CSCI 356 – Computer Networking – Exam 2 Review – Spring 2017

Topics: Mostly TCP, but also DNS, DDOS attacks, and UDP. We have covered all of Chapter 3, except ATM/ABR networks (3.6.3). Nearly all review questions and exercises from that chapter are suitable study material for the exam. TCP is full of surprises, so I expect this exam to be a challenge. You should be familiar with each one of these terms (what it means, how it is used in TCP, what tradeoffs it might entail, etc.):

- Handshaking, SYN and FIN flags
- TCP header, checksum, sender port number, receiver port number
- Sequence number, acknowledgement number
- Cumulative ACK, Piggybacked ACK
- Delayed ACK
- Congestion control, flow control
- Receiver window, advertised window, congestion window, send window
- Slow start, congestion avoidance, fast recovery, timeouts
- RTT Probing, Exponential Weighted Moving Average (EWMA), Exponential Backoff
- Bandwidth Delay Product, Additive Increase Multiplicative Decrease (AIMD)
- Triple-duplicate ACK
- Congestion collapse, buffer bloat
- Nagle's Algorithm

You do not need to memorize exact numeric details (e.g. the layout of the TCP header fields, or the specific parameter values used for EWMA).

Format will be similar to HW4 and HW5. See the solutions (to be posted on the web site). Below are a few review questions culled from various sources. I do not have solutions for these, but am happy to discuss by email or in person before the exam.

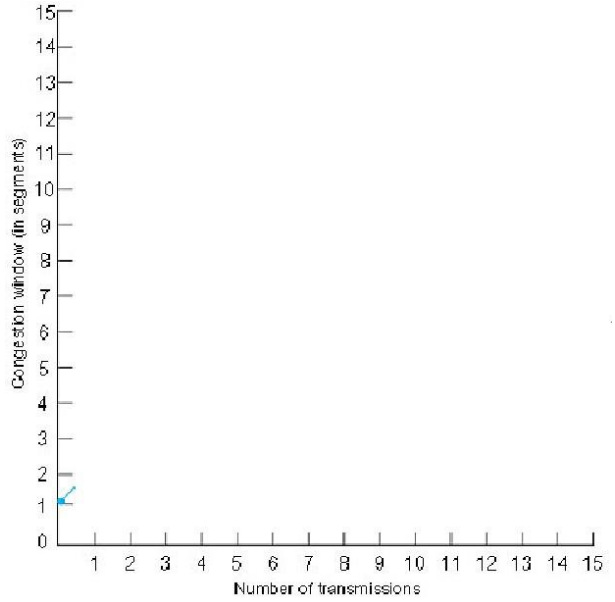
[Some questions courtesy Illinois CS 241]

Review Question 1. Consider the TCP connection establishment protocol. How many segments are sent? Which of these segments are client initiated? In the first segment, which flag bits are set?

Review Question 2. Consider hosts A and B communicating over a TCP connection. Assume unrealistically that the initial sequence number for each of A and B is 0. Assume that all segments sent between A and B have 20 byte headers. A sends B a segment with a 20 byte payload, B responds with a segment with a 30 byte payload and then another segment with a 40 byte payload, and finally A responds with a segment with a 50 byte payload. Give the value of the sequence number field and acknowledgement number fields for each segment.

Review Question 3. Consider TCP congestion control. Assume we have a round trip time RTT of 2 seconds. Assume that the segment size is 1 kilobyte. Assume that the bandwidth of the connection is 100 kilobits per second. What is the smallest window size for which there will be no stalling ("gaps" in sending) ? Show your work.

Review Question 4. Fill in the following graph showing the congestion window size for TCP Reno assuming that the initial ss-threshold is 8 and that a loss event will occur when the window size is 14. Recall that TCP Reno employs the fast recovery mechanism that skips slow start after a loss.



Review Question 5. Assume that you have 3 long lived TCP connections over a single bottleneck link with bandwidth R. With only this information, the average (over a long time) bandwidth that each connection receives would be expected to be about how much? Does your answer change if you are told that one of the connections has an RTT of about 60ms, while the other two connections have RTTs closer to 30ms? Explain (or illustrate) your reasoning. [we will cover this in class on Tuesday after Easter].

Review Question 6. A UDP header has four fields. Name or describe them, and name the purpose for each header field.

Review Question 7. A TCP header has several fields. Name or describe several of the more significant fields, and name the purpose for each.

Review Question 8. Assume a TCP process A first measures the actual round trip time to another TCP process to be 30 ms, and A thus sets its estimated round trip time to be 30 ms. The next actual round trip time that A sees is 60 ms. In response A increases its estimated round trip to 50 ms. The next actual round trip time that A sees is 40 ms. What is the next estimated round trip computed by A? Justify your answer.

Review Question 9. How does TCP detect corrupt segments? What happens after a corrupt TCP segment is detected? How does UDP detect corrupt datagram? What happens after a corrupt UDP datagram is detected?

Review Question 10. Does DNS use TCP or UDP? Give a few reasons why this choice is sensible. Name at least drawback of this choice, and explain how DNS overcomes or avoids that drawback.

Review Question 11. For the entire Internet, there are less than 20 root name servers. Each of these servers can handle less than 10,000 simultaneous requests, meaning that less than 200,000 simultaneous DNS lookups to the root name server can be made at one time. However, there are tens of millions of simultaneous DNS requests made on the Internet. How is this possible?

Review Question 12. A client wants to look up the IP for hostname www.illinois.edu. Assuming that no information is cached, what all name servers need to be contacted in order to resolve this host name into an IP address? Say what glue records (if any) will likely be needed as part of the resolution.

Review Question 13. Describe one way an attacker could interfere with DNS. Be specific – what specific actions would the attacker take, what packets or connections or operations would be involved, and how specifically would that affect DNS servers or clients. Choose an attack that is specific to DNS, i.e. an attack that relies on some DNS-related feature or protocol, rather than an attack that would affect networks or hosts in general.

See also TCP questions here:
http://pages.cs.wisc.edu/~akella/CS640/F07/work/midterm2.pdf