NAME:
Login name:

Computer Science 461, Final Exam
May 16, 2010, 1:00-3:00pm

This test has 10 questions. Put your name on ***every page except the last one***, and **write out and sign** the Honor Code pledge before turning in the test. The exam has 100 points and lasts for 120 minutes. Show your work for all problems. Partial credit will often be given.

"I pledge my honor that I have not violated the Honor Code during this examination."

Question	Score
1	/ 13
2	/ 8
3	/ 8
4	/ 9
5	/ 10
6	/ 7
7	/ 9
8	/ 16.5
9	/ 19.5
Total	/100

QUESTION 1: Network system engineering (13 points)

You have recently been hired by FinBook, the online social network for fish. FinBook currently runs on a single server. To support future growth, you hope to deploy multiple servers in multiple datacenters located at different points in the Internet, with a special focus on providing good performance and failure recovery. List some of the pros and cons of using each of the following technologies. Try to give the "best answer" and **be specific**. Vague comments such as "low overhead" will not get credit (overhead in terms of what?).

A) ***HTTP redirection***

1 advantage:

1 disadvantage:

B) ***DNS server-selection***

1 advantage:

2 disadvantages:

C) ***IP anycast***

2 advantage:

2 disadvantages:

D) ***NAT + load-balancer***

1 advantage:

1 disadvantage:

E) ***ARP spoofing***
(unsolicited announcement of your MAC with other's IP address)

1 advantage:

1 disadvantage:

QUESTION 2: More network system engineering (13 points)

(a) You graduated from Princeton (yay!) and joined a social media startup that wants to rival Facebook (at least you hope). The startup doesn't have any funding, so you took your implementation of simple router and are running it on a Linux box, using it as a router for your servers (instead of paying $$ to Cisco). As your company scaled, you started seeing some clients that use IPv6. Your servers understand IPv6, but your router doesn't. Describe two ways in which you can extend your router to handle IPv6 traffic:

Option 1: (answer <= 2 lines)

Option 2: (answer <= 2 lines)

(b) You are at Princeton for reunions and get a work phone call saying that the servers are running extremely slow and they believe the servers are under a DOS attack. You think this is your competitors (maybe Facebook is afraid of you after all!) and use your iPhone to ssh into your Linux machine. You remember that while implementing a flow table, 0 meant block and 1 meant allow. TCP's protocol # is 6 and UDP's is 17. What entries will you add in the flow table to do the following:

- Allow all TCP traffic from Princeton (128.112.0.0/16)
- Ban all traffic from 66.220.0.0/16
- Allow UDP traffic to server 69.65.28.126:3333

Your entries should have the following format:
<source IP, destination IP, protocol number, src Port, dst Port, 0 or 1>

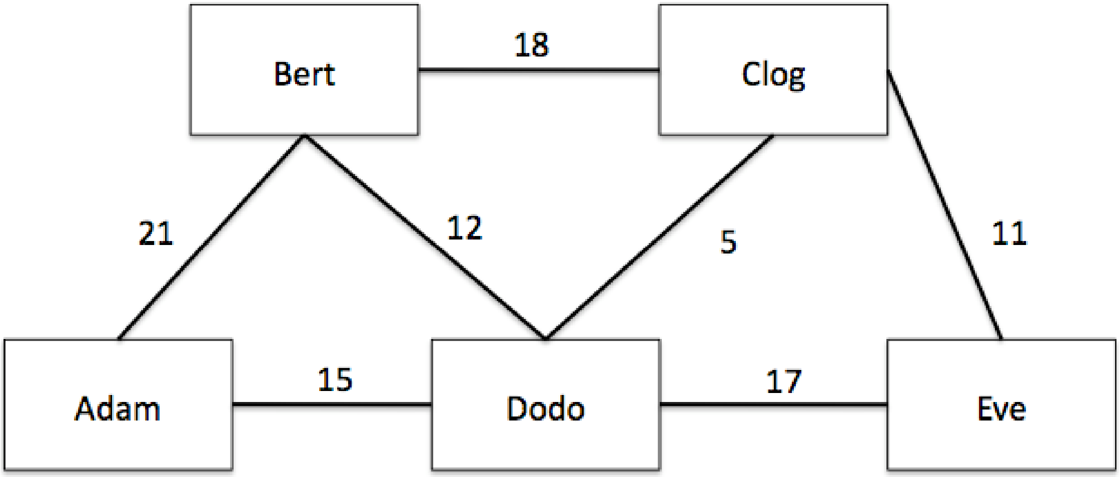
(c) Your company has grown and now has a couple of thousand users. You said farewell to the your simple router implementation and finally paid some $$ to Cisco. You have multiple servers and routers in your (small) datacenter now. One day you show up at work and find that some clients cannot connect to your servers. In a panic, you start dumping traffic on the ingress gateway router of the problematic servers and see the following packets (partial headers):

