IK1203 Networks and Communication

Solutions

2020-03-12

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. Internet consists of many Internet Service Providers (ISPs) that are interconnected. The ISPs have agreements that regulate how they may charge each other for the services. Assume that ISP A has a peering agreement with ISP B. What does that mean?

   A. A pays B, but B does not pay A.

   B. B pays A, but A does not pay B.

   C. Both of them pay the other.

   D. None of them pay the other.

   Comment:

2. A sending host sends a packet to a receiving host. The size of the packet is 500 bytes. There is one packet switch between the sending host and the receiving host. The propagation delay on the first link (from sending host to switch) is 0.2 milliseconds, and the propagation delay on the second link (from switch to receiving host) is 0.3 milliseconds. Each link has a bitrate of 10 Mb/s. How long does it take from that the sending host starts sending the packet until the receiving host has received the entire packet? Assume that the processing in the switch is infinitely fast.

   A. 0.5 milliseconds

   B. 0.9 milliseconds

   C. 1.3 milliseconds

   D. 1.7 milliseconds

   Comment: Let $L = 4000$ be the message size in bits and $r = 10 \times 10^6$ the link rate in bits per second. Then the transmission delay is $L/r = 4 \times 10^{-4}$ seconds on each link, i.e. 0.4 milliseconds. So the transfer from the sending host to the switch takes $0.2 + 0.4$ milliseconds, and from the switch to the receiving host takes $0.3 + 0.4$ milliseconds. In total, 1.3 milliseconds.

3. What is an Internet standard document called?

   A. Work In Progress (WIP)

   B. Request for Comments (RFC)

   C. Internet Protocol Specification (IPS)

   D. Internet Draft (ID)

   Comment: Internet Drafts are preliminary RFCs with limited lifetime.

4. Sending an email from a sender to a receiver can involve several different protocols, such as SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), and IMAP (Internet Message Access Protocol). Consider the case when the sender first sends an email to an outgoing mail server, the outgoing mail server sends the mail to an incoming mail server, and the receiver finally gets the email from the incoming mail server. IMAP and SMTP are used for this. Which of the following alternatives describes the likely order in which those two protocols would be used?

   A. SMTP, IMAP, SMTP

   B. SMTP, SMTP, IMAP

   C. IMAP, SMTP, SMTP

   D. IMAP, IMAP, SMTP

   Comment: SMTP from email sender to outgoing email server, SMTP from outgoing to incoming mail server, and IMAP for the receiver to fetch the email from the server.

5. HTTP proxy servers are used to improve performance of web communication. In what way does an HTTP proxy server help to speed up web communication?
   - A. An HTTP proxy server has a faster link to the Internet than regular hosts.
   - **B. An HTTP proxy saves copies of web objects recently requested by clients.**
   - C. An HTTP proxy downloads popular web objects in advance.
   - D. An HTTP proxy server helps clients to process web objects with complex content.

   Comment:

6. Suppose that you use DNS (Domain Name System) to translate the domain name "rufus.firefly.freedonia" to an IP address. This translation involves communication with several DNS servers. During the process of translation, you receive a response from a TLD (top-level domain) DNS server. What does the response from the TLD DNS server contain, most likely?
   - A. The name and IP address of the DNS server responsible for the domain "freedonia".
   - B. The name and IP address of the DNS server responsible for the domain "rufus.firefly.freedonia".
   - **C. The name and IP address of the DNS server responsible for the domain "firefly.freedonia".**
   - D. The IP address of the domain "rufus.firefly.freedonia".

   Comment: The top-level part of the domain name is "freedonia".

7. Which of the following statements about communication according to the client-server model *is correct*?
   - A. There can only be one connection from a host to a given server.
   - **B. In order to send a response back to a client, the server needs the client's IP address and port number.**
   - C. Two different servers (a mail servers and a web server for instance) cannot run on the same host.
   - D. The client needs to know the server's IP address, but not port number, in advance.

   Comment: The server learns the client's IP address and port number from the received packet.

8. Study the Java code below for a communication application. The code is simplified.

```
ServerSocket listenSocket = new ServerSocket(9876);
while (true) {
    Socket connectionSocket = listenSocket.accept();
    Runnable thread = new clientRequestHandler(connectionSocket);
    new Thread(thread).start();
    }
}
```

   Which is the best description of the code?
   - A. A sequential UDP server.
   - B. A concurrent UDP server.
   - **C. A concurrent TCP server.**
   - D. A sequential TCP server.

