Tietoliikenteen perusteet 1 2021,

syventäviä tehtäviä osa 2

Nämä syventävät tehtävät vastaavat tutkinto-opiskelijoiden toisen viikon harjoitustehtäviä. Ne liittyvät kurssisisältöön seuraavasti: tehtävä 1 osaan 2.4 (ja 4), tehtävä 2 osaan 3.1, tehtävät 3 ja 4 osaa 3.2 sekä tehtävät 5 ja 6 osaan 2.3. Tehtävien 1 ja 6 osalta osa tarvittavasta taustamateriaalista tulee vasta tietoliikenteen perusteet 2 -kurssilla.

1. Tarkastellaan pakettikytkentäisessä verkossa reittiä koneelta A koneelle B. Reitin varrella on kaksi kytkintä, joiden kautta paketit joutuvat kulkemaan. Reitin linkkien nopeus on 2 Mbps. Lähetettävän sanoman koko on $8*10^6$ bittiä.
    a. Oletetaan ensin, että sanoman lähetetään yhtenä kokonaisuutena pilkkomatta sitä ensin osiin. Kuinka kauan kestää siirtää paketti lähettäjältä A ensimmäiselle kytkimelle? Kytkin ottaa vastaan koko paketin ja lähettää vasta sen jälkeen eteenpäin. Kuinka kauan kestää sanoman lähettäminen vastaanottajalle B?
    b. Oletetaan seuraavaksi, että paketti pilkotaan 800 palaseen, joista jokainen on 10000 bittiä pitkä. Kuinka kauan kestää lähettää ensimmäinen palanen ensimmäiselle kytkimelle? Kun ensimmäinen kytkin on lähettämässä ensimmäistä palasta toiselle kytkimelle, A on lähettämässä toista palasta ensimmäiselle kytkimelle. Milloin ensimmäinen kytkin on saanut toisen palasen?
    c. Kuinka kauan kestää lähettää sanoma kohteelle B, kun käytetään sanoman pilkkomista? Vertaa tulosta a-kohdan tulokseen.
    d. Mitä muita syitä pakettien pilkkomiseen on kuin vain siirron nopeuttaminen?
    e. Mitä haittaa paketin pilkkomisesta voi olla?

2. Sovelluskerroksen ohjelmien suunnittelusta.
    a. Selitä, miksi asiakas-palvelijamallissa palvelimen pitää olla koko ajan saatavilla, mutta asiakkaan vain yhteyden aikana. Pohdi erityisesti, mitä tapahtuu, jos palvelija ei ole saatavilla, kun asiakas haluaa yhteyttä?
    b. Voiko sovelluskerroksen ohjelma, joka haluaa käyttää pysyvää yhteyttä käyttää kuljetuskerroksen protokollaa UDP tavanomaisen protokollan TCP sijaan? Perustele vastauksesi. [Huomaa: että voit perustella kumman tahansa vaihtoehdon oikeaksi.]

3. HTTP Tutustu http:n versioon 1.1 (RFC 2616). Oletetaan, että meillä on www-palvelin www.common.com
    a. Tee käsin http viesti, jossa on pyyntö, jolla voidaan noutaa dokumentti /usr/usrs/doc. Asiakas hyväksyy MIME version 1, GIF ja JPEG kuvia, mutta dokumentti ei saa olla 4 päivää vanhempi.
    b. Tee käsin onnistunut vastausviesti tähän pyyntöön.

    HUOM: Kirjoita siis paperille HTTP viestit sellaisina kuin ne kulkisivat asiakkaan ja palvelimen välillä. Voit oikaista attribuuttikentissä ja ottaa mukaan vain minimimäärän niitä.

    c. Ovatko seuraavat väitteet oikein vai väärin. Perustele!
        - Kaksi erillistä www-sivua (esim. www.mit.edu/research.html ja www.mit.edu/students.html) voidaan lähettää käyttäen samaa säilyvää (persistent) yhteyttä.

- Selaimen ja palvelimen ei-säilyvällä yhteydellä on mahdollista, että yksi TCP-segmentti kuljettaa kaksi erillistä http-pyyntöä.

