Chapter 3 Solutions

Review Questions

1. Which of the following is a reliable communications protocol?
a. UDP
b. TCP
c. IP
d. ICMP

2. Which of the following is used by the TFTP protocol?
a. UDP
b. TCP
c. ICMP
d. Telnet

3. Which of the following is a layer in the TCP/IP protocol stack? (Choose all that apply.)
a. Application
b. Presentation
c. Physical
d. Data Link
e. Internetwork

4. Which of the following is a TCP/IP Application layer protocol? (Choose all that apply.)
a. DNS
b. FTP
c. UDP
d. IP
e. ICMP

5. Which of the following is a TCP/IP Internetwork layer protocol? (Choose all that apply.)
a. ICMP
b. FTP
c. DNS
d. ARP
e. IP

6. Which of the following is a TCP/IP Transport layer protocol? (Choose all that apply.)
a. ARP
b. RARP
c. IP
d. UDP
e. TCP

7. If your Class C address has a three-bit subnet mask, which of the following would be a subnetwork identifier?
a. 203.16.34.33
b. 203.16.34.135
c. 203.16.34.32
d. 203.16.34.240

8. Which of the following would be a broadcast address for a Class C network?
a. 190.15.23.255
b. 190.42.25.255
c. 221.21.23.255
d. 129.21.15.255

9. Which of the following Class C IP addresses is a broadcast (assuming the subnet mask is 255.255.255.224)?

a. 219.129.32.5
b. 219.129.32.63
c. 219.129.32.97
d. 219.129.32.161

10. For a Class B broadcast, which octets will be completely binary ones?
a. 2nd
b. 2nd and 3rd
c. 1st and 2nd
d. 3rd and 4th

11. Which of the following is a Class A broadcast?
a. 11.255.255.255
b. 127.75.255.255
c. 193.255.255.255
d. 14.25.255.255

12. What is the purpose of the reserved numbers in a Class D address?
a. Unicast
b. Experimental
c. Broadcast
d. Multicast

13. What is the purpose of the reserved numbers in a Class E address?
a. Unicast
b. Broadcast
c. Multicast
d. Experimental

14. In a Class C address, which octets identify the network?
a. All of them
b. The first octet only
c. The first and second octet
d. The last octet
e. The first three octets

15. Class B addresses allow you to configure how many octets on your network for host IP addresses?
a. One
b. Two
c. Three
d. Four

16. Which of the following are valid network identifiers for Class A addresses?
a. 1-127
b. 1-126
c. 192-223
d. 224-240
e. 128-191

17. What would the value of the first octet of the subnet mask be if the CIDR notation for an address is 192.168.1.16/27?
a. 224
b. 254
c. 255
d. 265

18. What would the value of the last octet of the subnet mask be if the CIDR notation for an address is 192.168.1.16/28?
a. 192

b. 224
c. 240
d. 248
e. 252

19. Assuming that the address 165.24.3.6 uses the correct default mask, what is the host identifier?
a. 165.24
b. 24.3.6
c. 3
d. 3.6

20. How many bits (maximum) can be used from the last octet of a Class C address to subnet your network?
a. 2
b. 4
c. 6
d. 8

21. Which of the following address classes allows you to borrow a maximum of 14 bits to create a subnet mask?
a. Class A
b. Class B
c. Class C
d. None of the above

22. A subnet mask of 255.255.252.0 on a Class B network indicates that _____ bits have been borrowed from the host portion to subnet the network.
a. 2
b. 4
c. 6
d. 8
e. 10

23. Given the following CIDR address and mask, which of the following is a broadcast on its subnetwork 162.17.12.125/24?
a. 162.17.15.255
b. 162.17.12.255
c. 162.17.255.255
d. 255.255.255.255
e. None of the above

24. Given the address 190.14.20.255/20, which of the following statements is true?
a. This is a broadcast address.
b. This is a network address.
c. This is a host address.
d. This address is on network 190.14.20.0.
e. This address is on network 190.14.16.0.

25. Given the address 190.14.20.0/22, which of the following statements is true?
a. This is a broadcast address.
b. This is a network address.
c. This is a host address.
d. This address is on network 190.14.20.0.
e. This address is on network 190.14.16.0.

