Tietoliikenteen perusteet: Kokeeseen tulevista asioista

T. Karvi

October 2017

Kokeesta

- Kurssikoe ti 24.10.2017 klo 16:00, A111 ja B123.
- Uusintakoe pe 8.12.2017 klo 16:00, B123. Uusintakoe arvostellaan sekä erilliskokeena että kurssikokeena, ts. harjoituspisteet otetaan huomioon, jos opiskelija niin haluaa.
- Erilliskoe pe 26.1. 2018 klo 16:00, B123. Tämän kokeen järjestää todennäköisesti Tiina Niklander.

Esimerkkikoe v.2017 I

1. **Toiminta usean koneen kautta (15 p)**
   Olet kirjautunut koneelle A ja sinun pitäisi siirtää tiedosto t.txt koneelta C koneelle A. Kone C hyväksyy vain yhteyspyynnöt koneelta B, johon sinulla on myös käyttäjätunnus. Mitään muita kuin ssh-komentoa kone C ei hyväksy koneelta B ja muilta koneilta ei mitään komentoja. Lisäksi kone C voi antaa komentoja ssh ja sftp vain koneelle B. Sinulla on siis käyttäjätunnnukset kaikille kolmelle koneelle ja käytösssäsi on vain komennot ssh ja sftp. Näiden komentojen syntaksi on seuraava:
   - ssh B.cs.helsinki.fi: kirjaudutaan koneelle B.
   - sftp B.cs.helsinki.fi: otetaan ftp-yhteys koneeseen B, jonka jälkeen tiedostoja voidaan siirtää komennolla put koneesta A koneelle B ja komennolla get koneesta B koneelle A.

   Kirjoita komennot, joiden avulla siirrät tiedoston t.txt koneelta C koneelle A ollessasi koko ajan kirjautuneena koneelle A.

Esimerkkikoe v.2017 II

2. **NAT (network address translation), 15 p)**
   Kuvaile, miten reititys toimii NATin yhteydessä. Mitkä ovat NATin hyvät ja huonot puolet?
3. **Ruuhkanhallinta.**
   Esittele TCP:n ruuhkanhallinta. (15 p)
4. **Suorituskykylasku**
   Oletetaan, että 160 000 bitin tiedosto lähetetään koneelta A koneelle B piirikytkentäisessä verkossa. Oletetaan, että kaikki linkit verkossa käyttävät 12 aikajakson TDM:ää nopeudella 1,536 Mbps. Lisäksi oletetaan, että piirin perustaminen kestää 600 ms. Vasta piirin perustamisen jälkeen A voi lähettää. Kuinka kauan tiedoston lähettäminen kestää? (15 p)

Esimerkkikoe v. 2016 I

1. Selitä lyhyesti seuraavat käsitteet ja lyhenteet:
   a) Yhteydellinen viestinvälityspalvelu (connection oriented).
   b) ISO OSI -viitemalli.
   c) Vertaistoimijamalli. Anna myös esimerkki.
   d) Nimipalvelimen rekursiivinen kysely.
   e) UDP.
   f) TCP:n nopea uudelleenlähetys (fast retransmit).
   g) Reitittimen ristikytkentä (crossbar). Piirrä kuva!
   h) DHCP.
   i) Kytkin (switch).
   j) IEEE 802.11
   k) Haaste eli nonssi (nonce).
   l) Turvayhteyskanta (Security Association Database IPsec:ssä).
   m) Sovellustason yhdyskäytävä.

Esimerkkikoe v. 2016 II

(13 pistettä)

2. a) AB-protokollassa lähettäjä lähettää paketin, käynnistää ajastimen ja jää odottamaan kuittausta. Jos kuittaus tulee, lähettäjä lähettää uuden paketin samoin kuin edellisenkin. Jos oikeaa kuittausta ei tule, ajastin laukeaa ja lähettäjä lähettää uudestaan saman paketin. Oletetaan, että protokollaa käytetään siirtämään 10 megatavun tiedostoa koneelta A koneelle B. Koneiden välimatka on 4000 km ja signaalin nopeus kanavassa 200 000 km/s. Kanavaan voi lähettää nopeudella 10 megabittiä sekunnissa. Kuinka kauan tiedoston lähettäminen kestää, kun käytetään AB-protokollaa ja tiedosto pilkotaan 1000 tavun kokoisiksi paketeiksi, jotka lähetetään erikseen? Kuittausten koko on 1000 bittiä. Kanava toimii virheettömästi. (10 pistettä)

Esimerkkikoe v. 2016 III

b) Kuten edellinen kysymys, mutta nyt kanava kadottaa 10% sanomista, joista puolet on datasanomia, puolet kuittauksia. Ajastin laukeaa 5 sekunnin kuluttua, jos kuittausta ei ole saapunut. (7 pistettä)

3. Selitä, miten koneet selvittävät MAC-osoitteen. (15 pistettä)
4. Esittele salalohkojen ketjutus -menetelmä (Cipher Block Chaining, CBC) ja analysoi, miten monta pakettia menee sekaisin, jos yhden paketin lähetyksessä tapahtuu yhden bitin virhe. (15 pistettä)

Luento 1 I

- Palvelumallit: asiakas/palvelija, vertaistoimija.
- Yhteydellinen, yhteydetön ja luotettava, epäluotettava kommunikointi.
- Pakettikytkentä, piirikytkentä.
- Protokollan käsite.
- Etappivälitys (Store and Forward).
- Viiveet: prosessointi, siirto, eteneminen, jonotus.
- FDM, TDM.
- Yksinkertaisia suorituskykylaskuja. Ei binomikaavaa (s. 29).
- Läpäisy (throughput).

