VALTAKUNNALLINEN YRITYSVERKKO

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Esko Salomaa

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

SALOMAA, ESKO: Valtakunnallinen yritysverkko

Tietotekniikan opinnäytetyö, 42 sivua, 14 liitesivua

Kevät 2006

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee valtakunnallisen yritysverkon toimitusta Finnetin tuotteilla. Työssä tutustutaan uuteen MPLS-tekniikkaan ja sen antamiin mahdollisuuksiin yritysverkon toteuttamisessa. Tarkoituksena on kertoa yritysverkon toteuttamisesta erään yritysverkkoprojektin pohjalta, jossa yhdistetään noin 60 toimipistettä. Yritysverkkoprojekti on Tampereen Puhelimen asiakkaalle rakennettava MPLS-verkko.

Opinnäytetyössä perehdytään ATM- ja MPLS-tekniikoiden teoriaan ja näistä tekniikoista kehitettyihin tuotteisiin. MPLS on uusi, uraauurtava tekniikka, jonka käyttö kasvaa kovaa vauhtia. Yritysverkkojen toteutustapana monipuolinen ja mukautuva MPLS on varteenotettava kilpailija iäkkäälle ATM-tekniikalle. Yritysverkko toteutettiin MPLS-tekniikalla. Valintaa tuki monta seikkaa, esille nousi etenkin verkon joustavuus kytkennöissä. Perinteiset VPN-tekniikat toimivat kahden pisteen välillä kuten myös ATM käytettäessä PVC-kytkentää. Usean toimipisteen yhdistäminen näillä tekniikoilla vaatii tehokkaan keskittimen.

Tarkastellussa projektissa liitetään yhteen 60 liittymää. Aluksi verkon topologia on tähtimäinen eivätkä toimipisteet näe toisiaan. Tämä kuitenkin tulee muuttumaan IP-puheluiden eli VoIP:n tullessa mukaan kuvioon.

Uuden verkon käyttöönotto tapahtui nopeassa aikataulussa syksyllä 2005. Toteutusta helpotti se, ettei asiakkaalla ollut pohjalla minkäänlaista verkkoa yhdistämässä toimipisteitä. Vaikeuksia aiheuttivat muiden puhelinyhtiöiden vaihtelevat toimintatavat MPLS-toimituksissa.

Avainsanat: MPLS, ATM, yritysverkko

Lahti University of Applied Sciences
Faculty of Technology

SALOMAA, ESKO: Nation-wide corporate network

Bachelor's Thesis in Telecommunications, 42 pages, 14 appendices

Spring 2006

ABSTRACT

This thesis deals with the creation of a nation-wide corporate network with Finnet products. The thesis focuses on the new MPLS technology and its possibilities. The empirical part was the construction of corporate network, which consist of about 60 offices. The corporate network was built for a client of Tampereen Puhelin.

The thesis presents into the theory of ATM and MPLS as well as products that have been developed from these technologies. MPLS is a groundbreaking, new technology whose usage grows at an increasing rate. Being a versatile and adaptive technology, it is a tough adversary for the aged ATM.

The corporate network was carried out with MPLS. Many factors supported this choice, especially adaptive topology. Traditional VPN technologies and ATM PVC operate between two points. It requires a powerful hub to connect many offices into a shared network. In this network project there were over 60 offices, which were to be connected together.. At first the topology is starshaped and the offices do not see each other. The topology will be changed to full-mesh when it is time to add VoIP into the network.

The new corporate network was taken in use with a tight schedule in fall 2005. The implementation was easy because there was no existing network connecting the offices. Other telephone companies caused difficulties with their variable operational habits concerning MPLS deliveries.

Keywords: MPLS, ATM, corporate network

SISÄLLYS

LYHENNELUETTELO

LYHENNELUETTELO

AAL = ATM Adaption Layer, ATM sovituskerros
ABR = Available Bit Rate, käytettävissä olevan nopeuden yhteydet
ADSL = Asymmetric Digital Subscriber Line, asynkroninen nopea tilaajayhteys
AES = Advanced Encryption Standard, kehittynyt salausstandardi
AH = Autenthication Header, autentikointi otsikko
ATM = Asynchronous Transfer Mode, asynkroninen tiedonsiirto
BGP = Border Gateway Protocol, reititysprotokolla
CBR = Constant Bit Rate, vakionopeuden yhteydet
CE = Customer Edge, verkon tilaajarajapinta
CLP = Cell Loss Priority, soluhukkaprioriteetti
DES = Data Encryption Standard, lohkosalaukseen perustuva salausalgoritmi
ESP = Encapsulating Security Protocol, kapsuloiva suojausprotokolla
FTP = File Transfer Protocol, tiedonsiirtoprotokolla
GRE = Generic Routing Encapsulation, IP-tunnelointiprotokolla
HEC = Header Error Check, otsikon oikeellisuuden tarkistuskenttä
HTTP = Hyper Text Transfer Protocol, www-selaimen käyttämä protokolla, jolla siirretään tieto selaimen ja www-palvelimen kesken
ICMP = Internet control message protocol, TCP/IP-pinon kontrolliprotokolla, jolla lähetetään nopeasti viestejä koneesta toiseen.
IETF = Internet Engineering Task Force, standardointielin
IGB = Interior Gateway Protocol, sisäinen reititysprotokolla
IKE = Internet Key Exchange, IETF:n avaintenhallintaprotokolla
IP = Internet Protocol, Internet protokolla
IPsec = Internet Protocol Security, IP-liikenteen suojaaminen salaamalla,
ISAKMP = Internet Security Association and Key Management Protocol, suositus turvallisuuden tunne ja avaintenhallintaprotokollaksi
ISDN = Integrated Services Digital Network, piirikytkentäinen puhelinverkkojärjestelmä
ISO = International Organization for Standardization, kansainvälinen standardointielin
ITU-T = International Telecommunications Union, kansainvälinen telekommunikointiunioni

L2F = Layer 2 Forwarding, 2-kerroksen edelleenlähetys

L2TP = Level 2 Tunneling Protocol, tunnelointiprotokolla

MPLS = Multiprotocol label switching, reititystekniikka, jossa IP-paketin eteen lisätään lyhyt kenttä joka sisältää mm. reititystiedon.

NIST = National Institute of Standards and Technology, Amerikan yhdysvaltojen kauppaministeriön kansallinen standardoinnin ja teknologian laitos

NNI = Network Node Interface, verkko-verkko liitäntä

nrt-VBR = non real time Variable Bit Rate, epätosiaikaiset vaihtelevan nopeuden yhteydet

OSI = Open Systems Interconnection, Kansainvälisen standardointijärjestön ISO:n malli avointen tietojärjestelmien yhteenliittämiseksi.

OSPF = Open Shortest Path First routing protocol, reititysprotokolla

PE = Provider Edge, verkon operaattorirajapinta

PPP = Point-to-Point Protocol, protokolla jonka avulla luodaan kahden pisteen välinen yhteys, useimmiten IP

PPTP = Point-To-Point Tunneling Protocol, protokolla VPN-liikenteen tunnelointiin

PT = Payload Type, ATM- otsikon kenttä, joka ilmaisee hyötykuorman tyypin

PVC = Permanent Virtual Channel, kiinteä virtuaaliyhteys

RIP = Routing Information Protocol, reititysprotokolla

rt-VBR = real time Variable Bit Rate, tosiaikaiset vaihtelevan nopeuden yhteydet

SA = Security Association, turvallisuusassosiaatio

SKEME = Versatile Secure Key Exchange Mechanism For Internet, eräs vaihtoehto IPsecin avaintenvaihtoprotokollaksi

SMTP = Simple Mail Transfet Protocol, sähköpostin siirtoprotokolla

SNMP = Simple Network Management Protocol, verkon valvonta- ja hallintaprotokolla IP ympäristössä

SPI = Security Parameter Index, yksilöi turvallisuusassosiaation

SSH = Secure Shell, Suosittu tapa muodostaa salattu yhteys kahden laitteen välillä

SVC = Switched Virtual Channel, kytketty virtuaaliyhteys

SYN = Synchronize, synkronoitu

SYN/ACK = Synchronize/ Acknowledgement, TCP:hen liittyvä kuittaus lähettäjälle tietopaketin vastaanottamisesta

TCP = Transmission Control Protocol, luotettava yhteydellinen tiedonsiirtoprotokolla IP:lle

UBR = Unspecified Bit Rate, määrittelemättömän nopeuden yhteydet

UDP = User Datagram Protocol, yhteydetön tiedonsiirtoprotokolla IP:lle

UNI = User Network Interface, käyttäjä-verkko liitäntä

VCC = Virtual Channel Connection, virtuaalikanavayhteys

VCI = Virtual Channel Identifier, virtuaalikanavan tunnistin

VLAN = Virtual Local Area Network, virtuaalilähiverkko

VoIP = Voice over IP, Yleistermi IPn päällä kuljetettavalle puheelle

VPI = Virtual Path Identifier, virtuaaliväylän tunnistin

VPN = Virtual Private Network, yleisen dataverkon kautta luotu salattu yhteys

VRF = VPN Routing and Forwarding Table, VPN reititystaulu

WAN =Wide Area Network, laaja-alueverkko

1 JOHDANTO

1.1 Taustaa

Nykyään Internet on arkipäivää. Yritys, jolla ei ole Internet-yhteyttä, antaa kilpailijoilleen merkittävän kilpailuedun. Vielä 90-luvun puolivälissä yrityksistä vain suurimmat ja teknologiapainotteiset toteuttivat toimipisteiden välisiä datayhteyksiä valtakunnallisesti tai kansainvälisesti. Tänä päivänä tietoliikenteen avulla hoidetaan sekä yrityksen asiakassuhteita että välitetään yrityksen sisäistä informaatiota. Erityisesti yrityksen sisäisessä tietoliikenteessä oma, yksityinen yritysverkko on tarpeellinen. Sen sisällä voi toimia erilaiset työnohjaus-, valvonta- ja hallintajärjestelmät. Myös puhelinliikenne voidaan hoitaa verkon kautta VoIPin muodossa. Mahdollisuudet ovat varsin laajat.

Yrityksen julkisuuskuvaa hoidetaan www-sivuilla, joka on halpa tapa lisätä yrityksen näkyvyyttä. Omalla www-sivulla yritys voi kertoa esimerkiksi historiastaan, tuotteistaan ja palveluistaan. Säästöt ovat varsin suuria verrattaessa siihen, miten paljon maksaisi jakaa sama tieto paperimuodossa. Internetissä oleva tieto on näkyvillä koko maailmalle, ellei toisin määritellä. Paperimedia taasen jaetaan yleensä vain varsin paikallisesti.

Lisääntyneen Internet-käytön myötä myös verkkokapasiteettia tarvitaan lisää. Tämä näkyy mm. kuituyhteyksien lisääntymisenä, josta hyvä esimerkki on Helsingin Arabianrannan alueverkko, jonka rakentaa Helsingin Energia. Alueella tulee olemaan 10000 asukkaan ja satojen yritysten asiakaskunta. Kuiturunkoverkon nopeus on 1 gigabitti ja asiakkaille tarjotaan 10/10 megabitin liittymiä. (LAN&WAN 2006.)

1.2 Opinnäytetyön tavoite ja rajaukset

Tämä opinnäytetyö käsittelee Finnetin kahta palvelua, Lan-to-Lania ja MPLS:ää. Palvelut ovat tekniikaltaan erilaisia, ja opinnäytetyön tarkoituksena on selvittää tekniikoiden soveltuvuus esimerkkinä olevaan Tampereen Puhelimen

yritysprojektiin. Opinnäytetyössä käydään lisäksi läpi ATM (Asynchronous Transfer Mode)- ja VPN (Virtual Private Network) -tekniikat, sillä Lan-to-Lan on rakennettu ATM-tekniikan päälle, kun taas VPN-protokolliin kuuluva MPLS uudempana tekniikkana käyttää ATM- ja IP -tekniikoiden ominaisuuksia. Työssä tutustutaan myös muihin yleisesti VPN-yhteyksissä käytettäviin protokolliin.

1.3 Finnet-yhtiöt ja Tampereen Puhelin

Finnet-ryhmään kuuluu 35 paikallista puhelinyhtiötä, Finnet Oy ja Finnet-liitto ry. Finnet-ryhmä työllistää Suomessa noin 5 100 henkilöä. Finnet-ryhmän valtakunnallisista liiketoiminnoista vastaa Finnet Oy tytäryhtiöineen. Finnet Oy:n omistus on Finnet-ryhmän puhelinyhtiöillä. (Finnet Oy 2006a.)

Finnet-ryhmän yhtiöiden elinkeino ja toimintapoliittinen etujärjestö sekä yhteistyöfoorumi on nimeltään Finnet-liitto ry. Finnet-liiton tehtäviin kuuluu vastata jäsenistönsä edunvalvonnasta sekä kansallisesti että kansainvälisesti. (Finnet Oy 2006a.)

Finnetin tarjoamat palvelut antavat erilaisia mahdollisuuksia koko valtakunnan kattavan yritysverkon rakentamiseen. Tampereen Puhelin on Finnet-yhtiöihin kuuluva varsin tuore yhtiö, jonka omistaa Pohjois-Hämeen Puhelin, Ikaalisten-Parkanon Puhelin sekä Satakunnan Puhelin. Tämä opinnäytetyö tehdään erään Tampereen Puhelimen yritysprojektin pohjalta. Projektissa hyödynnetään Finnetin yritysverkkopalvelua mm. maksuliikenteessä.

