Name and surname: _____

ID number: _____

Bachelor Programme
Computing

Communication Networks

Midterm exam example

Question	Solved - **YES/NO**	Points
9		
10		
11		
12		
13		
14		
15		
16		
	Sum	

I declare that, during this exam, I will neither enlist help of other participants, nor provide them with any help, and that I will not use any forbidden facilities. Such activities constitute a gross violation of the Behavior code and can cause permanent expulsion from the Faculty.

I also declare that my health status allows for me to take this exam.

Signature: _____

Multiple choice questions

Question 1
1 point

Which physical network topology is most commonly applied when deploying a local area network (LAN) that is based on the *Gigabit Ethernet* technology?

(a) Bus.
(b) Star.
(c) Ring.
(d) Complete connectivity.

Question 2
1 point

When an Ethernet switch receives a frame for which it does not know the outgoing port pertaining to the frame's destination MAC address, then the switch:

(a) creates and broadcasts an ARP query, in order to find out which port the destination station is connected to.
(b) changes the destination MAC address of the frame to "ff:ff:ff:ff:ff:ff", so that the frame can be delivered to all the stations connected to the switch.
(c) sends the frame out on all of its ports, except on the port that the frame was received on.
(d) drops the frame.

Question 3
1 point

Flooding, as a static routing algorithm, results in the forwarding of all incoming packets on a routing node:

(a) to all the interfaces of that node, except the interface the packet came from, if it is a packet this node hasn't already received.
(b) only to the interface that has the shortest distance to the next node (obtained by running the Dijkstra algorithm).
(c) only to the interface that has the shortest distance to the next node (obtained by using distance vector routing).
(d) to all the interfaces of that node.

Question 4
1 point

What does "early collision" in an Ethernet network indicate?

(a) The case when a terminal detects collision on a link during transmission of its frame.
(b) The case when a terminal detects collision on a link before beginning the transmission of its frame.
(c) The case when a terminal detects a collision on a link immediately after completing the transmission of its frame.
(d) The case when a terminal detects a collision on a link immediately after transmitting a jam signal.

Question 5
1 point

If the length of an ICMP message encapsulated in an IP-datagram equals 1100 octets, and the length of the corresponding IP-header is 20 octets, the value written in the *Total Length* field of the IP-header will be

(a) 1080 octets.
(b) 1100 octets. Total Length field defines the entire packet size in bytes
(c) 1120 octets. (data+header)
(d) 1500 octets.

Question 6
1 point

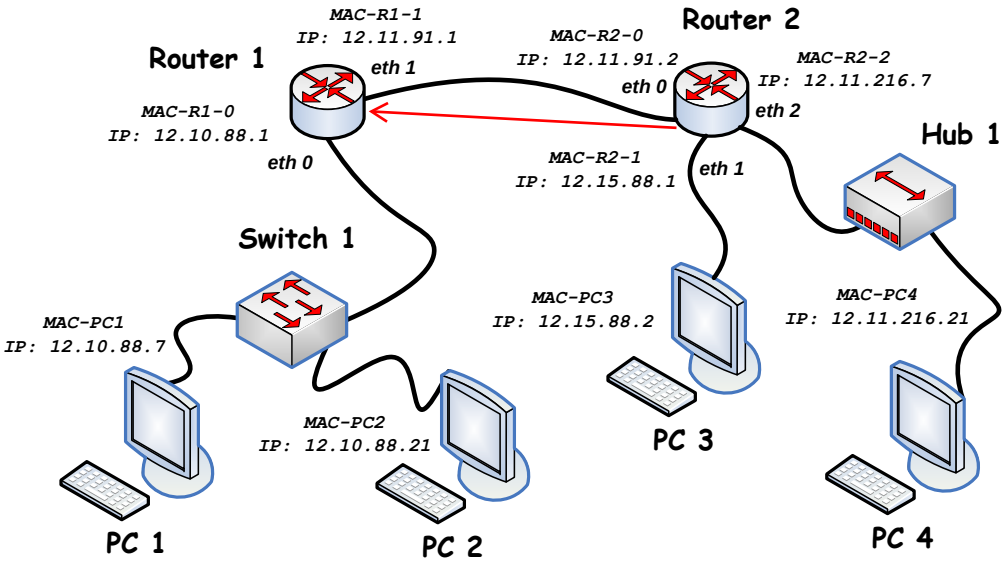
An IP-address range is defined as 192.168.10.128/28 (prefix-based IP representation). What is the total number of IP-addresses in the given range?