Ver	Length	TOS	TTL	Protocol	Source Addr	Destination Addr
4	38	0	250	17	139.133.217.110	69.65.28.126
4	40	0	214	06	121.69.24.120	69.65.28.126
4	84	0	249	01	18.69.204.150	69.65.28.126
4	55	0	250	06	192.0.0.15	192.0.0.0
4	84	0	243	01	18.69.204.150	69.65.28.126
4	84	0	249	01	128.109.24.10	69.65.28.127
4	84	0	237	01	18.69.204.150	69.65.28.126
4	40	0	208	06	121.69.24.120	69.65.28.126

What is going wrong? Or, explain why this information is useless.
(answer <= 2 lines)

QUESTION 3: Distance-Vector Routing (9 points)

The CS department at Princeton bought new Sun Fire V210 servers. They decided to run a distance-vector protocol for routing between these servers (even though it is a rather small network). They are currently configured as the picture below, with respective edge costs.



The CS staff asked for your help. Write down each step of building the distance-vector routing table for 'Eve' so they can compare it to the output of their implementation. You can use abbreviations e.g., 'A' for Adam and 'E' for Eve.

The initial routing table at node A is:

Destination	***Cost***	***Next Hop***
B	21	B
C	∞	---
D	15	D
E	∞	---

(a) Show the initial routing table of node E:

Destination	***Cost***	***Next Hop***
A		
B		
C		
D		

(b) Show the routing table of node E after one iteration of the algorithm:

Destination	***Cost***	***Next Hop***
A		
B		
C		
D		

(c) Show the routing table of node E after two iterations of the algorithm:

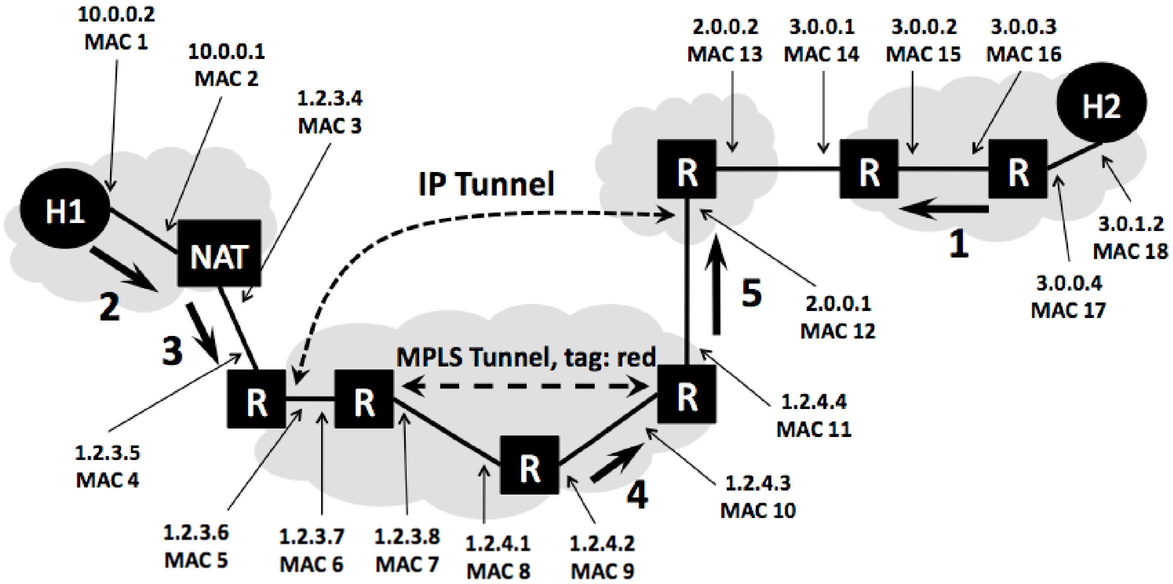
Destination	***Cost***	***Next Hop***
A		
B		
C		
D		

(d) In some failure situations, the administrator notices that it takes an exceptionally long time for the routing protocol to stabilize in this network.

