TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

OPINNÄYTETYÖRAPORTTI

Taloyhtiöverkkojen tekniikat

Jaakko Tani

Tietojenkäsittelyn koulutusohjelma
Marraskuu 2006
Työn ohjaaja: Harri Hakonen

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä(t): Jaakko Tani

Koulutusohjelma(t): Tietojenkäsittely

Tutkintotyön nimi: Taloyhtiöverkkojen tekniikat

Title in English: Techniques used in real estate networks

Työn valmistumis-kuukausi ja -vuosi: marraskuu 2006

Työn ohjaaja: Harri Hakonen **Sivumäärä:** 46

TIIVISTELMÄ

Tämä opinnäytetyö on tehty LanWorld Finland Oy:n toimeksiannosta. Työ sai alkunsa, kun LanWorldin runko-operaattorit ilmoittivat siirtyvänsä verkoissaan PPPoA-pohjaisista ratkaisuista PPPoE-pohjaisiin ratkaisuihin. Tarkoituksena on esitellä taloyhtiöverkoissa yleisimmin käytettyjä verkkotekniikoita ja miettiä, miten verkkoratkaisuita voisi parantaa. Lisäksi tarkoitus on tutkia PPPoA:n ja PPPoE:n välisiä eroja LanWorld Finland Oy:n näkökulmasta.

Esilletuomani parannusehdotukset olen pyrkinyt pitämään mahdollisimman yksinkertaisina toteuttaa sekä teknisesti että taloudellisesti. Näen, että LanWorld Finland Oy:n nykyään käyttämät verkkoratkaisut ovat toimivia, mutta verkkojen toimintaa ja hallittavuutta voitaisiin parantaa muun muassa ottamalla käyttöön VLANit ja asentamalla käytettyjä verkon aktiivilaitteita tasaisemmin taloyhtiöiden sisällä. Runko-operaattoreiden verkoissa tapahtuvat muutokset eivät puolestaan aiheuta suuria toimenpiteitä LanWorld Finland Oy:n kohteissa.

Opinnäytetyön tuloksena toimeksiantajalla on yhteenvedot heidän käyttämiensä tekniikoiden perusteista sekä perusteltuja muutosehdotuksia heidän nykyisten kohteidensa verkkoratkaisuihin.

Avainsanat: OSI ADSL Ethernet ATM Taloyhtiöverkko

TAMPERE
POLYTECHNIC

Author(s): Jaakko Tani

Degree Programme(s) Business Information Systems

Title: Techniques used in real estate networks

Month and year: November 2006

Supervisor: Harri Hakonen **Pages:** 46

ABSTRACT

This thesis was initated by LanWorld Finland Oy when they heard that their core service providers announced that they were going to make changes in their networks. The biggest change would be the transiotion from PPPoA (Point-toPoint Protocol over ATM) to PPPoE (Point-to-Point Protocol over Ethernet). My goal is to find out the differences between PPPoA and PPPoE from LanWorld's point of view. I'm also going to go over the most common network techniques used by LanWorld and try to come up with ways to improve their current solutions.

The improvements which i came up with are as simple as possible both technically and financially. I think that the solutions used currently by LanWorld are good but they could improve the efficciency of their networks by implementing VLANs and installing their equipment using a bit more scattered pattern. In my thesis I came to a conclusion that the change from PPPoA to PPPoE won't affect LanWorld Finland's current solutions much.

As a result of this thesis LanWorld Finland Oy now has a summary of the basics of the techniques most used by them in their networks. In addition they now have justified suggestions on how to improve their current network solutions even more.

Keywords: OSI ADSL Ethernet ATM Real estate network

Sisällysluettelo

1 JOHDANTO

Opinnäytetyöni aihe syntyi kun suoritin harjoittelujaksoani LanWorld Finland Oy:ssä kevättalvella 2006. LanWorld tarjoaa laajakaistaisia internetliittymiä kuluttajille. Yksittäisten käyttäjien lisäksi LanWorld tarjoaa liittymiä kokonaisille taloyhtiöille, joihin viittaan opinnäytetyössäni kiinteistöinä. Työssä mainitsemani kiinteistöt ja taloyhtiöt koostuvat useista rakennuksista. LanWorld tarjoaa yhteyksiä ADSL (Asymmetric Digital Subscriber Line)-, Ethernet- ja HomePNA-tekniikoilla (Home Phoneline Networking Alliance). Näistä HomePNA:ta ei käsitellä opinnäytetyössäni lainkaan, sillä kyseinen yhteystyyppi on vanhentunut, eikä uusia HomePNA kohteita ole näillä näkymin tulossa. Ethernetin ja ADSL:n lisäksi käsittelen opinnäytetyössäni myös Point-to-Point -protokollaa (PPP) ja sen käyttöä ATM (Asynchronous Transfer Mode)- ja Ethernet-verkkojen yli (PPPoA ja PPPoE). PPPoE (Point-to-Point Protocol over Ethernet) ja PPPoA (Point-to-Point Protocol over ATM) ovat tärkeä osa opinnäytetyötäni, sillä LanWorld Finland Oy:n käyttämät runko-operaattorit siirtyvät ratkaisuissaan PPPoA:sta PPPoE:hen. Opinnäytetyöni on siis Case-tutkimus LanWorld Finland Oy:n verkkoratkaisuista.

Aiheen kehittely lähti liikkeelle, kun kuulin, että LanWorldin runko-operaattorit olivat siirtymässä verkoissaan PPPoA:sta PPPoE-pohjaisiin ratkaisuihin. Mietimme yhdessä LanWorldin silloisen teknologiajohtajan kanssa, olisiko muutoksessa tarpeeksi sisältöä opinnäytetyötäni varten. Tulimme siihen tulokseen, että aihe on riittävä ja opinnäytetyö kannattaisi tehdä. Myöhemmin LanWorldilta toivottiin, että käsittelisin myös Ethernet- ja ATM-verkkojen perusteita ja yrittäisin tuoda uutta näkökulmaa yrityksen käyttämiin verkkoratkaisuihin.

Opinnäytetyöni alkaa OSI-mallin (Open Systems interconnection Reference Model) perusteiden esittelyllä, sillä teleoperaattorilta vaaditaan hyvää perusosaamista useasta eri tekniikasta, ja OSI-malli voidaan nähdä tärkeänä perustana monen muun verkkotekniikan, mutta myös vianmäärityksen ymmärtämiselle. Tämä on tärkeää myös siksi, että taloyhtiöiden kohdalla vaaditaan kykyä nopeaan vianmääritykseen ja -ratkaisuun, sillä vian ilmetessä se vaikuttaa usein koko taloyhtiön käyttäjiin. Omissa kehitysehdotuksissani olen pyrkinyt keskittymään ratkaisuihin, joiden avulla verkkojen vianmääritystä ja korjausta voitaisiin kehittää entisestään.

OSI-mallin käsittelyn jälkeen siirryn käsittelemään Ethernet- ja ATM-tekniikoiden perusteita, koska nämä ovat LanWorldilla runsaassa käytössä. Tämän jälkeen käsittelen Point-to-Point -prokollaa yleisesti, ja tutkin PPPoA:n ja PPPoE:n välisiä eroja. Lopuksi keskityn OSI-mallin käyttöön vianmäärityksessä sekä LanWorldin nykyisten verkkoratkaisuiden ja niissä esiintyneiden ongelmien kuvaamiseen. Tarkoituksenani on edelleen käsitellä edellä mainittuja protokollia LanWorldin näkökulmasta. Pyrin erityisesti tuomaan esiin uusia näkökantoja siihen, miten esiin tulleista ongelmista voitaisiin päästä eroon.

2 OSI-MALLI

OSI-malli (Open Systems Interconnection) kehiteltiin 1980-luvun alussa ISO:n (International organization for Standardization) toimesta. Tarkoituksena oli tuolloin kehittää tekniikka, joka korjaisi eri verkkotekniikoiden keskinäiset yhteensopivuusongelmat. Näin ei kuitenkaan käynyt, sillä kehitetyt standardit olivat raskaita ymmärtää ja toteuttaa. OSI-mallin sijasta TCP/IP-protokollapino saavutti suurempaa suosiota. Anttilan mukaan OSI-malli on kuitenkin tärkeä niin sanottu referenssipino, jonka kerroksiin perustuva perusajatus on sama kaikissa protokollissa. (Granlund 2003, 9-10; Anttila 2000, 31.)

Edellä mainitusta syystä johtuen tulen opinnäytetyöni edetessä vertaamaan eri protokollia ja laitteita, sekä niiden toimivuutta juuri OSI-mallin eri kerroksilla. Käsittelen OSI-mallin käyttöä vianmäärityksessä osiossa 6.

OSI-malli on seitsemästä erilaisesta kerroksesta koostuva kerrosarkkitehtuuri. Kerrosten toimintaperiaate on Kai Granlundin mukaan sellainen, että jokainen kerros n tuottaa palveluja kerrokselle n+1 samalla, kun se käyttää hyväksi kerroksen n-1 antamia palveluja. Kerrosmallin avulla jokainen kerros voidaan toteuttaa itsenäisenä kokonaisuutena, joka puolestaan helpottaa toiminnan ymmärtämistä ja suunnittelua, sekä nopeuttaa uusien toteutuksien kehitystyötä. (Granlund 2003, 8-9.) Seuraavassa kuvassa (kuva 1) on esitelty OSI-mallin seitsemän kerrosta.

Kuva 1: OSI-Malli (Gralund 2003, 9)

Kuten kuvasta 1 voidaan huomata, OSI-mallia luetaan yleensä alhaalta ylöspäin. Alimpana on fyysinen kerros ja päällimmäisenä sovelluskerros. Seuraavaksi käsittelen lyhyesti OSI-mallin eri kerrokset ja niiden tehtävät.

1) Fyysinen kerros
Fyysisellä kerroksella määritellään eri verkkotekniikoille kuuluvia tiedon välitykseen liittyviä asioita, kuten esimerkiksi liittimien tyypit ja käytettävät koodaustavat. Granlundin mukaan fyysisen kerroksen toimintaa kuvataan useassa eri suosituksessa, ja tunnetuimpia fyysisen kerroksen suosituksia ovat esimerkiksi tietokoneen COM-porttia määrittelevät suositukset V.24 ja V.28. (Granlund 2003, 9; Anttila 2000, 34.)

2) Siirtoyhteyskerros
Siirtoyhteyskerroksen tehtävänä on varmistaa yhteyden virheettömyys kahden pisteen välillä. Kerros rakentaa kehyksen, jonka sisälle pakataan verkkokerrokselta saatu data jo aiemmin mainitun, Granlundin esittämän, periaatteen mukaan. OSI-mallin jokainen kerros tuottaa siis seuraavalle kerrokselle palveluita käyttäen hyväkseen edelliseltä kerrokselta saamiaan palveluita. Siirtoyhteyskerroksella kehyksiin lisätään myös otsikot, joihin kuuluu muun muassa lähettäjän ja vastaanottajan siirtoyhteyskerrosten osoitteet. Siirtoyhteyskerros ja fyysinen kerros ovat hyvin riippuvaisia toisistaan. (Granlund 2003, 9; Anttila 2000, 34.)

3) Verkkokerros
Verkkokerroksella hoidetaan varsinainen reititys. Tämä tarkoittaa sitä, että verkkokerroksella kuljetuskerrokselta saatu data pakataan verkkoon mahtuviin paketteihin ja välitetään vastaanottajalle tämän verkkokerroksen osoitteen perusteella. Granlundin mukaan reititys on tyypillisesti riippumatonta alempien kerrosten tekniikoista. Dataa voidaan reitittää joko saman lähiverkon sisällä tai reitittimen kautta verkosta toiseen. Esimerkkinä verkkokerroksella toimivista protokollista voidaan mainita IP (Internet Protocol). (Granlund 2003, 9, Anttila 2000, 34.)

4) Kuljetuskerros
Kuljetuskerros tarjoaa luotettavan ja virheettömän yhteyden kahden pisteen välille. Lisäksi kuljetuskerroksella pilkotaan ylemmiltä kerroksilta saatu data sopivan kokoisiksi palasiksi, eli segmentteihin, ja toimitetaan eteenpäin. Kuljetuskerroksella on kaksi lähetystapaa: yhteydellinen ja yhteydetön. Yhteydellisessä lähetyksessä varmistetaan ensin yhteyden muodostus ja data lähetetään tämän jälkeen. Sen sijaan yhteydettömässä lähetyksessä data lähetetään eteenpäin ilman yhteyden muodostumisen varmistusta ja toivotaan, että tieto saapuu perille ilman ongelmia. Kuljetuskerroksella toimivia protokollia ovat esimerkiksi TCP (Transmission Protocol) ja UDP (User Datagram Protocol). (Granlund 2003, 9; Anttila 2000, 34.)

5) Yhteysjaksokerros
Grandlundin (2003, 9) mukaan yhteysjaksokerroksen tehtävänä on koordinoida sovellusten välisiä toimintoja. Esimerkkeinä Granlund mt., 9) mainitsee yhteyden muodostamisen, lähetyksen käynnistämisen ja pysäyttämisen sekä yhteyden päättämisen ja resurssien vapautuksen. Tämä kerros huolehtii myös datan välittämisestä oikeassa järjestyksessä. Anttila (2000, 33) lisää, että yhteysjaksokerroksesta käytetään myös nimitystä istuntokerros.

6) Esitystapakerros
Tällä kerroksella sovitaan päätelaitteiden välisestä yhteisestä tiedonesitystavasta. Erilaisia esitystapamäärityksiä ovat Anttilan mukaan ainakin JPEG-kuvakoodaus ja ASCII-merkistö. Anttila toteaa lisäksi, että esitystapakerroksen tehtäviin kuuluu tulkkina oleminen esimerkiksi käännettäessä ASCII-merkistöön perustuvaa tietoa ISO-8859-1 merkistöä käyttäväksi. (Anttila 2000, 33.)

7) Sovelluskerros
OSI-mallin päällimmäisenä kerroksena toimii sovelluskerros. Tämän kerroksen tehtävänä on tarjota verkkopalveluja eri sovelluksille. Sovelluskerros toimii siis rajapintana sovelluksien ja OSI-mallin välillä. Granlund antaa eri sovelluksista esimerkkeinä muun muassa tiedonsiirron, sähköpostin ja hakemistopalvelut. (Granlund 2003, 10)

OSI-mallin kerroksien esittämiseen on myös toinen versio, jota Anttila (2000, 32) kutsuu ryhmitetyksi versioksi. Ryhmitetty versio koostuu seitsemän sijaan kolmesta kerroksesta: ensimmäinen kerros on sovelluskerros, joka käsittää sovellus-, esitystapa - ja yhteysjaksokerrokset. Toisena kerroksena on kuljetuskerros, joka on samanlainen kuin aiemmin esitetyssä versiossa. Kolmas ja viimeinen kerros on fyysinen kerros, joka koostuu verkko-, siirtoyhteys- ja fyysisestä kerroksesta. (Anttila 2000, 33.)

3 ETHERNET

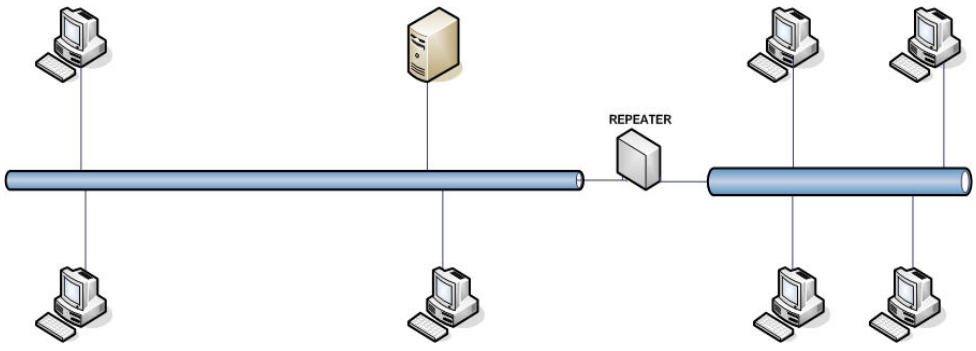
Tässä luvussa keskityn kuvaamaan Ethernetin perusteita. Ethernet on oleellinen osa LanWorld Finland Oy:n verkkoratkaisuja, mutta sen merkitys kasvaa jatkuvasti myös yleisesti ottaen. Käsittelen tässä osiossa lyhyesti Ethernetin taustaa ja kehittymistä. LanWorldin käyttämiä ethernetratkaisuja, niissä esiintyneitä ongelmia sekä parannusehdotuksia käsittelen tarkemmin osioissa 7 ja 8.

