**Question 1**
**1 point**

Computer *PC 2* sends an IP-datagram with an *Echo Request* ICMP-message to computer *PC 4*. Before sending the ICMP-message, *PC 2* sends an ARP-query. Which computers receive the mentioned ARP-query?

(a) Only computer *PC 1*
(b) Computer *PC 1* and router *Router 1*.
(c) Computer *PC 1* and routers *Router 1* and *Router 2*.
(d) Computers *PC 1*, *PC 3*, *PC 4*, and routers *Router 1* and *Router 2*

**Question 2**
**1 point**

What is the address of the „next hop" for the default route in the routing table of computer *PC 2*?

(a) 12.11.91.1
(b) 12.10.88.1
(c) 12.11.216.7
(d) 12.10.88.21

**Question 3**
**1 point**

A TCP-connection is established between two endpoints. If we assume that the receiver received a stream of segments with sequence numbers **0-1-2-3-5-6-4**, the receiver will generate the following acknowledgments:

(a) 0-1-2-3-4-5-6
(b) 0-1-2-3-5-6-4
(c) 1-2-3-4-6-7-5
(d) 1-2-3-4-4-4-7

**Question 4** (1 point)

POP3 (Post Office Protocol) uses:

(a) well-known TCP ports on both the client side and the server side.
(b) well-known UDP ports on both the client side and the server side.
(c) a well-known TCP port only on the server side.
(d) a well-known TCP port only on the client side.

**Question 5** (1 point)

During the processing in the protocol stack, a UDP-packet is encapsulated into:

(a) an IP-datagram.
(b) a TCP-segment.
(c) a Ethernet-frame.
(d) an application-layer protocol data unit.

**Question 6** (1 point)

Which of the following security requirements is violated by eavesdropping on unencrypted information during the transmission from source to destination?

(a) Confidentiality.
(b) Integrity.
(c) Availability.
(d) Authenticity.

**Question 7** (1 point)

What does „www" refer to, as a part of the symbolic address www.fer.unizg.hr?

(a) Domain.
(b) Computer.
(c) Subdomain.
(d) Fully Qualified Domain Name (FQDN).

**Question 8**
**1 point**

An association is a relationship established between the client and server processes on top of a given transport connection (e.g., TCP connection or UDP-binding). What information needs to be known in order to establish an association between the client and the server?

(a) Client and server IP-addresses, port numbers, application protocol. TRANSPORT?
(b) Client and server IP-addresses, client and server MAC-addresses, transport protocol, port numbers, application protocol. NO MAC?
(c) Client and server IP-addresses, client and server MAC-addresses, transport protocol, port numbers. ×
(d) Client and server IP-addresses, transport protocol, port numbers. APPLICATION?

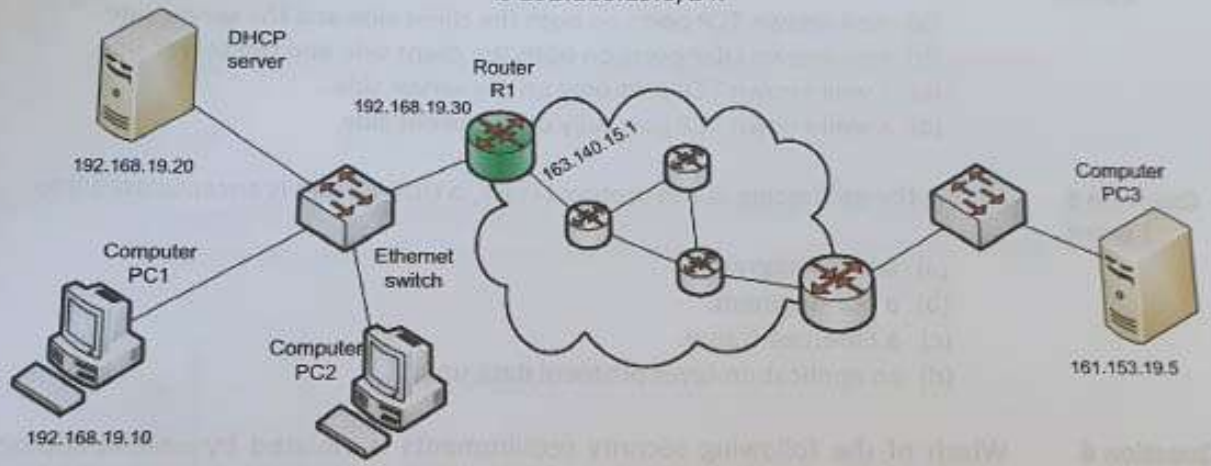
**Question 9**
**1 point**

Root DNS servers are the servers at the top of the Domain Name System hierarchy. Which of the following records is **not** contained in a root DNS server?