26. The TCP acknowledgment process is _____.
a. expectational
b. sequential
c. exceptional

d. sesquicentennial

27. Which of the following are NOT ICMP message types?
a. Echo & destination unreachable
b. Source quench & redirect
c. Relay and reroute
d. Parameter problem & information
e. Timestamp & time exceeded

28. How does CIDR conserve IP addresses?
a. By charging more for IP address assignments
b. By allocating IP network numbers on criteria other than traditional bit boundaries
c. By using traditional octet boundary subnet masks
d. By aggregating routes

29. Which of the following routing protocols support VLSM? (Choose all that apply.)
a. RIP version 1
b. IGRP
c. OSPF
d. EIGRP

30. What is the purpose of summarization?
a. To reduce the number of routing table entries
b. To prevent route flapping
c. To conserve IP addresses
d. To reduce the cost of acquiring IP addresses

Case Projects

Case Project 1
IP addresses beginning with the decimal number 10 are part of the private address ranges. These reserved numbers cannot be used on networks whose IP addresses are seen on the Internet because many people are using these same numbers and all "seen" IP addresses must be unique. Private addresses are to be used behind a firewall of some type that will hide the private IP scheme and present different and unique IP addresses to the outside networks. IP addresses beginning with the decimal number 127 can never be assigned in any circumstances because the entire 127.0.0.0 network is used for loopback testing. If you ping 127.0.0.1 (or any valid IP address on that network), a positive reply means your TCP/IP protocol stack is installed and functioning correctly. IP addresses beginning with 223 and above cannot be used because they are part of Class D and E networks which are reserved for multicasting and experimentation respectively.

Case Project 2
The purpose of sliding windows is to provide flow control at layer 4 between communicating hosts when TCP is the transport protocol in use. It allows more than one packet to be sent at once to the receiving host. In essence, the source computer lets the destination computer know how many data packets it is willing to send before it requires an acknowledgement (ACK) that the data has been received. Large data transfers require large windows; otherwise, there would be a lot of additional network traffic generated by ACKs for each communication. Smaller networks that send small amounts of data can use smaller windows. Using large windows with small data transfers can force the sending computer to wait a disproportionate time for an ACK. It may then retransmit the data, which could result in getting an ACK for both the original, and the retransmitted data. Devices can dynamically adjust their window size.

Case Project 3
TCP/IP hosts examine frame headers of packets being transmitted on the network and learn which IP addresses are associated with which MAC addresses. They put these IP to MAC

mappings in their ARP table in RAM. If a host wants to send data, it first must determine if the destination host is on the same network as it is. It does this by ANDING the IP addresses with their respective subnet masks. Next, the source puts its own IP and the destination's IP in the network layer header. At the data link layer both the source and destination MAC addresses are required. While the source computer knows its own MAC it may not know the destination's MAC. It looks in its ARP table for the correct mapping. If it is not there, the source host will send an ARP request which is a broadcast. All hosts on the local network (plus the router) will accept the broadcast at the data link layer, but only the host with the matching destination MAC address will answer with an ARP reply, which is a unicast packet. All hosts will use the ARP request information to update their ARP tables with the source IP and MAC information. Once it gets an ARP reply, the source host can send a unicast packet with the data correctly addressed to the destination. If the destination is determined not to be on the same network in the ANDING process, the source will send the packet to the default gateway. It will need an IP and MAC address for the default gateway and will ARP for the MAC address if necessary. Source hosts do not ARP for the final destination host if the destination host is determined to be on a different network. This is because broadcasts are not forwarded through a router and ARP requests are broadcasts.

Case Project 4

Sometimes companies want to use diskless workstations rather than typical PCs that have hard drives in them. Usually, security is the reason for not using hard drives. Because IP configuration information is stored on hard drives, diskless workstations cannot retain this configuration information. Since a source host must have both an IP and MAC address to send data on a TCP/IP network, the diskless workstation must have some way to obtain its IP address. A device on the network can serve as a RARP server. A RARP server maintains a table with IP to MAC address mappings. When they boot, RARP clients broadcast a RARP request in order to obtain an IP address. The RARP server sends a RARP reply back to the client with the desired information. A workstation holds this IP information in RAM and it remains there until the workstation is shut off. Diskless workstations already know their MAC address because it is physically burned into the NIC card. The DHCP protocol is based on RARP but it is more sophisticated. RARP servers rely on a table of IP to MAC mappings so the given computer will always receive the same IP address. DHCP servers have a range of IP addresses they can assign to any host so a given computer may not always receive the same IP address. Also, DHCP can assign additional configuration parameters besides IP.