# Kolokvare

Kolokvara 2019/20

## 1. naloga: Osnove ter bootp in DHCP. VPRAŠANJA

**A) Kaj naj bi ščitil SecureBoot?**

a) SecureBoot ščiti pred zlonamerno programsko opremo oz. pred neavtentičnimi poizvajalci.

**B) Peter se je na vajah naučil, kako postaviti svoj strežnik DHCP. Doma si ga je postavil na naslovu 192.168.1.10. Ko ga je postavil, je opazil, da mu na omrežju nekdo že dodeljuje IP-je. Petrova konfiguracija izgleda takole:**

*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) Kje se ta (drugi) DHCP strežnik najverjetneje fizično nahaja? Upoštevajte, da gre za tipično domače omrežje. (ii) Na žalost odjemalci, ki dobijo naslov od Petra, ne pridejo do Interneta, odjemalci, ki dobijo naslov od drugega DHCP strežnika, pa. Katero nastavitev menite mora Peter popraviti? (iii) S katerimi ukazi / natančno kako izve prave vrednosti, ki jih mora nastaviti? (iv) Ali sploh lahko na istem omrežju sobiva več strežnikov DHCP? Utemeljite odgovor.**

b) i) na njegovem usmerjevalniku.
ii) najverjetneje mora popraviti *option routers* na njegov privzeti prehod
iii) z ukazom ip a pogleda, kateri je njegov privzeti prehod in ga popravi z le-tem.
iv) Da lahko, vendar moramo paziti, da ima vsak DHCP strežnik svoje naslove, ki jih razdeljuje, zato da zagotovimo, da ima vsak client avtentični naslov.

**C) Petrov ISP ponudnik mu je ponudil še nabor IPv6 naslovov, ki jih je seveda Peter z veseljem sprejel. Zatika pa se mu z DHCP strežnikom. Nekje je prebral, da mora namestiti nov, DHCPv6 strežnik. (i) Kakšna je tehnična omejitev, ki preprečuje možnost uporabe DHCP protokola za IPv6? Utemeljite odgovor. (ii) Tudi bootp storitev deluje samo na IPv4. Kako bi le lahko z uporabo le-te postavili računalnik, ki bi bil povezan v IPv6 omežje? Opišite rešitev. (iii) Kaj pa protokol tftp, ta deluje na IPv6? Utemeljite odgovor.**

c) i) IPv6 uporablja posebno verzijo standarda DHCP, ki se imenuje DHCPv6, zato ga ne moremo uporabiti pri *IPv4* DHCP serverju. Je konstrukturiran drugače kot DHCP.
ii) bootp bi morali implementirati tako, da bo lahko vseboval podoben tip komunikacije brodcasta pri IPv4, ker ga IPv6 ne vsebuje. Lahko bi pri IPv6 naredili grupo za vse lokalne naslove ter bi nato pošiljali multicast le-tem in bi s tem simulirali brodcast.

iii) tftp protokol deluje na IPv6. IPv6 uporablja ukaz copy za prejemanje in pošiljanje preko tftp.

## 2. naloga Upravljanje omrežji VPRAŠANJA

A) **Pri SNMP protokolu imamo tri vrste komunikacije: vprašanje/odgovor med upravljalcem in upravljancem, sporočilo upravljanca upravljalcu in sporočila med upravljalci. (i) Ukaz snmpget uporablja katero od treh vrst komunikacije? Utemeljite odgovor. (ii) Peter je na predavanjih o upravljanju omrežij slišal o treh standardih: MIB, SNMP in BER. Ali se slednji (BER) uporablja pri standardu MIB ali SNMP? Utemeljite odgovor. (iii) Peter se je odločil namestiti še drugo upravljalsko vozlišče, a ne ve, ali mora biti v istem lokalnem omrežju (LAN) kot prvo. Kaj menite vi? Utemeljite odgovor. (iv) Ena od uprabljanih naprav v zgoraj opisanem Petrovem omrežju je tudi 3D tiskalnik. Kje vse se hrani podatek o teži vseh natisnjenih predmetov na tiskalniku? Utemeljite odgovor.**

i) vprašanje/odgovor. Ker upravljanec najprej pošlje zahtevo upravljalcu, nato pa upravljalec odgovori.
ii) BER se uporablja pri standardu MiB. Uporablja se zato, - da se podatki na eni in na drugi strani intepretira enolično
iii) Ne, ni potrebno, da je v istem lokalnem omrežju. SNMP deluje tudi preko WAN
iv) Hrani se na MDB in na clientu. MDB hrani za vsako upravljalsko napravo konkretne vrednosti za MiB objekte / parametre.

