Carnegie Mellon

Computer Science Dept.
Carnegie Mellon University

15-744 Spring 2001

Final Exam

Name: _Harry Bovik_

INSTRUCTIONS:

- There are 12 pages (numbered at the bottom) make sure you have all of them.
- Please write your name on this cover and at the top of each page in this booklet.
- If you find a question ambiguous, be sure to write down any assumptions you make.
- It is advantageous to partially answer a question than not attempt it at all.
- Be clear and concise. Limit your answers to the space provided.

SCORING:

A	B	C	D	E	F	Total
/24	/24	/20	/15	/15	/2	/100

NAME: _____

A. Multiple Choice - Circle ALL answers that apply (4 points each)

1. Which of the following is true about multicast routing?

(A) PIM-sparse mode uses the IP loose source routing to ensure that packets pass through the rendezvous point en route to all receivers.**(-2 pts)**

(B) Without truncation in a DVMRP network, packets are flooded throughout the entire network until routes are pruned back. **(+2 pts)**

(C) MOSPF routers must keep forwarding state for a group even when there are no transmissions to the group.**(+2 pts)**

(D) In PIM sparse mode, routers must keep a forwarding entry for each source in a group, i.e. a (S, G) entry. **(-2 pts)**

2. Which of the following is true about Mobile IP?

(A) It is a replacement for Dynamic Host Configuration Protocol (DHCP) in the sense that one should not use DHCP and Mobile IP at the same time. **(-4 pts)**

(B) It requires that the home agent be at most one IP hop away from the mobile host. **(-4 pts)**

(C) It provides a way to keep a TCP connection alive even if a host is mobile between different IP networks. **(+4 pts)**

(D) It does not work if both ends of a TCP connection are mobile hosts. **(-4 pts)**

3. Which of these is true about Freenet?

(A) It provides anonymity for both producers and consumers of information. **(+4 pts)**

(B) It guarantees permanent file storage. **(-4 pts)**

(C) Because its routing tables are based on key proximity, items that are about similar subjects are likely to be stored on the same node. **(-2 pts)**

(D) It always fetches a file from the physically closest server (with that file) on the network. **(-2 pts)**

NAME: _____

4. Which of the following is true of the Receiver-driven Layered Multicast (RLM) scheme?

(A) Shared learning, where one receiver learns about the state of the network from another's experience, is used to advance from a lower layer to a higher layer. **(-2 pts)**

(B) It is possible for a receiver to actually be experiencing congestion, but not drop a layer in response. **(+1 pts)**

(C) RLM requires that a "fast leave" feature be implemented in the multicast routers for it to function well. **(+1 pts)**

(D) Shared learning helps RLM scale to larger session sizes. **(+2 pts)**

5. Which if the following is true about the ANTS active networking system?

(A) ANTS cannot support routing protocols since capsules of different types cannot share state. **(-2 pts)**

(B) The use of the MD5 hash of the associated code as the type of a capsule prevents attackers from providing incorrect code for a capsule. **(+2 pts)**

(C) Active routers must use IP-in-IP encapsulation to tunnel capsules through non-active routers. **(-2 pts)**

(D) The active code associated with a capsule does not have to fit within a single packet. **(+2 pts)**

6. Which of the following is accurate about the four ad-hoc routing protocols, DSDV, TORA, DSR, AODV?

(A) AODV combines techniques from TORA and DSR to create an on-demand routing protocol based on virtual "heights". **(-2 pts)**

(B) DSDV maintains routing information in the absence of any traffic and is therefore not "on-demand" like the other protocols. **(+2 pts)**

(C) DSR typically imposes a higher routing overhead in bytes than AODV, due to the cost of carrying source routes in every packet. **(+2 pts)**

(D) TORA performs better than DSR at high mobility since its routing messages are delivered using a reliable protocol. **(-2 pts)**

NAME: _____

B. Short Answer (4 points each)

7. PIM sparse mode makes a separate tree for high bandwidth sources. What problem common in other core-based routing protocols does this solve?

Answer: In core-based trees all traffic is concentrated along a single shared tree - possibly causing congestion. By having per-source trees, PIM allows traffic to be more spread out in the network. Delay is also reduced (but typically only by a small factor) and this may not be critical for such applications. Answers about delay got 2 pts.

8. Answer the following about the SRM protocol.

(A) In SRM, the request-for-retransmission is multicast. Give **TWO** advantages of multicasting the request instead of unicasting it to the source.