3.1 Ethernetin tausta ja sen kehittyminen

Ethernet on pakettikytkentäinen lähiverkkoratkaisu, jonka perusajatus kehitettiin jo 1960-luvun lopulla Hawajin yliopistolla ALOHA-nimisenä. Nykyään Ethernet on kiistatta käytetyin lähiverkkotekniikka. (Anttila 2000, 48.)

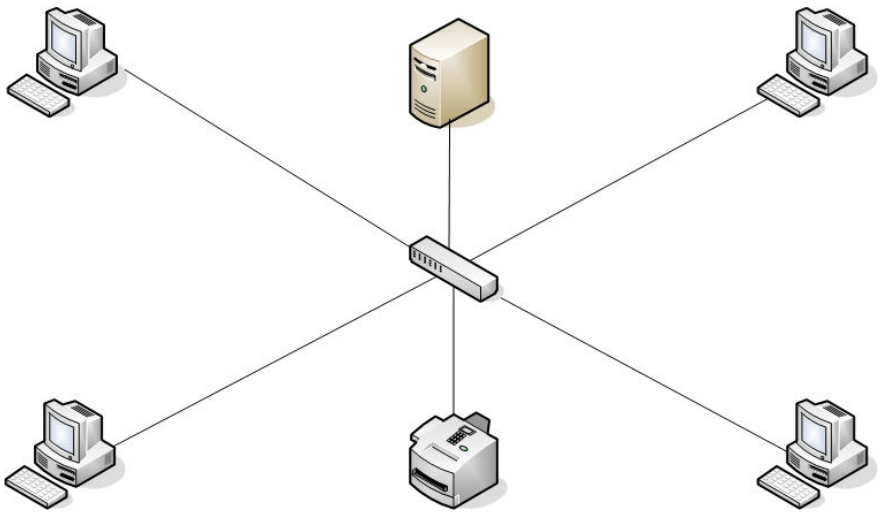
Ethernetverkot ovat yleistymässä myös LanWorldin tapauksessa: yhä useammin uusiin kiinteistöihin asennetaan rakennusvaiheessa sisäinen ethernetkaapelointi. Tämä tuo runsaasti mahdollisuuksia verkkojen toiminnallisuuden lisäämiseen.

Alun perin ethernetverkko oli topologialtaan väylämäinen (Bus topology). Tämä tarkoittaa sitä, että kaikki verkossa olevat laitteet olivat yhteydessä samaan kaapeliin. Jokainen laite tarvitsi yhteyttä varten oman erillisen lähetin-vastaanotin -yksikkönsä (transceiver). Pian kehitettiin digitaalinen vahvistin, toistin (repeater), jonka avulla yhden kaapelin liikenne pystyttiin toistamaan toiseen kaapeliin. Alun perin toistimia sai kytkeä peräkkäin vain kaksi kappaletta, mutta vuonna 1985 sallittiin neljän peräkkäisen toistimen käyttö, mikä mahdollisti viiden verkkosegmentin käytön. (Anttila 2000, 52; Jaakohuhta 2003, 62.) Alla oleva kuva (kuva 2) havainnollistaa väylätyyppistä Ethernet-topologiaa.



Kuva 2: Väylätyyppinen Ethernet-topologia

Väylätopologiaa korvaamaan kehitettiin tähtimäinen verkkotopologia (star topology). Tämä topologia koostuu keskellä olevasta keskittimestä, johon kaikki laitteet liittyvät omalla johdollaan. Tähtimäinen topologia on käytössä myös LanWorldin Ethernet-kohteissa, joita käsittelen hieman myöhemmin. Kuva 3 havainnollistaa tähtimäisen topologian rakennetta.



Kuva 3: Tähtimäinen verkkotopologia

Muista Ethernet-topologioista voidaan mainita myös Full Mesh -topologia, jossa kaikki verkon laitteet ovat yhteydessä suoraan toisiinsa omilla johdoilla. Seuraavaksi siirryn käsittelemään tarkemmin Ethernet-kehystä ja sen rakennetta.

3.2 Ethernet-kehys (Frame)

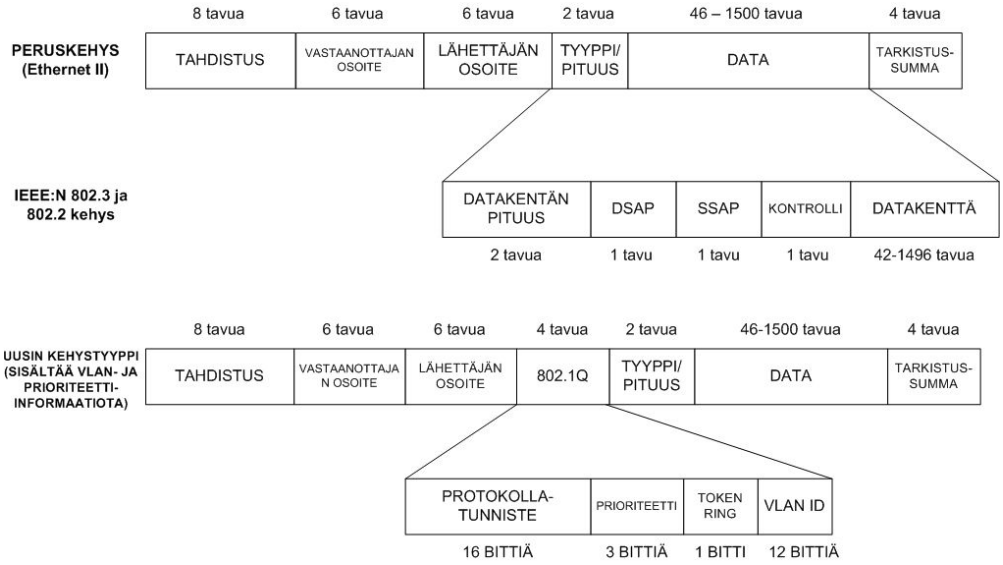
Ethernetverkossa kulkevia viestejä kutsutaan kehyksiksi (frames). Kehykset kulkevat OSI-mallin toisella kerroksella, eli siirtoyhteyskerroksella. Kehyksiä käytetään Ethernetin lisäksi kaikissa siirtoyhteyskerroksen mekanismeissa. (Anttila 2000, 50–51.)

Ethernetin peruskehys on nimeltään Ethernet II -kehys. Siitä on olemassa erilaisia muunnoksia, joissa on tuotu alkuperäiseen kehykseen lisää ominaisuuksia. Ethernet II -kehyksen maksimikoko on 1518 tavua, joista 18 tavua on otsikkokenttää ja 1500 tavua otsikoita ja dataa. Uuden 802.1Q-määrittelyn mukainen Ethernet-kehys on maksimikooltaan 1522 tavua ja sisältää uusina ominaisuuksina VLAN sekä prioriteetti-informaatiota. Näiden kahden kehystyypin välimuotona voidaan pitää IEEE:n 802.3 -määrittelyn mukaista kehystä. (Anttila 2000, 50–51.)

Ethernet-kehyksen minimikoko on puolestaan 64 tavua. Mikäli lähetettävän kehyksen koko on jäämässä alle tämän koon, otetaan käyttöön datakenttään

lisättävät täytetavut (padding). Tämän osion koko muokkautuu sen mukaan, kuinka paljon kehyksen koko jää alle 64 tavun. (Anttila, 2000, 51.)

Periaatteessa kehyksen koon kasvattaminen 1518 tavusta 1522 tavuun voi tuoda yhteensopivuusongelmia vanhojen laitteiden kanssa, mutta IEEE:n kehitystyöryhmä on katsonut mahdollisten haittojen olevan pienempiä kuin saavutettavan hyödyn. (Anttila 2000, 51–53.) Seuraavassa kuvassa (kuva 4) esitetään Ethernetin eri kehystyypit Anttilaan (2000, 51–53) tukeutuen:



Kuva 4: Ethernetin kehystyypit (Anttila 2000, 51)

Kuten kuvasta voi huomata, ovat eri kehystyypit perusosiltaan hyvin samankaltaisia. Kaikissa tyypeissä on samankokoiset tahdistus-, vastaanottajan osoite-, lähdeosoite- sekä tarkistussummaosat. Seuraavaksi käsittelen eri kehysten osat ja niiden tehtävät edelleen Anttilaan (2000, 51–53) perustaen.

1) Tahdistus (Preamble)
Tahdistusosa on kahdeksan tavun mittainen bittijono, jonka avulla vastaanottaja tietää, milloin itse kehys alkaa ja pystyy synkronoimaan vastaanottonsa lähettäjän kanssa. Tahdistusosaa ei lasketa itse kehyksen pituuteen.

2) Vastaanottajan osoite (Destination address)
Tämä kuuden tavun mittainen osa kertoo vastaanottajan osoitteen. Osoite voi olla joko yksilöllinen (unicast), ryhmälähetys (multicast) tai levitysviestiosoite (broadcast). Unicastia, multicastia ja broadcastia käsittelen tarkemmin luvussa 3.3.

3) Lähettäjän osoite (Source address)
Lähettäjän osoite on kuuden tavun mittainen kenttä, joka kertoo lähettäjän osoitteen. Lähettäjän osoite on aina yksilöllinen, yhden verkkokortin osoite. Ensimmäiset kolme tavua kertovat verkkokortin valmistajan: esimerkiksi 3Comin valmistaman verkkokortin ensimmäiset kolme tavua ovat ”00-20-

AF". Jaakohuhdan (2003, 60) mukaan valmistajakohtaiset tiedot annetaan valmistajille IEEE:n toimesta. Nämä tiedot pätevät lähettäjän osoitteen lisäksi myös vastaanottajan osoitteeseen.

4) Tyyppi / Pituus (Type / length)
Tämä kenttä on pituudeltaan kaksi tavua. Kenttä kertoo joko lähetettävän datan tyypin tai datakentän pituuden. Jos kyseessä on Ethernet II -tyypin kehys, kentällä voi olla esimerkiksi heksadesimaaliarvo 0800, joka kertoo kehyksen kuorman olevan IP-protokollaa. IEEE:n 802.3 -määrittelyn mukaisessa kehyksessä tämä tyyppi/pituuskenttä ilmoittaa kehyksen datakentän pituuden.

5) Data
Data-kenttä on 46–1500 tavun mittainen kenttä, joka sisältää kehyksen varsinaisen datan. Kuten jo aiemmin mainitsin, mikäli data-kentän koko jää alle 46 tavun, tarvittava koko saavutetaan käyttämällä täytetavuja (padding), jotka pitävät huolen siitä, että kehyksen yhteiskooksi saadaan tarvittavat 64 tavua. Jaakohuhdan (2003, 60) mukaan IEEE:n kehyksen data-kentässä on lisäksi IEEE 802.2 -määrittelyjen mukaisia ohjaustietoja, jotka on tarkoitettu pääsääntöisesti korvaamaan alkuperäisen kehyksen tyyppikenttätietoja.

6) Tarkistuskoodi (Frame Check Sum)
Tämä neljän tavun pituinen kenttä toimii tarkisteena viallisen kehyksen varalta. Kenttään muodostetaan lähettäjän puolella tarkistuskoodi, joka lasketaan vastaanottajan puolella uudelleen. Mikäli koodit täsmäävät, voidaan luottaa siihen, että kehys ei ole viallinen.

Nämä edellä kuvatut kentät löytyvät siis kaikista eri Ethernet-kehyksistä. Kuten aikaisemmin esitetystä kuvasta puolestaan huomataan, sisältävät uudemmat kehystyypit kenttiä, joita ei Ethernet II -kehyksestä löydy. Seuraavaksi esittelenkin nämä Ethernet II -kehykseen kuulumattomat kentät Anttilaan (2000, 54) perustuen.

Ensimmäinen kenttä on nimeltään VLAN-tagi, joka on jaettu kahteen osaan ja on neljän tavun mittainen, kuten kuvasta numero 4 voidaan huomata. Ensimmäiset kaksi tavua sisältävät protokollatunnisteen, jota käytetään nyt jo poistumassa olevassa Token Ring- ja FDDI-verkoissa. Jäljelle jääneistä kahdesta tavusta kolme bittiä käytetään prioriteetin ilmaisemiseen. Yhdellä bitillä ilmaistaan, että kyseessä on Ethernet-kehykseen kapseloitu Token Ring -kehys ja 12 bittiä käytetään VLANin tunnistamiseen.

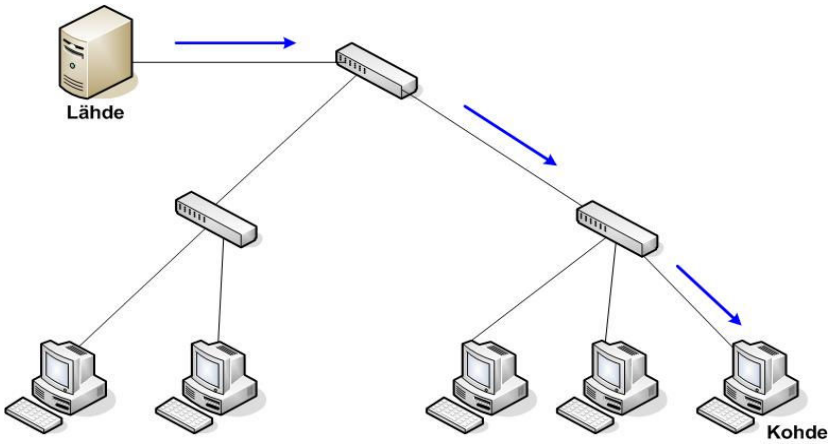
Toisena kenttänä esittelen ohjaustietoja sisältävät kentät. Nämä Ethernet-kehykseen liitetyt, yhteensä kolmen tavun mittaiset kentät, ovat IEEE:n määrittelemän LLC-ohjauskerroksen (Logical Link Control) osia. Käytännössä LLC määrittelee, mikä sovellus vastaanottaa dataa. LLC:hen liittyvät kentät ovat nimeltään DSAP (Destination Service Access Point, yksi tavu), SSAP (Source Service Access Point, yksi tavu) ja kontrolli (Control, yksi tavu).

3.3 Tiedon välittäminen

Kun Ethernet-kehyksen osat on määritelty, voidaan eritellä, kuinka kehyksiä välitetään. Jaakohuhdan (2003, 57) mukaan lähiverkkojen nopea kehittyminen on asettanut tiettyjä vaatimuksia tiedon siirtämiselle. Kuten jo aiemmin totesin, Ethernet-kehykset liikkuvat OSI-mallin toisella kerroksella. Ethernet kehyksiä lähetetään kolmella eri tavalla: unicast-, multicast- ja broadcast-kehyksinä. Jokaiselle lähetystavalle löytyy oma käyttötarkoituksensa sen mukaan, minkälaista dataa on tarkoitus lähettää ja kuinka monelle käyttäjälle. Seuraavaksi esittelen lyhyesti nämä lähetystavat Jaakohuhtaa mukaillen (2003, 57).

3.3.1 Unicast

Unicast-lähetysten kehyksillä on tietty lähde- ja kohdeosoite. Tätä osoitetta kutsutaan MAC-osoitteeksi. Jokaisella verkon aktiivilaitteella on uniikki MAC-osoite. Anttilan mukaan (2000, 32 ja 51) Suurin osa ethernetverkossa kulkevasta liikenteestä on unicast-liikennettä. Tämä liikenne kulkee ainoastaan lähettäjän (lähde) ja vastaanottajan (kohde) välillä.). Allaoleva kuva (kuva 5) havainnollistaa unicastin toimintaa.

