

# Midterm 1: CST8182 Networking Fundamentals

Winter 2011

Time: 50 minutes; Total Marks available: 45 marks + 4 bonus marks  
(Allocation of marks is shown beside each question)

## Version A

### 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? \_\_\_\_\_

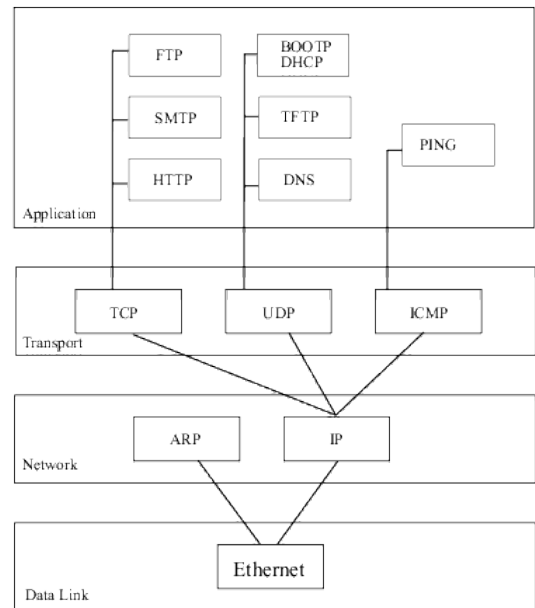
Student Id? \_\_\_\_\_

(Continued on next page)

1. [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] Examine the bottom layer in the following diagram of a Networking model. What OSI layers correspond to the bottom layer in the diagram?

- (a) Data Link
- (b) Layer 1
- (c) Physical layer
- (d) Layer 2
- (e) Layer 2 and Physical layer **correct**



3. [1 mark] Which of the following correctly gives a difference between FTP and TFTP?
- (a) FTP is client-server; TFTP is peer-to-peer
  - (b) TFTP uses ACKs but FTP does not
  - (c) FTP requires a password and account to login, TFTP does not **correct**
  - (d) FTP is secure, TFTP is not
  - (e) This is a trick question; there is no such thing as TFTP

4. [1 mark] Which of the following application protocols is used when *retrieving* email?

- (a) POP **correct**
- (b) UDP
- (c) TCP
- (d) SMTP
- (e) HTTP

5. [1 mark] Which of the following transport protocols is used when *retrieving* email?

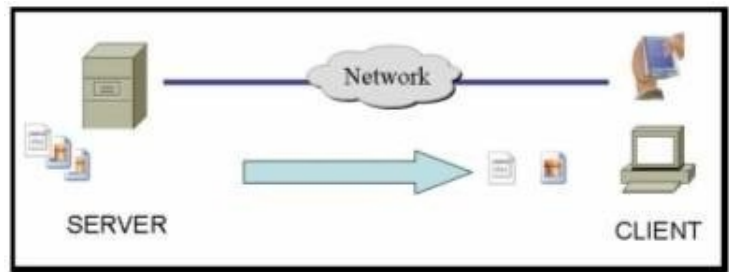
- (a) POP
- (b) UDP
- (c) TCP **correct**
- (d) SMTP
- (e) HTTP