Answer:
It enables the suppression of other requests for the same retransmission.
It allows nearby hosts that received the packet to retransmit instead of the sender.

(B) In SRM, the timers for requests and replies are randomized. What purpose does this randomization serve?

Answer: This improves the behavior of the suppression mechanism in SRM.Randomization is especially critical in topologies where clients are similar distances from the source.

9. Harry Bovik studied the Snoop protocol in 15-744 and makes the following claim:

"Under normal operating conditions with a Snoop basestation (no handoffs and no lack of buffer space in the basestation), the wireline TCP sender may timeout for a packet lost on the wireless link but will never fast retransmit it"

Is Harry's claim true or false? Explain why.

Answer: Harry is correct (for a change!). Snoop basestations will suppress all dupacks for packets it has received. This prevents the sender from fast retransmitting a packet. However, if Snoop spends too much time trying to retransmit the packet locally, the sender may timeout.

10. Why does the implementation of TCP using the Congestion Manager system (TCP/CM) use the asynchronous (request/callback) API instead of the buffered API?

Answer: The asynchronous API is used for applications that want to decide what to send at the last possible moment (just before a packet is sent out). The buffered API is for applications that are willing to choose the order of transmitted packets well in advance.At the last possible moment, TCP needs to choose between retransmitting old packets (based on timer expiration or dupack arrival) and tranmitting new data packets. This is why it uses the asynch API. Most people just described the difference in APIs not why TCP needs one or the other.

11. Consider a stock ticker application where getting messages from the sender at a rate of $> d_1$ bps is best (corresponding to a maximum utility U_m), and getting messages between d_1 bps and d_2 bps leads to continuous linear performance degradation from U_m down to zero. Receiving messages at less than d_2 bps is useless (zero utility). In a network dominated by this application, do you think admission control will help increase the aggregate utility? Explain your answer.

Answer: Yes, admission control will help. An obvious situation that admission control can fix is when the network is too crowded and all flows are getting 0 utility.

12. Harry Bovik happens to have two phone lines and two modems at home. He decides to use multi-link PPP to use the two connections he has in parallel. Basically, packets are sent in a round-robin fashion across the different links. He decides to download a simple packet-pair based bandwidth measurement tool to test his new setup. When he runs the test, the bandwidth reported makes no sense to him. Help Harry by answering the following.

(A) On average, should the tool report a higher, lower, or correct bandwidth value (correct = 2 x modem speed)? Why?

Answer: Typically higher. The two packets in the packet pair will be transmitted in parallel across the links. Therefore, they will arrive closer together in time than if they had been queued behind each other. The smaller spacing results in a higher estimate.

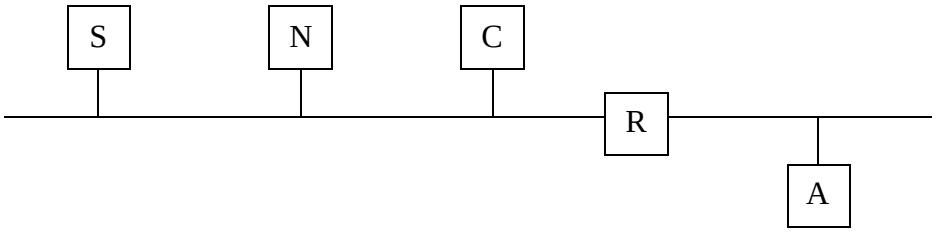
(B) What modification to the bandwidth measurement tool would provide a more accurate measurement?

Answer: Use packet bunch mode from Paxson's paper.

NAME: _____

C. Web Transfer (20 points)

In the topology shown below, machine A is a desktop client, N is a name server (but not the authoritative name server for S), C is a Web cache, R is a router and S is a Web server. Client A is configured to use Web cache C for all requests (assume that the Web cache resolves the name for any Web server and that the client is configured with the IP address of the cache). All wires/links are ethernet segments.



Assume the following:

- All the machines were just booted and their associated caches (ARP, DNS, Web, persistent connection) are all empty
- http://S/index.html fits in a single packet
- Persistent HTTP connections are used among A, C & S (i.e. you should assume that once any connection between these hosts is established it is never closed)

13. The user on machine A, requests the web page http://S/index.html. The table below shows a number of messages sent/received in servicing this request (this is not necessarily a complete list of all packets). In addition, there are a few bogus packets that are never sent/received. The packets are not listed in temporal order - fill in the order column to indicate the order in which each packet was sent/received (1=first, 2=second, etc.). Place an X in the order column if the packet is bogus.