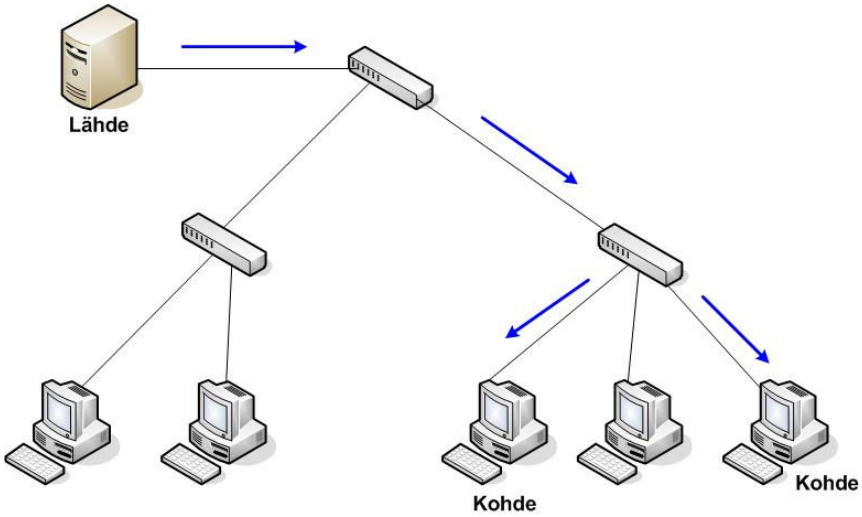


Kuva 5: Unicast

3.3.2 Multicast

Multicast-lähetyksessä lähetetään kehyksiä lähteestä joukolle vastaanottajia. Tätä kehystä käytetään, kun sama data halutaan lähettää kerralla usealle vastaanottajalle, kuten esimerkiksi videoneuvotteluissa tai työryhmäsovelluksissa. Tällaisissa tapauksissa on luonnollisesti järkevämpää lähettää tieto kaikille vastaanottajille samalla kertaa sen sijaan, että tieto lähetettäisiin jokaiselle käyttäjälle omana unicast-lähetyksenään. Anttilan (2000, 32 ja 51) mukaan myös seuraavat IP-reititysprotokollat käyttävät multicast-kehyksiä:

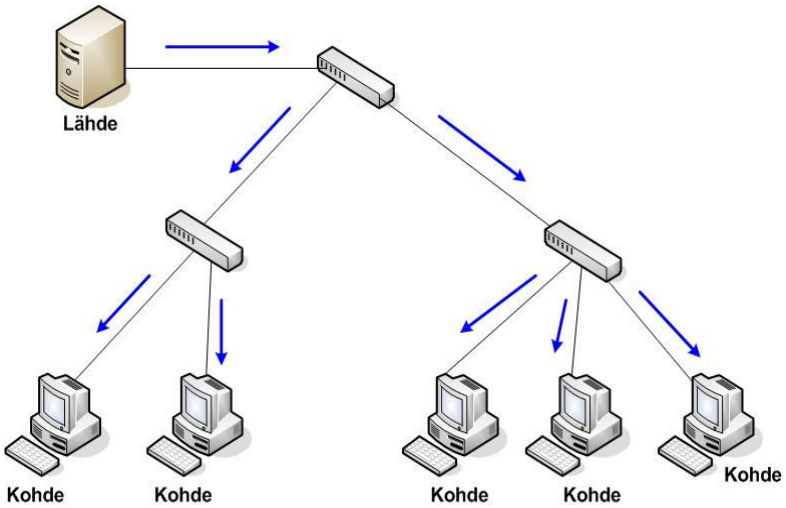
Routing Information Protocol (RIP) version 2, Open Shortest Path First (OSPF) ja Extended Interior Gateway Routing Protocol (EIGRP).). Allaoleva kuva (kuva 6) havainnollistaa multicastin toimintaa.



Kuva 6: Multicast

3.3.3 Broadcast

Broadcast-kehykset lähetetään kaikille vastaanottajille, jotka sijaitsevat samalla lähetysalueella (broadcast domain). Lähetyksen lähteenä voi toimia mikä tahansa verkon aktiivilaite (esim. yksittäinen työasema, verkkotulostin tai reititin). Allaoleva kuva (kuva 7) havainnollistaa broadcastin toimintaa.



Kuva 7: Broadcast

4 ATM (Asynchronous Transfer Mode)

Seuraavaksi käsittelen ATM:n perusteita. Keskityn ATM-solun rakenteeseen ja käsittelen ATM:n suhdetta ADSL-tekniikkaan, jota käytetään LanWorld Finland Oy:n verkoissa runsaasti. Sen lisäksi, että yritys tarjoaa käyttäjilleen ADSL-yhteyksiä, kaikkien kiinteistöjen verkot liitetään runko-operaattorin verkkoon ADSL-yhteydellä. Käsittelen LanWorldin ADSL-ratkaisuja ja niiden ongelmia sekä parannusehdotuksia tarkemmin osioissa 9 ja 10.

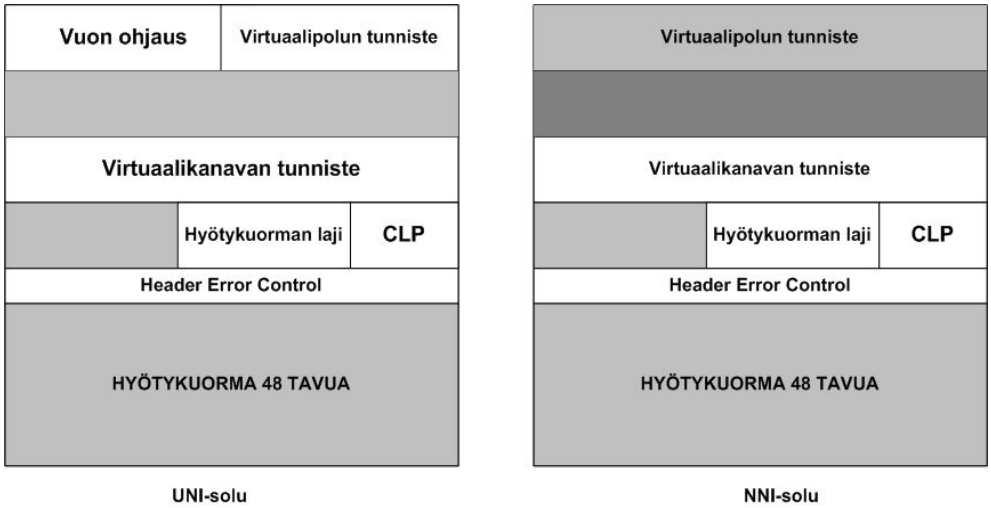
4.1 Yleistä ATM:stä

ATM (Asynchronous Transfer Mode) on asynkroninen verkkotekniikka, joka kehitettiin alun perin B-ISDN-tekniikan toteuttamiseksi. Asynkronisuus ATM:n tapauksessa tarkoittaa sitä, että tietovirrassa kulkevan sanoman sijainnilla ei ole mitään tekemistä reitin tai määränpään kanssa. Kukin sanoma varustetaan ohjaustiedoilla, jotka sisältävät tiedot reitistä ja määränpäästä. ATM on täten suunniteltu säilyttämään eri liikennetyyppien palvelutaso yhden verkon yli tapahtuvan siirron aikana. ATM-yhteys pystyy yhdistämään esimerkiksi puhe-, video- ja dataliikenteen käyttäjäpäässä olevalla laitteella (CPE, Customer Premises Equipment) ja jakamaan sen soluiksi, joita ATM-yhteyksissä käytetään Ethernetin kehyksien sijaan. Nämä solut ovat aina samankokoisia (53 tavua). Kiinteämittainen solurakenne yksinkertaistaa sisään- ja ulospäin menevän liikenteen järjestelemistä jonoihin. Lisäksi verkon toiminnan ennustettavuus paranee huomattavasti, kun verkon kuormitus ei riipu enää eri tapahtumien pituudesta, vaan niiden lukumäärästä. (Granlund 2003, 389–390; Anttila 2000, 76 -77.)

4.2 ATM-Solu

ATM toimii OSI-mallin siirtoyhteyskerroksella kuten Ethernetkin. ATM jakautuu kuitenkin ATM-kerrokseen ja ATM-sovituskerrokseen. Näitä sovituskerroksia on määritelty neljä kappaletta, jotka ovat AAL1, AAL2, AAL3/4 ja AAL5. Lyhenne AAL tulee sanoista ATM Adaptation Layer. Sovituskerroksen tehtävänä on ottaa sovellukselta saatu data ja pilkkoa se 48 tavun palasiin, jotka voidaan välittää ATM-kerrokselle, jossa soluihin lisätään viiden tavun mittainen otsikkokenttä, ja ne siirretään edelleen fyysiselle kerrokselle. 48 tavun hyötykuormalla ja viiden tavun otsikolla koostetaan siis ATM-solun koko, joka on jo aiemmin mainitsemallani tavalla 53 tavua. ATM-solun koko ei ole digitaalitekniikan kannalta paras ratkaisu. Solun koko on kompromissi Yhdysvaltojen ja ITU:n ehdotuksien välillä. ATM-kerros käsittelee kahdenlaisia soluja: UNI (User Network Interface) ja NNI (Network Node Interface). Solujen rakenne Granlundin mukaan esite-

tään seuraavassa kuvassa (kuva 8). (Granlund 2003, 389–390; Anttila 2000, 76–77.)



Kuva 8: UNI- ja NNI-solujen rakenne (Granlund 2003, 390)

UNI-solua käytetään laitteiden, kuten tietokoneiden tai reitittimien liittämisessä ATM-verkkoon. NNI-solu puolestaan vastaa ATM-solmujen välisestä liikenteestä. Kuten kuvasta 8 voidaan huomata, solujen suurin keskinäinen ero on otsikoiden alussa. UNI-solun otsikkoon kuuluu neljä bittiä, jotka on omistettu vuon ohjaukselle. NNI-solun otsikossa nämä neljä bittiä käytetään virtuaalipolun tunnisteen jatkamiseen. (Granlund 2003, 389–390; Anttila 2000, 76-77.) Seuraavaksi käsittelen lyhyesti ATM-solujen eri osat.

1) Vuon ohjaus (Generic Flow Control)
Vuon ohjaus on neljän bitin tietue, joka esiintyy, kuten aiemmin mainitsin, ainoastaan UNI-soluissa. Nimensä mukaan vuon ohjauksen tehtävänä on hallita ATM-verkon ja paikallislaitteen (CPE) välistä vuota paikallisesti. Tämän kentän sisältöä ei siis käytetä verkon sisäisessä liikenteessä. (Granlund 2003, 389–390; Anttila 2000, 76–77.)

2) Virtuaalisen polun tunniste (VPI)
VPI on reitityksessä tarvittava tieto. UNI-solussa VPI:lle on varattu kahdeksan bittiä, kun taas NNI-solun vastaava koko on 12 bittiä. (Granlund 2003, 389–390; Anttila 2000, 76–77.)

3) Virtuaalikanavan tunniste (VCI)
VCI:tä käytetään loogisen yhteyden tunnistamiseen yhteyden kummassakin päässä (Anttila 2000, 76–77). VPI- ja VCI arvot ovat tuttu käsite monelle ADSL-yhteyden käyttäjälle, sillä nämä arvot saattavat poiketa toisistaan eri ADSL-operaattoreiden yhteyksissä, ja mikäli arvot ovat väärin, ei yhteys luonnollisestikaan toimi. Itse törmäsin vääriin VPI/VCI- arvoihin säännöllisesti toimiessani tietoliikenneasentajana.

4) Hyötykuorman laji

Hyötykuorman laji kertoo solun varsinaisen hyötykuorman sisällön. Tämä osa koostuu kolmesta bitistä, jotka voivat ilmaista, onko kyseessä käyttäjä- vai kontrollisolu. Kolmas vaihtoehto tälle osalle on ilmaista ruuhkaa. Tämä osa voi muuttaa arvoaan lähetysvaiheessa. Granlundin mukaan solu voi lähteä lähettäjältä arvolla, joka kertoo verkon olevan ruuhkaton, mutta kun vastaanottaja saa solun, voi se ilmoittaa, että verkko on ruuhkautunut lähetyksen aikana. (Granlund 2003, 389–390; Anttila 2000, 76–77.)

5) Hävikkiprioriteetti (CLP)
CLP kertoo verkolle, miten solun kohdalla tulee toimia ruuhkatilanteissa. Osio on yhden bitin kokoinen ja sen arvoiksi voidaan luonnollisesti asettaa 0 tai 1. Mikäli CLP on 1, kertoo se vastaanottajalle, että solun saa ruuhkatilanteessa tiputtaa pois ennen soluja, joiden CLP on 0, jotta ruuhkatilannetta voitaisiin helpottaa. (Granlund 2003, 389–390; Anttila 2000, 76–77.)

6) Otsikon tarkistusluku (Header Error Control)
Lähettävä osapuoli laskee sanoman otsikolle tarkistusluvun, ennen kuin solu lähetettään verkkoon. Tämä tarkistusluku on nimeltään Header Error Control eli HEC. Luku lasketaan käyttämällä CRC-menetelmää otsikon neljästä ensimmäisestä tavusta. Tätä kenttää käytetään solujen rajojen havaitsemiseen. (Granlund 2003,392; Anttila 2000, 78.)

4.3 ATM-verkon toiminta

ATM-verkon soluvirtoja käsitellään palveluluokkien avulla. Näitä luokkia voidaan käyttää eri sovellusten kanssa, joiden mukaan luokat on jaettu. Seuraavaksi käsittelen eri luokat lyhyesti Granlundin ja Anttilan teoksiin pohjautuen.

1) Constant Bit Rate (CBR)
CBR on palvelu joka toimii kiinteällä nopeudella siirtäen tietoa kahden pisteen välillä. CBR:ää voidaan käyttää esimerkiksi tilanteessa, jossa tarkoituksena on emuloida piirikytkentäistä (Circuit Switched) verkkoa. Yleisiä sovelluksia ovat esimerkiksi reaaliaikaisen videon tai audion siirto. (Granlund 2003, 397; Anttila 2000, 78.)

2) Real Time – Variable Bit Rate (RT-VBR)
RT-VBR muistuttaa osittain CBR:ää, sillä kuten CBR myös RT-VBR on yleisesti käytössä reaaliaikaisen kuvan ja äänen siirrossa. Verkko ohjaa solujen keskimääräistä saapumisaikaa, joka ehkäisee kuvaan tai puheeseen mahdollisesti muodostuvaa huojuntaa. CBR-palveluun verrattuna RT-VBR sallii tiedon purskeittaisen siirron, jota voidaan tasata puskuroimalla dataa. (Granlund 2003, 397; Anttila 2000, 79.)

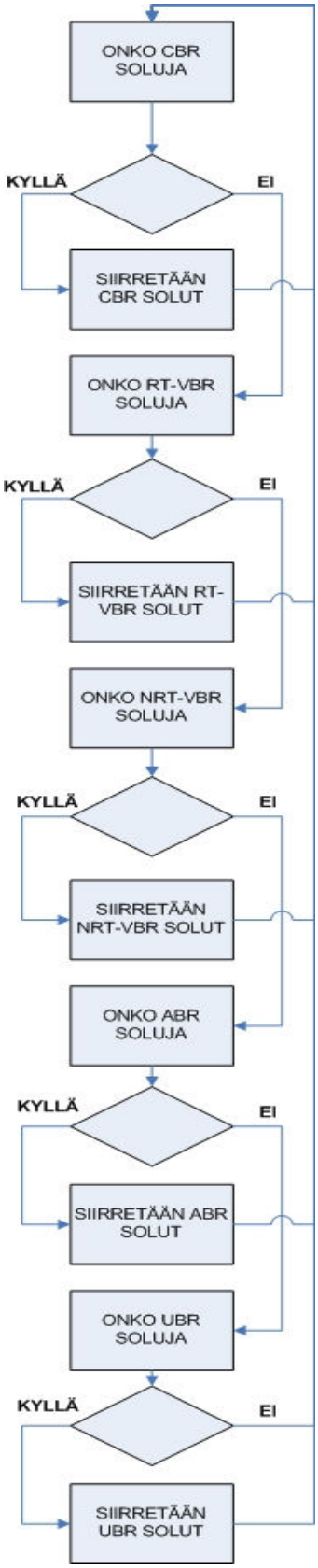
3) Non-Real Time – Variable Bit Rate (NRT-VBR)

Tämä palvelu on tarkoitettu reaaliaikaisille sovelluksille, joissa tiedon saapumistapa ei vaikuta sen laatuun, mutta tiedolle on tästä huolimatta taattava tietty kaista tai latenssi. Toisin kuin CBR tai RT-VBR, NRT-VBR ei siis sovellu videon tai audion reaaliaikaiseen siirtoon kahden pisteen välillä. (Granlund 2003, 397; Anttila 2000, 79.)

