Midterm 2: CST8182 Networking Fundamentals

Winter 2010

Time: 60 minutes; Total Marks available: 50 marks + 6 bonus marks
(15% of final mark; allocation of marks is shown beside each question)

Master Version

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).
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.

What is your:

NAME? _____ Student Id? _____

(Continued on next page)

1. [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 checksum and identifier
   (b) The identifier and sequence number **Correct** (repeat from Midterm #1)
   (c) The source and destination addresses
   (d) The source and type field
   (e) The type and checksum

2. [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?
   (a) no other hosts at all
   (b) only hosts on the local LAN, but not any other networks
   (c) only hosts on the local LAN and at most one hop away
   (d) only hosts on the same subnet, but not on any other subnets **Correct** (repeat from MT1)
   (e) only hosts identified by numeric IP address, but not hosts identified by name

3. [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** (repeat from Midterm #1)

4. [1 mark] How does TFTP ensure reliable delivery of data?
   (a) TFTP adds its own reliability at the application layer by sending its own ACK datagrams **Correct**
   (b) TFTP relies on the reliability mechanisms built into the transport layer protocol
   (c) Reliability is ensured by setting the ACK flag in the header of the TCP transport layer
   (d) Reliability is ensured by setting the ACK flag in the header of the UDP transport layer
   (e) TFTP does not have any reliability at any layer, so there is no guarantee of reliability

5. [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) 1.2.3.15
   (b) 1.2.3.31
   (c) 1.2.3.47 **Correct** (repeat from Midterm #1)
   (d) 1.2.3.63
   (e) none of the above

6. [2 marks] Given a starting network of 172.16.32.0/21 that is subnetted to provide 3 subnets, what is the address of **host #11** on **subnet #3**?
   (a) 172.16.35.96
   (b) 172.16.36.11
   (c) 172.16.38.11 **Correct** (repeat from Lab 6)
   (d) 172.16.39.96
   (e) none of the above

7. [2 marks] Given a starting network of 172.45.0.0/16 that is subnetted to provide 222 subnets, what is the address of **host #9** on **subnet #9**?
   (a) 172.45.9.9 **Correct** (from Lab 6)
   (b) 172.45.9.144
   (c) 172.45.144.9
   (d) 172.45.144.144
   (e) none of the above

8. [2 marks] Rogers has subnetted one of their starting networks 24.128.0.0/9 to provide subnets with 512 hosts per subnet. What is the address of **host #257** on **subnet #12**?
   (a) 24.128.25.1
   (b) 24.128.49.1 **Correct** (repeat from Lab 6)
   (c) 24.128.13.1
   (d) 24.224.1.1
   (e) none of the above

9. [2 marks] Algonquin wants to subnet their internal network of 10.0.0.0/8 into 1000 subnets. What is the address of **host #256** on **subnet #256**?
   (a) 10.64.1.0 **Correct** (repeat from Lab 6)
   (b) 10.64.0.255
   (c) 10.128.1.0
   (d) 10.128.2.0
   (e) none of the above

10. [2 marks] Given the host address 131.23.98.45/23 and the fact that the starting network was 131.23.96.0/20, calculate the **subnet #** for this host address.
   (a) 1 **Correct**
   (b) 2
   (c) 3
   (d) 8
   (e) none of the above

11. [2 marks] What is the **last valid host** on the subnet 172.17.22.0/23?
   (a) 172.17.22.254
   (b) 172.17.22.255
   (c) 172.17.23.254 **Correct**
   (d) 172.17.23.255
   (e) none of the above

12. [2 marks] What is the **first valid host** on the network 20.74.209.189/9?
   (a) 20.0.0.0
   (b) 20.0.0.1 **Correct**
   (c) 20.74.209.1
   (d) 20.74.209.189
   (e) none of the above

13. [2 marks] What is the **broadcast address** for the network 75.191.8.215/18?
   (a) 75.191.8.255
   (b) 75.191.63.255 **Correct**
   (c) 75.191.127.255
   (d) 75.191.255.255
   (e) none of the above

