IK1203 Networks and Communication

Solutions

2019-03-13

Instructions

The exam consists of two sections: Section A (20 points) and Section B (16 points). Section A consist of 20 multiple choice questions, where every question has exactly one correct alternative. Each correct answer is worth one point. If you do not score at least 14 points on Section A, Section B will not be marked.

Submit your answers for Section A on the separate solution sheet labelled "Section A Solution Sheet".

Important: the exams are individual, and marked with a *grading code* that you should copy to the solution sheet. It is very important that you copy the grading code to your solution sheet; if you do not, Section A of your exam cannot be graded.

Section B consist of questions (typically worth 2 to 6 points each) where *answers are handed in on separate sheets, one answer per sheet.* Label each sheet with the question number and your name. Keep your solutions short and to the point.

This exam consists of 9 pages. Before you start, make sure that you have all pages.

Grading

The *preliminary grading scale* for this exam is as follows:

- grade A, at least 14 points on Section A, and 13 points on Section B
- grade B, at least 14 points on Section A, and 10 points on Section B
- grade C, at least 14 points on Section A, and 6 points on Section B
- grade D, at least 13 points on Section A
- grade FX, at least 12 points on Section A (changed to grade E upon completion of complementary assignment)
- grade F, less than 12 points on Section A

Tools

No tools allowed.

Grading code 1234

Copy the grading code to "Section A Solution Sheet", under "2 Grading code"

Section A

1. Which of the following is a function of the network layer in the Internet model?

   A. Congestion control

   B. Routing

   C. Flow control

   D. Medium access control

   Comment:

2. Consider a transfer of a message over a 10 km long link. The signal's propagation speed over the link is 2×10^8 m/s. The link bitrate is 400 Mb/s, and the size of the message is 1500 byte. How long does it take from that the sender starts sending the message until the receiver has received the entire message?

   A. 30 μs

   B. 50 μs

   C. 60 μs

   D. 80 μs

   Comment: Let $L = 12000$ be the message size in bits and $r = 400 \times 10^6$ the link rate in bits per second. Then the transmission delay is $L/r = 3 \times 10^{-5}$ s. The propagation delay d/s is $10 \times 10^3 / 2 \times 10^8 = 5 \times 10^{-5}$. The total transfer time is propagation delay plus tranmission delay: 8×10^{-5} s.

3. Which organization develops Internet protocol standards?

   A. Internet Engineering Task Force (IETF)

   B. Institute of Electrical and Electronics Engineers (IEEE)

   C. Internet Corporation for Assigned Names and Numbers (ICANN)

   D. International Organization for Standardization (ISO)

   Comment: ICANN does not standardize protocols. Even if IEEE and ISO might have standards that are relevant for the Internet, it is the IETF that is the main standardization body for Internet protocols.

4. A client requests a web page from an HTTP server. The page consists of nine parts: two text objects and seven advertisements (image objects). From that the client sends its first request to the server, how many HTTP responses will the client receive in total from the server?

   A. One

   B. Nine

   C. Ten

   D. Eighteen

   Comment: The page is represented as a separate object. Each object requires one request/response transaction.

5. Applications need different kinds of services from the underlying protocol layer, depending on the demand of the application. Consider an email application. If you rank the following services by their importance for the application, which of the following would be the most important (or most probable) service for this application to require from the protocol layer below?

   A. Low latency (delay).

   B. Guaranteed minimum capacity.

   C. Reliable data transfer.

   D. Flow control.

   Comment: Email requires the information to be transfered without errors, but has little demands otherwise.

6. Suppose that you use DNS (Domain Name System) to translate a domain name to an IP address. You send a DNS query to a DNS server, and tell the server that it is a *recursive* query. The server does not know the answer to your query. What does the server do?

    A. It responds that the domain name could not be found.

    B. If responds with whatever it knows about the domain name.

    C. It finds out the answer for you, by asking other DNS servers.

    D. It responds with the name and IP address of the authoritative DNS server for the domain.

    Comment: Recursion means that the server finds out the answer for you.

