Midterm 1: CST8182 Networking Fundamentals

Winter 2010

Time: 60 minutes; Total Marks available: 50 marks + 10 bonus marks
(15% of final mark; allocation of marks is shown beside each question)

Version A

STOP!

Mark your test version in the field titled "Grade or Educ" on the scantron form.
(A = 1, B = 2, C = 3, D = 4, E = 5, F = 6)
Do it NOW!

Instructions:

1. 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!

2. Be sure to **mark your name and version of this midterm** on the scantron answer sheet.

3. All answers should be circled on this test paper **and** then marked on the scantron answer sheet.

4. If you do not find an answer which is clearly the correct choice, choose the *best* answer.

5. 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. [1 mark] In general, what network device responds to pings that exceed the TTL value?
   (a) The very *first host* along the path towards the destination host
   (b) The very *first server* along the path towards the destination host
   (c) The very *first router* along the path towards the destination host
   (d) Some router will respond, always the router which decrements the TTL value to zero **Correct**
   (e) The router along the path that is closest to the destination host

2. [1 mark] In general, what network device responds to pings to a fictitious (ie. non-existent) destination?
   (a) The very *first host* along the path towards the subnet of the non-existent destination
   (b) The very *first server* along the path towards the subnet of the non-existent destination
   (c) The very *first router* along the path towards the subnet of the non-existent destination
   (d) The *first router* that does *not have a route* to the subnet of the non-existent destination **Correct**
   (e) The *host that would be closest* to the non-existent destination

3. [1 mark] Why does an ICMP checksum change from one ping request to the next? Choose the **best** answer.
   (a) Any change in the destination address causes a change in the ICMP checksum
   (b) Any change in the sequence number causes a change in the ICMP checksum
   (c) Any change in the message data causes a change in the ICMP checksum
   (d) Any change in *any* of the ICMP header fields, but not the IP header fields, causes a change in the checksum **Correct**
   (e) Any change in *any* of the ICMP header fields, or the IP header fields, causes a change in the checksum

4. [1 mark] What fields are used by a host to match up a specific ICMP echo request with the corresponding ICMP echo reply?
   (a) The source and destination addresses
   (b) The source and type field
   (c) The type and checksum
   (d) The checksum and identifier
   (e) The identifier and sequence number **Correct**

5. [1 mark] What is an “RFC”?
   (a) It's a document describing how a host computer should operate
   (b) It's a “Remote Function Call” describing how network devices should work
   (c) It's a “Request For Comments” describing how a protocol should work **Correct**
   (d) It's a “Required Functions Commentary” describing how routers should operate
   (e) It's not actually a networking term, but a common mis-spelling of “KFC”

6. [1 mark] Which field or fields are used in calculating the checksum for an ICMP message?
   (a) Type
   (b) Code
   (c) Addresses (both source and destination)
   (d) Sequence number and identifier
   (e) All of the above **Correct**

7. [1 mark] What three parameters **must** be configured for any network device to communicate to other hosts throughout a large network?
   (a) Data, voice, and video
   (b) FTP, HTTP, and Telnet
   (c) TCP, UDP, and IP
   (d) IP address, DNS, and default gateway
   (e) IP address, mask, and default gateway **Correct**

8. [1 mark] What type of cable do you need to directly connect two workstations?
   (a) a cross-over cable **Correct**
   (b) a roll-over cable
   (c) a straight-through cable
   (d) a straight-up cable
   (e) any cable; workstations will always auto-configure themselves

9. [1 mark] What command could produce the following output?

