B** NMAP and HPING are utilities that can perform port scans, searching for vulnerabilities on the server. A **Distributed Denial of Service** (**DDOS**) attack would harm server performance and come from several multiple IP addresses.
73. **Answer: A** Telnet is used for remote logins, not remote file transfers, so Serena would get caught and not transfer any files. Serena is likely to get caught using FTP because it does not encrypt. SSH is used for remote logins. To transfer files, she would need to use **Secure Copy** (**SCP**). Using HTTP services appears normal, so it would not alert system administrators.
74. **Answer: B Asymmetric Digital Subscriber Line** (**ADSL**) modems generally download eight times faster than they upload. Since she's transferring data to the office, it's uploading from home, at a much slower rate. **Symmetric Digital Subscriber Line** (**SDSL**) would be an upgrade for her from ADSL, giving her much faster upload speeds from home. C and D are not correct because the network administrator states the network is running fine.
75. **Answer: C and D** Routers operate at layer 3 and connect two disparate networks.
76. **Answer: B** CSMA/CD works in Ethernet bus networks only, which are half-duplex, so a message can only be sent when the network is clear. Full-duplex allows traffic to be sent without delay, such as in fiber networks. Wireless networks use **Carrier Sense Multiple Access/Collision Avoidance** (**CSMA/CA**).
77. **Answer: A** Hubs, in general, are insecure because users can observe all traffic passing through the hubs, even data not intended for them. Switches allow traffic to connect directly to targets, making it more difficult for attackers to eavesdrop.
78. **Answer: B** Bluetooth is short-range, extending to about 10 meters, and fiber and Ethernet would require permission from the landowner between the two buildings. Yagi is best for site-to-site connections with ranges of up to several miles, as long as there is no interference.
79. **Answer: D** Since users are able to send emails, an email client and server are installed and running. Since users are able to send emails, SMTP is working fine on port **25**.
80. **Answer: B** Yep, RIP is a layer 7 protocol. Encryption and decryption are generally done at layer 6 but can also occur at other layers, including layer 3, depending on the protocol. MAC addresses are utilized at layer 2. Reference: https://www.geeksforgeeks.org/routing-information-protocol-rip/.
81. **Answer: B** Many technologies exist to perform hackback, but it is against the law.
82. **Answer: C** The **Layer 2 Tunneling Protocol** (**L2TP**) provides no encryption. **Wired Equivalent Privacy** (**WEP**) is the weakest wireless standard. **Wi-Fi Protected Access** (**WPA**) provides even stronger security to wireless networks using TKIP to strengthen initialization vectors, which provides more variance to encryption keys. **Point-to-Point Tunneling Protocol** (**PPTP**) is a tunneling protocol to secure VPNs.
83. **Answer: C Indicators of Compromise** (**IOCs**) that match patterns are used in signature-based detection and prevention systems. Since the question specifically mentioned a prevention system, an IDS would be an incorrect answer. These systems can either be host- or network-based, and heuristic IOCs are measured against some baseline. When the IOC is outside of that baseline, it is flagged as malware.

84. **Answer: A** Phishing attacks use spoofed emails to gain the victim's trust, and usually contain links that forward users to fake websites when they click them. IP forwarding is used to re-route packets to an alternate network, for example, from the WAN to the LAN. Flooding is used as an availability attack on a website, sending noise so that others cannot access the site.
85. **Answer: B** The **Time-to-Live** (**TTL**) field decrements a counter for each router hop it takes for a packet to reach its destination. If the counter reaches zero before reaching the destination, the packet drops.
86. **Answer: A and D** Among other issues, Telnet and FTP both transmit data in clear text, allowing man-in-the-middle attackers to view entire conversations, including login names and passwords. SSH and HTTPS encrypt entire conversations, making it very difficult for hackers to run their exploits.
87. **Answer: B** An open system provides no security at all, allowing users to access a wireless access point without a password. WEP offers authentication, but it is very easy for even a script kiddie to attack. WPA is very strong, but WPA2 is the strongest and best solution for a secure area when using wireless access points.
88. **Answer: A and B** RADIUS and Kerberos are single-sign-on systems allowing users to access a network of systems with a single login and password. L2TP is the recommended VPN protocol over PPTP because it uses IPsec for encryption.
89. **Answer: B** The **127.0.0.0/8** network range is the localhost. Every computer has a localhost address, and it points to itself. **169.254.0.0/16** is the APIPA address suite, where a temporary IP address is provided for LAN usage, but not the internet. A DHCP server will provide an address for internet use once the server is up and running. **192.16.0.0/8** is an example of a public IP address.
90. **Answer: D** Encryption will also encrypt malware signatures that a firewall will not recognize. Firewalking is a method used to detect firewalls. Data fragments are mitigated by most firewalls to recognize malware signatures. After an IP address change, data still flows through the system.
91. **Answer: B** UDP, IP, and ICMP do not use SYN or ACK to confirm a connection.
92. **Answer: A and B** IPv6 address consist of 8 hextets using hexadecimal math where values go from **0** through *F*. A full IPv6 address looks like **1234:0000:4321:abcd:deef:feed:4321:9090**, but the system allows shortcuts. **0000:0000:0000:0000:0000:0000:0000:0001** or **::1** is the localhost address that every node has (equivalent to IPv4's **127.0.0.1**). **A:B:C:D:D:C:B:A** is the shortcut for **000A:000B:000C:000D:000D:000C:000B:000A**.
93. **Answer: B** The **Digital Signature Standard** (**DSS**) is an asymmetric encryption standard for signing and verification only. AES is a symmetric encryption standard for securing Wi-Fi connections. MD5 is a hashing algorithm for integrity checking.
94. **Answer: D** IPsec operates in two modes, transport and tunnel. Transport mode encrypts the data only, whereas tunnel mode encrypts the data and the message headers, providing additional location secrecy.
95. **Answer: B** Running out of disk space reduces availability, but in most cases this is easily fixed by increasing disk space or removing files. Change management systems will not allow the use of corporate-mandated email clients. Poor passwords are mitigated through policy and password validation tools. Phishing attacks can lead to network-wide ransomware, putting the organization at risk of going out of business.

96. **Answer: B** Layer 1 (physical), and layer 2 (data link) of the OSI model are equivalent to the network layer of the TCP/IP model. The TCP/IP model is four layers: layer one is the network interface, layer two is internetworking, layer three is transport, and layer 4 is the application.
97. **Answer: C** The seven layers of the OSI model are physical, where hubs operate; data link, where switches operate; network, where routers and some firewalls operate; transport; session, where stateful firewalls operate; presentation; and application, where application firewalls operate.
98. **Answer: A and C** ICMP operates at the network layer of the OSI model, and **Reverse Address Resolution Protocol** (**RARP**) resolves MAC addresses into IP addresses and operates between the data link and network layers.
99. **Answer: A** ARP collects the MAC address information from the data link layer and the **Internet Protocol** (**IP**) address information from the network layer.
100. **Answer: B** The **Security Operations Center** (**SOC**) monitors user ingress and egress as well as user activities on fax machines and other computers in the SOC. The SOC has integrity and transmission security controls in place as well.

Chapter 4
Communication and Network Security (Domain 4)

1. What important factor differentiates Frame Relay from X.25?
    1. Frame Relay supports multiple PVCs over a single WAN carrier connection.
    2. Frame Relay is a cell-switching technology instead of a packet-switching technology like X.25.
    3. Frame Relay does not provide a committed information rate (CIR).
    4. Frame Relay only requires a DTE on the provider side.
2. During a security assessment of a wireless network, Jim discovers that LEAP is in use on a network using WPA. What recommendation should Jim make?
    1. Continue to use LEAP. It provides better security than TKIP for WPA networks.
    2. Use an alternate protocol like PEAP or EAP-TLS and implement WPA2 if supported.
    3. Continue to use LEAP to avoid authentication issues, but move to WPA2.
    4. Use an alternate protocol like PEAP or EAP-TLS, and implement Wired Equivalent Privacy to avoid wireless security issues.
3. Ben has connected his laptop to his tablet PC using an 802.11g connection. What wireless network mode has he used to connect these devices?
    1. Infrastructure mode
    2. Wired extension mode
    3. Ad hoc mode
    4. Stand-alone mode

4. Lauren's and Nick's PCs simultaneously send traffic by transmitting at the same time. What network term describes the range of systems on a network that could be affected by this same issue?
    1. The subnet
    2. The supernet
    3. A collision domain
    4. A broadcast domain
5. Sarah is manually reviewing a packet capture of TCP traffic and finds that a system is setting the RST flag in the TCP packets it sends repeatedly during a short period of time. What does this flag mean in the TCP packet header?
    1. RST flags mean "Rest." The server needs traffic to briefly pause.
    2. RST flags mean "Relay-set." The packets will be forwarded to the address set in the packet.
    3. RST flags mean "Resume Standard." Communications will resume in their normal format.
    4. RST means "Reset." The TCP session will be disconnected.
6. Gary is deploying a wireless network and wants to deploy the fastest possible wireless technology. Due to technical constraints, he is limited to using a 2.4 GHz option. Which one of the following wireless networking standards should he use?
    1. 802.11a
    2. 802.11g
    3. 802.11n
    4. 802.11ac
7. Match each of the numbered TCP ports listed with the associated lettered protocol provided:

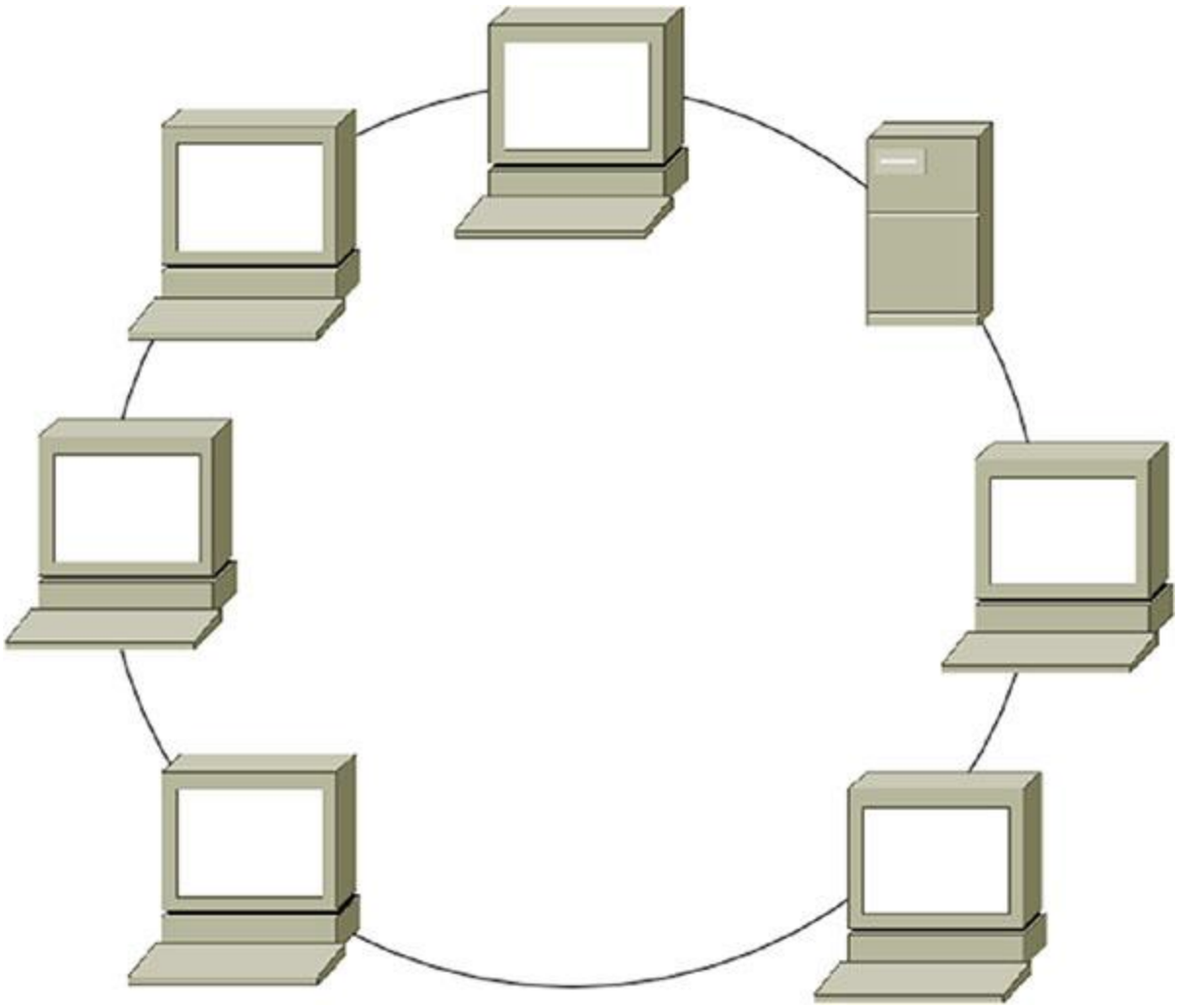
    TCP ports

    1. 23
    2. 25
    3. 143
    4. 515

    Protocols

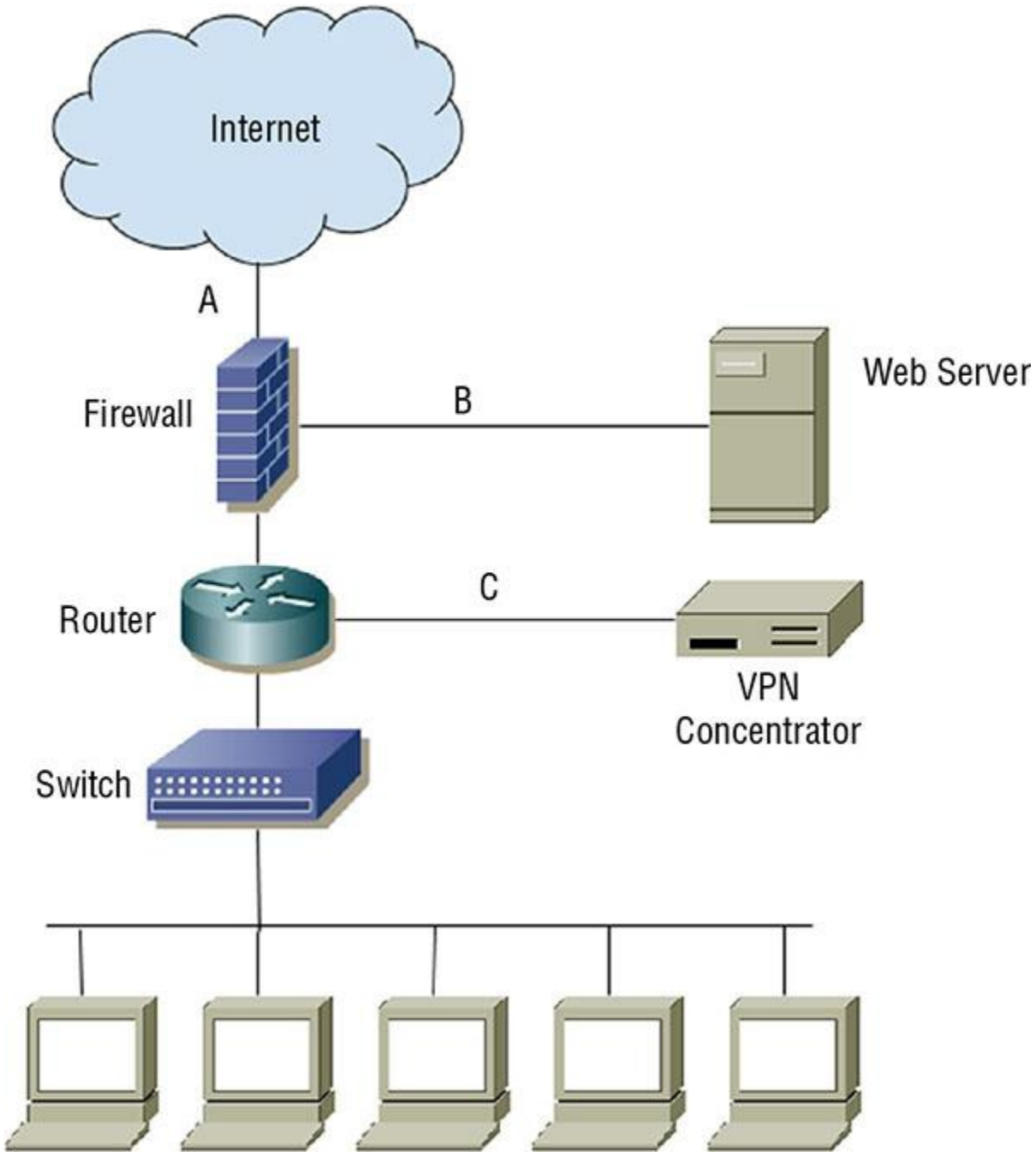
    5. SMTP
    6. LPD
    7. IMAP
    8. Telnet
8. Chris is configuring an IDS to monitor for unencrypted FTP traffic. What ports should Chris use in his configuration?
    1. TCP 20 and 21
    2. TCP 21 only
    3. UDP port 69
    4. TCP port 21 and UDP port 21

9. FHSS, DSSS, and OFDM all use what wireless communication method that occurs over multiple frequencies simultaneously?
    1. WiFi
    2. Spread Spectrum
    3. Multiplexing
    4. Orthogonal modulation
10. Brian is selecting an authentication protocol for a PPP connection. He would like to select an option that encrypts both usernames and passwords and protects against replay using a challenge/response dialog. He would also like to reauthenticate remote systems periodically. Which protocol should he use?
    1. PAP
    2. CHAP
    3. EAP
    4. LEAP
11. Which one of the following protocols is commonly used to provide backend authentication services for a VPN?
    1. HTTPS
    2. RADIUS
    3. ESP
    4. AH
12. What network topology is shown in the following image?



1. A ring
2. A bus
3. A star
4. A mesh

Chris is designing layered network security for his organization. Using the following diagram, answer questions 13 through 15.



13. What type of firewall design is shown in the diagram?
    1. A single-tier firewall
    2. A two-tier firewall
    3. A three-tier firewall
    4. A four-tier firewall
14. If the VPN grants remote users the same access to network and system resources as local workstations have, what security issue should Chris raise?
    1. VPN users will not be able to access the web server.

2. There is no additional security issue; the VPN concentrator's logical network location matches the logical network location of the workstations.
3. Web server traffic is not subjected to stateful inspection.
4. VPN users should only connect from managed PCs.

15. If Chris wants to stop cross-site scripting attacks against the web server, what is the best device for this purpose, and where should he put it?
    1. A firewall, location A
    2. An IDS, location A
    3. An IPS, location B
    4. A WAF, location C
16. Susan is deploying a routing protocol that maintains a list of destination networks with metrics that include the distance in hops to them and the direction traffic should be sent to them. What type of protocol is she using?
    1. A link-state protocol
    2. A link-distance protocol
    3. A destination metric protocol
    4. A distance-vector protocol
17. Ben has configured his network to not broadcast an SSID. Why might Ben disable SSID broadcast, and how could his SSID be discovered?
    1. Disabling SSID broadcast prevents attackers from discovering the encryption key. The SSID can be recovered from decrypted packets.
    2. Disabling SSID broadcast hides networks from unauthorized personnel. The SSID can be discovered using a wireless sniffer.
    3. Disabling SSID broadcast prevents issues with beacon frames. The SSID can be recovered by reconstructing the BSSID.
    4. Disabling SSID broadcast helps avoid SSID conflicts. The SSID can be discovered by attempting to connect to the network.
18. What network tool can be used to protect the identity of clients while providing Internet access by accepting client requests, altering the source addresses of the requests, mapping requests to clients, and sending the modified requests out to their destination?
    1. A gateway
    2. A proxy
    3. A router
    4. A firewall
19. During troubleshooting, Chris uses the nslookup command to check the IP address of a host he is attempting to connect to. The IP he sees in the response is not the IP that should resolve when the lookup is done. What type of attack has likely been conducted?
    1. DNS spoofing
    2. DNS poisoning
    3. ARP spoofing
    4. A Cain attack
20. A remote access tool that copies what is displayed on a desktop PC to a remote computer is an example of what type of technology?
    1. Remote node operation
    2. Screen scraping
    3. Remote control

