Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Jarmo Laine

Tietoliikenneoperaattorin vaihto suuressa yrityksessä

Insinöörityö 27.4.2009

Ohjaaja: järjestelmäasiantuntija Heikki Strengell
Ohjaava opettaja: yliopettaja Matti Puska

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä Otsikko Sivumäärä	Jarmo Laine Tietoliikenneoperaattorin vaihto suuressa yrityksessä 61
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja Ohjaava opettaja	järjestelmäasiantuntija Heikki Strengell yliopettaja Matti Puska

Opinnäytetyössä dokumentoitiin toisen tietoliikenneoperaattorin rinnalle otto Lemminkäinen konsernissa. Projektin tavoitteena oli kahdentaa pääkonttorin tietoliikenneyhteydet toisella operaattorilla, siirtää noin puolet yrityksen toimipisteistä uuden operaattorin verkkoon ja mahdollistaa kahden operaattorin välinen kilpailutus tulevaisuudessa muiden toimipaikkojen liittymien osalta.

Aloituspalaveri uuden operaattorin kanssa pidettiin alkuvuodesta 2008 ja sen yhteydessä käynnistettiin projekti, jonka aikana suunniteltiin, rakennettiin ja testattiin uuden operaattorin yhteydet pääkonttorille ja pilottina toimivaan Vantaanportin toimipaikkaan. Kun pääkonttorin kahdennettu yhteys ja yhteydet Vantaanporttiin saatiin toimimaan halutulla tavalla, yliheitettiin pilottipaikka uuden operaattorin verkkoon.

Toimipaikan siirtäminen toisen operaattorin MPLS-verkkoon tehtiin luomalla uusi verkko Lemminkäisen tietojärjestelmiin, jolloin toimipaikan kytkeytyessä toisen operaattorin kautta pääkonttoriin, kaikki oli valmiina ja vain IP-osoitteet muuttuivat. Työssä on esitelty tarvittavat muutokset ja asetukset, joilla uusi verkko luodaan ja varmistutaan, ettei toimipaikan uuteen verkkoon siirtäminen aiheuta pitkää tietoliikennekatkosta tai muita suurempia ongelmia toimipaikan työntekijöille.

Onnistuneen pilottipaikan yliheiton jälkeen siirryttiin projektista tuotantovaiheeseen, jolloin yksittäisen toimipaikan yliheitto toisen operaattorin verkkoon oli dokumentoitu ja ”tuotteistettu” Lemminkäisen tietohallinnon osalta.

Työssä on esitetty myös ongelmakohtia edellisen operaattorin kanssa, kuin myös ongelmia uuden operaattorin käyttöönotossa.

Työtä voidaan käyttää ohjekirjana uusien toimipaikkojen yliheittojen suorittamisessa tai käyttöönotoissa Lemminkäisellä. Työtä voidaan myös hyödyntää vastaavanlaisessa projektissa Lemminkäisellä, samoin kuin myös muussa isossa yrityksessä.

Hakusanat	tietoliikenneoperaattori, VPN, MPLS

Helsinki Metropolia University of Applied Sciences **Abstract**

Author	Jarmo Laine
Title	Changing Internet service provider in large company
Number of Pages	61
Date	27 April 2009
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor	Heikki Strengell, Systems Specialist
Supervisor	Matti Puska, Principal Lecturer

The purpose of this thesis was to document Lemminkäinen Group's project of having a new Internet service provider working in parallel with the existing one. The main purpose of the project was to duplicate the head office's data communication lines with the new ISP, move half of the branch offices to work in the new ISP's network and to gain financial benefits by lauching a bidding contest between the ISP's.

Following the first meeting with the new ISP that was in the winter of 2008, the kick-off project was started. During the kick-off project a new network in the head office and in the pilot office in Vantaanportti was designed, built and tested. When the new network and new communication lines between head office and Vantaanportti were working properly, the office in Vantaanportti was moved into the new ISP's network.

Moving a branch office into the new ISP's MPLS network was done by creating new network in the data systems of Lemminkäinen. That way everything was ready by the time the new ISP was introduced, and only new IP-addresses were assigned. The necessary changes in data systems are presented in this thesis to make the ISP-to-ISP move as easy and quick as possible. That way the employees will not be harmed through a long break in data traffic.

After a successful pilot the kick-off project was ended, and the project's so called "stage of production" was started. At this point the move from ISP to ISP was documented, which made the following moves easy.

The problems with the previous ISP as well as the problems encountered in the introduction of the new ISP are presented in this thesis. This thesis may be used as a manual when moving branch offices from ISP to ISP or taking a new ISP's subscribers on board at Lemminkäinen. This thesis may be also used as a guide for doing similar projects at Lemminkäinen or in another large company.

Keywords	Internet service provider, VPN, MPLS

Sisällys

Lyhenteet, käsitteet ja määritelmät

@450	Lähes koko Suomen kattava langaton laajakaistaverkko, joka perustuu Flash-OFDM-tekniikkaan ja käyttää NMT-450-verkon entistä taajuusaluetta.
3G	*Kolmannen sukupolven matkapuhelinteknologia*. Langaton laajakaistaverkko, joka tarjoaa mobiiliyhteyden jopa nopeudella 2 Mbit/s.
ADSL	*Asymmetric Digital Subscriber Line*. Puhelinverkossa käytetty korkeiden taajuuksien modeemitekniikka.
ATM	*Asynchronous Transfer Mode*. Alun perin 1980-luvun puolivälissä kehitetty tiedonsiirtoteknologia.
b	*Bitti*. Tietotekniikassa käytettävän informaation pienin osa. Ilmaisee joko arvoa 1 tai arvoa 0.
BGP	*Border Gateway Protocol*. Internetin tärkein reititysprotokolla, joka hoitaa reitityksen autonomisten järjestelmien välillä.
DC	*Domain Controller; toimialueen ohjauskone*. Sisältää palveluita, jotka nopeuttavat toimialueen tietokoneiden toimintaa. Voi sisältää simerkiksi kopion päätoimialueen ohjauskoneen DNS-nimipalvelusta.
DHCP	*Dynamic Host Configuration Protocol*. Verkkoprotokolla, jolla jaetaan IP-osoitteita verkkoon kytketyille laitteille.
DNS	*Domain Name System; nimipalvelujärjestelmä*. Muuntaa IP-osoitteet verkkotunnuksiksi ja päinvastoin.
DSLAM	*Digital Subscriber Line Access Multiplexer.* Laite, joka erottaa tilaajaliitännässä puheliikenteen dataliikenteestä.
ESP	*Encapsulating Security Payload*. Tietokuorman salausprotokolla, jota käytetään mm. IPsecissä.
FEC	*Forwarding Equivalent Class*. FEC-luokka kertoo MPLS-verkossa, mihin palvelusvaatimusluokkaan kyseinen paketti kuuluu.
Gt	*Gigatavu*. Tavun moninkerta, binäärijärjestelmässä 2^{30} t.
IPLS	*IP-Only LAN-Like Service*. VPN yhteyksissä käytetty tekniikka, jolla yhdistetään useita lähiverkkoja.
IPsec	*IP Security*. Sarja protokollia, turvaamaan IP:n (Internet Protocol) tiedonsiirtoa.

IP	*Internet Protocol*. TCP/IP-mallin protokolla, joka IP-tietoliikennepakettien perille toimittamisesta pakettikytkentäisessä Internet verkossa.
IPv6	On nykyisen IP-protokollan IPv4 seuraajaksi kehitetty protokolla. Sen tärkein ero verrattuna IPv4:een on osoiteavaruuden laajuus.
IS-IS	*Intermediate System to Intermediate System*. Reititysprotokolla verkon parhaiden reittien laskemiseen.
L2F	*Layer 2 Forwarding*. Tunnelointiprotokolla, jota käytetään VPN-yhteyksissä.
LAN	*Local Area Network; lähiverkko*. Tietoliikenneverkko, joka on rajatulla maantieteellisellä alueella. Esimerkiksi yhden talon tietokoneiden muodostama tietokoneverkko.
LDP	*Label Distribution Protocol*. MPLS-tekniikassa käytetty leimanjakoprotokolla.
LSR	*Label Switch Router*. MPLS-verkon leimakytkentäreititin.
MAC	*Media Access Control*. Osoite, joka yksilöi jokaisen Ethernet-verkkoon kytkettävän laitteen. Osoite koostuu 12 heksadesimaalisesta numerosta ja se on kirjoitettu kiinteästi jokaiselle laitteelle jo tehtaalla.
Mbit/s	*Megabittiä sekunnissa*. Tiedonsiirtonopeutta kuvaava suure. Käytetään usein operaattoreiden ilmoittamissa yhteysnopeuksissa.
MPLS	*Multiprotocol Label Switching*. Nopean kytkentäisyyden ja IP-reitityksen yhdistävä tekniikka, jossa IP-pakettiin lisätään liikennevirran tunniste.
Mt	*Megatavu*. Tavun moninkerta, binäärijärjestelmässä 2^{20} t.
Mt/s	*Megatavua sekunnissa*. Tiedonsiirtonopeutta kuvaava suure. Käytetään usein tiedoston kopioimisen yhteydessä.
NAT	*Network Address Translation; osoitteenmuunnos*. Prosessi, jolla voidaan piilottaa ja säästää IP-osoitteita. Käytetään erityisesti julkisten IP-osoitteiden kanssa.
OSI-malli	*Open Systems Interconnection Reference Model*. Tiedonsiirtoprotokollien kuvaaminen seitsemässä kerroksessa.
OSPF	*Open Shortest Path First*. Dynaaminen reititysprotokolla.
PE	*Provider Edge; palveluntarjoajan reunakohta*. Esimerkiksi PE-reititin on palveluntarjoajan reititin, johon asiakkaat yhdistyvät.

