Communication Protocols and Network Security 2020/21
First Midterm

This test must be taken individually. Any and all literature may be used while taking this test. Answer diligently *all* questions.

Bonus points might be awarded if you at least partially correctly answer each question.

Duration of the test: 75 minutes.

We wish you a lot of success!

TASK	POINTS	MAX. POINTS	TASK	POINTS	MAX. POINTS
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Basics, bootp and DHCP.

QUESTIONS:

A) For what type of application protocols is UDP more appropriate as a transport layer protocol (we assume that the desired properties can only be provided by the transport layer and application protocols do not implement them themselves)? Justify the answer.

   (a) Traffic, where we do not require that packets arrive in the correct order, but we require that they arrive reliably.
   (b) Traffic, where we demand that packets arrive in the correct order, but we do not require that packets arrive reliably.
   (c) Traffic, where we do not require the correct order nor reliable arrival, but we require fast establishment of communication.
   (d) Neither.

B) Peter has a network at home on which an OpenWRT router takes care of Internet access. (i.) Can he have in the same network a DHCP server that is not on the same computer as the default gateway? Justify the answer. (ii.) How clients find out where to send packets if they default gateway does not assign addresses?

C) Ana and Borut run companies between which transactions often take place. Always one party executes the transaction and notifies the other party. The transaction is not valid until the first party receives confirmation from the second party. The transaction description is small enough that it can be transmitted with a single IP packet. Peter was given the task of outlining a protocol that Ana and Borut would be able to use. The first step was to opt for the UDP protocol on the transport layer because transactions happen really fast. (i.) Which fields should Peter's protocol contain (how should the datagram look like) to meet Ana's and Borut's requirements? What is the role of the fields you have defined. (ii.) How should Peter upgrade the protocol to ensure integrity? Justify the answer.

2. naloga: Network management.

QUESTIONS:

A) How does SNMPv3 prevent replay attacks?

B) (i.) What is MIB and what is it for? (ii.) Why is the existence of MIB good for the economy/industry? Justify the answer. (iii.) Let's say Peter has installed a new service on the server that reads the value of the thermometer. What

does Peter have to do to be able to operate a thermometer just like a router, for example? Justify the answer.

C) On his computer, which has the address 192.168.1.10, Peter ran:

```
peter@marogla: $
snmpwalk -c public -v1 localhost
iso.3.6.1.2.1.1.9.1.3.1 = STRING:
  "The SNMP Management Architecture MIB."
peter@marogla: $
snmpwalk -c vaglvuglbambam -v1 192.168.1.10
  iso.3.6.1.2.1.1.9.1.3.1
Timeout: No Response from 192.168.1.10.
```

(i.) Why does the snmpwalk command work the first time and not the second time? Describe at least two possible reasons. (ii.) Peter expected the printout to be longer. What does snmpwalk usually print out? In which file under GNU/Debian do we set this? Do we need to fix the file on the server or where we run snmpwalk? (iii.) Peter thinks that by using a really good secret string instead of *public*, he has secured his network well. Is this true? Justify the answer.

3. naloga: Real time.

QUESTIONS:

A) What protocol does NTP use for transport? Why this protocol?

B) In the form of real-time traffic packets, we mentioned that each packet contains at least a sequence number and a timestamp. (i.) However, if TCP were used on the transport layer instead of the UDP protocol, one of the two data could be omitted. Which one and why? (ii.) If you think about it, if the time stamps determine the sequence of packets. Why is a packet sequence number needed in addition to the timestamp? (iii.) The SRTP protocol allows data obfuscation. In fact, in addition to the data, most of the fields in the header could be obfuscated except one. Which one and why?

C) Peter set the clock on his computer in EFI. It worked properly for him under Microsoft Windows, but when he started GNU/Linux, the clock was one hour behind. (i.) Why could the problem described above occur? (ii.) If he set the clock in EFI, can he set it correctly using NTP? Will the clock remain set after restart? Justify the answer. (iii.) Which is better - that the time in the EFI and the time you show the user are the same or different? When could problems occur if they are, and when if they are not? Which problems are more severe?

HINT: At the end of October, you slept better than usual for at least one day. One day at the end of March, you slept worse.

4. naloga: Multicast

QUESTIONS:

A) Can *11110000...01* be a binary representation of an IPv6 multicast address?

B) The basic protocol for joining and leaving a multicast group is IGMP. (i.) Which transport protocol does it use? (ii.) Write down the field values in the IGMP packet and the recipient and sender addresses in the IP part of the packet if the device at IP address 1.2.3.4 wants to leave group 224.223.222.221? (iii.) Justify your answer.

C) OPTIONAL AND NOT FOR GRADING. This year we are celebrating the 250th anniversary of the birth of the amazing composer. Among other things, he admired the revolutionary leader Napoleon and dedicated one of his compositions to him, but the dedication was later revoked. (i.) What was the original name of the composition from 1803-1804? (ii.) What did he later rename it to when Napoleon was crowned emperor? (iii.) Who was this composer?

D) Peter is setting up his DHCP server. Wanting to find out how it communicates with the computer, he decided to capture some traffic. He ran the command below.

```
sudo /usr/sbin/tcpdump -i wlp4s0 port 67 or port 68
14:15:06.771635 IP 0.0.0.0.bootpc >
  255.255.255.255.bootps: BOOTP/DHCP,
  Request from 90:32:4b:35:2f:09 (oui Unknown),
  length 292
```

(i.) What is 255.255.255.255 in this case - the source or destination address? Justify the answer. (ii.) Can we talk about ports when we use multicast traffic, if the ports are used with TCP. For TCP we know that it does not support multicast. Justify the answer. (iii.) If Peter wanted to set his computer to always get the same address on the basis of which data or. data that the computer sends to the server can it do so? Justify the answer.