Network Systems (201600146/201600197), Test 3

March 22, 2019, 13:45–15:15

- This is an open-book exam: you are allowed to use the book by Peterson & Davie and the reader that belongs to this module, and the handout about peer-to-peer communication (i.e., the part of the Kurose&Ross book distributed via Canvas). Furthermore, use of a dictionary is allowed. Use of a simple (non-graphical) calculator is allowed.
- For accessing the on-line books, use of the UT-provided Chromebook is allowed.
- Other written materials, and laptops, tablets, graphical calculators, mobile phones, etc., are not allowed. ***Please remove any such material and equipment from your desk, now!***
- Visiting the toilet without explicit permission of the supervisor is not allowed. During the last 30 minutes of the exam, no toilet visits are allowed.
- Write your answers to open questions on this paper, in the provided boxes, and hand this in.
- Questions marked with (MC) must be answered on the separate multiple-choice form, at the number indicated in the circle.
- Total number of pages: 6.
- Total number of points: 30.

Your name:

(please underline your family name (i.e., the name on your student card), so that we know how to sort)

Your student number:

1. Addressing and IPv6

3 pt (a) For each of the following IPv6 address notations, choose one of the following answers:

A. This is not a valid IPv6 address.
B. This is a valid IPv6 address, but it does not belong to the `1200:5678:9000::/18` subnet.
C. This is a valid IPv6 address, and it belongs to the `1200:5678:9000::/18` subnet.

MC01 `::1`

MC02 `12:5678:9:1::0`

MC03 `1200:4000:9000::0`

MC04 `1200:5678::face:1:0`

MC05 `1200:5678:9000:1:2:3`

MC06 `1200:5678:9000::1:0::`

MC07 `1200:7678:1::0`

MC08 `1200:9678:1::0`

MC09 `1200:5678:face::1:0`

1 pt (b) Consider the use of tunnelling to provide IPv6 connectivity over an IPv4-only network. What consequence does this have for the MTU (Maximum Transfer Unit, i.e., maximum unfragmented packet size)?

MC10

A. The MTU for IPv6 will be smaller than the MTU for IPv4.
B. The MTU for IPv6 will be the same as the MTU for IPv4.
C. The MTU for IPv6 will be larger than the MTU for IPv4.
D. This depends on whether the IPv6 header is larger or smaller than the IPv4 header.
E. The MTU depends on the end hosts, not on the network.

1 pt (c) Could one apply the HD ratio also to *part* of the Internet, e.g., the network of a single university having a single /16 IPv4 address block?

MC11

A. No, as the numerator of the HD ratio would not be well-defined.
B. No, as the denominator of the HD ratio would not be well-defined.
C. Yes and no: one can compute it, but the result would be meaningless as a /16 is only part of the total address space.
D. Yes, it would be a good measure for how tight the address allocation within that university is, and the threshold for when the allocation becomes problematic would still be about 87%.
E. Yes, it would be a good measure for how tight the address allocation within that university is, but the threshold for when the allocation becomes problematic needs to be adjusted because the network is smaller.
F. Yes, but it would still be a measure for how tight the address allocation *outside* that university is.

1 pt (d) It is to be expected that there will never be more than 2^{64} computers in the world, so 64 bits should suffice for the addresses. But IPv6 addresses are very much longer that 64 bits. Why?

MC12

A. This makes it possible to use hexadecimal notation, which is handy for giving hosts recognizable addresses like `2001:1234::face:b00c`.
B. If we made the addresses shorter, much space in the IPv6 header would be unused and thus wasted.
C. This makes systematic address allocation possible, to reduce the forwarding table sizes.
D. This is needed to make full use of the Hop Limit field, which can represent numbers up to 128.
E. Politics: the Animal Rights party demanded that every animal can get its own subnet.

1 pt (e) Compare fragmentation in IPv4 and IPv6. What happens if all ICMP packets are blocked (e.g., by an overzealous firewall) ?

MC13

A. Fragmentation will still work fine for both IPv4 and IPv6.
B. Fragmentation will fail for IPv4, but work fine for IPv6.
C. Fragmentation will fail for IPv6, but work fine for IPv4.
D. Fragmentation will fail for both IPv4 and IPv6.
E. Long IPv4 packets will be converted to IPv6 fragments.
F. Long IPv6 packets will be converted to IPv4 fragments.

Continued on next page...

2. Routing

We consider a distance vector routing algorithm without *split horizon* or *poison reverse*. We consider a node A, which has links to two other nodes: a link to node B with link cost 1, and a link to node C with cost 2. Let us now assume that node A receives a packet from B containing the following distance vector: (B, 0), indicating that B currently only knows a path to itself at cost 0. Likewise, A will receive from C: (C, 0).

1 pt (a) Which is the distance vector that A will send back to B and C? Please use as notation: (N_1, c_1), (N_2, c_2), etc., where N_i is the name of the i-th node in the distance vector, and c_i is the cost to N_i, just like it is done in the rest of this question.