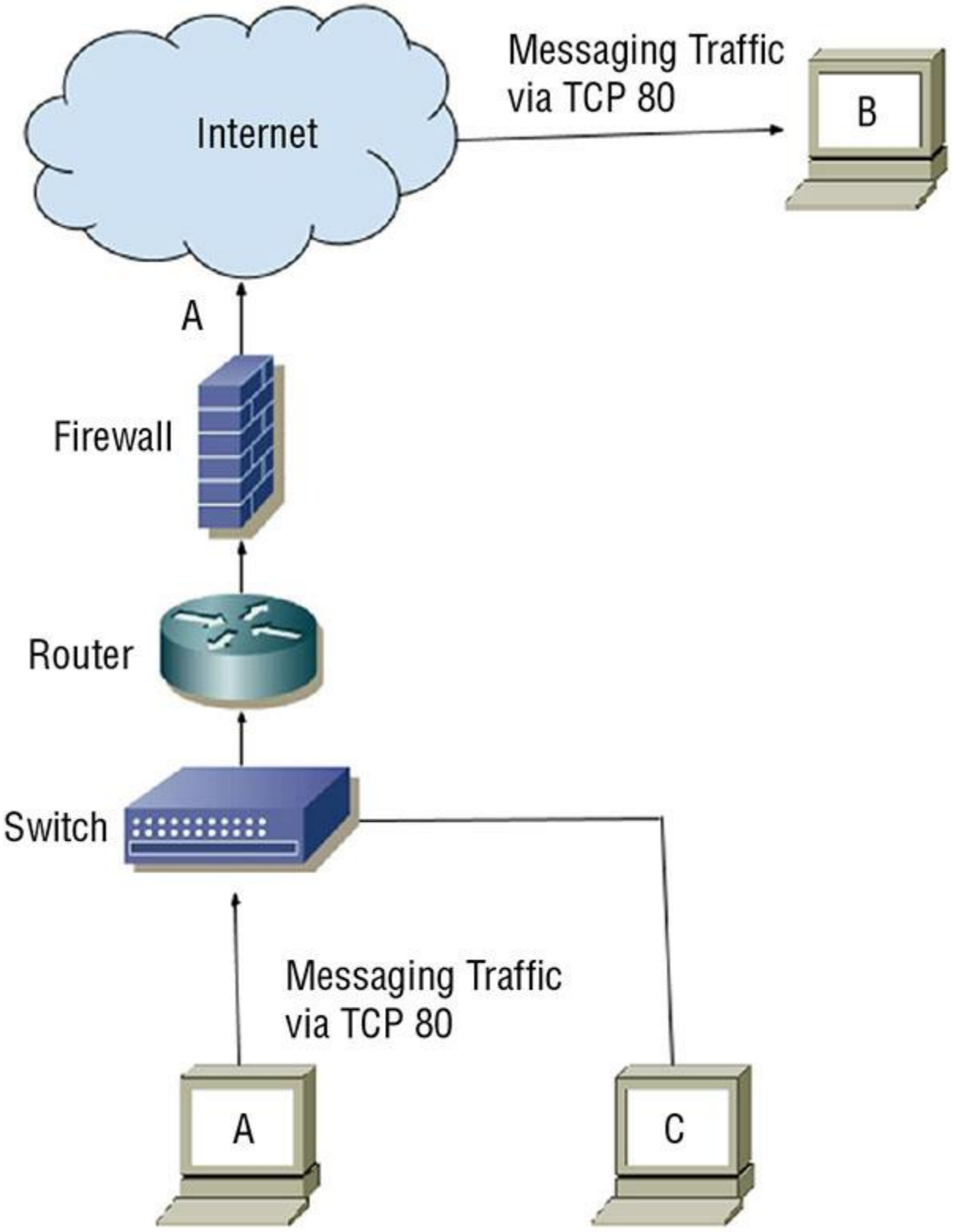
4. RDP

21. Which email security solution provides two major usage modes: (1) signed messages that provide integrity, sender authentication, and nonrepudiation; and (2) an enveloped message mode that provides integrity, sender authentication, and confidentiality?
    1. S/MIME
    2. MOSS
    3. PEM
    4. DKIM
22. During a security assessment, Jim discovers that the organization he is working with uses a multilayer protocol to handle SCADA systems and recently connected the SCADA network to the rest of the organization's production network. What concern should he raise about serial data transfers carried via TCP/IP?
    1. SCADA devices that are now connected to the network can now be attacked over the network.
    2. Serial data over TCP/IP cannot be encrypted.
    3. Serial data cannot be carried in TCP packets.
    4. TCP/IP's throughput can allow for easy denial of service attacks against serial devices.
23. What type of key does WEP use to encrypt wireless communications?
    1. An asymmetric key
    2. Unique key sets for each host
    3. A predefined shared static key
    4. Unique asymmetric keys for each host
24. Arnold is receiving reports from end users that their internet connections are extremely slow. He looks at the firewall and determines that there are thousands of unexpected inbound connections per second arriving from all over the world. What type of attack is most likely occurring?
    1. A worm
    2. A denial of service attack
    3. A virus
    4. A smurf attack
25. What speed and frequency range is used by 802.11n?
    1. 54 Mbps, 5 GHz
    2. 200+ Mbps, 5GHz
    3. 200+ Mbps, 2.4 and 5 GHz
    4. 1 Gbps, 5 GHz
26. The Address Resolution Protocol (ARP) and the Reverse Address Resolution Protocol (RARP) operate at what layer of the OSI model?
    1. Layer 1
    2. Layer 2
    3. Layer 3
    4. Layer 4
27. Which of the following is a converged protocol that allows storage mounts over TCP, and which is frequently used as a lower-cost alternative to Fibre Channel?
    1. MPLS
    2. SDN

3. VoIP
4. iSCSI

28. Chris is building an Ethernet network and knows that he needs to span a distance of more than 150 meters with his 1000BaseT network. What network technology should he use to help with this?
    1. Install a repeater or a concentrator before 100 meters.
    2. Use Category 7 cable, which has better shielding for higher speeds.
    3. Install a gateway to handle the distance.
    4. Use STP cable to handle the longer distance at high speeds.

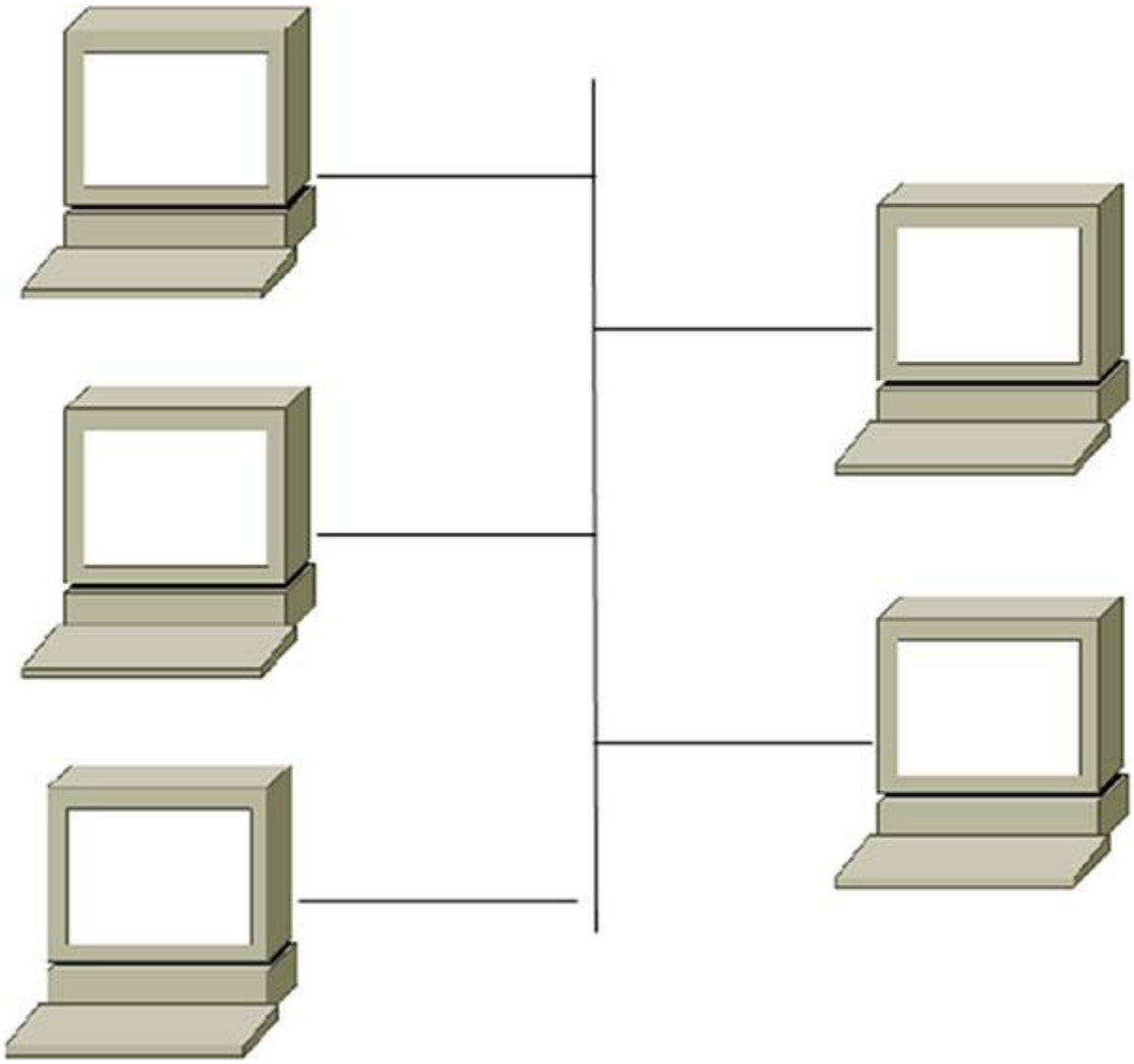
    Lauren's organization has used a popular messaging service for a number of years. Recently, concerns have been raised about the use of messaging. Using the following diagram, answer questions 29 through 31 about messaging.



