IK1203 Networks and Communication

Solutions

2018-06-05

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. The Internet model consits of five layers. Which layer defines how hosts (such as computers and smartphones) that are connected with routers can communicate with each other?

   A. Link layer.

   B. Network layer.

   C. Physical layer.

   D. Application layer.

   Comment:

2. Which of the following protocols is not an application layer protocol?

   A. SMTP (Simple Mail Transfer Protocol)

   B. DHCP (Dynamic Host Configuration Protocol)

   C. ICMP (Internet Control Message Protocol)

   D. IMAP (Internet Message Access Protocol)

   Comment: ICMP is a network-layer protocol.

3. Consider the following statements about HTTP (Hypertext Transfer Protocol) and web applications. Which is (most) correct?

   A. HTTP is defined as a session-based protocol, where each HTTP session consists of the client opening an HTTP connection to the server, performing a series of HTTP transactions, and then closing the HTTP connection.

   B. Since HTTP is text-based and all HTTP transactions are in cleartext, HTTP is unsuitable to use for applications with security requirements.

   C. By using cookies, a web server can keep track of users and manage user-specific information (settings, for instance).

   D. By using a web cache, computationally demanding web pages can be displayed faster in slow web browsers (e.g., for JavaScript games and high resolution video).

   Comment: The purpose of web cookies is to make it possible for web servers to keep track of information about users.

4. Consider the following statements about web caching. Which statement *is false*?

   A. Web caching takes place on the web server, where the web server keeps copies of recently used objects.

   B. A caching web proxy server acts as client and server at the same time.

   C. With a web cache in an organization, it is possible to reduce the load on the organization's access link to the Internet.

   D. Having a web cache does not always give shorter response time. For instance, when there is a cache miss, the response time could get longer.

   Comment:

5. Which of the the following statements about DNS (Domain Name System) servers is correct?

   A. Each DNS query is first sent to a root server. If the root server does not know the answer, it forwards the question to some other server.

   B. The TLD server ("top-level domain") for a certain domain keeps track of all host names within that domain. For example, the TDL server for the "se" top-level domain knows all hosts with names endimg with ".se".

   C. An authoritative name server for an organization knows all host names with within that organization. For exampel, KTH's authoritative server knows all host names within KTH.

   D. A local server only responds to queries about name s within the local organization.

   Comment:

6. Which of the following statements about the client-server model is incorrect?

   A. Clients that have data to send to other clients, send the data via a server.

   B. Communication betweeen client and server is always initiated by the client.

   C. The client needs to have a permanent IP address.

   D. In practice, the server may not be a single machine. Instead, it can often consist of many machines that together handle the clients that are using the service.

   Comment: The client may have a dynamic IP address, the only requirement is that the client does not change IP address in the during the communication with the server.

7. Which of the following statements about TCP is correct?

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

   B. TCP provides a two-way connection between two processes, but data can only be sent in one direction at a time.

   C. TCP always accumulates enough data from the application to send as large segments as the MTU (Maximum Transmission Unit) allows.

   D. If several TCP connections are established over the same link, the first establised TCP connection will get most of the link capacity.

   Comment:

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

   A. With TCP congestion control, the reciever detects packet reordering and signals this by sending an ACK with window size 0 back to the sender.

   B. With TCP congestion control, TCP assumes that congestion has occurred if the sender does not get an ACK in time. TCP will then adapt the sending rate.

   C. With TCP congestion control, the receiver detects congestion and signals this back to the sender by decreasing the window size so that the sender decreases the sending rate.

   D. With TCP congestion control, the sender starts with sending data at the rate given by the receiver window and then adapts the sending rate when the receiver announces a new window size.

   Comment:

9. Which of the following statements about UDP is (most) correct?
   A. UDP can detect packet loss, but cannot notify the sender about it.
   B. UDP can detect packet loss and can notify the sender about it.
   C. UDP can detect bit errors in packet, and can notify the sender about it.
   D. UDP can detect bit errors in packets, but cannot notify the sender about it.