PPP	*Point-to-Point Protocol.* Protokolla, jota käytetään muodostamaan yhteys kahden pisteen välille. Voi sisältää myös tietoturvaa parantavia toiminteita, kuten käyttäjän tunnistus ja salaus.
PPVPN	*Provider Provisioned Virtual Private Networks*. Erilaiset VPN-tekniikat koottuna yhteen.
PPTP	*Point-to-Point Tunneling Protocol*. Tunnelointiprotokolla, jota käytetään VPN-yhteyksissä.
QoS	*Quality of Service; palvelunlaatu*. Tietoliikenteen tärkeyttä kuvaava arvo.
SNMP	*Simple Network Management Protocol*. Tietoliikenneprotokolla, jota käytetään TCP/IP-verkkojen hallinnassa.
t	*Tavu*. Tietotekniikassa käytetty tallennuskapasiteetin mittayksikkö. 1 t = 8 b.
TCP/IP	*Transmission Control Protocol / Internet Protocol*. Usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.
TO1	*Tietoliikenneoperaattori 1*. Lemminkäinen Oyj:n edellinen tietoliikenneoperaattori, jonka rinnalle uusi operaattori otettiin.
TO2	*Tietoliikenneoperaattori 2*. Lemminkäinen Oyj:lle käyttöönotettu uusi tietoliikenneoperaattori.
VPN	*Virtual Private Network; virtuaalinen yksityisverkko*. Tietoliikenneverkko, joka on rakennettu yksityiseen käyttöön julkisen infrastruktuurin välityksellä.
VPLS	*Virtual Private LAN Service*. Lähiverkkojen yhdistämistekniikka.
VPWS	*Virtual Private Wire Service*. Lähiverkkojen yhdistämistekniikka.

1 Johdanto

Suurissa organisaatioissa jaetaan tietoa useiden kymmenien kiinteiden toimipisteiden, satojen työmaiden ja tuhansien työntekijöiden kesken taukoamatta, kellonajasta ja paikasta riippumatta. Aikana, jolloin verkosta pois kytkettynä oleminen koetaan kuin olisi kytketty ulos maailmasta, eivät toimintavarmat ja nopeat tietoliikenneyhteydet ole pelkästään kaiken tehokkaan toiminnan edellytys vaan itsestäänselvyys. Näin oli Lemminkäinen Oyj:ssä vielä talvella 2007, jonka jälkeen yhteistyö tietoliikenneoperaattorin kanssa alkoi mennä hankalaksi.

Tämän opinnäytetyön tarkoituksena on dokumentoida tietoliikenneoperaattorin vaihto ja kahden tietoliikenneoperaattorin rinnakkaiskäyttö Suomen suurimpiin rakennuskonserneihin lukeutuvassa Lemminkäinen Oyj:ssä.

Lemminkäinen-konserni toimii kaikilla rakentamisen osa-alueilla, ja se on jaettu neljään toimialaan:

Talonrakentaminen (Lemminkäinen Talo Oy tytäryhtiöineen)

- asuinrakentaminen
- liike- ja toimitilarakentaminen
- teollisuus- ja logistiikkarakentaminen
- urheilu- ja vapaa-ajanrakentaminen

Infrarakentaminen (Lemminkäinen Infra Oy tytäryhtiöineen)

- tie-, katu- ja rataverkoston rakentaminen ja ylläpito
- kallio- ja pohjarakentaminen

Talotekniikka (Tekmanni Oy tytäryhtiöineen)

- talo- ja kiinteistötekniikka
- teollisuuspalvelut

Rakennustuotteet (Lemminkäinen Katto Oy, Lemminkäinen Betonituote Oy ja Omni-Sica Oy)

- katto- ja vedeneristystuotteiden sekä betoni- ja ympäristötuotteiden valmistus, myynti ja urakointi. [1.]

Lemminkäinen konsernin toiminta on painottunut Itämeren ympäristöön mutta asiakkaita palvellaan rakentamisen erikoisosaamisella ympäri maailmaa. Konsernin palveluksessa on noin 9200 henkilöä, joista neljännes työskentelee ulkomailla. Lemminkäinen-konserniin kuuluvilla 35 yrityksellä on Suomessa kiinteitä toimipisteitä noin 70 ja käynnissä olevien työmaiden määrä vuonna 2008 vaihteli 150–200 välillä. [1.]

Tietoliikenneoperaattorin vaihto saattaa asiaan perehtymättömälle kuulostaa tunnin vierailulta uuden operaattorin myyntitoimistossa. Kun puhutaan kahden eri tietoliikenneoperaattorin rinnakkaiskäytöstä, tuhansien käyttäjien MPLS (Multiprotocol Label Switching) -verkossa ja hallituista toimistokohtaisista yliheitoista operaattorilta toiseen, nousee toiminnan suunnittelu ja testaus yhdessä operaattorin kanssa kantavaksi osaksi koko projektia ja kestää helposti useita kuukausia.

Työn esimerkkitapauksena käsitellään vuonna 2008 toteutunutta projektia Lemminkäinen Oyj:ssä, jonka pohjalta on laadittu yksityiskohtainen dokumentointi tietoliikenneoperaattorin vaihdosta suuressa yrityksessä. Työssä käsitellään operaattorin vaihtoon liittyviä syitä, ongelmia ja käytännön järjestelyjä nykyajan tietoliikennekriittisessä maailmassa. Työ vastaa muun muassa kysymyksiin, miten kyseinen projekti käynnistetään, millaisia asioita tulee huomioida ja miten se päätetään tekniseltä kuin myös taloudelliselta kannalta hyvään lopputulokseen.

Työssä kerrotaan ongelmatilanteista edellisen operaattorin kanssa, kuin myös yrityksen saamasta palvelusta uuden operaattorin kanssa. Jotta operaattoreiden mainostamiselta, niin hyvässä kuin huonossa, vältytään, käytetään työssä operaattoreiden nimien tilalla aliaksia TO1 ja TO2 (tietoliikenneoperaattori 1 ja 2).

Päätäntöosassa pohditaan miten Lemminkäisen tilanne muuttui vuoden 2007 tilanteeseen nähden, miten projektissa onnistuttiin ja mitä tietoliikenneoperaattorin vaihdolla saavutettiin.

2 VPN – virtuaaliset yksityisverkot

2.1 Mihin virtuaalista yksityisverkkoa tarvitaan

Etäkäyttö on tärkeämpää kuin koskaan aikaisemmin ja vaikuttaa tulevan tärkeämmäksi edelleen, kun organisaatiot ovat levittäytyneet usealle paikkakunnalle ja jopa useaan eri maahan mutta kaikki toimipaikat tarvitsevat saman tiedon ja pääsyn samoihin palveluihin, jotka on useimmiten keskitetty organisaation pääkonttoriin. Myös mobiilien käyttäjien tulee päästä samoihin palveluihin käsiksi paikasta ja ajasta riippumatta. Edes syvimmässä metsässä ei tarvitse olla tiedotteiden tavoittamattomissa, kun sähköposti liitetiedostoineen ja kuvineen vastaanotetaan puhelimella ja kannettava tietokone yhdistyy organisaation verkkoon mobiiliverkon välityksellä. [2, s. 48.]

