Network Systems (201600146/201600197), Test 4

April 9, 2018, 13:45–15:15

Answers (updated 2018-04-13)

1. Congestion control

1 pt (a) A.

1 pt (b) B.

1 pt (c) A.

1 pt (d) C.
This is not discussed in the book, but it was discussed at the lecture (see slides 19 – 21 of the lecture on congestion control), and at a tutorial exercise where you went through this fast recovery procedure step-by-step.
Answer E was often chosen, but is wrong: the lost packet is at the beginning of the window (everything before it has been acknowledged, so the window can move on to no longer contain those sequence numbers), so there's no need to enlarge the congestion window for it to be contained.

2 pt (e) For each received ACK, check how many new bytes it acknowledges, say n. Then increase the cwnd by n. As a result, it takes acks for a total of MSS bytes for cwnd to advance by 1 MSS.

Alternative: keep track of which sequence numbers were a segment boundary, and only increase cwnd by 1 MSS when an ack passes a segment boundary.

1 pt (f)

$$\frac{(0.25+0.75)^2}{2\cdot(0.25^2+0.75^2)} = 0.8$$

The formula is on page 491 in the book, easily found via the index. I was surprised how many students (not called Jain) invented their own formulas.

1 pt (g) A.
The text on page 519 of the book explains this.
Many chose B. This is not totally incorrect, but the notification is only very slightly faster than detecting congestion via packet loss and a triple duplicate ack. This is because the ECN notification still has to travel to the destination and be echoed back to the source. So the only gain is that the sender doesn't have to wait for the 2nd and the 3rd duplicate acks to arrive, as the ECN notification could be on the first ack that would otherwise be a duplicate ack.

2. QoS

1 pt (a) B.

1 pt (b) C.

1 pt (c) C.

1 pt (d) B.
Fair queueing tries to fairly divide the total 100 Mbit/s, so that's 50 Mbit/s per flow, when there are packets of both classes in the queue. However, the red flow uses only 40 Mbit/s, so part of the time there are no red packets in the queue. At those moments, all bandwidth is available for blue. Thus, blue gets at a total of 60 Mbit/s.

1 pt (e) D.

1 pt (f) F.
The largest amount the source could send in a 1 ms interval, occurs if it has been quiet before that 1 ms

interval. In that case, the bucket is full at the start of the 1 ms interval, so 2000 bits can immediately be sent. Furthermore, during the 1 ms interval another 1000 tokens arrive, so 1000 more bits can be sent. Thus, in total 3000 bits can be sent during this interval.

1 pt (g) C.
Note that such a token bucket specification is only a maximum of how much the source is allowed to send. It is allowed to send less.

---

3. Security

1 pt (a) C.
Note that only the encryption of the *message* is omitted. A man-in-the-middle could change the message (because that is not encrypted), but he cannot adapt the signature to match (for that, he would need to have the sender's private key).

1 pt (b) A.
The sender is authenticated to the receiver when the receiver verifies the digital signature: he trusts that only the sender has the private key needed to construct this signature.
The receiver is authenticated to the sender in the sense that only the intended receiver has the private key needed to decrypt session key and hence the message; thus, the sender can be sure only the intended receiver will be able to decrypt the message.

1 pt (c) B.
Note that the server is authenticated using certificates etc., but there's nothing which authenticates the browser to the server in HTTPS. (That's why you need to e.g. enter a password when logging in to a service on the web: there's no other mechanism for the server to know whom it's talking to.)

1 pt (d) B or F.
TCP connections started from within the company will use a random source port number above 1024. The packets returning for these connections will have that as their destination port number, so those must not be blocked by the firewall. Hence answer B.
A stateful firewall, which can distinguish between connections set up from outside and those set up from inside the company's network, would of course also work. But it is not *needed* here: since the only stated requirement on the firewall is that it blocks access to the file server on port 137, the stateless firewall configured according to answer B suffices.
The formulation of answer F, using the word "need", was intended to imply that it should only be chosen if none of the other options would be good enough. But since this was not totally clear, we've also accepted answer F.

1 pt (e) E.
A is false because for a DDoS the contents of the packets don't matter, so the same sequence number can be used.
B is false because for a DDoS the contents of the packets don't matter, so there's no need to synchronize the sequence numbers (and anyway, TCP sequence numbers from different hosts don't need to be synchronized even for normal, non-DDoS, traffic).
C doesn't make sense because for a DDoS you simply want to send a lot of data; waiting for the ack for your previous packet will only slow your DDoS down, and in fact if the DDoS is effective, you won't even get the ack!
D is simply not true; there's no reason why TCP packets are larger than UDP packets.

1 pt (f) D.
The webcam listens on some IP address and TCP port number; the firewall could be configured to drop packets destined for that address and port number.