14. [2 marks] What is the **subnet ID** for the IP address 77.18.81.193/11?
   (a) 77.0.0.0/11 **Correct**
   (b) 77.18.0.0/11
   (c) 77.18.81.0/11
   (d) 77.18.81.192/11
   (e) none of the above

15. [2 marks] Given the host address 10.10.45.33/30 and the fact that the starting network was 10.10.45.0/25, what is the **host #** of this IP address?
   (a) 1 **Correct** (repeat from Lab 6)
   (b) 2
   (c) 32
   (d) 33
   (e) none of the above

16. [1 mark] How many hosts can you have on the network 9.8.64.0/21?
   (a) 13
   (b) 14
   (c) 254
   (d) 2046 **Correct**
   (e) none of the above

17. [2 marks] Which of the following is a suitable address for a default gateway?
   (a) 172.10.31.0/24
   (b) 172.10.31.127/25
   (c) 172.10.31.129/26 **Correct**
   (d) 172.10.31.255/27
   (e) none of the above

18. [2 marks] During the lecture for Wk06Day2, we saw the "whois" information for Algonquin. The college owns the addresses: 205.211.26.0/23, 205.211.28.0/22, 205.211.32.0/19, 205.211.64.0/21, 205.211.72.0/22, 205.211.76.0/23, and 205.211.78.0/24 . What is the **broadcast** address for Algonquin college?
   (a) 205.211.26.255
   (b) 205.211.27.255
   (c) 205.211.78.255
   (d) 205.211.255.255
   (e) none of the above **Correct**

19. [1 mark] What is the highest level of addressing in a CDP frame?
(a) Layer 1
(b) Layer 2 **Correct**
(c) Layer 3
(d) Layer 4
(e) none of the above; CDP uses direct communication

20. [1 mark] What is the purpose of using STP, as seen in Wireshark?
(a) STP is used between switches to communicate the layout of the network and to prevent any loops forming if there are spare or redundant links. **Correct**
(b) STP is a Cisco-specific protocol allowing communication between switches to prevent spare or redundant links from causing loops.
(c) STP is used between routers to communicate the layout of the network and to prevent any loops forming if there are spare or redundant links.
(d) STP stands for "Specifically Treated Petroleum" and is a brand of oil used to ensure the network equipment functions smoothly.
(e) This is a trick question; Wireshark can **not** detect whether cables are UTP or STP.

21. [1 mark] In which pane does Wireshark show the Ethernet preamble field?
(a) top pane only
(b) middle pane only
(c) bottom pane only
(d) middle and bottom panes
(e) none of the above **Correct**

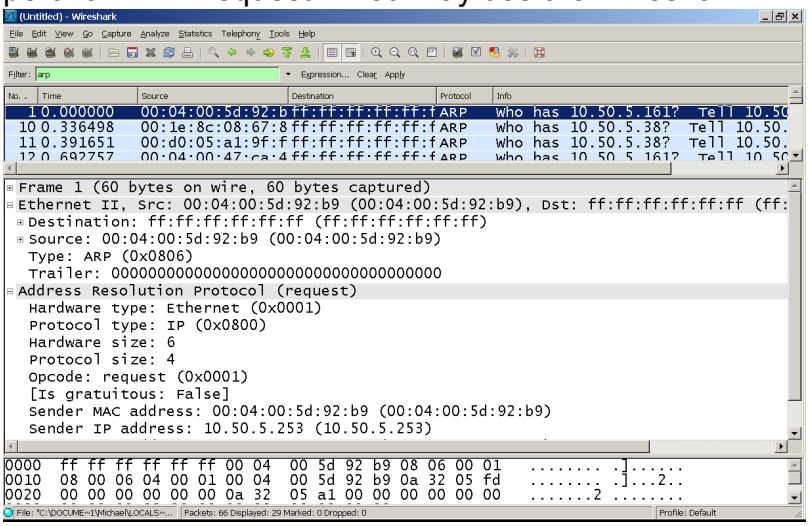
22. [1 mark] Using Wireshark to determine the OUI of a computer can help you determine:
(a) which OS the computer is running
(b) the manufacturer of the computer **Correct**
(c) whether the computer is acting as a host or a server
(d) whether the computer is configured with a proper value for the gateway
(e) the "serial number" of the computer