4) Available Bit Rate (ABR)
ABR on palvelu, joka takaa verkolle tietyn minimisiirtotason. Tämä taso on mahdollista ylittää, mutta käyttäjän tulisi olla tietoinen siitä, että mikäli siirtotaso ylitetään ja verkko ruuhkautuu, tason ylittäneet solut saatetaan hylätä. ABR on tarkoitettu purskeiseen tiedonsiirtoon. (Granlund 2003, 397; Anttila 2000, 79.)

5) Unspecified Bit Rate (UBR)
UBR on palvelu, jossa mitään ei luvata eikä taata. Lähetettäville soluille ei siis ole luvattu minkäänlaista kaistanleveyttä tai maksimilatenssia. UBR on suosittu lähi- ja laajaverkkoympäristöissä, joissa sitä käytetään esimerkiksi tiedostojen siirtoon ja sähköpostin lähetykseen. (Granlund 2003, 397; Anttila 2000, 79.)

Seuraava kuva (kuva 9) esittää eri palveluluokkien keskinäiset prioriteetit Granlundia (2003, 397) mukaillen. Kuvasta 9 voidaan huomata, kuinka CBR on prioriteetiltaan selkeästi suurin kun taas UBR-soluja siirretään silloin, kun muuta liikennettä ei ole siirrettäväksi.



Kuva 9: Palveluluokkien keskinäiset prioriteetit

4.3.1 Palvelun laatu

Palvelun laadulla tarkoitetaan käyttäjän ja palveluntarjoajan välistä sopimusta, jossa määritetään joukko ehtoja, joihin palveluntarjoaja sitoutuu. Palvelun laatu tunnetaan myös nimellä Quality of Service (QoS). (Granlund 2003, 398.) Ehdoissa määritellään palvelun enimmäis- ja vähimmäistason vaatimukset muun muassa seuraavassa lueteltavien ominaisuuksien osalta:

1) Peak Cell Rate (PCR)
PCR määrittelee suurimman nopeuden, jolla ATM-yhteyttä tullaan käyttämään. Mittayksikkönä käytetään "siirretyt solut per aika-yksikkö". (Granlund 2003, 398.)

2) Sustained Cell Rate (SCR)
SCR määrittää käyttäjän keskimääräisen siirtonopeuden soluina per aikayksikkö (Granlund 2003, 398).

3) Minimum Cell Rate (MCR)
MCR merkitsee solujen vähimmäismäärää, jonka verkko pystyy välittämään per aikayksikkö (Granlund 2003, 398).

4) Cell Variation Delay Tolerance (CVDT)
CVDT määrittelee solujen saapumisajan hajonnan (Granlund 2003, 398).

5) Cell Loss Ratio (CLR)
CLR määrittää kuinka monta solua hukataan tai kuinka moni solu myöhästyy annetuista rajoista suhteessa kaikkiin soluihin. (Granlund 2003, 398).

6) Cell Transfer Delay (CTD)
CTD määrittää, kuinka kauan solu keskimäärin viipyy matkalla lähettäjältä vastaanottajalle (Granlund 2003, 398).

4.3.2 Ruuhkan hallinta

ATM-verkossa liikkuu suuria määriä soluja, joita välitetään vastaanottajille. Välitystä ohjaavat aiemmin esitellyt palveluluokat ja sovitut palvelulajit. Kun verkossa syntyy tilanne, jossa verkko ei pysty täyttämään sille asetettuja laatuvaatimuksia, syntyy ruuhka. Verkon ruuhka voidaan jakaa kahteen kategoriaan: lyhytaikaiseen ja pitkäaikaiseen ruuhkaan. Lyhytaikainen ruuhka on yleensä tilapäisen kuormitushuipun aikaansaama, kun taas pitkäaikainen ruuhka johtuu usein väärin suunnitellusta, ja mitoitetusta, verkosta. (Granlund 2003, 399.)

ATM-verkon liikenteen- ja ruuhkanhallinnan kohteita luetellaan kansainvälisen televiestintäliiton ITU-T:n suosituksessa I.271. Suosituksen mukaan ATM-verkon pitää tukea sellaisia palveluita, jotka ovat sopusoinnussa verkon suorituskyvyn kanssa. Ruuhkanhallinnan ei pidä perustua ATM-

sovitus- tai sovellustason ratkaisuihin. Lisäksi Ruuhkanhallinnan tulee minimoida verkon ja sovellusten monimutkaisuutta ja maksimoida verkon suorituskykyä. (Granlund 2003, 399.)

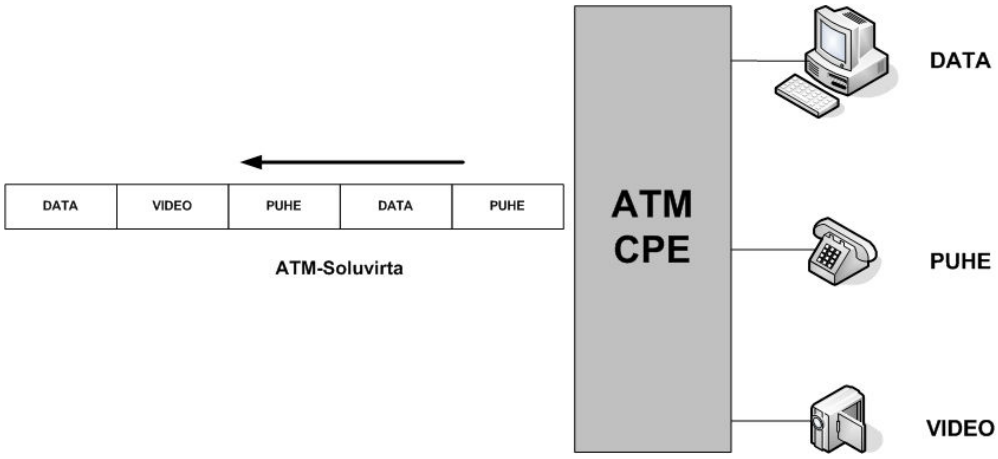
Granlundin (2003, 399) mukaan näiden tavoitteiden saavuttamiseksi voidaan toimia neljällä tasolla: Ensimmäisellä tasolla valvotaan, kuinka monta solua lähetetään per aikayksikkö. Tämä edustaa valvonnan alinta tasoa ja sen vaikutukset voidaan nähdä verkon suorituskyvyssä välittömästi. Toisella tasolla toimitetaan solun verkkoon lähettäneelle osapuolelle palautetta lähetetystä solusta. Tämä mahdollistaa solun siirtoajan valvomisen. Kolmanneksi varmistetaan, että verkko täyttää vaaditut palvelutasot ennen yhteyden avaamista. Neljäntenä tasona seurataan verkon kuormitusta pitkällä aikavälillä.

Varsinaisen ATM-verkon ruuhkanhallinnan Granlund (2003, 399–400) jakaa puolestaan kolmeen osaan: ensimmäiseksi uuden käyttäjän pääsy verkkoon tulee estää, mikäli käyttäjän vaatima palvelu johtaisi verkon ruuhkautumiseen. Toiseksi verkon resurssit tulee varata etukäteen ottaen huomioon eri käyttäjien vaatimat tarpeet. Resurssit varataan yhteyden muodostuksen aikana. Täten kaikki verkossa olevat kytkimet joutuvat noteeraamaan varatun kapasiteetin suuruuden ennen yhteyden muodostamista. Kolmantena osana Granlund mainitsee verkon ruuhkanhallinnan käytön aikana. Granlund perustelee väitettään ATM-Foorumin hyväksymällä ratkaisulla ABR-palvelun ruuhkanhallinnassa, jossa lähettäjä lähettää erityisen RM-solun (Resource Management) aina tietyn sanoman jälkeen. Vastaanottaja kopioi edellisen solun PT-kentän keskimmäisen bitin viestiin ja palauttaa viestin lähettäjälle. Tämä bitti asetetaan soluun silloin kun ohitetaan ruuhkainen paikka, joten tieto ruuhkasta palautuu alkuperäiselle lähettäjälle RM-solun mukana. (Granlund 2003, 399-400.)

Granlundin (2003, 400) mukaan ruuhkan purkamiseen on eri tapoja. Karkein tapa on poistaa ylimääräiset solut verkosta. Ylimääräiset solut tunnistetaan aiemmin esitetyllä tavalla, jossa solun CLP-bitti on yksi. CLP-bitin ollessa yksi, tiedetään, että kyseinen solu ylittää sille luvatun palvelutason ja se voidaan poistaa ruuhkatilanteen helpottamiseksi.

4.4 ATM ja ADSL

ATM:ää käytetään useimpien ADSL-toteutusten kehystystapana datan, videon ja puheen osalta. ATM on suunniteltu säilyttämään liikennetyyppien palvelutaso linkin yli tapahtuvan siirron aikana. Tämä tapahtuu segmentoimalla data jo aiemmin esitellyllä tavalla 53 tavun soluihin, joille voidaan määrittää eri palvelutasoja. Esimerkkinä korkean palvelutason vaativasta liikenteestä voidaan ottaa puhe, joka ei siedä korkeita latensseja. ATM:n avulla puheliikenne voidaan paketoida ja siirtää jonoon muiden pakettien kanssa. Puhepaketit lähetetään kuitenkin ennen muuta dataa, jolla on matalampi palvelutaso. Tällöin varmistetaan puheliikenteelle sen tarvitsema osa yhteydestä. (Ginsburg 2000, 54.) Alla oleva kuva (kuva 10) selventää datatyyppien muunnosta ATM-soluiksi Ginsburgin (2000, 54) esittämällä tavalla.



Kuva 10: Datatyyppien muunnos (Ginsburg 2000, 54)

Kuvasta 10 voidaan huomata, kuinka asiakkaan CPE (Customer Premises Equipment) kerää asiakkaan itsensä lähettämät tiedot, ja paketoi ne soluihin. ADSL-yhteyden ollessa kyseessä CPE:llä tarkoitetaan ADSL-reititintä. Nämä solut voidaan lähettää ulkomaailmaan siinä järjestyksessä kuin niiden palvelutason korkeus vaatii. Kuvan 10 esittämässä tapauksessa video- ja puheliikenne lähetettäisiin ennen muuta dataa.

5 PPP (Point-to-Point Protocol)

Seuraavaksi käsittelen Point-to-Point protokollaa (PPP). PPP yhdistää LanWorld Finland Oy:n verkkoratkaisuissa verkotetun taloyhtiön runko-operaattorin verkkoon. Ilman tätä yhteyttä taloyhtiöiden verkot eivät olisi lainkaan yhteydessä Internetiin. Käsittelen tässä luvussa lyhyesti PPP:n perusteita, jonka lisäksi käyn läpi PPPoA:n ja PPPoE:n perusteita ja keskinäisiä eroja. Nämä ovat sikäli tärkeitä asioita, että LanWorldin runko-operaattorit siirtyvät yhteyksissään PPPoA:sta PPPoE:tä tukeviin ratkaisuihin, joten on hyvä tietää, minkälaisia muutoksia voidaan odottaa. Pääasiallisena lähteenäni PPP-osiossa olen käyttänyt Internet Engineering Task Forcen (IETF) RFC-määrittelyjä.

5.1 Yleistä

Granlundin (2003, 205) mukaan Point-to-Point Protocol on "kahden osapuolen väliselle tietoliikenteelle tarkoitettu yksinkertainen protokolla, joka tarjoaa yhteyden osapuolille kaksisuuntaisen (full duplex) tietovuon". PPP toimii OSI-mallin toisella kerroksella, ja se tukee sekä synkronisia, että asynkronisia yhteyksiä. PPP on tärkeä osa opinnäytetyötäni, sillä työn idea lähti liikkeelle Elisan runkoverkon muutoksesta, joka aiheuttaa LanWorldin kiinteistöverkkojen runkoyhteyksien siirtymisen PPPoA:sta PPPoE:ksi.

PPP-yhteys koostuu kahdesta osasta: tiedon kapseloinnista (Encapsulation), ja yhteyden muodostamisesta. Nämä kaksi osiota mahdollistavat yhdessä PPP-yhteyden muodostumisen ja tiedon lähettämisen. Seuraavaksi käsittelen näitä osia tarkemmin.

5.2 Kapselointi

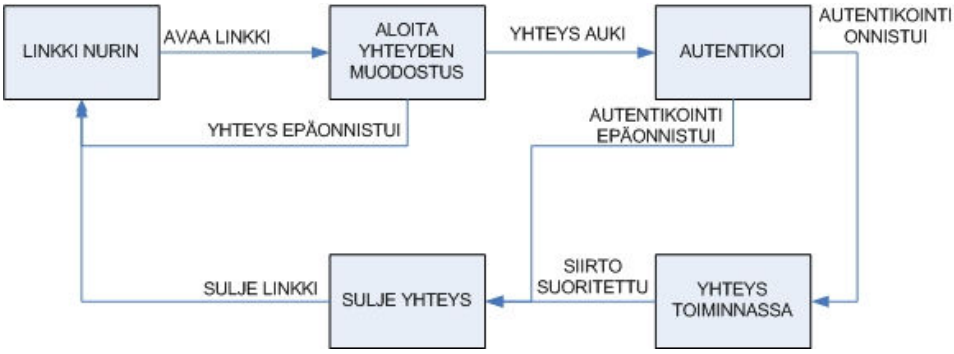
Kapselointi koostuu kolmesta kentästä: protokolla-, informaatio- ja täytekentistä. Prokolla-kenttä on pituudeltaan yhden tai kaksi oktettia. Tätä kenttää käytetään ohjaamaan informaatiokenttään kapseloitua informaatiota oikealle PPP-protokollalle. Informaatiokenttä sisältää PPP-sanoman varsinaisen hyötykuorman. Kentän suurin mahdollinen koko on 1500 tavua, jolloin koko sanoman maksimikooksi saadaan 1502 tavua (informaatiokenttä + protokollakenttä). (Granlund 2003, 205.)

Täytekenttää käytetään silloin, kun halutaan saavuttaa PPP-sanoman suurin koko (MRU, Maximum Receive Unit) tilanteessa, jossa informaatiokentän koko jäisi muuten alle 1500 tavun. Alla oleva kuva (kuva 11) selventää PPP-sanoman kapseloinnin osien järjestystä. (IETF 1994, rfc1661.)

Kuva 11: PPP-sanoma (IETF 1994, RFC 1661)

5.3 Yhteyden muodostaminen

LCP (Link Control Protocol) on PPP:n sisäinen menetelmä, jonka tehtävänä on muodostaa varsinainen PPP-yhteys kahden verkkolaitteen välille. Tämän lisäksi LCP poistaa mahdollisia silmukoita, eli yhteyksiä, jotka kiertävät loputtomiin. Silmukat voivat olla tulosta esimerkiksi huonosta verkonsuunnittelusta. Lisäksi LCP:n tehtäviin kuuluvat kapseloinnin asetusten automaattinen tarkistus, pakettien kokojen vaihtelun seuranta sekä linkin sulkeminen siirron jälkeen. Seuraava kuva (kuva 12) kuvaa PPP-yhteyden muodostumisen eri vaiheita RFC1661:n mukaan (IETF 1994, rfc1661). Käsittelen nämä vaiheet tarkemmin seuraavaksi.



Kuva 12: PPP-yhteyden muodostus (IETF 1994, rfc1661)

Kuten kuvasta 12 voidaan huomata, PPP-yhteyden muodostaminen alkaa ja loppuu aina tilaan, jossa laitteiden välinen linkki on nurin. Yhteyden muodostaminen aloitetaan siten, että yhteyden molemmat osapuolet lähettävät toisilleen LCP-paketteja, joiden avulla datayhteyden asetukset konfiguroidaan ja yhteyden toimivuus testataan OSI-mallin toisen kerroksen tasolla. Kun yhteys on todettu toimivaksi tällä tasolla, lähetetään erityinen Configure-Ack -paketti. Kun tämä paketti on vastaanotettu linkin kummassakin päässä, linkin taso asetetaan Yhteys auki -tilaan (LCP Open). Tässä vaiheessa yhteys hyväksyy ainoastaan LCP-paketteja. Mikäli jompikumpi osapuoli havaitsee muita paketteja yhteydenmuodostusvaiheessa, ne hylätään ilman erillistä ilmoitusta. (IETF 1994, rfc1661.)

