

# Komunikacijski protokoli in omrežna varnost 2019/20 Prvi kolokvij

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

Če boste uspešno vsaj delno vse naloge, bo možno dobiti dodatne točke.

Čas pisanja kolokvija je 60 minut.

Veliko uspeha!

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

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

ŠTUDENTSKA ŠTEVILKA: \_\_\_\_\_

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

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

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

## VPRAŠANJA:

- A) Kaj naj bi ščitil SecureBoot?
- 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 nastavitvev 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.
- 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.

**2. naloga:** Upravljanje omrežij.

## 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 upravljalško vozlišče, a ne ve, ali mora biti v istem lokalnem omrežju (LAN) kot prvo. Kaj menite vi? Utemeljite odgovor. (iv) Ena od upravljanjih naprav v zgoraj opisanem Petrovem omrežju je tudi 3D tiskalnik. Kje vse se hrani podatek o teži vseh natisnjenih predmetov na tiskalniku? Utemeljite odgovor.

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.

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  $65_{10}$ ): 2 2 4 80 4 2 73 80 2 2 4 72.

### 3. naloga: Stvarni čas.

VPRAŠANJA:

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

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

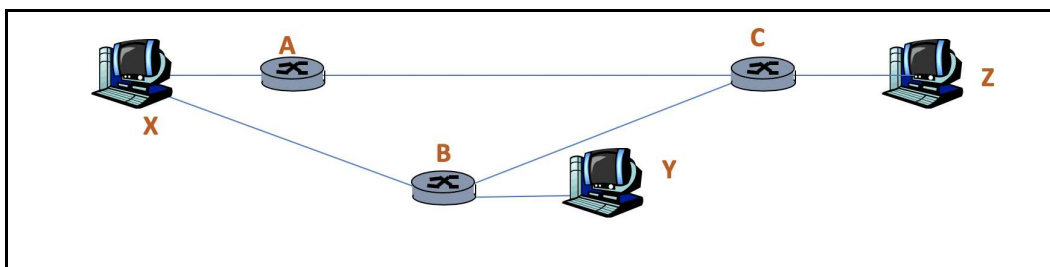
C) S pomočjo storitve NTP lahko pridobimo omrežni čas. (i) Kateri protokol uporablja storitev na prenosni plasti in zakaj? (ii) Petru Zmedi nikakor ni uspelo namestiti NTP strežnika v svojem omrežju. Zato se je odločil, da bo en strežnik vsako minuto po lokalnem omrežju razposlal (*multicast*) natančen čas, medtem ko bodo ostale naprave preprosto prejele paket in si ustrezno

popravile uro. Komentirajte Petrov pristop. V Petrovem omrežju je zgolj 42 naprav. (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.

#### 4. naloga: Razpošiljanje.

##### VPRAŠANJA:

- A) Kako lahko ugotovimo, ali je katera naprava na omrežju prijavljena na neko konkretno razpošiljevalno skupino (*multicast group*)? Utemeljite odgovor.
- B) Na sliki sl. 1 je topologija Petrovega omrežja. (i) Recimo, da naprava X po-



Slika 1: Poplavljanje.

plavi 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?

- C) NEOBVEZNO IN NI ZA OCENO. Letos proslavljamo 100 letnico ustanovitve Univerze v Ljubljani. (i) Kdo je bil njen prvi rektor, ali vsaj kaj je bilo njegovo področje raziskovanja? (ii) O čem je bilo prvo predavanje na novo ustanovljeni univerzi ali celo, kdo ga je imel?
- 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? (ii) Skupina 224.0.0.12 je rezervirana za "DHCP Server / Relay Agent". Kje v nastavitvah tipičnega strežnika DHCP se to odraža?

(iii) Če bi Peter rad nastavljal, da njegov računalnik vedno dobi isti naslov, na osnovi katerega podatka oz. podatkov, ki jih računalnik pošlje strežniku, lahko to stori? Utemeljite odgovor.