   Comment:

9. A TCP sender has the following parameter values for its connection: The congestion window is 16 kB, the slow start threshold value is 24 kB, and the remaining available space in the sender buffer is 8 kB. It has sent a full window of data in the latest transmission round. It receives an ACK for the amount of data sent, and a window update with a receiver window of 32 kB. How much will it send in the next transmission round?

   A. 8 kB

   B. 16 kB

   C. 24 kB

   D. 32 kB

   Comment:

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

    A. The very first TCP message sent when a TCP connection is being established has both the SYN flag and the ACK flag set.

    B. When a TCP connection is being established, a SYN message is sent in both directions with the same initial sequence number, so that both sides of the connection start sending data with the same sequence number.

    C. The first TCP message sent when a TCP connection is being established always has the RST flag (RESET) set.

    D. When a client is establishing a TCP connection to a server, it can piggyback data on the ACK sent to acknowledge the server's initial sequence number.

    Comment:

11. Which of the following statements about UDP is (most) correct?

    A. UDP can detect bit errors in packets and will then drop them.

    B. UDP has no mechanism to detect bit errors in packets.

    C. UDP can detect lost packets, but will not retransmit them.

    D. UDP can detect lost packets, and will retransmit them.

    Comment:

12. Assume we have a transport level connection with a capacity of 8 Mbit/s and that the connection between sender and receiver has a one-way delay of 8 ms. Which is the optimal window size the sender should use?

    A. 40000 bytes.

    B. 32000 bytes.

    C. 16000 bytes.

    D. 4000 bytes.

    Comment:

13. Eight bits of data, protected by an additional parity bit for error detection, are transmitted over a link where bit errors are likely to occur. The error detection algorithm is *even parity*. Consider the transmission of the nine bits "1100 0100 1", where the last bit is the parity bit. During the transmission there is an error that could affect one or more bits. Which of the following erroneous transmissions would be detected by the receiver?

    A. "1100 0100 1"

    B. "1101 0100 1"

    C. "0100 0111 0"

    D. "0101 0100 1"

    Comment: The number of ones should be even.

14. Wireless networks use CSMA/CA for medium access while wired networks use CSMA/CD. One of the statements below is *false*. Which one?

    A. A node with data to send first listens to determine if someone else is sending, before it starts to send any data. This is true both for CSMA/CA and CSMA/CD.

    B. If a collision occurs when several nodes send at the same time, the sending nodes will wait a randomly chosen time and then try again. This is true for both CSMA/CA and CSMA/CD.

    C. Collision avoidance (as in CSMA/CA) is more efficient than collision detection (as in CSMA/CD). However, CSMA/CA requires the medium to be full duplex, which CSMA/CD does not.

    D. A problem in wireless networks is that the signal can be weakened and blocked by obstacles. This means in turn that that the MAC protocol cannot be based on the assumption that any arbitrary node can hear all traffic, which is a requirement for CSMA/CD.

    Comment: CSMA/CD is more efficient than CSMA/CA. CSMA/CA does not require full duplex (if it were full duplex, a medium access protocol would not be needed!)

15. Which of the following statements about ARP is correct?

    A. ARP is used to distribute routing information on a Local Area Network (LAN).

    B. ARP stands for *ARPANET Routing Protocol* and is a routing protocol for the Internet.

    C. Every network device has a permanent identifier. ARP takes care of the translation between IP addresses and such permanent identifier.

    D. Most ISPs only give out a single IP address to each customer, so if you want to have more than one computer at home connected to the Internet, addresses need to be translated between the home network and the Internet. ARP takes care of this address translation.

    Comment:

16. An Ethernet switch builds its MAC address table through *learning*. How does learning work?

    A. For each frame the switch receives, the switch examines the source address. If the source address is not present in the address table, the switch adds the source address to the table.

    B. For each frame the switch receives, the switch adds the source address and the destination address to the table.

    C. For each frame the switch receives, the switch examines the destination address. If the destination address is not present in the address table, the switch adds the source address to the table.