6. [1 mark] From your lab work, you've seen that a simple "ping" command can trigger many network exchanges. What is the correct sequence of operations for ping on a freshly booted PC? (Assume all caches are cleared & empty.)
- (a) ARP, DNS, ICMP reply, ICMP request
  - (b) DNS, ARP, ICMP reply, ICMP request
  - (c) ICMP request, ICMP reply, ARP, DNS
  - (d) ARP, DNS, ICMP request, ICMP reply **Correct**
  - (e) TTL, ARP, DNS, ICMP request, ICMP reply
7. [1 mark] Which of the following are connection-oriented networking protocols? Choose **all** that apply.
- (a) ADC
  - (b) ICMP
  - (c) IP
  - (d) TCP **Correct**
  - (e) UDP
8. [1 mark] Which of the following is a network socket? (... Do you remember *what* a socket is?)
- (a) a matching pair of SYN and ACK numbers
  - (b) a matching pair of ICMP echo request and reply Identifiers
  - (c) a matching pair of ICMP echo request and reply Sequence numbers
  - (d) 172.16.254.16:80 **Correct**
  - (e) something that you plug a hair dryer or a lamp into
9. [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 **Correct**
10. [1 mark] What do the following protocols have in common?  
PING, HTTP, FTP, Telnet
- (a) they are all application layer protocols **Correct**
  - (b) they all use TCP for their transport layer
  - (c) they are all considered secure
  - (d) they don't require any passwords or authentication
  - (e) none of the above **I may accept this answer, but you must see me to explain why**
11. [1 mark] What do the following protocols have in common?  
ARP, DHCP, DNS, IP,
- (a) none of them is an application layer protocol **Correct**
  - (b) they all use TCP for their transport layer
  - (c) they are all considered secure
  - (d) they don't require any passwords or authentication **Also correct**
  - (e) none of the above

12. [1 mark] What port can DNS use on the **client** side? (Can you remember your lab work?)
- (a) 0
  - (b) 53
  - (c) 80
  - (d) any port from 1 – 1023
  - (e) any port from 1024 – 65534 **Correct**
13. [1 mark] What port does DNS use on the **server** side? (Can you remember your lab work?)
- (a) 0
  - (b) 53 **Correct**
  - (c) 80
  - (d) any port from 1 – 1023
  - (e) any port from 1024 – 65534
14. [1 mark] Which of the following could be used to remember the correct ordering, *from top to bottom*, of network layers in the OSI model?
- (a) All People Should Teach Networking Daily Please **Correct**
  - (b) All Things Inspire Networking
  - (c) Please Do Not Throw Pizza Sauce Away
  - (d) Please Do Not Touch Steve's Pet Alligator
  - (e) none of the above
15. [1 mark] What is the correct Wireshark filter expression to see only ARP and ping? (Choose the **best** answer, and then move on!)
- (a) ARP or ping
  - (b) ARP || ping
  - (c) arp or PING
  - (d) arp || PING
  - (e) arp || ping **Correct**
16. [1 mark] At the Transport layer, TCP performs a whole lot of roles and services, and UDP does not. So what feature(s) *does* UDP provide? Choose **all** that apply.
- (a) enables multiple applications to use the network at the same time **Correct**
  - (b) ensures reliable delivery of data
  - (c) ensures data is processed in the correct order
  - (d) performs flow control
  - (e) retransmission of anything **not** received
17. [1 mark] Which of the following is **not** a function or service of TCP?
- (a) Initiating a session
  - (b) provides fast, connection-less oriented data flow **Correct**
  - (c) segmenting and reassembling the data streams
  - (d) ensuring reliable delivery of data and performing flow control
  - (e) Session termination

18. [1 mark] Referring to the diagram, which term applies to a data transfer in the direction indicated by the large arrow?

- (a) download **Correct**
- (b) data read
- (c) data write
- (d) upload
- (e) none of the above



19. [1 mark] The figure shows a partial Wireshark capture. What sequence is visible?

- (a) 3-way handshake
- (b) 4-way handshake
- (c) 3-way teardown **Y**
- (d) 4-way teardown
- (e) 4-layer OSI model