**B) Peter je na svojem računalniku, ki ima naslov 192.168.1.10, pognal:**

*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) Zakaj ukaz snmpget prvič deluje in drugič ne? (ii) Peter uporablja snmpd na OS Debian, katero datoteko mora popraviti? (iii) Kako napadalec na omrežju lahko pride do skrivnega niza (vaglvuglbambam)? Odgovor utemeljite.**

B) i) ali je problem v IP ju kamor pošljemo zahtevo ali pa vaglvuglbambam comunity ne obstaja (nimamo pojma)
ii) /etc/snmp/snmpd.conf
iii) Če se uporablja SNMPv1 ali SNMPv2 lahko prestreže ukaz preko mreže. Če pa se uporablja SNMPv3 pa ne, ker SNMPv3 uporablja avtentikacijo in enkripcijo

**C) Kaj pomeni naslednji niz zlogov v zapisu ASN.1 BER (vrednosti so desetiške in prvi zlog, ki je prišel, je na levi in upoštevajte, da je ASCII koda za črko A je 6510.): 2 2 4 80 4 2 73 80 2 2 4 72.**

C) ŠE SAM DEMORGAN NEVE

2 (int) 2 (length) 4 80 (value) 00000100 01010000 -> 1024 + 80 = 1104

4 (string) 2 (length) 73 80 (value) -> I P

2 (int) 2 (length) 4 72 -> 00000100 01001000 -> 1024 + 72 = 1096

## 3. naloga: Stvarni čas

**A)Zakaj TCP protokol ni primeren za prenos podatkov v stvarnem času? Utemeljite odgovor.**

TCP ni primeren zato, ker lahko pride do zakasnitev. TCP za vsak paket preverja ali je prišel na cilj ter zaradi tega lahko pride do zakasnitev.

**Peter bi rad sinhroniziral svojo uro s strežnikom na Internetu. Na žalost mu to nikakor ne uspe.**

**Pognal je rdate ntp1.arnes.si, s čimer naj bi nastavil uro na čas, ki ga sporoči strežnik ntp1.arnes.si (za katerega vemo, da obstaja), in dobil odgovor:**

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

**i) Ali bi bilo kaj bolje, če bi namesto ntp1.arnes.si uporabil 193.2.1.117? Utemeljite odgovor.**

i) To bi lahko pomagalo, če je napaka na DNS strežniku. Mogoče DNS te domene ne prepozna in je ne more preusmeriti na IP naslov le-te.

**(ii) Naštejte vsaj 2 razloga, zakaj bi do napake lahko prišlo ter za vsakega, kako ga odpraviti.**

ii) s tem naslovom ne more dostopati do tega DNS strežnika ali nima pravilne konfiguracije v etc/hosts ali v etc/services (verjetno)

**(iii) Peter je ugotovil, da ima njegov računalnik na lokalnem omrežju naslov 169.254.1.2. Kako ga je pridobil? Kaj vse bi moral storiti, da bi s (samo) tem naslovom zgornji ukaz deloval?**

iii) Pridobil ga je z ukazom ip a. Moral bi ga dodati v etc/hosts

**C) S pomočjo storitve NTP lahko pridobimo omrežni čas.**

**i) Kateri protokol uporablja storitev na prenosni plasti in zakaj?**

i) Na prenosni plasti uporablja UDP. Zato, ker potrebuje podatke v čim manjšem času.

**(ii) Petru Zmedi nikakor ni uspelo namestiti NTP strežnika v svojem omrežju. Zato se je odločil, da bo en strežnik vsako minuto po lokalnem omrežju razposlal (multicast) natančen čas, medtem ko bodo ostale naprave preprosto prejele paket in si ustrezno popravile uro. Komentirajte Petrov pristop. V Petrovem omrežju je zgolj 42 naprav.**

ii) V omrežju bo povečan promet, ki je nepotreben, saj vsaka naprava ne potrebuje osveževati čas vsako minuto. Čas bo nepravilen zaradi zakasnitev. Nimamo nobenega preverjanja ali je čas pravilen. Peter dobi njegov čas od odjemalca glavnega strežnika in odjemalec glavnega strežnika dobi podatek od glavnega strežnika. Sepravi ostalih 42 naprav so šele 4 na vrsti da njihov čas kar pomeni dosti večja zakasnitev.

**(iii) Recimo, da je trenutni čas na napravi 02:06:06 in da dobi sporočilo, da je resnični čas 02:06:02. Kaj naj naredi? Kar prestavi čas v nazaj? Utemeljite svoj odgovor**

iii) Počaka, da se ujame z resničnim časom???

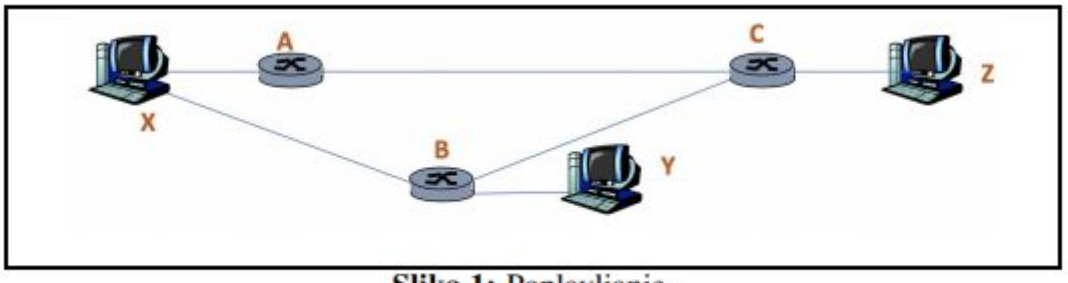
## 4. naloga: Razpošiljanje. VPRAŠANJA:

**A) Kako lahko ugotovimo, ali je katera naprava na omrežju prijavljena na neko konkretno razpošiljevalno skupino (multicast group)? Utemeljite odgovor.**