Subsequently, A receives a new distance vector from B: (B, 0), (A, 1), (C, 100), (D, 200). Furthermore, it receives from C: (C, 0), (A, 2), (B, 100), (D, 5).

2 pt (b) Which is the distance vector that A will now send to B and C?

Subsequently, A receives a new distance vector from B: (B, 0), (A, 1), (C, 3), (D, 8). Furthermore, it receives from C: (C, 0), (A, 2), (B, 3), (D, 5).

2 pt (c) Please make a drawing of the network graph, assuming that no changes in links and link costs have taken place since the initial messages A has received from B and C.

Now, let us suppose that A detects that its link to B has disappeared. A sends a message to C with a distance vector reflecting this change.

1 pt (d) How many packets with distance vectors (each resulting in an update from A to C) will C send to A **before** the real distance from C to B is given in C's distance vector?

For each of the following three statements indicate if it is true for link state (LS) routing and if it is true for distance vector (DV) routing.

1 pt (e) After convergence it finds the least cost paths to all destinations.

MC14

A. Not true for LS and DV
B. True for LS, not true for DV
C. Not true for LS, true for DV
D. True for both LS and DV

1 pt (f) After convergence a node knows the complete path to each destination.

MC15

A. Not true for LS and DV
B. True for LS, not true for DV
C. Not true for LS, true for DV
D. True for both LS and DV

1 pt (g) The *count to infinity* problem can be solved by defining the cost of a failed link as infinite.

MC16

A. Not true for LS and DV
B. True for LS, not true for DV
C. Not true for LS, true for DV
D. True for both LS and DV

1 pt (h) Why does a router with an interested receiver for a multicast group in PIM-SM first have to become a part of the shared tree before setting up a source-specific tree?

MC17

A. Because each source-specific tree is part of the shared tree.
B. This is more efficient, because the shared tree is shared with other receivers.
C. Because initially, this router does not know which source is sending packets to the multicast address.
D. As long as there are no receivers, which indicated their interest with the IGMP protocol, the router will stay on the shared tree.

1 pt (i) In AODV, how does a router on the path between source and destination know where to forward a RREP message to?

MC18

A. The next hop router is contained in the RREP message.
B. From its forwarding table that it has built using the outcome of the Dijkstra algorithm.
C. From the state information it has stored when receiving the corresponding RREQ message.
D. It will flood the message on all outgoing interfaces, except for the one on which it received the RREP message.
E. It does not matter, since the wireless medium is a broadcast medium, all neighbours will receive its transmissions anyway.

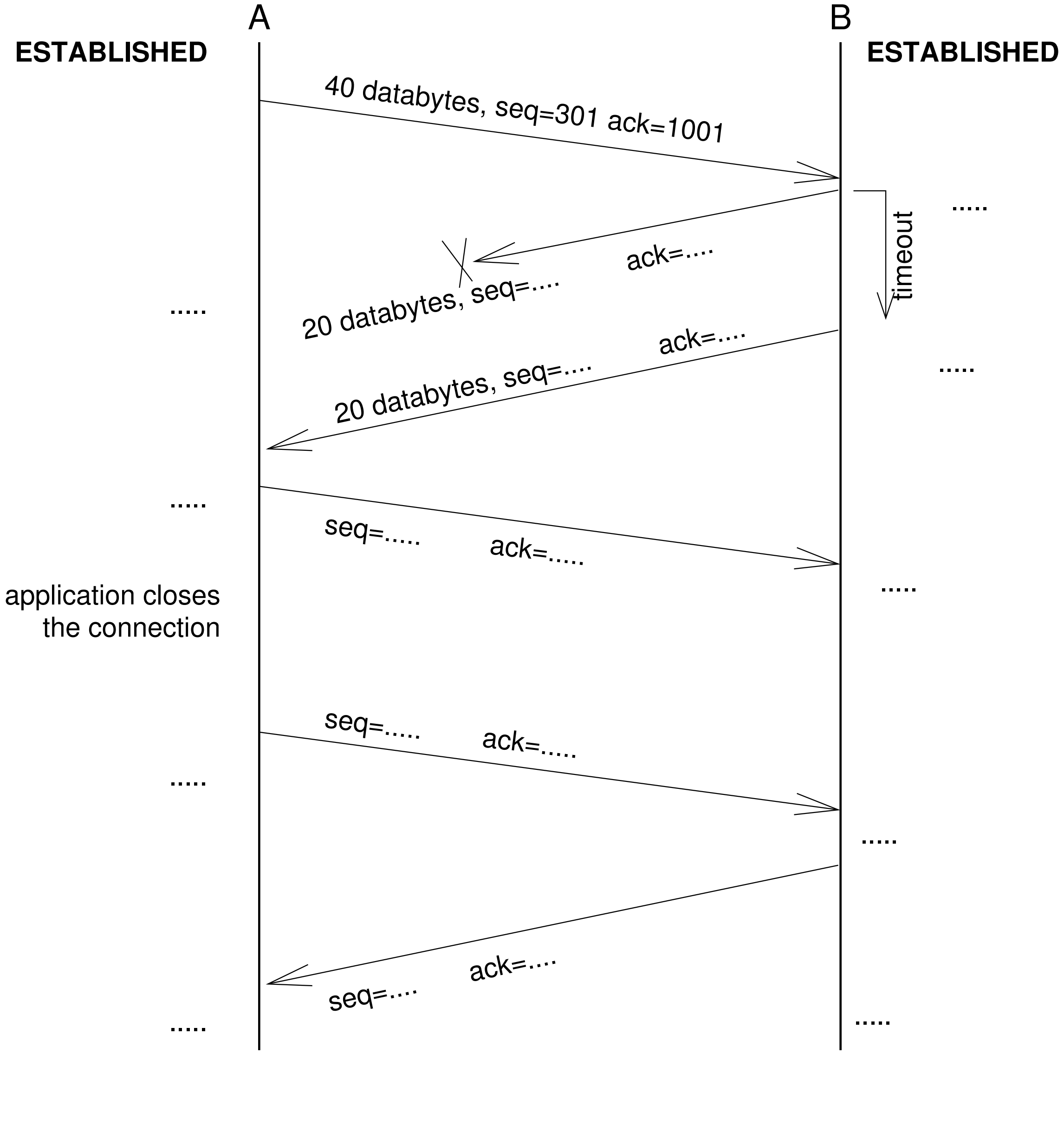
Continued on next page...