   Comment:

10. Which of the following statements is not correct?
   A. *Stop-and-Wait* often results in low utilization.
   B. Neither *Go-Back-N* nor *Stop-and-Wait* means that the sender needs to buffer multiple packets.
   C. In *Go-Back-N* it happens that packets which arrive correctly at the receiever are retransmitted.
   D. *Go-Back-N* can deal with situations where packets arrive in the wrong order.

   Comment:

11. CRC (cyclic redundancy check) is a technique used for error detection at the link layer. What is true?
   A. CRC can detect single bit errors only. If there is more than one bit error in a frame, CRC will not be able to detect it.
   B. CRC is used on wireless networks only. Bit errors are so rare on wired networks that error detection isn't needed.
   C. There need to be as many bits of CRC as there is data in the frame. If there are N bits of data, the CRC field should be N bits long.
   D. CRC can be efficiently implemented in hardware. Therefore, it is well suited for error detection at the link layer.

   Comment: CRC is implemented in dedicated hardware on the network adapter.

12. Link layer addresses (or "MAC" addresses) are used at the link layer to identify devices. Which of the following statements about link layer addressing *is false*?
   A. IP adresses are not used at the link layer; they need to be translated to MAC addresses.
   B. Even though MAC addresses, in principle, are globally unique, they are not used for global addressing and routing.
   C. MAC addresses are assigned by a DHCP server.
   D. In order for a client to connect to a server, the client needs to know the MAC address of the server.

   Comment: DHCP assigns IP addresses, not MAC addresses.

13. An Ethernet switch connects a number of computers into a network. Which of the following statements is correct?
   A. Two computers connected to different ports on the switch can send packets at the same time without causing collisions.
   B. The switch is self-learning, and learns where the computers are by examining IP addresses in the packets it receives.
   C. If a switch receives a packet to a computer it does not recognize, the packet is sent to the all-ones broadcast address (FF:FF:FF:FF:FF:FF).
   D. A computer can be connected to the switch with a cable or with a wireless connection.

   Comment:

14. Which of the following statements is correct about wireless communication in IEEE 802.11 wireless networks?

    A. Traffic in a wireless networks always goes via access points.

    B. "Hidden terminal" means that the access point cannot detect the signal from the wireless unit.

    C. In "ad hoc mode," there is no predetermined structure; the wireless units make up the network themselves.

    D. When multiple wireless units are connected to the same access point, they use different radio channels and therefore do not interfere with each other.

    Comment:

15. Wireless local area networks (LANs) and wired LANs use different protocols for *medium access control* (MAC). For instance, IEEE 802.11 ("WiFi") uses CSMA/CA, while Ethernet uses CSMA/CD.

    Why do we not use the same MAC protocol for wireless networks and wired LANs?

    A. In a wireless LAN, we cannot assume that all frames that are sent will reach all devices (*hosts*) that are connected to the LAN.

    B. In wired LANs, we need not worry about security, and therefore we can use CSMA/CD even though it is not a secure protocol that encrypts communication.

    C. Since the radio spectrum is a limited resource and its usage is highly regulated by authorities, we cannot use a protocol based on the principle of "random access" for wireless communication.

    D. With CSMA/CD, there can be collisions. We cannot allow collisions to happen on a wireless network, and therefore we use CSMA/CA instead.

    Comment: In a wireless network, a device can be located in a place that the signal from some other device does not reach.

16. Consider a subnet (IP version 4) with the prefix 10.18.19.0/24. Which of the following statements is correct?

    A. The adress 10.18.19.44 belongs to the subnet.

    B. The subnet consists of 512 different addresses.

    C. The address 10.18.19.127 is the subnet's broadcast address.

    D. The subnet's prefix can be aggregated with the prefix 10.18.18.0/24 to the prefix 10.18.19.0/23.

    Comment:

17. 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, it is not possible to make a server on your local network available to clients outside the local network.