4.A) Z IGMP sporočilom tipa 17 »group membership query«

| Dejanje | IGMP sporočilo | IP Destination Address | IGMP Multicast Group Address |
|---|---|---|---|
| pridružiti se želim skupini | Group Membership Report | naslov skupine | naslov skupine |
| kdo vse je član določene skupine? | Group Membership Query | naslov skupine | naslov skupine |
| katere skupine obstajajo? | Group Membership Query | vsi vmesniki (224.0.0.1) | 0.0.0.0 |
| sem član skupine, o kateri se poizveduje, želim se odzvati, da sem član | Group Membership Report | naslov skupine | naslov skupine |
| zapustiti želim skupino | Group Leave Report | vsi usmerjevalniki (224.0.0.2) | naslov skupine |

**B) Na sliki sl. 1 je topologija Petrovega omrežja. (i) Recimo, da naprava**




**Slika 1:** Poplavljanje.

**X poplavi omrežje s paketi. Kako mora izgledati usmerjevalna tabela na usmerjevalniku C, da bo le-ta upošteval paket, ki bo od X prišel z usmerjevalnika B in ne usmerjevalnika A? Utemeljite odgovor.**

**(ii) Kakšna usmerjevalna drevesa se gradijo v gostih omrežjih? Zakaj?**

ii) C bi moral poznati samo usmerjevalnik B.

Usmerjevalna drevesa v gostih omrežjih se gradijo na **source based** omrežjih.

**D) Peter nastavlja svoj DHCP strežnik. Ker bi rad ugotovil, kako se le-ta pogovarja z računalnikom, se je odločil, da zajame nekaj prometa. Pognal je spodnji ukaz.**

*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) Kakšen naslov je 255.255.255.255?**

i) Naslov 255.255.255.255 je broadcast naslov.

**(ii) Skupina 224.0.0.12 je rezervirana za ”DHCP Server / Relay Agent”. Kje v nastavitvah tipičnega strežnika DHCP se to odraža?**

ii) v DHCP.conf?

**(iii) Ce bi Peter rad nastavil, da njegov računalnik vedno dobi is ˇ ti naslov, na osnovi katerega podatka oz. podatkov, ki jih računalnik pošlje strežniku, lahko to stori? Utemeljite odgovor.**

iii) DHCP reservation?

Kolokvara 2018/19

## 1. naloga: Osnove. VPRASANJA ˇ :

**A) Imamo napravi z IP naslovoma 192.168.2.10 in 192.168.3.15. Kdaj si lahko neposredno pošiljata promet in kdaj potrebujeta posrednika? Utemeljite odgovor**

A) Neposredno si lahko pošiljata promet, ko je maska manjša od 23. Če je maska manjša od 23 sta napravi v istem omrežju.

**B) Peter ima dve mreži - 192.168.1.64/26 in 192.168.1.128/26. (i) Najmanj koliko DNS strežnikov potrebuje, da bo njegovim uporabnikom normalno deloval svetovni splet?**

i) Potrebuje najmanj en DNS strežnik.

**(ii) Kaj in kako bo moral nastaviti (poleg samih strežnikov), če bo hotel, da bo uporabnikom ponudil pravi DNS čim bolj preprosto?**

ii) Nastaviti bo moral DHCP server, ki bo uporabnikom sporočal DNS

**C) (i) Kot rečeno ima Peter dve mreži in koliko strežnikov z operacijskim sistemom potrebuje, da bodo nudili tftp storitev? Utemeljite odgovor.**

i) Potrebuje 1 TFTP strežnik, saj ni nujo daj je tftp strežnik v istemo omrežju. Računalnik mora poznati IP prehoda.

**(ii) Storitvi bootp in tftp smo spoznali v povezavi z zagonom stroja. Ali ju lahko uporabimo tudi, ko je operacijski sistem že delujoč na stroju? Utemeljite odgovor.**

ii) Da lahko ju uporabimo tudi takrat. Ker se bootp in tftp ne ozirata na trdi disk (delujeta preko mreže). Lahko poženemo OS preko mreže ali trdega diska.

## 2. naloga: Peter je slišal, da lahko preveri, koliko prostora ima na disku, če izvede:

*snmpget -v1 -c studentje localhost .1.3.6.1.4.1.2021.9.1.9.1.*

## VPRASANJA ˇ :

**A) Sedaj ga zanima, katere ostale podatke o disku lahko dobi. (i) S katerim ukazom si lahko pomaga? Napišite celoten ukaz z vsemi argumenti.**
i) snmpwalk -Os -c public -v 2c <vrouter-ip> HOST-RESOURCES-MIB::hrStorage
**(ii) Kaj je v zgornjem ukazu studentje?**
ii) studentje je “community”
**(iii) Ali so ukazi, ki jih uporablja, varni? Utemeljite odgovor.**
iii) Ne, ker uporabljamo vetzijo 1 SNMP-ja kateri ni imel enkripcije in avtentikacije in so lahko zlonamerneži prestregli podatke prek mreže.