(a) 15
(b) 16 actual number = 14 = 2^4 - 2 (4 = 32-28, -2 from reserved)
(c) 31
(d) 32

*MAC addresses of the network interfaces are given symbolically (MAC-PC1, MAC-PC2, etc.). Network devices are connected to a 100BASE-T type Ethernet network. Routing tables on all the computers are static (i.e., **there is no prior communication between routers**), and they have been set properly. The implied value of the TTL parameter is 64 for all the computers. **All caches are empty.***

Figure 1.

Questions 7-8 relate to the network shown in Figure 1.



Question 7
1 point

In the network shown in Figure 1, computer PC 1 checks the availability of computer PC 3 by using the *ping* tool. Network traffic is being captured by Wireshark on interface ***eth0*** **of Router 2**. What will be the source and destination MAC address of the captured frame that carries the ***Echo Reply*** message?

(a) Source MAC-R1-1, destination MAC-R2-0
(b) Source MAC-PC-3, destination MAC-PC-1
(c) Source MAC-R2-0, destination MAC-R1-1
(d) Source MAC-PC-3, destination MAC-R1-1

Question 8
1 point

In the network shown in *Figure 1*, computer *PC 1* is sending a message to computer *PC 2*. Will the communication between those two computers at any point in time go through a router?

(a) Yes, always.
(b) Yes, but only when an ARP request is being sent.
(c) Yes, but only when the source does not know the MAC address of the destination.
(d) No, never.

Other questions

Question 9
2 points

500 GB of data is being transported between two computer centers in Zagreb and Vienna. The infrastructure the data is traveling through consists of 115 km of copper cables between Zagreb and Ljubljana, which have a transmission rate of 1 Gbit/s and a wave propagation speed of $2.3 \cdot 10^8$ m/s, and 280 km of fiber optic cable between Ljubljana and Vienna, which has a transmission rate of 10 Gbit/s and a wave propagation speed of $2 \cdot 10^8$ m/s. If the processing time along the way is disregarded, how long will the transmission between the two computer centers take?

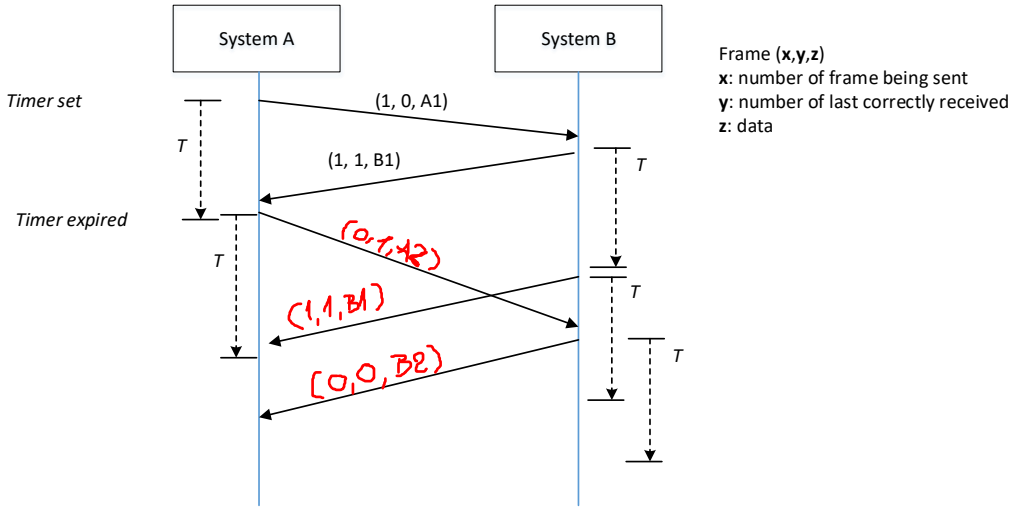
~~Transmission time LJ-V = 500*8*10^9 / 10*10^9 = 400 s~~ -> WE ONLY TAKE THE SLOWEST

Propagation time Z-LJ = 115*10^3 / 2.3*10^8 = 0.0005 s
Propagation time LJ-V = 280*10^3 / 2*10^8 = 0.0014 s
Transmission time Z-LJ = 500*8*10^9 / 1*10^9 = 4000 s
Total time = 4000.0019 seconds

Question 10
4 points

The figure shows a full-duplex protocol for a noisy channel and the first two frames in the communication between System A and System B.