2 TIETOLIIKENTEEN PERUSMALLIT

2.1 OSI-malli

Koska opinnäytetyö keskittyy pitkälti erilaisiin protokolliin ja standardeihin, on tarpeen kertoa myös OSI (Open System Interconnection)- ja TCP/IP-malleista. Kansainvälinen standardointiorganisaatio ISO (International Organization for Standardization) kehitti 1980-luvun alussa seitsenkerroksisen pinomallin, jonka oli tarkoitus poistaa yhteensopimattomuus ongelmat eri verkoissa. Raskaudestaan johtuen malli ei kuitenkaan tullut erityisen suosituksi, ja sitä käytetäänkin lähinnä ohjenuorana. (Keogh 2001, 64.)

Laitteet käyttävät alemman kerroksen palveluja hyväkseen siirtäessään tietoa. Jokainen kerros on oma itsenäinen kokonaisuutensa, jota voidaan kehitellä muista osista riippumatta. On myös huomattava, että jokainen kerros lisää oman otsikkonsa varsinaiseen dataan, näin ollen varsinaisen hyötykuorman suhde siirrossa tarvittaviin tietoihin pienenee. (Keogh 2001, 64.)

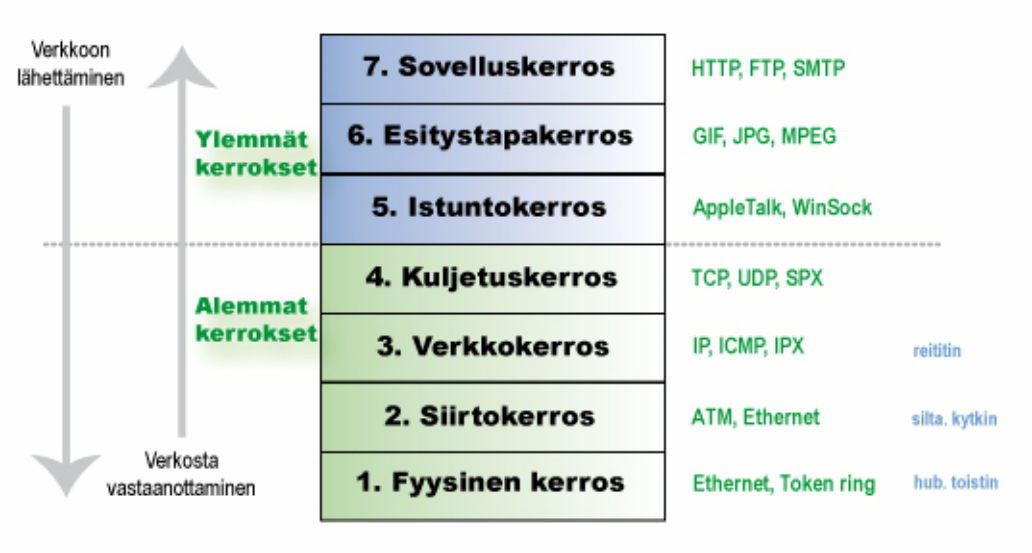
OSI-mallin kerrokset ovat Keoghin (2001, 64) mukaan:

1. **fyysinen kerros** (Physical layer)
2. s**iirtoyhteyskerros** tai siirtokerros (Data Link layer)
3. v**erkkokerros** (Network layer)
4. **kuljetuskerros** (Transport layer)
5. **istuntokerros** (yhteysjakso, Session layer)
6. e**sitystapakerros** (Presentation layer)
7. **sovelluskerros** (Application layer)

Fyysisen kerroksen tehtävänä on käsitellä sähköimpulsseja, valoa tai muuta fyysistä tekniikkaa. Siirtoyhteyskerros hoitaa paikallisen lähiverkon laitteiden välisen liikennöinnin. Verkkokerroksen tehtävänä on hoitaa globaalireititys sekä etsiä Internetistä kohdekone. Kuljetuskerros pitää huolen siitä, että paketit tulevat perille ja ne järjestetään oikeaan järjestykseen. Kuljetuskerros huolehtii lisäksi myös vuonhallinnasta. Istuntokerroksen tehtävänä on huolehtia useiden yhdessä yhteydessä kulkevien istuntojen multipleksoinnista. Esitystapakerros muuttaa

datan käyttäjälle sopivaan muotoon. Sovelluskerrokseen sijoittuvat käyttäjälle näkyvät sovellukset. (Keogh 2001, 64-65.)

Alla olevassa kuviossa näkyy kerrosten sijoittuminen ylempiin ja alempiin kerroksiin sekä esimerkkejä kerroksilla toimivista protokollista.



KUVIO 1. OSI-malli ja eri kerroksilla toimivia protokollia (Wikipedia 2006)

TAULUKKO 1. OSI-mallin tapahtumat kerros kerrokselta. (Keogh 2001, 64.)

Lähettävä kerros	**Tapahtuma**	**Vastaanotta-va kerros**	**Tapahtuma**
7. Sovellus	muunnos sovelluksen käyttämästä muodosta välimuotoon	7. sovellus	muunnos välimuodosta sovelluksen käyttämään muotoon
6. Esitystapa	salakirjoitetaan pakataan	6. esitystapa	salaus avataan pakkaus puretaan

(jatkuu)

TAULUKKO 1. (jatkuu)

5. Istunto	aloittaa istunnon, tarkistaa verkko-oikeudet, lisää tarkistuskohtia, päättää istunnon	5. istunto	tarkistuskohdat poistetaan
4. Kuljetus	luo paketit	4. kuljetus	pakettien seuranta, pyytää pakettien uudelleenlähetystä, purkaa paketit
3. Verkko	muuntaa loogisen osoitteen fyysiseksi osoitteeksi, selvittää parhaan reitin verkon läpi kohteeseen	3. verkko	poistaa osoitteet
2. Siirto	sijoittaa paketit verkkokehyksiin, asettaa CRC:n, lähettää kehyksiä uudelleen	2. siirto	selvittää, onko kehys osoitettu kyseiselle tietokoneelle, selvittää tapahtuuko tiedonsiirtovirheitä, vastaanottaa kehyksen kuittauksen, poistaa kehyksen ja CRC:n
1. Fyysinen	lähettää kehyksen	1. fyysinen	vastaanottaa kehyksen

2.2 TCP/IP-malli

Internet Protokolla (IP) on koko Internetin ydin, mutta se ei yksinään pysty tarjoamaan kaikkia tarpeellisia palveluita. Se vuoksi on kehitetty TCP/IP-protokollaperhe. (Keogh 2001, 139.)

TCP/IP tarkoittaa IP:n ympärille rakentunutta protokollaperhettä, jossa IP toimii verkkokerroksella ja Transmission Control Protocol (TCP) tai User Datagram Protocol (UDP) kuljetuskerroksella. TCP on yhteydellinen tiedonsiirtoprotokolla ja UDP vastaava yhteydetön. Sovelluskerroksella toimivat esimerkiksi Simple Network Management Protocol (SNMP) ja File Transfer Protocol (FTP). (Keogh 2001, 139-140.)

TCP/IP on pyritty tekemään yksinkertaiseksi, ja siinä onkin vähemmän kerroksia kuin OSI-mallissa. TCP/IP:ssä on vain neljä kerrosta OSI-mallin seitsemää vastaan. TCP/IP-mallin kerrosten tehtävät ovat lähes samat kuin samalla kohdalla kuvassa olevien OSI-kerrostenkin. (Comer 2002, 186.)

Kuviossa 2 on esitetty OSI-mallin kerrosten sijoittuminen TCP/IP-mallin kerroksiin nähden.

KUVIO 2. TCP/IP-malli verrattuna OSI-malliin (Heikkilä 2002, 40)

2.2.1 TCP- ja IP-protokollat

IP-protokolla on verkkokerroksen protokolla. Sen tehtävänä on huolehtia IP-pakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa. Voidaan sanoa, että se on myös koko Internetin ydin, koska se on ainoa asia, joka yhdistää

kaikkia Internetiin liitettyjä koneita. IP-paketti ei välttämättä ole pienin verkossa kuljetettava yksikkö vaan joissakin tapauksissa se joudutaan jakamaan vielä pienemmiksi osapaketeiksi (fragmenteiksi). Tällä hetkellä Internetissä on yleisimmin käytössä IP-protokollan neljäs versio, IPv4. (Ogletree 2001, 232.)

IP-paketit toimitetaan verkossa perille IP-osoitteiden perusteella. IP-osoite on tavallisesti muotoa "192.168.11.1" (IPv4) tai 2002:a00::260:1dff:fe22:5a85/64 (IPv6). IP-pakettien perille toimittaminen on reitittämistä, ja sen tekevät reititysprotokolliin perustuvat reitittimet. (Comer 2002, 610.)

IPv6-version on jo kauan odotettu korvaavan nykyinen IPv4-versio. Toistaiseksi IPv6:n käyttö on kuitenkin vähäistä, vaikka se on saatavissa useimmille tietokoneille. IPv6-version tärkeimpänä uudistuksena on osoitteiden pidentäminen. Uudistuksen myötä osoitettavia tietokoneita voi olla paljon nykyistä neljää miljardia enemmän. Osoitteenmuunnosratkaisut nykyisessä IPv4-versiossa ovat auttaneet osoitteiden riittävyydessä ja vähentäneet näin tarvetta siirtyä käyttämään uutta IPv6-versiota. Oman hankaluutensa IPv6-version käyttöönottoon tuovat myös vanhat laitteet, sillä IPv6-tietoliikennettä ei pystytä käsittelemään sellaisilla tietokoneilla ja reitittimillä, jotka tukevat vain IPv4:ää. (Comer 2002, 610.)

TCP-protokolla on 4. kerroksen tietoliikenneprotokolla, jolla luodaan yhteyksiä Internet-tietokoneiden välille. Esimerkiksi www-sivujen hakemisessa selaimen ja palvelimen välille muodostetaan TCP-yhteys. Yhteydessä selain lähettää tavujonoja palvelimelle ja palvelin tavujonoja selaimelle. TCP-protokollan tehtävänä on huolehtia, että yhteyden tavujonot pilkotaan IP-paketeiksi ja että paketit saapuvat perille oikeassa järjestyksessä. TCP-protokolla lähettää myös uudelleen matkalla kadonneet paketit. (Comer 2002, 209.)

TCP-yhteys sisältää kolme vaihetta. Yhteyden muodostamisessa asiakaspään laite lähettää ensiksi palvelinpään laitteelle SYN-paketin, seuraavaksi palvelinpään laite vastaa SYN/ACK-paketilla. Asiakaspään laitteen vastattua ACK-paketilla, datan siirto voi alkaa. (Comer 2002, 211-212.)

Tiedon siirtovaiheen aikana datan eheyden tarkistamisessa käytetään useita eri mekanismeja. Sekvenssinumerointia käytetään TCP-pakettien järjestyksen varmistamiseen. Virheiden tarkistusta varten ovat tarkistussummat sekä hukattuja paketteja ja viiveitä varten ajastimet ja tunnistimet. Datavirrasta tunnistetaan kullekin yhteydelle kuuluvat paketit sekvenssinumeroiden avulla. Numerot jaetaan yhteyden muodostuksen aikana. Lähettäjä saa kuittauksen jokaisesta vastaanotetusta TCP-paketista. TCP-protokolla lähettää paketin uudestaan, jos kuittausta ei tule. (Comer 2002, 255.)

Yhteys päätetään kun molemmat osapuolet lähettävät FIN-paketin ja molemmat kuittaavat sen ACK-paketilla. TCP-protokollan varaan on rakennettuja useita protokollia. Näitä ovat esimerkiksi HTTP, SMTP, Telnet, SSH sekä FTP. (Comer 2002, 240-244.)

2.3 Mallien erot

OSI- ja TCP/IP-mallin välillä on kaksi merkittävää eroa. Ensimmäinen ero on tapa varmistaa tiedonsiirto. Toinen ero koskee järjestelmän ”älyn” sijaintia.

OSI-malli havaitsee ja käsittelee virheet kaikissa kerroksissa. Siirtoyhteyskerroksen mutkikkailla protokollilla varmistetaan pakettikytkimen ja työaseman virheetön tiedonsiirto. Siirretyt paketit sisältävät tarkistussumman, ja vastaanottaja kuittaa vastaanottamansa paketin. Kerroksen algoritmit varmistavat tietojen säilymisen siirrettäessä. Verkkokerroksella suoritetaan verkkoon lähetettävien pakettien virheenkäsittely tarkistussummia ja uudelleenlähetystekniikoita käyttämällä. Lopuksi kuljetuskerros varmistaa päätepisteiden välisen siirtotien siten, että lähettäjä voi varmistaa tiedon saapumisen suoraan vastaanottajalta. (Comer 2002, 185.)

TCP/IP-malli jättää luotettavan tiedonsiirron toteuttamisen päätepisteiden huoleksi. Verkko mitoitetaan kuorman mukaan eikä kadonneita tietoja yritetä palauttaa verkkokerroksen protokollilla. Virheentarkistus ja uudelleenlähetys hoidetaan kuljetuskerroksessa. Paketteja katoaa väistämättä, ja

korjaustoimenpiteet tehdään lähettävässä ja vastaanottavassa työasemassa. TCP/IP-malli keskittää luotettavan tiedonsiirron edellyttämät toiminnot kuljetuskerrokseen. (Comer 2002, 186.)