3. Transport layer protocols

Consider the following time-sequence diagram, showing a TCP connection between hosts A and B. Assume that the connection has been set up successfully before the diagram starts, but no data has been exchanged yet.

As indicated, the first packet from host B gets lost, and at some later point in time host A decides to close the connection. Host B does not decide to close the connection (within the timespan of this diagram).

5 pt (a) Fill in the dots in this diagram: sequence/acknowledgement numbers of the packets, and TCP state names along the left and right side of the diagram. If any packet(s) has the SYN or FIN flag set, then write that clearly near the packet (no dots are provided for this).



1 pt (b) In the diagram of question (a), why is the first packet from A not retransmitted, even though the reply sent by host B is lost?

MC**19**

A. Host B knows that its first packet has been lost.
B. Host A knows that host B's first packet has been lost.
C. Packets are never retransmitted in the "ESTABLISHED" state.
D. The first packet from host A does not need to be acknowledged.
E. The timeout used by host A is longer than the timeout used by host B.
F. The timeout used by host A is shorter than the timeout used by host B.

1 pt (c) At the end of the diagram of question (a), which host(s) can still send new data?

MC20
A. Neither can.
B. Only host A can.
C. Only host B can.
D. Both hosts can.

1 pt (d) Consider a chat application. Is TCP or UDP more suitable as a transport-layer protocol?

MC21
A. TCP, because the messages are short.
B. UDP, because the messages are short.
C. TCP, to ensure that the messages are not lost.
D. UDP, to ensure that the messages are not lost.
E. TCP, to avoid duplication due to retransmission.
F. UDP, to avoid duplication due to retransmission.
G. Either, but only if it the port numbers are standardized.

1 pt (e) The URL of a web page sometimes contains a port number, like the 1234 in `http://www.utwente.nl:1234` When such a page is fetched, what are the port numbers in the connection setup packet sent by the client?

MC22
A. Source port = random, destination port = 80.
B. Source port = random, destination port = 1234.
C. Source port = 80, destination port = random.
D. Source port = 1234, destination port = random.
E. Source port = 80, destination port = 1234.
F. Source port = 1234, destination port = 80.
G. Source port = random, destination port = random.

1 pt (f) Consider a TCP connection initiated by a client to a server. In which TCP packet(s) is the ACK flag set to 1?

MC23
A. Only in the SYN sent by the client.
B. Only in the SYN sent by the server.
C. In all packets, except the SYN sent by the client.
D. In all packets, except the SYN sent by the server.
E. Only in packets which acknowledge databyte 1.
F. Only in packets which acknowledge databytes that have been acknowledged before.
G. Only in packets which acknowledge databytes that have not been acknowledged before.

1 pt (g) In what situation could the use of the Window Scaling be beneficial even if the PAWS (Protection Against Wrapped Sequence numbers) extension is not used?

MC24
A. Never.
B. On a connection with small bandwidth and a small round-trip time.
C. On a connection with a ver large bandwidth but small round-trip time.
D. On a connection with a small bandwidth but large round-trip time.
E. On a connection with a large bandwidth and a large round-trip time.

1 pt (h) What problem on high-speed links can be solved using the TCP timestamp extension?

MC25
A. Inaccuracy of clocks.
B. Reuse of sequence numbers.
C. Lack of bits in window field.
D. Scalability to large numbers of hosts.
E. Mismatch of send and receive window.

End of this exam.