

CSE 123B Communications Software
Spring Quarter, 2002
Final Exam

Instructor: Stefan Savage

Name _____
Student ID _____

Attention: This exam has 6 sections worth a total of 93 points. You have 165 minutes (2:45) minutes to complete the questions. As with any exam, you should read through the questions first and start with those that you are most comfortable with.. If you believe that you cannot answer a question without making some assumptions, state those assumptions in your answer. For partial credit, be sure to show how you arrived at your answer as well as the answer itself.

1	/12
2	/18
3	/15
4	/18
5	/12
6	/18
Total	/93

3. (15 points) TCP issues

- a) TCP acknowledgements are not reliable – they are not retransmitted if they are lost in transit. Assume that 50% of all TCP acknowledgements are lost. Does this affect the reliability of a session? If so, in what way? Does this impact congestion control? If so, in what way?
- b) The well known utility called “ping” allows a host to measure the round-trip time to some destination by sending an ICMP Echo Request packet to the destination and measuring the time until an ICMP Echo Response packet arrives from the destination in response. However, for security reasons, such ICMP packets are increasingly being blocked and ping cannot always be used (this is why you can’t ping www.microsoft.com for example). An alternative strategy would be to build a similar tool that used TCP packets for round-trip-time measurements instead. Describe how you might make this work (there are multiple ways to do this, but don’t forget about delayed acknowledgements on the receiver). Draw a picture of the protocol interactions (like the diagrams we’ve used in class).

4. (18 points) Putting it all together

One day your friend calls you up and says “Dude, I just bought the domain name ucsdrocks.com, and I’ve got a bitchin’ Web page going on there. Check it out!”. You direct your browser to www.ucsdrocks.com after which you become the first person on the planet to read 10,000 bytes of text promoting the virtues of combining beer, sunbathing and homework. You find that the page also contains a 3,000 byte embedded image of your friend doing just that. Describe, completely, the series of packets that will be sent to and from your host to produce this Web masterpiece. You may make the following assumptions: The maximum packet size is 1500 bytes. No IP or TCP options are used. Routing is stable and no routing packets are required. No packets are lost. Your Web browser supports only one connection at a time, opens a new connection for each object and does not implement pipelining.

(12 points) Web caching & CDNs

- a) Name three advantages of Content Distribution Networks over traditional Client/Server systems.

- b) Your bonehead friend gets hired (somehow) into the IT department of a small high-tech startup company in Sorento Valley which shares office space with several other firms. Your friend is charged with reducing the amount of money spent on Internet bandwidth. He notices that the company uses a Web cache to reduce the number of redundant requests for Web content. Since the current Web cache only has a 30% hit rate with a 100Mbyte disk, he figures that he can get significant improvements by increasing the size of the disk to 1Gbyte. What advice do you give him about this approach and what other options might you suggest?

(18 points) Security issues

- a) Describe the following security properties: confidentiality, authenticity and integrity. What technologies are used to achieve each?

- b) In class we discussed the ACK division attack on TCP congestion control in which a receiver sends multiple acknowledgements for each packet covering a portion of each packet. Describe why this attack works and how might you prevent this attack from working without changing the TCP protocol itself (i.e. by only changing the implementation of TCP at the sender)

- c) Network worms take over a host by exploiting some vulnerability in a network service (e.g. a bug in Microsoft's Web server) and then propagate themselves by infecting other hosts on the network. Typically, the worm will try to spread itself by picking a random IP address and probing it to see if the associated host has the vulnerable service. If it does, the worm infects the new host and then both machines continue to spread to other hosts. In this manner, a large number of hosts can be compromised very quickly. Describe how this kind of worm activity might bias the "backscatter analysis" approach to detecting denial-of-service attacks described in class. How might you distinguish worm traffic from denial-of-service backscatter packets?