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix  . :
 IP Address. . . . . . . . . . . . : 172.16.1.2
 Subnet Mask . . . . . . . . . . . : 255.255.0.0
 Default Gateway . . . . . . . . . : 172.16.255.254
```

   (a) ifconfig
   (b) ipconfig **Correct**
   (c) netstat -r
   (d) show ip interface
   (e) none of the above

10. [1 mark] Of the following destinations, which has the best "guarantee" of *ping* working?
   (a) the IP address 127.0.0.1 **Correct**
   (b) the default gateway
   (c) the DNS server
   (d) the IP address of the host's NIC card
   (e) None of the above is any more certain or reliable than any other

11. [1 mark] A routing table lists groups or ranges of IP addresses together with the interface (NIC) to use for reaching the group. What IP address does a routing table use to designate the "default route"?
   (a) 0.0.0.0/0 **Correct**
   (b) 127.0.0.0/8
   (c) 127.0.0.1/8
   (d) 127.0.0.1 mask 255.0.0.0
   (e) 255.255.255.255

12. [1 mark] Different companies sometimes have different words for some terms. For example, Cisco commands will display something that is called “gateway of last resort”. Which term below means the same thing?
   (a) the broadcast address
   (b) the default route **Correct**
   (c) the address of the DNS server
   (d) the host's own IP address
   (e) the localhost

13. [1 mark] Can a router have a default route?
   (a) Yes **Correct**
   (b) Yes, but only if it **is** being used as a default gateway
   (c) Yes, but only if it **is not** being used as a default gateway
   (d) No
   (e) How should I know? I didn't pay attention to the Lab 4 Post-lab questions!

14. [1 mark] Which of the following is the correct “top down” order of the OSI networking model?
   (a) application, transport, internet, network access
   (b) network access, internet, tranportation, application
   (c) application, presentation, session, transport, internet, network access
   (d) application, presentation, session, transport, network, data link, physical **Correct**
   (e) application, data link, network, physical, presentation, session, transport

15. [1 mark] What is the difference between the names “Network” and “Network Access” when referring to standard network models?
   (a) there is no difference in meaning
   (b) “network” refers to layer 1 and “network access” refers to layer 2
   (c) “network access” refers to layer 1 and “network” refers to layer 2
   (d) “network” refers to layer 3 and “network access” refers to layers 1 & 2 **Correct**
   (e) “network access” refers to layer 3 and “network” refers to layers 1 & 2

16. [1 mark] Which protocols can be considered “secure”?
   (a) IPv4 and IPv6
   (b) TCP and UDP
   (c) DHCP, DNS, and ARP
   (d) HTTP and TFTP
   (e) None of the above **Correct**

17. [1 mark] What do the following protocols have in common?
   ARP, DNS, FTP, HTTP, POP, SMTP
   (a) they are all application layer protocols
   (b) they all use TCP for their transport layer
   (c) they all provide security in the form of passwords
   (d) they are all considered insecure **Correct**
   (e) none of the above

18. [1 mark] Which of the following provide *reliability* ?
   (a) Ethernet
   (b) IP
   (c) UDP
   (d) TCP **Correct**
   (e) None of the above

19. [1 mark] Which of the following is considered a client-server protocol?
   (a) DNS
   (b) FTP
   (c) HTTP
   (d) POP
   (e) all of the above **Correct**

20. [1 mark] Which protocol provides connectionless network layer services?
   (a) Ethernet
   (b) IP **Correct**
   (c) OSI
   (d) TCP
   (e) UDP

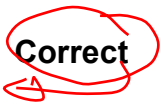
21. [1 mark] By the time a (modern, network-aware) application's data is transferred over the wire, how many layers of addressing have been added?
   (a) 0
   (b) 1
   (c) 2
   (d) 3 **Correct**
   (e) 4

22. [1 mark] What is the most important reason for the 3-way handshake in the Transport layer?
   (a) it is used to confirm that the host at the other end is responding (sort of like a “ping”)