**B) Pri SNMP protokoli imamo tri vrste komunikacije: vprašanje/odgovor med upravljalcem in upravljalcem, sporočilo upravljanca upravljalcu in sporočila med upravljalci. Poleg tega imamo več tipov sporočil (PDU Type, Protocol Data Unit Type). (i) Katere tipe sporočil poznate in pri kateri vrsti komunikacije se uporabljajo? Dodajte primer, ko se uporabljajo.**

- i) *GetRequest* (vrednost) *GetNextRequest* (naslednja vrednost) *GetBulkRequest* (blok podatkov)
- *setRequest* (nastavi vrednost v MIB)
- *response* ("tukaj je vrednost", odgovor na Request)
- *trap* (obvestilo upravljalcu o izrednem dogodku).
- *InformRequest* (medsebojno posredovanje vrednosti iz MIB)
-

**(ii) Protokol SNMP ni nič kaj varen protokol. Kako se branimo pred napadi s ponavljanjem? Kakšne vire na napravah in na katerih zahteva ta obramba.**
ii) Pred napadi s ponavljanjem se branimo z uporabo enkratnih žetonov. Zahteva MAC

## 3. naloga: Stvari čas VPRAŠANJA:

**A) Ali za zakrivanje RTP prometa lahko uporabimo protokol SSL/TLS? Utemeljite odgovor.**
Ne nemoremo, saj je RTP uporablja UDP, ki nima SSL plasti.Zato moramo za zagotovitev varnosti uporabiti kriptiranje s tokom šifer.

**B) Protokol RTP zagotavlja dve osnovni funkcionalnosti.**

**C) (i) Kateri in kako?**

- i) Skrbi za pravo zaporedje paketov (sequence number)
- skrbi za časovne značke dogodkov (timestamp)

**(ii) Recimo, da bi se dogovorili, da za prenosni protokol uporabimo namesto UDP protokola protokol TCP. Kateri del glave paketa RTP bi postal nepotreben in zakaj?**
ii) Sequence number. Ker UDP ne gleda vrstnega reda paketov.
**iii) Peter je v svojem podjetju vzpostavil videofonski sistem z uporabo protokola RTP. Za vzpostavitev povezave je uporabil storitev SIP. Kako naj**

**zagotovi celovitost (integriteto) toka podatkov? Opišite predlog svoje rešitve čim bolj natančno.**
iii) ?
**C) Protokol TIME (oziroma rdate) lahko na prenosni plasti uporablja tako TCP kot UDP. V katerem primeru bi izbrali enega oziroma drugega? Utemeljite odgovor.**
C) **UDP** kadar je pomembna enostavnost / hitrost povezave in ko uporabljamo zanesljivo omrezje.
**TCP** pa ko je pomembno da podatki prispejo v celoti na cilj in ko ne zelimo da nekdo prisluskuje (imamo enkripcijo).

## 4. naloga: razpošiljanje VPRAŠANJA

A) **Ali DHCP protokol uporablja razpošiljevalne naslove? Utemeljite odgovor. NAMIG: Upoštevajte, kateri protokol je na mrežni plasti**

Da. Da lahko dostopa do novih računalnikov, ki se priklopijo v omrežje

B) **Imamo napravo z naslovom 1.4.6.7, ki se prijavlja na razpošiljevalno skupino 224.0.24.32.**

**(i) Zapišite naslovnikov in pošijateljev naslov v IP glavi ter vsebino IGMPv2 paketa. Utemeljite zakaj so vrednosti takšne, kot ste jih zapisali?**
i) Type = 0x16

- Max Resp Time = naključno določeno
- Group Address = 224.0.24.32,
- Checksum = ?

**(ii) Na predavanjih smo zapisali, da je vrednost TTL polja 1. Kdaj je smiselno, da je večja kot 1? Opišite primer.**

ii) Da je TTL vrednost večja kot 1 je smiselno takrat, ko hočemo naš request poslati izven trenutnega omrežja. Če je 1 pomeni da pošiljamo samo na trenutnem omrežju.
**(iii) Ali IGMP protokol vsebuje zaščito, ki zagotavlja celovitost (integriteto) sporočila? Odgovor utemeljite.**
**NAMIG: Ce menite, da jo vsebuje, opišite kako deluje in če ne, opiˇ ˇsite kako lahko napadalec spremeni sporočil ne da bi prejemnik vedel za spremembo.**
iii) Da, verzija 3 vsebuje celovitost sporočila
**D) V Butalah je spet rdeči alarm. Nekaj gre hudo narobe in Peter Zmeda sumi, da je v ozadju ponovno Cefizelj. Zato se je lotil problema tako, da je zajel omrežni promet in dobil je naslednji zapis:**

*Frame 1543: 62 bytes on wire (496 bits),*
*62 bytes captured (496 bits) on interface 0*
*Ethernet II, Src: 00:6c:bb:2f:30:00 (00:6c:bb:2f:30:00), Dst: IPv4mcast 16 (01:00:5e:00:00:16)*
*Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.22*
*Internet Group Management Protocol*
*[IGMP Version: 3]*

*…*
*Num Group Records: 1*
*Group Record : 224.1.1.1 Mode Is Include*
*Record Type: Mode Is Include (1)*
*Aux Data Len: 0*
*Num Src: 2 Multicast Address: 224.1.1.1*
*Source Address: 192.168.1.2*
*Source Address: 8.8.8.8*

i) 10.0.0.2, ker je to naslov vira
ii) Cefizelj se hoče pridružiti multicast skupini.

# Kolokvara 2017/18

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

```
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#
```

**VPRASANJA:**
**A) (i) Ali računalnik ima IPv4 naslov? Kaj pa IPv6? (ii) Ce 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?**
A)
i) Računalnik ima IPv4 in IPv6 naslov
ii)
iii)
iv) eth1

**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.**

B)
i) Zadnji paket je manjši od največje dovoljene velikosti. Ker to pomeni, da je zadnji.
ii) Ne bi nam bilo treba poslati zadnjega paketa, saj lahko TCP poskrb, da vemo da smo poslali zadnji paket.