29. What protocol is the messaging traffic most likely to use based on the diagram?
    1. SLACK
    2. HTTP

3. SMTP
4. HTTPS

30. What security concern does sending internal communications from A to B raise?
    1. The firewall does not protect system B.
    2. System C can see the broadcast traffic from system A to B.
    3. It is traveling via an unencrypted protocol.
    4. Messaging does not provide nonrepudation.
31. How could Lauren's company best address a desire for secure messaging for users of internal systems A and C?
    1. Use a third-party messaging service.
    2. Implement and use a locally hosted service.
    3. Use HTTPS.
    4. Discontinue use of messaging and instead use email, which is more secure.
32. Which of the following drawbacks is a concern when multilayer protocols are allowed?
    1. A range of protocols may be used at higher layers.
    2. Covert channels are allowed.
    3. Filters cannot be bypassed.
    4. Encryption can't be incorporated at multiple layers.
33. What network topology is shown in the following image?



1. A ring
2. A star
3. A bus
4. A mesh

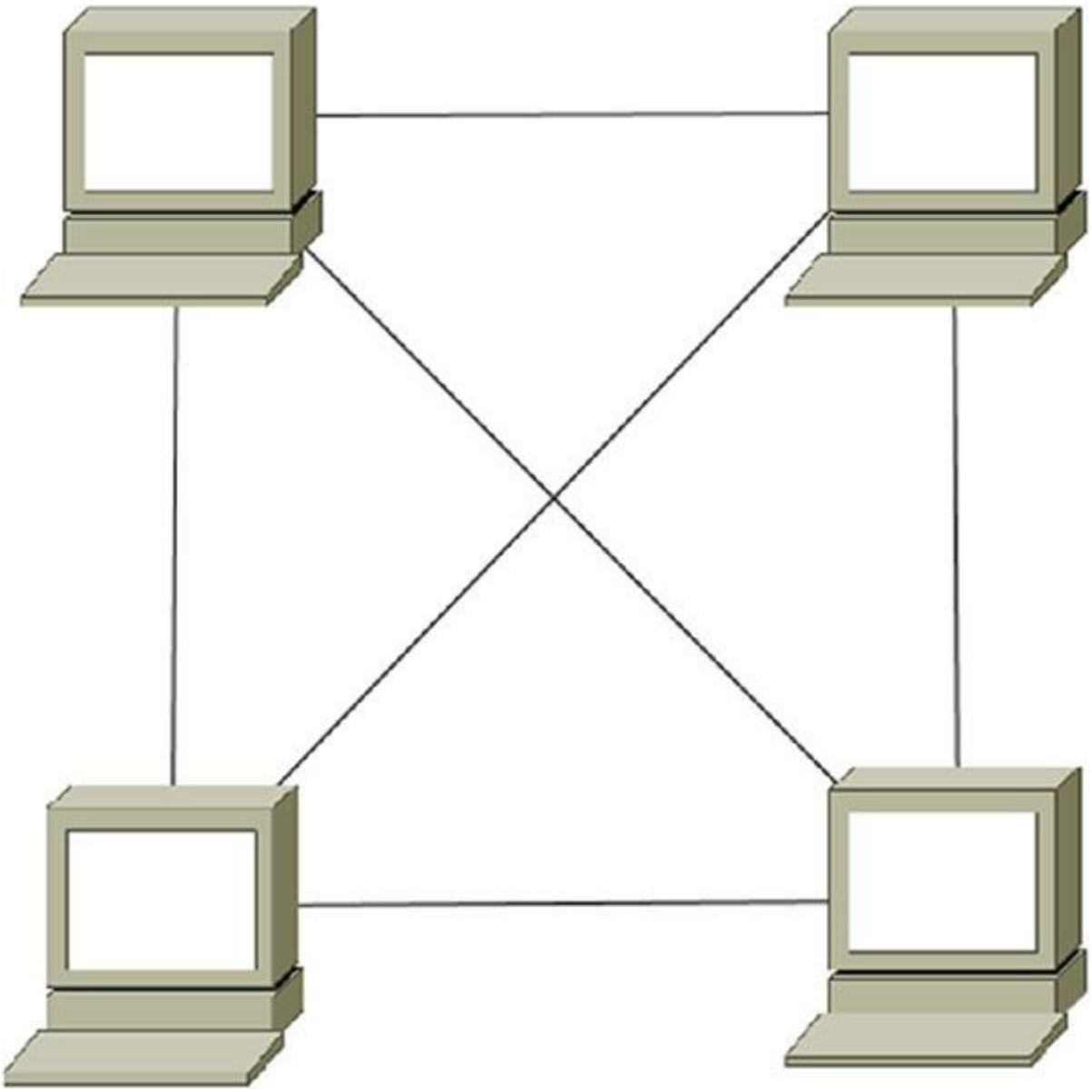
34. Chris uses a cellular hot spot (modem) to provide internet access when he is traveling. If he leaves the hot spot connected to his PC while his PC is on his organization's corporate network, what security issue might he cause?
    1. Traffic may not be routed properly, exposing sensitive data.
    2. His system may act as a bridge from the internet to the local network.
    3. His system may be a portal for a reflected DDoS attack.
    4. Security administrators may not be able to determine his IP address if a security issue occurs.
35. In her role as an information security professional, Susan has been asked to identify areas where her organization's wireless network may be accessible even though it isn't

intended to be. What should Susan do to determine where her organization's wireless network is accessible?

1. A site survey
2. Warwalking
3. Wardriving
4. A design map

36. The DARPA TCP/IP model's Application layer matches up to what three OSI model layers?
    1. Application, Presentation, and Transport.
    2. Presentation, Session, and Transport.
    3. Application, Presentation, and Session.
    4. There is not a direct match. The TCP model was created before the OSI model.
37. One of Susan's attacks during a penetration test involves inserting false ARP data into a system's ARP cache. When the system attempts to send traffic to the address it believes belongs to a legitimate system, it will instead send that traffic to a system she controls. What is this attack called?
    1. RARP flooding
    2. ARP cache poisoning
    3. A denial of ARP attack
    4. ARP buffer blasting
38. Sue modifies her MAC address to one that is allowed on a network that uses MAC filtering to provide security. What is the technique Sue used, and what nonsecurity issue could her actions cause?
    1. Broadcast domain exploit, address conflict
    2. Spoofing, token loss
    3. Spoofing, address conflict
    4. Sham EUI creation, token loss
39. Jim's audit of a large organization's traditional PBX showed that Direct Inward System Access (DISA) was being abused by third parties. What issue is most likely to lead to this problem?
    1. The PBX was not fully patched.
    2. The dial-in modem lines use unpublished numbers.
    3. DISA is set up to only allow local calls.
    4. One or more users' access codes have been compromised.
40. SMTP, HTTP, and SNMP all occur at what layer of the OSI model?
    1. Layer 4
    2. Layer 5
    3. Layer 6
    4. Layer 7
41. Lauren uses the ping utility to check whether a remote system is up as part of a penetration testing exercise. If she does not want to see her own ping packets, what protocol should she filter out from her packet sniffer's logs?
    1. UDP
    2. TCP
    3. IP
    4. ICMP

42. Lauren wants to provide port-based authentication on her network to ensure that clients must authenticate before using the network. What technology is an appropriate solution for this requirement?
    1. 802.11a
    2. 802.3
    3. 802.15.1
    4. 802.1x
43. Ben has deployed a 1000BaseT 1 gigabit network and needs to run a cable to another building. If Ben is running his link directly from a switch to another switch in that building, what is the maximum distance Ben can cover according to the 1000BaseT specification?
    1. 2 kilometers
    2. 500 meters
    3. 185 meters
    4. 100 meters
44. Jim is building the network for a remote site that only has ISDN as an option for connectivity. What type of ISDN should he look for to get the maximum speed possible?
    1. BRI
    2. BPRI
    3. PRI
    4. D channel
45. SPIT attacks target what technology?
    1. Virtualization platforms
    2. Web services
    3. VoIP systems
    4. Secure Process Internal Transfers
46. What does a bluesnarfing attack target?
    1. Data on IBM systems
    2. An outbound phone call via Bluetooth
    3. 802.11b networks
    4. Data from a Bluetooth-enabled device
47. Which of the following options includes standards or protocols that exist in layer 6 of the OSI model?
    1. NFS, SQL, and RPC
    2. TCP, UDP, and TLS
    3. JPEG, ASCII, and MIDI
    4. HTTP, FTP, and SMTP
48. What network topology is shown here?



1. A ring
2. A bus
3. A star
4. A mesh

49. There are four common VPN protocols. Which group listed contains all of the common VPN protocols?
    1. PPTP, LTP, L2TP, IPsec
    2. PPP, L2TP, IPsec, VNC
    3. PPTP, L2F, L2TP, IPsec
    4. PPTP, L2TP, IPsec, SPAP
50. What network technology is best described as a token-passing network that uses a pair of rings with traffic flowing in opposite directions?
    1. A ring topology

2. Token Ring
3. FDDI
4. SONET

51. Which OSI layer includes electrical specifications, protocols, and interface standards?
    1. The Transport layer
    2. The Device layer
    3. The Physical layer
    4. The Data Link layer
52. Ben is designing a Wi-Fi network and has been asked to choose the most secure option for the network. Which wireless security standard should he choose?
    1. WPA2
    2. WPA
    3. WEP
    4. AES
53. If your organization needs to allow attachments in email to support critical business processes, what are the two best options for helping to avoid security problems caused by attachments?
    1. Train your users and use antimalware tools.
    2. Encrypt your email and use antimalware tools.
    3. Train your users and require S/MIME for all email.
    4. Use S/MIME by default and remove all ZIP (.zip) file attachments.
54. Segmentation, sequencing, and error checking all occur at what layer of the OSI model that is associated with SSL, TLS, and UDP?
    1. The Transport layer
    2. The Network layer
    3. The Session layer
    4. The Presentation layer
55. The Windows ipconfig command displays the following information:

    BC-5F-F4-7B-4B-7D

    What term describes this, and what information can usually be gathered from it?