   (b) it is used to confirm the port number to be used at each end
   (c) it is used to exchange the sequence number that will be used by the server
   (d) it is used to exchange the sequence numbers for both the client and the server **Correct**
   (e) This a trick question: the 3-way handshake is in the *Network* layer, **not** the Transport!

23. [2 marks] A student in the lab is trying to finish a lab quickly, so does not bother to configure a default gateway. What hosts will the student be able to reach? [**Bonus**]
   (a) no other hosts at all
   (b) only hosts on the same subnet, but not on any other subnets **Correct**
   (c) only hosts on the local LAN, but not any other networks
   (d) only hosts on the local LAN and at most one hop away
   (e) only hosts identified by numeric IP address, but not hosts identified by name

24. [1 mark] Which of the following is a good basis (or reason) to group hosts?
   (a) based on geography or location
   (b) based on job function of the people using the hosts
   (c) based on security requirements
   (d) based on expected network (ie. bandwidth) usage
   (e) all of the above **Correct**

25. [1 mark] Two hosts, Host1 and Host2, are connected through a switch. Host1 is in the process of setting up a TCP session with Host2. Host1 has sent a SYN message to begin session establishment. What happens next?
   (a) Host1 sends a segment with the ACK flag = 0, SYN flag = 0 to Host2
   (b) Host1 sends a segment with the ACK flag = 1, SYN flag = 0 to Host2
   (c) Host1 sends a segment with the ACK flag = 1, SYN flag = 1 to Host2
   (d) Host2 sends a segment with the ACK flag = 1, SYN flag = 0 to Host1 **Correct**
   (e) Host2 sends a segment with the ACK flag = 1, SYN flag = 1 to Host1



26. [1 mark] Which of the following is **not** a correct pairing?
   (a) application – data
   (b) internet – IP
   (c) network access – MAC
   (d) transport – port
   (e) none; all of the above are correct **Correct**

27. [1 mark] In Wireshark, what is the correct filter expression to see **all** the activity that could be caused by a *ping* command?
   (a) icmp
   (b) ICMP
   (c) icmp || tcp
   (d) icmp | arp | dns
   (e) icmp || arp || dns **Correct**

28. [1 mark] What uniquely identifies the first TCP datagram of a new connection?
   (a) It is the only one where the source port is 0, until the new connection is established
   (b) It is the only one with just FIN set
   (c) It is the only one with both the FIN and ACK flags set
   (d) It is the only one with just the SYN flag set **Correct**
   (e) It is the only one with both the SYN and ACK flags set

29. [1 mark] With HTTP, the server port is 80. What will the browser's port number be?
   (a) 0
   (b) 80
   (c) 255
   (d) possibly any port from 1024 – 65534 **Correct**
   (e) possibly any port from 1 – 65535

30. [1 mark] How does TFTP ensure reliable delivery of data?
   (a) TFTP relies on the reliability mechanisms built into the transport layer protocol
   (b) Reliability is ensured by setting the ACK flag in the header of the TCP transport layer
   (c) Reliability is ensured by setting the ACK flag in the header of the UDP transport layer
   (d) TFTP adds its own reliability at the application layer by sending its own ACK datagrams **Correct**
   (e) TFTP does not have any reliability at any layer, so there is no guarantee of reliability

31. [2 marks] To which subnet does the IP address 10.10.10.44/28 belong?
   (a) 10.10.8.0/28
   (b) 10.10.10.0/28
   (c) 10.10.10.16/28
   (d) 10.10.10.32/28 **Correct**
   (e) 10.10.10.48/28

32. [2 marks] Which of the following is a valid subnet ID?
   (a) 2.5.10.12/30 **Correct**
   (b) 2.5.20.20/29
   (c) 2.5.30.24/27
   (d) 2.5.30.24/28
   (e) none of the above

33. [2 marks] What is the first and last usable address for 3.6.9.72/30?
   (a) 3.6.9.72 and 3.6.9.74
   (b) 3.6.9.72 and 3.6.9.75
   (c) 3.6.9.72 and 3.6.9.76