Toinen ero TCP/IP- ja OSI-mallin välillä on tietokoneiden osallistuminen verkon ohjaukseen ja hallintaan. OSI-mallin mukainen verkko on monimutkainen, itsenäinen järjestelmä, johon voidaan kytkeä melko yksinkertaisia tietokoneita. TCP/IP-mallin mukainen verkko on OSI-verkkoon verrattuna yksinkertainen järjestelmä, jossa virheentarkistus ja -korjaus, osa reitityspäätöksistä ja verkonhallinnasta tehdään TCP/IP-verkkoon liitetyissä tietokoneissa. (Comer 2002, 186.)

3 LÄHIVERKKOJEN YHDISTÄMINEN

3.1 Taustaa

Tiedon siirtyminen nopeasti, luotettavasti ja turvallisesti yrityksen toimipisteiden välillä on edellytys liiketoiminnan onnistuneelle hoitamiselle. Lähiverkkojen yhdistäminen yhtenäiseksi kokonaisuudeksi tuo toimintaan joustavuutta ja tehokkuutta. Finnetin tuotteissa on kaksi palvelua lähiverkkojen yhdistämiseen jotka soveltuvat käytettäväksi yritysverkkoprojektissa, joita ovat uusi MPLS-palvelu ja vanhempi Lan-to-Lan. Jälkimmäinen on käytännössä ATM PVC-kytkentä tähtimuotoisessa verkossa.

3.2 ATM

ATM tulee sanoista Asynchronous Transfer Mode eli tahdistamaton siirtotapa. Periaatteessa ATM on tietoliikennekuri, tapa pilkkoa bittivirta pieniksi, tasakokoisiksi soluiksi, joita voidaan käsitellä äärimmäisen nopeasti ja limittää joustavasti käytettävissä olevaan kaistaan. Solujen tasakokoisuus on keskeinen asia ATM:ssä. Kiinteämittaisten solujen ansiosta voidaan siirto toteuttaa monimutkaisenkin verkon läpi erittäin nopeasti. (Comer 2002, 358.)

ATM:ää käyttämällä kaikki informaatio datasta ääneen ja videokuvaan mahtuu samanaikaisesti samaan siirtokanavaan. ATM on siis tapa sovittaa erilaiset liikenteen muodot samalla kaistalle.

3.2.1 ATM-verkon rakenne

ATM-kytkimet ja niitä yhdistävät virtuaaliyhteydet muodostavat kokonaisuudessaan ATM-verkon. Kytkimien perustoiminta on yksinkertaista. Ne vastaanottavat ATM-soluja yhdestä liitännästään ja lähettävät solut eteenpäin toista liitäntää pitkin. Kytkimien toiminta perustuu kytkentätauluihin, joiden mukaan lähetys ja vastaanotto tapahtuu. ATM-verkoissa siirrettävät solut ovat

kaikki vakiomittaisia. Tällä menettelyllä solujen kytkentää voidaan yksinkertaistaa ja nopeuttaa. (Koivisto 1998.)

ATM-verkon datan ensisijaisia lähteitä ovat ATM-päätelaitteet. Päätelaitteet voivat olla mitä tahansa laitteita, jotka kytkeytyvät verkkoon aidolla ATM-liitännällä. Tämä liitäntä on nimeltään UNI (User Network Interface). ATM-kytkimet liittyvät toisiinsa puolestaan NNI-liitännällä (Network Node Interface). (Koivisto 1998.)

ATM-kytkin kytkee soluja yhdestä liitännästä toiseen seuraavasti:
Kytkin vastaanottaa solun. Se katsoo kyseisen liitännän VPI-taulukosta VPI-kentän arvon mukaan oikean VCI-taulun. VCI-kentän avulla kytkin hakee vastaavat uloslähtevät linkit, virtuaalipolun ja virtuaalikanavan. Kytkin sijoittaa kyseiseen soluun oikeat arvot ja lähettää sen eteenpäin. (Koivisto 1998.)

3.2.2 ATM-verkon ominaisuudet

Keskeisin ATM-verkon ominaisuus on sen kytkentäisyys. Ennen datan lähettämistä on muodostettava virtuaaliyhteys verkon yli lähettäjältä vastaanottajalle. ATM-verkoissa yhdistetään useista lähteistä tulevaa liikennettä. Yhteydet erotetaan Koiviston (1998) mukaan toisistaan seuraavasti:

- **Virtuaaliyhteydet** - yhdistävät kytkimet toisiinsa.
- **Virtuaalipolut** - erotellaan toisistaan virtuaalipolkutunnuksen (VPI) avulla.
- **Virtuaalikanavat -** erotellaan virtuaalikanavatunnuksilla (VCI).

Datansiirto tapahtuu virtuaaliyhteyksiä (VCC, Virtual Channel Connection) pitkin, jotka ovat päästä päähän yhteyksiä lähettäjältä vastaanottajalle. VCC toimii aina parina (yksi molempiin suuntiin), koska se on yksisuuntainen. Jokaisessa siirrettävässä solussa on kaksi tunnusta: VPI ja VCI. Tunnukset yksilöivät virtuaaliyhteyden, jolle solut kuuluvat. Koska solussa on vain 53 tavua, solussa

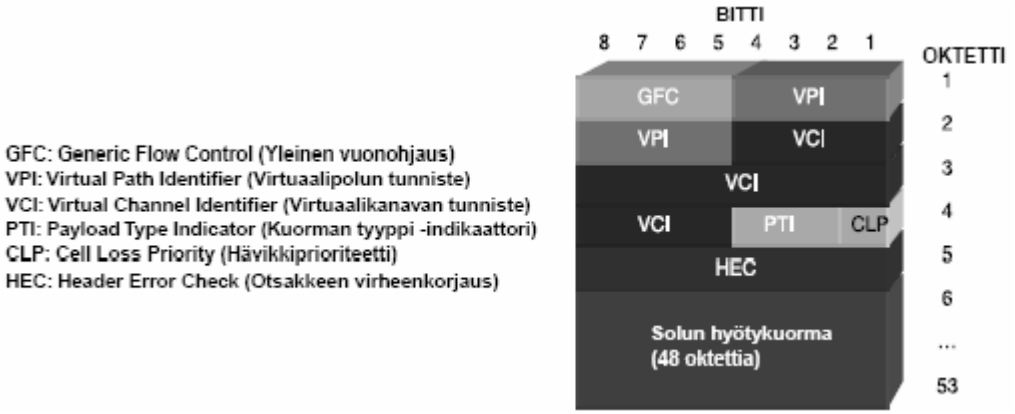
itsessään ei ole osoitetta. Osoitteen laittaminen soluun veisin liian suuren osan solun tavumäärästä. (Koivisto 1998.)

Virtuaaliyhteydet ryhmitellään virtuaalipoluiksi. Samaan virtuaaliyhteyteen kuuluvat solut siirretään lähettäjältä vastaanottajalle samaa reittiä. Tämän takia solut saapuvat perille aina samassa järjestyksessä, kuin missä ne on lähetetty. Ylemmän kerroksen protokollien ei tällöin tarvitse huolehtia oikean järjestyksen palauttamisesta. Ero on merkittävä perinteisiin reitittäviin verkkoihin verrattuna. Niissä samalle yhteydelle kuuluvat paketit voivat kiertää eri reittejä, ja siten myös perille saapuminen väärässä järjestyksessä on mahdollista. Vaikka järjestyksen säilyminen helpottaa ylempien protokollien toimintaa, ATM-verkot eivät ole yhtä joustavia virhetilanteiden hallinnassa kuin perinteiset IP-verkot. Ne pystyvät automaattisesti reitittämään paketteja vaihtoehtoisia reittejä alkuperäisen vikaantuessa. (Koivisto 1998.)

3.2.3 ATM-solu

Kaikki data siirretään ATM-verkoissa vakiomittaisissa soluissa. ATM-solu on kokonaisuudessaan 53 tavua. Solu koostuu 5 tavun mittaisesta otsikkokentästä ja 48 tavun mittaisesta informaatiokentästä (Koivisto 1998.)

Otsikko vaihtelee sen mukaan missä solu on luotu. Käyttäjä-Verkko eli UNI-liitännässä solun ensimmäinen kenttä on nimeltään Generic Flow Control. Verkko-Verkko eli NNI-liitännässä tätä kenttää ei ole, vaan VPI-kentässä on enemmän bittejä, mikä mahdollistaa suurempien VPI-arvojen käytön. Muuten solut ovat yhteneviä. Kuviossa 3 on esiteltynä ATM-solun rakenne sekä kenttien sijoittuminen ATM-solun sisällä. (Koivisto 1998.)



KUVIO 3. ATM-solu. (Ginsburg 2000, 59)

ATM-solussa on Koiviston (1998) mukaan seuraavat kentät:

VPI ja VCI: Virtual Path Identifier määrittelee virtuaalipolun, jolle solu kuuluu. Virtual Channel Identifier määrittelee käytetyn virtuaalikanavan. VCI määrittelee yhdessä VPI:n kanssa virtuaaliyhteyden, jota pitkin data siirretään. Alle 31 olevat VCI- ja VPI-arvot on varattu signalointi- ja muihin erityistarkoituksiin. Tyhjien solujen VPI:n ja VCI:n arvot ovat nollia.

PT: Payload Type -kentän erottaa varsinaisen käyttäjädatan hallinta- ja ohjausliikenteestä.

CLP: Cell Loss Priority -kentän arvo on 1, kun kyseisen solun prioriteetti on alhainen. Tietoa käytetään hyväksi ylikuormitustilanteissa, joissa kytkin ei pysty käsittelemään kaikkia soluja. Tällöin alemman prioriteetin solut poistetaan ensiksi.

HEC: Header Error Check -kenttä on yhden tavun eli kahdeksan bitin mittainen. Sen avulla tarkistetaan otsikon oikeellisuus. Koska oletuksena on, että ATM-verkossa on hyvät siirtoyhteydet, kenttä tarkastaa ainoastaan otsikon oikeellisuuden. Data-kentän oikeellisuutta ei tarkasteta ollenkaan.

3.2.4 PVC ja SVC

ATM muodostaa verkon tietokoneiden välille rajapinnan, jossa tietokoneet voivat kommunikoida keskenään. ATM-yhteyksien perustyypit ovat nimeltään PVC ja SVC. (Comer 2002, 356.)

Kiinteät virtuaaliyhteydet (PVC) muodostetaan manuaalisesti esimerkiksi verkonhallinnan toimesta. Tässä tapauksessa verkon operaattorit kirjoittavat kunkin virtuaaliyhteyden vaatimat kytkennät kaikkiin kytkimiin. Tämä tekee kuitenkin reitin muuttamisen työlääksi. Manuaalisten yhteyksien hyvä puoli on kuitenkin se, ettei kytkinten tarvitse tällöin keskustella keskenään ja ne voivat näin ollen olla eri valmistajan laitteita. (Koivisto 1998; Comer 2002, 356.)

Kytketyt virtuaaliyhteydet (SVC) verkko muodostaa automaattisesti itsestään. SVC-yhteydet eivät tarvitse manuaalista ohjausta, vaan ATM-verkon merkinanto huolehtii tarvittavien kytkentätietojen siirtymisestä kaikille yhteydellä oleville kytkimille. Tietokoneessa pyörivä ohjelma lähettää yhteyspyynnön paikalliselle kytkimelle. Pyyntö sisältää etätietokoneen osoitteen ja yhteyden parametrit. Sitten tietokone odottaa kunnes ATM-verkko muodostaa yhteyden. (Koivisto 1998; Comer 2002, 356.)

3.2.5 ATM-palveluluokat

Nykyiset ATM-palveluluokat mahdollistavat useiden eri palvelutasojen käyttämisen. Siirtokaista voidaan tällöin sovittaa eri liikennetyyppien vaatimusten mukaan. ATM-kerroksen tarjoamat palvelut on jaettu Ogletreen (2001, 571.) mukaan viiteen eri palveluluokkaan:

Vakionopeuden yhteydet (CBR, Constant Bit Rate). CBR-luokkaa käytetään sovelluksia varten, joilla on tiukat vaatimukset ajastuksen suhteen. Luokka varaa kiinteän enimmäismäärän siirtokaistaa sovelluksia varten. Tämä palveluluokka sopii reaaliaikaisille sovelluksille, kuten puheen, äänen ja videon siirtoon.

Tosiaikaiset vaihtelevan nopeuden yhteydet (rt-VBR, real-time Variable Bit Rate). Palveluluokka on tarkoitettu lähteille, joilla on tiukat ajastusvaatimukset, mutta jotka eivät pidä yllä aina samaa siirtonopeutta.

Epätosiaikaiset vaihtelevan nopeuden yhteydet (nrt-VBR, non-real-time Variable Bit Rate). Tämän palveluluokan yhteydet vastaavat edellisen luokan yhteyksiä siinä määrin, että liikenne on luonteeltaan purskeista. Tämän luokan tietoliikenne kuitenkin sietää jonkin verran viivettä. Sekä tosiaikaiset että epätosiaikaiset vaihtelevan nopeuden yhteydet soveltuvat esimerkiksi puheen siirtoon, kunhan käytetään tiivistystekniikoita.