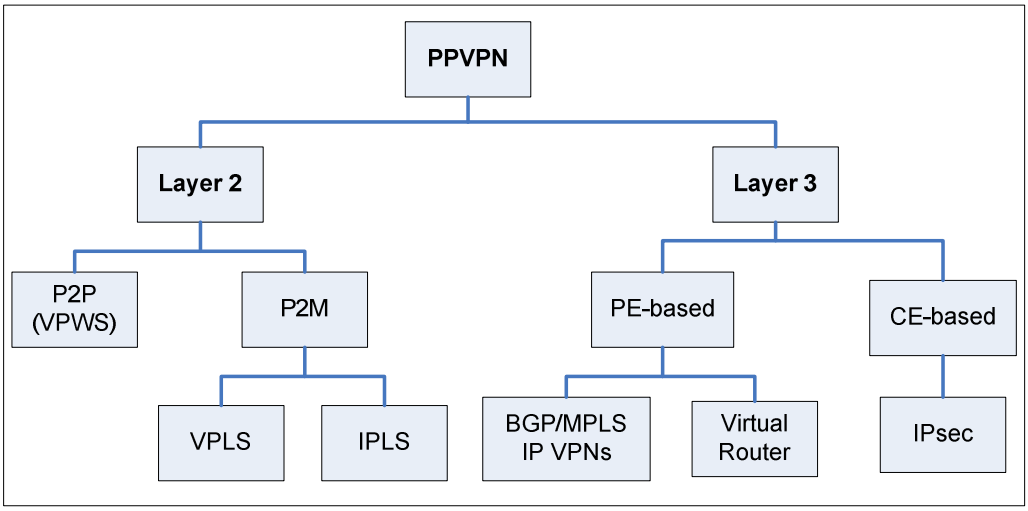
Palveluiden keskittäminen ja niiden etäkäyttö tuo mukanaan ongelman nimeltään tietoturva tai pikemminkin turvattomuus. Tärkeään tietoon on päästävä käsiksi mistä ja milloin vain, jolloin liikennöintiin on käytettävä julkista Internetiä. Mutta miten saadaan tieto turvallisesti julkisen verkon läpi? Entä olisiko mahdollista päästä käyttämään kaikkia samoja palveluja kuin pääkonttorin sisäverkosta? Turvallisen liikennöinnin julkisen verkon läpi mahdollistaa VPN (Virtual Private Network), joka nimensä mukaan muodostaa virtuaalisen yksityisverkon kahden pisteen välille.

Virtuaalinen yksityisverkko käsitteenä

Dave Kosiur [3, s. 19] yksinkertaistaa VPN:n määritelmän seuraavasti: virtuaalinen yksityisverkko on virtuaalipiireillä rakennettu verkko, jonka läpi kuljetetaan yksityistä liikennettä. VPN on siis julkisesta verkosta asiakkaan käyttöön määritetty looginen verkko, joka mahdollistaa sisäverkon turvallisen jatkamisen julkisen infrastruktuurin läpi [4]. Näiden määritysten mukaan VPN voi laajimmillaan tarkoittaa mitä hyvänsä yksittäisen asiakkaan mistä hyvänsä julkisesta verkosta määriteltyä loogista verkkoa [4].

Käytännössä VPN käsitteenä ei kerro mitään tekniikasta, jolla verkko toteutetaan ja teknologian pitkän historian aikana virtuaalisia yksityisverkkoja on rakennettu niin

monella tavalla ja niin moniin eri tarkoituksiin, että aluksi on hyvä määritellä aihe josta puhutaan [4]. Andersson ja Madsen [5] jaottelevat erilaiset palveluntarjoajien verkkoa hyödyntävät VPN-ratkaisut eli PPVPN:t (Provider Provissioned Virtual Private Network) kuvan 1 mukaisesti.



Kuva 1. Jako erilaisten PPVPN teknologioiden kesken. [5]

PPVPN:t jaetaan kuvassa 1 kahteen osaan, OSI-kerrosten mukaan. Siirtoyhteyskerroksella (Layer 2) VPN-yhteydet luodaan P2P (Point-to-Point) eli kahden laitteen välille tai P2M (Point-to-Multipoint) eli yhdestä laitteesta useaan laitteeseen. P2M-yhteydet luodaan käyttämällä VPLS:ää (Virtual Private LAN Service) tai IPLS:ää (IP-Only LAN-Like Service), joiden avulla on mahdollista yhdistää useita lähiverkkosegmenttejä, jolloin yhteenkytketyt segmentit saadaan käyttäytymään kuin yksittäinen lähiverkko. [5; 6, s. 97.]

Tämän työn kannalta ei ole tarpeellista paneutua kuin siihen osaan, joka käsittelee käytännön osuudessa käytettyä tekniikkaa. Tutustumme siis tekniikkaan, jota Lemminkäinen käyttää yhdistäessään toimipisteitä keskenään ja etätyöntekijät sisäverkkoon. Tämä tapahtuu kolmoskerroksen VPN:llä.

Tarjoajapohjainen (PE-based) VPN on palveluntarjoajan laitteilla tehty VPN-yhteys, jossa eri toimipisteiden asiakaspään laitteet näkevät toisensa, kuin olisivat samassa sisäverkossa. Tällöin palveluntarjoajan laitteet tietävät liikenteen olevan VPN-

liikennettä ja reitittävät liikenteen tunneleiden läpi. Reititys perustuu vastapään IP-osoitteeseen tai pakettiin lisättyyn IP-otsikkotietoon. Tarjoajapohjaisessa VPN-ratkaisussa voidaan hyödyntää liikenteenhallintaa ja parantaa verkon suorituskykyä. [5.]

Asiakaspohjainen (CE-based) VPN on asiakkaan hallinnoima virtuaalinen yksityisverkko. Asiakaspohjaisessa ratkaisussa asiakas hoitaa itse tunneloinnin omalla laitteistollaan (VPN-reititin, palomuuri), joka sijaitsee sisäverkon ja palveluntarjoajan verkon välissä. Sama asia voidaan toteuttaa myös ohjelmallisesti, ilman erillistä VPN-reititintä tai -palomuuria. Tässä tapauksessa palveluntarjoaja ei ole tietoinen, että sen läpi kulkee VPN-liikennettä ja liikenne reititetään samalla tavalla kuin julkinen liikenne. Tämä heikentää VPN-yhteyden suorituskykyä. [5.]

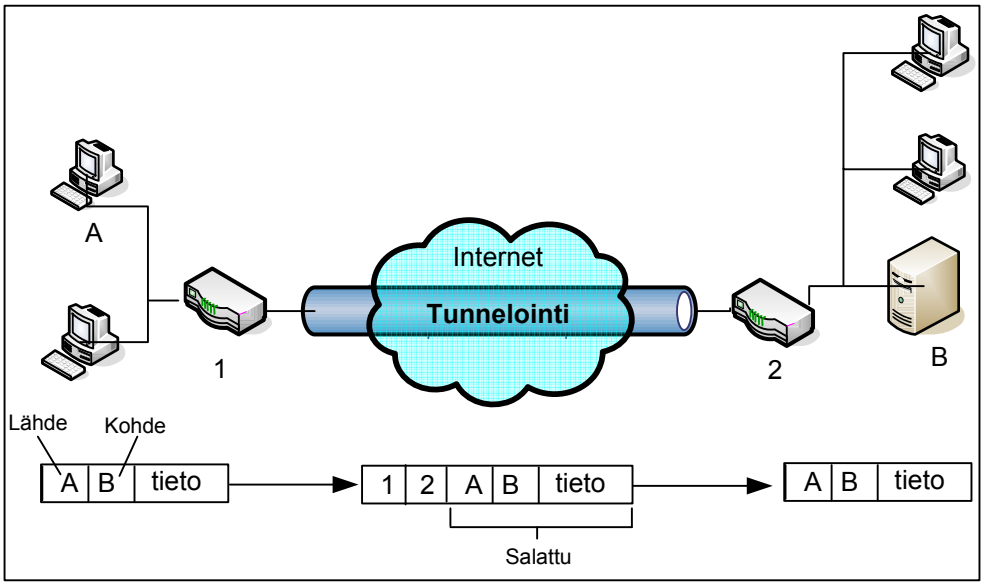
2.2 Virtuaalisten yksityisverkkojen rakenne

Internetin läpi muodostuva VPN (Internet VPN) voidaan prosessina jakaa karkeasti kahteen osaan, virtuaalisuus ja yksityisyys. Tunnelointi on niistä ensimmäinen ja se muodostaa virtuaalisen osan VPN:stä; toinen osa on useat tietoturvaan liittyvät toimenpiteet, jotka pitävät VPN-yhteyden läpi kulkevan tiedon yksityisenä. [3, s. 39.]

2.2.1 Tunnelointi

Virtuaalisissa yksityisverkoissa virtuaalisuus tarkoittaa sitä, että yhteys on dynaaminen, eli yhteyttä ei ylläpidetä vaan se muodostetaan vain silloin, kun sitä tarvitaan. Kun yhteys on pois käytöstä, vapautetaan kaista muulle liikenteelle. Virtuaalisella tarkoitetaan myös sitä, että vaikka yhteys muodostetaan julkisen Internetin ja palveluntarjoajan verkon läpi, ei käyttäjälle tai edes laitteille näy mitkään muut kuin oman sisäverkon laitteet. Palveluntarjoajan ja Internetin rakenteen piilottamista kutsutaan tunneloinniksi. Käsitteenä tunnelointi kuvaa tapahtumaa erittäin hyvin, sillä se on kuin ajettaisiin junalla vuoren läpi kulkevaan rautatietunneliin, jolloin itse nähdään vain tunnelin lähtö- ja loppupiste eikä myöskään tunnelin ulkopuolelta voi matkaajia tunnelin aikana nähdä. [3, s. 40.]