(a) (3 points) Indicate the content of the **next three frames**.

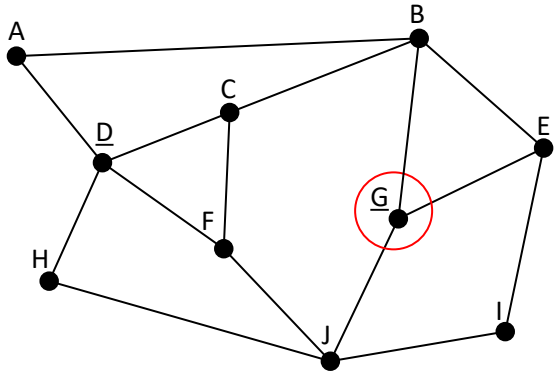


(b) (1 point) What is the size of a sliding window in the previous example? How could the efficiency of the given protocol be improved?

By increasing the size of a sliding window.
Increased sliding window size allows the sender to send more frames before needing acknowledgment.

Question 11
2 points

For the network in the figure below, assume that distance vector-based routing is used, with the goal being to create a routing table for node G based on known delay values. Delay vectors that node G has received from its neighbors are given in the table. The delays that have been measured between node G and its neighbors are also provided. Complete the routing table for node G, considering the known values.



Network graph

Delay vectors received from the neighbouring nodes

From: / To:	B	E	J
A	17	18	32
B	0	6	18
C	8	11	23
D	13	16	28
E	10	0	25
F	19	22	11
G	11	14	10
H	20	23	10
I	26	6	4
J	21	20	0

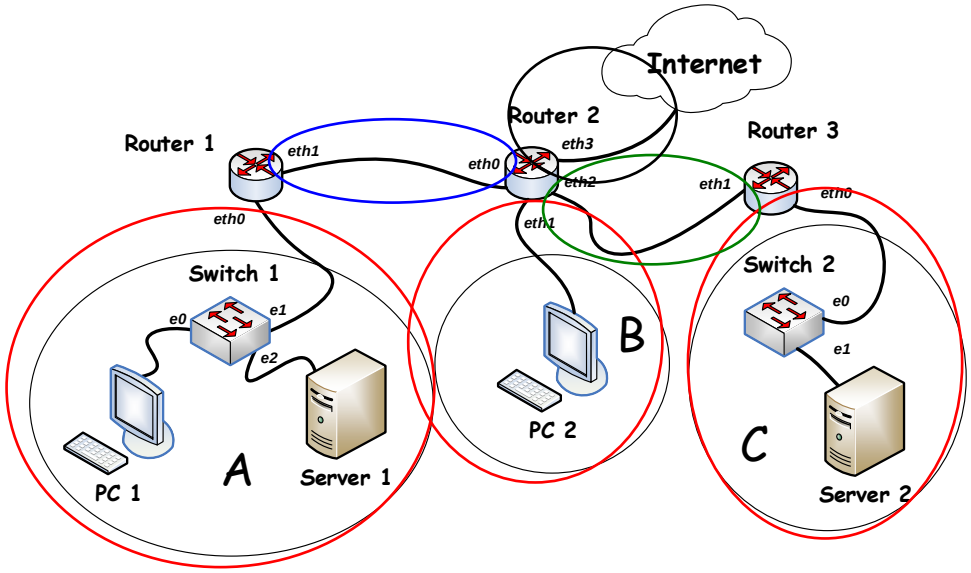
Node G routing table

To:	distance	interface
A	23	B
B	**6**	B
C	14	B
D	19	B
E	**7**	E
F	19	J
G	**0**	–
H	18	J
I	12	J
J	**8**	J

Measured delay:	G to B	G to E	G to J
	6	7	8

Figure 2.

Question 12 relates to the network shown in Figure 2.