Käytettävissä olevan nopeuden yhteydet (ABR, Available Bit Rate). Tämä palveluluokka on tarkoitettu sovelluksille, joilla ei ole tiukkoja aikavaatimuksia. Luokan sovellukset tyytyvät käyttämään saatavilla olevaa siirtokaistaa. Yhteydet voivat määritellä vähimmäissiirtokaistatason. Jos verkossa on saatavilla enemmän kaistaa, yhteydet kykenevät kaistan hyödyntämään.

Määrittelemättömän nopeuden yhteydet (UBR, Unspecified Bit Rate). Tämä palveluluokka on tarkoitettu sovelluksille, joilla ei ole erityisiä vaatimuksia yhteyden suhteen. Luokka sopii kiireettömään liikenteen siirtoon. Esimerkkeinä voidaan mainita tiedostojen siirrot ja sähköposti.

Vaikka sovellukset huolehtivatkin tiedonsiirrosta ATM-verkossa, ne eivät lue eivätkä kirjoita soluja. Tietokone kommunikoi ATM-verkon kanssa ATM:n sovituskerroksen (ATM Adaption Layer) kautta. Kerroksen tehtäviin kuuluvat esimerkiksi solujen katoamiseen tai korruptoitumiseen liittyvien virhetilanteiden käsittely. (Comer 2002, 358.)

ATM-verkoissa voidaan siirtää erityyppistä liikennettä, kuten puhetta, dataa ja liikkuvaa kuvaa. Erilaiset sovellukset vaativat verkolta erilaista palvelua. Esimerkiksi tiedoston siirrossa kaikki siirtovirheet on korjattava. Puhelinkeskustelussa taasen pienet virheet eivät vaadi korjausta, koska siirtoviiveen minimointi on paljon tärkeämpää. (Koivisto 1998.)

ATM-verkon sisäiset ominaisuudet on sovitettava mahdollisimman hyvin eri käyttötarkoituksia varten, jotta verkko voisi palvella erityyppisiä tiedonsiirtotarpeita. ATM:ssä sovituskerroksen eli AAL:n (ATM Adaption Layer) tehtävänä on huolehtia sisäisten ominaisuuksien sovituksesta. (Koivisto 1998.)

ITU-T:n standardin I.363 määrittelemät ATM -sovituskerroksen eri luokat ovat Koiviston (1998) mukaan:

AAL-0 Solut siirretään läpinäkyvästi mitään muuttamatta sovellukselta toiselle.
AAL-1 Vakionopeuksisessa palvelussa ja kiinteän yhteyden emuloinnissa tarvittavat toiminnat sisältyvät tähän luokkaan.
AAL-2 tarjoaa vaihtelevan nopeuden palvelua tosiaikaisille ja epätosiaikaisille vaihtelevan nopeuden yhteyksille.
AAL 3/4 perustuu frame relay -palveluun ja tarjoaa mm. virheiden havaitsemisen ja puskurikoon hallintapalveluita. Tämä luokka on suunniteltu erityisesti datasiirtoa varten.
AAL-5 on yleisin AAL-luokka. Luokka on yksinkertaistettu versio AAL3/4:stä.

3.3 MPLS

MPLS (Multi Protocol Label Switching) sijoittuu perinteisen siirtoyhteyskerroksen ja verkkokerroksen välimaastoon. MPLS-tekniikan pääajatuksena on tarjota pakettikytkentäisessä IP-verkossa piirikytkentäisen verkon kaltaisia palveluita. Perusideana on vähentää verkkokerrosreitityksen tarvetta liittämällä paketteihin lyhyitä etikettejä (label, suomennetaan myös leimaksi). Etikettien pohjalta päätös edelleenreitityksestä voidaan tehdä yksinkertaisesti ja nopeasti. Etiketit voidaan koodata joko siirtoyhteyskerroksen paketin sisään tai suoraan sen otsikkotietoihin (esim. ATM:ssä). (EUnet Finland 2006; Ericsson 2005.)

3.3.1 Tekniikka

MPLS-tekniikassa avainasemassa ovat runko- ja reunalaitteet. Palveluntarjoajan reunalaitteet ovat nimeltään PE-reitittimiä (Provider Edge). Runkoverkon muita reitittimiä kutsutaan P-reitittimiksi. Niihin luetaan runkoverkon ydinreitittimet (Core) sekä muut kuin PE-reitittimet. Asiakkaan reunalaitteita kutsutaan CE-laitteiksi. Nämä laitteet yhdistyvät suoraan palveluntarjoajan reunalaitteisiin. Tilanteesta riippuen CE-laitteisiin ei välttämättä tarvitse tehdä mitään muutoksia VPN:iä muodostaessa, vaan kaikki muutokset tapahtuvat PE-reitittimissä. CE-laitteet reitittävät palveluntarjoajan verkosta tulleet paketit kohdeosoitteisiin. PE-reitittimet pitävät huolen siitä, että CE-laitteille ei pääse paketteja, jotka eivät kuulu määriteltyyn VPN:ään. (Lamberg, Laiho 2002, 3.)

Palveluntarjoajan hallinnan piiriin voi kuulua myös CE-reitittimien hallinta. CE-laitteille ei ole yhteyttä palveluntarjoajan runkoverkosta, kun VPN:t muodostetaan käyttämällä VRF-tauluja fyysisillä liitynnöillä. Jotta CE-reitittimiä kyetään hallitsemaan keskitetysti palveluntarjoajan hallintaverkosta ja työasemista, tulee tällöin rakentaa ns. hallinta-VPN (Management VPN). Hallinta-VPN:ään tuodaan tieto verkossa hallittavista CE-laitteista ja näille CE-laitteille kerrotaan reitti hallintaverkkoon. (Lamberg ym. 2002, 19.)

3.3.2 MPLS kytkentä ja reititys

MPLS-kytkentä perustuu siihen, että MPLS-alueen reunalla kohdeverkkoon liitetään etiketti, jonka pohjalta paketti kytketään siirtoyhteyskerroksen tapahtumana ilman erillistä raskasta verkkokerroksen pakettianalysointia. Näin pakettien välitys yksinkertaistuu ja siirtyy samalla ohjelmistotasolta laitteistotasolle. ATM-verkossa MPLS-etiketti korvaa VPI/VCI-osoitekentän, koska käytettävissä olevat menetelmät ovat jo käytössä ATM-kytkentälaitteissa. Saavuttaessa MPLS-alueen toiselle reunalle etiketti poistetaan ja liikenteen välitys jatkuu verkossa normaalin IP-reitityksen tavoin. Tuloksena on nopea ja tehokas IP-pakettivälitys. (EUnet Finland 2006; Ericsson 2005.)

MPLS-VPN toiminta perustuu VRF:iin (VPN Routing and Forwarding Table) eli VPN-reititystauluihin. Nämä reititystaulut sijaitsevat PE-reitittimissä, joissa voi olla useita erillisiä VRF-tauluja. VPN sisältää yksinkertaisimmillaan yhden VRF-taulun jokaisessa PE-reitittimessä. Samaan VPN:ään voi kuulua kuitenkin myös useampia VRF-tauluja. VRF-taulu sisältää reitit, jotka ovat käytössä tietylle ryhmälle verkkoja ja asemia. Käytännössä VRF-taulusta ilmenevät tietyn VPN:n reitit muihin saman VPN:n sisällä oleviin verkkoalueisiin. (Lamberg ym. 2002, 4.)

PE-reitittimeen asetetaan VRF-taulu asiakkaan sisääntuloliitynnälle tai aliliitynnälle. Tällöin kyseisestä liitynnästä tulevat paketit reitite tään VRF-taulun mukaan. Tämä muuttaa myös reitittimen IP-reititystaulua. Kyseinen liityntä ja sen takana sijaitsevat asiakkaan verkot esiintyvät tämän jälkeen ainoastaan kyseisessä VRF-taulussa eikä niitä näy reitittimen normaalissa IP-taulussa. Pakettien toimitus kohdeosoitteeseen tapahtuu seuraavasti. Kun PE-reititin havaitsee, että liitynnästä tullut paketti kuuluu VPN:ään, se reitite tään PE-reitittimeltä runkoverkon läpi toiselle PE-reitittimelle. Sieltä paketti jatkaa matkaansa CE-laitteelle ja edelleen kohdeosoitteeseensa. (Lamberg ym. 2002, 4.)

VRF-tauluille voidaan jokaiselle määritellä erikseen, mitkä reitit tauluun tuodaan (import) ja mitkä reitit taulusta viedään (export) muihin VRF-tauluihin. Route target -arvolla määrätään, kenelle omia VPN-reittejä mainostetaan ja mitkä reitit tuodaan omaan VRF-tauluun. Täysin kytketyssä verkossa import- ja export-reitit ovat samoja. (Lamberg ym. 2002, 6.)

Reititystiedon välitykseen MPLS tarjoaa Lambergin ym. (2002, 8) mukaan neljä eri vaihtoehtoa.

Staattiset reitit ovat helppo ja nopea tapa kertoa PE-reitittimelle CE-laitteen takaa löytyvät verkot. Jos asiakkaan reunalaite ei ole reititin, joka pystyy välittämään reititystietoa sen takaa löytyvistä verkoista, niin staattisten reittien käyttäminen on pakollista. Myös tietoturvan kannalta staattisten reittien käyttö on järkevämpää kuin käyttämällä protokollia PE- ja CE-laitteiden välillä. Staattisia reittejä käyttämällä CE-laitteen ei tarvitse tietää PE-reitittimen sisääntuloliitynnän IP-osoitetta ja näin saavutetaan parempi tietoturva.

PE- ja CE-reitittimet voivat käyttää reititystiedon vaihtamiseen **RIP-** (Routing Information Protocol) tai **OSPF**- (Open Shortest Path First) reititysprotokollaa. Tällöin on erittäin tärkeää, että käytettävä IGP-protokolla (Interior Gateway Protocol) ei välitä PE-reitittimelle VPN:ään kuulumattomia reittejä. Jos asiakkaalla on jo jokin MPLS VPN:n tukema IGP-protokolla käytössä ja koko asiakkaan verkko halutaan liittää VPN:ään, niin IGP-protokollan käyttäminen on tällöin järkevää. OSPF-protokollaa käytettäessä asiakkaiden alueista kannattaa kustakin tehdä oma OSPF-alueensa (OSPF area). Tällöin CE- ja PE-reitittimet ovat molemmat alueiden rajareitittimiä (ABR, Area Border Router). Palvelun tarjoajan verkko on tällöin oma OSPF-alueensa, ja asiakkaan OSPF-alue alkaa CE-laitteesta. Asiakkaan OSPF-alueeseen kuuluu PE-reitittimen liityntä CE-reitittimelle. Lisäksi OSPF-reititystiedoista täytyy tuoda tieto PE-reitittimen VRF-tauluihin.

BGP (Border Gateway Protocol) on suunniteltu nimensä mukaisesti reititystietojen vaihtamiseen eri autonomisten alueiden välillä. BGP-protokollan käyttö on Lambergin ym. (2002, 9) mukaan perusteltua koska:

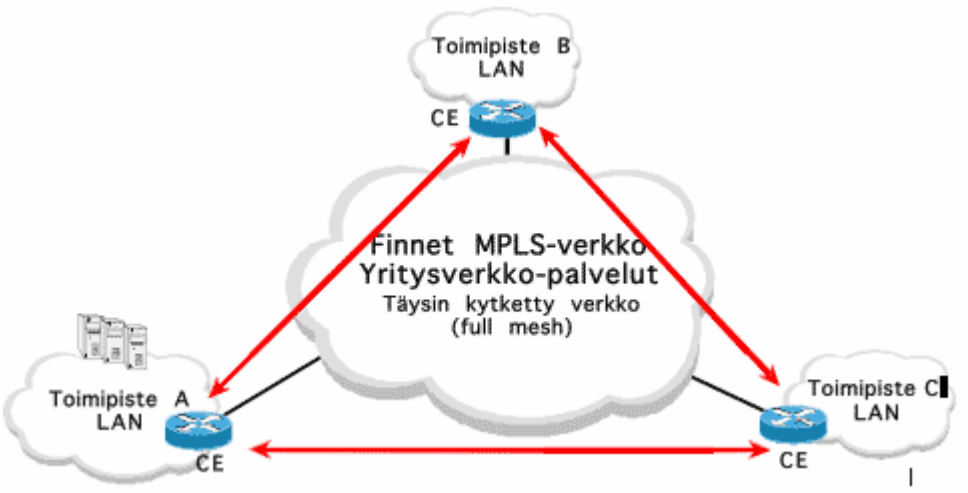
- protokolla vähentää PE-reitittimen kuormitusta, jos PE-reititin on yhteydessä useampaan CE-laitteeseen. Tällöin ei tarvitse ajaa useita reititysalgoritmeja.
- BGP on tarkoitettu toimimaan hallinnollisesti toisistaan erillään olevien verkkojen rajalla.
- BGP on useasti jo käytössä asiakkaan ja palveluntarjoajan verkkojen rajalla. Tällöin sen käyttöönotto on helppoa.
- Joissain tapauksissa on myös mahdollista, että muut reititystiedon välittämiseen suunnitellut tavat eivät toimi. Tällaisissa tapauksissa CE-laitteella on usein BGP-yhteys myös toisiin ei-PE-reitittimiin.
- Huomioitavaa on, että vaikka BGP:n käytön puolesta puhuu moni asia, niin BGP-protokollan käyttö vaatii myös asiakkaan puolelta osaamista BGP:stä. Toisaalta on myös mahdollista että palveluntarjoaja hallitsee myös asiakkaan CE-laitteita.