    C. 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.

    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:

18. Which of the following statements about IP routing is (most) correct?

    A. OSPF uses *flooding* to distribute link state updates to all other nodes in the network.

    B. BGP is a *link state* protocol.

    C. OSPF uses the Bellman-Ford algorithm to find the best path between two nodes in the network.

    D. An advantage with RIP is its ability to converge quickly.

    Comment:

19. Which of the following statements about IPv6 is correct?

    A. In IPv6, the header checksum that exists in IPv4 has been removed.

    B. The main reason for introducing IPv6 is to improve the support for QoS (Quality of Service) in IP.

    C. In IPv6 a host cannot do fragmentation of IP packets.

    D. For IPv6, ICMP has been removed and the corresponding support for error handling has been built into IPv6.

    Comment:

20. Which of the following statements about DHCP (Dynamic Host Configuration Protocol) is *not correct*?

    A. DHCP is one of the few exceptions when it is OK to use an unspecified (0.0.0.0) IP source address.

    B. DHCP can be used to inform a unit about what DNS server it should use.

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

    D. DHCP uses TCP as the transport protocol.

    Comment:

Section B

1. Explain how TCP congestion control works in TCP. A complete answer should include the different phases of congestion control as well as how the sender's window size changes during the different phases. (4 p)

Solution:

The sender maintaiens two different windows per TCP conection: receiver-advertized window and congestion window (CWND). The window used at a given time is the smallest of the two. Congestion control consists of the following phases: slow start (exponential increase), congestion avoidance (additive increase), and congestion detecation (multiplicative decrease). Initially, CWND is set to 1 MSS. During slow start, it is increased exponentially until a certain threshold value is reached. Thereafter, congestion avoidance takes over and the CWND is increasing linearly. This increase continues until any of the following happens: 1) reciever-advertized window is reached, 2) duplicate ACKs are detected, or 3) the retransmission timer expires. If three duplicate ACKs in a row are detected, CWND will be decreased to a value somewhat below the previous threshold value and go to congestion avoidance. If the retransmission timer expires, CWND will be decreased to 1 MSS and go to slow start.

2. A client establishes a TCP connection to a server to transfer 48 kB of data. The one-way delay is 3 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. (2 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 = 6 ms (calculating the last ACK will also be considered OK, i.e. 1.5*RTT = 9 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 6 transmission rounds: 2 + 4 + 8 + 16 + 16 + 2 = 48 kB.

Thus it takes in total 1 RTT (connection establishment) + 5*RTT + RTT/2 = 6 + 5*6 + 6/2 = 39 ms. In this calculation, we did not include the ACK of the last segment. If that ACK is included, the transfer time is 42 ms. If the connection establishment was calculated as 1.5*RTT, the corresponding transfer times would be 42 and 45 ms respectively.

3. A key component in DNS is the 13 so called root servers. The root servers are "logical" servers, where each root server really consists of many servers located at different places in the world, and all servers have the same IP address. The root server "i.root-servers.net" with IP adresses "192.36.148.17" and "2001:7fe::53" consists for example of 55 different servers spread out over the world. (4 p)

   Explain how it is possible for several servers to have the same IP address. Discuss what the reasons could be for using this method. Give both advantages and disadvantages of the method.

Solution:

There is nothing that says that an IP address only can be at one place in the network. When the same IP address is announced by IP routing from several places, the routing protocols will automatically find the closest place.

An advantage with the method is that it makes sure that the nearest server with the given IP address is found, and that there is no need for special algorithms or protocols to locate the best server – IP routing takes care of it automatically! Should a server disappear for some reason, it will also be handled by IP routing, which will redirect traffic to another server.