23. [1 mark] A host will never know, and thus never use, the actual MAC address for which network devices? Choose **all** that apply.
(a) of any device on the local segment (ie. the directly connected LAN)
(b) of any device **not** on the local segment (ie. the directly connected LAN) **Correct**
(c) of the default gateway
(d) of any router
(e) None of the above. Frames are always sent out with the MAC address of the final destination.

24. [1 mark] From our lab work, what is the difference between an "ARP cache" and a "MAC table"?
(a) there is no difference; they're different names for the same thing
(b) the ARP cache has dynamic entries, a MAC table has static entries
(c) the ARP cache has IP – MAC entries; a MAC table has MAC – port entries **Correct**
(d) the only difference is the location: a PC has an ARP cache, a switch has a MAC table
(e) the only difference is the location: a PC has an ARP cache, a router has a MAC table

25. [1 mark] What is the difference between a *dynamic* and a *static* ARP entry?
   (a) Dynamic entries are created by computers; static entries are created by humans **Correct**
   (b) Static entries time out more quickly (eg. 2-3 min) than dynamic entries (eg. 10 min)
   (c) Dynamic entries appear on a PC, static entries appear on a switch
   (d) Dynamic ARP entries can increase network security by preventing MAC address spoofing
   (e) This is a trick question; *dynamic* and *static* refer only to MAC tables, not ARP

26. [1 mark] What is the Ethernet type of an ARP request? You may use the Wireshark capture below to help you.
   (a) 0x0001
   (b) 0x0800
   (c) 0x0806 **Correct**
   (d) "request"
   (e) "Who has ..."



27. [1 mark] Use the output of "netstat -r" command below to answer the next 4 questions.

```
C:\>netstat -r
Route Table
===========================================================================
Interface List
0x1 ...................MS TCP Loopback interface
0x2 .00 21 6a 8a 10 a8 .Intel(R) WiFi Link 5300 AGN
0x3 .00 23 26 b6 a0 61 .Intel(R) 82567LM Gigabit Network Connection
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.50.5.1      10.50.5.83      20
         10.50.5.0    255.255.255.0      10.50.5.83      10.50.5.83      20
        10.50.5.83  255.255.255.255       127.0.0.1       127.0.0.1      20
   10.255.255.255  255.255.255.255      10.50.5.83      10.50.5.83      20
        127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1       1
        224.0.0.0        240.0.0.0      10.50.5.83      10.50.5.83      20
  255.255.255.255  255.255.255.255      10.50.5.83      10.50.5.83       1
  255.255.255.255  255.255.255.255      10.50.5.83               2       1
Default Gateway:          10.50.5.1
===========================================================================
Persistent Routes:
  None
```

What is the Ethernet address of a wireless network card?
   (a) 00:21:6a:8a:10:a8 **Correct**
   (b) 00:23:26:b6:a0:61
   (c) 10.50.5.83
   (d) We cannot tell which of the addresses above belongs to the wireless card.
   (e) It is **not** shown anywhere above.

28. [1 mark] Referring to the “netstat -r” output above, what is the address of the “MS TCP Loopback interface”?
   (a) 0.0.0.0
   (b) 10.50.5.83
   (c) 127.0.0.1 **Correct**
   (d) We cannot tell which of the addresses above belongs to that interface **weak; ok this time**
   (e) It is **not** shown anywhere above.