3.3.3 Topologiavaihtoehdot

MPLS-tekniikka mahdollistaa perinteisten ns. tähtimallisen sekä täysin kytketty -tyyppisten topologioiden rakentamisen sekä näiden eri välimuotojen toteuttamisen. (Finnet Oy, 2006c.)

Yksi suurimmista haasteista perinteisissä Frame Relay- tai ATM-tekniikoilla toteutetuissa VPN-verkoissa on verkkotopologian ja siihen liittyvien kapasiteettien suunnittelu. Tämä korostuu erityisesti silloin, kun ollaan rakentamassa vikasietoisia ratkaisuja. Syynä tähän on se, että perinteiset ratkaisut toteutetaan aina kahden toimipisteen välille yksittäisinä yhteyksinä. Sama tilanne tulee esille myös IPsec-tekniikalla toteutetuissa yhteyksissä. Näihin yhteyksiin on kuitenkin yhteyksien näennäisestä ilmaisuudesta johtuen helpompi toteuttaa myös edistyneempiä topologioita. (Finnet Oy, 2006c.)

Oletustopologiana MPLS VPN -tekniikassa on täysin kytketty verkko. Perustilanteessa kaikki toimipisteet kykenevät kommunikoimaan suoraan toistensa kanssa eikä yhteyksien tarvitse kulkea jonkin kolmannen toimipisteen kautta. Liikenne välitetään täten aina optimaalisesti eikä erillistä topologiasuunnittelua ja liikennelaskentaa tarvitse suorittaa. Tämä on merkittävä ero verrattuna esimerkiksi ATM-tekniikoilla toteutettuihin VPN-verkkoihin. Näissä tyypillinen topologia on tähtimuotoinen, ja kaikki verkon liikenne kulkee keskuspisteen kautta. Tähtitopologia on toiminut hyvin datasovellusten osalta, mutta uusien multimediasovellusten, kuten VoIPin ja videokonferenssien kanssa, tähtitopologia ei ole enää optimaalinen ratkaisu. Tähtitopologiassa syntyvä viive aiheuttaa datansiirrossa korkeintaan hidastumista, mutta esimerkiksi VoIP:issa viive saattaa aiheuttaa koko puhelun epäonnistumisen. Tämä on merkittävä asia puhuttaessa MPLS-verkon puolesta. IPsec-tunneleilla muodostettavissa VPN-verkoissa voi esiintyä samanlaisia ongelmia. Yleensä IPsec-verkoissa tilanne kyetään kuitenkin hoitamaan rakentamalla useampia tunneleita päätepisteiden välille. Alla on esitetty MPLS-verkon oletustopologia. (Finnet Oy, 2006c.)



KUVIO 4. MPLS-verkon oletustopologia (Finnet Oy, 2006c)

MPLS mahdollistaa myös muitakin topologioita kuin pelkästään täysin kytketyn verkon. Osittain kytketty tai keskipiste-reuna-topologiat ovat myös mahdollisia. Myös extranet-tyyppiset ratkaisut on helppo rakentaa MPLS:n kautta. Tällöin esimerkiksi kumppaniorganisaatiolle voidaan tarjota pääsy johonkin yrityksen tiettyyn toimipisteeseen. Asiakasverkot liitetään tällöin yhteen reitityksen kautta jo MPLS-verkon puolella. Palomuuria voidaan käyttää lisäksi tietoturvan tason varmistamiseksi eri kohdissa verkkoa. (Finnet Oy, 2006c.)

4 VPN

4.1 Yleistä

VPN (Virtual Private Network) tarkoittaa virtuaalista sisäverkkoa. VPN on joko laitteisto- tai ohjelmistototeutuksena tehtävä ratkaisu. VPN:n avulla organisaation sisäverkko voidaan ulottaa turvallisesti turvattoman julkisen verkon, kuten Internetin yli. (Viestintävirasto 2001.)

VPN-tekniikalla yhdistetään esimerkiksi kaksi tai useampia sisäverkkoja keskenään tai yksittäinen tietoliikennelaite, esimerkiksi yhteistyökumppanin työasema, organisaation verkkoon. VPN-yhteydessä siirrettävän tiedon suojaamiseen käytetään salausta. Salauksen tehtävänä on estää julkisessa verkossa välitettävän liikenteen sisällön paljastumisen kolmansille osapuolille. VPN-ratkaisuissa käytetään salaamisen lisäksi myös osapuolten todentamista. Todentamisella varmistetaan ennen yhteyden muodostamista osapuolten oikeellisuus. (Viestintävirasto 2001.)

VPN-yhteys muodostetaan käytännössä tunneloimalla kaikki liikenne jonkin liikenteen salaavan protokollan sisään. Tunnelointiprotokollat jaetaan joko kerroksen 2 tai kerroksen 3 protokolliksi niiden toiminnan mukaan. Jako on tehty OSI-mallin perusteella. Yleisesti käytössä olevia VPN-protokollia ovat IPsec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point to Point Tunneling Protocol). Myös MPLS yleistyy nopeasti VPN-protokollana. Kaikki turvattoman verkon yli VPN-tunnelissa lähetettävä liikenne voidaan suojata VPN-tekniikalla. Suojaus ei ole tällöin riippuvainen sovellustason protokollista. (Viestintävirasto 2001; Perlmutter 2001, 104.)

4.2 IPsec

IPsec (Internet Protocol Security) on Internet-yhteisön (IETF) kehittämä sarja protokollia, joiden tarkoituksena on taata turvallisuuspalveluja kaikelle verkkokerroksen IP-liikenteelle. Se toimii TCP/IP-mallin siirtokerroksella, joten

ylemmän tason protokollat ja sovellukset toimivat suoraan sen kanssa. IPsec määrittelee salauksen lisäksi IPsec-tunnelin. Tunneli koostuu palvelimesta ja asiakkaasta, jotka on määritelty käyttämään IPsec-tunnelointia ja salausalgoritmia. IPsec-tunnelia käytetään kokonaisten IP-pakettien salaamiseen ja siirtoon IP-verkon yli. (Innanen 2003, 6-8.)

IPsec tarjoaa Perlmutterin (2001, 106-107) mukaan seuraavat ominaisuudet suojatulle tiedonsiirrolle:

Todennus (autentikointi) takaa vastaanottajan ja lähettäjän identiteetin oikeellisuuden.

Salauksen avulla voidaan siirrettävä tieto salata siten, että se on luettavissa vain oikean avaimen avulla.

Avaimenhallinnan avulla sovitaan salattu avainarvo lähettäjän ja vastaanottajan välille.

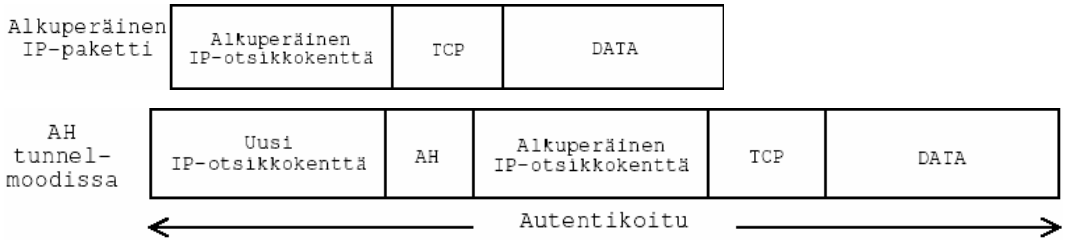
Yhteensopivuus ohi laitteistovalmistajien sekä ympäristöjen asettamien rajojen.

4.2.1 IPsec-tietoturvaprotokollat

IPsec-tietoturvaprotokollat tarjoavat yksittäiselle IP-paketille luottamuksellisuuden, eheyden ja todennuksen. Tämä tapahtuu lisäämällä jokaiseen pakettiin oma tietoturvaotsikko. Tietoturvaprotokollia on kahta tyyppiä: AH (Authentication Header) ja ESP (Encapsulating Security Protocol). (Alakoski 2003, 3.)

AH tarjoaa IP-paketille varmistuksen alkuperästä ja eheydestä sekä suojan uudelleenlähetyksiä vastaan. Otsikkoa voidaan käyttää sellaisenaan suojaamaan IP-pakettia tai sitten yhdessä ESP-otsikon kanssa. Otsikkoa voidaan käyttää myös tunneloitaessa tiedonsiirtoa. Tällöin alkuperäinen IP-paketti sisällytetään

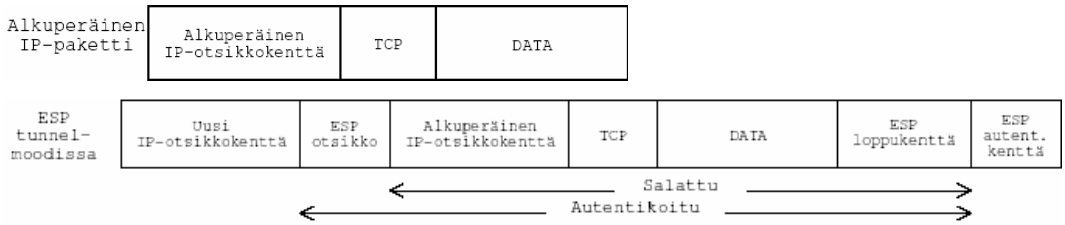
kokonaisuudessaan uuden paketin sisälle. AH-otsikoitu paketti on todennettu kokonaisuudessaan, joten mahdolliset muokkausyritykset havaitaan. AH-otsikon sijainti IPv4-paketissa sekä otsikon rakenne ovat esitetty seuraavassa kuviossa. (Alakoski 2003, 5.)



KUVIO 5. Authentication Header (Alakoski 2003)

ESP-otsikon päätarkoitus on IP-pakettien sisällön luottamuksellisuuden takaaminen. ESP tarjoaa muuten samat palvelut kuin AH, mutta ESP:ssä on lisänä salaus. Salaus toteutetaan käyttämällä salausalgoritmeja. (Alakoski 2003, 6.)

ESP-otsikon palvelu eroaa AH-otsikon palvelusta siten, että se ei tarjoa aivan yhtä kattavaa eheyden tarkistusta ja autentikointia. ESP-otsikoidun paketin eheydentarkistuksesta jätetään kuljetusmoodissa pois aina alkuperäinen IP-otsikko ja autentikointidata, joka tekee ESP:n eheydentarkistuksesta ja autentikoinnista heikomman verrattuna AH:iin. ESP:tä voidaan käyttää AH:n kanssa yhtä aikaa, jolloin saadaan AH:n tarjoamat paremmat autentikointipalvelut käyttöön tiedon salaamisen lisäksi. Kuitenkaan useimmat IPsec-toteutukset eivät tue tätä, koska ESP:n tunnelointimoodilla saadaan todennettua paketti lähes yhtä kattavasti. ESP-otsikoidun IPv4-paketin sekä itse otsikon rakenne on esitetty kuviossa 6. (Heikkilä 2003, 65.)



KUVIO 6. Encapsulating Security Payload (Alakoski 2003)

ESP lisää kuvan mukaisesti 3 uutta aluetta tietosähkeeseen. ESP-otsikko sijoittuu IPsec-paketissa kahteen eri paikkaan.. Ensimmäinen osa on heti IP-paketin otsikon jälkeen, ennen salakirjoitettua dataa. Loput ESP-otsikosta sijaitsevat IP-paketin data-osan jäljessä. Myös ESP-otsikon loppuosa salakirjoitetaan datan kanssa. Salakirjoitetun osan perässä on ESP-autentikointikenttä. (Comer 2002, 586.)

IPsecillä siirretyssä paketissa on mukana eheys- ja todennussumma. Tämä kulkee AH- ja ESP-paketeissa nimellä Authentication data -kenttä. Tämän summan avulla tarkastetaan vastaanotetun tiedon alkuperä ja eheys suhteessa lähetettyyn tietoon. Tämä tapahtuu laskemalla summa uudelleen vastaanottopäässä. Tämä on tärkeää etenkin, kun tietoa on siirretty suojaamattoman yhteyden yli. (Heikkilä 2003, 32-35.)

4.2.2 Salaustekniikat

IPsecin salaus perustuu algoritmeihin. DES-algoritmi on julkaistu vuonna 1977 US National Bureau of Standardsin (nykyisin NIST) toimesta. DES on standardin mukaan pakollinen IPsecissä. IPsec generoi uusia avaimia koko yhteyden ajan, joka estää koko tiedonsiirron luottamuksellisuuden rikkomisen, mikäli yksi avain on saatu murrettua. DES-algoritmin lisäksi käytettävissä on myös vahvempi 3DES-algoritmi. 3DES-algoritmin käyttö on suositeltavaa, mutta se myös vaatii laitteilta enemmän laskentatehoa. (Heikkilä 2003, 24.)

Internetyhteisön IPsec-standardiehdotuksen määrityksiin kuuluu myös muiden algoritmien, kuten AES:n käyttö. AES-algoritmi on nopeampi kuin 3DES, joten oletettavaa on, että AES tulee tulevaisuudessa syrjäyttämään 3DESin IPsecissä. (Heikkilä 2003, 76.)

4.2.3 IKE

IKE (Internet Key Exchange) on IETF:n avaintenhallintaprotokolla, joka koostuu OAKLEY-, ISAKMP- ja SKEME-protokollista, jotka on kehitetty aiemmin. Alun perin IKE tehtiin IPsec-järjestelmiä varten, mutta sitä voidaan käyttää myös muille protokollille. IKE toteuttaa osia sekä OAKLEY- että SKEME-avaintenhallintaprotokollista. (Alakoski 2003, 16.)

