

(4. tehtävä paperin kääntöpuolella)

1. Kerro lyhyesti (2-3 lausetta) mitä seuraavat protokollat tai järjestelmät tekevät ja mihin niitä käytetään, sekä mitä kuljetuskerroksen protokollan päälle ne on rakennettu. (6 p)
 - a. Domain Name Service (DNS)
 - b. Hypertext Transfer Protocol (HTTP)
 - c. Real-time Transport Protocol (RTP)

2. Sinulla on käytössäsi mielikuvituksellinen suora linkki Espoosta Melbournen lähistöllä olevaan pikkukylään, johon etäisyyttä on 15000 kilometriä. Lähetyksenopeus linkillä on 100 megabittiä sekunnissa, ja voit olettaa että bitit siirtyvät nopeudella $2 \cdot 10^8$ m/s. Lähetät linkin yli 1500:n tavun kokoisia paketteja.

(6 p)

- a. Kuinka kauan kestää lähetyksen aloittamisesta ennen kuin ensimmäinen paketti on perillä?
- b. Kuinka kauan aikaa kuluu yhden gigatavun perillesaapumiseen, jos oletetaan että yksikään paketti ei huku, eikä käytössä ole ruuhkanhallintaa tai muita hidastavia tekijöitä?
- c. Kuinka monta kokonaista pakettia ehdit lähettää ennen kuin saat ensimmäisestä paketista kuittauksen?

Kerro vastauksen lisäksi kussakin kohdassa laskutoimitus miten pääsit lopputulokseen, sekä mahdolliset lisäoletukset. Kannattaa olla tarkkana yksiköiden kanssa. *(Mikäli käytössäsi ei ole laskinta, anna ainakin laskutoimitus riittävän seikkaperäisesti, sekä päässä tai paperilla laskettu arvio lopputuloksesta)*

3. Vastaa seuraaviin kysymyksiin koskien Transport Layer Security (TLS)-tietoturvaprotokollaa (6p)

- a. Kuvaile TLS:n toiminta pääpiirteissään: mikä sen tarkoitus on, ja mihin se asettuu tietoliikennepinossa. Pystytkö esimerkiksi Wireshark-ohjelmalla selvittämään mitkä kuljetuskerroksen portit ovat käytössä?
- b. Mitä voit sanoa TLS:n käytön vaikutuksesta yhteydenmuodostuksen kestoon? Kuinka monta sanomanvaihtoa tarvitaan ennen kuin olet sovellus pääsee lähettämään hyötykuormaansa? Kauanko tämä neuvottelu kestäisi esimerkiksi ylläolevan esimerkin tapauksessa, kun avattaisiin yhteys Melbourneen (hyvin perusteltu arvio riittää)?
- c. Mikä on sertifikaattien rooli TLS:n yhteydessä?

4. Oheinen kuva esittää TCP:n ruuhkaikkunan käyttäytymistä erään yhteyden alkuvaiheissa kymmenen lähetyskierroksen ajan. Lähetyskierros vastaa siis aikaa, jonka aikana yksi ikkunallinen paketteja ehditään lähettää ja kuitata. Kuvaile yksityiskohtaisesti mitä missäkin kohdassa tapahtuu ja miksi. (6p)