29. [1 mark] Referring to the “netstat -r” output above, the Network Destination “0.0.0.0” is:
   (a) the address of the default gateway
   (b) the address for the wireless card (there's no access point nearby, so it's still blank)
   (c) the internal address of 10.50.5.1
   (d) a routing table entry which says to use the default gateway when no other route matches
   (e) none of the above **Answer “D” is correct**

30. [1 mark] Referring to the “netstat -r” output above, there are two entries for “Intel” network adapters with different ID numbers. You're not sure whether the teacher has changed or “faked” the output. How can you verify whether the ID's are likely correct?
   (a) Try using both ID's with ping; if you get a response, they're correct
   (b) Try using both ID's with ARP; if you get a response, they're correct
   (c) Look up each ID in the IEEE OUI database
   (d) Look up the first half of each ID in the IEEE OUI database **Correct**
   (e) Simply ask the teacher during the midterm; he'll probably tell you.

31. [1 mark] Which network device(s) decrement the TTL value of IP packets? Choose **all** that apply.
   (a) the end host computer
   (b) only the default gateway
   (c) all routers **Correct**
   (d) all servers
   (e) all switches

32. [1 mark] How is **`traceroute`** (or **`tracert`**) able to identify all the routers in the path?
   (a) It sends out an Identify Request (ID Req) message that all routers respond to
   (b) It sends out a ping destined to each router in turn, then prints out their name/IP address
   (c) It sends out a DNS request to each router in turn, then prints out their name/IP address
   (d) It sends out ICMP requests to the destination but changes the TTL value, trying to get each router to respond **Correct**
   (e) It sends out a ping to the destination and scans the response for the list of all routers that handled the reply.

33. [1 mark] Which protocol automates all of the following functions for hosts on a network: IP configuration, IP address, subnet mask, default gateway, and DNS server information?
   (a) ARP
   (b) CDP
   (c) DNS
   (d) DHCP **Correct**
   (e) SNMP

34. [1 mark] From our lab work, identify the protocols that ICMP uses. Choose **all** that apply.
   (a) TCP
   (b) UDP
   (c) IP **Correct**
   (d) ARP
   (e) none of the above

35. [1 mark] Which of the following are sources of noise for fiber optic cabling? Choose **all** that apply.
   (a) EMI
   (b) RFI
   (c) cross-talk from other fibers
   (d) wireless communications
   (e) none of the above **Correct**

36. [1 mark] Which of the following is **not** a wireless standard? Choose **all** that apply.
   (a) 802.3 **Correct**
   (b) 802.11
   (c) 802.15
   (d) 802.16
   (e) WiMAX

37. [1 mark] If you were going to assign a TTL value to a L2 frame, what would be the most appropriate value?
   (a) 0
   (b) 1 **Correct**
   (c) 64
   (d) 128
   (e) 255

38. [1 mark] Which of the following are **not** part of the generic structure of L2 frames? Choose **all** that apply.
   (a) frame start/end
   (b) addressing
   (c) control fields and error detection
   (d) payload
   (e) none of the above **Correct**

39. [1 mark] Which of the following is **not** true of fiber optic cables?
   (a) They use either a laser or an LED as the light source.
   (b) They use a photodiode as a detector at the receiving end.
   (c) There are two main types: single mode and multi-mode
   (d) Single mode are faster because they are full-duplex, multi-mode are only half-duplex
   (e) none of the above. **D is the Correct answer**

40. [1 mark] What is the minimum rating of UTP cable required to run 100Mbps Ethernet?
   (a) Cat 4
   (b) Cat 5 **Correct**
   (c) Cat 5e
   (d) Cat 6
   (e) any of the above.

41. [1 mark] What is the minimum rating of UTP cable required to run 1Gbps Ethernet?
   (a) Cat 4
   (b) Cat 5
   (c) Cat 5e **Correct**
   (d) Cat 6
   (e) any of the above.

42. [1 mark] Which of the following is **not** a consideration for choosing a cable?
   (a) bandwidth
   (b) cost
   (c) susceptibility to noise or interference
   (d) maximum transmission distance
   (e) none of the above **Correct**

43. [1 mark] True or false? A packet travelling across 10 hops could have a unique type of L2 encapsulation for **each** hop between source and destination.
   (a) True **True: Ethernet (over copper), WiFi Ethernet, WiMAX,**
   (b) False **ATM, Frame Relay, ISDN, POS, HDLC, satellite, SONET/SDH, etc.**