Question 12
3 points

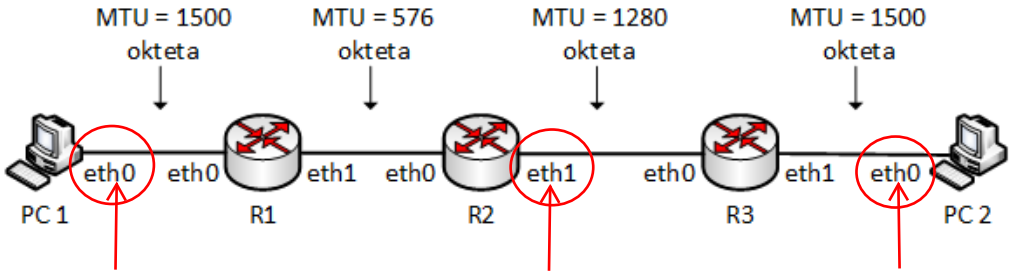
Assume you are a network administrator in a company called Networx Corp. and you need to configure all of the devices in the company network. The network topology is shown in Figure 2. Your task is to fill out the devices/interfaces table below with the corresponding values. IP-addresses of subnets A, B, and C are given below, while other subnet IP-addresses are arbitrary.

Subnet A: 10.0.0.128/28, subnet B: 10.0.0.160/28, subnet C: 10.0.0.224/28
NOTE: For inapplicable fields, write a dash (-).

Device (interface)	IP address	Default router IP address
Router 2 (eth3)	161.53.19.72	161.53.19.1
Router 1 (eth0)	10.0.0.129	10.0.0.145
Switch 1 (e0)	-	-
Switch 1 (e1)	-	-
Switch 1 (e2)	-	-
PC 1	10.0.0.130	10.0.0.129
Server 1	10.0.0.131	10.0.0.129
Router 1 (eth1)	10.0.0.144	10.0.0.145
Router 2 (eth0)	10.0.0.145	161.53.19.1
Router 2 (eth1)	10.0.0.161	161.53.19.1
PC 2	10.0.0.162	10.0.0.161
Router 2 (eth2)	10.0.0.200	161.53.19.1
Router 3 (eth1)	10.0.0.201	10.0.0.200
Router 3 (eth0)	10.0.0.225	10.0.0.200
Switch 2 (e0)	-	-
Switch 2 (e1)	-	-
Server 2	10.0.0.226	10.0.0.225

Question 13
3 points

A network is given in the figure below.



Computer PC 1 checks the availability of computer PC 2 with the *ping* command. The IP-datagram that carries the ICMP *Echo Request* message from PC 1 to PC 2 has a given size of 1300 octets, and the size of the ICMP *Echo Reply* message from PC 2 to PC 1 is the same. The figure shows MTU (*Maximum Transmission Unit*) values for each segment on the route from PC 1 to PC 2. Network traffic is being captured by *Wireshark* on the following network interfaces: *eth0* of PC 1, *eth1* of router R2, and *eth0* of PC 2.

Below are symbolically displayed the parts of the datagram relevant to the task: the *MF* flag (*More Fragments*), the field *Offset* (the Fragment Offset) and the data part of the IP datagram.

a) The IP datagram containing the ICMP message *Echo Request* sent from *PC 1* to *PC 2* is captured on the *eth0* network interface of computer *PC 1*. In the same way, sketch all IP datagrams captured on the *eth1* network interface of router R2 that were part of the previously sent ICMP message *Echo Request*.

Was already fragmented by earlier router

MTU = 576, data needs to have %8 = 0 true, header is 20 bytes
---> datagram = 552(data) + 20(header) = 572 bytes total

Echo Request

MF	Offset	DATA =
0	0	1 - 1280

1	0	1 – 552
1	69	553 – 1104
0	138	1105 – 1280

PC1-eth0 *R2-eth1*

b) The IP datagram containing the ICMP message *Echo Reply (*response to *Echo Request*) is captured on the *eth0* network interface of computer *PC 2*. In the same way, sketch all IP datagrams captured on the *eth1* network interface of router R2 that were part of the previously sent ICMP message *Echo Reply*.