(i) What problem with the distance vector protocol is the cause?

(ii) The administrator is told that BGP does not suffer from this problem. What prevents BGP from having this problem?

QUESTION 4: Routing, addressing, and tunneling (9 points)



The above figure shows a network topology connecting two LANs. The LAN on the left uses a NAT to connect to the Internet and includes a client host H1. The LAN on the right includes a webserver H2. Packets between the two LANs are routed along the path shown by a heavy dark lines, which includes both an IP tunnel and an MPLS tunnel. All packets which traverse the path use both tunnels. The various network interfaces have IP and MAC addresses as shown.

H1 has established an HTTP session with web server H2 and data packets are flowing between the two machines. As an example, we have filled in the headers for packet 1 (traveling from the server H2 to the client H1). If there shouldn't be any source or destination field for the header type, write an "X" in that table entry.

Header Type	*Source*	*Destination*
Ethernet	MAC 16	MAC 15
IP	3.0.1.2	1.2.3.4

You have to fill in the header type and the source and destination address for the network and data-link layer headers for packets 2, 3, 4, and 5 (these packets are all traveling from the client H1 to the server H2). Note: You might not need to use all the rows supplied.

(a) Header for packet 2:

Header Type	***Source***	***Destination***

(b) Header for packet 3:

Header Type	***Source***	***Destination***

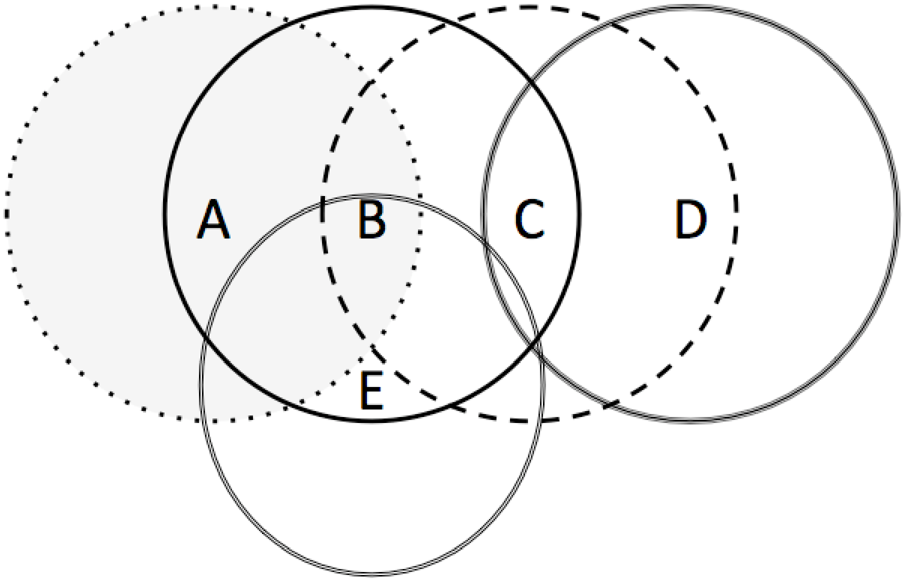
(c) Header for packet 4:

Header Type	***Source***	***Destination***

(d) Header for packet 5:

Header Type	***Source***	***Destination***

QUESTION 5: Wireless (10 points)



Consider the wireless topology above, comprised of 5 nodes. A (shown in the dotted, shaded circle), B, C, and D all have equi-sized transmission ranges, while E has a smaller range. Assume that if the transmissions of two nodes' will interfere at a location if and only if they transmit at the same time and their transmission areas overlap. In these problems, assume that losses only occur due to collisions.

(a) When node A transmits to node B, list the potential hidden terminals (in either direction, i.e., those who might clobber A's transmission or those who A's transmission might clobber) and exposed terminals.