7. A *local Domain Name System (DNS) server* stores the answers it gets for its questions in a cache. It could happen that an answer in the cache gets invalid, for instance if the DNS database is updated in the server that answered the question. How is this dealt with?

    A. This situation can always occur, therefore there is a limit for how long an answer may be stored in the cache.

    B. A server that answers a question guarantees that the answer will not change during the limited period of time when the answer is stored in the cache.

    C. Before a local server uses an answer from its cache, the local server checks with the server from which it got the answer in the first place, that the answer still is valid.

    D. If a server needs to update its DNS database, it informs all local DNS servers that have copies in their caches that the entry is being updated.

    Comment: It might happen that the cached answer is no longer valid. Therefore a TTL value (time to live) is used to limit how long the answer can stay in the cache.

8. Which of the following statements about TCP is (most) correct?

    A. TCP cannot be used in combination with IP multicast.

    B. TCP provides a one-way connection between two processes.

    C. TCP accumulates data from the application and decides how large segments to send.

    D. All segments sent over a TCP connection take the same path trough the network between sender and receiver.

    Comment:

9. Which of the following statements about TCP congestion control is (most) correct?

    A. During the congestion avoidance phase, the congestion window increases linearly in size.

    B. With fast retransmit and fast recovery a retransmission is made for every duplicate ACK.

    C. During the slow start phase, the congestion window increases exponentially in size, and the increase does not stop until the window reaches the receiver-advertized window size.

    D. The congestion window increases in size until the sender gets an ACK timeout.

    Comment:

10. Which of the following statements about UDP is (most) correct?
    - A. UDP always protects data with a checksum.
    - **B. UDP does not guarantee that datagrams arrive to the receiving application in the correct order.**
    - C. UDP never protects data with a checksum.
    - D. UDP provides a connection-oriented unreliable service.

    Comment:

11. Assume we have a transport level connection with a capacity of 10 Mb/s and that the connection between sender and receiver has an RTT of 8 ms. Which is the optimal window size the sender should use?
    - **A. 10000 byte.**
    - B. 20000 byte.
    - C. 5000 byte.
    - D. 80000 byte.

    Comment:

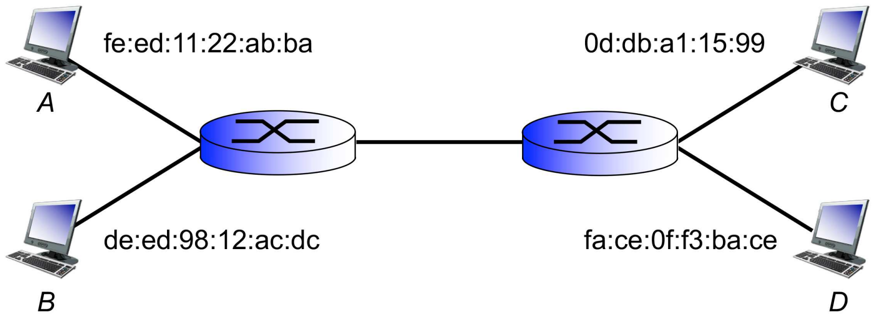
12. MAC addresses are used for addressing by link layer protocol such as Ethernet and Wireless LAN. Which of the following statements about MAC addresses is *false*?
    - A. MAC addresses are permanent, assigned by the manufacturer. They will not change if a device is moved.
    - B. MAC addresses are assigned to network interfaces, so a device with multiple network interfaces will have multiple MAC addresses.
    - **C. MAC addresses are organized hierarchically. A bit-mask (network mask) determines what addresses are present on a network.**
    - D. Applications do not need to be aware of MAC addresses.

    Comment: MAC addresses are flat, i.e., they don't have any particular structure.