    D. For each frame the switch receives, the switch adds the source address to the table.

    Comment:

17. Consider a subnet (IP version 4) with the prefix 130.215.1.0/24. Which of the following statements is *not* correct?

    A. The subnet's prefix can be aggregated with the prefix 130.215.2.0/24 to form the prefix 130.215.1.0/23.

    B. The address 130.215.1.229 belongs to the subnet.

    C. It is OK to have 235 different hosts connected at the same time to the subnet.

    D. The subnet can be divided into the following two subnets: 130.215.1.0/25 and 130.215.1.128/25

    Comment:

18. Which of the following statements about NAT (Network Address Translation) is *not* correct?

    A. If you use NAT between your local network and your Internet provider, it is enough to have only one public IP address even though you have several computers connected to your local network.

    B. If you use NAT between your local network and your Internet provider, you can renumber you addresses on your local network without notifying your operator and still be able to access the Internet.

    C. If you use NAT between your local network and your Internet provider, you have to use a proxy server at the provider to make a server on your local network reachable to clients outside your local network.

    D. If you use NAT between your local network and your Internet provider, you can change to another Internet operator without having to renumber the addresses on your local network.

    Comment:

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

    A. Distance vector is based on each node sending information to its neighbors about what nodes it can reach and the cost to these nodes.

    B. Distance vector routing is based on each node sending routing information to all other nodes in the network.

    C. Through distance vector routing, each node in the network will get full knowledge about the topology.

    D. Distance vector routing is well suited for large networks with many nodes, thanks to fast and efficient loop detection.

    Comment:

20. Which of the following statements about DCHP (Dynamic Host Configuration Protocol) is (most) correct?

    A. DHCP can be used for time-limited assignment of IP addresses.

    B. DHCP uses TCP as the transport protocol.

    C. DHCP is one of the few exceptions when it is allowed to use a broadcast address (255.255.255.255) as source address.

    D. DHCP cannot be used to inform a host about which DNS server to use.

    Comment:

Section B

1. Consider a web page that consists of a number of objects: a base document (an HTML document) and three images. All objects are on the same web server. (1+1+2 p)

   HTTP can manage TCP connections in two ways: as persistent connections or non-persistent connections. A persistent TCP connection is left open (that is, not closed) between objects, so that the same TCP connection can be used to fetch multiple objects from the server. With non-persistent TCP connections, the TCP connection is closed after each object.

   Assume that the time it takes to set up a TCP connection is T_{TCP}, and the time it takes to do an HTTP transaction (that is, to send an HTTP request and receive a response) is T_{HTTP}. All other delays are negligible. Also assume that the closing of a TCP connection takes place in the background, so neither the client nor the server needs to wait for a connection to close.

   (a) How long would it take to fetch the web page if persistent TCP connections are used?

   (b) How long would it take to fetch the web page if non-persistent TCP connections are used?

   (c) In reality, the time it takes for a web server to process a request can vary a lot between objects. Some objects can be returned very quickly, such as static text objects. Other objects may involve complicated computations, communication with other servers, and so on, and therefore can take much longer for the server to return. Taking the large variations in processing time into consideration, it would be an advantage if HTTP could operate in the following way:

   - The client can send several requests at once to the server, without having to wait for the server to respond. In this way, a client may have many requests outstanding at a server.
   - The server can send a response as soon as it has finished processing the request. This means that responses may arrive at the client in a different order than the client sent the requests. For example, the response to the first request may arrive last.

   Explain why this way of communication is not supported by HTTP. What kind of changes to HTTP would be necessary in order to support this way of communication?

   Solution:

   (a) One T to set up the TCP connection, then one T to fetch each object. Total $T_{\text{TCP}} + 4T_{\text{HTTP}}$.

   (b) For each object: One T to set up the TCP connection, and one T per object. Total $4T_{\text{TCP}} + 4T_{\text{HTTP}}$.

   (c) HTTP is a request/response protocol. An HTTP client cannot send a new request before it has received the response to the previous request. Therefore, HTTP does not have a way to match responses to requests – that is implicit, since there cannot be more than one request outstanding. One way to support this would be to add a unique request identifier to the HTTP header. The client adds an identifier to each HTTP request, and the server includes the identifier in the HTTP header of the response.