Hidden terminals:

Exposed terminals:

(b) What about when node B transmits to node C?

Hidden terminals:

Exposed terminals:

(c) Suppose A is sending data to B and C is sending data to D, both at a constant bit rate equal to the physical capacity of the wireless channel ("as fast as they can").

(i) Assume that no mechanism is used to detect or avoid collisions. What is the throughput of each transfer as a fraction of its send rate? (No math required.)

A to B:

C to D:

(ii) Now suppose that each node uses CSMA/CA. Again, express the throughput of each transfer as a fraction of its send rate. (No math required.)

A to B:

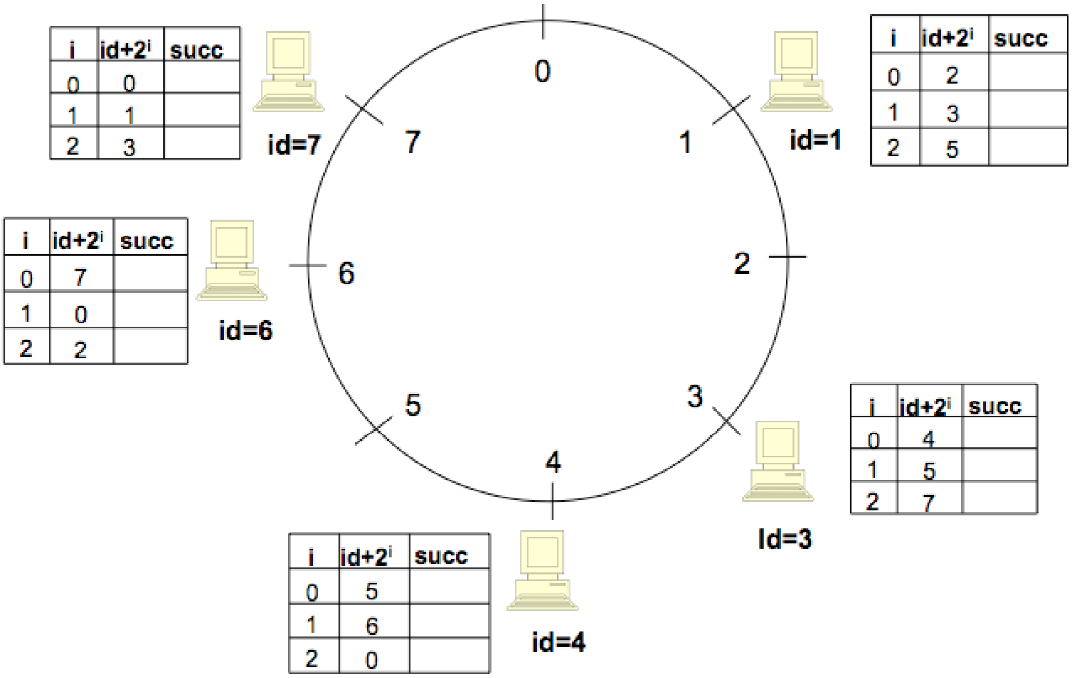
C to D:

(iii) Now assume that we also use an RTS/CTS scheme (like one we learned in class): An RTS is sent if and only if no other RTS or CTS has been heard recently, and the same goes for a CTS. Assume that RTS/CTS exchanges are small compared to data packets and have negligible overhead. Again, express the approximate throughput of each transfer as a fraction of its send rate. (No math required.)

A to B:

C to D:

QUESTION 6: Distributed Hash Tables (7 points)



i	$id+2^i$	succ
0	0	
1	1	
2	3	

i	$id+2^i$	succ
0	2	
1	3	
2	5	

i	$id+2^i$	succ
0	7	
1	0	
2	2	

i	$id+2^i$	succ
0	4	
1	5	
2	7	

i	$id+2^i$	succ
0	5	
1	6	
2	0	

Consider the above illustration of a Chord DHT, comprised of only 5 nodes. We show the finger tables for each node (i.e., the particular id distribution from which a node's routing table neighbors should be drawn), but we don't actually yet fill in the routing tables. Each node may be storing some items according to the Chord assignment rule (remember that Chord assigns keys to nodes in the same way as consistent hashing does, i.e., a successor mod N relationship).

(a) Fill in the routing table for the node with id 1 above.