(a) An **NS** record for the name server of the .edu domain.
(b) An **NS** record for the name server of the .mit.edu subdomain.
(c) An **NS** record for the name server of the .hr domain.
(d) An **A** record for the name server of the .hr domain.

The IP address of the subnet to which the DHCP server and computers *PC1* and *PC2* belong to is 192.168.19.0/24.

**Figure 2.**




***Question 10 pertains to the network topology in Figure 2.***

**Question 10**
**1 point**

Router *R1* carries out the NAT (*Network Address Translation*) function for subnet 192.168.19.0/24. Computer *PC1* is sending an IP datagram to computer *PC3*. What are the source (label *Src*) and destination (label *Dst*) IP addresses of a datagram that is captured on the network interface of computer *PC1*?

(a) Src: 192.168.19.10, Dst: 192.168.19.30
(b) Src: 192.168.19.10, Dst: 163.140.15.1
(c) Src: 192.168.19.10, Dst: 161.153.19.5
(d) Src: 163.140.15.1, Dst: 161.153.19.5

## Other questions

**Question 11**
**2 points**

State 4 properties of the *User Datagram Protocol* (UDP) that make it **unreliable**:

- UNRELIABLE TRANSFER (LACK OF ACKNOWLEDGEMENTS, NO GUARANTEE OF DATA BEING DELIVERED)
- NO GUARANTEE REGARDING IN-ORDER DELIVERY
- DOES NOT PERFORM FLOW CONTROL
- DOES NOT DETECT PACKET LOSS, NOR DOES IT RETRANSMIT LOST PACKETS

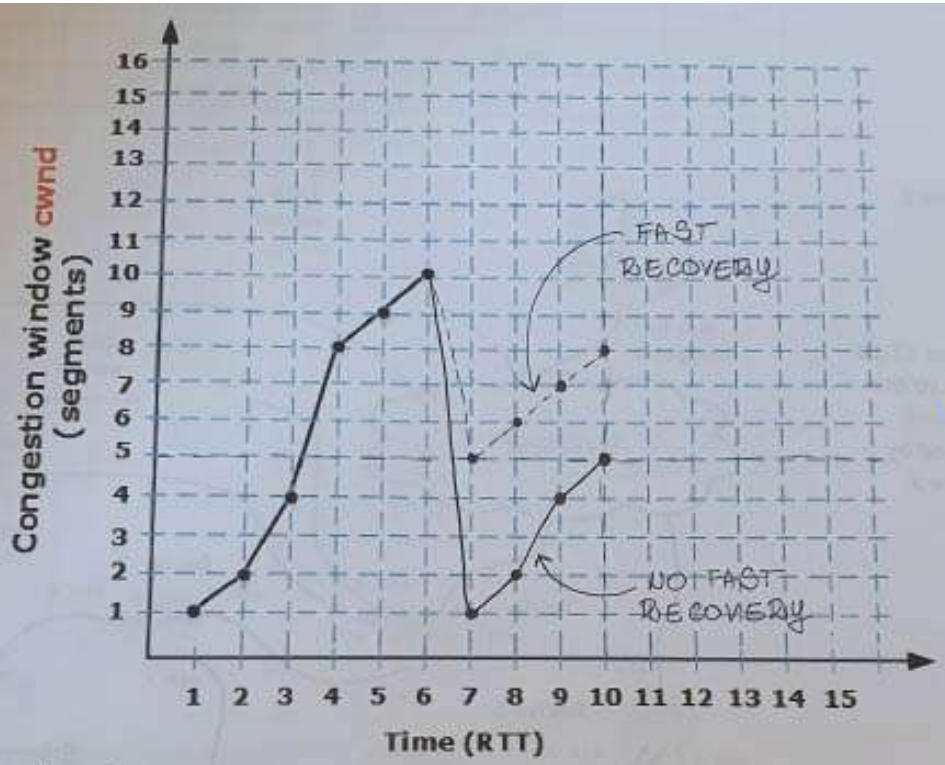
**Question 12**
**3 points**

The figure below shows how the congestion window size (cwnd) for a TCP-connection changes through time.

a) (1 point) Specify the starting and the ending point for the Slow Start phase.