Table 1: HTTP Request

ID	Src	Dst	Src Port	Dst Port	Protocol	Contents	Order
1	C	DNS root		DNS	UDP	query for S	**X**
2	A	C		Web Cache	TCP	get http://S/ index.html	**2**
3	N	DNS root		DNS	UDP	query for S	**3**
4	C	S		HTTP	TCP	SYN	**5**
5	C	S		HTTP	TCP	get index.html	**6**
6	S	A	HTTP		TCP	index.html	**X**
7	A	broadcast			ARP	who is R	**1**
8	C	A	Web Cache		TCP	index.html	**8**
9	N	C	DNS		UDP	address for S	**4**
10	S	C	HTTP		TCP	index.html	**7**

NAME: _____

14. Assume that C is an ICP enabled cache and has two sibling caches, D and E and that E has http://S/index.html cached.

(A) Assuming that no packets are lost, list all ICP messages that are generated. Assume that the ICP cache is configured to contact sibling caches before contacting the server.

Table 2: ICP messages

Src	Dst	Src Port	Dst Port	Protocol	Contents
C	**D**	**ICP**	**ICP**	**UDP**	**ICP Query**
C	**E**	**ICP**	**ICP**	**UDP**	**ICP Query**
D	**C**	**ICP**	**ICP**	**UDP**	**ICP Miss**
E	**C**	**ICP**	**ICP**	**UDP**	**ICP Hit or HitObj**

(B) As a result of the use of ICP, some of the entries in Table 1 would be modified. Use the table below to indicate these changes. Use the ID column from Table 1 to identify the messages. For messages where there is an **equivalent** in the ICP setup (e.g., DNS lookup for X replaced by DNS lookup for Y), enter the new message contents. For messages that are **completely** eliminated, just enter the message ID and the word "eliminated". Do not list any additional messages! You may assume that C is configured with the IP addresses for D & E.

Answer: 4,5,10 could be eliminated if you used HitObj in part A.

Table 3: HTTP Request

ID	Src	Dst	Src Port	Dst Port	Protocol	Contents
4	**C**	**E**		**Web Cache**	**TCP**	**SYN**
5	**C**	**E**		**Web Cache**	**TCP**	**get http://S/ index.html**
10	**E**	**C**	**Web Cache**		**TCP**	**index.html**
3	**Eliminated**					
9	**Eliminated**					

15. Assume that the client A has no Web or DNS cache and that cache C has no DNS cache. However, all other cacheable information is cached. On a subsequent request for http://S/ index.html which of the messages from Table 1 would be eliminated (use the ID column to name the messages)?

Answer: 3, 4, 5, 7, 10

NAME: _____

D. Integrated Services (15 points)

16. The table below shows the transmission schedule for a given flow. The table shows the number of packets sent in the first second and in each subsequent second. The flow must stay within the bonds of a token bucket filter. Assume the bucket is initially full of tokens. What bucket depth does the flow need for a token rate of 2 packets per second?

Table 4: Transmission Schedule

Time (seconds)	Packets Sent
0	5
1	5
2	1
3	0
4	6
5	1

Answer: 7. Assume an empty bucket - the maximum deficit is -7 in the 5th second (4 in table)

17. Suppose a router has accepted flows with the token bucket parameters shown in the table below. All flows are in the same direction, and the router can forward one packet every 0.1 second.

Table 5: Token Bucket Parameters

r	B
1	10
2	4
4	1

(A) What is the maximum delay a packet might face?

Answer: 1.5 seconds. The router can handle the steady rate of packets. However, the max burst is 15 packets = 1.5seconds. A common incorrect answer was 10 sec = B/r. This is Parekh's worst case bound in a bit-by-bit FQ system that is fully saturated.

(B) What is the minimum number of packets from the third flow that the router would send over 2.0 seconds, assuming that the flow sent packets at its maximum rate uniformly?

Answer: The maximum number of packets sent by all other flows = B + rt = (10 + 4) + (1 + 2) * 2 = 20. The router can forward 20 packets per second, so the third flow could send none if it is low priority. Based on assumptions on how tokens are generated, upto 3 packets could be sent.

NAME: _____

18. You are given the below input pattern for a router that implements all three service types (guaranteed, predictive and best effort). A non-empty row indicates a single packet was received for the particular stream, in the particular time period. Use the entry in the row as the name of the packet in your answer.