No. .	Source	Destination	Protocol	Info
17247	192.168.0.1	192.168.0.166	SSHv2	Encrypted response packet len=64
17248	192.168.0.166	192.168.0.1	TCP	33873 > ssh [ACK] Seq=2384 Ack=2352 Win=9088 Len=0 TSV=2571961
17249	192.168.0.1	192.168.0.166	SSHv2	Encrypted response packet len=32
17250	192.168.0.166	192.168.0.1	TCP	33873 > ssh [ACK] Seq=2384 Ack=2384 Win=9088 Len=0 TSV=2571962
17251	192.168.0.166	192.168.0.1	TCP	[TCP segment of a reassembled PDU]
17252	192.168.0.166	192.168.0.1	TCP	[TCP segment of a reassembled PDU]
17253	192.168.0.166	192.168.0.1	TCP	33873 > ssh [FIN, ACK] Seq=2480 Ack=2384 Win=9088 Len=0 TSV=257
17254	192.168.0.1	192.168.0.166	TCP	ssh > 33873 [FIN, ACK] Seq=2384 Ack=2481 Win=8712 Len=0 TSV=764
17255	192.168.0.166	192.168.0.1	TCP	33873 > ssh [ACK] Seq=2481 Ack=2385 Win=9088 Len=0 TSV=2571963
17256	192.168.0.166	192.168.0.10	SMB	[TCP Retransmission] Locking AndX Request, FID: 0x3597
17257	192.168.0.10	192.168.0.166	SMB	Locking AndX Response, Error: STATUS_FILE_LOCK_CONFLICT

▸ Frame 17249 (98 bytes on wire, 98 bytes captured)  
 ▸ Ethernet II, Src: Cisco-Li\_2d:9b:50 (00:13:10:2d:9b:50), Dst: Intel\_bb:5f:7c (00:16:ea:bb:5f:7c)  
 ▸ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.166 (192.168.0.166)  
 ▸ Transmission Control Protocol, Src Port: ssh (22), Dst Port: 33873 (33873), Seq: 2352, Ack: 2384, Len: 32  
 ▾ SSH Protocol  
   ▾ SSH Version 2 (encryption:aes128-ctr mac:hmac-md5 compression:none)

20. [1 mark] In the Wireshark capture above, which port is the client using?

- (a) 22
- (b) 64
- (c) 33873 **Correct**
- (d) the ssh port (exact number not shown)
- (e) it can **not** be determined from the diagram above

21. [1 mark] The following is a header diagram for which layer?

- (a) layer 1
- (b) layer 2
- (c) layer 3 **Correct**
- (d) layer 4
- (e) layer 7

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options (optional)				

22. [1 mark] The following is a header diagram for which layer?

- (a) layer 1
- (b) layer 2
- (c) layer 3
- (d) layer 4 **Correct**
- (e) layer 7

SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	NOT USED	CODE BITS		WINDOW	
CHECKSUM			URGENT POINTER		
OPTIONS (if any)					
BEGINNING OF DATA					
⋮					

23. [1 mark] Which field is modified so that traceroute gets responses from increasingly distant devices?
- (a) ICMP flags
  - (b) ICMP checksum
  - (c) ICMP type
  - (d) IP TTL **correct**
  - (e) IP checksum
24. [1 mark – **Bonus**] Which of the following is an invalid mask?
- (a) 127.0.0.0 **Correct**
  - (b) 128.0.0.0
  - (c) 192.0.0.0
  - (d) 224.0.0.0
  - (e) 255.0.0.0
25. [1 mark] What DOS command will continue pinging the address 192.168.0.1 forever?
- (a) ping -a 192.168.0.1
  - (b) ping -d 192.168.0.1
  - (c) ping -i 192.168.0.1
  - (d) ping -t 192.168.0.1 **Correct**
  - (e) ping -w 192.168.0.1
26. [1 mark] Convert the dotted quad mask 255.224.0.0 into CIDR "/xx" notation.
- (a) /3
  - (b) /9
  - (c) /11 **Correct**
  - (d) /19
  - (e) /24
27. [1 mark] Convert the CIDR mask "/21" into dotted quad notation.
- (a) 252.0.0.0
  - (b) 255.128.0.0
  - (c) 255.252.0.0
  - (d) 255.255.128.0
  - (e) 255.255.248.0 **Correct**
28. [1 mark] Given the IP address 1.2.3.4/27, what is the broadcast address for its subnet?
- (a) 1.2.3.255
  - (b) 1.2.3.127
  - (c) 1.2.3.64
  - (d) 1.2.3.63
  - (e) 1.2.3.31 **Correct**
29. [1 mark] What subnet mask would be used with hosts in the 15.16.0.0/12 network?
- (a) 15.15.255.255
  - (b) 15.16.255.255
  - (c) 15.31.255.255
  - (d) 255.16.0.0
  - (e) 255.240.0.0 **Correct**