**C) Kakšen je vrstni red (od najmanjšega proti največjemu) (i) IPv4, (ii) IPv6 in (iii) MAC naslovov ter (iv) številka vrat glede na število možnih vrednosti? Odgovor utemeljite.**
C)
Številka vrat (20-bit)
IPv4 (32-bit)
MAC (48-bit)
IPv6 (128-bit)

**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 bolje, če bi upravljalec agenta na tiskalniku spraševal o stanju papirja s pomočjo zahteve in odgovora? Utemeljite odgovor.**
A)
i) Z ukazom trap lahko Cefizelj ponovno pošilja to sporočilo (replay attack).
ii) Da, saj bi na vprašanje odgovoril tiskalnik.

**B) Kako protokol SNMPv3 preprečuje napade s ponovitvijo (replay attack)? Utemeljite odgovor.**
B) Z uporabo varnostnih mehanizmov. Avtentikacija, uporaba enkratnih žetonov

**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.**
C)
i) snmpget -v2 -c public hostname .1.3.6.1.4.1.2021.9.1.9.1
ii) /etc/snmp/snmpd.conf. pri access bo moral spremeniti pravice.

iii) snmptranslate .1.3.6.1.4.1.2021.9.1.9.1

**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.**
A)
i) Časovne značke dogodkov. To služi temu, da so paketi pravilno časovno razvrščeni.
ii) Ne bi potrebovali oštevilčenja paketov, saj bi za to poskrbel TCP.
iii) TRP uporablja UDP, ker je hitrejši in nima zakasnitev kot TCP, bolj je pomembno da hitreje dobimo podatke kot pa da jih gotovo dobimo.
**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.**
B)
i) c) samo vsebino RTP paketa
ii) Preostanek ni šifriran, ker je potreben, da paket pride do prejemnika. Vsebina je šifrirana, da je napadalec ne more prebrati vsebine.

**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.**
A) b) ne, ker se PIM uporablja le do domačega usmerjevalnika, medtem ko na domače omrežje ti paketi ne pridejo.
Ko clientov paket pride na usmerjevalnik ki je clientov privzeti prehod, usmerjevalnik pogleda v PIM drevo, kje je ta skupina in kateremu usmerjevalniku izven njegovega omrežja mora poslati, da bo to izvedeno najhitreje.

**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.**

B)

i) /home/pavel/bin/listRP | head -n 1 | /home/pavel/bin/setRP

ii) echo 192.168.1.12 | /home/pavel/bin/setRP

**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 naj 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.**

D)

i) FF02::1

ii) PIM-SM, ker so prijatelji razpršeni po celem svetu in ne poplavlja omrežja kot PIM-DM

iii) KUAAAA FFFFF

# Kolokvara 2016/17

1. **naloga: Osnove ter bootp in DHCP**

**VPRAŠANJA:**

A) **Ali naprava z IP naslovom 192.168.2.10 lahko pošlje omrežni paket napravi z IP naslovom 192.168.3.15? Utemeljite odgovor - če da, zakaj in kako, in če ne, zakaj ne.**

A) Da, če je maska manjša od 24.

B) **Peter postavlja domače omrežje in zanj bo potreboval DHCP strežnik. V omrežju bo imel največ 50 računalnikov. (i) Predlagajte, katere naslove naj uporabi v bazenu DHCP strežnika in kakšna naj bo omrežna maska, da bo porabill čim manj naslovov. Utemeljite odgovor. (ii) Če ima 50 računalnikov, koliko naslovov mu bo ostalo neuporabljenih? Utemeljite svoj odgovor.**

B) i)192.168.0.1/26 - 192.168.0.62. Z masko 26 lahko uporabi 62 naslovov, kar je najmanjša maska ki jo lahko uporabimo za 50 naprav.

ii)62-50=12. Ostalo mu bo 12 naslovov, saj imamo lahko z masko 26 največ 62 naslovov.

C) **V paketu bootp protokola nastopa polje xid - identifikator zahteve. (i) Čemu služi in kaj slabega bi se lahko zgodilo, če bi ga ne bilo? Utemeljite odgovor.**
**Peter Zmeda je, kot vemo, initiativen fant. No, sedaj bi rad nadomestil protokol tftp s pravim ftp. (ii) Ali je to možno? Utemeljite svoj odgovor.**
**Namig: Če menite, da ne, utemeljite, zakaj ne gre; in, če menite da da, potem natančno opišite, kaj vse je potrebno narediti, da bi zamenjava delovala.**

C)i)Služi temu da client ve, če so prihajajoča sporočila namenjena njemu. Lahko bi se zgodilo, da sporočilo pride do napačnega clienta
ii) lhka, sam Bog ve kako

**2. VPRAŠANJA:**

A) **Ali lahko stanje omrežnega (IEEE 802.3) stikala nadziramo brez SNMP? Utemeljite odgovor.**

Da. Lahko uporabimo spletne vmesnike, ki jih ponujajo proizvajalci opreme.

