

# Komunikacijski protokoli in omrežna varnost 2017/18 Prvi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena. Odgovorite pazljivo na *vsa* vprašanja.

Če boste uspešno vsaj delno odgovorili na *vsa* vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 60 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: \_\_\_\_\_

ŠTUDENSKA ŠTEVILKA: \_\_\_\_\_

DATUM: \_\_\_\_\_

PODPIS: \_\_\_\_\_

**1. naloga:** Peter je pognal `ifconfig` in zagledal naslednje:

```

root@bombica:/home/student# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:12:34:58
          inet addr:169.254.129.66  Bcast:169.254.255.255
Mask:255.255.0.0
          inet6 addr: fe80::5054:ff:fe12:3458/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1494394 (1.4 MiB)  TX bytes:627710
(612.9 KiB)
          Interrupt:11 Base address:0xa000
root@bombica:/home/student#

```

## VPRAŠANJA:

- A) (i) Ali računalnik ima IPv4 naslov? Kaj pa IPv6? (ii) Če ima internetni naslov, kakšen je? Če nima, kako veste, da nima? (iii) Ali računalnik ima dostop do `www.google.com`? Utemeljite odgovor. (iv) Kateri omrežni vmesnik, ki ga imajo običajno računalniki, manjka?
- B) Protokol `tftp` uporablja za prenos protokol `udp`. (i) Pri prenosu datotek je zadnji paket v `tftp` različen od vseh prejšnjih. Kako in zakaj? (ii) Recimo, da bi `tftp` uporabljal za prenos protokol `tcp`. Kako bi ga lahko spremenili in se izognili omejitvi iz prejšnjega vprašanja? Utemeljite svoj odgovor.
- C) Kakšen je vrstni red (od najmanjšega proti največjemu) (i) IPv4, (ii) IPv6 in (iii) MAC naslovov ter (iv) številke vrat glede na število možnih vrednosti? Odgovor utemeljite.

**2. naloga:** Peter Zmeda uporablja protokol `SNMPv2` in tiskalnik v tretjem nadstropju mu neprestano sporoča, da mu je zmanjkalo papirja. Peter je poklical servis, ki je nedvoumno ugotovil, da stikalo za zaznavo papirja in celoten tiskalnik delujeta brez napake. Peter je zato pričel sumiti, da je nekaj narobe s protokolom. Tiskalnik pošlje sporočilo o tem, da je zmanjkalo papirja, kot obvestilo (*trap*).

## VPRAŠANJA:

- A) (i) Opišite, kaj bi lahko ušpičil Cefizelj, da bi sprehajal Petra? Utemeljite odgovor. (ii) Ali bi bilo kaj boljše, če bi upravljalca agenta na tiskalniku spraševal o stanju papirja s pomočjo zahteve in odgovora? Utemeljite odgovor.

- B) Kako protokol SNMPv3 preprečuje napade s ponovitvijo (*replay attack*)? Utemeljite odgovor.
- C) Peter bi rad uporabljal SNMP za nadzor svojih računalnikov – predvsem ga zanima, koliko prostora ima vsak računalnik na disku. Na Internetu je zasledil, da je ta podatek na voljo pod OID .1.3.6.1.4.1.2021.9.1.9.1. (i) Kako bi prebral ta podatek? Napišite konkreten ukaz. (ii) Peter je ukaz zagnal, a ne dobi podatka. Sumi, da nekaj ni v redu z njegovimi pravicami. Katero datoteko bo moral popraviti in kako, da bo lahko do podatka prišel? (iii) Kako bi lahko dani OID spremenil v kaj človeku prijaznejšega? Napišite konkreten ukaz.