Tunneloinnissa lähetettävä paketti tiivistetään IP-paketiksi, jolloin alkuperäinen paketti salataan ja siihen liitetään ylimääräinen otsikkotieto, joka sisältää lähde- ja kohdeosoitteen. Tunnelin toisessa päässä yhdyskäytävässä erotetaan ylimääräinen otsikkotieto, puretaan salaus ja välitetään paketti alkuperäisen kohdeosoitteen osoittamaan paikkaan (kuva 2). Tunnelin pää voi olla joko yksittäinen tietokone tai lähiverkon päätelaite, kuten reititin tai palomuuri. Kytkettäessä VPN-yhteys lähiverkosta lähiverkkoon (LAN-to-LAN), hoitavat päätelaitteet tunneloinnin ja lähiverkkojen tietokoneet pystyvät keskustelemaan keskenään samassa lähiverkossa. Kun yksittäinen tietokone kytkeytyy VPN-yhteydellä lähiverkkoon (client-to-LAN), käytetään yksittäisessä koneessa VPN-yhteyteen tarkoitettua ohjelmistoa, joka suorittaa tunneloinnin. [3, s. 40–41.]

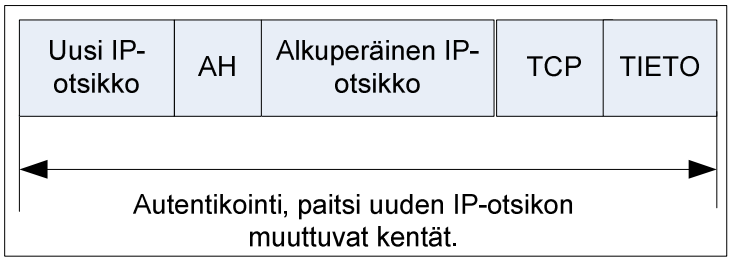


Kuva 2. Pakettien kulku tunneloinnissa. [3, s. 41]

2.2.2 VPN-protokollat

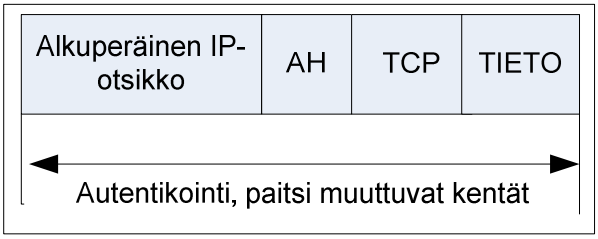
IPsec (IP security) on nykypäivänä käytetyin VPN-protokolla, ja se tarjoaa IP-paketeille koskemattomuutta ja luottamuksellisuutta. Näitä tarjotakseen IPsec koostuu kolmesta perustekijästä, jotka tekevät siitä erityisen hyödyllisen VPN-protokollana: todennus (pakettitasolla, ei käyttäjätasolla), salaus ja avaimenhallinta. IPsec kehitettiin, koska alkuperäiset TCP/IP-protokollat eivät sisältäneet minkäänlaisia tietoturvaominaisuuksia. [2, s. 106.]

IPsecin todennuksessa voidaan käyttää AH-otsikkoa (Authentication Header), joka sisältää kryptografisen tarkistussumman IP-paketin sisällöstä. Kuten kuvista 3 ja 4 voi huomata, AH-otsikko lisätään IP-paketissa IP-otsikon eteen muiden mahdollisten otsikoiden jälkeen. [7, s. 21–23.]



Kuva 3. AH-tunnelointitilassa. [7, s. 21].

AH:lla on kaksi tilaa, tunnelointitila (kuva 3) ja kuljetustila (kuva 4).



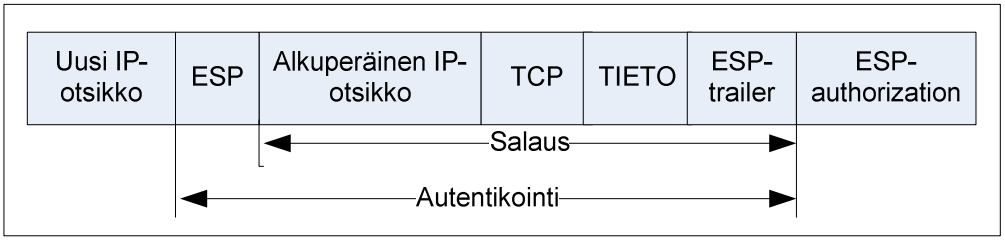
Kuva 4. AH kuljetustilassa [7, s. 21].

Salauksesta IPsecissä vastaa ESP-protokolla (Encapsulation Security Protocol). Kuten AH:ssa, ESP-otsikko asetetaan IP-paketissa otsikon eteen. ESP sisältää salauksen lisäksi

myös todennuksen. AH:ta ja ESP:tä voidaan käyttää myös yhdessä, jolloin todennus tehdään kahdesti. [2, s. 107.]

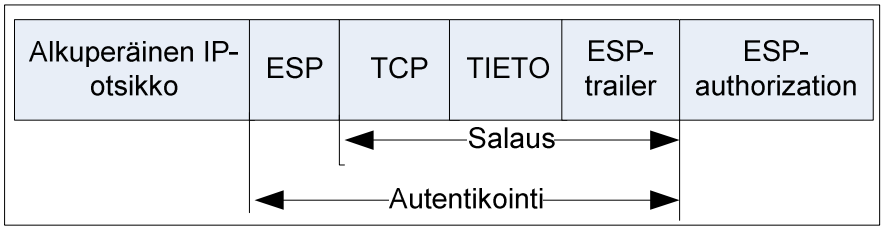
ESP:llä kaksi toimintatilaa – tunnelitila ja kuljetustila.

Tunnelitila kapseloi alkuperäisen IP-paketin ”uloimman” IP-paketin sisälle, muodostaen täysin uuden paketin, jonka kuormana alkuperäinen paketti on. Tunnelitilaa käytetään usein ”omana” tunnelointiprotokollana, koska se sisältää salauksen. [2, s. 107-108]



Kuva 5. ESP tunnelointitilassa [7, s. 22].

Kuljetustila lisää ESP-otsakkeen alkuperäiseen pakettiotsakkeeseen, ennen kuin se lähetetään edelleen. Käytetään kun alkuperäisen paketin tietokuorma on jo turvattu, ennen kuin se on lähetetty verkkoon. [2, s. 107–108.]



Kuva 6. ESP kuljetustilassa [7, s. 22].

ESP-protokolla tarjoaa sekä tiedon salauksen että eheyden tarkistuksen ja on siten turvallisempi kuin AH.

IPsecissa hyvää on:

- toimii itsenäisesti korkeampien OSI-kerrosten seassa
- on tehty osaksi IPv6:sta
- mahdollistaa IP-osoitteiden piilotuksen ilman NATin (Network Address Translation) käyttöä
- mukautuu uusiin salausmenetelmiin
- sisältää sisäänrakennetun salauksen ja todennuksen
- sisältää avaintenhallinnan
- on yhteensopiva eri laitevalmistajien kanssa. [3, s. 46; 2, s. 114; 7, s. 23.]

PPTP (Point-to-Point Tunneling Protocol) suunniteltiin helpottamaan turvattua tiedonsiirtoa etäasiakkaalta yrityspalvelimelle käyttäen Internetiä kuljetusvälineenä. PPTP muodostaa VPN:n tunneloimalla PPP-kehykset (Point-to-Point Protocol) TCP/IP-pohjaisen verkon, kuten Internetin, kautta. [2, s. 114.]

PPTP suoriutuu VPN-tunnelointiprotokollana monista asioista hyvin, mutta siinä on paljon ongelmakohtia, kuten

- heikko suorituskyky
- heikko laajennettavuus
- heikko turvallisuus. [2, s. 122–123.]

L2TP (Layer 2 Tunneling Protocol) on tunnelointiprotokolla, joka on yhdistelmä PPTP:n ja L2F:n (Layer 2 Forwarding) määrityksistä, jotka yhdistettiin yhdeksi protokollaksi. L2TP ei tue salausta, eikä ylipäänsä mitään edistynyttä turvallisuutta. L2TP on hyvä tunnelointiprotokolla ja sen kanssa suositellaan käytettävän IPsec-kuljetustilaa komento- ja valvontapakettien turvaamiseksi. L2TP on hyvä protokolla ja parempi kuin PPTP, muttei vastaa IPseciä. [2, s.124–134.]