From t = 1 to t = 4

b) (2 points) Continue the scenario from the figure: draw the window size between moments t=6 and t=10, assuming that a segment loss occurred in the moment t=6.



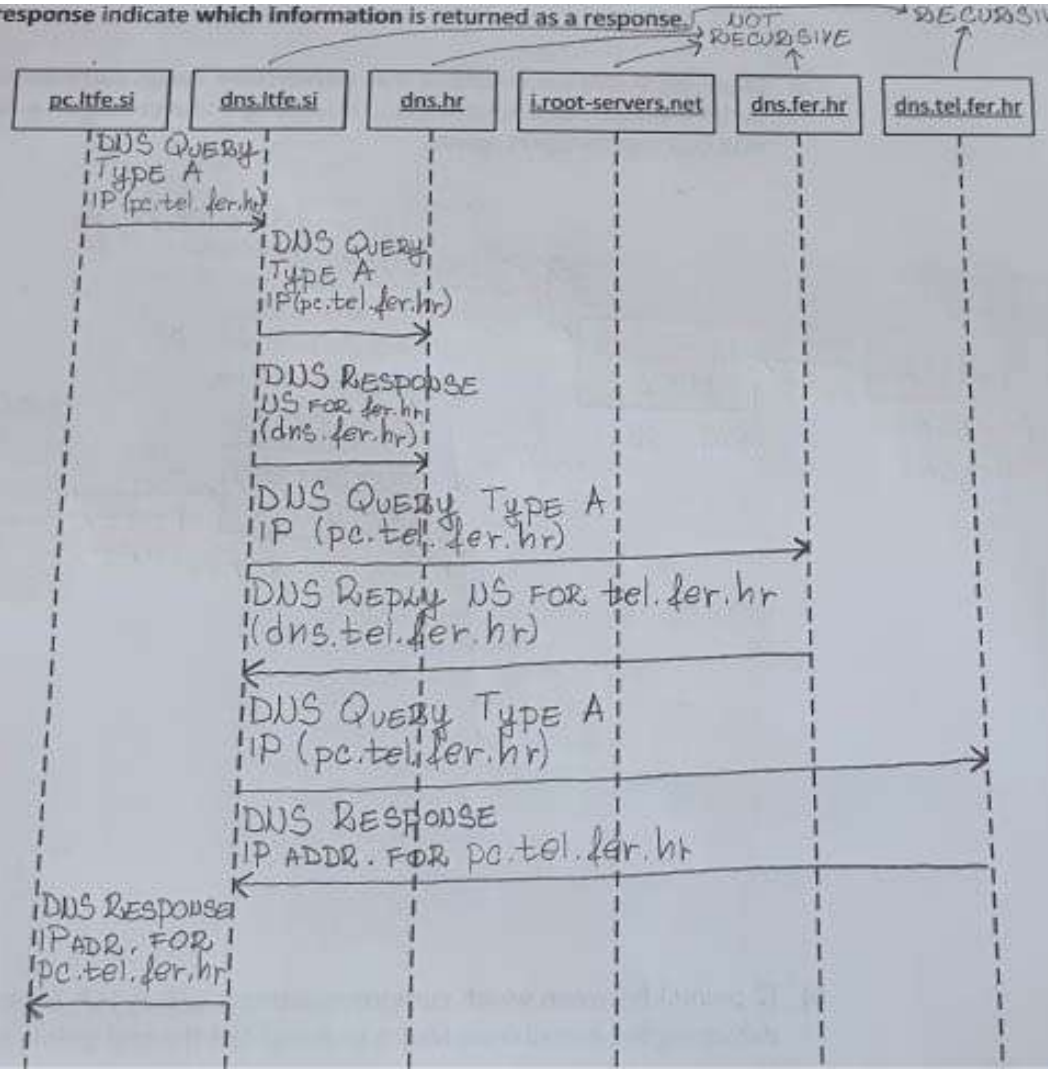

AT $t = 6$:

