Model Question Keys for CS656-004 Final Exam.

March 12, 1999

Forward. The final exam is comprehensive. You should review all materials, starting from the very beginning of the semester. It is well advisable that you study the midterm review and the midterm itself and that you also review all homework problems before and after the midterm.

Disclaimer. Use the following questions as a help after having familiarized yourself with all course materials. Those questions are not comprehensive, meaning that some exam questions will not be like any of them — I guarantee it. Also there are questions in this document that go beyond merely memorizing and understanding course materials and that require some thinking; such questions are marked “(Challenging).”

Network Layer and Switching Technologies.

1. What are the differences between connection-oriented and connectionless network layer services?
   Ans. See Pages 3 and 4 of Network slides. Note that you should not assume a connection-oriented service is reliable and a connectionless service is unreliable.

2. Circle one or more of the following combinations that is feasible (not necessarily popular in the real world):
   - unreliable, connection-oriented transport service above an unreliable connectionless network layer
• reliable, connection-oriented transport service above an unreliable connectionless network layer

• reliable, connection-oriented transport service above a reliable connectionless network layer

• unreliable, connectionless transport service above a reliable, connection-oriented layer

Ans. All four combinations are possible and should be circled.

3. Compare and contract circuit switching with virtual circuit switching. (hint: you should be able to answer this type of questions for any two switching technologies.)

Ans. See page 9 of Switching Technologies

4. (Challenging) Based on what we described in class regarding ATM virtual circuit establishment, what is most likely routing method used by ATM networks (distance vector, link state, path vector)? Explain your answer.

Ans. Link-state routing, because the VC establishment process requires the ingress switch to come up with a complete path to reach the destination. (Note: if this were an exam question, I will be more flexible in grading: path vector routing can also provide complete path info and will be acceptable. In the real world LSR is used because it can better support multiple routing criteria, required by the different types of ATM services)

5. Define the following terms: PNNI, CBR, interated networks, and VCI.

Network Routing.

1. Circle the routing protocol(s) that is/are used by the Internet.
   OSPF
   PNNI
   RIP
   BGP

Ans. OSPF, RIP, and BGP
2. Circle the routing method(s) that uses broadcast for the exchange of information among routers.
   - distance vector
   - link state
   - path vector
   Ans. LSR

3. Circle the routing protocol(s) that uses link-state routing:
   - OSPF
   - PNNI
   - RIP
   - BGP
   - IS-IS
   Ans. OSPF, PNNI, and IS-IS

4. Consider the network topology shown on page 12 of IP Multicast slides (but discard the routing tables shown on the same page). Starting with an initial distance vector that contains exactly one entry which describes how to reach itself with cost 0, show the contents of distance vectors at all routers after B, C, and D in that order sending their vectors.
   \[ A: (A, -1, 0), (B, 0, 1), (C, 1, 2), (D, 1, 1) \]
   \[ B: (B, -1, 0), (C, 0, 1) \]
   \[ C: (B, 0, 1), (C, -1, 0), (D, 1, 1) \]
   \[ D: (B, 0, 2), (C, 0, 1), (D, -1, 0) \]
   \[ E: (B, 0, 3), (C, 0, 2), (D, 0, 1), (E, -1, 0) \]
   \[ F: (B, 0, 2), (C, 0, 1) \]

5. Give two disadvantages of distance vector routing.
   Ans. See page 16 of Routing.

6. Give two advantages of link state routing.
   (General hint: you should be able compare and contrast any two routing methods.)
   Ans. See pages 22 and 23 of Routing.
7. Explain the reason why path vector routing can avoid routing loop problems, which haunt distance vector routing.

   Ans. It can checks an advertised path for loops.

8. Use one sentence to define each of the following terms: LSA, flooding, and IS-IS.

**Internet Protocol.**

1. The OSI model has 7 layers. The Internet uses a different number of layers. List those layers, top to bottom.

2. Circle the hostid part of each of the following IP addresses:
   
   200.14.80.9
   10.192.8.20
   155.12.60.42

   Ans. 9

3. Name three most important network and transport layer protocols of the Internet and briefly describe their purposes.

   Ans. IP, UDP, TCP (see page 4 of Internet Architecture)

4. What is fragmentation? Which fields in the IP header are involved in fragmentation?

   Ans. see pages 15 and 16 of Internet Architecture

5. IP datagram headers include a 16-bit checksum which, somewhat surprisingly, is not a CRC code. How is the checksum generated? Also give the reason(s) why we use this method.