Kun yhteys on todettu toimivaksi, siirrytään vapaaehtoiseen autentikointivaiheeseen. Tämä vaihe ei siis ole pakollinen, ja sitä käytetään ainoastaan, mikäli yhteyden tietoturva koetaan erityisen tärkeäksi. LanWorldin tapauk-

sessa tämä tulee ilmi hyvin, sillä yrityksellä on käytössä runkoverkkoyhteyksiä kahdelta eri toimittajalta, joista toinen vaatii yhteyksissään autentikoinnin käyttämistä ja toinen ei. Autentikointivaiheessa linkin läpi sallitaan kolmenlaisia paketteja: LCP-, autentikointi- sekä linkin laatua mittaavia paketteja. Mikäli autentikointi vaaditaan ja se epäonnistuu, siirrytään yhteydessä kuvan mukaisesti suoraan linkin sulkemiseen. Autentikointi tulisi RFC 1661-määrittelyn ohjeiden mukaisesti konfiguroida siten, että autentikoinnin epäonnistumisen syyksi ei katsota pelkästään viivettä. Lisäksi tulisi mahdollistaa useampi autentikointiyritys tällaisissa tilanteissa. (IETF 1994, rfc1661.)

Kun linkin avaus ja mahdollinen autentikointi on suoritettu, siirrytään OSI-mallin kolmannelle eli verkkokerrokselle. Tätä vaihetta kutsutaan NCP-vaiheeksi (Network Control Protocol). NCP-vaiheessa konfiguroidaan käytettävän verkkokerroksen protokollan asetukset. Yleisin nykyään käytettävä verkkokerroksen protokolla on Internet Protocol (IP). Kun NCP-yhteys on auki, voidaan PPP-linkin yli välittää ennaltasovittuja verkkokerroksen protokollapaketteja. Mikäli linkin yli yritetään lähettää jonkin muun protokollan paketteja, hylätään ne ilman erillistä ilmoitusta, kuten aiemmin LCP-vaiheessakin ei-halutuille paketeille tehtiin. Tässä vaiheessa PPP-yhteys on toiminnassa ja valmis välittämään tietoa. (IETF 1994, rfc1661.)

Seuraava vaihe PPP-yhteyden toiminnassa on yhteyden sulkeminen. Kuten aikaisemmasta kuvasta (kuva 12) voidaan huomata, PPP-yhteys voidaan sulkea missä yhteyden muodostuksen vaiheessa tahansa. Yhteyden sulkemisen syitä voivat olla järjestelmänvalvojan tarkoituksellisen sulkemisen lisäksi esimerkiksi jo edellä käsitelty autentikoinnin epäonnistuminen tai yhteyden riittämätön laatu, joka pitää sisällään käytännössä kaikki OSI-mallin 1- ja 2-kerroksiin liittyvät ongelmat. Yhteyden sulkeminen hoidetaan LCP-paketeilla aivan kuten yhteyden avaaminenkin. Sulkemisesta kerrotaan yhteyden molemmille osapuolille erityisillä sulkemispaketeilla (Terminate packets). Sulkemisvaiheessa 3. kerroksen protokollille ilmoitetaan linkin sulkeutumisesta, jolloin protokollat osaavat tehdä tarvittavat toimet sulkeutumista varten. (IETF 1994, rfc1661.)

Seuraavaksi käsittelen PPPoA:ta ja PPPoE:tä. Tällä hetkellä suurin osa LanWorldin kohteista on yhdistetty runkoverkkoon PPPoA:n kautta. Nämä yhteydet ovat kuitenkin muuttumassa PPPoE-pohjaisiksi. Tarkoitukseni on käsitellä erikseen sekä PPPoA:ta että PPPoE:tä, jonka jälkeen käsittelen niiden keskinäisiä eroavaisuuksia sekä niiden etuja ja haittoja toisiinsa nähden.

5.4 PPPoA (Point-to-point Protocol over ATM)

5.4.1 Yleistä

PPPoA käyttää ATM-sovituskerroksen AAL5-osiota, jonka mainitsin kohdassa 4.2, PPP-kapseloitujen pakettien kehystykseen. Tämä mahdollistaa PPP-sanomien lähettämisen ATM-verkon yli, mikäli käytössä oleva ATM-verkko tukee Point-to-point -yhteyksiä. Lähetettäessä tietoa PPPoA:lla, PPP-kerros vastaa ATM-sovituskerroksen mukaista AAL5-virtuaaliyhteyttä. Tämä yhteys voi olla joko jatkuva (dedicated), joka tarkoittaa yhteyttä, joka on auki jatkuvasti, riippumatta siitä, onko linkin yli aikomus lähettää dataa. Yhteys voi olla myös kytketty (switched), joka tarkoittaa sitä, että yhteys muodostetaan ainoastaan silloin kun linkin yli on tarvetta lähettää tietoa. (IETF 1998, rfc 2364.)

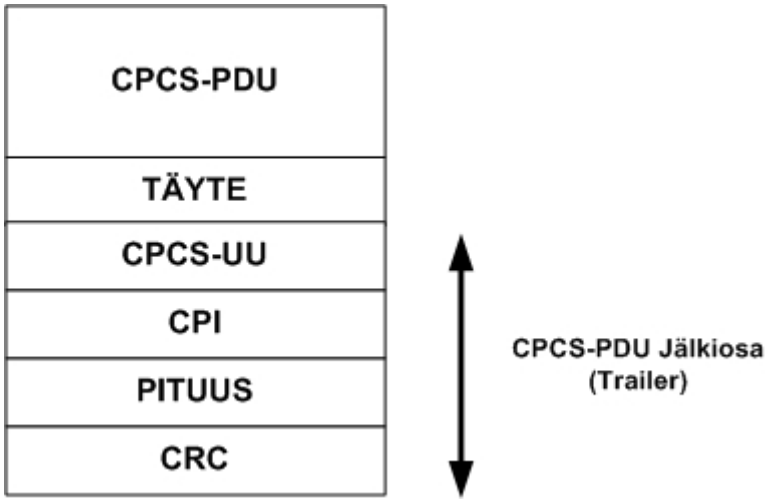
PPPoA käyttää kahta eri tapaa tunnistaakseen PDU:n (Protocol Data Unit) tietosisällön protokollatyypin:

1. Virtuaalipiiriin pohjautuva monivalinta (multiplexing).
2. Ethernet-osiossa esitelty Logical Link Control (LLC).

Seuraavaksi käsittelen näitä tunnistustapoja tarkemmin.

5.4.2 Virtuaalipiiriin pohjautuva monivalinta

Seuraavassa kuvassa (kuva 13) esitetään AAL5 PDU -paketin osat IETF:n RFC-2364-julkaisun mukaan.



Kuva 13: AAL5 PDU-paketti (IETF 1998, RFC 2364)

Paketin osien koot ja tarkoitukset ovat seuraavat (IETF 1998, rfc 2364.):

1) CPCS-PDU- osio sisältää käyttäjäinformaatiota ja on kooltaan 2^16-1 oktettia.

2) Täyte toimii tässä paketissa samalla tavalla kuin esimerkiksi Ethernet-kehyksissä. Täytteen avulla varmistetaan, että paketti on juuri oikean kokoinen, jotta se voidaan lähettää ATM-solussa. Täyteosion koko vaihtelee tarpeen mukaan 0-47 oktetin välillä.

3) CPCS-UU (User-To-User indication) mahdollistaa CPCS (Common Part Convergence Sub-layer) – käyttäjätiedon lähettämisen. RFC-2364:n mukaan tällä osiolla ei ole käyttöä tämänkaltaisessa moniprotokollakapseloinnissa, joten osion arvo voi olla mikä tahansa.

4) CPI (Common Part Indicator) on yhden oktetin kokoinen osio, joka auttaa vastaanottajaa tulkitsemaan PDU:ta.

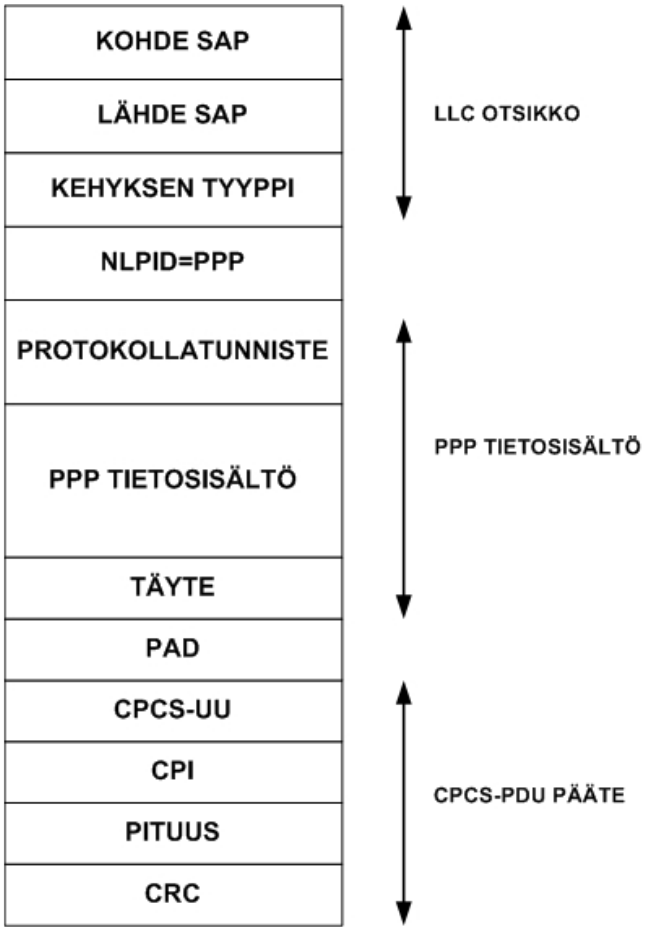
5) Pituusosio on kooltaan kaksi oktettia, ja se kertoo nimensä mukaisesti kuinka monta oktettia paketin tieto-osuus sisältää. Tämän osion maksimiarvo on 65535 oktettia. Pituusosiolla voidaan määrittää lähetyksen keskeytys. Tällöin osion arvoksi asetetaan 0x00.

6) CRC-osiota käytetään koko paketin turvaamiseen. CRC-osio itsessään jää kuitenkin suojaamatta.

Osa LanWorldin käyttämistä runkoyhteyksistä on toteutettu virtuaalipiiriin pohjautuvan monivalinnan avulla. Käytännössä yhteyden konfiguroinnissa tarvitsee ottaa huomioon ainoastaan se, että yhteys asetetaan tällaisissa tapauksissa käyttämään VC-MUX tekniikkaa, jolla tarkoitetaan nimenomaan virtuaalipiiriin pohjautuvaa monivalintaa.

5.4.3 LLC kapseloitu PPPoA

Kuten aiemmin mainitsin, virtuaalipiiriin pohjautuvan monivalinnan lisäksi PPPoA-paketti voidaan kapseloida myös LLC:n avulla. Seuraavassa kuvassa (kuva 14) esitetään LLC kapseloidun PPPoA-paketin osat IETF:n RFC-2364-julkaisun mukaan.



Kuva 14: LLC-kapseloitu PPPoA-paketti (IETF 1998, RFC 2364)

Kuten kuvasta 14 voidaan huomata, koostuu tämä paketti osittain samoista osista kuin virtuaalipiiriin pohjautuva monivalintapaketti (IETF 1998, rfc 2364). Seuraavaksi käsittelen paketin eri osat ja niiden käyttötarkoitukset IETF:n RFC 2364:n mukaan. (IETF 2000, rfc2974; IETF 1998, rfc 2364.)

1) LLC-Otsikko
LLC-otsikko koostuu kohde- ja lähde-SAP:ista (Session announcement Protocol) sekä kehyksen tyyppitiedoista (IETF 2000, rfc2974).

2) NLPID
NLPID (Network Layer Protocol Identifier) kentässä kerrotaan, mitä OSI-mallin verkkokerroksen protokollaa käytetään. Tässä tapauksessa arvoksi asetetaan luonnollisesti PPP.

3) Protokollatunniste
Protokollatunniste on kooltaan 1-2 oktettia (8-16 tavua). Tunniste auttaa käytetyn protokollan määrittelyssä.

4) PPP-tietosisältö
PPP-tietosisältö on koostumukseltaan sama kuin jo aiemmin esitelty PPP-sanoma (ks. kuva 11).

5) CPCS-PDU pääte
Kuten kuvasta 14 voidaan huomata, on CPCS-PDU -pääte koostumukseltaan ja käyttötarkoitukseltaan samanlainen kuin virtuaalipiiriin pohjautuvan monivalintapaketin viimeiset osat.

Valinta LLC-kapseloidun ja virtuaalipiiriin pohjautuvan monivalinnan välillä tehdään yhteyden muodostamisvaiheessa yhteyden aloittajan toimesta. Aloittaja lähettää vastaanottajalle pyynnön paketista, joka sisältää asetukset joko LLC-kapseloidulle tai virtuaalipiiriin pohjautuvalle yhteydelle. Mikäli yhteyden aloittaja vastaanottaa jostain syystä paketin, joka sisältää asetukset jollekin muulle yhteystyypille, se hylätään välittömästi. (IETF 1998, RFC 2364.)

5.5 PPPoE (Point-to-Point Protocol over Ethernet)

5.5.1 Yleistä

Siinä missä PPPoA käyttää hyväkseen ATM-soluja, PPPoE mahdollistaa PPP-sanomien lähetyksen Ethernet-kehykseen kapseloituna. PPPoE mahdollistaa loppukäyttäjien yhteyksien käsittelyn erillisinä yhteyksinä vastaanottajapäässä sen sijaan, että kaikkien loppukäyttäjien yhteydet käsiteltäisiin yhtenä yhteytenä. (IETF 1999, rfc 2516.) Käytännössä tämä tarkoittaa sitä, että kiinteistöverkon jokaisen käyttäjän autentikointi voidaan hoitaa runko-operaattorin laitteilla jokaiselle erikseen.

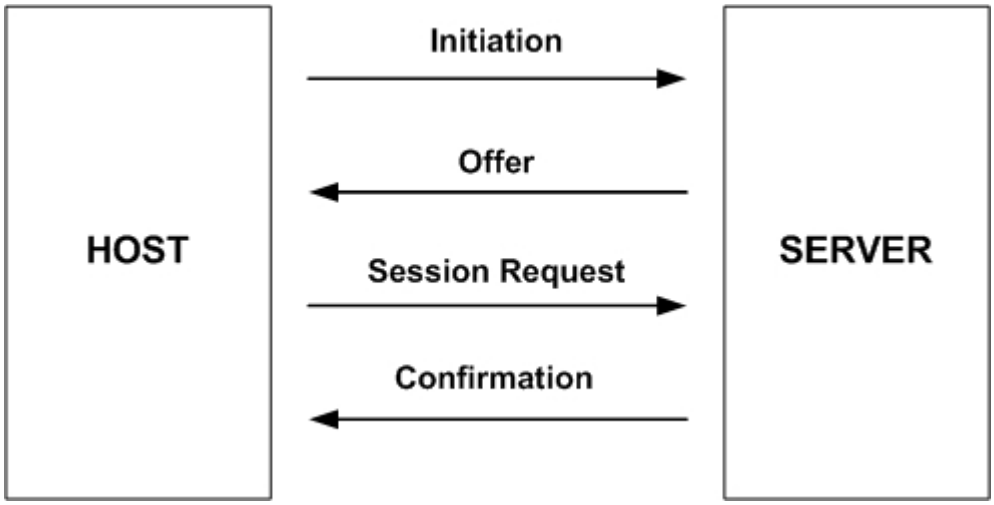
LanWorld Finlandin tapauksessa näin ei kuitenkaan tehdä. LanWorldin kohteissa PPPoE:tä käyttää ainoastaan kiinteistön puhelinjakamossa sijaitseva reititin, joka tarjoaa runkoyhteyden muulle kiinteistölle. Itse näen tämän lähinnä hyvänä asiana, sillä mielestäni asiakaskohtainen autentikointi lisää yhteyden käyttöön jälleen vaiheen, jossa asiakas voi tehdä virheen. Mikäli autentikointia käytettäisiin, lisääntyisivät kadonneita salasanoja koskevat tukipuhelut runsaasti, ja asiakastuen kuormitus nousisi.

