Joti 2010 kierros 3 arvosteluohje

tehtävä 1

```
Verkko:                 130.          233.          194.             0
Binäärinä: 10000010.11101001.11000010.00000000
Netmask:   11111111.11111111.11111111.00000000
```

/24 tarkoittaa, että 24 bittiä osoitteesta on verkko-osaa, loput 8 bittiä koneosaa. Verkko-osan bitit ovat pysyvät aina samoina. Verkko-osoite on verkon ensimmäinen osoite, eli sen koneosan bitit ovat nollia. Broadcast-osoitteessa koneosan bitit ovat kaikki ykkösiä.

Netmaskin perusteella tiedetään, että vapaana on on kahdeksan bittiä eli 256 (2^8)
osoitetta. Aloitetaan osoitteiden jako suurimmasta verkosta.

40 työasemaa
130.233.194.0/26
Broadcast: 130.233.194.63
netmask: 255.255.255.192

37 akateemista työasemaa
130.233.194.64/26
Broadcast: 130.233.194.127
netmask: 255.255.255.192

32 palvelinta ja virtuaalikonetta
130.233.194.128/26
Broadcast: 130.233.194.191
netmask: 255.255.255.192

Osoitteet .0-.128 on nyt jaettu.Vapaana on vielä /26-verkko eli 64 osoitetta. Jaetaan ne hallintatyöasemien ja ylläpitoasemien kesken.

15 hallintatyöasemaa
130.233.194.192/27
Broadcast: 130.233.194.223
netmask: 255.255.255.224

8 ylläpitoasemaa
130.233.194.224/27
Broadcast: 130.233.194.127
netmask: 255.255.255.192

Viimeisen verkon koko olisi voinut olla myös /28, jolloin jäljelle olisi jäänyt yksi /28-verkko eli 16 osoitetta. On makuasia jättääkö tyhjää tilaa vai tekeekö liian ison verkon.

a. verkkojaosta 2p. Selityksestä 4p. Selityksen ei tarvitse olla ihan hirveän kummoinen, mutta siitä pitää näkyä ymmärrys.

b. IP-aliverkotus on rakenteeltaan binääripuu, jossa kuljetaan osoitteen bittien mukaan puussa oikealle tai vasemmalle. Aliverkkojen tulee olla kokonaisia alipuita, joten niiden koko on rajoitettu kakkosen potensseihin, mikä aiheuttaa häviötä.

Tämä tai muuten hyvä päättely antaa 1p. Suurimman vapaan aliverkon pitäisi olla 16 osoitetta, mutta sitäkään ei tietenkään tarvinnut jättää vapaaksi.(1p) Isompia lukuja tulee karsastaa.

tehtävä 2

a. Merkin binääriesitys 0100 0000. Kirjan mallin mukaan lisätään 3 nollaa (4:nnen asteen polynomin jakojäännös on kolminumeroinen) perään kertomalla luvulla 2^3, eli saadaan luku 0100 000 000.

Itse jakolaskun tulos on jätetty yläriviltä pois, koska se on merkityksetön. Välilyönnit helpottavat nollien hahmottamista. Annetun merkin binäärilukuesityksessä nollat vilisevät.

```
  G      D  + 2^r
----  -------------
1011 |0100 0000 000
       101 1
       -----
         1 100
         1 011
          ----
          1110
          1011
           101 0
           101 1
               100 = R
```

b. Esimerkiksi “K”, joka sattuu olemaan 0100 1011 (eli alkuperäinen merkki + jakaja). Tulokseen voi päätyä iteroimalla tai päättelemällä.

tehtävä 3

a. Jujuna tehtävässä on se, että IPSec on ns. “oikea tapa” siirtää salattua liikennettä IP-tasolla. Pakettien sisältö kryptataan ja IP-tason otsakkeet sisältävät kaiken olennaisen tiedon. Lähettäjä voi vain purkaa paketin ja asettaa IP-otsakkeen lähettäjä-kentän uusiksi.

OpenVPN puolestaan toimii SSL/TLS:n päällä siten, että se muodostaa sovellustason putken kahden pisteen välillä. Lähettäjäpää ohjaa halutun osan liikenteestä putkeen ja vastaanottajapää paketoi tiedon uudelleen IP-tasolle ja teeskentelee olevansa lähettäjä.

OpenVPN:ssä alemman tason liikennettä kuljetetaan ylemmän tason protokollan päällä väliaikaiseksi.

Olennaisen ymmärtämisestä piste, ansiokkaista perusteluista toinen.

a. IPSec vaatii selkeästi enemmän konfigurointia. OpenVPN-palvelin ja sovellus ovat molemmat käyttäjän prosesseja, kun taas IPSec vaatii tukea käyttöjärjestelmän ytimen TCP/IP-stäckistä. Jopa wikipedia tietää kertoa, että OpenVPN on helpompi konffata.

b. Karkea arvio riittää. Roadwarrior-setupissa luonnollisestikin kaikki liikenne välittäjäpalvelimella on kaksinkertainen, koska se vastaanottaa ja lähettää kaikki yhteyden paketit. Välittäjältä lopulliselle palvelimelle ei synny overheadia kummastakaan teknologiasta. IPSecissä overheadia syntyy Security Associationin (SA) muodostamisesta päiden välille (ei tarvitse mainita) ja lisäotsakkeista jokaisessa IP-paketissa. OpenVPN:ssä overheadia syntyy SSL:ää kuljettavan TCP-yhteyden ylläpidosta, mikä on kalliimpaa kuin pelkkä IP-otsakkeen lisääminen.

Arviolta yhden IP-otsakkeen lisääminen jokaiseen pakettiin lisää joitain prosentteja. Tyypillinen pakettikoko Ethernetissä on 1500 tavua ja ipsec-kapsulointi vie minimissään alle 20 tavua.

Vastaavasti OpenVPN-ratkaisussa tulee SSL/TLS:n mukana tuleva overheadi, joka on suurempi. Tämän laskeminen ei ole fiksua, mutta TCP/IP-stäkkiä ajattelemalla pitäisi pystyä päättelemään tai arvaamaan, että overheadi on suurempi kuin IPSecissä, koska jos käydään korkeammalla tasolla ja palataan alemmalle, hukataan alemman tason edullisuutta tuovat ominaisuudet. Tämänsuuntaisesta näkemyksestä piste.