   Ans. Exclusive-OR. It allows incremental update of the checksum when some header fields need to be changed in the process of delivering the datagram. Specifically the TTL is decremented each time the datagram is forwarded by a router. Also the Fragment-Offset and Total-Length fields will have new values when a router fragments the datagram.
6. What is the purpose of ARP? Describe in 3 sentences how it works.
   Ans. See page 17 of Internet Architecture.

7. Define the following terms: AS, CIDR, RIP, DNS, and ARPANET.

**Queueing Theory**

1. Generalize the results of the T1-line example to show that, when \( N \) users share a communication link, packet switching is \( N \) times more efficient than circuit switching.
   Ans. Basically, you simply substitute 24 by \( N \).

2. Do problem #1 of HW# 3.
   My apology. I meant the first problem of HW #4. Here the answers.
   (a) they can be treated as independent queues because their customer arrivals are exponentially distributed, according to a property described at the beginning of the HW, their service times are exponentially distributed (this is because packet lengths are exponentially distributed) and the queues have infinite capacities. The “servers” is the two queueing systems are the communication links, which are the part that get the job/service, namely, transmitting packets, done.
   (b) 1000 packets per second
   (c) \( 0.8/(1 - 0.8) = 4 \)
   (d) \( 1/(2000 - 1200) = 1.25 \text{ msec} \)
   (e) \( 5 \times 0.4 + 1.25 \times 0.6 = 2.75 \text{ msec} \)
   (f) \( 4 + 1.5 = 5.5 \)

3. Consider the configuration shown below. Inter packet arrival times are exponentially distributed (mean rates shown in the figure). Packet lengths are exponentially distributed with average 250 bits per packet. We assume that the queue associated with port 0 has infinite capacity. Compute the average number of messages in the router, including the one that is currently under transmission.
Ans. The combined arrival rate $\lambda = 3000$ (this works due to a property of the exponential distribution we discuss in class). Service rate is $1,000,000/250 = 4000$. Utilization is $\rho = 0.75$. We have $N = 0.75/0.25 = 3$.

4. In the real world, what will happen to a packet that, when it arrives at a router, the router runs out of buffer space?

Ans. They get dropped. This is one of the reasons why the Internet is unreliable.

**Transport Layer and TCP**

1. Give four functions of the transport layer.

Ans. See page 2 of Transport

2. What item is found in a UDP datagram and a TCP segment, but is not found in the IP header?

Port number

3. Why does every byte in a TCP segment have a unique sequence number associated with it?

TCP provides stream delivery. Byte is the basic data unit, not packets.

4. How is the initial sequence number of a TCP connection selected?

According to the current time.
5. Describe how an outgoing TCP flow is limited by the network capacity (that is, slowed down if the network cannot sustain the current flow rate).

When network could not delivery the segments of the flow, it drops those packets. The source times out, and the multiplicative decrease machanism is in effective.

6. (Challenging) This problem is designed to help you gain further insight into the additive recovery mechanism of the TCP, which increases the size of the sliding window by 1 each time an ACK is received.

Consider a TCP connection between two machines X and Y. The round-trip time between the two machines is $T$. Assume that at time $t_0$, X’s window size is 1 and X sends the first segment (here we use the DLL convention that the size of a window is the number of packets it can hold). Answer the following questions.

(a) Determine the size of the window at time $t_0 + T$, the moment when the acknowledgment of the first segment arrives at X.
   Ans. $1 + 1 = 2$

(b) Let $W_1$, be your answer in the previous questions. X sends at time $t_0 + T$ $W_1$ segments. Assume that the time for X to transmit segments is negligible compared to the round-trip time $T$ and thus that all the acknowledgments of these $W_1$ segments will return to X by time $t_0 + 2T$. Determine the size of the window at that moment.
   Ans. $2 + 2 = 4$ (2 segments where sent at $t_0 + T$, and hence two ACKs are received at $t_0 + 2T$.

(c) Repeat the previous question for $t_0 + 3T$ and so forth, and find a general solution for $t_0 + n \times T$.
   Ans. $2^n$. Actually, the additive recovery mechanism allows the window to grow pretty fast!