PPPoE yhteys koostuu kahdesta vaiheesta: etsintävaiheesta (Discovery stage) ja PPP-istuntovaiheesta (PPP Session stage). Vaiheet suoritetaan yhteyden muodostuksessa aina siten, että yhteyden muodostus aloitetaan etsintävaiheella, jonka jälkeen voidaan siirtyä istuntovaiheeseen. Seuraavaksi käsittelen näitä vaiheita tarkemmin.

5.5.2 Etsintävaihe

Kun käyttäjä (host) haluaa muodostaa PPPoE-yhteyden, tulee sen siirtyä etsintävaiheeseen. Etsintävaiheessa käyttäjä tunnistaa vastaanottajan Ethernet MAC -osoitteen ja luo yhteydelle PPPoE-session id:n, joka toimii yhteyden tunnisteena. Vaikka PPP-yhteys itsessään on käyttäjältä-käyttäjälle yhteys (peer-to-peer), etsintävaihe on nimenomaisesti käyttäjä-palvelin yhteys (Client-Server). Etsintävaiheessa käyttäjä (Host) etsii käytettävissä olevat palvelimet (Server) ja valitsee niistä oikean. Valinta tapahtuu lähettämällä saatavilla oleville palvelimille paketti, joka kertoo käyttäjän halusta muodostaa PPPoE-yhteys (Initiation). Tämän jälkeen saatavilla olevat palvelimet lähettävät käyttäjälle paketin, jossa tarjoudutaan yhteyden toiseksi osapuoleksi (Offer). Seuraavaksi käyttäjä valitsee tarjouspakettien perusteella halutun palvelimen jolle lähetetään istuntopyyntöpaketti (Session Request). Tämän jälkeen valittu palvelin lähettää käyttäjälle erillisen varmistuspaketin (Confirmation packet), jonka jälkeen osapuolet ovat valmiita siirtymään istuntovaiheeseen. (IETF 1999, rfc 2516.)

Alla oleva kuva (kuva 15) havainnollistaa etsintävaiheessa lähetettävien pakettien keskinäistä järjestystä.



Kuva 15: Etsintävaihe

5.5.3 Istuntovaihe

Seuraava vaihe on istuntovaihe, jonka aikana yhteyden osapuolet voivat lähettää PPP-kapseloitua tietoa toisilleen ethernetverkon yli. Kaikki tieto lähetetään unicastina, jonka toimintaperiaate on käsitelty aiemmin Ethernet-osiossa. Lähetettävän paketin suurin mahdollinen koko (MRU) ei saa ylittää 1492 oktettia. Tämä johtuu siitä, että Ethernet-kehyksen suurin mahdollinen koko on 1500 oktettia. Näistä 1500 oktetista täytyy varata kuusi oktettia

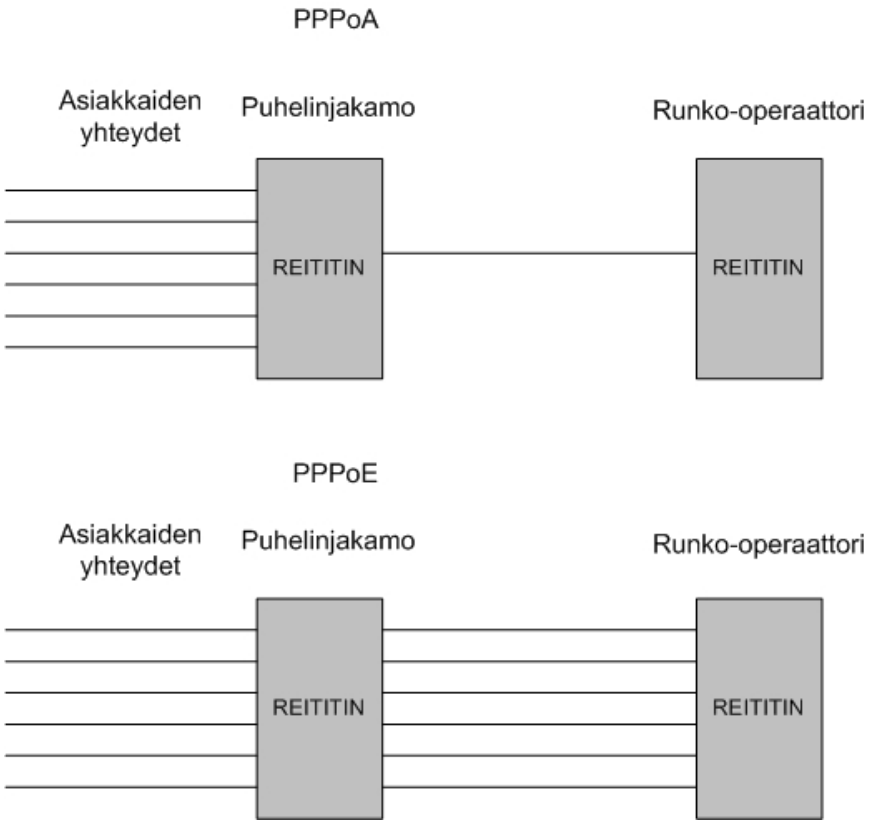
PPPoE-otsikolle, ja PPP-protokollatunnisteelle kaksi oktettia. Kun nämä osat lasketaan yhteen, jää Ethernet-kehyksen maksimikoosta käyttämättä yllämainitut 1492 oktettia, jotka voidaan hyödyntää lähetettävässä sanomassa. (IETF 1999, rfc 2516.)

PPPoE-yhteyden sulkeminen tapahtuu lähettämällä erillinen paketti, joka kertoo yhteyden sulkemisesta. Tämä paketti on nimeltään PADT (PPPoE Active Discovery Terminate Packet). PADT:in lähettämisen jälkeen paketin vastaanottaja sulkee yhteyden, jonka jälkeen samaa yhteyttä pitkin ei voida lähettää mitään tietoa. Mikäli yhteys on lopetettu liian aikaisin ja tietoa on jäänyt lähettämättä, tulee osapuolien palata etsintävaiheeseen ja luoda uusi PPPoE-istunto uudella PPPoE -session ID:llä. (IETF 1999, rfc 2516.) Runkoyhteyksien muutoksista huolimatta LanWorldin liittymiä käyttävien asiakkaiden yhteydet eivät toimi PPPoE:n mukaan, sillä ainoastaan puhelinjakamossa sijaitseva runkoyhteysreititin toimii PPPoE:n avulla.

5.6 PPPoA:n ja PPPoE:n keskinäiset erot

Olen käsitellyt aikaisemmin PPPoA:ta ja PPPoE:tä erillisinä tekniikoina. Seuraavaksi aion syventyä niiden keskinäisiin eroihin. Asia on tärkeä, sillä LanWorldin runko-operaattorit ovat siirtymässä yhteyksissään PPPoA-pohjaisista ratkaisuista PPPoE:hen perustuviin ratkaisuihin. Tarkoitukseni on selvittää, minkälaisia vaikutuksia muutoksilla on LanWorldin näkökulmasta.

Ensisilmäyksellä PPPoA ja PPPoE ovat hyvin samankaltaisia. Molemmat mahdollistavat PPP-liikenteen tietyn protokollan yli. Selkeä ero tekniikoiden välillä on esimerkiksi siinä, miten ne käsittelevät sisäänpäin tulevia yhteyksiä palveluntarjoajan päässä. PPPoA käsittelee kaikki samasta lähteestä tulevat yhteydet samana yhteytenä, kun taas PPPoE pystyy käsittelemään yhteydet erillisinä. Yhteydet eritellään loogisella tasolla, joten fyysisen tason yhteyksiä ei tarvita kummassakaan tekniikassa kuin yksi. (IETF 2000, rfc 2974; IETF 1998, rfc 2364.) Alla oleva kuva (kuva 16) havainnollistaa PPPoA:n ja PPPoE:n yhteyksien käsittelyn keskinäisiä eroja.



Kuva 16: PPPoA:n ja PPPoE:n yhteyksien käsittelyn erot

LanWorldin verkoissa yhteyksien käsittelyn eroavaisuus ei ole oleellinen, sillä vaikka runkoyhteys muutettaisiinkin PPPoE:ksi, asiakkaiden yhteydet säilyisivät ennallaan. Käytännössä verkon käyttäjien yhteydet siis yhdistetään edelleen puhelinjakamossa yhdeksi yhteydeksi, eikä esimerkiksi autentikointia hoideta runko-operaattorin toimesta asiakaskohtaisesti, jonka PPPoE mahdollistaisi.

Wikipedian mukaan (Wikipedia 2006) PPPoA vaatii vähemmän resursseja laitteilta kuin PPPoE. Ero ei kuitenkaan mielestäni ole merkittävä (0.58 %). Lisäksi PPPoA ei kärsi samoista ongelmista kuin PPPoE, jonka MTU (Maximum Transmission Unit) on pienempi kuin standardin Ethernetin MTU. Nämä ongelmat esiintyvät kuitenkin lähinnä ainoastaan huonosti konfiguroitujen palomuurien yhteydessä. Näiden lisäksi kummatkin tekniikat tukevat LLC-, sekä virtuaalipiiriin pohjautuvaa monivalintakapselointia, jotka olen esitellyt tarkemmin PPPoA-osiossa (Osio 5.4).

Kaiken kaikkiaan runkoyhteyden muutos PPPoA:sta PPPoE:ksi ei tule juurikaan vaikuttamaan LanWorld Finland Oy:n toimintaan. Perustelen mielipidettäni sillä, että muutokset eivät käytännössä kosketa kuin runko-operaattoriin yhteydessä olevaa reititintä. Muu verkko voidaan säilyttää konfiguraatioiltaan täysin samana sekä Ethernet- että ADSL-kohteissa. Esittelen näitä konfiguraatioita tarkemmin osioissa 7 ja 9.

6 OSI-malli vianmäärityksessä

Toisessa osiossa esittelemääni OSI-mallia hyödynnetään myös vianmäärityksessä, johon malli sopii hyvin. OSI-mallin avulla vianmääritys voidaan suorittaa helposti järjestyksessä mallin kerroksia mukaillen. Vikaa voidaan ruveta etsimään OSI-mallin avulla kolmella eri lähestymistavalla: ylhäältä alaspäin etenevällä tavalla, alhaalta ylöspäin etenevällä tavalla tai hajoita ja hallitse -tavalla. Nämä vianmääritystavat ovat esimerkki siitä, miten OSI-mallia voidaan käyttää viitekehyksenä ja ohjenuorana muuhunkin kuin uusien verkkotekniikoiden ja -sovellusten suunniteluun.

Seuraavaksi käsittelen lyhyesti OSI-malliin nojautuvien vianmääritystapojen käyttöä omien kokemuksieni kautta. Olen työskennellyt asiakkaiden tietoteknisten ongelmien kanssa useissa eri tehtävissä. Ensimmäiseksi tukitehtäväkseni lasken IT-tukiopiskelijana toimimisen Savitaipaleen lukiossa. Tehtäviini kuuluivat lähinnä koulun intranetin kehittäminen ja ylläpito, mutta tämän lisäksi autoin koulun henkilökuntaa ja opiskelijoita heidän tietotekniikkaan liittyvissä ongelmissaan. Jo tuolloin huomasin, että suurin osa ongelmista liittyi lopulta aivan muihin syihin kuin ainoastaan toimimattomiin ohjelmiin, mihin kuitenkin usein ennen varsinaista vianmääritystä saatettiin viitata.

Lukion jälkeen aloitin opintoni Tampereen Ammattikorkeakoulussa syksyllä 2003. Toisena opiskeluvuotenani aloitin työt yrityksessä, joka tarjosi IT-neuvontaa ja -konsultointia kuluttajille. Työssäni huomasin jälleen tutun asian: asiakkailla saattoi olla ongelmia ohjelmien toiminnassa, mutta ongelmien syyt löytyivätkin muualta kuin itse ohjelmasta.

Maaliskuussa 2005 lopetin työni yrityksessä ja aloitin harjoittelun loppuosan suorittamisen LanWorld Finland Oy:ssä tietoliikenneasentajana. Harjoitteluni aikana työskentelin myös paljon asiakkaiden käyttöongelmien parissa. Tälläkään kertaa ongelmat eivät koskeneet niinkään ohjelmien toimimattomuutta vaan internetyhteyksien ongelmia. Näissäkin tapauksissa ongelma löytyi useasti muualta kuin itse yhteyden toimimattomuudesta.

Vianmäärityksessä on siis osattava ottaa huomioon asiakkaan usein riittämättömät tiedot ongelmien paikallistamisessa. Esimerkiksi sähköpostiohjelman toimimattomuuden kohdalla voi vika olla itse ohjelman lisäksi esimerkiksi palomuurissa, rikkinäisessä verkkokortissa, ADSL-modeemissa tai käyttäjän omassa osaamattomuudessa. Käyttäjätason ongelmiin viitataan usein kahdeksannen tason ongelmana.

Jo edellä sivuamallani tavalla käsittelen vianmäärityksen tapausesimerkkinä sähköpostiohjelman toimimattomuutta, ja vianmääritystä etätukena. Mielestäni tämä esimerkki on sopiva siksi, että sähköposti on sovellus, jota suuri osa Internetin ja tietokoneen käyttäjistä käyttää enemmän tai vähemmän

säännöllisesti. Usein sähköpostia käytetään selainpohjaisen webmail-sovelluksen kautta, mutta monet käyttävät erillistä sähköpostiohjelmaa kuten Microsoft Outlook:ia tai Mozilla Thunderbird:ia. Seuraavassa yritän tuoda esiin OSI-malliin pohjautuvia vaihtoehtoisia vianmääritysmalleja esimerkkiongelmani kautta. Perustan pohdintani Cisco Certified Network Professional –kurssilla oppimaani.

6.1 Ylhäältä alaspäin malli

Tilanteessa, jossa asiakas ilmoittaa, että sähköpostiohjelma ei toimi, lähdetään vikaa helposti etsimään suoraan sähköpostiohjelman asetuksista: tällaista lähestymismallia kutsutaan ylhäältä alaspäin eteneväksi lähestymistavaksi. Tällöin vian määrittäminen aloitetaan OSI-mallin sovelluskerrokselta, jolla sähköpostiohjelma vaikuttaa. Mikäli vika löytyykin edellä esitetyllä tavalla ohjelman asetuksista, on ongelma helposti ratkaistu ylhäältä alaspäin –mallin avulla.

6.2 Alhaalta ylöspäin -malli

Ongelmaa ei kuitenkaan välttämättä saada ratkaistua ylhäältä alaspäin etenevän mallin avulla. Tällaisia ovat esimerkiksi tapaukset, joissa sähköpostiohjelman asetukset ovat kunnossa, mutta silti ilmenee edelleen ongelmia. Kokemukseni perusteella ylhäältä alaspäin –malli ei välttämättä ole paras mahdollinen lähestymistapa myöskään sellaisten ongelmien kohdalla, joissa vika esiintyy ohjelmistossa, joka käyttää esimerkiksi Internet-yhteyttä.

Vianmääritys onkin järkevämpää aloittaa selvittämällä asiakkaan koneen fyysinen taso. Tällä tarkoitetaan muun muassa johtojen ja verkkokortin liitäntöjen tarkistusta. Mikäli johdot, verkkokortti ja koneen muu fyysinen taso ovat kunnossa, voidaan siirtyä esimerkiksi mahdollisen ADSL-modeemin toiminnallisuuden tarkistamiseen. Esimerkkinä edellä mainitusta voidaan mainita ADSL-modeemin valojen tarkistus: lähes kaikissa modeemeissa on erillinen ”Line” valo, joka kertoo, onko modeemilla yhteys palveluntarjoajan verkkoon. LanWorldin tapauksessa yhtäjaksoisesti palava valo kertoo yhteyden olevan kunnossa kiinteistön puhelinjakamossa sijaitseviin DSLAM:eihin (Digital Subscriber Line Access Multiplexer). Mikäli valo palaa, eikä yhteys toimi, olisikin hyvä testata yhteys toisella koneella, ja mikäli mahdollista myös toisella modeemilla. Jos yhteys ei toimi edelleenkään, voidaan vian usein olettaa olevan puhelinjakamossa sijaitsevissa laitteissa tai vielä kauempana eli runko-operaattorin verkossa. Mikäli yhteys taas toimii laitteiden vaihdon jälkeen, voidaan sähköpostiohjelman toimivuus testata uudelleen. Jos ohjelma toimii, voidaan suurella varmuudella sanoa ongelman olevan alemmilla kerroksilla.