**B) Naš prijatelj Peter Zmeda je na vajah spoznal net-snmp, s katerimi lahko prebere katerikoli podatek, ki je na računalniku dostopen prek SNMP.**
**Na žalost niti ne ve, kateri podatki so na voljo. Kako jih lahko najde? Napišite točen ukaz, pri čemer razložite, kaj pomeni vsak od argumentov.**

snmpwalk -c public -v3 -m all localhost
snmpwalk [options] [community string/authentification information] [host name/address] [OID]

**C) Peter je končno na vse računalnike spravi SNMPv3 agente. Sedaj bi rad spremljal njihovo stanje na neki nadzorni spletni strani.**
**(i) Katere MIB datoteke bo potreboval na strežniku s spletno stranjo? Odgovor utemeljite. (ii) Predlagajte vsaj en obstoječ spletni program za nadzor in izris grafov, ki ga lahko uporabi. (iii) Kateri del nastavitev mora zavarovati pred Cefizljem, da le-ta ne bo mogel prisluškovati prometi med agenti in nadzornim sistemom. Odgovor utemeljite.**

i) status, object name, syntax, access/max-access???
ii) SolarWinds Network Performance Monitor

iii)

**3. VPRAŠANJA**

**A) Razvili smo lasten aplikacijski protokol ABC. na transportni plasti smo se odločili za UDP protokol. Kako to vpliva na zanesljivost komunikacije med dvema udeležencema v ABC protokolu? Utemeljite odgovor**

A)UDP ne zagotavlja, da bodo vsi podatki prišli in da bodo dostavljeni v pravem vrstnem redu. Komunikacija ni zanesljiva

**C) Za prenos koncerta so uporabili protokol RTP. Da bi bila Petrova zadrega še večja, njegova zvočna tehničarka Špela ni sedela na ušesih in si je ime skladatelja skrbno zapisala. Vključila ga je tudi v prenos. (i) Kje v prenosu bi lahko Peter našel ime skladatelja? (ii) Pred prenosom je Peter razlagal Špeli, da bodo uporabili tudi protokol SIP. Se vam to zdi smotrno? Utemeljite odgovor.**
**NAMIG: Podrobneje kot boste odgovorili na podvprašanji, več točk boste dobili. Npr. v primeru (i), če polog protokola opišite tudi kje v prenesenih prenesenih paketih se lahko skriva ime.**

C)i)RTCP Source Description Items
ii) RTP z uporabo SIP-a bi bla brezsmiselna, saj ne potrebujemo dvosmerne komunikacije za prenos koncerta, kar SIP prinaša.
Za prenos koncerta bi bilo smiselno uporabljati protokol RTSP, ki je bolj primeren in namenjen stremanju koncertev