Ennen salatun tiedonsiirron aloittamista täytyy lähettäjän ja vastaanottajan sopia yhteinen sopimus siirrosta. Tämän sopimuksen eli SA:n (Security Association) tekemisen hoitaa IKE. Yhteyttä muodostavien koneiden välille neuvoteltava SA on ainutkertainen. Kun IKE alkaa luoda uutta SA:ta, se muodostaa ensin oman SA:n. Ipsecin turvallisuusassosiaatiot luodaan tämän IKE:n oman turvallisuusassosiaation suojassa. (Alakoski 2003, 16.)

Useamman yhtäaikaisen yhteyden tunnistamiseen SA käyttää SPI:tä (Security Parameter Index). IKE hoitaa SA-neuvottelut kahdessa vaiheessa. Ensimmäisen vaiheen tehtävänä on luoda osapuolten välille autentikoitu ja suojattu siirtokanava. Toisen vaiheen tehtävänä on pääasiassa hoitaa turvallisen yhteyden ylläpitäminen ja avainten uusiminen. Toisessa vaiheessa syntyviä turvallisuusassosiaatioita luodaan ja tuhotaan tarpeen mukaan. Yleensä tuhoaminen tapahtuu turvallisuusassosiaatiolle määritellyn eliniän tultua täyteen. IKE SA pysyy kuitenkin voimassa, vaikka sen sisäisiä turvallisuusassosiaatioita tuhotaan. Täten autentikointi tarvitsee suorittaa vain yhden kerran. (Alakoski 2003, 20.)

4.2.4 IPsecin rajoitukset

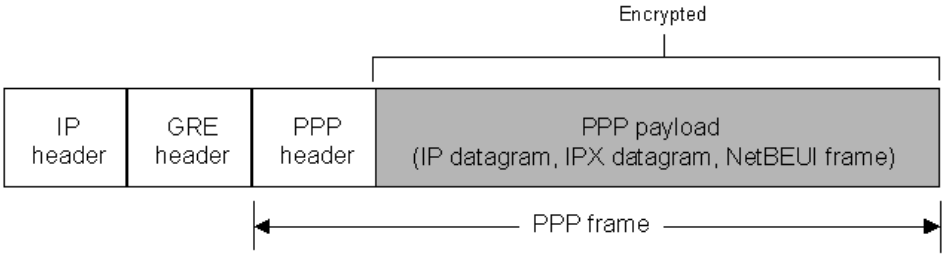
IPsecin käytössä on kaksi rajoittavaa tekijää. Ensimmäinen rajoitus IPsecissä on, että se ei kohdistu muihin verkkoprotokolliin kuin IP-protokollaan. Jotta muita verkkoprotokollia noudattava liikenne voitaisiin suojata IPsecin avulla, se on kapseloitava IP:n sisälle. Tämä taas aiheuttaa sen, että datapaketteihin tulee ylimääräistä sisältöä. Toinen IPsecin rajoitus liittyy yhteensopivuuteen. Useimmat Ipsecin versiot eivät ole yhteensopivia eri ohjelmisto- ja laitevalmistajien välillä. (Perlmutter 2001, 114.)

4.3 PPTP

PPTP (Point-to-Point Tunneling Protocol) on Microsoftin alun perin Windows NT-palvelimia varten vuonna 1996 kehittämä tunnelointikäytäntö. Sitä on laajennettu jälkikäteen muiden kehittäjien VPN-yhteyksien rakentamiseen sopivaksi. Olennaisena osana PPTP:ssä on tuki myös valinnaisille puhelinyhteyksille. PPTP onkin laajennus puhelinyhteyksissä käytetylle PPP (Point-to-Point Protocol) -protokollalle. PPTP:tä voidaan hyödyntää myös muilla kuin TCP/IP-protokollalla, koska PPTP ei ole TCP/IP riippuvainen. (Innanen 2003, 5.)

PPTP kapseloi PPP-kehyksen IP-verkon yli siirrettäväksi IP-paketiksi. PPP-kehykset kapseloidaan käyttäen GRE-protokollaa (Generic Routing Encapsulation). PPTP:tä voidaan käyttää reitittimien yhdistämiseen tai etäyhteyksien muodostamiseen. (Perlmutter 2001, 116.)

PPTP käyttää kahta erityyppistä pakettia: datapaketteja ja valvontapaketteja. Datapaketit sisältävät hyötykuorman, valvontapaketteja käytetään merkinantoon ja tilantiedusteluun. PPTP-paketin rakenne on esitetty alla olevassa kuviossa. (Perlmutter, 2001, 116.)

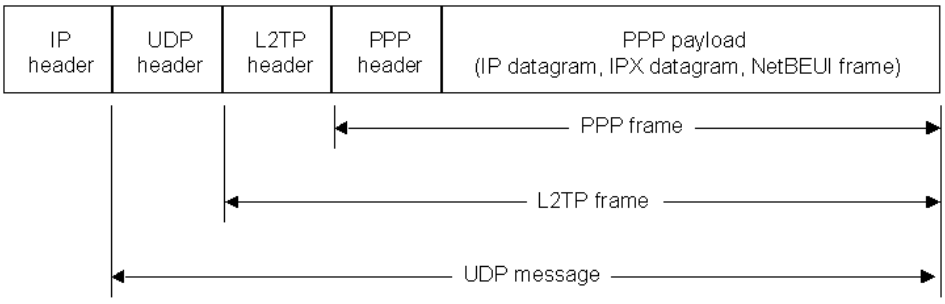


KUVIO 8. PPTP-datapaketin rakenne (Microsoft 1999, 12)

PPTP ei itsessään salaa siirrettävää tietoa, vaan salaus on ylempien kerrosten tehtävä. PPTP:n tietoturvassa onkin ollut runsaasti ongelmia, nykyään PPTP:n kehitys on melkein pysähtynyt. PPTP on päätetty yhdistää L2TP-tekniikkaan, ja kiinnostus IPsec-tekniikkaan on lisääntynyt. (Innanen 2003, 6.)

4.4 L2TP

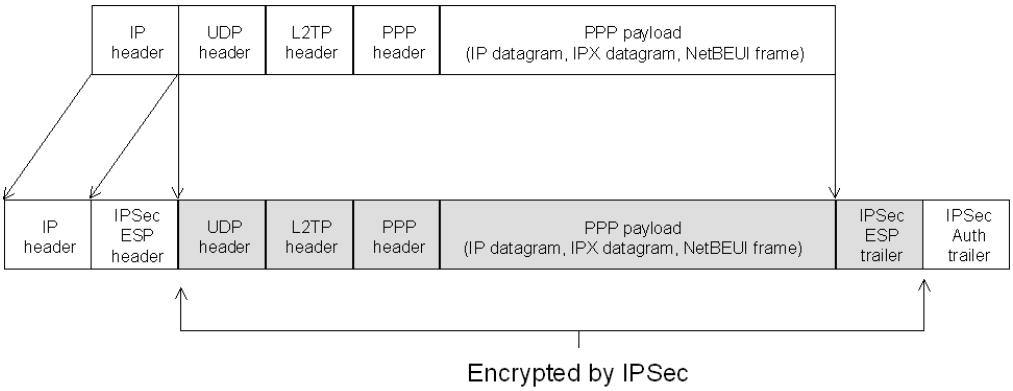
Myös L2TP (Layer Two Tunneling Protocol) kapseloi PPP-kehyksen. L2TP sallii IP, IPX tai NetBEUI-liikenteen salaamisen ja lähettämisen minkä tahansa point-to-point -yhteyksiä tukevan siirtotien yli. Se yhdistää PPTP:hen L2F-tekniikan (Layer 2 Forwarding), jonka taustavaikuttajana on Cisco Systems. PPP-kehyksiä voidaan tämän protokollan avulla kapseloida ja lähettää eri verkkojen yli. Verkon tyyppi voi olla esimerkiksi IP, X.25, Frame Relay, tai ATM. Käytettäessä kuljetustapana IP:tä, voidaan L2TP:tä käyttää tunnelointiin Internetissä. Kuviossa 9 on esiteltynä L2TP-paketin rakenne. (Microsoft 1999, 13; Innanen 2003, 6.)



KUVIO 9. L2TP-paketin rakenne (Microsoft 1999, 12)

4.4.1 L2TP/IPsec

Kun L2TP-liikennettä salataan IPsec:in avulla, tuloksena saadaan L2TP/IPsec. L2TP/IPsecissä yhdistetään tehokkaasti molempien protokollien hyviä puolia. Kuviosta 10 nähdään mitä muutoksia L2TP-pakettiin tulee, kun se salataan IPsecillä. (Innanen 2003, 7.)



KUVIO 10. L2TP-paketti salattuna IPsec:iä käyttäen (Microsoft 1999, 13)

Tiedon salaus IPsecillä aloitetaan ennen kuin PPP-yhteyttä on muodostettu. L2TP/IPsec käyttää DES-salausta (Data Encryption Standard), joka paloittelee salattavan tiedon 64-bitin lohkoihin. Salausavain on 56-bittinen. L2TP/IPsec vaatii käyttäjätunnistuksen lisäksi työasematason tunnistuksen. Tämä hoidetaan käyttäjätunnuksella, salasanalla sekä sertifikaatilla. (Innanen 2003, 7.)

5 VALTAKUNNALLINEN YRITYSVERKKO

5.1 Yleistä

Yrityksellä tarkoitetaan tässä toimijaa, joka yhdistää tieto-, tietoliikenne-, tietojenkäsittely- ja varastointiresurssinsa. Yritysverkko on yleensä julkisten ja yksityisten verkkojen sekoitus. (Chappel 1999, 10.)

Yritysverkon ominaisuuksiin kuuluvat Chappelin (1999 10.) mukaan

- keskenään yhdistetyt lähiverkot, jotka mahdollistavat asiakas- ja palvelinsovelluksien yhdistäminen vanhojen keskitettyjen sovellusten kanssa.
- loppukäyttäjän tarve suurempaan kaistanleveyteen. Kaistanleveys voidaan yhdistää kokonaisuudeksi kytkimellä ja toimittaa ennaltamäärätyllä siirtotiellä.
- aiemmin erillisinä olleiden tietoverkkojen yhdistäminen siten, että purskeeton ääni- tai videoliikenne voidaan hoitaa samassa verkossa.
- WAN (Wide Area Network) -verkolle suunnatut välityspalvelut, joista erityisen nopeasti kasvaa frame relay ja hieman hitaammin soluvälitys.

5.2 Finnet Lan-to-Lan -palvelu

Finnettiin kuuluvan operaattorin tietoliikenneverkossa Lan-to-Lan palvelu on toteutettu ATM PVC- (Permanent Virtual Circuit) ja VLAN (Virtual Local Area Network) -tekniikoilla. PVC on tapa, jolla ATM -kehykset jaetaan osiin ja paketoidaan erillisiin lähetysyksiköihin. Lähetysyksiköt välitetään eteenpäin ATM-verkossa. PVC-yhteys muodostetaan jonkun ulkoisen mekanismin, esimerkiksi verkonhallinnan, toimesta. Tässä tapauksessa verkon operaattorit kirjoittavat kunkin virtuaaliyhteyden vaatimat kytkennät kaikkiin kytkimiin. (Finnet Oy 2005c, 4.)

Fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin virtuaalilähiverkon eli VLANin avulla. Tämä tarkoittaa sitä, että yrityksen eri osastojen jakaminen omiin verkkoihinsa on mahdollista niiden fyysisestä sijainnistaan riippumatta. VLAN vaatii tuen kytkimiltä ja reitittimiltä. VLANia tukevat laitteet lisäävät paketteihin tunnuksia. Paketin vastaanottava laite tietää täten, mihin verkkoon vastaanotettu paketti kuuluu. Kun paketti välitetään laitteelle, joka ei tue VLAN-tekniikkaa, siitä poistetaan tunnus. (Jaakohuhta 2000, 165.)

5.3 Finnet MPLS -palvelu

MPLS-tekniikalla toteutettavat toimipisteiden väliset VPN-yhteydet mahdollistavat uudenlaisia ratkaisuja yrityksen tietoliikennetarpeiden hoitamiseen. MPLS-verkko on täysin kytketty toimipisteiden välillä. MPLS-verkossa eri liikennelajeja voidaan priorisoida yrityksen tarpeiden mukaan. Tällöin IP-verkoissa voidaan siirtää myös puhetta laadukkaasti. Finnet suosittelee asiakkailleen, että he sisällyttäisivät MPLS-palveluun myös yrityksen puhelinvaihteet yhdistävän IP-vaihdeverkkopalvelun. Tällöin yrityksen kaikki liikenne kulkisi yhden verkon kautta ja sen hallinnoiminen olisi helpompaa. (Finnet Oy 2006a.)

MPLS-tekniikan etuja ovat kustannustehokkuus, toimipisteiden välinen optimoitu liikenteen välitys, taattu IP-tason palvelun laatu päästä-päähän, tietoturvalliset yhteydet sekä suljetut käyttäjäryhmät frame relay- ja ATM-yhteyksien tapaan. (Finnet Oy 2006a.)