(b) List the node(s) that will receive a query from node 1 for item 5 (i.e., the item named by key 5)

(c) Suppose node 4 crashes, and the network converges to a new routing state. List the node(s) that will receive a query from node 7 for item 5.

QUESTION 7: STCP (6 points)

You're up late at night, trying to debug an issue with your unreliable STCP implementation. Basically, your client connects to the server and downloads a file perfectly, but the next client connection to the server hangs. After several rounds of trial and error hacks, you decide to sit down and figure out the issue once and for all.

(a) To start out, write down the state transitions and sequence numbers for the socket connection between client and server. Note that the seq = sequence number of the first packet sent in the given state and ack = last ack sent. The client ISN is 1000 and the server is 2000. You should fill out those entries with a "*" in its box.

client	state	seq	ack
socket()	CLOSED		
connect()	SYN_SENT	1000	*
send/recv()	*	*	*
close()	FIN_WAIT_I, FIN_WAIT_II	*	10002
	CLOSED		

server	state	seq	ack
socket()	CLOSED		
bind()	CLOSED		
listen()	LISTEN		
accept()	*	*	*
recv/send()	*	*	1051
close()	CLOSE_WAIT, LAST_ACK	*	*
	HANG!		

(b) Then you realize: wait, the server never reaches the CLOSED state. Of course! It's because STCP is missing a state from the TCP FSM. Which state is missing?

(c) Hmm...but why can the second client still connect even though the server doesn't fully close its connection?

(d) Ok, so why would this missing state, under unreliable conditions, cause the server to hang and fail to enter the CLOSED state?

QUESTION 8: Multiple Choice (16.5 points)

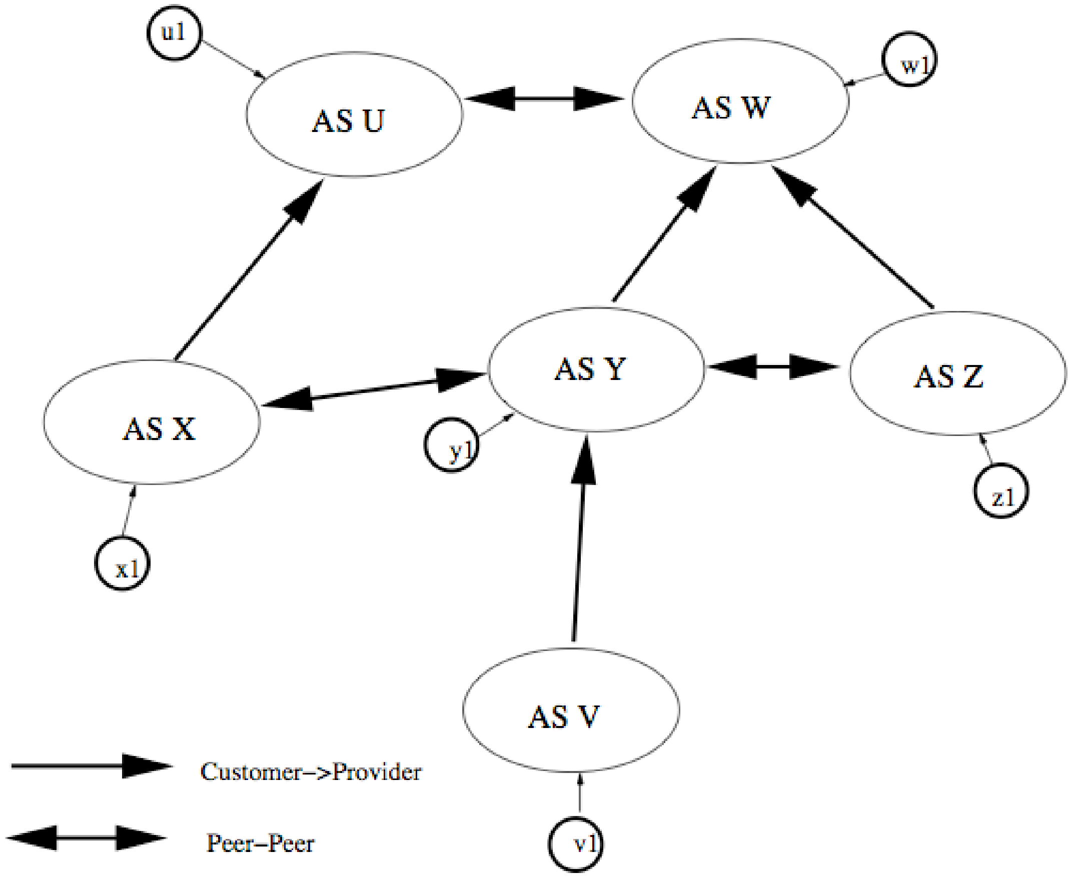
1) Which of the following about multicast is/are true? (circle ALL that are true)
   (a) The primary goal of multicast is to deliver the same packet to multiple destinations more efficiently than unicast.
   (b) Application-level multicast is more efficient than IP multicast.
   (c) Application-level multicast requires router support.
   (d) IP Multicast can easily use TCP as a transport protocol to achieve reliability.
   (e) In IP multicast, multicast-enabled routers must keep a list of all clients interested in the multicast group. This is necessary to properly route data.