A disadvantage of the method is that it breaks the addressing structure of the Internet, which is based on the principle that addresses that share a common subnet prefix are located near each other. Instead the entire address must be used by the routring protocols (that is, a subnet mask that is 32 bits long for IPv4), and that entire IP addresses for root servers must be stored in routing tables. That is a reason why this "trick", which is called "anycast", is only allowed for few servers on the Internet.

4. Consider the following forwarding table. (2 p)

Destination	Network mask	Next hop	Interface (port number)
110.0.0.0	255.0.0.0	–	m0
192.16.7.0	255.255.255.240	193.14.15.193	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
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

Specify next hop and outgoing interface for each of the following destination addresses: 192.16.7.14, 192.16.7.212, 194.17.22.4 och 193.14.5.188.

Solution:

192.16.7.13: 193.14.5.193, m1
192.16.7.17: 111.15.16.32, m0
194.17.22.4: 111.30.31.18, m0 (default route)
193.14.5.189: 193.14.5.189, m2 (destination directly connected on the subnet)

5. The network in Fig. 1 consists of two subnets, six computers (A to F) and two routers (R_1 and R_2). The IP addresses are specified by giving the network prefixes for each subnet, and for each network port there is a corresponding "host number" given for the subnet in question. Computer E has address 10.0.2.3., for example. For the MAC addresses, the following apply: Computer A has MAC address MAC_A, computer B has MAC address MAC_B, and so on. The MAC addresses for the router ports are given in the following way: Port P_1 on R_1 has MAC address MAC_{1-1}, P_2 on R_1 has MAC address MAC_{1-2}, osv. You can assume that all devices have compltet routing tables in the sense that each device knows the best (shortest) path to every other device in the network, as well as to the Internet. (4 p)

   a) Computer A has recently communicated with all other devices that appear in the figure. Specify the ARP table in A.
   b) Specify the routing table in router R_1, by filling in the table below. Assume that the table is complete, in the sense that R_1 knows the paths to all other devices in the network, as well as to the Internet.

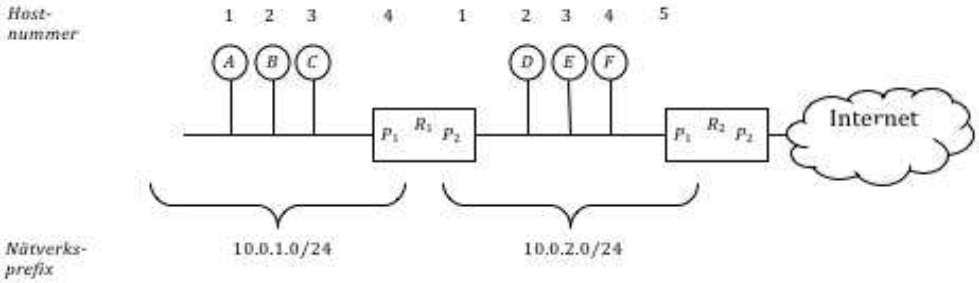

Fig 1: Network with two subnets

Destination	Network mask	Gateway	Interface (port number)

c) Node A sends an IP datagram to node E. The datagram will be placed in a frame, that cleary will go through R_1. Give the MAC addresses and IP addresses that appear in the frame received by R_1, and sent by R_1.

Solution:

a)

IP-adress	MAC-adress
10.0.1.1	MAC_A
10.0.1.2	MAC_B
10.0.1.3	MAC_C
10.0.1.4	MAC_{1-1}

b)

Destination	Network mask	Gateway	Interface (port number)
10.0.1.0	255.255.255.0	–	P_1
10.0.2.0	255.255.255.0	–	P_2
0.0.0.0	0.0.0.0	10.0.2.5	P_2

c) Frame received by R_1: IP source 10.0.1.1, IP destination 10.0.2.3, MAC source MAC_A, MAC destination MAC_{1-1}.

Frame sent by R_1: IP source 10.0.1.1, IP destination 10.0.2.3, MAC source MAC_{1-2}, MAC destination MAC_E.