6.3 Hajota ja hallitse -malli

Kuten jo edellä mainitsin, ei ylhäältä alaspäin –malli, mutta ei myöskään alhaalta ylöspäin etenevä malli ole välttämättä parhaita mahdollisia lähestymistapoja esimerkkinäni käyttämäni ongelman ratkaisussa. Vianmääritystä ei ole järkevää aloittaa itse ohjelman asetuksista, koska usein ei voida olla varmoja esimerkiksi siitä, onko asiakkaan Internet-yhteys kunnossa. Toisaalta vianmääritystä ei ole järkevää aloittaa fyysiseltä tasoltakaan, varsinkaan, mikäli vianmääritys tapahtuu puhelimitse. Tämä johtuu jälleen siitä, että asiakas ei välttämättä osaa varmistaa oikeiden johtojen kytkentöjä. Lisäksi olen huomannut, että jopa ADSL-modeemin valojen tarkastus saattaa aiheuttaa asiakkaalle ongelmia.

Etäongelmanratkaisuun onkin parempi lähteä hieman asiakasystävällisemmin. Voidaan edetä esimerkiksi siten, että aluksi yksinkertaisesti varmistetaan, toimiiko asiakkaan Internet-yhteys. Helpoin tapa varmistua asiakkaan Internet-yhteyden toimivuudesta on neuvoa asiakasta avaamaan selain ja pyytää lataamaan jokin tietty sivusto. Vianmäärityksessä on hyvä valita sellainen sivusto, jota asiakas ei ole käyttänyt, jotta saadaan poistettua mahdollisuus siitä, että sivu on tallentunut selaimen välimuistiin ja latautuu sieltä. Olen havainnut, että esimerkiksi eri kaupunkien kotisivut ovat nopea ja yksinkertainen tapa testata Internet-yhteyden toimivuutta.

Mikäli yhteys testaamisen jälkeen toimii, voidaan seuraavassa vaiheessa siirtyä suoraan sovellustason vianmääritykseen, eli sähköpostiohjelman asetuksien tarkastukseen. Mikäli sivut eivät tällöin lataudu, on hyvä tarkistaa asiakkaalta, onko hänellä käytössään palomuurisovellusta. Mikäli palomuuri on käytössä, on mahdollista, että se estää Internet-liikenteen kulun. Palomuurin asetuksien läpikäynti on varsinkin puhelimitse usein käytännössä mahdotonta. Ongelma voidaan kuitenkin yrittää kiertää hieman riskialttiilla tavalla, eli sulkemalla hetkeksi koko palomuuri yhteyden testauksen ajaksi. Kunhan yhteys on saatu toimimaan muutoin, voidaan keskittyä itse sovelluksen asetuksien tarkistukseen.

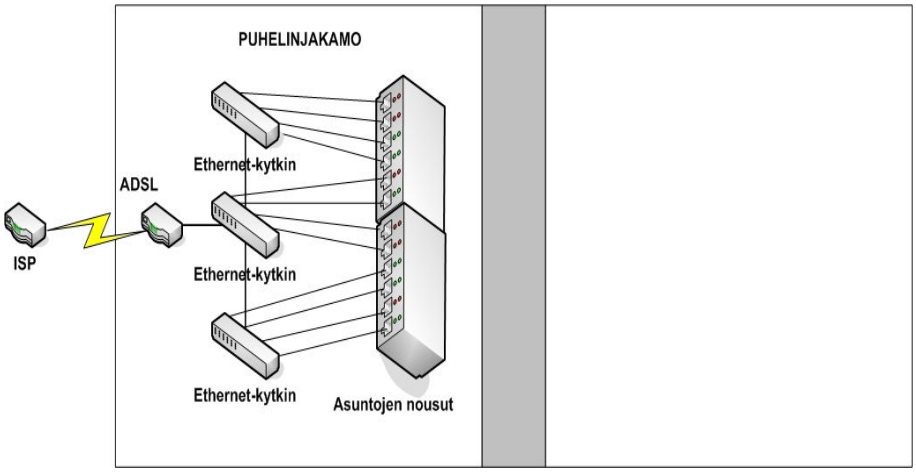
Kuten edellä esitetyn perusteella voidaan huomata, viimeinen tapa eroaa kahdesta ensin mainitusta lähestymistavasta siten, että se on ainakin näennäisen järjestäytymätön OSI-malliin nähden. Tällä tarkoitan sitä, että vianmääritystä tehdessä hypitään OSI-mallin kerrokselta toiselle epäjärjestyksessä. Omalla kohdallani käytäntö on lisäksi osoittanut, että varsinkin puhelimitse tapahtuvassa vianmäärityksessä asiakkaiden puutteelliset IT-taidot johtavat helposti siihen, että järjestyksellinen ylhäältä alas- tai alhaalta ylös etenemismalli ei yleensä ole tehokkain, mutta ei myöskään varmin tapa nopeaan vianmääritykseen. Lisäksi olen havainnut, että usein vastaavanlaisissa tehtävissä toimivat asiakaspalvelijat ovat omaksuneet vianmääritystavan, joka muistuttaa paljon tässä luvussa käsittelemääni hajota ja hallitse -lähestymistapaa, vaikka heillä ei olisikaan pohjatietoja OSI-mallista tai edes tietoverkoista yleisesti. Vianmääritystapaa voisi kuitenkin tehostaa tutustumalla OSI-malliin hieman tarkemmin. Mallin edes pintapuolinen sisäistämi-

nen saattaa auttaa ymmärtämään eri kerroksien välisiä yhteyksiä ja tuomaan uutta tietoa myös käytännön työntekoon.

7 LanWorldin Ethernet-ratkaisut

Kuten totesin osiossa 3, ovat Ethernet-ratkaisut uusissa kiinteistöissä yleistymässä kovaa vauhtia. Yhä useammin kiinteistöihin lisätään kiinteä ethernetkaapelointi jo rakennusvaiheessa. Tämä auttaa toimivan kiinteistöverkon käyttöönotossa huomattavasti: verkkoa ei tarvitse toteuttaa tällöin kiinteistön puhelinverkkoa käyttäen. Puhelinverkot ovat monesti, varsinkin vanhoissa kiinteistöissä, ongelmallisia johtojen huonon kunnon takia. Pahimmillaan huono kaapelointi johtaa lähetettävän signaalin heikkenemiseen siinä määrin, että verkon käyttäjät joutuvat kärsimään toistuvista yhteyskatkoista.

Käytännössä LanWorldin Ethernet-kohteet toteutetaan yhdellä ADSL-reitittimellä, joka tuo runkoyhteyden kiinteistön pääjakamoon. Reititin yhdistetään Ethernet-kytkimeen tai -kytkimiin, jonka porteista kytketään RJ-45 -kaapelit puhelinjakamossa oleviin asuntojen ethernetkaapeleihin. Seuraavassa kuvassa (kuva 17) esittelen tyypillisen Ethernet-verkossa toimivan kiinteistön verkkotopologian. Esimerkkitapaus on sikäli mielikuvituksellinen, että se ei ole suoraan mikään olemassa oleva kohde, vaan yleismuotoinen esitys LanWorldin perusmallisesta Ethernet-kohteesta.



Kuva 17: Ethernet-kohteen topologia

Kuten kuvasta (kuva 17) voidaan huomata, verkko on jaettu kolmeen osaan: puhelinjakamoon, kiinteistökaapelointiin ja asuntoon. Puhelinjakamo toimii keskuksena kiinteistön puhelin- sekä tässä tapauksessa ethernetkaapeleille. Kaikista asunnoista vedetyt kaapelit päätyvät puhelinjakamoon. Joissakin kohteissa on puhelinjakamon lisäksi välijakamot jokaiselle kiinteistön talol-

le tai jokaisen talon eri rapuille. Välijakamot asettautuisivat yllä esitetyssä kuvassa kiinteistökaapeleiden ja asunnon välille. Puhelinjakamoon asennetaan ADSL-reititin, joka konfiguroidaan runkoverkko-operaattorin antamien asetusten mukaan. Reititin toimii porttina Internetiin. LanWorld käyttää kohteissaan enimmäkseen ZyXelin Prestige-sarjan ADSL-reitittimiä. Näiden lisäksi käytössä on jonkin verran Ciscon 800-sarjan reitittimiä. Reitittimet konfiguroidaan Ethernet-kohteissa usein reitittävään muotoon, jolloin LanWorldin reititin vastaa esimerkiksi asiakkaille jaetuista IP-osoitteista. Saman kiinteistön eri asunnot ovat siis keskenään samassa lähiverkossa. Yleisimmin käytetty osoitteisto näille verkoille on 192.168.1.0/24, joista ensimmäinen osoite (192.168.1.1/24) on varattu itse reitittimelle. Tästä verkosta voidaan jakaa asiakkaiden käyttöön DHCP:lla (Dynamic Host Configuration Protocol) 253 eri osoitetta automaattisesti. Asiakkaiden ei siis tarvitse tehdä muuta kuin kytkeä ethernetjohto verkkokortista asunnon ethernetpistokkeeseen, ja oikeat IP-asetukset määritetään tietokoneelle automaattisesti.

Vaikka LanWorldin käyttämissä ADSL-reitittimissä yleensä on useampia ethernetportteja, ei niitä kuitenkaan käytännössä ole koskaan riittävästi koko kiinteistön tarpeisiin. Tämä ongelma ratkaistaan erillisillä ethernetkytkimillä. Kuvan 8 esimerkissä kaikki kytkimet ovat puhelinjakamossa, mutta tietyissä tapauksissa kiinteistön jokaiselle talolle tai rapulle asennetaan oma kytkin kyseisen talon tai rapun välijakamoon. LanWorldin käyttämät ethernetkytkimet ovat yleensä 12- tai 24-porttisia. Kytkimiä asennetaan kiinteistöön niin monta, että jokaiselle asunnolle on oma porttinsa.

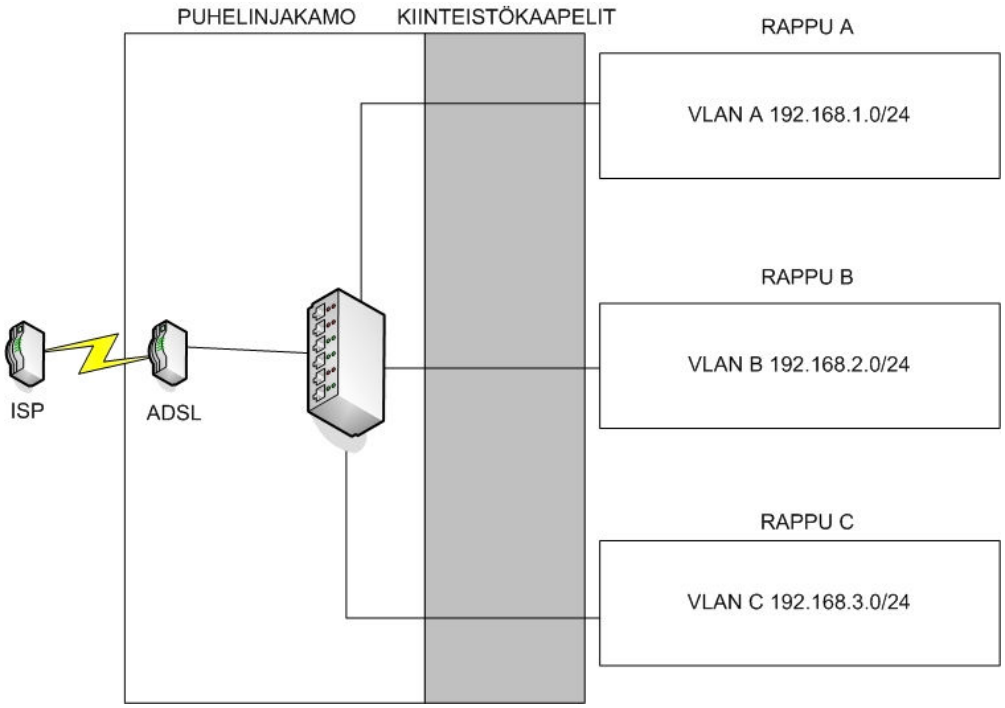
Asunnonnousuilla tarkoitetaan jokaisen asunnon ethernetjohdon loppupäätä. Kaikkien asuntojen johdotukset kerätään samaan pisteeseen puhelinjakamossa, jossa ne kytketään LanWorldin ethernetkytkinten portteihin. Uusien asiakkaiden kytkentä tapahtuu lisäämällä uusi ethernetjohto asiakkaan asunnonnoususta vapaaseen kytkinporttiin. Hyvin merkityillä asunnonnousuilla voidaan nopeuttaa uusien asiakkaiden kytkentää, ja minimoida mahdollisia asentajien tekemiä kytkentävirheitä merkittävästi verrattuna esimerkiksi ADSL-kohteisiin, joita käsittelen myöhemmin.

8 LanWorldin Ethernet-ratkaisujen ongelmia ja parannusehdotuksia

Ongelmat, joihin olen itse törmännyt LanWorldin Ethernet-kohteissa, eivät niinkään ole verkon suorituskyvystä johtuvia vaan esimerkiksi asiakkaiden taitamattomuudesta sekä laitevioista johtuvia. Hyvänä esimerkkinä tästä voidaan mainita tapaus, jossa erään kiinteistön asiakkaat ilmoittivat verkkoyhteyden katkenneen. Kun asiaa ruvettiin tutkimaan, huomattiin, että asiakkaat olivat saaneet IP-osoitteensa eri verkosta kuin LanWorldin oma reititin niitä jakoi. Loppujen lopuksi selvisi, että eräs asiakas oli hankkinut käyttöönsä ADSL/WLAN-reitittimen aikomuksenaan käyttää yhteyttään langattomasti. Reititin oli kuitenkin konfiguroitu toimimaan myös DHCP-palvelimena ja kun laite yhdistettiin kiinteistön sisäverkkoon, levisivät väärät IP-tiedot asiakkaan itsensä lisäksi myös muille kiinteistöverkon käyttäjille. Tässä tapauksessa ongelma saatiin ratkaistua käymällä asiakkaan luona ja konfiguroimalla asiakkaan verkkolaite siltaavaan muotoon, jolloin väärien IP-osoitteiden leviäminen saatiin loppumaan. Ne asiakkaat, jotka olivat ehtineet saada osoitteen väärästä verkosta, joutuivat uusimaan osoitteensa verkkoyhteyksien korjaus-toiminnolla, jolloin väärä osoite vapautettiin ja uusi osoite saatiin oikeasta verkosta.

Ongelman leviämiseen vaikutti sisäverkon avoimuus: koska kaikki asiakkaat olivat samassa verkossa, pääsivät väärät IP-osoitteet leviämään kaikkien käyttäjien laajuudella. Avoimuutta voitaisiin vähentää, tinkimättä kuitenkaan verkon toimivuudesta. Eräs keino tähän olisi määritellä ethernetkytkimille ainoastaan tietyt portit, joilta sallitaan esimerkiksi DHCP-tietojen välitys. Nämä portit olisivat luonnollisesti ne, jotka ovat suoraan yhteydessä ADSL-reitittimeen. Tällöin asiakkaiden IP-osoitteita jakaisi ainoastaan haluttu laite, eivätkä ylläkuvatut asiakkaiden väärinkonfiguroidut laitteet pääsisi aiheuttamaan ongelmia. Tämä ratkaisu on toisaalta hyvinkin laiteriippuvainen: kaikissa kytkimissä ei ole mainitunlaista toiminnallisuutta.

Mikäli edelläkuvattu konfiguraatio on mahdoton toteuttaa käytössä olevilla laitteilla, tulisi pohtia, miten ongelman aiheuttaja saataisiin eristettyä muista käyttäjistä mahdollisimman tehokkaasti. Liikkeelle voitaisiin lähteä esimerkiksi siitä, miten VLANeja voitaisiin hyödyntää ongelman rajoittamisessa. VLAN (Virtual Local Area Network) voisi oikeinkäytettynä rajata esimerkiksi kiinteistön eri raput omiin lähiverkkoihinsa alla olevan kuvan (kuva 18) mukaisesti.