2) Which of the following about wireless networks is/are true? (circle ALL that are true)
   (a) All wireless networks must use access points.
   (b) The sender can always detect a collision without feedback from receiver.
   (c) Collisions can still happen when RTS/CTS mechanism is used.
   (d) TCP congestion control mechanisms are well designed for wireless environments.
   (e) Wireless networks generally have higher loss rates than that in wired networks.

3) We discussed three different routing protocols: link state routing (LS), distance vector routing (DV), and path vector routing (PV). Answer each of the following by circling each protocol (LS, DV, and/or PV) for which the claim is TRUE:

   (a) LS, DV, PV - Requires flooding
   (b) LS, DV, PV - Requires a map of the complete topology
   (c) LS, DV, PV - Sends its routing table to its neighbors
   (d) LS, DV, PV - Suffers the count to infinity problem
   (e) LS, DV, PV - BGP builds on this type of routing protocol

4) In the network depicted below, which paths may packets take between a pair of end-hosts under normal BGP routing policy assumptions (i.e., the Gao-Rexford model, which includes valley-free routing)? (circle ALL that are true)



(a) x1 → AS X → AS Y → AS Z → z1

(b) x1 → AS X → AS U → AS W → AS Y → AS V→v1

(c) v1 → AS V → AS Y → AS Z → z1

(d) v1 → AS V → AS Y → AS Z → AS W → w1

(e) u1 → AS U → AS W → AS Y → y1

5) Mike is traveling to a conference, and so only finished writing the exam while on the road. He needs to send the exam to the course TAs, who will be administering the exam. Unfortunately, Mike knows how creative Princeton students can be, and he even thinks some students work at OIT and thus can login to Princeton's routers. He's concerned that the real exam might fall into student hands or be replaced by a false or old exam! Thankfully, Mike has several options to use cryptography for security. At the beginning of the class, both Mike and Muneeb exchanged a shared symmetric key *k*. Also, both use PGP and know each other's public PGP key (PK_{Mike} and PK_{Muneeb}), corresponding to the public/private key pairs (PK_{user}/SK_{user}). Assume that no keys have been compromised.

For each of the following, consider whether the exam can be stolen or replaced. Circle either YES or NO for each property.

(a) Mike signs the exam with SK_{Mike} and sends it.

i) Can be stolen? YES or NO

ii) Can be replaced? YES or NO

(b) Mike encrypts and MACs the exam with the shared secret *k*.

i) Can be stolen? YES or NO

ii) Can be replaced? YES or NO

(c) Mike realizes that he lost a copy of Muneeb's public key, so he goes on the COS-461 website and downloads Muneeb's public key PK. He then encrypts the exam with this key PK, signs it with his private key SK_{Mike}, and sends it.

i) Can be stolen? YES or NO

ii) Can be replaced? YES or NO

(d) Mike decides to get a little fancy and create his own cryptographic protocol. So before Mike sends the exam *M* to Muneeb, he first calculates $H = Hash(M)$ using a well-known hash function such as SHA-1. He then transmits the tuple (M, H) to Muneeb. Upon receiving this tuple, Muneeb calculates $H' = Hash(M)$, and only accepts the exam as valid if $H == H'$. You can assume that *Hash* is cryptographically strong (i.e., one-way, collision and pre-image resistant).