### 3. naloga: Stvarni čas.

#### VPRAŠANJA:

- A) Protokol RTP ponuja prenos paketov tako, da prejemnik lahko ugotovi njihov vrstni red in še nekaj. (i) Kaj je druga stvar in čemu služi? (ii) Recimo, da bi RTP uporabljal za prenos protokol tcp, katerega od omenjenih dveh podatkov bi ne bilo več potrebno prenašati v paketu in zakaj? (iii) Zakaj uporablja RTP udp kot prenosni protokol? Zapišite vsaj dva razloga.
- B) SRTP je varni RTP protokol. (i) Koliko RTP paketa šifriramo z njim: (a) IP, UDP in RTP del; (b) celoten RTP paket; (c) samo vsebino RTP paleta, ali (č) tako UDP kot RTP del? (ii) Utemeljite *zakaj* je prav ta del šifriran in preostanek (npr. MAC glava in še kaj) pa ne.
- C) Peter se je odločil, da je NTP prezapleten, zato bo raje razširil protokol rdate tako, da bo čas prenešen kot 32-bitno nepredznačeno število, ki predstavlja stotinke sekund od 1. 1. 1970 ob polnoči. Za svoj protokol bo uporabil vrata 3700. Napišite odjemalca za novi protokol v poljubnem programskem jeziku. Lahko si pomagate s spodnjim ne povsem delujočim rdate odjemalcem v jeziku Java.

```
import java.util.Date; import java.io.*; import java.net.*;
class RDate {
    public static void main(String[] args)
        throws IOException {
        Socket s = new Socket("ntp1.arnes.si", 73);
        long d;
        d = new DataInputStream(s.getInputStream()).readInt();
        System.out.println(new Date(d * 1000 - 22089888001));
    }
}
```

**4. naloga:** Razpošiljanje.

## VPRAŠANJA:

A) Ali lahko pričakujemo PIM pakete na domačem omrežju: (a) ne, ker se PIM uporablja na omrežjih, kjer med dvema točkama obstaja več kot ena pot; (b) ne, ker se PIM uporablja le do domačega usmerjevalnika, medtem ko na domače omrežje ti paketi ne pridejo; (c) da, saj PIM potrebujemo za razpošiljanje, ali (č) da, saj PIM potrebujemo za gledanje televizije prek IP. Odgovor utemeljite z opisom scenarija, ki nastopi pri vašem odgovoru – kdo kaj od koga hoče in kaj zato komu pošlje.

B) Peter je v podjetju prevzel v upravljanje računalnik, ki skrbi za razpošiljanje (*multicast*) v podjetju. V ta namen sta na računalniku dva programa – `listRP`, ki izpiše vsa možna osrednja vozlišča (*rendez-vous points*) ter `setRP`, ki nastavi osrednje vozlišče. Petru so pojasnili, da če razpošiljanje neha delovati, ga lahko popravi tako, da se prijavi na računalnik in požene ukaz: `../pavel/bin/listRP | head -n 1 | ../pavel/bin/setRP`. (i) Kako bi isti ukaz zapisal tako, da bi uporabil le poti, ki se začnejo s /? Privzemite, da je njegovo uporabniško ime `peter` in da se njegov domači imenik nahaja na običajnem mestu. (ii) Recimo, da `listRP` izpiše:

```
192.168.1.1
192.168.1.2
192.168.1.7 .
```

Napišite ukaz, ki ga Peter lahko uporabi, da nastavi osrednje vozlišče na naslov 192.168.1.12, ki bo deloval ne glede na to, v katerem imeniku je Peter trenutno.

C) NEOBVEZNO IN NI ZA OCENO. Peter Zmeda je zbiratelj slikanic. V svoji zbirki je še posebej ponosen na prvo slovensko slikanico, ki je izšla pred natanko sto leti. Kdo je avtor besedila, kdo avtor slik in kakšen je njen naslov?

D) Iz slikanice je Peter naredil risanko, ki jo bo poslal prijateljem z uporabo razpošiljanja (*multicasting*) v IPv6 omrežju. Želi še, da bi si risanko lahko ogledali samo njegovi prijatelji. (i) Kakšen naslov nas si izbere za razpošiljevalno skupino in zakaj? (ii) Prijatelji so razpršeni po svetu in zato bo uporabil za gradnjo usmerjevalnih tabel kateri PIM protokol ter zakaj? (iii) Kako naj zagotovi, da bodo lahko risanko gledali samo prijatelji? Utemeljite odgovor.

NAMIG: Opišite postopek od tega, ko prijatelj izrazi željo do tega, da lahko gleda risanko ter vse tako Petrove kot prijateljeve korake.