Izpit RKVB, VSS, FRI, 1. letnik, 25. 8. 2015

Ime: _____

Priimek: _____

Vpisna številka: _____

RKVB

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

1) (20%) TCP oddajnik odpošlje 2 velika segmenta (prvi ima 5180, drugi pa 3840 bajtov), ki se zapakirata vsak v en velik datagram. Na poti do cilja naletita povezavo z MTU = 3800. Kaj se zgodi z njima? V naslednjem koraku morata 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? (Opozorilo: pri izračunih ne pozabite upoštevati velikosti glave IP datagrama!)

2) (10%) Kaj pomenita CS in CD v CSMA/CD? Pojasnite. Na katero plast sodi?

3) (15%) V enem stavku (za vsako) opišite, kaj so naslednje vrednosti pri protokolu TCP in kdaj se navadno spreminjajo:
   a) Zamašitveno okno (Congestion Window)
   b) Sprejemno okno (Receive Window)
   c) MSS (max. Segment size)

4) (15%) Primerjamo naprave: razdelilnik (hub), stikalo (switch), usmerjevalnik (router).
   a) Za vsako od naslednjih naprav napišite, ali imajo MAC naslove in ali imajo IP naslove. Odgovore utemeljite.
   b) Kjer je odgovor pozitiven, napišite koliko najmanj in koliko največ naslovov MAC ali IP imajo.
   c) Na katerih plasteh delujejo te naprave?

5) (10%) Prejemniku boste poslali sporočilo, vendar vas skrbi, da ga bo med prenosom napadalec prestregel in spremenil. Zato želite zagotoviti integriteto in zaupnost. Denimo da znamo uporabljati samo asimetrično kriptografijo, ključi pa so že vzpostavljeni. Katere od naslednjih postopkov boste uporabili in v kakšnem zaporedju? Kaj boste kriptirali? Dopišite pojasnilo.
   a) Enkripcija s simetričnim ključem
   b) Enkripcija z zasebnim ključem prejemnika
   c) Enkripcija z lastnim zasebnim ključem
   d) Dekripcija z lastnim zasebnim ključem
   e) Dekripcija z javnim ključem prejemnika
   f) Dekripcija s svojim javnim ključem
   g) Enkripcija z javnim ključem prejemnika
   h) Zgoščevanje

6) (10%) Za naslov 212.235.180.205/29 napišite:
   a) Naslov podomrežja v desetiški obliki, masko v desetiški.
   b) Najmanjši naslov naprave v desetiški obliki.
   c) Naslov broadcast v desetiški obliki.
   d) Največji naslov naprave v desetiški obliki.
   e) Število naprav, ki jih lahko priklopimo v to podomrežje.

7) (10 %) S programom Wireshark smo zajeli spodnji okvir:

```
IEEE 802.11 Beacon frame, Flags:
Type/Subtype: Beacon frame (0x08)
Frame Control: 0x0080 (Normal)
 Version: 0
 Type: Management frame (0)
 Subtype: 8
 Flags: 0x0
 .... ..00 = DS status
 .... .0.. = More Fragments
 .... 0... = Retry
 ...0 .... = PWR MGT
 ..0. .... = More Data
 .0.. .... = Protected flag
 0... .... = Order flag
Duration: 0
Destination address: ff:ff:ff:ff:ff:ff
Transmitter address: 00:0c:41:f3:f1:c9
Source address: 00:0c:41:f3:f1:c9
BSS Id: 00:0c:41:f3:f1:c9
Fragment number: 0
Sequence number: 3745
Nadaljevanje na desni >
```

```
IEEE 802.11 wireless LAN management frame:
Fixed parameters (12 bytes)
 Timestamp: 0x000000008858B185
 Beacon Interval: 0,102400 [Seconds]
 Capability Information: 0x0015
 .... .... .... ...1 = ESS capabilities
 .... .... .... ..0. = IBSS status
 .... ..0. .... 01.. = CFP participation cap.
 .... .... ...0 .... = Privacy
 .... .... ..0. .... = Short Preamble
 .... .... .0.. .... = PBCC
 .... .... 0... .... = Channel Agility
 .... ...0 .... .... = Spectrum Management
 .... .0.. .... .... = Short Slot Time
 .... 0... .... .... = Automatic Power Save
 ..0. .... .... .... = DSSS-OFDM
 .0.. .... .... .... = Delayed Block Ack
 0... .... .... .... = Immediate Block Ack
Tagged parameters (32 bytes)
 SSID parameter set
 Tag Number: 0
 Tag length: 7
 SSID: "channel"
 Supported Rates: 1,0(B) 2,0(B), 56, 150
 DS Parameter set: Current Channel: 6
 CF Parameter set: CFP count 1, CFP period 2,...
 Traffic Indication Map (TIM): DTIM 0 ...
```

a) Za kateri protokol povezavne plasti gre in za kakšeno funkcionalnost ima ta okvir?
b) Kakšno je ime omrežja?
c) Na podlagi katerega podatka lahko zagotovo vemo preko katere naprave smo priključeni v to omrežje?
d) Ali to omrežje podpira šifriran promet? Katere zastavice nam to povedo in kako so nastavljene?
e) Koliko strojnih naslovov je lahko v 802.11 glavi in za kaj se uporabljajo?
f) Kolikšna je najnižja in najviša hitrost prenosa v tem omrežju?

8) (10 %) S programom Wireshark smo zajeli spodnji zahtevi HTTP, ki jih prikazujeta izpis 1 in izpis 2.

```
Izpis 1:
GET
/form.php?ime=Rdeca&priimek=Kapica&poslji=Do+it%21
HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg,
image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: sl
User-Agent: Mozilla/5.0 (Windows NT 6.1)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0
Accept-Encoding: gzip, deflate
Host: ubuntu
Connection: Keep-Alive
```

```
Izpis 2:
POST /form.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg,
image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: sl
User-Agent: Mozilla/5.0 (Windows NT 6.1)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: ubuntu
Content-Length: 40
Connection: Keep-Alive
Cache-Control: no-cache
ime=Rdeca&priimek=Kapica&poslji=Do+it%21.
```

a) Kakšen je tip zahteve HTTP v izpisu 1? Kakšen je tip zahteve HTTP v izpisu 2?
b) Kakšna je glavna razlika med prikazanima tipoma zahtev HTTP?
c) Kakšne je vrednost polja priimek v obeh primerih?
d) Za katero različico protokola HTTP gre v obeh primerih?
e) Kateri program (spletni brskalnik) smo uporabili za pošiljanje zahteve? Odgovorite kar se da natančno.