30. [1 mark] How many usable host addresses exist in the subnet 97.86.75.64/27?
- (a) 16
  - (b) 30 **Correct**
  - (c) 32
  - (d) 62
  - (e) 64
31. [2 marks] Which IP address is an actual subnet address?
- (a) 13.14.15.16/30
  - (b) 21.22.23.24/29
  - (c) 42.44.46.48/28
  - (d) 65.54.43.32/27
  - (e) all of the above **Correct**
32. [2 marks] What is the first and last usable address for 1.2.3.4/30?
- (a) 1.2.3.0 and 1.2.3.3
  - (b) 1.2.3.1 and 1.2.3.4
  - (c) 1.2.3.4 and 1.2.3.7
  - (d) 1.2.3.5 and 1.2.3.6 **Correct**
  - (e) none of the above
33. [3 marks] Given a starting network of 88.77.66.0/25 that is subnetted into 4 subnets, what is the broadcast address of subnet #1?
- (a) 88.77.66.0
  - (b) 88.77.66.63 **Correct**
  - (c) 88.77.66.127
  - (d) 88.77.66.191
  - (e) 88.77.66.255
34. [2 marks] Given a network address of 192.168.1.0/24, what is the maximum number of subnets you can create if each subnet must support sixty four (64) hosts?
- (a) 2 **Correct**
  - (b) 4
  - (c) 8
  - (d) 16
  - (e) 32
35. [2 marks] A starting network 64.32.16.0/24 is subnetted into smaller subnets. Given the subnet ID 64.32.16.48/28, which subnet is this?
- (a) #1
  - (b) #2
  - (c) #3 **Correct**
  - (d) #4
  - (e) none of the above

36. [2 marks] Given a starting network of 30.31.32.0/21, what is the number of usable hosts when subnetting to provide 8 subnets with as few extra subnets as possible?
- (a) 16
  - (b) 62
  - (c) 64
  - (d) 254 **Correct**
  - (e) 256
- 18 marks done/6 marks to go
37. [1 mark] Convert 201 to binary.
- (a) 1100 1001 **Correct**
  - (b) 1010 1010
  - (c) 1001 0011
  - (d) 0100 1010
  - (e) 1010 1010
38. [2 marks] Given the IP and Mask 177.136.223.178/11 determine the broadcast address
- (a) 177.136.223.255
  - (b) 177.136.255.255
  - (c) 177.139.255.255
  - (d) 177.159.255.255 **Correct**
  - (e) 177.255.255.255
39. [2 marks] Given a starting network of 218.37.124.0/24 that is subnetted into 4 subnets, what is the subnet ID for the first subnet?
- (a) 218.37.124.0/24
  - (b) 218.37.124.0/26 **Correct**
  - (c) 218.37.124.64/24
  - (d) 218.37.124.64/26
  - (e) 218.37.124.128/26
40. [1 mark] What is the broadcast address for a host with IP address 8.172.47.10/15?
- (a) 8.172.47.255
  - (b) 8.172.255.255
  - (c) 8.173.47.255
  - (d) 8.173.255.255 **Correct**
  - (e) 8.191.255.255
41. [1 mark] Which of the following addresses could **never** appear in a Wireshark capture?
- (a) 127.0.0.1 **Correct**
  - (b) 128.255.255.255
  - (c) 172.16.255.254
  - (d) 172.16.255.255
  - (e) 255.255.255.255