i) Can be stolen? YES or NO

ii) Can be replaced? YES or NO

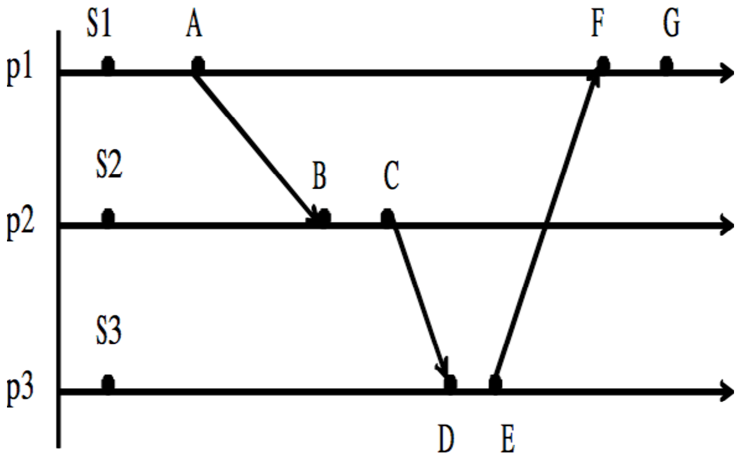
QUESTION 9: Short Answer (29 points)

1) HTTP and content distribution networks

(a) Which scenario benefits the most from using persistent HTTP connections, as opposed to establishing a new connection per HTTP request: Web pages with large objects or pages with small objects? Give two brief reasons why.

(b) Most browsers don't have pipelining turned on by default. Ignoring implementation complexity reasons, describe why pipelining might not always give better performance. Be specific (but brief).

2) Clocks



Processes 1, 2, 3 are using a logical clock to keep a consistent time. The horizontal arrow represents physical time and the crossing arrow represents a message being passed. Each point on the horizontal lines is an event.

(a) (Lamport Clock) You find out that the processes above are using Lamport's logical clock, but not all the clock values are not known to you. The initial logical time S1, S2 and S3 were 11, 1 and 0 respectively, and you observe that the clock was 16 at E. What is the value of the clock at A, B, C, D, and F?

A	
B	
C	
D	
F	

(b) (Vector Clock) This time, you find out that the processes are using vector clocks, but not all values are known. The initial time S1, S2 and S3 were (0,0,0) , (0,1,0) and (0,0,11), respectively. What are the values for A, B, D, E, and F?

A	
B	
D	
E	
F	

3) Suppose host A is sending to a multicast group. The recipients are leaf nodes of a tree rooted at A with depth 3. The tree is full and perfected balanced, with each non-leaf node having 2 children. Thus, there are $2^3 = 8$ recipients.

(a) How many more individual link transmissions are involved if A sends unicast messages to each individual recipient, as opposed to multicasting the message?

(b) Muneeb realizes that the quality of the multicast stream is actually quite poor, so he wishes to add reliability to the transfer. He decides to invent his own reliable multicast protocol and asks you to help him decide between a few alternatives. For each, describe under what condition this approach works ***well***.

Have each client ACK or NAK (negative ACK) each received message.

(i) ACK

(ii) NAK:

If the sender fails to get an ACK (or receives a NAK), it can re-multicast the message to the entire group, or unicast it to particular senders.

(iii) multicast

(iv) unicast:

(c) If you decide to use the NAK and multicast approach, describe two optimizations for multicast receivers on the same LAN that can reduce the amount of work by the sender to ensure reliable delivery.

4) David is hired by a local company to set up a router that both serves as the network's firewall to the Internet and also NATs hosts in the corporate network.

(a) The corporate network consists of about 75,000 machines that simultaneously access the Internet using port-based NAT. Assume that users of these machines do a lot of intensive Web surfing throughout their workday. What problem does David point out could arise if the corporate network only has a single public IP address?

(b) The company wants to run a Web server on a machine behind the firewall. It desires to make this accessible from the public Internet. However, they wish to continue using a single external IP address. How can David set this up?

4) Easy final half-point!

Name one of the authors of your course textbook. (Hint: one of the authors is a professor in the computer science department at Princeton.)