D) Peter se je odločil, da je NTP prezapleten, zato bo raje razširil protokol rdate tako, da bo čas prenešen kot 48-bitno nepredznačeno število, ki predstavlja milisekunde 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));
  }
}
```

D) demorgan 42

**4. VPRAŠANJA:**

A) **Kako lahko ugotovimo, ali je katerikoli računalnik na omrežju prijavljen na neko konkretno razpošiljevalno skupino (*multicast group)* - recimo na 224.6.1.2?**
Pošljemo IGMP Membership query (Group-specific query) (0x11).

B) **Peter je v svoj domači imenik razpakiral dva programa za upravljanje z osrednjim vozliščem (*rendez-vous point).* V podimeniku *nastaviRP* se nahaja prvi, ki se imenuje *setrp,* v podimeniku *poisciRP* se nahaja prvi, ki se imenuje *setrp* v podimeniku *poisciRP* pa drugi, ki se imenuje *findrp.* Načil se je, da lahko *setrp* požene z zaporedjem ukazov: *cd~/nastaviRP; ./setrp.* (i) Kako bi isti ukaz zapisal tako, da bi uporabil le poti, ki se začnejo z /? Privzemite, da je njegovo uporabniško ime *peter* in da se njegovi domači imenik nahaja na običajnem mestu. (ii) Kako bi lahko brez uporabe absolutnih poti ali bližnjice ~ pognal *findrp*, če se nahaja v imeniku, kjer je *setrp?***
B) i) cd /home/peter/nastaviRP/setrp
ii) ./findrp

C) **V prejšnjem vprašanju je omenjeno osrednje vozlišče. (i) Kakšno vlogo ima pri razpošiljanju? (ii) Omenili smo, da obstajata dva osnovna načina delovanja razpošiljanja. V katerem načinu razpošiljanja se osrednje vozlišče pojavlja? (iii) Zakaj v tem načinu in zakaj v drugem ne? (iv) Recimo, da bi morali Petru pomagati spisati oba programa omenjena v prejšnjem vprašanju. Katere parametre bi morali imeti vsak od programov setrp in findrp, da bi imeni programov bili smiselni? Utemeljite odgovor.**
C) i) dobro je, ker lahko olajša prijavo novi napravi, ker če ni želenega ruterja, lahko naprava pošlje osrednjemu, da bo zagotovo dobil prijavni paket na aparatima
ii) poznamo dva osnovna načina delovanja razpošiljanja:

- **group shared** (če imamo malo vozlišč) - tukaj se nahaja centralno vozlišče
- **source based** (če jih je pa veliko, pa težko spreminjamo infrastrukturo)

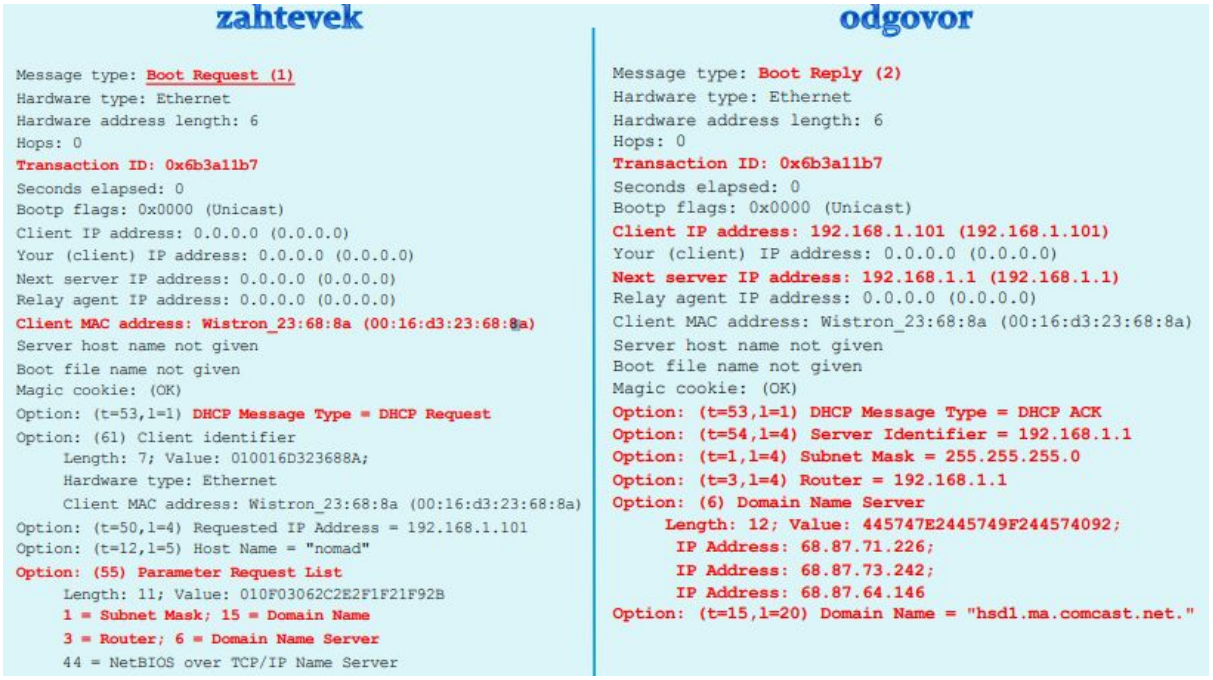
iii) ni v source based ker vsako novo vozlišče lahko pomeni popolno spremembo infrastrukture

iv) KUA JE TUUU

## 1. naloga: bootp in DHCP. VPRAŠANJA :

**1. V osnovi pri DHCP protokolu ena stran pošlje vprašanje in druga odgovor. (i) Kako prva stran ve, da je odgovor za njo in kako ve, odgovor na katero vprašanje je prejela?**

prvo client pošlje DHCP REQUEST z in strežnik odgovori odjemalcu z DHCP ACK. Sedaj sta pripravljena za komunikacijo. To je razvidno v glavi datagrama iz Transcation ID, ker sta enaka.



**zahtevek**

```
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP Request
Option: (61) Client identifier
     Length: 7; Value: 010016D323688A;
     Hardware type: Ethernet
     Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
     Length: 11; Value: 010F03062C2E2F1F21F92B
     1 = Subnet Mask; 15 = Domain Name
     3 = Router; 6 = Domain Name Server
     44 = NetBIOS over TCP/IP Name Server
```

**odgovor**

