Tietoliikenteen perusteet 1 2021, syventäviä tehtäviä osa 1

Nämä syventävät tehtävät vastaavat tutkinto-opiskelijoiden ensimmäisen viikon harjoitustehtäviä. Ne liittyvät tämän kurssin oletettuihin esitietoihin (tehtävät 1 ja 2), osaan 1.1 (tehtävä 4), osaan 1.2 (tehtävän 6 ensimmäinen osa) sekä osaan 2.4 (tehtävä 3). Lisäksi mukana on orientoivia tehtäviä (tehtävä 5 ja tehtävän 6 loppuosa), joihin liittyvät tarkemmat käsitteet tulevat vastaan tällä kurssilla tai seuraavalla Tietoliikenteen perusteet 2 –kurssilla. Näihin orientoiviin tehtäviin on lisäselitystä tässä tiedostossa sivuilla 3, 4 ja 5.

1) Tietokoneen toiminta –kurssilla on tutustuttu tietokoneen rakenteeseen ja sen perustoiminnallisuuteen. Koska tietoliikenteen toiminnallisuus nivoutuu yhteen laitteiston ja käyttöjärjestelmän toimintojen kanssa, niin kerrataan joitakin keskeisiä asioita tästä kurssilta.
   a) Mikä on keskeytys? Mitä silloin tapahtuu?
   b) Mitä ovat laiteajuri ja laiteohjain? Mitä ne tekevät ja miten ne toimivat yhdessä?
   c) Millaisia I/O:n toteutusvaihtoehtoja laitteistolla on?

2) Bittejä ja lukuja.
   a) Selitä bitin (bit) ja tavun (byte) ero “rautalangasta vääntämällä”.
   b) Laske yhteen kolme binäärilukua: 10010011, 10101010 ja 01110111. (Allekkainlasku onnistuu hyvin binääreillä!)
   c) Esitä seuraavat luvut binäärilukuna ja heksadesimaalilukuna: 21, 246 ja 430. (Kokeile laskea käsin, mutta kannattaa myös selvittää, miten muutos tehdään näppärästi laskimella tai wolframalpha.com sivustolla.)
   d) Jos tunnistekentälle (numeromuotoinen luku) on varattu tilaa 8 bittiä, miten monta tunnistetta voidaan esittää? Entä jos tilaa on nelinkertainen määrä eli 32 bittiä, monta tunnistetta silloin voidaan erottaa toisistaan?
   e) Miten suuria lukuja tarkoittavat etuliitteet nano, tera, piko ja peta? (Palauta muutkin etuliitteet eli SI-järjestelmän kerrannaisyksiköt mieleesi esim. Wikipedian taulukosta.)

3) Oletetaan, että sinun pitää mahdollisimman nopeasti toimittaa 4 teratavua (TB) dataa Helsingistä Rovaniemelle. Data mahtuu siis näppärästi tällä hetkellä myynnissä olevalle ulkoiselle usb-levylle.
   a) Käytettävissäsi on linkki, jonka nopeus on 1 Gbps. Lähettäisitkö datan tällä linkillä vai käyttäisitkö jotain pikatoimituspalvelua (esim. DHL Express, joka lupaa toimitukseen seuraavaan päivään klo 12 mennessä)? Miksi?
   b) Entä jos linkin nopeus olisi vain 100 megabittiä sekunnissa, mutta data pitäisi toimittaa Uuteen Seelantiin, jonne pelkät lennot kestävät 34 tuntia? Laivarahti puolestaa vie muutaman viikon? Mikä on silloin nopein tapa?

4) Verkon liikenteestä ja rakenteesta
   a) FUNET julkaisee oman kytkentäpisteensä FICIXin kautta kulkevia liikennemääriä. Millaisia selityksiä keksit liikennemäärien vaihtelulle? Kuinka suurta tuo vaihtelu on (eli mikä on pienin ja suurin liikennemäärä, entä keskiarvo)? Kuinka paljon paketteja yhdyspisteen kautta kulkee? Mikä kolmesta FICIX-pisteestä välittää eniten liikennettä (katso luvut vuoden ajalta)? Missä nämä pisteet sijaitsevat?
   b) Valtaosa mannerten välisestä liikenteestä tapahtuu merikaapeleilla. Verkkosivulla https://www.submarinecablemap.com/#/ on esitetty tämänhetkiset merikaapelit. Miltä paikkakunnilta Suomessa kaapeleita lähtee ja minne ne menevät?