MPLS-palvelulla yrityksen eri toimipisteiden lähiverkot voidaan yhdistää tietoturvalliseksi yritysverkoksi, jolloin informaatio on heti jokaisen työntekijän käytössä välimatkoista huolimatta. Valtakunnallinen palvelu mukautuu pienestä muutaman toimipisteen verkosta aina satojen toimipisteiden verkkoihin. Myös ulkomailla sijaitsevien toimipaikkojen suljetut yhteydet saadaan liitettyä osaksi palvelukokonaisuutta. (Finnet Oy 2006a.)

6 TAMPEREEN PUHELIMEN MPLS-PROJEKTI

6.1 Projektin taustaa

Maanlaajuisen yritysverkon rakentamiseen on useita tekniikoita. Tässä opinnäytetyössä on kuitenkin keskitytty vain kahteen Finnetin käyttämään tekniikkaan, koska opinnäytetyön pohjana on Finnettiin kuuluvan Tampereen Puhelimen yritysprojekti.

Vuoden 2005 kesällä Tampereen Puhelimelta pyydettiin tarjous yritysverkosta, joka sisältää noin 60 liittymää. Asiakas halusi tehostaa myymälöidensä tiedonkulkua ja selkeyttää maksuliikennettä, jossa oli paikkakunnittain vaihteleva palveluntarjoaja. Yritysverkkoa oli tarkoitus hyödyntää myös tuotetietojen myymäläkohtaisessa päivittämisessä. Finnetin tuotteissa oli kaksi mahdollisuutta yritysverkon toteuttamiseen, MPLS ja Lan-to-Lan. Näistä molemmista toteutustavoista tehtiin tarjous asiakkaalle, joka päätyi tilaamaan yritysverkon MPLS-palvelulla toteutettuna.

MPLS:n valintaa yritysverkon pohjaksi puolsivat seuraavat asiat:

- VoIP-valmius
- laajennuksen ja ylläpidon vaivattomuus
- toimipisteet yhteydessä toisiinsa ilman erillisiä, istuntokohtaisia toimenpiteitä (vrt. VPN-putken avaus)
- tietoturva ilman erillisen salauksen käyttämistä

Asiakkaan MPLS-verkko on jo otettu käyttöön, ja se on osoittautunut toimivaksi ratkaisuksi. Tulevaisuudessa verkon liittymämäärä tulee kasvamaan noin 100 kappaleeseen ja mukaan tulee IP-puhelinverkko.

Esimerkkinä toimiva verkko on suunniteltu siten, että asiakkaan mikrotuesta huolehtivalla yrityksellä on pääsy MPLS-verkon kautta jokaiseen toimipisteeseen. Projektin suunnitteluvaiheessa todettiin, että aluksi toimipisteiden ei ole tarpeen

olla suoraan yhteydessä toisiinsa. Verkon topologiasta tehtiin näin ollen tähtimäinen. Topologia muuttuu kuitenkin täysin kytketyksi IP-puheluiden tullessa käyttöön.

IP-puhelut eli VoIP on omanlaisensa haaste. Verkon laajuus asettaa vaatimuksia puheluiden ohjautumiselle, esimerkiksi hätäpuhelut tulee ohjautua oikean paikkakunnan hälytyskeskukseen. VoIP on kuitenkin täysin oma projektinsa, ja se toteutetaan, kun dataverkko on toimitettu kokonaan. Tässä opinnäytetyössä ei ole syytä perehtyä tarkemmin VoIP-projektiin.

6.2 Toteutus

Toimittavat puhelinyhtiöt tekivät projektin päätelaiteasennukset. Työtilaukset teki Tampereen Puhelimen toimituskoordinointi, työasema-asennuksesta huolehti pääasiassa asiakkaan projektipäällikkö. Tampereella sijaitsevassa päätoimipisteessä oli muita toimipisteitä enemmän tehtävää; siellä asennuksia tekivät Tampereen Puhelimen asentajat sekä asiakkaan mikrotuesta huolehtiva yritys. Päätoimipisteeseen sijoitettiin ns. nielu, jonka kautta myymälät liikennöivät Internettiin. Päätoimipisteessä Tampereella sijaitsee myös verkon palomuuri sekä erinäisiä palvelimia.

Maksutapahtumien varmentamisen keskittäminen ja selkeyttäminen oli yksi projektin pääasioita. Maksuvarmenne-palvelin sijoitettiin päätoimipisteeseen. Muiden toimipisteiden työasemat tekevät varmennekyselyt MPLS-yhteyttä käyttäen keskitetysti tälle palvelimelle, joka on salatun yhteyden kautta yhteydessä maksuvarmennuspalveluita tarjoavaan yritykseen. Tämä on suuri muutos vanhaan järjestelyyn, jossa jokaisella toimipisteellä oli oma soittosarja- tai ISDN-yhteys paikalliseen pankkiin.

Verkon päätelaitteeksi valittiin Ciscon uusi malli 877. Ciscon 837-malli on hyvin samankaltainen, mutta siinä ei pysty priorisoimaan liikennettä. Liikenteen priorisointi oli yrityksen tulevaisuudensuunnitelmat huomioiden tärkeä valintakriteeri. Toimipisteiden kaistat ovat verrattain pieniä, ja VoIPin tullessa

käyttöön priorisointi on tärkeää IP-puheluiden kannalta. Verkkoon valitun päätelaitteen kuvaus on liitteessä 1.

Päätelaitteen konfiguraatio tilattiin Finnetin valvomosta, joka myös valvoo valtakunnallisia liittymiä. Tähän päädyttiin jo senkin takia, että töiden määrä ei sallinut konfiguraation miettimistä oman väen voimin Seuraavassa muutamia otteita MPLS-konfiguraatiosta. Konfiguraatio ei eroa rakenteeltaan sellaisesta konfiguraatiosta, johon ei liity MPLS.

Alla olevilla riveillä kerrotaan ATM0.100 liitynnälle minkä IP-osoitteen takaa PE-laitteen vrf-taulu löytyy, ja minkä IP-osoitteen itse liityntä saa.

```
interface ATM0.100 point-to-point
  bandwidth 512
  ip address 10.10.195.18 255.255.255.252
  ip access-group 100 in
  ip mtu 1500
  atm route-bridged ip
  pvc 0/100
  protocol ip 10.10.195.17 broadcast
  encapsulation aal5snap
```

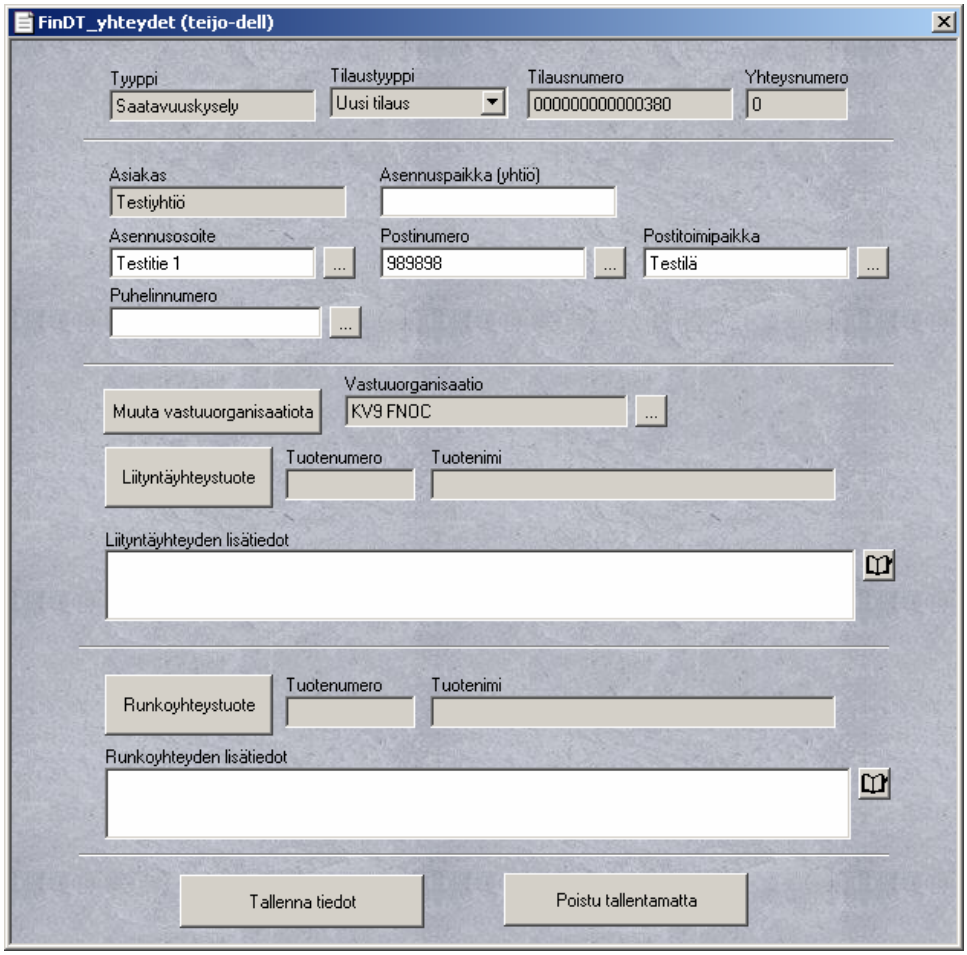
Alla on esitelty pääsylistoissa muutama huomionarvoinen rivi. Näillä riveillä sallitaan pääsy Tampereen päätoimipisteestä, mutta kielletään pääsy sivutoimipisteistä. IP-osoitteet on muutettu esimerkkejä varten kokonaan erilaisiksi.

```
access-list 100 permit ip 192.168.4.0 0.0.0.31 any
access-list 100 deny   ip 192.168.4.0 0.0.0.255 any
access-list 100 deny   ip 192.168.5.0 0.0.0.255 any
```

6.2.1 Prosessin kulku Finnet-yhtiöissä

Finnet-yhtiöissä on käytössä FinDT-tilausjärjestelmä, jolla hoidetaan kaikkien liittymien tilaukset toisen Finnet-yhtiön alueelle. Järjestelmää käytettiin myös MPLS-projektissa.

FinDT-järjestelmässä tilauslomakkeelle syötetään toimitusosoite ja asiakkaan tiedot. Tilattava tuote valitaan listasta. Tuote valitaan halutun liittymän ja halutun nopeuden mukaan. Kuviossa 11 on FinDT:n tilauslomake, jolla liittymien tilaukset hoidetaan.



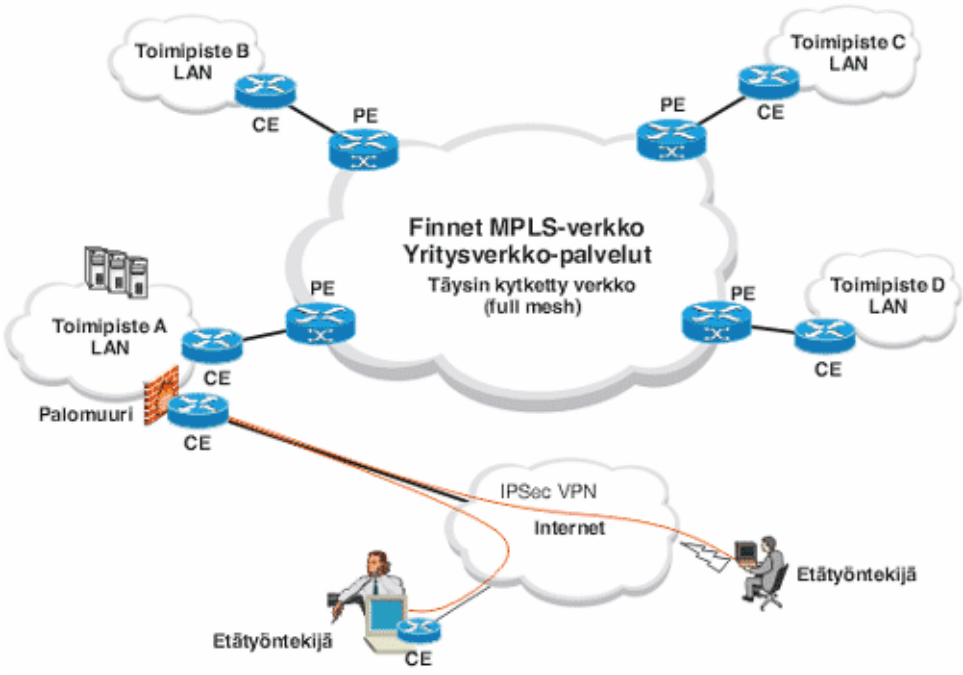
KUVIO 11. FinDT tilauslomake (Kalliomäki, 2003)

Järjestelmä lähettää tiedon tilauksesta toimittavalle Finnet-yhtiölle ja Finnet Carrier Oy:lle, joka tekee vaadittavat määritykset Finnetin runkoverkkoon. Tämä

toimintatapa on sama MPLS:n ja Lan-to-Lanin osalta. Kun määritykset on tehty, tiedot lisätään FinDT-tilauslomakkeelle niille varattuihin kenttiin. Toimittava yhtiö tarvitsee nämä tiedot tehdessään määrityksiä omaan verkkoonsa. Lisäksi toimittava yhtiö tarvitsee tiedot asiakkaan MPLS-verkon IP-osoitteistuksesta. Jos liittymään halutaan monipuolisempi päätelaite, esimerkiksi Ciscon tuote, on tapana ollut, että tilaava yhtiö toimittaa päätelaitteen konfiguraation. Tästä konfiguraatiosta toimittava yhtiö saa selville myös IP-osoitteistuksen.