4. Evästeitä voidaan käyttöön moneen eri tarkoitukseen. Materiaalissa oli yksinkertainen esimerkkikuva evästeiden käytöstä. Piirrä vastaava kuva, mutta sellaisessa tilanteessa, jossa evästeitä käytetään mainonnassa kohdennetun mainonnan apuna. Huomaa, että mainokset tulevat muualta kuin asiakkaan käyttämältä www-palvelimelta. Mieti siis sellainen evästeiden käyttöön liittyvä skenaario, jossa evästeet tukevat kohdennettua mainontaa. Skenaariossa on mukana vain nuo edellä mainitut kolme osapuolta.

5. DHCP
   a. Etsi kurssimateriaalista ja internetistä (wikipedia, RFCt) mitä tietoja DHCP-palvelija lähettää viestissä DHCP offer.
   b. Kurssimateriaalissa on tarkasteltu tilannetta, jossa aliverkon yhdyskäytävä toimii itse DHCP-palvelimena. Näin ei kuitenkaan aina ole, vaan DHCP-palvelin voi olla myös aliverkon ulkopuolella. Millä nimellä kutsutaan aliverkon yhdyskäytävän toimintoa, joilla se ohjaa DHCP pyynnöt DHCP-palvelijalle?

6. NAT ja P2P: [*Huomaa, että tehtävän täydellinen ratkaiseminen edellyttää myöhemmin kurssilla vastaantulevaa tietoa. Ongelman hahmottamisen ja ratkaisujen ideoinnin pitäisi onnistua jo tässä vaiheessa kurssia.]*
   NAT on suunniteltu tukemaan asiakas-palvelija –mallia, jossa asiakas on NATin takana olevassa aliverkossa ja palvelin julkisessa Internetissä. NAT-laite muuntaa oman yksityisen aliverkon laitteiden IP-paketteja siten, että ne näyttäisivät tulevan tältä NAT-laitteelta. Se osaa ohjata myöhemmin saapuvat vastauksen ylläpitämänsä muunnostaulun perusteella oikeaan suuntaan. Tämä toiminnallisuus samalla estää yhteydenotot julkisen verkon laitteilta suoraan yksityisen verkon laitteille.
   Vertaisverkoille (P2P) on taas tyypillistä se, että vertaiset kommunikoivat suoraan toistensa kanssa.
   a. Mikä on perusongelma NATin ja P2P sovellusten kanssa? Miten sen voi välttää? (Vinkkinä: ratkaisusta käytetään nimiä NAT traversal tai Hole punching)
   b. Oletetaan että P2P verkon vertainen (peer) Arnold löytää tiedon, että vertaisella Bernard on hallussaan tiedosto, jonka Arnoldkin haluaa ladata itselleen. Sekä Arnold että Bernard ovat molemmat omien NAT-reitittimiensä takana. Millaisella ratkaisulla Arnold voi ottaa yhteyttä Bernardiin? Keksitkö muunlaisia ratkaisuvaihtoehtoja? Onko mahdollista keksiä sellaista ratkaisua, jossa ei olisi mitään lisäelementtejä?
   c. Onko tilanne erilainen, jos jommallakummalla vertaisista on julkinen IP-osoite? Onko väliä kummalla julkinen osoite on? Miten yhteydenotto nyt voisi toimia?

☆ Ylimääräinen tehtävä: Jos olet kiinnostunut tutkimaan viestien sisältöä analysointiohjelmalla wireshark, niin tutustu valmiiseen kaappaukseen http.cap (http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=http.cap). Analysoinnissa voit vaikka selvittää, kuinka monta HTTP-protokollan mukaista viestiä tässä kaappauksessa on. Entä TCP-protokollan paketteja. Voit myös pohtia, mitä voit havaita/päätellä pakettien otsikoista. Koska valmis kaappaus on tehty salaamattomasta http-protokollasta, niin voit myös lukea sivujen sisältöjä ja ainakin nähdä, mitä www-sivuja viesteissä kulkee.

Huomaa, että wireshark ohjelmalla voit myös itse kaapata verkkoliikennettä. Tämä ei ole kuitenkaan aina luvallista, joten mikäli niin aiot tehdä, niin varmista aina ensin verkon omistajalta tämän luvallisuus.