2.2.3 Tietoturva ja yksityisyys

Internet koostuu käsittämättömän suuresta määrästä yhteen kytkettyjä verkkoja, joissa suurimmassa osassa kaikki tieto vaihdetaan salaamatta. Internet VPN:n suurimpana

hyötynä onkin tietoturva ja yksityisyyden takaaminen. VPN-yhteys antaa turvaa seuraaviin aiheisiin:

- Todennus varmistaa, että tieto tulee sieltä lähteestä, josta sen kuuluukin tulla.
- Pääsynhallinta pitää huolen, ettei verkkoon pääse käsiksi kukaan ulkopuolinen.
- Luottamuksellisuus varmistaa, ettei tunnelin läpi lähetettävää tietoa pääse lukemaan tai kopioimaan, sen matkatessa Internetin läpi.
- Eheys varmistaa että liikutettavaan tietoon ei pääse kukaan tekemään muutoksia. [3, s. 42.]

Tietoturvallisuuteen vaikuttavia toimenpiteitä voidaan suorittaa kaikilla OSI-mallin kerroksilla. Internet VPN:n tietoturvasta puhuttaessa, tapahtuu käyttäjien tunnistaminen ja tiedon koskemattomuuden varmistaminen OSI-mallin kakkos- ja kolmoskerroksilla eli siirtoyhteyskerroksella (Data Link layer) ja verkkokerroksella (Network layer). [3, s. 42–43; 6, s. 97.]

Vaikka jo tunnelointi itsessään sisältää salauksellisia toimenpiteitä ja se helpottaa tiedon siirtämistä Internetin läpi, ei se yksinään riitä turvaamaan tietoa. Käyttäjien tunnistamiseen ja tiedon koskemattomuuden varmistamiseen käytetään kryptografisia toimenpiteitä, kuten digitaalista allekirjoitusta ja salausta. Salaus ja digitaalinen allekirjoitus tehdään yksinkertaisimmillaan avaimen ja yksisuuntaisen funktion avulla, joita käytetään muuttamaan tieto mahdottomaksi ymmärtää, vaikka sen pystyisi lukemaan. Avain on suuri luku, joka sijoitetaan yksisuuntaiseen funktioon alkuperäisen tiedon kanssa ja tuloksena saadaan tieto salattuna. Funktio on julkinen ja se on teoriassa mahdollista ”laskea auki” mutta käytettynä satoja bittejä pitkän avaimen kanssa salauksen purkaminen nykytekniikalla ilman avainta kestäisi satoja vuosia. Avaimen avulla salaus voidaan kuitenkin purkaa helposti. [3, s. 42–43; 72–76.]

Tietoturvaan liittyvät toimenpiteet voidaan suorittaa suoraan kahden tietokoneen välillä (end-to-end) tai kahden päätelaitteen, kuten palomuurin tai reitittimen, eli kahden eri verkon välillä (node-to-node). Kahden verkon tapauksessa tietoturvaan liittyvät toimenpiteet ovat näkymättömiä käyttäjille, sillä palomuuri tai reititin hoitaa salaukselliset toimenpiteet. Kun VPN-yhteys muodostetaan kahden koneen välillä tai

tietokoneesta palomuuriin tai reitittimeen, suoritetaan salaukselliset toimenpiteet tietokoneeseen asennetulla ohjelmistolla ja käyttäjän salasanalla. Salasana voi olla pysyvä tai kertakäyttöinen, jolloin se voidaan jakaa käyttäjälle salasanageneraattorin avulla. [3, s. 43–44.]

2.3 MPLS-verkot

MPLS-tekniikassa (Multiprotocol Label Switching) IP-paketin eteen lisätään MPLS-verkon reunalla 32-bittinen tunniste (label), joka antaa lisäinformaatiota paketin reitityksestä. Leiman avulla jokaisen paketin kulku on ennalta määrätty MPLS-verkossa, ja näin IP-liikenne kulkee kuin yhteydellisessä verkossa. Leimaa käytetään paketin tunnistamiseen ja siten se osataan kytkeä eteenpäin oikealle reitittimelle. IP-paketin poistuessa MPLS-verkosta leima poistetaan ja paketti jatkaa matkaansa normaaliin tapaan IP-verkossa. MPLS:n etuna on se, että suurin osa paketin käsittelystä tehdään jo verkon reunalla ja jokaisen hypyn väliset laskutoimitukset on minimoitu, näin pakettien käsittely on nopeaa. [8, s. 9.]

2.3.1 Kolmoskerroksen MPLS IP VPN

MPLS IP-VPN palvelussa operaattori tarjoaa asiakkaalle virtuaalisen yritysverkon oman laajaverkkonsa sisällä. Operaattorilla on jokaiselle asiakkaalle oma reititystaulukko, joka mahdollistaa rekisteröimättömien IP-osoitteiden käytön asiakkaan verkossa. Yrityksen tietoliikenne eristetään julkisesta liikenteestä MPLS-tekniikalla ja näin saadaan laajennettua yrityksen sisäverkko kattamaan haluttu alue. Tällainen alue voi hyvin suuri, Lemminkäisen tapauksessa se on tällä hetkellä koko Suomi ja tulee mahdollisesti tulevaisuudessa leviämään myös ulkomaille. [9.]

Toimipisteiden välinen reititys voi olla vapaa tai rajoitettu. Mikäli reititys on vapaa, kaikista toimipisteistä voidaan liikennöidä suoraan muihin toimipisteisiin. Rajoitettua reititystä käytettäessä voidaan yksityiskohtaisesti määritellä, mistä pisteestä pääsee liikennöimään mihinkin toimipisteeseen. Lemminkäisen tapauksessa käytetään

rajoittamatonta reititystä, sillä kaikkea liikennettä ei tarvitse kierrättää pääkonttorin palomuurin kautta. [9.]

MPLS:n ajatuksena on, että reititinverkon ytimen, esimerkiksi Internet-operaattorin verkon, muodostaa joukko MPLS-toiminnallisuudella varustettuja reitittimiä. Tämän niin sanotun ydinverkon reunoille, esimerkiksi asiakkaiden toimipisteisiin, sijoitetut reitittimet jakavat sisään tulevan liikenteen merkityiksi tietovirroiksi, joille on ydinverkossa määritelty esireititetyt polut. [10.]

Ydinverkon reitittimet tutkivat paketeista vain tunnisteen ja kytkevät ne sen perusteella suoraan eteenpäin, reititystiedoista välittämättä ja päivittävät tunnistekentän vastaavasti. Näin reitittimien ei tarvitse tuntea koko polkua, vain omien porttiensa suhde määriteltyjen polkujen tunnuksiin riittää. Menettely muistuttaa tunnelointia, koska alkuperäisen osoiteinformaation sijasta paketit ohjataan ydinverkossa pelkkien tunnistekenttien perusteella. Mikäli tavoitteena on vain liikennevirtojen eristäminen toisistaan, eikä paketteja tarvitse salata, MPLS riittää VPN-infrastruktuurin luomiseen. [10.]

Kolmoskerroksen MPLS IP VPN:n toiminta

MPLS-verkon reitittimiä kutsutaan LSR-reitittimiksi (Label Switch Router). Verkon reunalla olevat LSR-reitittimet lisäävät IP-pakettiin oikean leiman, sen tullessa verkkoon tai vastaavasti poistavat leiman paketin poistuessa verkosta. Ennen oikean leiman käyttöä LSR-reitittimet ratkaisevat reitin, tai vaihtoehtoiset reitit kohteeseen. Jotta leimoja voidaan käyttää, ne täytyy jakaa verkkoon käyttämällä leimanjakeluprotokollaa, esimerkiksi juurikin siihen tehtävään kehitettyä LDP:tä (Label Distribution Protocol). Lisäksi pakettien kuljettamiseen ja reittien parametrien laskemiseen tarvitaan reititysprotokollaa, joista useimmiten käytettyjä ovat OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) ja BGP (Border Gateway Protocol). [8, s. 9–12, 11.]

Leima on yksikäsitteinen vain kahden toisiinsa kytketyn LSR:n välillä. Kukin LSR pitää omaa tunnistetaulua (label map), minkä mukaan paketti leimataan ennen edelleen lähettämistä. Leiman arvo määritellään paketin tarpeiden mukaan sen saapuessa reunareitittimelle. Reunareititin tarkastaa mitä verkkokerroksen palveluja paketti vaatii ja määrittelee sille FEC-ryhmän, sekä reitin verkon läpi, ottaen huomioon paketin vaatimat laatuvaatimukset (QoS). Reunareitittimellä leimattu paketti jatkaa matkaansa seuraavalle LSR:lle, joka hakee reittitaulustaan paketille uuden leiman edellisen tilalle ja lähettää paketin seuraavalle LSR:lle. Ennen kuin paketti saavuttaa MPLS-verkon toisen pään reunareitittimen, leima poistetaan siitä viimeistä edellisellä LSR:llä. Paketti lähetetään eteenpäin sen sisältämän verkko-osoitteen mukaan. [8, s. 10.]