    1. The IP address, the network location of the system
    2. The MAC address, the network interface card's manufacturer
    3. The MAC address, the media type in use
    4. The IPv6 client ID, the network interface card's manufacturer
56. Chris has been asked to choose between implementing PEAP and LEAP for wireless authentication. What should he choose, and why?
    1. LEAP, because it fixes problems with TKIP, resulting in stronger security
    2. PEAP, because it implements CCMP for security
    3. LEAP, because it implements EAP-TLS for end-to-end session encryption
    4. PEAP, because it can provide a TLS tunnel that encapsulates EAP methods, protecting the entire session

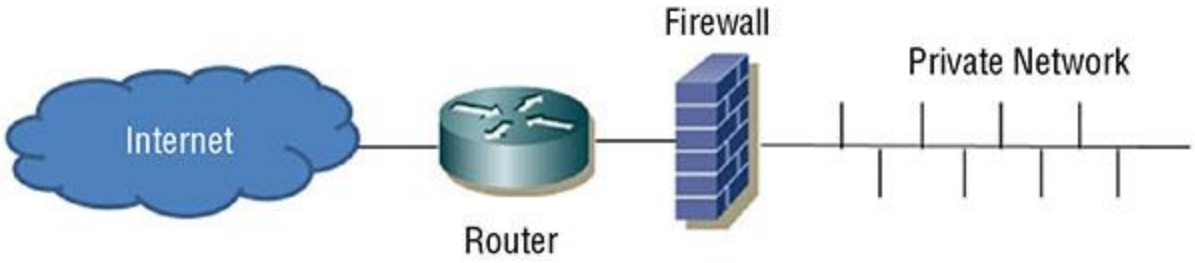
57. Ben is troubleshooting a network and discovers that the NAT router he is connected to has the 192.168.x.x subnet as its internal network and that its external IP is 192.168.1.40. What problem is he encountering?
    1. 192.168.x.x is a nonroutable network and will not be carried to the Internet.
    2. 192.168.1.40 is not a valid address because it is reserved by RFC 1918.
    3. Double NATing is not possible using the same IP range.
    4. The upstream system is unable to de-encapsulate his packets and he needs to use PAT instead.
58. What is the default subnet mask for a Class B network?
    1. 255.0.0.0
    2. 255.255.0.0
    3. 255.254.0.0
    4. 255.255.255.0
59. Jim's organization uses a traditional PBX for voice communication. What is the most common security issue that its internal communications are likely to face, and what should he recommend to prevent it?
    1. Eavesdropping, encryption
    2. Man-in-the-middle attacks, end-to-end encryption
    3. Eavesdropping, physical security
    4. Wardialing, deploy an IPS
60. What common security issue is often overlooked with cordless phones?
    1. Their signal is rarely encrypted and thus can be easily monitored.
    2. They use unlicensed frequencies.
    3. They can allow attackers access to wireless networks.
    4. They are rarely patched and are vulnerable to malware.
61. Lauren's organization has deployed VoIP phones on the same switches that the desktop PCs are on. What security issue could this create, and what solution would help?
    1. VLAN hopping; use physically separate switches.
    2. VLAN hopping; use encryption.
    3. Caller ID spoofing; MAC filtering.
    4. Denial of service attacks; use a firewall between networks.

    For questions 62–65, please refer to a stateful inspection firewall running the rulebase shown here. The source ports have been omitted from the figure, but you may assume that they are specified correctly for the purposes of answering questions 62–64.

Rule	Action	Source IP	Source Port	Destination IP	Destination Port
1	ALLOW	ANY	_____	10.1.0.50	80
2	DENY	15.246.10.1	_____	10.1.0.50	80
3	ALLOW	ANY	_____	10.1.0.26	25
4	ALOW	ANY	_____	10.1.0.26	465

62. Which one of the following rules is not shown in the rulebase but will be enforced by the firewall?
    1. Stealth
    2. Implicit deny
    3. Connection proxy
    4. Egress filter
63. What type of server is running at IP address 10.1.0.26?
    1. Email
    2. Web
    3. FTP
    4. Database
64. The system at 15.246.10.1 attempts HTTP and HTTPS connections to the web server running at 10.1.0.50. Which one of the following statements is true about that connection?
    1. Both connections will be allowed.
    2. Both connections will be blocked.
    3. The HTTP connection will be allowed, and the HTTPS connection will be blocked.
    4. The HTTP connection will be blocked, and the HTTPS connection will be allowed.
65. What value should be used to fill in the source port for rule #3?
    1. 25
    2. 465
    3. 80
    4. Any
66. Data streams occur at what three layers of the OSI model?
    1. Application, Presentation, and Session
    2. Presentation, Session, and Transport
    3. Physical, Data Link, and Network
    4. Data Link, Network, and Transport

67. Chris needs to design a firewall architecture that can support a DMZ, a database, and a private internal network in a secure manner that separates each function. What type of design should he use, and how many firewalls does he need?
    1. A four-tier firewall design with two firewalls
    2. A two-tier firewall design with three firewalls
    3. A three-tier firewall design with at least one firewall
    4. A single-tier firewall design with three firewalls
68. Lauren's networking team has been asked to identify a technology that will allow them to dynamically change the organization's network by treating the network like code. What type of architecture should she recommend?
    1. A network that follows the 5-4-3 rule
    2. A converged network
    3. A software-defined network
    4. A hypervisor-based network
69. Cable modems, ISDN, and DSL are all examples of what type of technology?
    1. Baseband
    2. Broadband
    3. Digital
    4. Broadcast
70. What type of firewall design is shown in the following image?



    1. Single tier
    2. Two tier
    3. Three tier
    4. Next generation
71. During a review of her organization's network, Angela discovered that it was suffering from broadcast storms and that contractors, guests, and organizational administrative staff were on the same network segment. What design change should Angela recommend?
    1. Require encryption for all users.
    2. Install a firewall at the network border.
    3. Enable spanning tree loop detection.
    4. Segment the network based on functional requirements.
72. ICMP, RIP, and network address translation all occur at what layer of the OSI model?
    1. Layer 1
    2. Layer 2
    3. Layer 3
    4. Layer 4

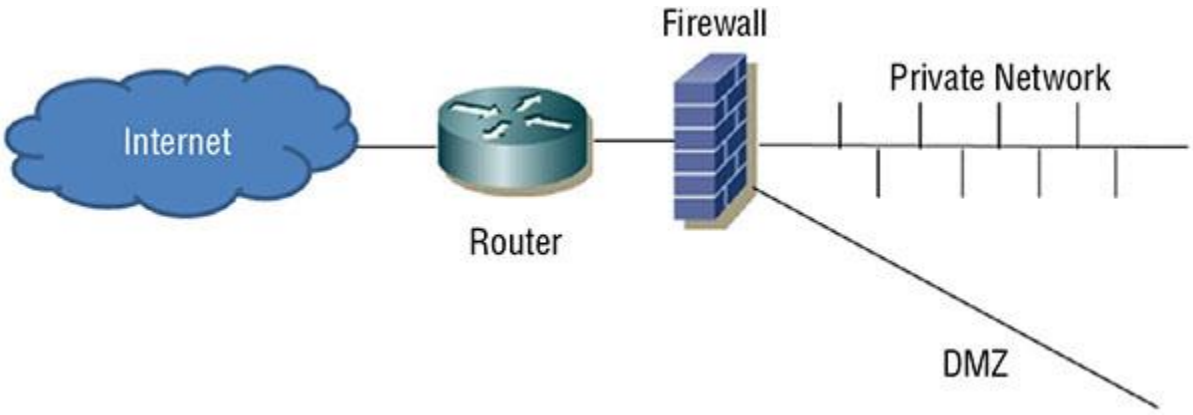
For questions 73–75, please refer to the following scenario:

Ben is an information security professional at an organization that is replacing its physical servers with virtual machines. As the organization builds its virtual environment, it is decreasing the number of physical servers it uses while purchasing more powerful servers to act as the virtualization platforms.

73. The IDS Ben is responsible for is used to monitor communications in the data center using a mirrored port on the data center switch. What traffic will Ben see once the majority of servers in the data center have been virtualized?
    1. The same traffic he currently sees
    2. All inter-VM traffic
    3. Only traffic sent outside the VM environment
    4. All inter-hypervisor traffic
74. The VM administrators recommend enabling cut and paste between virtual machines. What security concern should Ben raise about this practice?
    1. It can cause a denial of service condition.
    2. It can serve as a covert channel.
    3. It can allow viruses to spread.
    4. It can bypass authentication controls.
75. Ben is concerned about exploits that allow VM escape. What option should Ben suggest to help limit the impact of VM escape exploits?
    1. Separate virtual machines onto separate physical hardware based on task or data types.
    2. Use VM escape detection tools on the underlying hypervisor.
    3. Restore machines to their original snapshots on a regular basis.
    4. Use a utility like Tripwire to look for changes in the virtual machines.
76. WPA2's Counter Mode Cipher Block Chaining Message Authentication Mode Protocol (CCMP) is based on which common encryption scheme?
    1. DES
    2. 3DES
    3. AES
    4. TLS
77. When a host on an Ethernet network detects a collision and transmits a jam signal, what happens next?
    1. The host that transmitted the jam signal is allowed to retransmit while all other hosts pause until that transmission is received successfully.
    2. All hosts stop transmitting, and each host waits a random period of time before attempting to transmit again.
    3. All hosts stop transmitting, and each host waits a period of time based on how recently it successfully transmitted.
    4. Hosts wait for the token to be passed and then resume transmitting data as they pass the token.
78. What is the speed of a T3 line?
    1. 128 kbps
    2. 1.544 Mbps

3. 44.736 Mbps
4. 155 Mbps

79. What type of firewall design does the following image show?



1. A single-tier firewall
2. A two-tier firewall
3. A three-tier firewall
4. A fully protected DMZ firewall

80. What challenge is most common for endpoint security system deployments?
1. Compromises
2. The volume of data
3. Monitoring encrypted traffic on the network
4. Handling non-TCP protocols

81. What type of address is 127.0.0.1?
1. A public IP address
2. An RFC 1918 address
3. An APIPA address
4. A loopback address

82. Susan is writing a best practices statement for her organizational users who need to use Bluetooth. She knows that there are many potential security issues with Bluetooth and wants to provide the best advice she can. Which of the following sets of guidance should Susan include?
1. Use Bluetooth's built-in strong encryption, change the default PIN on your device, turn off discovery mode, and turn off Bluetooth when it's not in active use.
2. Use Bluetooth only for those activities that are not confidential, change the default PIN on your device, turn off discovery mode, and turn off Bluetooth when it's not in active use.
3. Use Bluetooth's built-in strong encryption, use extended (8 digit or longer) Bluetooth PINs, turn off discovery mode, and turn off Bluetooth when it's not in active use.
4. Use Bluetooth only for those activities that are not confidential, use extended (8 digit or longer) Bluetooth PINs, turn off discovery mode, and turn off Bluetooth when it's not in active use.