Luento 2 I

- DSL, ADSL.
- Kaapeliverkon periaatteet.
- Valvottu eli ohjattu ja avoin siirtotie.
- Parikaapeli, koaksiaalikaapeli, valokuitu.
- Langattoman tiedonsiirron ongelmia, mikroaalto, LAN,mobiiliverkko, satelliittiverkko.
- TCP/IP- ja OSI-pino.
- Internetin rakenne, verkkojen verkko.

Luento 3 I

- Prosessit ja pistokeet, prosessien kommunikointi.
- Käyttöjärjestelmän rooli tietoliikenteessä.
- IP-osoite ja porttinumero.
- Käsitys eri sovellusten tiedonsiirtovaatimuksista.
- Http:n perustoiminta.
- RTT, vastausaika.
- Säilyvä, ei-säilyvä yhteys.
- Evästeet, hyödyt ja haitat.
- Verkkovälimuisti (proxy).
- Ehdollinen GET.

Luento 4 I

- Nimipalvelimien hierarkia.
- Iteratiivinen ja rekursiivinen kysely.
- DNS-välimuisti ja sen myrkytyshyökkäykset.
- Sähköpostin komponentit. Kokeeseen ei kysymyksiä ftp:stä.
- Bittorrentin toiminta: hajautettu hajautustaulu, circular DHT esimerkkinä, vertaisten tuleminen ja poistuminen.

Luento 5 I

- Kuljetuskerroksen tehtävät ja tarpeellisuus.
- TCP:n ja UDP:n tehtävät.
- TCP-segmentin oleelliset tiedot.
- Alternoivan bitin protokolla (stop and wait) ja sen tehokkuus.
- Liukuvan ikkunan protokolla: lähetys- ja vastaanottoikkuna, go back N, selective repeat.

Luento 6 I

- TCP:n järjestysnumero ja tavunumerointi.
- Kuittausten säännöt.
- Nopea uudelleen lähetys.
- TCP:n vuonvalvonta.
- TCP-kättely, yhteyden purku.
- Ruuhkanhallinta: Reno (ei ajastinkaavoja), kynnysarvo.
- UDP-tarkistussumma.
- SYN-tulva ja sen torjumiskeinoja.
- Optimistinen hyökkäys.
- Istunnon kaappaus ja sen torjunta.

Luento 7 I

- Verkkokerroksen motivaatio.
- Datagrammiverkko, virtuaalinen piirikytkentäverkko.
- Etsintä reititystaulusta (longest prefix matching).
- Reitittimen ja kytkimen rakenne.
- Kolme erilaista kytkentätapaa.
- IPv4-paketin rakenne.
- Tunnelointi.

Luento 8 I

- IPv4-osoitteet, aliverkkomaski.
- Esimerkki: Verkkotunnuksen alkuosa 192.168.56.128/26. Eli viimeinen tavu on muotoa 10000000. Bitit 10 kuuluvat vielä aliverkon tunnukseen. Sen jälkeen käytössä on vielä kuusi bittiä ja kaikki yhdistelmät ovat mahdollisia. Eli viimeinen tavu voi olla aliverkossa muotoa 10111111 eli $128 + 32 + 16 + 8 + 4 + 2 + 1 = 191$.
- DHCP
- NAT
- Dijkstra
- Etäisyysvektorireititys ja sen ongelmatilanteita.
- RIP, OSPF, BGP: missä käytetään.

Luento 9 I

- Linkkikerroksen tehtävät.
- CRC.
- Kanavatyypit.
- Lähetysvuorojen jakelu yhteiskäyttökanavassa.
- Aloha ja viipaloitu Aloha.
- CSMA, CSMA/CD.
- MAC-osoitteet. (Pysyviä, käyttöjärjestelmä voi luoda väliaikaisen MAC-osoitteen esim. virtuaalikoneelle.)
- ARP.
- Lähettäminen toiseen verkkoon.
- Kytkin. (Perinteelliset keskittimet eivät juurikaan enää käytössä. Älykkäät keskittimet tulleet markkinoille älykodin yhteydessä.

Luento 10 I

- WLAN: CSMA/CA, osoitteiden käyttö.
- Osattava selitttää mitä tapahtuu ja mitkä protokollat ovat toiminnassa, kun käyttäjä käynnistää jonkin tavallisen sovelluksen.