Midterm 2: CST8182 Networking Fundamentals

Winter 2011

Time: 50 minutes; Total Marks available: 45 marks + 3 bonus marks
(Allocation of marks is shown beside each question)

Master Version

Instructions:

1. **NO CALCULATORS ALLOWED**
2. BEFORE answering any questions, please check that your copy of the test has all pages (as indicated in the footer at the bottom of each page). Please read all questions carefully, then answer question 1 first!
3. Be sure to **mark your name and version of this midterm** on the scantron answer sheet.
4. All answers should be circled on this test paper **and** then marked on the scantron answer sheet.
5. If you do not find an answer which is clearly the correct choice, choose the ***best*** answer.
6. If you are uncertain what a question is asking, make reasonable assumptions, write those assumptions down on this test paper, and continue answering the question.

1. What is your:

NAME? _____ Student Id? _____

(Continued on next page)

1. [0 marks] What version of the test are you writing? The version letter is located on the cover sheet.
   (a) A
   (b) B
   (c) C
   (d) D
   (e) XYZZY

2. [1 mark] Which of the following correctly gives a difference between FTP and TFTP?
   (a) FTP is secure, TFTP is **not**
   (b) TFTP uses ACKs but FTP does **not**
   (c) FTP is client-server; TFTP is peer-to-peer
   (d) FTP requires a password and account to login, TFTP does **not**
   (e) FTP operates in client-server mode; TFTP operates in server-client mode

3. [1 mark] Which of the following are connection-oriented networking protocols? Choose **all** that apply.
   (a) IP
   (b) TCP
   (c) UDP
   (d) ADC
   (e) ICMP

4. [1 mark] When does the ACK value match the SYN value for a transmitted segment?
   (a) Only for the very first segment
   (b) On **all** segments that are properly transmitted and received
   (c) On **all** segments **after** the three-way handshake
   (d) Only on the very last segment
   (e) never; at best they will differ by 1

5. [1 mark] What DOS command will continue pinging the address 192.168.0.1 forever?
   (a) ping –i 192.168.0.1
   (b) ping –t 192.168.0.1
   (c) ping –a 192.168.0.1
   (d) ping –d 192.168.0.1
   (e) ping –w 192.168.0.1

6. [1 mark] Which of the following optical fiber **connectors** provide for bidirectional data? (Choose **all** that apply.)

   (a) 

   (b) 

   (c) 

   (d) 

7. [1 mark] In which pane does Wireshark show the preamble field?
   (a) top pane only
   (b) middle pane only
   (c) bottom pane only
   (d) middle and bottom panes
   (e) none of the above

8. [1 mark] What is the decimal equivalent of the binary value `1 0101 0110` ?
   (a) 234
   (b) 342
   (c) 432
   (d) 101,010,110
   (e) I don't know because my teacher never told me the answer to that one.

9. [2 marks] Given the starting network ID 90.125.0.0/16, subnet to provide 323 usable subnets with as few extra subnets as possible. What is the number of usable hosts per subnet ?
   (a) 64
   (b) 128
   (c) 256
   (d) 512
   (e) none of the above

10. [2 marks] Given the starting network ID 70.96.0.0/12, subnet to provide 512 usable subnets with as few extra subnets as possible. What is the new mask?
   (a) /12
   (b) /20
   (c) /21
   (d) /22
   (e) none of the above

11. [2 marks] Given the network ID 66.64.0.0/11, subnet to provide 616 usable subnets with as few extra subnets as possible. What is the **actual** number of subnets created?
   (a) /20
   (b) 128
   (c) 256
   (d) 512
   (e) none of the above

12. [2 marks] Given the starting network ID 70.96.0.0/12, subnet to provide 512 usable hosts with as few extra hosts as possible. What is the number of subnets created?
   (a) /12
   (b) /20
   (c) /21
   (d) /22
   (e) none of the above

13. [2 marks] Given the network ID 4.150.128.0/17, subnet to provide 1924 hosts per subnet with as few extra hosts as possible. What is the new mask?
    (a) 255.255.128.0
    (b) 255.255.240.0
    (c) 255.255.255.0
    (d) 255.255.255.240
    (e) none of the above.