   (d) 3.6.9.73 and 3.6.9.74 **Correct**
   (e) 3.6.9.73 and 3.6.9.75

34. [2 marks] Given a starting network of 2.4.6.0/24 that is subnetted into 4 subnets, what is the broadcast address of subnet #1?
   (a) 2.4.6.63 **Correct**
   (b) 2.4.6.126
   (c) 2.4.6.127
   (d) 2.4.6.192
   (e) none of the above

35. [2 marks] You have a /23 address block and need to support 35 subnets, with as few extra subnets as possible. What mask would be the best choice?
   (a) 255.255.255.192
   (b) 255.255.255.224
   (c) 225.255.255.240
   (d) 255.255.255.248 **Correct**
   (e) none of the above

36. [2 marks] Given a starting network of 192.168.10.0/24 that is subnetted to /28, what is the usable host range for subnet #2?
(a) 192.168.10.1 to 192.168.10.15
(b) 192.168.10.1 to 192.168.10.31
(c) 192.168.10.16 to 192.168.10.63
(d) 192.168.10.32 to 192.168.10.64
(e) 192.168.10.33 to 192.168.10.47 **Correct**

Should actually be 46; this is still the closet/best answer!

37. [2 marks] Given the IP configuration 1.1.1.99/27, to which subnet does it belong?
(a) 1.1.1.32/27
(b) 1.1.1.64/27
(c) 1.1.1.96/27 **Correct**
(d) 1.1.1.128/27
(e) none of the above

38. [2 marks] Given a starting network of 1.2.3.0/24 that is subnetted to provide 8 hosts per subnet, what is the broadcast address of subnet #2?
(a) 1.2.3.47 **Correct**
(b) 1.2.3.15
(c) 1.2.3.31
(d) 1.2.3.63
(e) none of the above

39. [2 marks] Given a network address of 3.2.1.0/24, what is the maximum number of subnets you can create if each subnet must support at least seven hosts?
(a) 4
(b) 8
(c) 16 **Correct**
(d) 32
(e) 64

40. [2 marks] You are a systems administrator and you are about to assign static IP addresses to various servers on your network. For the network 192.168.20.24/29 the router is assigned to the first usable host address, while the last usable host address goes to your Sales server. Which one of the following commands would you enter into the IP properties box of the sales server? [This is an example of an actual CCNA exam question.]

(a) IP: 192.168.20.14 Mask: 255.255.255.248 Gateway: 192.168.20.9
(b) IP: 192.168.20.254 Mask: 255.255.255.0 Gateway: 192.168.20.1
(c) IP: 192.168.20.30 Mask: 255.255.255.248 Gateway: 192.168.20.25 **Correct**
(d) IP: 192.168.20.30 Mask: 255.255.255.240 Gateway: 192.168.20.17
(e) IP: 192.168.20.30 Mask: 255.255.255.240 Gateway: 192.168.20.25

41. [2 marks] The Network Architect at Algonquin College has subnetted using a subnet mask of 255.255.255.192. A duplicate IP address of 172.16.2.121 has accidentally been configured on workstation PC1 in this network. You must assign this workstation a new IP address within the same subnetwork. Which address could correctly be assigned to PC1?
(a) 172.16.1.80
(b) 172.16.2.64
(c) 172.16.2.80 **Correct**
(d) 172.16.2.127
(e) 172.16.2.128

42. [2 marks] Algonquin has a /24 network and you need ten subnets. You wish to have as many addresses available for hosts as possible. Which one of the following subnet masks should you use?
(a) 255.255.255.192
(b) 255.255.255.224
(c) 255.255.255.240 **Correct**
(d) 255.255.255.248
(e) 255.255.255.252

43. [2 marks] You need subnet a network block. How many subnetworks and hosts are available per subnet if you apply a /28 mask to the 210.10.2.0/24 network?
(a) 30 networks and 6 hosts
(b) 6 networks and 30 hosts
(c) 8 networks and 32 hosts
(d) 32 networks and 18 hosts
(e) 16 networks and 14 hosts **Correct**

44. [1 mark] Which of the following is the correct representation of mask 255.224.0.0?
(a) /8
(b) /10
(c) /11 **Correct**
(d) /12
(e) /16

45. [1 mark] What subnet mask would be used with hosts in the 128.107.176.0/22 network?
(a) 255.0.0.0
(b) 255.248.0.0
(c) 255.255.252.0 **Correct**
(d) 255.255.255.0
(e) 255.255.255.252

46. [1 mark] What subnet mask will provide the appropriate number of addresses for a network of 16 hosts, with minimal wasted addresses?
(a) /14
(b) /16
(c) /24 **Correct**
(d) /27
(e) /28