```
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
     Length: 12; Value: 445747E2445749F244574092;
     IP Address: 68.87.71.226;
     IP Address: 68.87.73.242;
     IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."
```

**(ii) DHCP protokol nima vgrajenega avtentikacijskega mehanizma. Predlagajte vsaj en način, da bo odjemalec (spraševalec) lahko verodostojno avtenticiral strežnik in utemeljite kakovost svojega predloga.**

ARP spoofing?

**2. Peter bi imel rad 2 DHCP strežnika. Ali lahko dodeljujeta naslove na istem področju? Če ne, zakaj ne? Če da, kako poskrbita, da ne dodelita istega naslova dvema različnima računalnikoma?**

Lahko dodeljujeta na istem naslovu, vedar je bolje, da imata ta polje ločeno na dve polji, na kateri bo vsak imel svoje področje.

Če si ne razdelita polja, morata imeti nek sistem, ki bo preverjal ali je IP naslov, ki se bo dodeliu računalniku že dodeljen z drugega DHCP-ja.

**3. Veronika je vzela Petra kot novega ponudnika Interneta. (i) Ali je sploh možno, da bi imela Veronika na svojem usmerjevalniku nastavljen DHCP način pridobivanja internetnega naslova in dobil statični IPv4 naslov? Utemeljite odgovor. Zal Peter v ponudbi nima statičnega IPv4 naslov.**

i) Seveda je možno da ima nastavljen DHCP način pridobivanja IP-ja, saj je Petrin usmerjevalnik svoje omrežje in lahko normalno dodeljuje naslove.

Da lahko, saj je na svojem omrežju ter ima lahko nastavljen statični naslov v svojem omrežju.

**(ii) Navedite vsaj en tehnični razlog, zakaj bi Peter ne ponujal statičnega IPv4 naslova.**

Peter ne more ponujati statičnega naslova, ker mu jih je zmanjkalo.

## 2. naloga:

## Upravljanje omrežij. VPRAŠANJA :

**1. Pri upravljanju omrežij smo omenili tri osnovne gradnike infrastrukture. Kateri so ti gradniki in opišite vlogo vsakega od njih.**

- upravljalec (aplikacija + človek)
- nadzaravana naprava (vseboje agenta NMA in nadzavarovanje objekte)
- protokol za upravljanje (SNMP)

**2. NaŠ prijatelj Peter Zmeda se je med pripravo na izpit naučil, da ni pošiljanje paketov SNMP prav nič varno. Ker upravlja omrežje v Butalah in ker tam strašni Cefizelj precej pogosto prisluškuje prometu, se je odločil, da implementiral varni SNMP (SSNMP). Za kriptiranje se je odločil uporabiti tehniko veriženja. (i) Opišite, kako deluje tehnika veriženja.**

**(ii) Ali protokol SNMP sploh omogoča kriptiranje s tehniko veriženja? Utemeljite odgovor.**

**3. Naš prijatelj Peter Zmeda je stvari končno postavil na pravo mesto in uspel sestaviti celotno upravljalsko omrežje, ki uporablja protokol SNMP. Sedaj ima novo aplikacijo, ki bi želela pridobiti neke podatke iz upravljalskega omrežja. KakŠen pristop je najbolj razŠirljiv in skladen? Utemeljite odgovor! UL FRI, KPOV 2015/16 – Prvi kolokvij 151124 3 3. naloga: Stvarni čas. Ste kdaj razmiŠljali o predvajalniku toka podatkov1 , ki hkrati tudi shranjuje prejete podatke? Shranjen tok podatkov (ali oddajo) si bi lahko kasneje ponovno ogledali. VPRAŠANJA : 1. NaŠ prijatelj Peter Zmeda se je odločil, da bo ustrezno nadgradil sprejemnik RTP prometa, da bo hkrati omogočal shranjevanje (snemanje) prejetih podatkov. Vse skupaj je skoraj v redu, le moti ga, da je kakovost posnete oddaje slaba, saj je a) kar nekaj paketov priŠlo prepozno in b) tudi precej jih sploh ni priŠlo. (i) Ali lahko kaj naredi glede zamujenih paketov (paketi a)? Utemeljite odgovor. (ii) Kaj lahko naredi glede izgubljenih paketov (paketi b)? Utemeljite odgovor! NAMIG: PopolnejŠi kot bo vaŠ posnetek, več točk boste dobili. 2. Aplikacija v stvarnem času prenaŠa govor oseb. Kako naj obravnava izgubo manjŠega Števila paketov? Utemeljite odgovor. 3. Peter zelo rad poganja igrico openra. Nekoč se je po nesreči prijavil na računalnik s korenskim geslom (kot root) in igrica se ni hotela zagnati - v lupini je dobil sporočilo: > openra bash: openra: command not found (i) Zakaj bi lahko do tega priŠlo? (ii) Kako naj kot uporabnik, ki mu ukaz openra deluje, ugotovi, kje se nahaja program openra? (iii) Kako lahko poskrbi,**

**da bo ukaz deloval tudi uporabniku root? 4. NEOBVEZNO IN NI ZA OCENO. Vojna je poraz cloveŠtva ˇ (Janez Pavel II). V zimskih mesecih v letih 1943 in 1944 je vojna odnesla življenji dveh odličnih mladih slovenskih pesnikov. Nesmiselne smrti enega od njih, Franceta Balantiča, se spominjamo prav na danaŠnji dan. Kdo je bil drugi, katerega nepotrebno smrt je vihra povzročila manj kot tri mesece kasneje? 4. naloga: RazpoŠiljanje. VPRASANJA ˇ : 1. Za usmerjanje razpoŠiljevalnega prometa v omrežju uporabljamo protokol PIM. Le-ta deluje lahko v gostem ali redkem načinu delovanja. V vsakem od načinov izgradi različno usmerjevalno drevo. (i) Katero razpoŠiljevalno 1Tok podatkov je lahko celo razpoŠiljan. 4 UL FRI, KPOV 2015/16 – Prvi kolokvij 151124 drevo zgradi v katerem načinu in zakaj? (ii) Spoznali smo tudi osrednjo točko rendez-vouz point. V katerem načinu dela protokola PIM nastopa in zakaj? (iii) Ali je osrednja točka smiselna tudi v drugem načinu delovanja? Utemeljite odgovor. 2. Kako lahko ugotovimo, ali je kateri koli računalnik na omrežju prijavljen na razpoŠiljevalno skupino (multicast group) 224.7.8.7? Utemeljite odgovor! 3. Cefizelj je zloben. V svojem najljubŠem urejevalniku besedil je ustvaril datoteko skripta.sh z naslednjo vsebino: #!/bin/bash skripta.sh & skripta.sh (i) Kaj naj bi njegov umotvor naredil? (ii) Kaj mora storiti, da bo ustvarjeno datoteko lahko sploh zagnal? (iii) Kaj mora Še storiti, da bo delovala? Privzemite, da skripte ne sme spreminjati. Predlagajte dve možni reŠitvi**