1	0
0	157

1 – 1256
1257 – 1280

MTU = 1280,
---> datagram = 1256(data) + 20(header) = 1276 bytes total

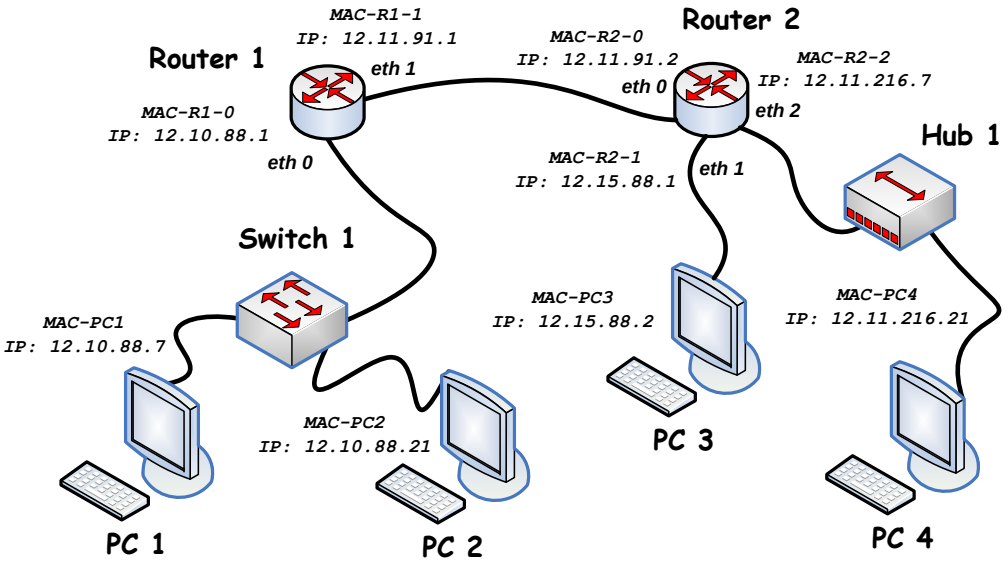
Echo Reply

MF	Offset	DATA =
0	0	1-1280

R2-eth1 *PC2-eth0*

*MAC addresses of the network interfaces are given symbolically (MAC-PC1, MAC-PC2, etc.). Network devices are connected to a 100BASE-T type Ethernet network. Routing tables on all the computers are static (i.e., **there is no prior communication between routers**), and they have been set properly. The implied value of the TTL parameter is 64 for all the computers. **All caches are empty.***

Figure 3.



Questions 14-16 relate to the network shown in Figure 3.

Question 14
2 points

In the network in Figure 3, the user of computer PC 1 wants to find out which nodes the packets addressed to computer PC 4 are likely to pass through. However, the *traceroute* tool, which is used for this purpose is not available on computer PC 1. Propose a series of *ping* commands that could be used to obtain wanted information about the path, and list the IP addresses of the nodes on the path, obtained from the output of the executed *ping* commands.

Reminder: Basic options of the ping command.

Option	Meaning
-c	number of *ping* packets to be sent
-i	wait interval between sending of *ping* packets, in seconds
-n	numeric output, instead of symbolic
-s	size of packets to be sent by the *ping* tool
-m	setting the TTL field of sent packets to a specified value

ping -m 1 12.11.216.21 //// TTL exceeded -> 12.10.88.1
ping -m 2 12.11.216.21 //// TTL exceeded -> 12.11.91.2
ping -m 3 12.11.216.21 //// TTL exceeded -> 12.11.216.21

Question 15
3 points

Network traffic is being captured by Wireshark on the network interface **eth1** of **router *Router 1***. Computer ***PC 2*** is sending an IP-datagram towards computer ***PC 4***. What is the source MAC address and what is the destination MAC address of the captured frame which contains that IP-datagram? What is the source IP address and what is the destination IP address of the IP-datagram that is carried by the captured frame?

Source MAC address	router1 mac
Destination MAC address	router2 mac
Source IP address	pc2 IP address
Destination IP address	pc4 IP address

What is the value of the TTL (Time To Live) field in the IP header of the captured IP-datagram? On which network node was the TTL value first decreased?

63 (64 -1 from router1)

Question 16
3 points

Network traffic is being captured by Wireshark on interface ***eth0* of Router 1**. Computer PC 1 checks the availability of computer PC 2 by sending the ICMP-message *Echo Request* to computer PC 2. After PC 1 successfully received the ICMP-message *Echo Reply,* computer PC 4 checks the availability of computer PC 2 in the same manner, by sending an ICMP-message *Echo Request* to computer PC 2, for which it receives a successful reply.

a) (2 points) Specify ICMP-message types, source and destination IP-addresses, and TTL values of IP-datagrams which are carrying ICMP-messages captured by Wireshark, in chronological order.

ICMP-message	Source IP-address	Destination IP-address	TTL
echo request echo reply	pc4 ID adress pc2 IP address	p2 IP address p4 IP address	62 64

b) (1 point) Specify entries in the ARP cache on computer PC4 after the scenario described in part (a) of the question has been completed.

ARP cache (*PC 4*)	
12.11.216.7	MAC-R2-2