5) Verkon rakenteesta. Pakettien reittejä voi tarkastella komennon traceroute avulla. Suorita traceroute komentoa jollakin laitoksen koneella tai kotikoneellasi. (Traceroute on unix/linux komento, vastaava komento windowsissa on tracert.)
Huomaa, että verkon omistaja voi estää tracerouten käyttämän protokollan viestien kulkemisen omassa verkossaan, jolloin kaikista kohteista ei voi saada tietoa.

   a) Miten traceroute selvittää reittiä kohteeseen? (Lue vaikka man-sivu ja yritä hahmottaa perustoiminnallisuus. Kerää samalla ylös termit, joita et vielä ymmärtänyt.)
   b) Suorita traceroute komento muutamaan eri kohteeseen. Esimerkiksi
      i) Tee traceroute johonkin pohjoismaiseen (tai kotimaiseen) kohteeseen (vaikka Tukholmaan KTH: www.kth.se).
      ii) Tee traceroute komento johonkin Keski- tai Itä-Eurooppalaiseen kohteeseen (vaikka ETH Zürichissä: www.ethz.ch)
      iii) Tee traceroute komento johonkin kaukokohteeseen Pohjois-Amerikassa, Australiassa, tms (vaikka Sydneyn yliopisto sydney.edu.au)
   c) Analysoi nyt tekemiäsi traceroute kyselyjä.
      i) Millaisia havaintoja teit?
      ii) Kuinka monta hyppyä tarvitaan ennen kuin ollaan vastaanottajalla asti?
      iii) Onko kiertoviiveissä eroja? Millaisia?
      iv) Löydätkö yhteysvälin/yhteysvälejä, joissa viesti on kulkenut merikaapelissa?
      v) Mitä voit päätellä näiden kokeiden perusteella verkon rakenteesta?
   d) Ping on tracerouten lisäksi toinen paljon käytetty komento. Sillä voi vain selvittää onko kohde laite juuri nyt aktiivisena verkossa, verkkoyhteys kohdelaitteeseen olemassa ja kuinka kauan viestit kulkevat johonkin kohteeseen ja takaisin. Mittaa vielä ping-komennolla kommunikoinnin kestoja äskeisiin kohteisiin. Onko luvuissa eroja tracerouten näyttämiin lukuihin?

6) Osoitteista
   a) Selvitä oman tietokoneesi tietoja
      i) Mikä on koneen IP-osoite ja MAC-osoite?
      ii) Onko koneellasi IPv6:n mukaista osoitetta? Jos, niin mikä se on?
      iii) Mikä on koneellesi määritelty aliverkon peite (network mask)?
      iv) Missä verkossa nämä tiedot selvitit? Tiedot ovat erilaisia eri verkoissa!
   b) Whois –tietokannassa säilytetään verkko-osoitteisiin liittyviä julkisia tietoja. Funet (kuten monet muutkin organisaatiot) tarjoaa helpon kyselymahdollisuuden tähän tietokantaan: https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/whois-palvelu-nayttaa-verkkotunnuksen-julkiset-tiedot
      i) Selvitä mitä tästä tietokannasta löytyy www.helsinki.fi:stä?
      ii) Entä helsinki.fi:stä?
      iii) IP-osoitteeesta 128.214.4.29?
      iv) mooc.fi:stä?

☆ Ylimääräinen tehtävä: Piirrä kurssin kuluessa itsellesi oma miellekartta, käsitekartta tai muu havainnollistava kaavio, joka helpottaa sinua kurssilla vastaan tulevien käsitteiden sitomisessa isompaan kokonaisuuteen. Täydennä tätä nyt aloittamaasi kaaviota kurssin kuluessa.

Taustatietoa muutamasta komennosta, josta voivat auttaa tehtävien tekoa Linux-ympäristössä:

ip addr (tai ifconfig)

ip on tärkeä konsolityökalu linuxissa jonka avulla saadaan paljon selville tietokoneen senhetkisistä IP-osoitteista ja verkkoliitännöistä. Vastaava toiminnallisuus löytyy myös vanhemmasta ifconfig-ohjelmasta. Tarkastellaan erästä tulostetta yliopiston verkossa:

Vaikka esimerkissä on ifconfig, ainakin pajakoneilla kannattaa kokeilla uudempaa ip addr -komentoa.

```
$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
       inet 127.0.0.1  netmask 255.0.0.0
       inet6 ::1  prefixlen 128  scopeid 0x10<host>
       loop  txqueuelen 1000  (Local Loopback)
       RX packets 6631  bytes 411901 (411.9 KB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 6631  bytes 411901 (411.9 KB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp60s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.112.23.213  netmask 255.255.240.0  broadcast 10.112.31.255
       inet6 fe80::603f:ba78:cfdc:3453  prefixlen 64  scopeid 0x20<link>
       ether 38:37:8b:f2:ec:ce  txqueuelen 1000  (Ethernet)
       RX packets 434551  bytes 578335175 (578.3 MB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 252521  bytes 31597734 (31.5 MB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Tässä esimerkissä tietokoneesta löytyy kaksi eri verkkoliitäntää: lo eli loopback ja wlp60s0, joka on tässä tapauksessa langaton verkkosovitin. Varsin usein tietokoneesta löytyy myös fyysinen verkkoportti, jolloin listalta löytyisi myös sen tiedot. Pääsääntöisesti kaapeliliittymässä nimessä on eth-liite (ethernet) ja langattomassa liittymässä wl-liite (wireless). Loopback on liittymä. jota tietokone käyttää sisäiseen kommunikointiin. Loopback siis kirjaimellisesti ohjaa siihen kytkeytyvän tietoliikenteen takaisin laitteeseen itseensä.

Kun liittymät ovat selvillä, on aika selvittää tärkeimmät tiedot mitä ifconfig tarjoaa. Alla on selitykset yleisimmille lyhenteille:

inet IP-osoite. Osoite on IPv4-protokollan mukainen.
Inet6 IPv6-osoite.
netmask Aliverkon peite. Usein myös subnet mask tai network mask.
brd tai **broadcast** Yleislähetysosoite.
ether tai **link/ether** MAC-osoite.
RX Vastaanotettu data (received).
TX Lähetetty data (transmitted).

Käyttämällä komentoa ip addr aliverkon peite ei ole esitetty erikseen, mutta aliverkolle varattujen bittien määrä löytyy inet-osoitteen lopusta vinoviivan jälkeen (esimerkiksi 16). Aliverkon peitteen voit laskea esimerkiksi osoitteessa http://jodies.de/ipcalc (kurssilla opetetaan myöhemmin miten aliverkon peitteen voi laskea itse).

ping

Ping on työkalu jonka avulla on tarkoitus selvittää toisen laitteen saavutettavuus ja sen kesto. Ping lähettää paketin kohteeseen ja mittaa kuinka pitkään kestää että vastaanottaja lähettää takaisin vastauksen. Alla esimerkki komennon tulosteesta:

```
$ ping www.google.fi
PING www.google.fi (172.217.21.163) 56(84) bytes of data.
64 bytes from fra07s64-in-f163.1e100.net (172.217.21.163): icmp_seq=1
ttl=56 time=7.25 ms
64 bytes from fra07s64-in-f163.1e100.net (172.217.21.163): icmp_seq=2
ttl=56 time=7.45 ms
64 bytes from fra07s64-in-f163.1e100.net (172.217.21.163): icmp_seq=3
ttl=56 time=8.04 ms
64 bytes from fra07s64-in-f163.1e100.net (172.217.21.163): icmp_seq=4
ttl=56 time=7.91 ms
^C
--- www.google.fi ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 7.253/7.667/8.045/0.331 ms
```

Esimerkissä “pingattiin” googlen palvelinta. Googlen palvelimille lähetettiin neljä pakettia, joiden ping oli keskimäärin 7.667ms. Ohjelman suorituksen voi pysäyttää painamalla Ctrl + C.

traceroute

Traceroute on työkalu jonka avulla saadaan selville mitä reittejä pitkin viesti kulkee vastaanottajalle. Alla on käytetty traceroutea selvittämään mitä pitkin viesti päätyy googlen julkiselle DNS-palvelimelle eli osoitteeseen 8.8.8.8:

```
$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1  10.112.16.3 (10.112.16.3)  3.237 ms  3.144 ms  3.103 ms
2  nat-eduroam-hy-138-163.fe.helsinki.fi (128.214.138.163)  3.471 ms  3.441 ms
3.408 ms
3  kumpula1-viikki2.fe.helsinki.fi (128.214.173.11)  3.373 ms  3.702 ms  3.675
ms
4  r1-kumpula1.fe.helsinki.fi (128.214.173.241)  10.928 ms  11.254 ms  11.184 ms
5  helsinki6-ae1-1.ip.funet.fi (193.167.253.8)  3.927 ms  4.311 ms  4.302 ms
6  se-tug.nordu.net (109.105.102.102)  10.377 ms  9.416 ms  9.352 ms
7  se-kst2.nordu.net (109.105.97.25)  9.270 ms  9.261 ms  9.208 ms
8  72.14.196.42 (72.14.196.42)  9.176 ms  9.147 ms  9.119 ms
9  108.170.253.177 (108.170.253.177)  10.862 ms 108.170.253.161
(108.170.253.161)  9.851 ms 108.170.253.177 (108.170.253.177)  10.818 ms
10  72.14.236.85 (72.14.236.85)  9.762 ms 209.85.251.233 (209.85.251.233)  9.734
ms 216.239.58.47 (216.239.58.47)  9.663 ms
11  google-public-dns-a.google.com (8.8.8.8)  10.680 ms  10.502 ms *
```

Tässä esimerkissä välietappeja vaikuttaisi olevan yksitoista. Traceroute lähettää sarjassa kolme pakettia, jotka lopulta päätyvät kohteeseensa hieman eri reittiä. Viimeisimmän paketin ilmaisema tähti (*) tarkoittaa arvoa jota ei ole: paketti on todennäköisesti hylätty tai ICMP viestiä lähetetty.

nslookup

Nslookup on työkalu jonka avulla saadaan selville verkkotunnusten IP-osoitteet. Alla esimerkki Googlen palvelimesta (esimerkissä Google on tavoitettavissa sekä IPv4 että IPv6 -osoitteiden kautta.):

```
$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.21.132
Name:   www.google.com
Address: 2a00:1450:400f:80d::2004
```