13. An Ethernet switch has an address table consisting of MAC addresses (link layer addresses) and port numbers. Assume that an Ethernet frame arrives that is destined to a MAC address not in the table. What will the switch do?
    - **A. Send the frame to all ports, except the one on which the frame was received.**
    - B. Send an error message "Destination unreachable" to the source of the frame.
    - C. Send an ARP (Address Resolution Protocol) message to ask for the MAC address.
    - D. Send the frame to the broadcast address (FF:FF:FF:FF:FF:FF).

    Comment: Flooding – when a switch has not learned the receiver address.

14. Consider the network in the figure below consisting of two switches and four computers (A to D). The computers' MAC addresses are shown. Suppose that computer B sends a message to computer A. Computer A answers with a message to computer B. Assuming that the address tables initially are empty, what MAC addresses will be in the address table of the switch to the right after the two messages?



A. de:ed:98:12:ac:dc och fe:ed:11:22:ab:ba

B. fe:ed:11:22:ab:ba

C. de:ed:98:12:ac:dc

D. None

Comment: The first message from B to A is flooded and then the right switch learns B's address.

15. An important component in a wireless LAN (WLAN) is how to prevent different units connected to the same access point from disturbing each other. Consider a network with one access point and several wireless devices. Which of the following statements is correct?

A. If a collision occurs, all units involved will discover this and immediately abort their transmissions.

B. The access point assigns different radio channels to different units to reduce the risk that they disturb each other.

C. A successful transmission from a unit to the access point is confirmed with an ACK frame from the the access point. In case of a collision, there will be no ACK frame.

D. Each device is assigned a certain priority by the access point. The priority defines the order in which the units can transmit to the access point.

Comment: All units share the same channel according to the random access principle. The absence of an ACK is the only way to detect that something went wrong.

16. Consider an access point that connects a wireless network (WLAN) and a wired network (Ethernet). What is true?

A. The access point is a router that forwards frames with IP packets between the wireless network and the Etnerhet.

B. A device that sends a frame from the Ethernet to a device on the WLAN does not need to specify that the frame should be sent via the access point.

C. An access point is "transparent", in the sense that it does not modify the frames that are sent between the wireless network and the Ethernet.

D. An access point coordinates the communication on both sides (wireless and wired) and therefore prevents collisions from happening.

Comment:

17. One of the following statements about ICMP is incorrect. Which one?

    A. Each time a router drops an IP packet, it sends an ICMP error message to the source of that packet.

    B. ICMP does not use a transport protocol, so ICMP messages are encapsulated directly in IP.

    C. A router can send an ICMP message that says that the destination address cannot be reached.

    D. If a router detects TTL = 0, it will send an ICMP error message back to the source of that packet.

    Comment:

18. IP address 130.237.15.74 belongs to a host on a subnet with the netmask 255.255.255.240. Which of the following statements is correct?

    A. 30 different IP addresses can be given to hosts connected to the subnet.

    B. The subnet is 130.237.15.64/28.

    C. The broadcast address on the subnet is 130.237.15.127.

    D. The subnet is 130.237.15.32/28.

    Comment: The subnet covers the address range 130.237.15.64 – 130.237.15.79. The last address is broadcast.

19. Which of the following statements about distance vector routing is (most) correct?

    A. BGP uses Dijkstra's algorithm to calculate the shortest path between nodes in the network.

    B. In OSPF, a node regularly sends its distance vector to its neighbor nodes.

    C. In RIP, a node regularly sends its distance vector to its neighbor nodes.

    D. An advantage with RIP is that it scales well to large ASes (Autonomous Systems) with many nodes.

    Comment:

20. DHCP (Dynamic Host Configuration Protocol) has a message called DHCP Discover. This message has:

    A. 0.0.0.0 as the source IP address, and 255.255.255.255 as the destination IP address.

    B. 0.0.0.0 as the source IP address, and 0.0.0.0 as the destination IP address.

    C. 255.255.255.255 as the source IP address, and 0.0.0.0 as the destination IP address.

    D. 255.255.255.255 as the source IP address, and 255.255.255.255 as the destination IP address.

    Comment:

Section B

1. A client establishes a TCP connection to a server to transfer 64 kB of data. The one-way delay is 2 ms and the advertized receiver window is 16 kB. Assume an initial congestion window of 2 kB. There is no congestion in the network and the transmission time is negligible. The time it takes to establish a connection should however be considered. Calculate the total transfer time. (3 p)

Solution:

TCP uses a three-way handshake (SYN, SYN+ACK, ACK), and data can be sent directly after the SYN+ACK. This takes 1 RTT = 4 ms (calculating the last ACK will also be considered OK, i.e. 1.5*RTT = 6 ms).

TCP will then begin in slow start. TCP sends 2 kB (initial CWND). After 1 RTT, TCP sends 4 kB, aftr 2 RTT another 8 kB, after 3 RTT another 16 kB, which is when the receiver-advertized window has been reached. After that point, the sender can transmit max 16 kB at a time until all data has been transferred. This results in 7 transmission rounds: 2+4+8+16+16+16+2=64 kB

Thus it takes in total 1 RTT (connection establishment) + 6*RTT + RTT/2 = 4 + 6*4 + 4/2 = 30 ms. In this calculation, we did not include the ACK of the last segment. If that ACK is included, the transfer time is 32 ms. If the connection establishment was calculated as 1.5*RTT, the corresponding transfer times would be 32 and 34 ms respectively.

2. Consider the network in the figure below where all links are Ethernet links. The network consists of six computers (A to F), two routers (R_1 and R_2) and three switches (S_1 to S_3). Assume that intially all ARP and switch tables are empty. (4 p)

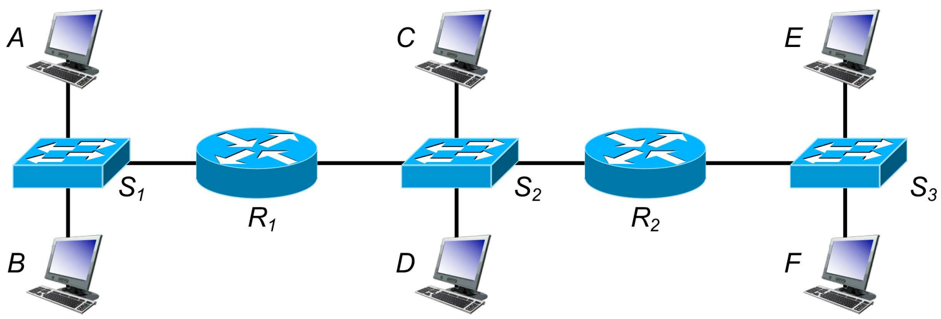
   (a) Computer F is about to send an IP packet to B and therefore first sends an ARP request. What is F asking for?

   (b) The ARP request is sent in an Ethernet frame. What MAC address does F use as destination for the Ethernet frame?

   (c) Specify the device (or devices) that will get the ARP query.

   (d) The IP packet is sent to B, which then responds with another IP packet to F. Specify the content of the switch table in switch S_1 after the second IP datagram is transferred.

   Ports are not named in the figure. If you need to name ports in your solution, use clear and unambigious names.



Solution:

(a) F asks for the MAC address of the east (right) port of R_2.

(b) The broadcast address (FF:FF:FF:FF:FF:FF).

(c) E and R_2. (Also F may be included in the answer.)

(d)

MAC address	port
B	south
R_1 west	east

3. Suppose that you come to KTH and connect to the wireless network. Then you open your web browseer and type in the domain name "hugo.z.hackenbush" in the navigation field. (Here we assume that someone has registered "hackenbush" as an top-level domain, presumably through the new gTLD program for generic top-level domains.) The first that then happens is that your web browser sends a DNS query to translate the domain name to an IP address. (2+2 p)
   (a) Four different DNS servers will be involved. For each of the four servers, describe the server and the function it has in the DNS system, and describe what answer it gives as a result of your question.
   (b) DNS uses UDP as transport protocol. UDP provides the service to transfer a message (datagram) with a limited maximum size. The limit can be as low as 512 byte. (In contrast to TCP, which can transfer a data stream without size limitations.) Suppose that the size of the data that DNS needs to transfer as a message exceeds UDP's limit. What happens then? Is it possible to send larger messages without modifying the DNS protocol? Motivate your answer! (You do not need to know any further details of the DNS protocol to answer the question.)