$ssthresh = max\{swnd/2, 2 \cdot MSS\} = max\{5, 2\} = 5\ MSS$

$cwnd = 1\ MSS$

(FAST RECOVERY: $cwnd = ssthresh = 5\ MSS$)

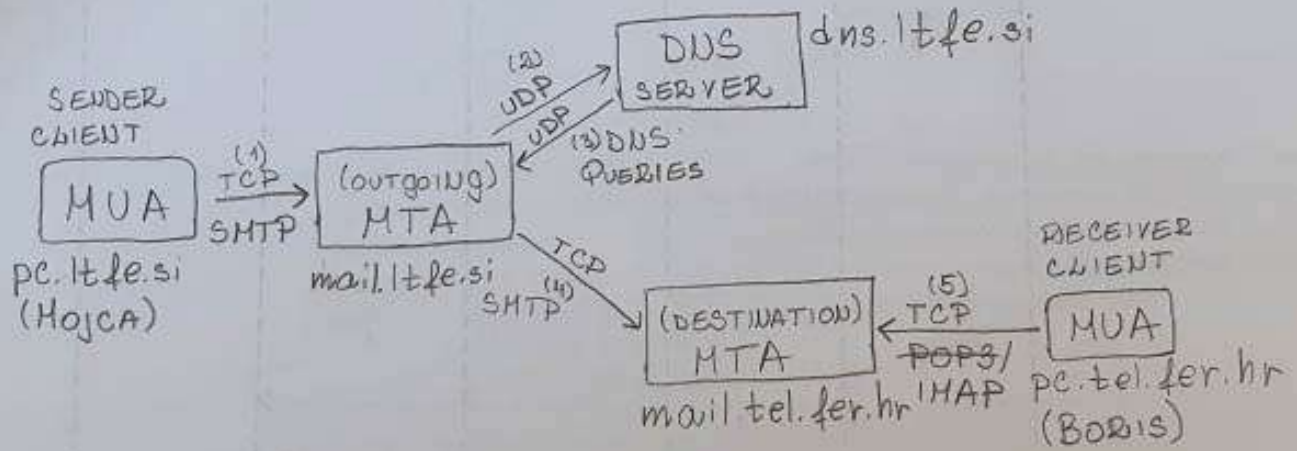
response indicate which information is returned as a response.



**Question 14**
**5 points**

Mojca is sending an e-mail from her address *mojca@ltfe.si* to Boris, whose address is *boris@tel.fer.hr*. The SMTP protocol, with well-known port 25, is used for sending the e-mail, and the IMAP protocol, with well-known port 143, is used for receiving the e-mail. Mojca is sending the e-mail from her computer named *pc.ltfe.si* and Boris is receiving the e-mail from his computer named *pc.tel.fer.hr*. The outgoing mail server in the *tel.fer.hr* domain is *mail.tel.fer.hr* and the outgoing mail server in the *ltfe.si* domain is *mail.ltfe.si*. DNS messages are sent over the UDP protocol.

a) (3 points) Sketch the electronic mail **architecture**. Assign corresponding computers used in the previously described scenario of sending and receiving an e-mail to your sketched mail user and transport agents.



b) (2 points) Between which computers/servers is(are) TCP connection(s) established while delivering the e-mail from Mojca to Boris? List the end-points of the required connections (the names of computers/servers and ports).

?

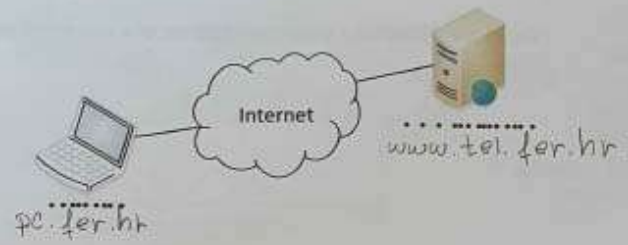
DYNAMICALLY ASSIGNED PORT

pc.ltfe.si → mail.ltfe.si
( ) (PORT 25)