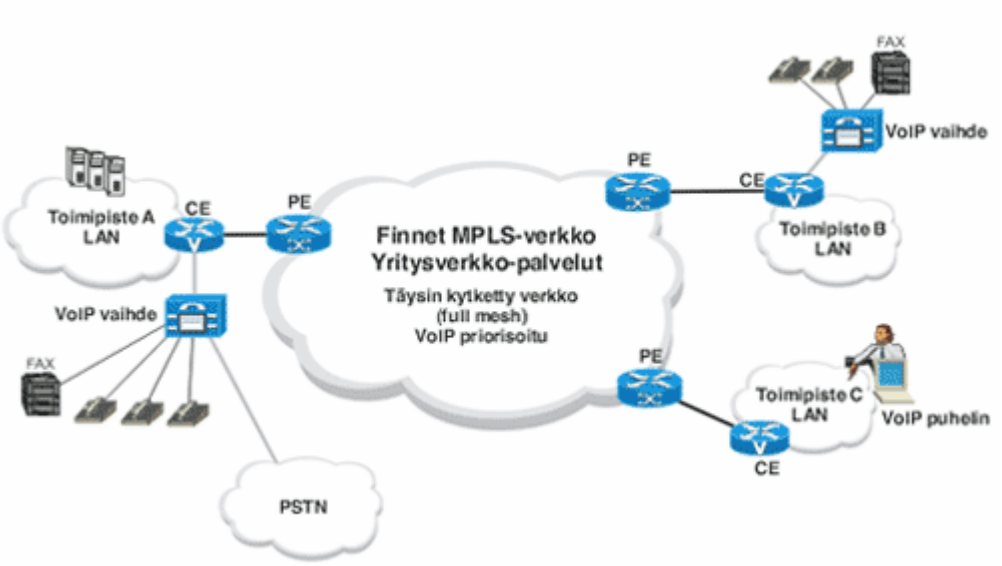
6.3 Yritysverkon toteutusesimerkit

Ensimmäisenä yritysverkon toteutusesimerkkinä on topologiatoteutus, jossa useat eri paikkakunnilla sijaitsevat toimipisteet ja pääkonttori muodostavat kokonaisuuden. Verkon laajentaminen, uusien toimipisteiden lisääminen topologiaan sekä verkkomuutosten tekeminen on vaivatonta. Etäkäyttäjien liittyminen yrityksen verkkoon onnistuu VPN-yhteyden, esimerkiksi IPsecin, avulla. Projektissa käytettiin juuri tätä kuviossa 12 esitettyä mallia. Erona malliin on, että toimipisteet eivät pääse liikennöimään keskenään.



KUVIO 12. Mallikuva MPLS-verkosta (Finnet Oy 2006c)

Edellisessä esimerkissä kuvattujen ominaisuuksien lisäksi erillisten virtuaaliverkkojen, VLANien, lisääminen yritysverkkoihin on myös mahdollista. Toisessa esimerkissä VLAN:ien toteutus tehdään konfiguroimalla päätelaitteiden WAN-liittymään useita loogisia alaliittymiä. Näin liikenne saadaan eriytettyä omaan verkkosegmenttiinsä VLAN-tunnuksen perusteella. Yhteen VLANiin voidaan esimerkiksi laittaa kulkemaan dataliikenne ja toiseen VLANiin VoIP-liikenne, joka ohjataan operaattorin puhelinverkkorajapintaan. Toteutus lisää myös tietoturvallisuutta, sillä verkon sisällä segmenttien välinen liikenne kulkee aina palomuurin kautta. Näin liikennöintiä voidaan erikseen kontrolloida vastaamaan asiakkaan tarpeita. Tätä tapaa tullaan noudattamaan, kun projektissa edetään VoIP-vaiheeseen. Alla esitetyssä kuviossa on VoIP-valmis verkko.



KUVIO 13. VLANien lisääminen verkkoon VoIP:tä varten (Finnet Oy 2006c)

6.4 Projektin yhteenveto

Finnet Lan-to-Lan ja Finnet MPLS omaavat kumpikin projektin kannalta hyviä ominaisuuksia. Kuitenkin MPLS-palvelun modernius ja laajennusmahdollisuudet veivät tässä projektissa voiton. Lan-to-Lan olisi ollut halvempi ja hiukan yksinkertaisempi toteuttaa, mutta se on vanhanaikainen eikä sovellu näin monen toimipisteen yhteenliittämiseen.

MPLS-verkko on osoittautunut toimivaksi ratkaisuksi asiakkaalle. Entiseen järjestelyyn verrattuna muutos on suorastaan huikea. Kun aikaisemmin toimipisteiden maksuvarmenneliikenne oli rakennettu paikallisten mahdollisuuksien mukaan, nyt kaikki toimipisteet hoitavat varmennuksen yhden keskitetyn pisteen kautta. Lisäksi myymälöihin tuli Internet-yhteys. Alussa ollut tiukka aikataulu oli haaste, mutta siitäkin selvittiin. Kiitos tästä kuuluu tietysti asiakkaalle, joka salli aikataulun muokkaamisen. Jälkeenpäin havaittiin että viivästykset joidenkin toimipisteiden toimituksissa koituivat hyödyksi, kun samalla suunnalla Suomea oli useampia toimipisteitä valmiina loppuasennukseen.

Ainut varsinainen ongelma on ollut toimittavien puhelinyhtiöiden vaihtelevat toimintatavat MPLS-toimituksissa. Tästä johtuivat useat viivästyksetkin projektissa. MPLS-yhteys pitäisi aina testata Finnetin valvomon kanssa. Paikalliset puhelinyhtiöt laiminlöivät testausta kuitenkin laajasti. Asiakkaan projektipäällikön mennessä paikanpäälle tekemään työasema-asennusta, hän joutui usein toteamaan yhteyden toimimattomuuden. Tämä aiheutti lisätöitä niin asiakkaalle kuin Tampereen Puhelimen toimituskoordinoinnillekin. Jos yhteys olisi heti testattu asennuksen yhteydessä, ongelma olisi havaittu ja korjattu jo varhaisessa vaiheessa.

Projektissa esiin tulleet ongelmat olivat kuitenkin loppujen lopuksi vähäisiä ja helposti korjattavia. Tämä kertoo MPLS-palvelun hyvästä suunnittelusta. Projektin aloituksen jälkeen on tapahtunut sen verran muutoksia, että Finnetin valvomo poistuu kevään 2006 aikana ja puhelinyhtiöt alkavat valvomaan itse MPLS-verkkojaan. Käytännössä Tampereen Puhelimen tapauksessa valvonta tapahtuu Satakunnan Puhelimella Porissa, jossa hoidetaan muutenkin Tampereen Puhelimen verkonhallinta.

Asiakkaan yritysverkko on saatu toimintakuntoon ja uusia toimipisteitä liitetään verkkoon tasaista tahtia. Voidaan katsoa että projektissa on onnistuttu ja on aika kirjoittaa projektiraportti asiakkaalle luovutettavaksi.

7 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli kertoa valtakunnallisen yritysverkon toimituksesta tätä tarkoitusta varten suunnitelluilla Finnetin tuotteilla. Pohjana käytettiin eräälle Tampereen Puhelimen asiakkaalle toimitettua yritysverkkoa, joka rakennettiin käyttäen MPLS-tekniikkaa.

Opinnäytetyössä käytiin aluksi läpi käytettyjen tekniikoiden teoriaa. Käsittelyssä oli projektin kannalta tärkeät tekniikat: MPLS ja ATM. Lisäksi luotiin katsaus VPN-tekniikoihin, joihin myös MPLS kuuluu.

MPLS VPN -tekniikan oletustopologiana on täysin kytketty verkko. Perustilanteessa kaikki toimipisteet kommunikoivat suoraan toistensa kanssa eikä yhteyksien tarvitse kulkea VPN-keskuspisteen kautta. Liikenne välitetään täten optimaalisesti, eikä erillistä topologiasuunnittelua tai liikennelaskentaa tarvita. MPLS-tekniikalla toteutettu verkko soveltuu hyvin multimediasovellusten, kuten VoIPin ja videopuheluiden käyttöön.

MPLS mahdollistaa täysin kytketyn -verkon lisäksi muitakin topologioita. Esimerkiksi osittain kytketty tai keskipiste-reuna-topologiat ovat myös mahdollisia. Myös extranet-tyyppiset ratkaisut on helppo toteuttaa MPLS:n kautta.

MPLS-kytkennässä MPLS-alueen reunalla kohdeverkkoon liitetään etiketti. Paketti kytketään etiketin pohjalta siirtoyhteyskerroksen tapahtumana, ilman erillistä, raskasta verkkokerroksen pakettianalysointia. Pakettien välitys yksinkertaistuu ja siirtyy ohjelmistotasolta laitetasolle. Saavuttaessa MPLS-alueen toiselle reunalle etiketti poistetaan ja liikenteen välitys verkossa jatkuu normaalin IP-reitityksen tavoin.

Yritysprojektin pääroolissa olleista Finnetin yritysverkkopalveluista kerrottiin julkisen tiedon pohjalta. Lan-to-Lan on jo vanha palvelu, ja siitä oli hankala löytää julkiseksi tarkoitettua tietoa. MPLS on sen sijaan uusi ja kehitettävä palvelu, ja siitä on löydettävissä kattavasti tietoa.

Projekti-luvussa kerrottiin Tampereen Puhelimen asiakkaan yritysverkon suunnittelusta, rakennuksesta sekä nykytilanteesta. Projekti oli puhelinyhtiön kannalta onnistunut, ja asiakas on ollut tyytyväinen valintaansa. Projektissa oli mukana monen osa-alueen asiantuntijoita päätelaitteen konfiguroinnista palomuurin suunnitteluun ja toteutukseen.

Viime aikojen kokemuksista voidaan päätellä, että MPLS on tulevaisuuden tekniikka. Tampereen Puhelimelta on pyydetty tarjouksia laajojen valtakunnallisten yritysverkkojen rakentamisesta. Eräässä tapauksessa yhteydet menisivät ulkomaille asti.

LÄHTEET

Alakoski T. 2003. Avainten vaihto ja jakelu IPsec-järjestelmässä. Diplomityö. Tampereen teknillinen yliopisto, Tietotekniikan osasto

Chappel L. 1999. Cisco reitittimet. IT Press, Jyväskylä

Comer D. 2002. TCP/IP. Gummerus Kirjapaino, Jyväskylä

Ericsson 2005. MPLS [online]. Helsinki, 2005 [viitattu 2.9.2005]. Saatavissa: http://www.ericsson.com/fi/technology/MPLS.shtml

EUnet Finland 2006. Multiprotocol Label Switching (MPLS) -tekniikkaa lyhyesti [online]. Espoo, 2006 [viitattu 28.3.2006]. Saatavissa: http://www.eunet.fi/tietoliikenne/yritysverkko.php#mpls

Finnet Oy. Finnet-ryhmän kotisivu [online]. Helsinki: Finnet Oy, 2006 [viitattu 3.10.2005]. Saatavissa: http://www.finnet.fi

Finnet Oy. KV9-runkoverkon tuotekuvaus.

Finnet Oy. Finnetin MPLS [online]. Helsinki: Finnet Oy, 2006 [viitattu 13.1.2006]. Saatavissa: http://www.finnetmpls.fi/pages/ammattilaisille.htm#4.1

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

Heikkilä T. 2002. Verkonhallintajärjestelmän suojaaminen IPSecin avulla. Tietotekniikan pro gradu -tutkielma. Jyväskylän yliopisto, tietotekniikan laitos

Innanen H. 2003. VPN. Lähiverkot-erikoistyökurssi. Lappeenrannan teknillinen yliopisto, Tietotekniikan osasto

Jaakohuhta H. 2000. Lähiverkot - Ethernet. Edita Oyj, Helsinki

Kalliomäki T. 2003. FinDT - Käyttäjän ohje. Finnet Oy, Helsinki

Keogh J. 2001. Verkkotekniikat – tehokas hallinta. Edita Oyj, Helsinki

Koivisto M. 1998. ATM:n perusteet [verkkodokumentti]. Saatavissa: http://oppimateriaalit.internetix.fi/fi/avoimet/6tekniikkatalous/atm/index

Lamberg J. ja Laiho M. 2002. BGP/MPLS-VPN raportti. Jyväskylän yliopisto

LAN&WAN. Arabianrannan alueverkon palvelut [online]. Espoo: Nordic LAN & WAN Communication Oy, 2006 [viitattu 5.9.2005]. Saatavissa: http://www.lanwan.fi/arabianranta/index.html

Microsoft. 1999. Virtual Private Networking in Windows 2000: An Overview

Ogletree T. 2001. Inside verkot. Oy Edita Ab, Jyväskylä

Perlmutter B. 2001. Virtuaaliset yksityisverkot – VPN. Edita Oyj, Helsinki

Viestintävirasto. VPN [online]. Helsinki: Viestintävirasto, 2001, päivitetty 1.9.2004 [viitattu 10.2.2006]. Saatavuus: http://www.ficora.fi/suomi/tietoturva/vpn.htm

Wikipedia. OSI-malli [online]. Helsinki: Wikimedia-säätiö, 2006 [viitattu 3.10.2005]. Saatavissa: http://fi.wikipedia.org/wiki/OSI-malli