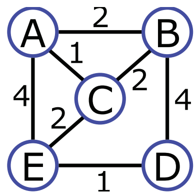
Solution:

(a) You send a DNS query to the local DNS server, which is a proxy that handles all DNS questions from an organization. The local server then sends the question to a root server, which is a DNS server that is responsible for keeping track of all top-level domain servers on the Internet. The root server responds with name and IP address of the authoritative server for the "hackenbush" top-level domain. THe authoritative server for the "hackenbush" domain is responsible for all names in that domain. The local server sends the question to that server, which server responds with name and IP address of the authoritative name server for the sub-domain "z.hackenbush". The local server then sends the question to that server, which responds with the IP address.

(b) No, it is not possible without modifications to the application protocol. It would require support for some kind of segmentation in the application protocol. UDP datagrams are independent, so all information that concern a DNS message must fit within one UDP datagram. The solution is to use TCP instead, which has no limits on data size. (In practice, that is how large DNS messages are dealt with, for instance for so called zone transfers or for DNS messages with information for cryptographic protection. So DNS is really a protocol that uses both UDP and TCP.)

4. Consider the network graph in the figure below with given link costs. (2 p)

   Calculate by using Dijkstra's algorithm the best paths (paths with least costs) from node A to all other nodes in the network. Each step in the algorithm should be shown. Use the following table template, which you should redraw and fill out.



Network graph with given link costs

step	N'	$D(B), p(B)$	$D(C), p(C)$	$D(D), p(D)$	$D(E), p(E)$
0					
1					
2					
⋮					

Table template

Solution:

step	N'	$D(B), p(B)$	$D(C), p(C)$	$D(D), p(D)$	$D(E), p(E)$
0	A	$2, A-B$	$1, A-C$	∞	$4, A-E$
1	AC	$2, A-B$		∞	$3, A-C-E$
2	ACB			$6, A-B-D$	$3, A-C-E$
3	$ACBE$			$4, A-C-E-D$	
4	$ACBED$				

5. Consider the following forwarding table. (2+1 p)

Destination	Network mask	Next hop	Interface (port number)
111.0.0.0	255.0.0.0	–	m0
192.16.7.0	255.255.255.240	193.14.5.193	m1
193.14.5.160	255.255.255.224	–	m2
193.14.5.192	255.255.255.224	–	m1
194.17.21.16	255.255.255.255	111.20.18.14	m0
192.16.7.0	255.255.255.0	111.15.17.32	m0
192.16.8.0	255.255.255.0	111.15.17.32	m0
194.17.21.0	255.255.255.0	111.20.18.14	m0
0.0.0.0	0.0.0.0	111.30.31.18	m0

(a) Specify next hop and outgoing interface for each of the following destination addresses: 192.16.8.132, 192.16.7.13, 194.17.22.12 och 193.14.5.198.

(b) The network administrator is thinking about aggregating the two subnets 192.16.7.0/24 and 192.16.8.0/24 to 192.16.7.0/23. Is this a good idea? Explain your answer.

Solution:

(a) 192.16.8.132: 111.15.17.32, m0
192.16.7.13: 193.14.5.193, m1
194.17.22.12: 111.30.31.18, m0 (default route)
193.14.5.198: 193.14.5.198, m1 (destination directly connected to subnet)

(b) It is not a good idea to aggregate 192.16.7.0/24 and 192.16.8.0/24 to 192.16.7.0/23. The 23 upper bits in the two subnets are not the same.