MPLS-verkossa kulkeville paketeille on mahdollista määritellä vaihtoehtoisia polkuja ja paketit voidaan jakaa leimoilla eri luokkiin. Paketteja voidaan myös välittää ilman leimaa vaihtoehtoisia ennalta määrättyjä reittejä pitkin. MPLS-verkossa voi olla samaan aikaan eri palveluvaatimuksilla varustettuja paketteja. [8, s. 10.]

Palvelun laatu ja MPLS

MPLS:n lähtökohtana on varmistaa liikennöinnin laatu. Reitityksen korvaaminen kytkennällä ei sinänsä vaikuta pakettien läpimenoaikoihin tai kaistan riittävyyteen, mutta MPLS tarjoaa mahdollisuuden hallita tarjottavissa olevaa laatua. [10.]

Ruuhkatilanteessa paketteja kohdellaan eri tavoin, vaikka ne olisivatkin menossa samaa reittiä. Jos kaksi pakettia on menossa samaa reittiä, mutta niiden QoS-vaatimukset poikkeavat, kuuluvat paketit eri FEC-luokkiin ja tarpeen vaatiessa pienemmällä palvelutasolla matkaavat paketit reititetään vaihtoehtoista reittiä pitkin. [8, s. 15.]

Erilaisille poluille määritellään siis erilaiset laatuparametrit. Esimerkiksi Internet-operaattori, joka haluaa tarjota IP-puheelle tai videoneuvottelulle riittävän laatutason, voi ohjata nämä paketit polulle, jolle on varattu riittävästi kaistaa ja jolla viive on pieni. MPLS tuntee kiireellisyysparametrin ohella tärkeysparametrin, jolla voidaan varmistaa paketin perille pääsy. [10.]

Kaiken kaikkiaan MPLS-tekniikka tarjoaa turvallista ja tehokasta liikennöintiä palveluntarjoajan verkon läpi. MPLS-yhteyksillä toimipisteitä yhdistämällä myös verkonhallinta jää palveluntarjoajalle, mikä helpottaa yrityksen tietohallinnon toimia.

3 Tietotekniset ratkaisut Lemminkäinen Oyj:ssä

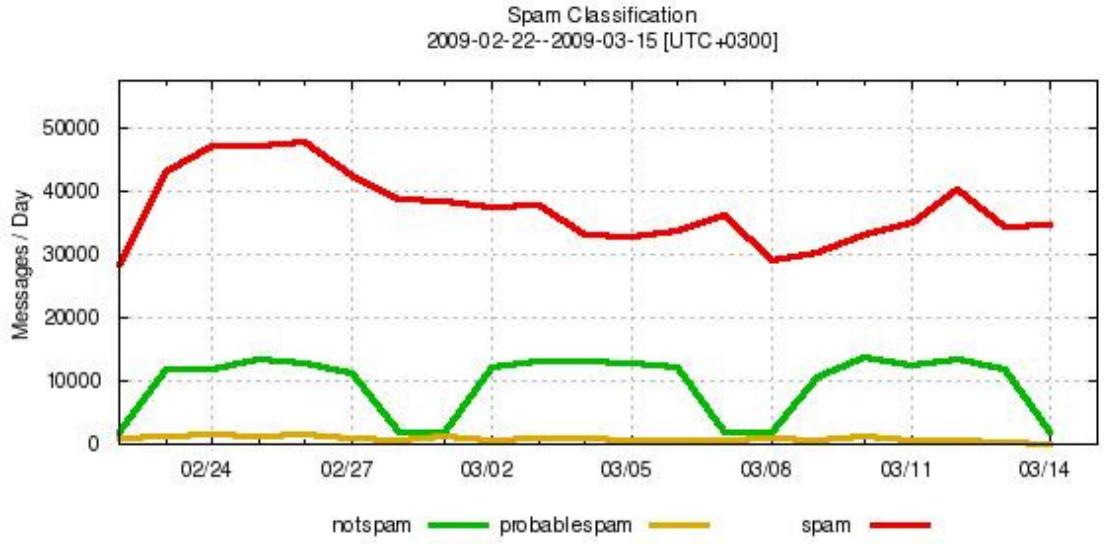
3.1 Pasila – kaiken keskus

Lemminkäinen-konsernin pääkonttori toimii vielä Helsingin Pasilassa, kunnes se muuttaa toiseen kaupunginosaan, Salmisaareen syksyllä 2009. Konsernin tietohallinnossa työskentelee noin 40 henkilöä, ja se on sijoitettu pääkonttorille. Pääkonttorin tietohallinnossa hoidetaan kaikki muut konsernin tietotekniset asiat, lukuun ottamatta Tampereelle keskitettyä ohjelmistosuunnittelua ja -kehitystä, jossa työskentelee kuusi henkilöä.

Pääkonttoriin on keskitetty lukematon määrä palveluita, joita käytetään ympäri maailmaa, esimerkiksi

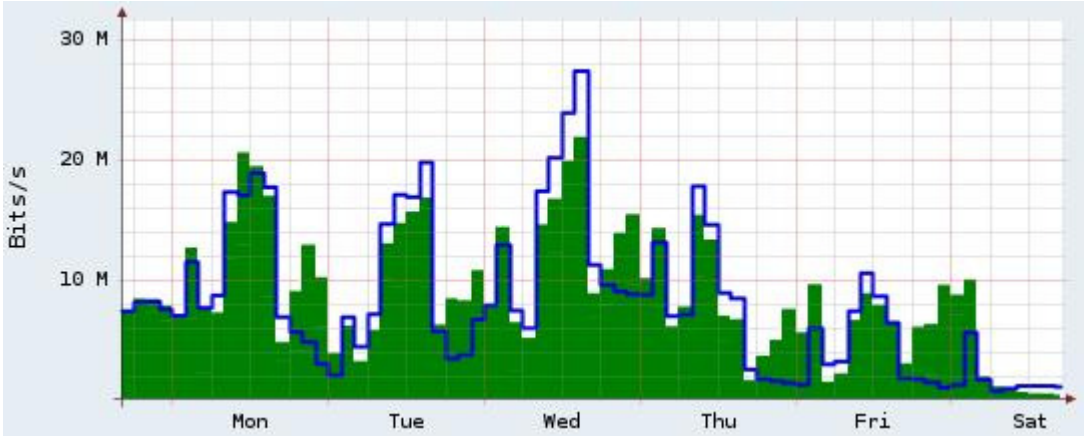
- sähköpostipalvelin (Exchange)
- metaframe-farmit
- lukuisia tietokantapalvelimia
- piirikonttorien varmistuspalvelimet
- mobiilisähköposti.

Pääkonttorin tietoliikenneyhteyksien kuormituksesta kertoo jo se, että jo pelkästään sähköpostia liikkuu joka päivä keskimäärin 47 000 kappaletta, joista suodatetaan päivästä riippuen noin 60–80 prosenttia roskapostina. Kuvassa 7 on esitetty sähköpostisuodattimen (Proofpoint) läpi kulkevan sähköpostin määrää kolmen viikon ajanjaksolta helmi–maaliskuussa 2009. Kuvassa 7 näkyy vihreällä normaalin sähköpostin määrä, joka on keskimäärin arkisin 11 000 ja viikonloppuisin 1800 viestiä päivässä, määrissä on niin lähetetty kuin vastaanotettukin posti.



Kuva 7. Roskapostin osuus sähköpostiliikenteestä. Punainen on roskapostia, vihreä normaaliliikennettä ja keltainen epäiltyä roskapostia.

Kokonaisliikenteen määrästä saa paremman kuvan tarkastelemalla pääkonttorin palomuurin läpi kulkevaa liikennettä, joka on esitetty kuvassa 8. Vihreä väri kuvaajassa kertoo sisään tulevan ja sininen ulosmenevän liikenteen.



Kuva 8. Palomuurin läpi kulkeva liikenne viikon ajalta.

Työasemia koko konsernilla on aktiivikäytössä ja verkossa noin 3500 ja palvelimia noin 150 kappaletta.

3.2 Kiinteät toimipisteet

Lemminkäinen käyttää MPLS IP VPN tekniikalla toteutettua yritysverkkoa kiinteissä toimipisteissä. Liikennettä prosessoidaan keskitetysti pääkonttorilla sijaitsevalla palomuurilla. Suurin osa sisäverkon liikenteestä toimipisteestä toiseen ja kaikki julkiseen Internetiin kulkeva liikenne kiertää Pasilan kautta.