83. What type of networking device is most commonly used to assign endpoint systems to VLANs?
    1. Firewall
    2. Router
    3. Switch
    4. Hub
84. Steve has been tasked with implementing a network storage protocol over an IP network. What storage-centric converged protocol is he likely to use in his implementation?
    1. MPLS
    2. FCoE
    3. SDN
    4. VoIP
85. What type of network device modulates between an analog carrier signal and digital information for computer communications?
    1. A bridge
    2. A router
    3. A brouter
    4. A modem
86. Place the layers of the OSI model shown here in the appropriate order, from layer 1 to layer 7.
    1. Application
    2. Data Link
    3. Network
    4. Physical
    5. Presentation
    6. Session
    7. Transport
87. A denial of service (DoS) attack that sends fragmented TCP packets is known as what kind of attack?
    1. Christmas tree
    2. Teardrop
    3. Stack killer
    4. Frag grenade
88. Phillip maintains a modem bank in support of several legacy services used by his organization. Which one of the following protocols is most appropriate for this purpose?
    1. SLIP
    2. SLAP
    3. PPTP
    4. PPP
89. One of the findings that Jim made when performing a security audit was the use of non-IP protocols in a private network. What issue should Jim point out that may result from the use of these non-IP protocols?
    1. They are outdated and cannot be used on modern PCs.
    2. They may not be able to be filtered by firewall devices.
    3. They may allow Christmas tree attacks.
    4. IPX extends on the IP protocol and may not be supported by all TCP stacks.

90. Angela needs to choose between EAP, PEAP, and LEAP for secure authentication. Which authentication protocol should she choose and why?
    1. EAP, because it provides strong encryption by default
    2. LEAP, because it provides frequent reauthentication and changing of WEP keys
    3. PEAP, because it provides encryption and doesn't suffer from the same vulnerabilities that LEAP does
    4. None of these options can provide secure authentication, and an alternate solution should be chosen.
91. Lauren has been asked to replace her organization's PPTP implementation with an L2TP implementation for security reasons. What is the primary security reason that L2TP would replace PPTP?
    1. L2TP can use IPsec.
    2. L2TP creates a point-to-point tunnel, avoiding multipoint issues.
    3. PPTP doesn't support EAP.
    4. PPTP doesn't properly encapsulate PPP packets.
92. Jim is building a research computing system that benefits from being part of a full mesh topology between systems. In a five-node full mesh topology design, how many connections will an individual node have?
    1. Two
    2. Three
    3. Four
    4. Five
93. What topology correctly describes Ethernet?
    1. A ring
    2. A star
    3. A mesh
    4. A bus
94. What type of attack is most likely to occur after a successful ARP spoofing attempt?
    1. A DoS attack
    2. A Trojan
    3. A replay attack
    4. A man-in-the-middle attack
95. What speed is Category 3 UTP cable rated for?
    1. 5 Mbps
    2. 10 Mbps
    3. 100 Mbps
    4. 1000 Mbps
96. What issue occurs when data transmitted over one set of wires is picked up by another set of wires?
    1. Magnetic interference
    2. Crosstalk
    3. Transmission absorption
    4. Amplitude modulation
97. What two key issues with the implementation of RC4 make Wired Equivalent Privacy (WEP) even weaker than it might otherwise be?
    1. Its use of a static common key and client-set encryption algorithms

2. Its use of a static common key and a limited number of initialization vectors
3. Its use of weak asymmetric keys and a limited number of initialization vectors
4. Its use of a weak asymmetric key and client-set encryption algorithms

98. Chris is setting up a hotel network and needs to ensure that systems in each room or suite can connect to each other, but systems in other suites or rooms cannot. At the same time, he needs to ensure that all systems in the hotel can reach the internet. What solution should he recommend as the most effective business solution?
    1. Per-room VPNs
    2. VLANs
    3. Port security
    4. Firewalls
99. During a forensic investigation, Charles is able to determine the Media Access Control address of a system that was connected to a compromised network. Charles knows that MAC addresses are tied back to a manufacturer or vendor and are part of the fingerprint of the system. To which OSI layer does a MAC address belong?
    1. The Application layer
    2. The Session layer
    3. The Physical layer
    4. The Data Link layer
100. Ben knows that his organization wants to be able to validate the identity of other organizations based on their domain name when receiving and sending email. What tool should Ben recommend?
    1. PEM
    2. S/MIME
    3. DKIM
    4. MOSS

Chapter 4: Communication and Network Security (Domain 4)

1. A. Frame Relay supports multiple private virtual circuits (PVCs), unlike X.25. It is a packet-switching technology that provides a Committed Information Rate (CIR), which is a minimum bandwidth guarantee provided by the service provider to customers. Finally, Frame Relay requires a DTE/DCE at each connection point, with the DTE providing access to the Frame Relay network, and a provider-supplied DCE, which transmits the data over the network.
2. B. LEAP, the Lightweight Extensible Authentication Protocol, is a Cisco proprietary protocol designed to handle problems with TKIP. Unfortunately, LEAP has significant security issues as well and should not be used. Any modern hardware should support WPA2 and technologies like PEAP or EAP-TLS. Using WEP, the predecessor to WPA and WPA2, would be a major step back in security for any network.
3. C. Ben is using ad hoc mode, which directly connects two clients. It can be easy to confuse this with stand-alone mode, which connects clients using a wireless access point but not to wired resources like a central network. Infrastructure mode connects endpoints to a central network, not directly to each other. Finally, wired extension mode uses a wireless access point to link wireless clients to a wired network.
4. C. A collision domain is the set of systems that could cause a collision if they transmitted at the same time. Systems outside a collision domain cannot cause a collision if they send at the same time. This is important, as the number of systems in a collision domain increases the likelihood

of network congestion due to an increase in collisions. A broadcast domain is the set of systems that can receive a broadcast from each other. A subnet is a logical division of a network, while a supernet is made up of two or more networks.

5. D. The RST flag is used to reset or disconnect a session. It can be resumed by restarting the connection via a new three-way handshake.
6. C. He should choose 802.11n, which supports 200+ Mbps in the 2.4 GHz or the 5 GHz frequency range. 802.11a and 802.11ac are both 5 GHz only, while 802.11g is only capable of 54 Mbps.
7. The TCP ports match with the protocols as follows:
    1. TCP port 23: D. Telnet.
    2. TCP port 25: A. SMTP.
    3. TCP port 143: C. IMAP.
    4. TCP port 515: B. LPD.

    These common ports are important to know, although some of the protocols are becoming less common. SMTP is the Simple Mail Transfer Protocol, IMAP is the Internet Message Access Protocol, and LPD is the Line Printer Daemon protocol used to send print jobs to printers.

8. A. The File Transfer Protocol (FTP) operates on TCP ports 20 and 21. UDP port 69 is used for the Trivial File Transfer Protocol, or TFTP, while UDP port 21 is not used for any common file transfer protocol.
9. B. Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Orthogonal Frequency-Division Multiplexing (OFDM) all use spread spectrum techniques to transmit on more than one frequency at the same time. Neither FHSS nor DHSS uses orthogonal modulation, while multiplexing describes combining multiple signals over a shared medium of any sort. WiFi may receive interference from FHSS systems but doesn't use it.
10. B. The Challenge-Handshake Authentication Protocol, or CHAP, is used by PPP servers to authenticate remote clients. It encrypts both the username and password and performs periodic reauthentication while connected using techniques to prevent replay attacks. LEAP provides reauthentication but was designed for WEP, while PAP sends passwords unencrypted. EAP is extensible and was used for PPP connections, but it doesn't directly address the listed items.
11. B. The Remote Access Dial In User Service (RADIUS) protocol was originally designed to support dial-up modem connections but is still commonly used for VPN-based authentication. HTTPS is not an authentication protocol. ESP and AH are IPsec protocols but do not provide authentication services for other systems.
12. A. A ring connects all systems like points on a circle. A ring topology was used with Token Ring networks, and a token was passed between systems around the ring to allow each system to communicate. More modern networks may be described as a ring but are only physically a ring and not logically using a ring topology.
13. B. The firewall in the diagram has two protected zones behind it, making it a two-tier firewall design.
14. D. Remote PCs that connect to a protected network need to comply with security settings and standards that match those required for the internal network. The VPN concentrator logically places remote users in the protected zone behind the firewall, but that means that user workstations (and users) must be trusted in the same way that local workstations are.
15. C. An intrusion protection system can scan traffic and stop both known and unknown attacks. A web application firewall, or WAF, is also a suitable technology, but placing it at location C would only protect from attacks via the organization's VPN, which should only be used by trusted

users. A firewall typically won't have the ability to identify and stop cross-site scripting attacks, and IDS systems only monitor and don't stop attacks.