Table 6: Input Pattern

TIME (seconds) --->	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Stream A (Guaranteed)	A1	A2	A3		A4	A5	A6
Stream B (Predictive)	B1	B2	B3	B4	B5		
Stream C (Predictive)	C1	C2			C3	C4	
Stream D (Best Effort)			D1		D2		

Assuming fixed sized packets, an output link capacity of 2 packets/second, show the output pattern that could result (use the table below for your answer).

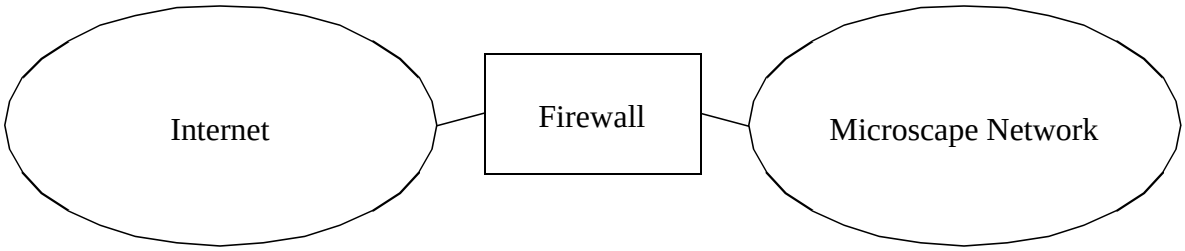
Table 7: Output Pattern

TIME(seconds)-->	**1**	**2**	**3**	**4**	**5**	**6**	**7**
packet 1	**A1**	**A2**	**A3**	**B3**	**A4**	**A5**	**A6**
packet 2	**B1/C1**	**B1/C1**	**B2/C2**	**B2/C2**	**B4**	**B5/C3**	**B5/C3**

NAME: _____

E. Firewalls (15 points)

Harry Bovik is given a job as network administrator for a Microscape. His first assignment is to setup a firewall for the company. He decides to use a simple packet filtering firewall. Unfortunately, Harry is not too familiar with firewalls and needs some help setting up his system. The topology of his network is shown below. The Microscape network uses 10.1/16 addresses.



Rules for this firewall are described using simple rules as shown in the table below. Both simple prefix matching (e.g. 128.32/16) and wildcards (*) are allowed. Packets that do not match any rule are discarded by default.

Table 8: Example Rules

Src Addr	Dst Addr	Src Port	Dst Port	Protocol	Action
128.32/16	*	*	telnet	TCP	discard
10.1/16	*	*	sendmail	TCP	allow

The first rule prevents hosts in the 128.32/16 network from telnetting into the Microscape network and the second rule allows hosts in the Microscape network to send mail to hosts in the Internet. These rules may effectively allow or disallow other traffic as well.

19. Write a simple rule(s) that allows Microscape employees to browse the Web. Make this rule(s) as restrictive as possible (i.e. it should not let other traffic into/out of Microscape if possible)

Table 9: HTTP Rules

Src Addr	Dst Addr	Src Port	Dst Port	Protocol	Action
*****	**10.1/16**	**HTTP**	*****	**TCP**	**allow**
10.1/16	*****	*****	**HTTP**	**TCP**	**allow**

NAME: _____

20. Suppose there were two hosts (A&B) inside the Microscape network. Assuming just the rules you added in question 19, Could an attacker in the Internet still perform a bandwidth denial of service attack that interferes with traffic between host A & B? Why or why not?

Answer: Yes, an attacker could still interfere. The attacker could send a flood of packets on port HTTP (80) to either A or B. These do not have to be part of an active connection. This is the weakness of simple packet filtering firewalls.

21. Harry installs an HTTP caching proxy in the Microscape network. He wants to ensure that all clients in Microscape use this proxy to browse the Web. How should he modify his rules from question 19 (you may write out the new rule or explain the changes)?

Answer: Replace all 10.1/16 with the proxy's IP address.

22. Assuming the resulting setup from question 21 and that the Web proxy is not on one of the links between host A & host B, can transfers between A & B be affected by a denial of service attack?

Answer: No. The proxy only forwards data to A or B (or into Microscape network in general) if it is part of an active Web request. Therefore, outsiders can send arbitrary amounts of traffic to the proxy but it will not affect the rest of the Microscape network

NAME: _____

F. Freebie (2 points)

23. What was your favorite part of 15-744?

Answer: Srini's exciting lectures. Any non-blank answer got a point.

24. What was your least favorite part of 15-744, other than the homework ;-)?

Answer: The best answer was to leave this blank ;-). Actually, any non-blank answer got a point.

THE END: HAVE A GOOD SUMMER!!