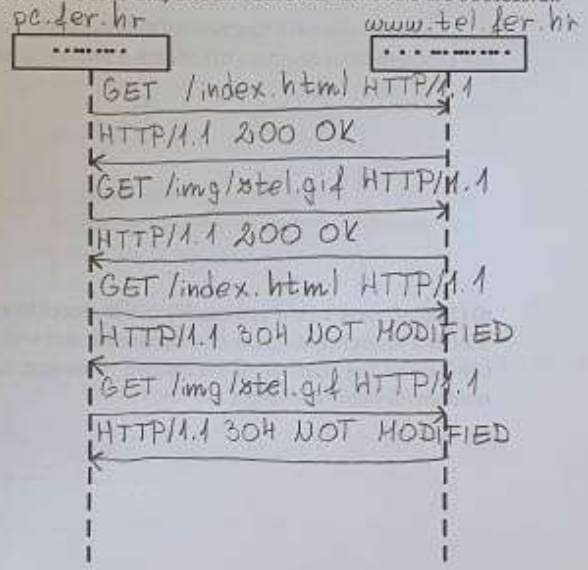
mail.ltfe.si → mail.tel.fer.hr
( ) (PORT 25)

pc.tel.fer.hr → mail.tel.fer.hr
( ) (PORT 143)

.hr, thus accessing the home page of the Department of Telecommunications. The web page ts of the HTML document *index.html* and an image *ztel.gif*, which is located on the same , with the exact location being /img/ztel.gif. After the web page is loaded, the user reloads me content.




(a) (3 points) Sketch all HTTP requests and HTTP responses in the sequence diagram below, indicating the first line of the request/response above every sketched message. Assume that at the start of the scenario the web browser cache on computer pc.fer.hr is empty and it stores all of the resources fetched during the scenario, that the HTTP protocol version used is 1.1, and all resource retrievals are successful.



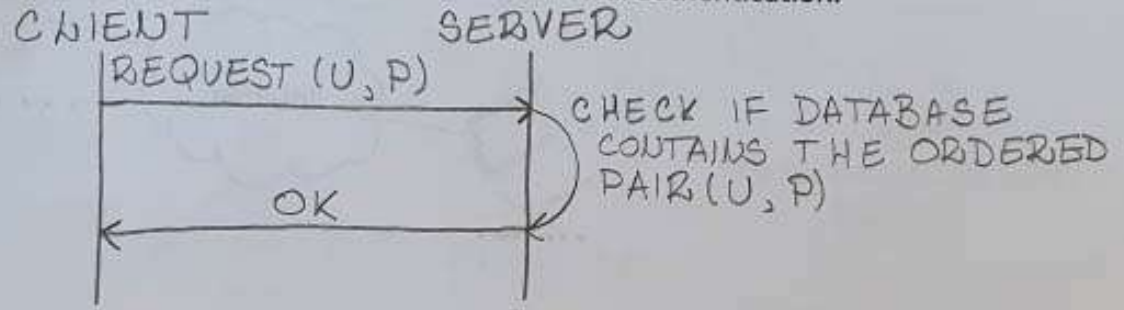

(b) (1 point) Explain how the web-browser on computer *pc.fer.hr* checks if cached content is fresh (up-to-date)? How does the server "know" if *pc.fer.hr* has an up-to-date copy of the resource or it needs to send it in a response?

IN ITS HTTP REQUEST, pc.fer.hr USES A CONDITIONAL GET WITH THE ATTRIBUTE if-modified-since PAIRED WITH THE TIME IT LAST GOT A RESPONSE WITH THIS RESOURCE.
IF www.tel.fer.hr's STORED RESOURCE HAS NOT BEEN MODIFIED SINCE THEN, pc.fer.hr HAS AN UP-TO-DATE COPY AND THE SERVER RETURNS 304 NOT MODIFIED.
IF THE STORED RESOURCE HAS BEEN MODIFIED SINCE THEN, THE SERVER RETURNS THE RESOURCE AND 200 OK.

**Question 16**
**4 points**

A client is authenticated on some server by sending a request containing a username (U) and password (P). The server then compares the received data with the values in its database. If the database stores an ordered pair username/password which correspond to the data that the server received, the authentication is successful (OK), and otherwise it is unsuccessful (FAIL). The decision about successful or unsuccessful authentication is sent as a response to the request (the response contains a string OK or FAIL). Answer the following questions:

(a) (1 point) Sketch a sequence diagram of a successful authentication.