14. [2 marks] Given the network ID 82.192.0.0/11, subnet to provide 182 hosts per subnet with as few extra hosts as possible. What is the **actual** number of hosts created?
    (a) 182
    (b) 184
    (c) 254
    (d) 256
    (e) 8192

15. [2 marks] Given the starting network 186.186.108.0/23, subnet to provide 112 subnets with as few extra subnets as possible. What is the subnet ID for subnet #2?
    (a) 186.186.108.2
    (b) 186.186.108.4
    (c) 186.186.108.8
    (d) 186.186.109.0
    (e) 186.186.109.4

16. [2 marks] Given the starting network 233.166.10.0/24, subnet to provide 34 subnets with as few extra subnets as possible. What is the address of host #2 in subnet # 12?
    (a) 233.166.10.2
    (b) 233.166.10.24
    (c) 233.166.10.46
    (d) 233.166.10.50
    (b) 233.166.12.2

17. [2 marks] Given the starting network 3.2.1.0/24, subnet to provide 14 subnets with as few extra subnets as possible. What is the last usable host address of subnet # 10?
    (a) 3.2.1.140
    (b) 3.2.1.158
    (c) 3.2.1.174
    (d) 3.2.1.175
    (e) 3.2.1.10.14

18. [1 mark] What does "VLSM" mean?
    (a) Variable Length Subnet Masking
    (b) Very Long Source Mask
    (c) Very Long Subnet Method
    (d) Virtual Lab Subnet Method
    (e) Virtual Logical Source Masking

19. [1 mark] What is the difference between CSMA-CD and CSMA-CA?
   (a) CSMA-CD is used on wired systems, CSMA-CA is used on wireless systems
   (b) CSMA-CD is used on wired systems, CSMA-CA is used with fiber optic systems
   (c) They're similar, but "CD" = "Confirmed Destination" and "CA"="Confirmed Address"
   (d) No difference: one is the North American protocol name, the other is the European name
   (e) Neither is correct, they should be written CDMA-CS (source) and CDMA-CD (destination)

20. [1 mark] True or False: When communicating on the same network segment, a default gateway is **not** required.
   (a) True
   (b) False
   (c) Maybe
   (d) I'm copying off my friend, and he's chosen answer "d" so I will too.
   (e) None of the above

21. [1 mark] From your lab work, what is the destination MAC address for an ARP request?
   (a) 00:00:00:00:00:00 because the station's MAC address is **not** known yet!
   (b) FF:FF:FF:FF:FF:FF
   (c) the MAC address of the host sending out the request
   (d) the MAC address that the host is trying to reach
   (e) the MAC address of the default gateway

22. [1 mark] Which of the following is a characteristic of multi-mode fiber-optic cable?
   (a) generally uses LEDs as the light source
   (b) relatively smaller core with few paths for the light to travel
   (c) more expensive than single-mode
   (d) generally uses lasers as the light source
   (e) generally used between cities, rather than between buildings or in a downtown area

23. [1 mark] What is the difference between *signaling* and *encoding*?
   (a) *Signaling* refers to transmitting bits over wire (copper) and *encoding* to bits over fiber
   (b) *Signaling* refers to communicating '1' or '0', *encoding* refers to the choice of bit patterns to represent actual data
   (c) *Signaling* refers to using only 2 levels for bits, *encoding* refers to using 3+ levels for bits
   (d) *Signaling* is always slower than *encoding*
   (e) There is no difference, they basically mean the same thing

24. [1 mark] Which of the following is **not** a signaling method (… that we studied in lectures)?
   (a) NRZ
   (b) NRZ**I**
   (c) NRZ2
   (d) MLT-3
   (e) Manchester

25. [1 mark] Which of the following is **not** a correct pairing?
   (a) Layer 4 – Host/server
   (b) Layer 3 – Router
   (c) Layer 2 – Switch
   (d) Layer 1 – Hub
   (e) All of the above are correct.

26. [1 mark] A **`ping`** command produces the following output:
   `Reply from 2.3.4.5: bytes=32 time=2ms TTL=125`
   How many routers are between the source and destination?
   (a) More than 3 but less than 25 (ie. "at least 4")
   (b) 3
   (c) 2
   (d) 1
   (e) 0

27. [1 mark] You would like to transfer a 100MB file over the network but want to first calculate how long it should take. An accurate estimate can be calculated based on which of the following?
   (a) The speed of the network card in the sending host (10, 100, 1000)
   (b) The colour of the network cable used to join the sender to the receiver
   (c) the bandwidth
   (d) the throughput
   (e) the goodput

