Izpit RKVB, VSS, FRI, 1. letnik, 7. 7. 2015

Ime: _____

Priimek: _____

Vpisna številka: _____

RKVB

*Pozorno preberite navodila! Lahko uporabljate knjigo in preprost kalkulator. Odgovarjajte kratko! Čas pisanja je **60** minut.*

1) (20%) Serija 3 datagramov, velikih po 5000 bytov, mora na poti do cilja po povezavi z MTU = 4000, nato po povezavi z MTU = 2500 in nazadnje še po povezavi z MTU = 1500. Koliko datagramov in kako velikih prispe na cilj? Napišite zaporedje datagramov in velikosti ločeno za vsak korak. Na kateri plasti se to dogaja?

2) (10%) Katere od naslednjih trditev veljajo za UDP – obkrožite DA ali NE.
   a. Vzpostavi virtualno povezavo od odjemalca do strežnika DA NE
   b. Izguba paketov ni možna. DA NE
   c. Protokol zagotavlja navzgor omejeno zakasnitev pri prenosu. DA NE
   d. Paketi gredo lahko tudi po različnih poteh. DA NE
   e. Funkcionalnost je minimalna, zato je protokol hiter in učinkovit. DA NE

3) (10%) Katere od naslednjih trditev veljajo za TCP
   a. Na isti vtič se lahko povežeta dva odjemalca. DA NE
   b. Če strežnik sprejme potrditev, v kateri je parameter RcvWindow nastavljen na 0, nemudoma neha s pošiljanjem podatkov. DA NE
   c. Kadar je ocena RTT enaka 100 ms in ocena odmika 120, to pomeni, da se paket ponovno pošlje, če 220 ms po oddaji še ne prispe potrditev. DA NE
   d. Če je zamašitveno okno veliko 120 MSS in pride do izteka časovne kontrole za pravkar oddani segment, se pri vseh različicah TCP zamašitveno okno zmanjša. DA NE
   e. Če je zamašitveno okno veliko 120 MSS, ko smo v fazi izogibanja zamašitvam in potrditve redno prihajajo, bo v naslednjem časovnem interval zamašitveno okno veliko 240 MSS. DA NE

4) (20%) Študent sedi za računalnikom in uporablja spletni brskalnik. Ko klikne na povezavo s spletnim naslovom, se generira http zahteva, ki se posreduje po skladu TCP/IP navzdol,nato do stikala, prek stikala do usmerjevalnika - prehoda čez NAT in od tam naprej v internet. Predpostavimo, da je poizvedba dovolj majhna, da je na vseh plasteh enkapsulirana v en sam protokolarni paket. Predpostavimo tudi, da so vse tabele na vseh napravah prazne, prav tako vsi medpomnilniki (cache). Zanimajo nas aktivnosti omrežja, ki se zgodijo zaradi prehoda tega paketa skozi omrežje, in se ne bi zgodile, če se paket ne bi prenašal.

   a. Izmed naslednjih aktivnosti izberi tiste, ki se zgodijo ob zgoraj opisanem prenosu paketa čez omrežje in jih razvrsti v pravilen vrstni red (posamezna aktivnost lahko nastopa tudi več kot enkrat): arp poizvedba, poplavljanje, posredovanje, zamenjava izvornega IP naslova, zamenjava ciljnega IP naslova, enkapsulacija, dekapsulacija, DNS poizvedba.
   b. V katerih od zgornjih aktivnosti nastopajo naslednje tabele: arp tabela, cam tabela (stikalna), usmerjevalna tabela? Na kateri napravi in na kateri plasti?
   c. Za vsako od teh treh tabel navedite, katere stolpce vsebuje in kaj se zapiše vanje (če sploh kaj) ob prehodu paketa?

