# Komunikacijski protokoli in omrežna varnost 2011/12 Prvi kolokvij

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.

Successfully – veliko uspeha!

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

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

**1. naloga:**

VPRAŠANJA:

1. There is only one computer at the company Peter Zmeda (a.k.a. Peter Confusion) works for, Horuk. He has assigned his computer the IP address 192.168.0.12 and the name `Peter.Horuk.intranet`. He has also bought another computer and assigned it the IP address 192.168.0.24 and the name `Pavel.Horuk.intranet`. Because he only has two computers, he has no need nor desire to set up a DNS server. What can he do on the first computer so that he can use simple commands like `ssh Pavel.Horuk.intranet`?

2. A bootp packet contains among other things a field called `xid`. Which functionality does the protocol provide using this field? Explain your answer.

3. The bootp protocol does not support any sort of protection against atackers who might slip a trojan horse onto our computers. They can get our computers to boot a maliciously modified operating system. Describe two methods of defending against such an attack. For each of the methods, describe which changes would be neccessarry on the client and server side. Would similar methods also be neccessary and work for DHCP?

**2. naloga:**

VPRAŠANJA:

1. Peter Zmeda added to its system besides (i) computers from the first question a (ii) printer. He also added an interface (iii) which he uses to monitor and manage telephone conversations. Furthermore, he would like to manage and control his whole system from one central point. To achieve that, he decided to build an entire management infrastructure. Which components should this infrastructure constist of? Name and describe each of the components. Write down where each of the components is located. At which component the MDB is located?

2. The SNMP protocol supports multiple types of messages. One of them is `InformRequest`. Describe an example usage of this type of message, applicable to Peter's company.

3. At the last CEO's meeting, Peter learned that the managers have to take care of employees' rest and relaxation. Apparently, rest and relaxation boost productivity. That is why Peter wrote an on-line game for his employees to play

with. The game has become extremely popular. It runs on the server, while the employees use their web browsers to play it. Because his SNMP infrastructure is already installed and he can use it to manage all his hardware, Peter has come up with the idea of using the same infrastructure to monitor and control the game server. How should he achieve this? Describe at least 5 components he should prepare. Describe two of the components in detail.

**3. naloga:**

VPRAŠANJA:

1. One of the modes of operation for the NTP protocol is also the periodic re-transmission of current time. When would it make sense to use multicast on the network layer for these re-transmissions? Explain your answer.

2. Which are the two core functionalities that the RTP protocol provides?

3. The RTP protocol allows transfer of a stream of data which is created in real time, from a server to a client. In such a stream of data, the source is specified in the SSRC field. Suppose that Peter Zmeda installs a transmitter in the bell-tower of st. Thomas church in the parish Novaki. There are four bells in the bell-tower. The transmitter transmits the ringing of the bells which signifies the passage of time, every 15 minutes. In Novaki, there's also a very active group of bell-ringers who use the bells as instruments. They play on the bells on special occasions, usually accompanied by pipe-organs. In all of the situations described above, the small bell is one of the event sources. Is in the data stream, the data from the small bell always marked with the same SSRC id? How can the receiver determine, which data comes from the small bell? Explain your answer. The more precise the answer is, the more points you will get.

4. The ringing every 15 minutes also marks the time. How can Peter ensure that the receivers will beleive, that the sound they are receiving is genuine and has not been forged (for example through a replay attack)?

**4. naloga:**

VPRAŠANJA:

1. Peter's network has a special router at the point of connection to the Internet. This router receives a packet with the address FF11:FF0E:FF05:: on its port connected to the Internet. What should it do with the packet? Explain your answer.

2. One of the queries that the IGMP protocol supports is a query of which groups exist. We mentioned that the address 224.0.0.1 is used as a parameter in this queries. Where exactly in the query message is this address used? Why this particular address is used?

3. When talking about multicast, we also mentioned a rendez-vous point – RP (central point). What is the role of such a node in multicasting? Does the IGMP protocol know anything about RP? Explain your answer.