28. [1 mark] In Lab 8, you looked at the ARP cache in MS-Windows. Two types of entries were identified in the command output. What are the two types?
   (a) port and MAC address
   (b) port and IP address
   (c) single-use and multiple-use
   (d) static and dynamic
   (e) I don't know; I let my lab partner do all the work

29. [1 mark] In Lab 8, you pinged each device in the network (R2-Central, R1-ISP, Eagle-server). Why wasn't there an ARP entry for every single host that was pinged?
   (a) One or more entries timed out, so **not** all were visible when the ARP cache was displayed.
   (b) It's possible to have more than one host using the exact same MAC address, in which case the ARP cache only shows one entry for multiple hosts.
   (c) A host **never** sees MAC addresses from any host that is **not** on the LAN, so there is nothing to store.
   (d) An ARP cache only saves entries for hosts that **are** on the LAN; there's so many entries for hosts beyond LAN that the table would overflow if we tried to save them all.
   (e) An ARP cache only saves entries from hosts that are **not** on the LAN, since we can get the MAC address of a host **on** the LAN almost instantly (... so why bother storing it?)

30. [1 mark] By reading lab 9.8.1 in the Cisco online textbook for the Lab 8 post-lab, you found out about ARP spoofing / ARP poisoning. What is ARP spoofing?
   (a) Overloading a host's ARP cache so that valid entries are discarded
   (b) Overloading a host's IP tables so that valid entries are discarded
   (c) Overloading a host's routing table so that valid entries are discarded
   (d) Using ARP messages to get an attacking machine's MAC address listed in the ARP cache
   (e) Using ARP messages to make a victim machine reset it's own MAC address

31. [1 mark] An ARP cache and MAC table hold their entries for several 100's. What unit of time goes with this value?
   (a) 100's of milliseconds
   (b) 100's of seconds
   (c) 100's of minutes
   (d) 100's of hours
   (e) 100's of days

32. [1 mark] What kind of Ethernet frame did we see in our labs for telnet, FTP, and HTTP?
   (a) 802.2
   (b) 802.3
   (c) 802.11
   (d) Ethernet II
   (e) TCP

33. [1 mark] To verify that all the data is transmitted correctly, an Ethernet frame uses:
   (a) a CRC value
   (b) a checksum value
   (c) a preamble
   (d) a length field
   (e) voodoo magic

34. [1 mark] Which of the following is **not** a valid term for a network topology?
   (a) ferris wheel
   (b) hub and spoke
   (c) physical bus
   (d) star
   (e) point to point

35. [1 mark] What kind of addressing is used in a PPP frame, for point to point connections?
   (a) HDLC
   (b) ATM
   (c) Frame Relay
   (d) SONET
   (e) none (it is optional)

36. [1 mark] A Canadian Government spy agency wants to make sure no one can eavesdrop (listen in) on their network traffic. What is the best type of media to use for their network?
   (a) fiber optic cable
   (b) co-ax cable with a very loosely woven shield
   (c) Cat 5 cable
   (d) Cat 6 cable
   (e) wireless connections

37. [1 mark] A firewall operates at least as high as which level of the OSI model?
   (a) level 4
   (b) level 3
   (c) level 2
   (d) level 1
   (e) level 0

38. [1 mark] What is a reason single-mode fiber is more expensive than multi-mode fiber?
   (a) the core is thinner because it is manufactured more precisely
   (b) the core is thicker because it needs to be stronger (to go longer distances)
   (c) the core has better shielding to prevent interference
   (d) the outside has better shielding to prevent interference
   (e) Apple Inc. is the largest manufacturer, so it's more expensive (like all Apple products)

39. [1 mark] Which of the following is **not** a Layer 2 protocol?
   (a) WAN
   (b) PPP
   (c) Frame Relay
   (d) Ethernet
   (e) ATM

40. [1 mark] A student says Wireshark has detected STP. How would you explain what hat is to the student?
   (a) STP is Shielded Twisted Pair; Wireshark detects it from improved signal quality.
   (b) STP is Shielded Twisted Pair and Wireshark detects it based on frame length.
   (c) STP is Spanning Tree Protocol and it prevents a frame from looping on itself.
   (d) STP is Spanning Tree Protocol; it prevents loops from forming in the network.
   (e) Wireshark would never detected STP so the student must have made a mistake.

41. [1 mark] What DOS command will show the network settings, including the DHCP settings?
   (a) ipconfig /a
   (b) ipconfig /all
   (c) ifconfig /a
   (d) ifconfig /all
   (e) netstat /all