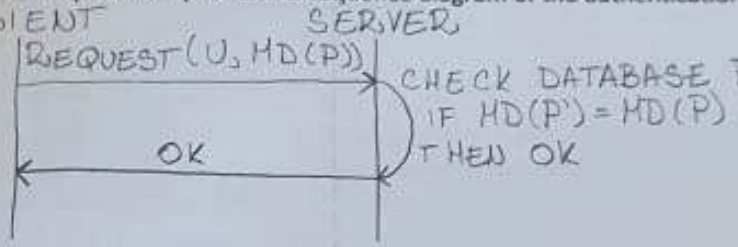



(b) (1 point) Which vulnerability exists in the system?

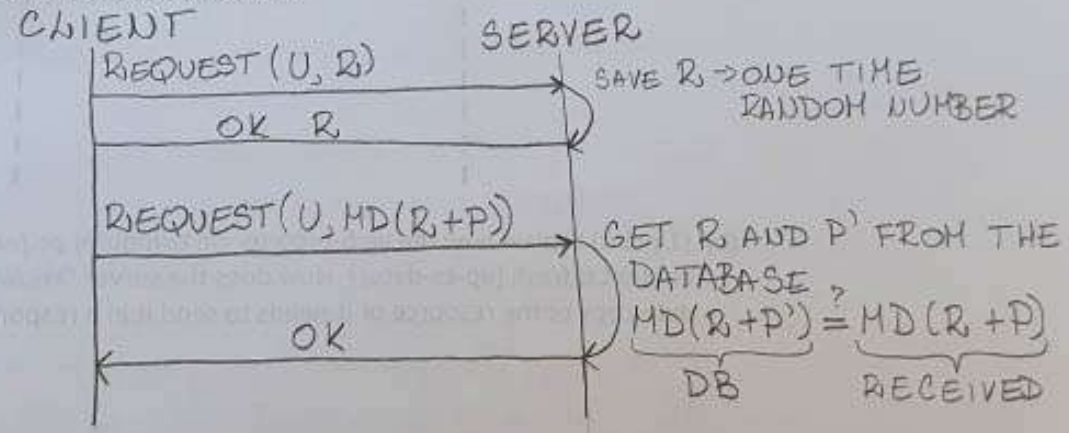
THE ATTACKER CAN INTERCEPT THE USERNAME AND PASSWORD AND CAN USE THEM TO AUTHENTICATE THEMSELVES AS THE CLIENT.

(c) (1 point) If the hash function MD() is available, how would you modify the protocol to solve the problem from question b)? Sketch a sequence diagram of the authentication in this case.

(c) (1 point) If the hash function MD() is available, how would you modify the protocol to solve the problem from question b)? Sketch a sequence diagram of the authentication in this case.




d) (1 point) How would you modify the protocol from question c) to prevent the replay attack? Sketch a sequence diagram of a successful authentication. Additional remarks: if needed, you can extend the number of exchanged messages to a total of 4 new messages, and/or add random numbers exchange.




THE SAME RANDOM NUMBER $R_1$ CAN'T BE REUSED, SO THE ATTACKER CAN'T USE IT

a) (2 points) Computers *PC 1* and *PC 2* establish TCP-connections with the computer *Server*. Computer *PC 1* is using source port 1555, while computer *PC 2* is using source port 1333. On the web-server *Server* the well-known port 80 is used. Enter the NAT-table entries on router *R* after both computers have established the connection with computer *Server*.

| *Private address: port* | *Public address: port* | *Destination address: port* |
|---|---|---|
| 10.0.0.5:1555 | 161.54.20.54.1555 | 151.73.22.8:80 |
| 10.0.0.3:1333 | 161.54.20.54.1333 | 151.73.22.8:80 |

b) (1 point) A web-browser is started on the computer *PC 1*. It is using HTTP protocol version 1.1 to access the web-server *Server* and load the web-page defined in the *index.html* file. The HTTP-request start line is specified as follows:

GET /web/index.html HTTP/1.1

Write the complete, absolute URI (*Uniform Resource Identifier*) for the *index.html* file, for which the HTTP-request was sent to the web-server:

http:// 151.73.22.8:80/web/index.html

IF BOTH PCs HAVE THE SAME PORT, WE WOULD HAVE TO CHANGE THE PORT IN THE PUBLIC MAPPING.