Kuva 18: VLANien käyttö kiinteistössä

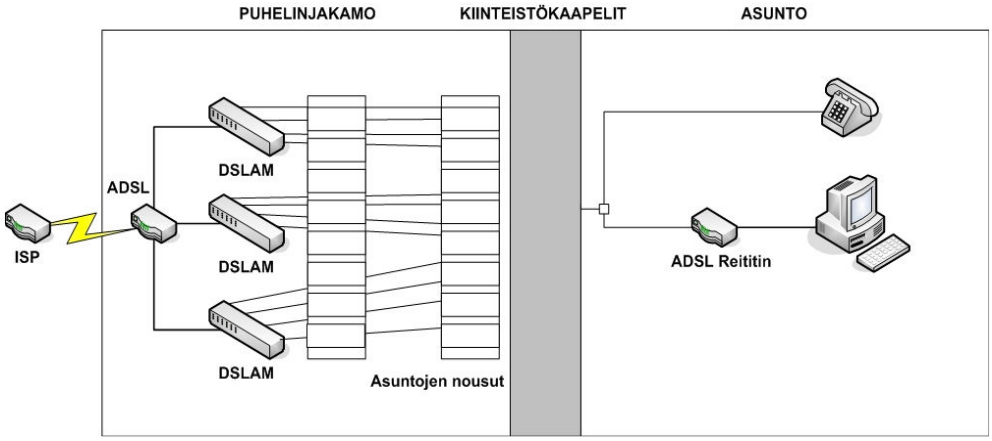
Kuten kuvasta 18 voidaan havaita, kiinteistön raput on jaettu omiin aliverkkoihinsa. Aliverkot ovat kooltaan hieman ylimitoitettuja, sillä jokaisessa aliverkossa on 254 laiteosoitetta jaettavaksi käyttäjille. Aliverkot voidaan tietysti jakaa pienemmiksi, jolloin käyttämättömiä osoitteita ei jää yhtä paljon. Aliverkon kokoa mietittäessä on kuitenkin hyvä ottaa huomioon mahdollinen käyttäjäkunnan kasvu. Nyrkkisääntönä voidaan pitää sitä, että verkkoon tulee varata osoitteita nykyisille käyttäjille kerrottuna kahdella. Kiinteistöverkkojen tapauksessa tämä ei ole niin tärkeä asia, sillä kiinteistöön mahtuu asuntoja vain tietty määrä, joka harvemmin kasvaa.

Kuvassa (kuva 18) kiinteistön reititys on toteutettu siten, että jokaiselta kytkimeltä on kytketty oma ethernetkaapeli reitittimenä toimivaan ADSL-reitittimeen. Kuvan esimerkissä on tosin käytetty ainoastaan yhtä kytkintä. Väärien DHCP-tietojen vuotaminen voitaisiin estää käyttämällä Ciscon laitteilla protected port-konfiguraatiota. Käytännössä tämä tarkoittaa sitä, että ainoastaan se kytkimen portti, joka on suoraan yhteydessä runkoyhteyden tarjoamaan ADSL-reitittimeen jätetään avoimeksi. Kaikki portit, jotka ovat asiakkaiden käytössä, asetetaan protected-tilaan. Protected-tilaan asetetut portit eivät hyväksy toisiltaan perusasetuksilla mitään liikennettä. Tällöin asiakkaalta vuotavat väärät IP-osoitteet eivät pääse muille käyttäjille asti. Portti asetetaan protected-tilaan komennolla switchport protected. VLANeja ja Protected port-konfiguraatiota käyttämällä voidaan kiinteistön eri raput segmentoida omiksi verkoikseen sen sijaan, että koko kiinteistö olisi yhtä suurta verkkoa.

Esitellynkaltainen verkkokonfiguraation muutos voisi siis auttaa edellä mainitun ongelman ehkäisyssä. Mikäli vääriä osoitteita tästä huolimatta pääsisi jonkin tietyn rapun aliverkkoon, olisi ongelma eristetty ainoastaan yhteen rappuun. Tällöin vika olisi helpompi ja nopeampi paikallistaa sillä mahdollinen ongelmanaiheuttaja löytyisi tietyn rapun käyttäjistä sen sijaan, että ongelman aiheuttajaa pitäisi etsiä koko kiinteistön käyttäjistä. Tämä olisi etu varsinkin suurissa kiinteistöissä, joissa käyttäjiä on runsaasti. Käytännössö kuitenkin jo pelkkä Protected port-konfiguraatio estää väärien IP-osoitteiden leviämisen. Ongelmia verkon konfiguroinnissa voi aiheuttaa runko-operaattorin antamat rajoitukset verkkoratkaisuille. Nämä rajoitukset tulisikin selvittää tarkasti ennen muutoksien tekemistä. Toisaalta en usko, että ongelmia tulee niin kauan kun tehdyt muutokset voidaan rajata kiinteistön omaan lähiverkkoon, koska tällöin yhteys runkoverkkoon säilyy muuttumattomana.

9 LanWorldin ADSL-ratkaisut

ADSL on yleisesti käytetty yhteystyyppi LanWorldin kohteissa. Yleisin toteutusmalli LanWorldin ADSL-yhteyksille on sillattu yhteys, jossa kiinteistön puhelinjakamoon asennetaan ADSL-reititin siltaavaan muotoon. Reititin on yhteydessä runko-operaattoriin, joka tarjoaa yhteyden Internetiin. Siltaava yhteys on sikäli hyvä ratkaisu, että tässä yhteysmuodossa itse reitittimeen kohdistuva rasitus on hyvin pientä: kaikki tieto siirretään reitittimeltä suoraan eteenpäin. Toisaalta siltaava yhteys asettaa rajoja kiinteistön oman verkon suhteen, koska varsinainen reititys tapahtuu runko-operaattorin laitteilla. Lisäkuluja aiheuttaa lisäksi yhteyksissä käytettävät julkiset IP-osoitteet, jotka joudutaan ostamaan erikseen runko-operaattorilta. Tämä tarkoittaa siis sitä, että yhteyksissä ei voida hyödyntää ilmaisia aliverkkoja, jotka määriteltäisiin LanWorldin laitteilla. Seuraavassa kuvassa (kuva 19) esittelen tyypillisen LanWorldin ADSL-kohteen. Kuten edellä esitellyssä Ethernetin tapauksessa, kuva ei ole mistään olemassa olevasta kohteesta suoraan, vaan se on yleisluontoinen kuvaus tyypillisestä ADSL-kohteesta.



Kuva 19: ADSL-kohteen topologia

Kuten kuvasta 19 voidaan huomata, käytetään ADSL-kohteissa kytkinten sijaan DSLAMeja (Digital Subscriber Line Access Multiplexer). DSLAMin avulla voidaan jakaa puhelinjakamoon tuleva ADSL-yhteys kaikille kiinteistöverkon käyttäjille. LanWorldin kohteissa DSLAMien portit on johdotettu erillisiin krone-paneeleihin, joista kytketään johdot käyttäjän asunnonnousuille. Uutta asiakasta kytkettäessä tulee ottaa huomioon mahdollinen käytössä oleva lankapuhelin. Mikäli asiakkaalla on lankaliittymä käytössä, tulee DSLAMille kytkeä johto sekä ADSL-linjalle että puhelinliittymälle. Tällaisessa tilanteessa asiakas tarvitsee asuntonsa puhelinpistokkeeseen jakosuotimen, joka mahdollistaa sekä ADSL:n että lankapuhelimen käyttämisen yhtä aikaa. Jakosuotimesta kytketään RJ-11 kaapelit sekä asunnon ADSL-reitittimeen että puhelimeen. Yhteys reitittimestä tietokoneeseen toteutetaan, laitteesta riippuen, joko USB- tai ethernetkaapelilla.

10 LanWorldin ADSL-ratkaisujen ongelmia ja parannusehdotuksia

Iso osa LanWorldin ADSL-kohteista tulevista vikailmoituksista johtuu joko runkoyhteyden katkeamisista tai attenuaatiosta eli lähetettävän signaalin heikentymisestä. Nämä ongelmat ovat sikäli vaikeasti kierrettävissä, että kumpikaan ongelma ei johdu LanWorldista. Runkoyhteyksien katkeileminen on viimekädessä runko-operaattorin vastuulla, ellei katkeaminen johdu LanWorldin laitteiden vioista. Attenuaatio puolestaan johtuu yleensä huonolaatuisista kaapeloinneista kiinteistön sisällä. Usein kiinteistön puhelinkaapeloinnit ovatkin yhtä vanhoja kuin kiinteistöt itse ja niitä uusitaan äärimmäisen harvoin. Seuraavaksi esitän parannusehdotuksia, joiden avulla esiteltyjä ongelmia voidaan korjata.

Attenuaatiota voitaisiin vähentää muuttamalla laitteistojen sijoitusta kiinteistöissä. Sen sijaan, että kaikkien talojen DSLAMit asennettaisiin kiinteis-

tön pääjakamoon, voitaisiin jokaisen kiinteistön talon DSLAMit asentaa talojen omiin välijakamoihin. Tällöin signaali voimistuisi jokaisen talon välijakamossa kulkiessaan laitteen lävitse. Lisäksi jokaiseen taloon voisi lisätä oman ADSL-reitittimen, jolle voitaisiin jakaa pääjaosta oma linja yhden DSLAmin kautta. Nykyisessä tilanteessa kiinteistöön tulee yksi ADSL-liittymä, jota jaetaan koko kiinteistön käyttäjille pääjakamosta käsin. Mikäli linja jaettaisiin osiin, voitaisiin varmistaa kiinteistön jokaiselle talolle tietty osa saatavilla olevasta siirtokapasiteetista. Kaistan varaus voidaan tosin tehdä DSLAMien porttiasetuksista, kuten LanWorldin kohteissa nykyään tehdäänkin.

Kustannussäästöä voitaisiin hakea tutkimalla mahdollisuutta muuttaa ADSL-kohteet siltaavista reitittäviksi. Mikäli kohteen muuttaminen reitittäväksi onnistuu runko-operaattorin puolesta, ei enää tarvitsisi ostaa erikseen runko-operaattorilta julkisia IP-osoitteita. Julkisten osoitteiden sijaan voitaisiin toimia samalla tavoin kuin Ethernet-kohteissa:. ottamalla käyttöön harmaan sarjan IP-osoitteet. Esimerkkinä olen aiemmin käyttänyt verkkoa 192.168.1.0/24. Huonona puolena reitittävässä mallissa on rasituksen lisääntyminen LanWorldin runkoyhteyttä ylläpitävällä reitittimellä.

11 Yhteenveto

Olen käsitellyt opinnäytetyössäni pääpiirteittäin tärkeimmät LanWorld Finlandin käyttämät yhteystyypit. Olen pyrkinyt käsittelemään asioita, jotka koen oleellisiksi huomioonottaen LanWorldin työntekijöiden tarpeet. Aiheen moniulotteisuuden vuoksi jouduin jättämään useita osa-alueita pois, ja tyytymään aiheen kannalta pintaraapaisuun opinnäytetyössäni. Toivoisin kuitenkin, että LanWorldin työntekijät kokisivat opinnäytetyöni kelvollisena johdatuksena esiteltyjen erilaisten verkkotekniikoiden käytön perusteisiin. Koen, että parhaimmassa tapauksessa käsillä olevan kaltainenkin, lyhyt johdatus aiheeseen voi johtaa innostukseen perehtyä aiheeseen syvemmin, ja että se puolestaan voisi parantaa muun muassa teknisen tuen vianmäärityksen tehokkuutta.

LanWorld Finland Oy:n nykyiset verkkoratkaisut ovat toimivia, mutta toisaalta suunnitteluvaiheessa ei välttämättä ole otettu huomioon mahdollisia käyttäjistä johtuvia ongelmia, kuten esimerkiksi DHCP-ongelmaa, jota käsiteltiin Ethernet-osiossa. Lukujen yhteydessä pyrin tuomaan esille sellaisia parannusehdotuksia, jotka olisi mahdollisia toteuttaa yksinkertaisesti ja ilman mainittavia lisäkuluja. ATM- ja ADSL-osiossa esittelemieni tekniikoiden perusteet ja kiinteistöverkkoihin kohdistuvat parannusehdotukset voivat auttaa yritystä tehostamaan verkkojensa toimivuutta. PPP-osion avulla yrityksen työntekijät voivat tutustua PPPoA:n ja PPPoE:n perusteisiin ja keskinäisiin eroihin. Kaiken kaikkiaan näkisin, että tuleva runkoyhteyksien muutos ei tule näkymään yrityksen verkoissa suurella tavalla. Tämä johtuu lähinnä siitä, että PPP-yhteyksiä ei käytetä kuin nimenomaan runkoyhteyksissä. Asiakkaiden yhteydet säilyvät muuttumattomina myös uudistuksen jälkeen.

Koen opinnäytetyössäni saavuttaneeni itse itselleni asettamat tavoitteet kohtuullisen hyvin ja onnistuneeni perehtymään aiheeseen asettamistani näkökulmista käsin. Aloitin opinnäytteen työstämisen heinäkuussa 2006. Varsinaisen kirjoittamisen aloitin elokuun puolivälin paikkeilla, ja kirjoitusprosessi on sujunut, muutamaa hiljaisempaa kautta lukuunottamatta, melko kivuttomasti. Luonnollisesti uusi kokoaikatyö on tuonut oman vaikutuksensa opinnäytetyöprojektiini, mutta aikaisemmin suunnittelemani aikataulu piti kuitenkin paikkansa yllättävän hyvin. Toisaalta olin ottanut aikataulua suunnitellessani huomioon sen, etten pystyisi käyttämään opinnäytteeseen päivittäin kovinkaan runsaasti aikaa.

Alkuperäiset suunnitelmat tiiviimmästä yhteistyöstä LanWorldin kanssa opinnäytetyöni osalta muuttuivat useista syistä: jo esiin ottamani uusi kokoaikatyöni, mutta lisäksi myös kontakti- ja tukihenkilöni siirtyminen LanWorld Oy:stä toisen yrityksen palvelukseen olivat kenties merkittävimpiä tällaisista seikoista. Käytännössä tämä tarkoitti siis sitä, että jouduin työstämään kehitysideoitani hyvin pitkälti omien kokemuksieni, mielenkiintoni ja

osaamiseni pohjalta. Tämä antoi toisaalta melko lailla vapaat kädet opinnäytetyöni tekemisessä, mutta toisaalta olisin ollut vielä halukas osallistumaan myös ehdotuksieni mahdolliseen kokeiluun tai käyttöönottoon.

Nykytilanne LanWorld Finland Oy:ssä on muuttunut opinnäytetyön aloittamisen jälkeen merkittävästi. Yritys on yhdistymässä WLANnetin kanssa. Yhdistyminen tulee todennäköisesti muuttamaan LanWorldin käyttämiä verkkoratkaisuja, mutta lähinnä ainoastaan runkoyhteyksien osalta. Itse kiinteistöissä käytettävät verkkoratkaisut tulevat todennäköisesti pysymään samoina, jolloin esille tuomani parannusehdotukset ovat käyttökelpoisia myös muutoksien jälkeen.

Lähdeluettelo

Anttila, A. 2000. TCP/IP tekniikka. Juva:WSOY

Granlund, K. 2003. Tietoliikenne. Docendo Finland Oy

Ginsburg, D. 2000. ADSL. Helsinki: Oy Edita Ab

Hedeman, G. 2000. Tietoverkon perusteet, Gunvald Hedeman. Vantaa: Tummavuoren kirjapaino Oy

Hölttä, P., Hämeen-Anttila, R. ja Niinoja, S. 1996. Tietoliikennejärjestelmät Helsinki : Oy Edita AB

Jaakohuhta, H. 2003. Local area networks Ethernet. Edita publishing Inc

Wikipedia 2006. PPPoA [Online][Viitattu 23.10.2006]. http://en.wikipedia.org/wiki/PPPoA

IETF 2000. RFC 2974 [Online][Viitattu 28.10.2006]. http://www.ietf.org/rfc/rfc2974.txt

IETF 1999. RFC 2561 [Online][Viitattu 25.10.2006]. http://www.ietf.org/rfc/rfc2516.txt

IETF 1998. RFC 2364 [Online][Viitattu 26.10.2006]. http://www.ietf.org/rfc/rfc2364.txt

IETF 1994. RFC 1661 [Online][Viitattu 25.10.2006]. http://www.ietf.org/rfc/rfc1661.txt