Varmistukset ja tiedonsiirto

Suuremmissa piirikonttoreissa on tiedostopalvelimet paikallisia varmistuksia varten ja toimialueen ohjauskoneet (Domain Controller) nopeuttamaan kirjautumista sekä palveluiden toimintaa (taulukko 2). Pienemmissä piirikonttoreissa on palvelimen virkaa ajaa tiedostopalvelimena toimiva työasema. Kaikkialla varmistetaan tietokonetta sammutettaessa käyttäjän henkilökohtaisen työaseman ”Omat Tiedostot” -kansio, käyttäjän kotihakemistoon, piirikonttorin palvelimelle. Käyttäjät voivat myös käyttää tallennusvälineenä tätä palvelimella sijaitsevaa kotihakemistoa (H-asema käyttäjän koneella). Päivittäin varmistetaan muuttuneet tiedostot ja viikoittain kaikki tiedostot piirikonttoripalvelimelta pääkonttorille.

Tämän lisäksi käyttäjät käyttävät yhteisiä tiedostoja suoraan palvelimilta, jotka ovat useimmiten eri paikassa kuin käyttäjän oma piirikonttori (Y-asema käyttäjän koneella). Hyvä esimerkki tästä on Pasilan palvelimelle tallennettu, suunnittelijan tekemä työmaan piirroskuva, jota kaikkien asianomaisten ympäri Suomea on päästävä yhtä aikaa lukemaan. Toisinaan tällaiset kuvat saattavat olla jopa kymmenien megatavujen kokoisia.

Tietoa liikkuu siis huomattavia määriä jo pelkkien varmistusten takia, sähköpostiliikenne on runsasta ja tietoa sekä tiedostoja vaihdetaan verkon kautta herkeämättä. Erilaisilla toimipisteillä on toki eroja, sillä jossain tehdään enemmän konttorityötä ja tietoa liikkuu enemmän, kun taas joissain toimipisteissä käydään vain lukemassa sähköpostit ja palataan taas lähialueella sijaitsevalle työmaalle. Joillekin

toimipisteille on myös keskitetty palvelimia, joiden palveluita myös lähialueen toimipisteet käyttävät.

Varmistusten vaikutus tietoliikennenopeuden valintaan

Mikäli toimistolla on 20 käyttäjää ja jokaisella heistä on varmistettavia tiedostoja 2 Gt, on palvelimella yhteensä 40 Gt varmistettavaa pääkonttorille. Varmistusten tekemiseen niin toimiston sisällä kuin toimistolta pääkonttorille, käytetään komentosarjaa (script), joka vertaa tiedostoja edelliseen varmistukseen ja kopioi pelkästään muuttuneet tiedostot. Komentosarja vertaa jokaisen tiedoston päivämäärää ja kokoa ja kopioi vain tuoreimman version.

Jos päivänä X, toimipisteessä on käyttäjien tiedostoja yhteensä 40 Gt, on erittäin epätodennäköistä, että jokainen käyttäjä tekisi muutoksia jokaiseen tiedostoonsa tai tiedostojen määrä kasvaisi huomattavasti yhden varmistusvälin aikana. Kuitenkin kaikki tiedostot varmistetaan viikoittain, joten lasketaan onnistuisiko varmistusten lähettäminen Pasilaan yhden yön aikana linjanopeudella 4 Mbit/s.

1 t = 8 bit, 1 Gt = 8*10^9 bittiä, 1 Mbit/s = 10^6 bittiä / sekunnissa
40 Gt:n siirtämiseen pääkonttorille teoreettisella maksiminopeudella 4 Mbit/s kestää:
40*8*10^9 bit / 4*10^6 bit/s = 80000 s = 22 t 13 min
Yksi yö ei siis riittäisi koko varmistuksen tekemiseen, vuorokausi jo riittäisi.

Taulukkoon 1 on laskettu yhtälöiden 1 ja 2 avulla esimerkkejä teoreettisista maksimi-tiedonsiirtonopeuksista. Näihin nopeuksiin päästään käytännössä hyvin harvoin, sillä koko kaista on harvoin kuormittamattomana. Taulukko 1 antaa suuntaa antavan kuvan, millaisista ajoista puhutaan, kun varmistuksia on siirrettävä erilaisia määriä.

Kaistanleveys ilmoitetaan yleisimmin megabitteinä sekunnissa (Mbit/s), kun taas siirtonopeudet megatavuina sekunnissa (Mt/s).

$$xMbit/s = 1/8 * xMt/s$$

$$1Gt = 2^{30} t = 2^{30} * 8bit$$

$$1Mt = 2^{20} t = 2^{30} bit$$

Alla on esitetty yhden gigatavun siirtämiseen kuluva aika minuutteina yhtälössä 1,

$$\frac{Gt}{\frac{x}{8} Mbit/s} * \frac{1}{60s} = (\frac{2^{30} t}{\frac{x}{8} * 2^{30} \frac{t}{s}}) * \frac{1}{60s} \quad (1)$$

jossa **x** on kaistanleveys ilmoitettuna megabitteinä sekunnissa (Mbit/s) ja **t** on tietotekniikassa tallennuskapasiteetille määritelty mittayksikkö, tavu.

Yhtälössä 2 on esitetty yhden tunnin aikana siirretty tieto ilmoitettuna gigatavuina,

$$\frac{\frac{x}{8} * 2^{20} \frac{t}{s}}{2^{30} t} * (60 * 60)s \quad (2)$$

jossa x on kaistanleveys ilmoitettuna megabitteinä sekunnissa (Mbit/s).

Taulukko 1. Erilaisten kaistanleveyksien teoreettisia maksimisiirtonopeuksia.

Kaistanleveys (Mbit/s)	**Kaistanleveys** (Mt/s)	**1 Gt siirto** [1] (min)	**10 Gt siirto** (t)	**1 t siirto** [2] (Gt)	**9 t siirto** (Gt)
1	0,125	133,3	22,2	0,45	4,05
2	**0,25**	**66,7**	**11,1**	**0,9**	**8,1**
3	0,375	44,4	7,4	1,35	12,15
4	**0,5**	**33,3**	**5,6**	**1,8**	**16,2**
5	0,625	26,7	4,4	2,25	20,25
6	0,75	22,2	3,7	2,7	24,3
7	0,875	19,0	3,2	3,15	28,35
8	1	16,7	2,8	3,6	32,4
9	1,125	14,8	2,5	4,05	36,45
10	**1,25**	**13,3**	**2,2**	**4,5**	**40,5**
50	**6,25**	**2,7**	**0,4**	**22,5**	**202,5**

Tietoliikenneyhteyden nopeus valitaan piirikonttorin koon ja arvioidun tietoliikenteen määrän perusteella. Nopeuden valintaan vaikuttaa myös toimipaikan tarjoamat palvelut muille toimipaikoille. Esimerkkejä nopeuksista ja käyttäjämääristä on taulukossa 2.

Taulukko 2. Konttoreiden käyttäjämäärät ja tietoliikennenopeudet.

Paikkakunta	**Käyttäjämäärä**	**Tiedostopalvelin Palvelin / Työasema**	**Toimialueen ohjaustietokone Kyllä / Ei**	**Yhteysnopeus (Mb/s / Mb/s) MPLS IP-VPN**
Pasila	300 + etäkäyttäjät	Palvelin	Kyllä	50 / 50
Oulu	40	Palvelin	Kyllä	10 / 10
Joensuu	10	Palvelin	Ei	4 / 4
Lappeenranta	8	Palvelin	Ei	4 / 4
Muijala	5	Palvelin	Ei	4 / 4
Pori	10	Palvelin	Ei	4 / 4
Seinäjoki	12	Palvelin	Ei	4 / 4
Kajaani	4	Työasema	Ei	2 / 2
Mikkeli	6	Työasema	Ei	2 / 2
Raahe	5	Työasema	Ei	2 / 2