7. (Challenging) Machine A uses a TCP connection to send a query to database server $S$ via a TCP connection. Both the query message and the server’s reply can be contained in one TCP segment. Determine the minimum number of TCP segments to the transaction. (Hint: you should try to include in connection establishment segments the request and the reply.)
Ans. 5 messages
A to B: connection request message including the database query.
B to A: connection acceptance message, which also acknowledges the query (note that when B receives the request message, the connection has not established at B and hence the query must be buffered in the sliding window of B and cannot be delivered to the database server)
A to B: connection confirmation message. When receiving the message, the TCP module of B considers the connection established and delivers the query to the database server.
B to A: the database server reply message, with FIN bit set to 1 (since the server knows this is the last segment of the connection).
A to B: an ACK to the server reply.
For A, the connection is closed when the final ACK is sent. For B, the connection is closed when the final ACK is received.

8. Define the following terms: multiplicative decrease, additive recovery, SYN, PSH, Nagle’s algorithm

Security

1. Point out the reason(s) why (35, 100) and (17, 100) is not a pair of legitimate RSA public/private keys.
   Ans. 100 is not a prime 35 and 17 does not satisfy the criteria we discussed.

2. Describe how Triple DES works.
   Ans. see page 11 of Network Security

3. Discuss the problem(s) when block ciphers, such as DES and IDEA, are used in true block cipher mode (that is, electronic code book mode).
   Ans. Blocks are encrypted and decrypted independently, enabling substituting individual blocks.
4. RSA algorithms are said to be much slower than traditional ciphers (such as DES and IDEA). With robust traditional ciphers at our disposal, what are RSA algorithms used for?

Ans. The advantage of RSA lies in the fact you don’t have to keep secret the key the other party uses to communicate with you. You can use RSA key to protect the exchanging process of the key of a traditional cipher, which is used to protect the messages (consider the PGP package).

5. What is the application of one-way hash functions, such as MD5, which cannot prevent a message from being read by the enemy?

authentication

6. Circle correct description(s) about RSA encryption.

- You pick two keys randomly, make one of the keys available to your friends, and keep the other to yourself.
  incorrect. The two keys must be mathematically related in the way we discussed in class.

- One way to enable your friend, upon receiving a message from you, to perform authentication is to encrypt the message with your private key.
  correct.

- Another way to enable authentication is to encrypt only the digest of the message with your public key.
  incorrect. Must use private key (otherwise, it has to be decrypted by the private key, which your communication partner does not have)

- To have both secrecy and authentication, you encrypt the message with both your private key and your public key.
  incorrect. Use your private key and the public key of your communication partner.

IP Multicast
1. Give two applications of multicast communications.

   See page 4 of Multicast slides

2. Which of the following multicast protocols involve the broadcast of group membership information: DVMRP, MOSPF, CBT?

   MOSPF

3. What is IGMP? Briefly describe its purpose.

   See page 6 to 8 of Multicast/

4. Using the network topology and routing tables shown on page 12 of IP multicast slides, answer the following questions.

   (a) Show the broadcast tree produced by the RPF algorithm when C is the source.

      Ans. C-D, B-C, E-D, A-D, F-C (note: you should focus on the routing entries from all other nodes to C, although the multicast flow is from C to others; this is why the algorithm is called “reverse path” forwarding)

   (b) Let M be the first multicast datagram from C. Count the number of times M is forwarded by routers, including the ones that are discarded by the receiver router.

      C performs 3 forwardings.
      B performs 1 forwarding, triggered by the forwarding from C.
      D performs 2, triggered by C
      F performs 0
      E performs 1, triggered by D
      A performs 2, triggered by D.

      The total is 9.

5. (Challenging) Compare and contrast the two broadcast methods we discussed in the course: RPF and flooding. (Hint: which one uses more bandwidth? which one depends on routing tables? which one has to remember the past, that is, to keep track of which broadcast has been received, and so forth)

   Ans. Flooding does not rely on routing tables; RPF does. With flooding, routers have to remember the past; with RPF, routers don't have to. Both methods use roughly the
same amount of bandwidth: they both have each router forward a broadcast message
to neighboring routers once.

6. Circle the multicast protocol(s) that involves Dijkstra's shortest path computation
algorithm:
   DVMRP
   CBT
   MOSPF
   Abs. MOSPF

7. Discuss the advantages and disadvantages of the source-rooted trees and shared tree.
   See pages 20 and 21 of Multicast

8. Argue against the following hypothesis: the core node of a CBT multicast tree with \( N \)
   members must have processed at least \( N \) JOIN-REQUEST messages (there could be
   more because some previous members may have quit).
   Since a JOIN-REQUEST message does not have to arrive at the core node, the core
   may not see all such messages.