Communication Protocols and Network Security 2021/22
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) The Internet service provider (ISP) provides Peter with a static IP address. (i.) Is it possible that Peter has a DHCP mode for obtaining an Internet address enabled on his router? Justify the answer. (ii.) Is your answer valid for IPv4 or IPv6? Justify the answer.

B) Peter would like to set up all the computers in the company to boot over the network. He would like to boot some computers to Linux, others to FreeBSD. (i.) If he uses PXELINUX, on what basis can he select a set of settings? (ii.) If he does not want to set anything in the PXELINUX settings, where and how else can he make the bootloader different for different computers?

C) Peter is the chief systems engineer at *Butsol*, while Cefizelj is the chief systems prankster. His latest idea is to set up his own DHCP server for the entire company. (i.) How can this jeopardize cyber security in a company? Justify the answer. (ii.) What can Peter do to protect the company's computers from Cefizl's threat?

   HINT: Think about what DHCP usually offers to the connecting computer.

2. naloga: Network management.

QUESTIONS:

A) Can we run multiple SNMP agents on one system? If so, how?

B) One of the possible network attacks is packet replay attack. (i.) Describe the case where replay attack in the SNMP protocol can cause damage. Your description should be as accurate as possible. (ii.) Is there a mechanism for protecting against replay attack in the SNMP protocol? Justify your answer. (iii.) Draw a schema of the entire SNMP message, including the network and transfer protocols, with the focus on the SNMP part of the message. (iv.) Where in the message schema is the data transmitted (e.g., the number of packets received on the device) and how is the data stored in the message?

   HINT: The value `12345` alone, which would mean 12345 received packets, will not be enough. There must also be a description somewhere of what this number actually means.

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

```
peter> snmpget -c ’sv#;-Z!?4.2XY’ -v1 192.168.1.10 iso.3.6.1.2.1.1.9.1.3.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING:
  "The SNMP Management Architecture MIB."
peter> snmpget -c public -v1 localhost iso.3.6.1.2.1.1.9.1.3.1
Timeout: No Response from 127.0.0.1.
```

(i) Why does the `snmpget` 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 `snmpget` usually display? Is there any other command that would print more? What is it and what does it show? (iii) Peter considers that by using the string `sv#;-Z!?4.2XY` for authentication, he has secured his network well. Is this true? Justify the answer.

3. naloga: Real time.

Questions:

A) How does a program which receives music over RTP and plays it back through a sound card know which format the music is in?

B) The NTP service is used to synchronize the local time on the device with the global time. (i.) The NTP protocol is a protocol on the application layer. Which of the protocols UDP or TCP does it use on the transport layer? Justify why this one. (ii.) Roughly, in order to set its own clock, the client sends a request NTP to the server, that respond with his clock. Draw a time diagram that includes sending and receiving a query and response, and the processing time on the server. (iii.) Express the round trip delay of the packets from the diagram.

Hint: In the time diagram, highlight the events and use the expression setting tags to calculate the roundtrip delay.

C) Peter Zmeda develops electronic blinds. The blinds will not have a built-in clock and will connect to a server that will tell them which week of the year it is. A table will be written in the roller shutter controller at which time the roller shutter should be raised and lowered in a given week. The server will therefore simply send the week number of the year to the client each time a connection is established. The blinds will only have a 4 year warranty, after that Peter will not care what happens to them; all that matters to him is that the amount of traffic on the server is kept to a minimum. (i.) At least how many bits will the roller shutter server need to have? How many bytes? Justify the answer! (ii.) What tool / system program can he use on Unix systems so that he does not have to deal with opening sockets in the program on the server? (iii.) Write a program in any programming language that will print the number of the week of the year on the standard output in the format that Peter will use. In doing so, assume that you have the `time()` function available, which returns the number of seconds from 1. 1. 1970 at midnight. Peter will start selling blinds in 2024; from 1. 1. 1970 to 1. 1. 2024 will take 1704067200 seconds.

4. naloga: Multicast

QUESTIONS:

A) Can a switch obtain information on multicast groups and avoid broadcasting multicast packets to all members of a subnet? Justify the answer.

B) Butal Mayor Luka Kratkohlačnica imagined that a local radio station would be set up in Butale because this is now fashionable. The station will only broadcast over the Internet. Peter installed all the necessary equipment and the station started broadcasting through the multicast group `239.0.0.42`. (i.) Soon there was a need to broadcast via IPv6 multicast group as well. Suggest the group's address/number. Justify your answer. (ii.) Sketch a IGMP message sent by a device with IP address `1.2.3.4/24` that accesses the Internet through the gateway `1.2.3.1` when logging in to traffic of group `239.0.0.42`. The image should also contain all lower layers up to and including the network layer. (iii.) The virtuous people of Tepanje, as usual, watched what their neighbors, the Butalci, were doing. They also decided to set up their own radio station and, as in Butale, they also chose the multicast group `239.0.0.42`. Will this work? Justify the answer.

C) OPTIONAL AND NOT FOR EVALUATION. For the second time in its history, Slovenia is chairing the EU Council. However, this is not the first time she has been entrusted with such an important role. Exactly 200 years ago, the *Holy Alliance* met in Ljubljana, Carniola. (i.) Which monarchies made up the Holy Alliance? To help, there were only three. (ii.) List at least three monuments/buildings/... that can still be found in Ljubljana today and are reminiscent of the Congress?

D) Peter would like to have only one DHCP server in the entire company, even though he has more than one subnet. (i.) Is this possible, or do we need one server for each network? Justify the answer. (ii.) Can it turn on booting of computers over a network on one subnet and not on another? Justify the answer. (iii.) Can a DHCP server also assign multicast addresses? Is such functionality useful? If yes, write how. If not, explain why not.