16. D. Distance-vector protocols use metrics including the direction and distance in hops to remote networks to make decisions. A link-state routing protocol considers the shortest distance to a remote network. Destination metric and link-distance protocols don't exist.
17. B. Disabling SSID broadcast can help prevent unauthorized personnel from attempting to connect to the network. Since the SSID is still active, it can be discovered by using a wireless sniffer. Encryption keys are not related to SSID broadcast, beacon frames are used to broadcast the SSID, and it is possible to have multiple networks with the same SSID.
18. B. A proxy is a form of gateway that provide clients with a filtering, caching, or other service that protects their information from remote systems. A router connects networks, while a firewall uses rules to limit traffic permitted through it. A gateway translates between protocols.
19. B. DNS poisoning occurs when an attacker changes the domain name to IP address mappings of a system to redirect traffic to alternate systems. DNS spoofing occurs when an attacker sends false replies to a requesting system, beating valid replies from the actual DNS server. ARP spoofing provides a false hardware address in response to queries about an IP, and Cain & Abel is a powerful Windows hacking tool, but a Cain attack is not a specific type of attack.
20. B. Screen scrapers copy the actual screen displayed and display it at a remote location. RDP provides terminal sessions without doing screen scraping, remote node operation is the same as dial-up access, and remote control is a means of controlling a remote system (screen scraping is a specialized subset of remote control).
21. A. S/MIME supports both signed messages and a secure envelope method. While the functionality of S/MIME can be replicated with other tools, the secure envelope is an S/MIME-specific concept. MOSS, or MIME Object Security Services, and PEM can also both provide authentication, confidentiality, integrity, and nonrepudiation, while DKIM, or Domain Keys Identified Mail, is a domain validation tool.
22. A. Multilayer protocols like DNP3 allow SCADA and other systems to use TCP/IP-based networks to communicate. Many SCADA devices were never designed to be exposed to a network, and adding them to a potentially insecure network can create significant risks. TLS or other encryption can be used on TCP packets, meaning that even serial data can be protected. Serial data can be carried via TCP packets because TCP packets don't care about their content; it is simply another payload. Finally, TCP/IP does not have a specific throughput as designed, so issues with throughput are device-level issues.
23. C. WEP has a very weak security model that relies on a single, predefined, shared static key. This means that modern attacks can break WEP encryption in less than a minute.
24. B. A denial of service attack is an attack that causes a service to fail or to be unavailable. Exhausting a system's resources to cause a service to fail is a common form of denial of service attack. A worm is a self-replicating form of malware that propagates via a network, a virus is a type of malware that can copy itself to spread, and a smurf attack is a distributed denial of service (DDoS) that spoofs a victim's IP address to systems using an IP broadcast, resulting in traffic from all of those systems to the target.
25. C. 802.11n can operate at speeds over 200 Mbps, and it can operate on both the 2.4 and 5 GHz frequency range. 802.11g operates at 54 Mbps using the 2.4 GHz frequency range, and 802.11ac is capable of 1 Gbps using the 5 GHz range. 802.11a and b are both outdated and are unlikely to be encountered in modern network installations.
26. B. ARP and RARP operate at the Data Link layer, the second layer of the OSI model. Both protocols deal with physical hardware addresses, which are used above the Physical layer (layer 1) and below the Network layer (layer 3), thus falling at the Data Link layer.

27. D. iSCSI is a converged protocol that allows location-independent file services over traditional network technologies. It costs less than traditional Fibre Channel. VoIP is Voice over IP, SDN is software-defined networking, and MPLS is Multiprotocol Label Switching, a technology that uses path labels instead of network addresses.
28. A. A repeater or concentrator will amplify the signal, ensuring that the 100-meter distance limitation of 1000BaseT is not an issue. A gateway would be useful if network protocols were changing, while Cat7 cable is appropriate for a 10Gbps network at much shorter distances. STP cable is limited to 155 Mbps and 100 meters, which would leave Chris with network problems.
29. B. The use of TCP port 80 indicates that the messaging service is using the HTTP protocol. Slack is a messaging service that runs over HTTPS, which uses port 443. SMTP is an email protocol that uses port 25.
30. C. HTTP traffic is typically sent via TCP 80. Unencrypted HTTP traffic can be easily captured at any point between A and B, meaning that the messaging solution chosen does not provide confidentiality for the organization's corporate communications.
31. B. If a business need requires messaging, using a local messaging server is the best option. This prevents traffic from traveling to a third-party server and can offer additional benefits such as logging, archiving, and control of security options like the use of encryption.
32. B. Multilayer protocols create three primary concerns for security practitioners: They can conceal covert channels (and thus covert channels are allowed), filters can be bypassed by traffic concealed in layered protocols, and the logical boundaries put in place by network segments can be bypassed under some circumstances. Multilayer protocols allow encryption at various layers and support a range of protocols at higher layers.
33. C. A bus can be linear or tree-shaped and connects each system to trunk or backbone cable. Ethernet networks operate on a bus topology.
34. B. When a workstation or other device is connected simultaneously to both a secure and a nonsecure network like the Internet, it may act as a bridge, bypassing the security protections located at the edge of a corporate network. It is unlikely that traffic will be routed improperly leading to the exposure of sensitive data, as traffic headed to internal systems and networks is unlikely to be routed to the external network. Reflected DDoS attacks are used to hide identities rather than to connect through to an internal network, and security administrators of managed systems should be able to determine both the local and wireless IP addresses his system uses.
35. A. Wardriving and warwalking are both processes used to locate wireless networks, but are not typically as detailed and thorough as a site survey, and *design map* is a made-up term.
36. C. The DARPA TCP/IP model was used to create the OSI model, and the designers of the OSI model made sure to map the OSI model layers to it. The Application layer of the TCP model maps to the Application, Presentation, and Session layers, while the TCP and OSI models both have a distinct Transport layer.
37. B. ARP cache poisoning occurs when false ARP data is inserted into a system's ARP cache, allowing the attacker to modify its behavior. *RARP flooding*, *denial of ARP attacks*, and *ARP buffer blasting* are all made-up terms.
38. C. The process of using a fake MAC (Media Access Control) address is called spoofing, and spoofing a MAC address already in use on the network can lead to an address collision, preventing traffic from reaching one or both systems. Tokens are used in token ring networks, which are outdated, and EUI refers to an Extended Unique Identifier, another term for MAC address, but token loss is still not the key issue. Broadcast domains refers to the set of machines a host can send traffic to via a broadcast message.
39. D. Direct Inward System Access uses access codes assigned to users to add a control layer for external access and control of the PBX. If the codes are compromised, attackers can make calls

through the PBX or even control it. Not updating a PBX can lead to a range of issues, but this question is looking for a DISA issue. Allowing only local calls and using unpublished numbers are both security controls and might help keep the PBX more secure.

40. D. Application-specific protocols are handled at layer 7, the Application layer of the OSI model.
41. D. Ping uses ICMP, the Internet Control Message Protocol, to determine whether a system responds and how many hops there are between the originating system and the remote system. Lauren simply needs to filter out ICMP to not see her pings.
42. D. 802.1x provides port-based authentication and can be used with technologies like EAP, the Extensible Authentication Protocol. 802.11a is a wireless standard, 802.3 is the standard for Ethernet, and 802.15.1 was the original Bluetooth IEEE standard.
43. D. 1000BaseT is capable of a 100-meter run according to its specifications. For longer distances, a fiber-optic cable is typically used in modern networks.
44. C. PRI, or Primary Rate Interface, can use between 2 and 23 64 Kbps channels, with a maximum potential bandwidth of 1.544 Mbps. Actual speeds will be lower due to the D channel, which can't be used for actual data transmission, but PRI beats BRI's two B channels paired with a D channel for 144 Kbps of bandwidth.
45. C. SPIT stands for Spam over Internet Telephony and targets VoIP systems.
46. D. Bluesnarfing targets the data or information on Bluetooth-enabled devices. Bluejacking occurs when attackers send unsolicited messages via Bluetooth.
47. C. Layer 6, the Presentation layer, transforms data from the Application layer into formats that other systems can understand by formatting and standardizing the data. That means that standards like JPEG, ASCII, and MIDI are used at the Presentation layer for data. TCP, UDP, and TLS are used at the Transport layer; NFS, SQL, and RPC operate at the Session layer; and HTTP, FTP, and SMTP are Application layer protocols.
48. D. Fully connected mesh networks provide each system with a direct physical link to every other system in the mesh. This is very expensive but can provide performance advantages for specific types of computational work.
49. C. PPTP, L2F, L2TP, and IPsec are the most common VPN protocols. TLS is also used for an increasingly large percentage of VPN connections and may appear at some point in the CISSP exam. PPP is a dial-up protocol, LTP is not a protocol, and SPAP is the Shiva Password Authentication Protocol sometimes used with PPTP.
50. C. FDDI, or Fiber Distributed Data Interface, is a token-passing network that uses a pair of rings with traffic flowing in opposite directions. It can bypass broken segments by dropping the broken point and using the second, unbroken ring to continue to function. Token Ring also uses tokens, but it does not use a dual loop. SONET is a protocol for sending multiple optical streams over fiber, and a ring topology is a design, not a technology.
51. C. The Physical layer includes electrical specifications, protocols, and standards that allow control of throughput, handling line noise, and a variety of other electrical interface and signaling requirements. The OSI layer doesn't have a Device layer. The Transport layer connects the Network and Session layers, and the Data Link layer packages packets from the network layer for transmission and receipt by devices operating on the Physical layer.
52. A. WPA2, the replacement for WPA, does not suffer from the security issues that WEP, the original wireless security protocol, and WPA, its successor, both suffer from. AES is used in WPA2 but is not specifically a wireless security standard.
53. A. User awareness is one of the most important tools when dealing with attachments. Attachments are often used as a vector for malware, and aware users can help prevent successful attacks by not opening the attachments. Antimalware tools, including antivirus software, can help detect known threats before users even see the attachments. Encryption,

including tools like S/MIME, won't help prevent attachment-based security problems, and removing ZIP file attachments will only stop malware that is sent via those ZIP files.

54. A. The Transport layer provides logical connections between devices, including end-to-end transport services to ensure that data is delivered. Transport layer protocols include TCP, UDP, SSL, and TLS.
55. B. Machine Access Control (MAC) addresses are the hardware address the machine uses for layer 2 communications. The MAC addresses include an organizationally unique identifier (OUI), which identifies the manufacturer. MAC addresses can be changed, so this is not a guarantee of accuracy, but under normal circumstances you can tell what manufacturer made the device by using the MAC address.
56. D. PEAP provides encryption for EAP methods and can provide authentication. It does not implement CCMP, which was included in the WPA2 standard. LEAP is dangerously insecure and should not be used due to attack tools that have been available since the early 2000s.
57. C. Double NATing isn't possible with the same IP range; the same IP addresses cannot appear inside and outside a NAT router. RFC 1918 addresses are reserved, but only so they are not used and routable on the Internet, and changing to PAT would not fix the issue.
58. B. A Class B network holds 2^16 systems, and its default network mask is 255.255.0.0.
59. C. Traditional private branch exchange (PBX) systems are vulnerable to eavesdropping because voice communications are carried directly over copper wires. Since standard telephones don't provide encryption (and you're unlikely to add encrypted phones unless you're the NSA), physically securing access to the lines and central connection points is the best strategy available.
60. A. Most cordless phones don't use encryption, and even modern phones that use DECT (which does provide encryption) have already been cracked. This means that a determined attacker can almost always eavesdrop on cordless phones, and makes them a security risk if they're used for confidential communication.
61. A. VLAN hopping between the voice and computer VLANs can be accomplished when devices share the same switch infrastructure. Using physically separate switches can prevent this attack. Encryption won't help with VLAN hopping because it relies on header data that the switch needs to read (and this is unencrypted), while Caller ID spoofing is an inherent problem with VoIP systems. A denial of service is always a possibility, but it isn't specifically a VoIP issue and a firewall may not stop the problem if it's on a port that must be allowed through.
62. B. All stateful inspection firewalls enforce an implicit deny rule as the final rule of the rulebase. It is designed to drop all inbound traffic that was not accepted by an earlier rule. Stealth rules hide the firewall from external networks, but they are not included by default. This firewall does not contain any egress filtering rules, and egress filtering is not enforced by default. Connection proxying is an optional feature of stateful inspection firewalls and would not be enforced without a rule explicitly implementing it.
63. A. SMTP uses ports 25 and 465. The presence of an inbound rule allowing SMTP traffic indicates that this is an email server.
64. C. The HTTP connection will be allowed, despite the presence of rule #2, because it matches rule #1. The HTTPS connection will be blocked because there is no rule allowing HTTPS connections to this server.
65. D. The firewall should be configured to accept inbound connections from any port selected by the source system. The vast majority of inbound firewall rules allow access from any source port.
66. A. Data streams are associated with the Application, Presentation, and Session layers. Once they reach the Transport layer, they become segments (TCP) or datagrams (UDP). From there, they

are converted to packets at the Network layer, frames at the Data Link layer, and bits at the Physical layer.

