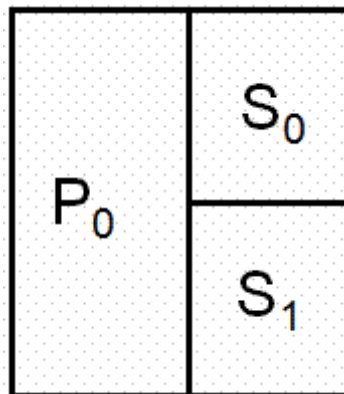


RK izpit 8. 6. 2010

- 1) TCP/IP protokolarni sklad
 - a. Narišite ga in navedite vse plasti.
 - b. Za najnižjo plast opišite naloge in en(katerikoli) način prenosa ničle oz. enice.
 - c. Za vse ostale plasti navedite po en standardni protokol.
- 2) Kaj so povezovalne in kaj usmerjevalne tabele? Kje se uporabljajo? Navedite podobnosti in razlike med enimi in drugimi.
- 3) Opišite izvedbo storitve Traceroute: kaj dela in kako to dela.
- 4) Nadzor zamašitev: TCP proces je nazadnje sprejel segment 1500 in ga potrdil z ACK 3000. Vsi segmenti naj bodo enako dolgi.
 - a. Kako dolg je bil segment?
 - b. Kakšna bo številka naslednjega prejetega segmenta in potrditve, ki jo bo oddal, če bo vse v redu na omrežju?
 - c. Kakšna bo številka naslednjega **prejetega** segmenta in potrditve, ki jo bo oddal, če se bo vmes en segment izgubil ?
 - d. Kaj je zamašitveno okno in kdo ga določa?
 - e. Kaj vse vpliva na določanje velikosti zamašitvenega okna ?
- 5) Opišite trojno rokovanje. Kateri protokol transportne plasti ga uporablja in kateri ga ne uporablja?
- 6) Elektronska pošta
 - a. Zakaj ima elektronsko sporočilo lahko v glavi večje število vrstic Received?
 - b. Navedite vsaj en razlog, zakaj bi želeli uporabljati raje POP3 kot IMAP.
 - c. Navedite vsaj en razlog, zakaj bi bilo bolje, da dan pred izpitom ne bi pošiljala asistentu nalog po elektronski pošti?.
- 7) Imamo kriptosistem, ki ga sestavlja škatla P0 in škatli S0 in S1. V kaj se kriptira 10101010? Pokažite tudi vmesne korake. Kriptosistem prikazuje spodnja slika, koder in dekoder v škatlah S sta podana v spodnji tabeli, permutacije v škatlah so:
 - P0 = (52130476)
 - P znotraj S0 = (6 1 7 3 15 0 8 13 12 14 9 10 5 2 4 11)
 - P znotraj S1 = (8 5 0 7 14 2 15 13 10 11 3 4 1 12 9 6)

4/16	
0000	8
0001	5
0010	13
0011	1
0100	12
0101	9
0110	6
0111	10
1000	11
1001	3
1010	4
1011	14
1100	2
1101	15
1110	0
1111	7

16/4	
0	1000
1	0110
2	1100
3	1111
4	0000
5	0111
6	1001
7	1010
8	1011
9	0001
10	0010
11	1101
12	1110
13	0011
14	0100
15	0101



8) S programom Wireshark smo zajeli spodnji paket:

```

Ethernet II, Src: Microsof_19:87:c6 (00:03:ff:19:87:c6), Dst: DigitalD_96:c6:57 (00:11:6b:96:c6:57)
  Destination: DigitalD_96:c6:57 (00:11:6b:96:c6:57)
  Source: Microsof_19:87:c6 (00:03:ff:19:87:c6)
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  opcode: reply (0x0002)
  [Is gratuitous: False]
  Sender MAC address: Microsof_19:87:c6 (00:03:ff:19:87:c6)
  Sender IP address: 212.235.189.158 (212.235.189.158)
  Target MAC address: DigitalD_96:c6:57 (00:11:6b:96:c6:57)
  Target IP address: 212.235.189.155 (212.235.189.155)

```

- Kateri protokol vsebuje okvir Ethernet II, ki smo ga zajeli?
- Opišite delovanje tega protokola.
- Opišite eno pomanjkljivost tega protokola.
- Zakaj so okviru Ethernet II dodani biti prikazani pri oznaki "Trailer"?

9) Na usmerjevalniku imamo spodnjo usmerjevalno tabelo:

Omrežje	Prehod	Vmesnik
10.1.0.0/16	10.1.0.1	A
10.2.0.0/16	10.2.0.1	B
192.168.1.0/24	192.168.1.1	C
192.168.1.0/25	10.1.0.2	A
0.0.0.0/0	192.168.1.2	C

Za vsakega od spodnjih naslovov IP določite prehod **in** vmesnik preko katerega, ga bo usmerjevalnik poslal:

- 193.2.1.66
- 10.2.0.129
- 192.168.1.64
- 192.168.1.130
- 10.1.0.2

10) S programom Wireshark smo zajeli spodnjo sejo:

```
220 Private FTP. Tresspassers will be shot.
USER tralala
331 Password required for tralala
PASS hopsasa
230 Logged on
SYST
215 UNIX emulated by FileZilla
PWD
257 "/" is current directory.
EPSV
229 Entering Extended Passive Mode (|||3932|)
LIST
150 Connection accepted
226 Transfer OK
QUIT
221 Goodbye
```

- Za kateri protokol gre?
- V eni od vrstic lahko preberete sporočilo "Entering Passive Mode". Ta protokol lahko deluje v aktivnem ali v pasivnem načinu. Kakšna je razlika med njima?
- Opišite eno (poleg tiste, ki jo rešuje pasivni način) pomanjkljivost protokola.
- Kako bi to pomanjkljivost (prejšnje vprašanje) odpravili?