Communication Protocols and Network Security 2019/20
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: 60 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.

VPRAŠANJA:

A) What is SecureBoot supposed to protect?

B) Peter has learned how to setup a personal DHCP server. He has setup his DHCP server on the following IP address 192.168.1.10. While he was configuring his server, he noticed that the server already got an IP address from someone else. Peters configuration looks like this:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100;
  option routers 192.168.1.10;
}
```

(i) Where does this (second) DHCP server physically exists? Keep in mind that you are working with typical home network. (ii) Unfortunately clients, that get IP address from Peter, do not get the access to the Internet, while the clients, that get IP address from other DHCP server, do. Which setting should Peter fix, to get the Internet working? (iii) With which commands / exactly how can he get the right settings, that he has to setup? (iv) Is it possible, that there are multiple DHCP server working inside a single network? Justify your answer.

C) Peter's ISP provider also offered a set of IPv6 addresses, which he gladly accepted. However, he is having issues with the setup of the DHCP server. He read somewhere, that he has to setup a new DHCPv6 server. (i) Which technical limitation prevents the use of DHCP protocol for IPv6? Justify your answer. (ii) Also `bootp` service only works over IPv4. How would you use it for setting up computers, that would be connected to a IPv6 network? Describe your solution. (iii) What about `tftp` protocol, does it work over IPv6? Justify your answer.

2. naloga: Network management.

VPRAŠANJA:

A) SNMP has three forms of communication: request/response between manager and agent, messages from agent to manager, and messages between managers. (i) Which of the three mentioned forms of communication does the `snmpget` command use? Justify your answer. (ii) On the lectures Peter heard about the following three network management standards: MIB, SNMP and BER. Is the BER standard used in the MIB or SNMP standards? Justify your answer. (iii)

Peter decided to setup a second management node, but he does not know, if it should be in the same local network (LAN) as the first one. What do you think? Justify your answer. (iv) One of the managed devices in the described Peter's network is also a 3D printer. Where are all possible location that store the data about the weight of all the printed objects? Justify your answer.

B) Peter's computer has an IP address 192.168.1.10, and he ran the following commands on it:

```
peter@marogla: $
snmpget -c public -v1 localhost 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@marogla: $
snmpget -c vaglvuglbambam -v1 192.168.1.10 iso.3.6.1.2.1.1.9.1.3.1
Timeout: No Response from 8.8.8.8.
```

(i) Why did the command `snmpget` work for the first time, but not for the second? (ii) If he is using SNMPD on Debian OS, which file does he have to fix? (iii) How would an attacker in the network get to the secret string (*vaglvuglbambam*)? Justify your answer.

C) What is the meaning of the following sequence of bytes written in ASN.1 BER format (the values are decimal the first byte that arrived is on the left and note that the ASCII code for the letter `A` is 65_{10}.): `2 2 4 80 4 2 73 80 2 2 4 72`.

3. naloga: Real time.

VPRAŠANJA:

A) Why is TCP protocol not suitable for the real-time data transfer? Justify your answer.

B) Peter would like to synchronize his time with the Internet server. Unfortunately he is not being successful. He ran `rdate ntp1.arnes.si`, with which he should set his time to the time of the `ntp1.arnes.si` server (for which we know that exists) and got the following response:

```
rdate: ntp1.arnes.si: Name or service not known
```

(i) Would it be any better if he used address `193.2.1.117` instead of FQN `ntp1.arnes.si`? Justify your answer. (ii) List at least 2 reasons why this error could occur and for each how to fix it. (iii) Peter noticed that his

computer on a local network has the IP address 169.254.1.2. How did he obtain it? What would he have to do, to get the mentioned command working, while using only this IP address?

C) With the help of NTP service we can access the network time. (i) Which protocol on the transport layer uses this service and why? (ii) Peter Zmeda failed to setup NTP server in his network. So, he decided, that one server will send a (*multicast*) packet with the exact time every minute, while other devices will simply receive the packet and setup their time accordingly. Discuss Peter's approach. In Peter's network there are only 42 devices. (iii) Let say, that the current time on the device is `02:06:06` and then it gets `ntp` message, where the real time is `02:06:02`. What should it do? Just simply move time backward? Justify your answer.

4. naloga: Multicast

VPRAŠANJA:

A) How can we determine whether any network device is a member of a particular multicast group? Justify your answer.

B) On Figure Figure 1 we have the topology of Peter's network. (i) Let say, that

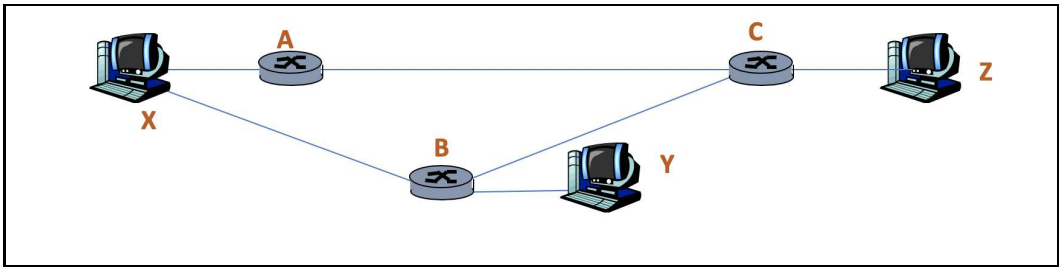

Figure 1: Flooding.

device `X` floods the network with packets. How should the routing table on the router `C` look like, that it will only acknowledge the packet coming from `X` over the router `B` and not over the router `A`. Justify your answer. (I) What type of routing trees are build in dense networks? Why?

C) OPTIONAL AND NOT FOR GRADING. This year we are celebrating the 100th anniversary of the University of Ljubljana. (i) Who was its first rector, or at least what was his research area? (ii) What was the first lecture about on a newly established university or even who had it?

D) Peter is setting up his DHCP server. Because he wants to know how it communicates with a computer, he decided to capture some network traffic. He ran the following command:

```
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 type of an IP address is 255.255.255.255? (ii) Group 224.0.0.12 is reserved for "DHCP Server / Relay Agent". Where in the configuration of the typical DHCP server can we see this? (iii) Peter wants to setup his computer in such a way, that it would always get the same IP address. On the basis of which information, that computer sends to DHCP server, can he achieve this? Justify your answer.