67. C. A three-tier design separates three distinct protected zones and can be accomplished with a single firewall that has multiple interfaces. Single- and two-tier designs don't support the number of protected networks needed in this scenario, while a four-tier design would provide a tier that isn't needed.
68. C. Software-defined networking provides a network architecture that can be defined and configured as code or software. This will allow Lauren's team to quickly change the network based on organizational requirements. The 5-4-3 rule is an old design rule for networks that relied on repeaters or hubs. A converged network carries multiple types of traffic like voice, video, and data. A hypervisor-based network may be software defined, but it could also use traditional network devices running as virtual machines.
69. B. ISDN, cable modems, DSL, and T1 and T3 lines are all examples of broadband technology that can support multiple simultaneous signals. They are analog, not digital, and are not broadcast technologies.
70. A. A single-tier firewall deployment is very simple and does not offer useful design options like a DMZ or separate transaction subnets.
71. D. Network segmentation can reduce issues with performance as well as diminish the chance of broadcast storms by limiting the number of systems in a segment. This decreases broadcast traffic visible to each system and can reduce congestion. Segmentation can also help provide security by separating functional groups who don't need to be able to access each other's systems. Installing a firewall at the border would only help with inbound and outbound traffic, not cross-network traffic. Spanning tree loop prevention helps prevent loops in Ethernet networks (for example, when you plug a switch into a switch via two ports on each), but it won't solve broadcast storms that aren't caused by a loop or security issues. Encryption might help prevent some problems between functional groups, but it won't stop them from scanning other systems, and it definitely won't stop a broadcast storm!
72. C. ICMP, RIP, and network address translation all occur at layer 3, the Network layer.
73. C. One of the visibility risks of virtualization is that communication between servers and systems using virtual interfaces can occur "inside" the virtual environment. This means that visibility into traffic in the virtualization environment has to be purpose-built as part of its design. Option D is correct but incomplete because inter-hypervisor traffic isn't the only traffic the IDS will see.
74. B. Cut and paste between virtual machines can bypass normal network-based data loss prevention tools and monitoring tools like an IDS or IPS. Thus, it can act as a covert channel, allowing the transport of data between security zones. So far, cut and paste has not been used as a method for malware spread in virtual environments and has not been associated with denial of service attacks. Cut and paste requires users to be logged in and does not bypass authentication requirements.
75. A. While virtual machine escape has only been demonstrated in laboratory environments, the threat is best dealt with by limiting what access to the underlying hypervisor can prove to a successful tracker. Segmenting by data types or access levels can limit the potential impact of a hypervisor compromise. If attackers can access the underlying system, restricting the breach to only similar data types or systems will limit the impact. Escape detection tools are not available on the market, restoring machines to their original snapshots will not prevent the exploit from occurring again, and Tripwire detects file changes and is unlikely to catch exploits that escape the virtual machines themselves.

76. C. WPA2's CCMP encryption scheme is based on AES. As of the writing of this book, there have not been any practical real-world attacks against WPA2. DES has been successfully broken, and neither 3DES nor TLS is used for WPA2.
77. B. Ethernet networks use Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) technology. When a collision is detected and a jam signal is sent, hosts wait a random period of time before attempting retransmission.
78. C. A T3 (DS-3) line is capable of 44.736 Mbps. This is often referred to as 45 Mbps. A T1 is 1.544 Mbps, ATM is 155 Mbps, and ISDN is often 64 or 128 Kbps.
79. B. A two-tier firewall uses a firewall with multiple interfaces or multiple firewalls in series. This image shows a firewall with two protected interfaces, with one used for a DMZ and one used for a protected network. This allows traffic to be filtered between each of the zones (Internet, DMZ, and private network).
80. B. Endpoint security solutions face challenges due to the sheer volume of data that they can create. When each workstation is generating data about events, this can be a massive amount of data. Endpoint security solutions should reduce the number of compromises when properly implemented, and they can also help by monitoring traffic after it is decrypted on the local host. Finally, non-TCP protocols are relatively uncommon on modern networks, making this a relatively rare concern for endpoint security system implementations.
81. D. The IP address 127.0.0.1 is a loopback address and will resolve to the local machine. Public addresses are non-RFC 1918, non-reserved addresses. RFC 1918 addresses are reserved and include ranges like 10.x.x.x. An APIPA address is a self-assigned address used when a DHCP server cannot be found.
82. B. Since Bluetooth doesn't provide strong encryption, it should only be used for activities that are not confidential. Bluetooth PINs are four-digit codes that often default to 0000. Turning it off and ensuring that your devices are not in discovery mode can help prevent Bluetooth attacks.
83. C. The assignment of endpoint systems to VLANs is normally performed by a network switch.
84. B. Fibre Channel over Ethernet allows Fibre Channel communications over Ethernet networks, allowing existing high-speed networks to be used to carry storage traffic. This avoids the cost of a custom cable plant for a Fibre Channel implementation. MPLS, or Multiprotocol Label Switching, is used for high performance networking; VoIP is Voice over IP; and SDN is software-defined networking.
85. D. A modem (MOdulator/DEModulator) modulates between an analog carrier like a phone line and digital communications like those used between computers. While modems aren't in heavy use in most areas, they are still in place for system control and remote system contact and in areas where phone lines are available but other forms of communication are too expensive or not available.
86. The OSI layers in order from layer 1 to layer 7 are:

- D. Physical
- B. Data Link
- C. Network
- G. Transport
- F. Session
- E. Presentation
- A. Application

87. B. A teardrop attack uses fragmented packets to target a flaw in how the TCP stack on a system handles fragment reassembly. If the attack is successful, the TCP stack fails, resulting in a denial

of service. Christmas tree attacks set all of the possible TCP flags on a packet, thus "lighting it up like a Christmas tree." *Stack killer* and *frag grenade attacks* are made-up answers.

88. D. The Point-to-Point Protocol (PPP) is used for dial-up connections for modems, IDSN, Frame Relay, and other technologies. It replaced SLIP in almost all cases. PPTP is the Point-to-Point Tunneling Protocol used for VPNs, and SLAP is not a protocol at all!
89. B. While non-IP protocols like IPX/SPX, NetBEUI, and AppleTalk are rare in modern networks, they can present a challenge because many firewalls are not capable of filtering them. This can create risks when they are necessary for an application or system's function because they may have to be passed without any inspection. Christmas tree attacks set all of the possible flags on a TCP packet (and are thus related to an IP protocol), IPX is not an IP-based protocol, and while these protocols are outdated, there are ways to make even modern PCs understand them.
90. C. Of the three answers, PEAP is the best solution. It encapsulates EAP in a TLS tunnel, providing strong encryption. LEAP is a Cisco proprietary protocol that was originally designed to help deal with problems in WEP. LEAP's protections have been defeated, making it a poor choice.
91. A. L2TP can use IPsec to provide encryption of traffic, ensuring confidentiality of the traffic carried via an L2TP VPN. PPTP sends the initial packets of a session in plaintext, potentially including usernames and hashed passwords. PPTP does support EAP and was designed to encapsulate PPP packets. All VPNs are point to point, and multipoint issues are not a VPN problem.
92. C. A full mesh topology directly connects each machine to every other machine on the network. For five systems, this means four connections per system.
93. D. Ethernet uses a bus topology. While devices may be physically connected to a switch in a physical topology that looks like a star, systems using Ethernet can all transmit on the bus simultaneously, possibly leading to collisions.
94. D. ARP spoofing is often done to replace a target's cache entry for a destination IP, allowing the attacker to conduct a man-in-the-middle attack. A denial of service attack would be aimed at disrupting services rather than spoofing an ARP response, a replay attack will involve existing sessions, and a Trojan is malware that is disguised in a way that makes it look harmless.
95. B. Category 3 UTP cable is primarily used for phone cables and was also used for early Ethernet networks where it provided 10 Mbps of throughput. Cat 5 cable provides 100 Mbps (and 1000 Mbps if it is Cat 5e). Cat 6 cable can also provide 1000 Mbps.
96. B. Crosstalk occurs when data transmitted on one set of wires is picked up on another set of wires. Interference like this is electromagnetic rather than simply magnetic, *transmission absorption* is a made-up term, and amplitude modulation is how AM radio works.
97. B. WEP's implementation of RC4 is weakened by its use of a static common key and a limited number of initialization vectors. It does not use asymmetric encryption, and clients do not select encryption algorithms.
98. B. VLANs can be used to logically separate groups of network ports while still providing access to an uplink. Per-room VPNs would create significant overhead for support as well as create additional expenses. Port security is used to limit what systems can connect to ports, but it doesn't provide network security between systems. Finally, while firewalls might work, they would add additional expense and complexity without adding any benefits over a VLAN solution.
99. D. MAC addresses and their organizationally unique identifiers are used at the Data Link layer to identify systems on a network. The Application and Session layers don't care about physical addresses, while the Physical layer involves electrical connectivity and handling physical interfaces rather than addressing.

100. C. Domain Keys Identified Mail, or DKIM, is designed to allow assertions of domain identity to validate email. S/MIME, PEM, and MOSS are all solutions that can provide authentication, integrity, nonrepudiation, and confidentiality, depending on how they are used.