5) (20%) Ana in Borut vzpostavljata ključ z metodo Diffie-Hellman. Ana izbere n = 5 in g=7, za skrivno število x pa si izbere 11. Borut si za skrivno število y izbere 13. Pri spodnjih odgovorih **napišite oboje** - formulo in rezultat izračuna!
   a. Kaj pošlje Ana Borutu?
   b. Kaj pošlje Borut Ani?
   c. Kaj je potem njun ključ?
   d. Kaj pa, če bi se napadalka vrinila v njuno komunikacijo ... Za svoje skrivno število z bi si izbrala 4. Kaj bi poslala Borutu v Aninem imenu? 5, 7, 1
   e. Kaj bi ji Borut poslal nazaj? Isto, 2
   f. Kaj bi napadalka poslala Ani? 1
   g. Kdo bi s tem vzpostavil ključ s kom in kakšen bi bil ta ključ?

6) (20%) Preučite zajete segmente in odgovorite na spodnja vprašanja:

No.	Source	Destination	Protocol	Length	Info
1	192.168.1.9	173.194.44.17	TCP	78	54264 > http [SYN] Seq=0 Win=65535
2	173.194.44.17	192.168.1.9	TCP	74	http > 54264 [SYN, ACK] Seq=0 Ack=1 Win=62392
3	192.168.1.9	173.194.44.17	TCP	66	54264 > http [ACK] Seq=1 Ack=1 Win=131872
4	192.168.1.9	173.194.44.17	TCP	73	54264 > http [PSH, ACK] Seq=1 Ack=1 Win=131872
5	173.194.44.17	192.168.1.9	TCP	66	http > 54264 [ACK] Seq=1 Ack=8 Win=62400
6	173.194.44.17	192.168.1.9	TCP	1134	http > 54264 [PSH, ACK] Seq=1 Ack=8 Win=62400
7	173.194.44.17	192.168.1.9	TCP	66	http > 54264 [FIN, ACK] Seq=1069 Ack=8 Win=62400
8	192.168.1.9	173.194.44.17	TCP	66	54264 > http [ACK] Seq=8 Ack=1069 Win=130800
9	192.168.1.9	173.194.44.17	TCP	66	54264 > http [ACK] Seq=8 Ack=1070 Win=131072
10	192.168.1.9	173.194.44.17	TCP	66	54264 > http [FIN, ACK] Seq=8 Ack=1070 Win=131072
11	173.194.44.17	192.168.1.9	TCP	66	http > 54264 [ACK] Seq=1070 Ack=9 Win=62400 Len=0

   a) Kateri segmenti predstavljajo rušenje TCP povezave? *Napišite številke segmentov.*
   b) Katere segmente potrjujejo vsi segmenti, ki jih je poslal računalnik z IPjem 173.194.44.17? *Napišite številke segmentov, ki jih potrjuje, ne pozabite upoštevati predhodnih potrditev!*
   c) Koliko »koristnih« podatkov (v bajtih) se prenese v 1, 2, 3, 4 in 6. segmentu?

8. S programom Wireshark smo zajeli spodnjo sejo (za prikaz smo uporabili možnost Follow TCP Stream):

```
220 mail.example.com ESMTP Postfix
HELO lrk.si
250-mail.example.com
MAIL FROM: <kapica@lrk.si>
250 2.1.0 Ok
RCPT TO: <volk@example.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: babica@lrk.si
To: volk@example.com
Subject: Kolokvij RK!!
Date: Fri, 31 May 2013 07:30:06 +0200

Babica pise kolokvij!
.
250 2.0.0 Ok: queued as 9BEB98320
QUIT
221 2.0.0 Bye
```

   a) Za kateri protokol aplikacijske plasti gre?
   b) Kateri protokol se uporablja na transportni plasti? Ali je možno tu uporabiti multicast? Razloži.
   c) Kdo je prejemnik e-pošte?
   d) Imamo interni poštni strežnik v podjetju. Kako lahko zagotovimo, da se uslužbencem podjetja, ki si medsebojno pošiljajo pošto, le te ne da prebrati z prisluškovanjem prometa na povezavah v podjetju? Navedi rešitev s konkretnimi protokoli! Je sploh mogoče to zagotoviti?
   e) Ko pošljemo PDF v sporočilu, za koliko se poveča njegova dolžina med prenosom?