2. A client establishes a TCP connection to a server to download a file of size 65 kB. The one-way delay is 5 ms and the RTT (Round Trip Time) is 10 ms. The MSS (Maximum Segment Size) is 1 kB. There is no congestion in the network, the transmission time is negligible, and TCP Reno is used. Calculate the total transfer time for the following two cases. You need to include the TCP connection establishment time in your calculations. (2+2 p)

(a) The client has an intial congestion window of 2 kB, a slow start threshold value of 16 kB, and advertizes a receiver window of 16 kB. The server has an intial congestion window of 2 kB, a slow start threshold value of 32 kB, and advertizes a receiver window of 32 kB.

(b) The client has an intial congestion window of 2 kB, a slow start threshold value of 12 kB, and advertizes a receiver window of 20 kB. The server has an intial congestion window of 2 kB, a slow start threshold value of 16 kB, and advertizes a receiver window of 24 kB.

Solution:

(a) TCP uses a three-way handshake (SYN, SYN+ACK, ACK). The client initiates the connection establishment and the server can start sending data after the ACK from the client has been received. This takes 1.5 RTT = 1.5*10 = 15 ms.

TCP will then begin in slow start. The server sends 2 kB (initial CWND). After 1 RTT, it sends 4 kB, after 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 + 3 = 65 kB

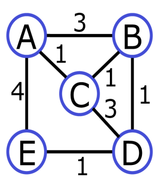
Thus it takes in total 1.5 RTT (connection establishment) + 6*RTT + RTT/2 = 15 + 6*10 + 10/2 = 80 ms. In this calculation, we did not include the ACK of the last segment. If that ACK is included, the transfer time is 85 ms.

(b) TCP uses a three-way handshake (SYN, SYN+ACK, ACK). The client initiates the connection establishment and the server can start sending data after the ACK from the client has been received. This takes 1.5 RTT = 1.5*10 = 15 ms.

TCP will then begin in slow start. The server sends 2 kB (initial CWND). After 1 RTT, it sends 4 kB, after 2 RTT another 8 kB, after 3 RTT another 16 kB, which is when the server's slow start threshold has been reached. After that point, the sender can increase its congestion window with 1 MSS at a time (1 kB at a time) until all data has been transferred. This results in 6 transmission rounds: 2 + 4 + 8 + 16 + 17 + 18 = 65 kB

Thus it takes in total 1.5 RTT (connection establishment) + 5*RTT + RTT/2 = 15 + 5*10 + 10/2 = 70 ms. In this calculation, we did not include the ACK of the last segment. If that ACK is included, the transfer time is 75 ms.

3. Consider the network graph below with given link costs. Calculate, by using Dijkstra's (3 p)



algorithm, the shortest paths (the paths with least cost) from node A to all other nodes in the network. Every step in the algorithm must be shown. Use the following table template, which you copy onto your solutions sheet, and fill in.

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

Solution:

step	N'	$D(B), p(B)$	$D(C), p(C)$	$D(D), p(D)$	$D(E), p(E)$
0	A	$3, A$	$1, A$	∞	$4, A$
1	AC	$2, C$		$4, C$	$4, A$
2	ACB			$3, C$	$4, A$
3	$ACBD$				$4, A$
4	$ACBDE$				

4. A router R with three ports P1–P3 has the following routing table. (3+2 p)

Destination	**Gateway**
130.237.112.0/26	P1
130.237.112.64/26	P2
130.237.112.128/27	P3
130.237.112.160/27	130.237.112.131
0/0	130.127.112.3

From the routing table, you can tell that the router R is in a network with several subnets, and that it is connected to one or more other routers.

(a) Draw a figure that shows all parts of the network where R is located. The figure should clearly show each subnet and each router that you can tell exists in the network. For each subnet, show the subnet prefix. For router R, also clearly indicate the ports.

(b) How will router R forward packets to the following destinations? For each destination, give the outgoing port on the router, and the IP address of the next hop.

- 130.237.112.80
- 130.237.112.225
- 130.237.112.33
- 130.237.112.180

(One point is deducted for each incorrect answer; zero points is the lowest score.)

Solution:

(a)

(b) **130.237.112.80** Port P2, next hop 130.237.112.80

130.237.112.225 Port P1, next hop 130.127.112.3

130.237.112.33 Port P1, next hop 130.237.112.33

130.237.112.180 Port P3, next hop 130.237.112.131