3.3 Työmaat

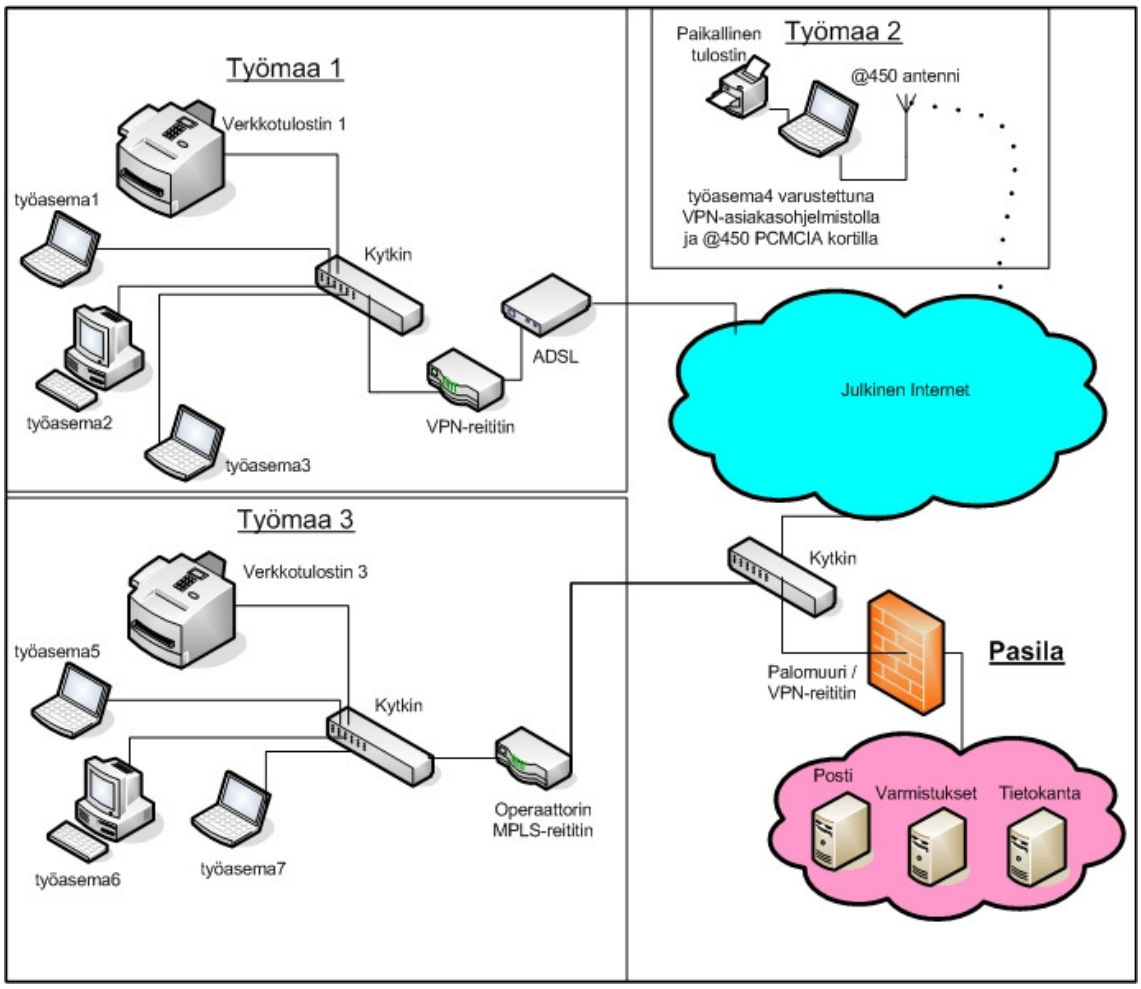
Toiminta on hyvin monipuolista, ja erilaisia työmaita ympäri Suomea avautuu ja sulkeutuu nopeassa tahdissa. Pienemmille ja lyhytkestoisemmille työmaille riittää kuuluvuusalueen niin salliessa langaton @450- tai 3G-yhteys ja IPsec VPN -tunnelointi asiakasohjelmiston (client) ja salasanageneraattorin (safeword token) avulla. Hyvä esimerkki mobiiliyhteyksiä käyttävästä yksiköstä on maantieverkostoamme kunnossapitävä päällystysyksikkö, jonka työmaa siirtyy useimmiten sitä vauhtia, kuin työt etenevät.

Riippuen työmaan kestosta ja yhteyksiä tarvitsevan henkilöstön määrästä työmaille hankitaan ADSL-yhteys (Asymmetric Digital Subsciber Line) tai yritysverkon liittymä eli MPLS IP-VPN. Taulukkoon 3 on listattu erilaisilla liittymillä ja käyttäjämäärillä varustettuja työmaita.

Taulukko 3. Työmaiden käyttäjämäärät ja yhteysnopeudet, sekä käytetty yhteysmuoto.

Paikkakunta	**Työmaan kesto (kk)**	**Käyttäjät**	**Yhteysmuoto**	**VPN-reititin / asiakasohjelmisto (client)**
Helsinki (Kortteli 63)	6	4	ADSL	VPN-reititin
Kerava	6	3	@450	asiakasohjelmisto
Salmisaari	48	30	MPLS IP-VPN	operaattorin MPLS-reititin

Kuvassa 9 on esitetty kolmen erilaisen työmaan peruskonfiguraatio. Työmaa 1:n esimerkistä nähdään, että IPSec VPN -tunnelointi voidaan tehdä keskitetysti käyttämällä VPN-reititintä ja jakamalla yhteys usealle käyttäjälle kytkimen avulla. Työmaa 2 on toteutettu mobiiliversiona, VPN asiakasohjelmiston avulla, kun taas Työmaa 3 on toteutettu MPLS IP-VPN -yritysliittymällä, jolloin liikenne ei kulje julkisen Internetin läpi matkallaan pääkonttorille.



Kuva 9. Työmaiden verkkojärjestelyjä.

Varmistukset työmailta

Käyttäjien ”Omat Tiedostot” -kansio varmistetaan työmaalta samalla tavalla kuin kiinteistä toimipisteistä ja varmistukset lähetetään sen toimipisteen palvelimelle, joka on lähimpänä työmaata, tai sen, joka on määritelty käyttäjän toimipisteeksi. Koska

työntekijät vaihtavat työmaita vilkkaaseen tahtiin, ei tietohallinnolla ole resursseja, eikä ole järkevää vaihdella yhtä mittaa käyttäjien varmistuspalvelinten sijaintia. Samalta työmaalta voi siis lähteä varmistuksia eri puolille Suomea, mikä aiheuttaa etenkin mobiiliyhteyksillä toisinaan hitautta henkilökohtaisten varmistusten tekemiseen.

4 Operaattorin vaihtoon liittyviä syitä

4.1 Lemminkäisen tilanne

Lemminkäinen Oyj on noin 15 vuoden ajan käyttänyt saman tietoliikenneoperaattorin palveluita. Uudesta toimipisteestä ja myös useimmiten avautuvasta työmaasta oli tieto hyvissä ajoin etukäteen ja näin tietoliikenneyhteydet saatiin tilattua operaattorilta ajoissa. Monissa paikoissa päästiin ihannetilanteeseen, eli liittymä on ollut käyttövalmiina, kun työmaan parakit on saatu paikoilleen ja yhteyksiä tarvitsevat työntekijät ovat saapuneet työmaalle.

Viime vuosina, johtuen muun muassa pörssitiedottamisen tuomasta asioiden tiedotusjärjestyksestä, työmaan alkamisesta on saatu varmuus vasta muutamia viikkoa ennen työmaan alkua. Valitettavasti samaan aikaan tietoliikenneoperaattorin toimitusajat ovat pidentyneet ja toimitusvaikeudet lisääntyneet. Samalla myös työmaahenkilökunnan keskitettyjen palveluiden määrä, laatu ja vaatimukset ovat kasvaneet ja omalta osaltaan kasvattaneet tietoliikenneyhteyksien tarpeellisuutta.

Useimmiten palvelut sijaitsee keskitetyssä paikassa, johon pääsee käsiksi monelta työmaalta yhtä aikaa. Seuraavassa listassa on mainittu esimerkkejä erilaisista tietoliikennettä vaativista toimenpiteistä ja palveluista, jotka helpottavat jokapäiväistä työskentelyä.

Dokumentinhallinta keskittää dokumentit yhteen pisteeseen kaikkien asianomaisten käytettäväksi paikasta riippumatta:

- piirustukset
- suunnitelmat

- listat työntekijöistä ja erikoismiehistä
- tiedotteet.

Sähköposti on monessa tilanteessa näppärämpi kuin matkapuhelin ja fakseista ollaan vähitellen luopumassa. Sähköpostilla hoituvat muun muassa

- tilaukset, kyselyt ja toimitukset eilaisissa hankinnoissa
- kuljetusten järjesteleminen
- tiedottaminen
- tiedon vaihto
- dokumenttien vaihto
- tuuraajien ja sairaspoissaolojen selvittäminen.

Keskitettyjen palveluiden avulla työmaan henkilöstö pitää toimistotyöntekijät ajan tasalla, samalla kun saavat tietoa työmaata koskevista asioista.

- Päällystysyksikön massantilausohjelma kertoo toimittajalle päivän tarpeen ja näyttää reaaliaikaisen tilanteen toimitusmahdollisuuksista.
- Kiviainesyksikön autovaakaohjelma punnitsee rekat louhoksella, josta yhteispaino autoa kohti lasketaan ja lähetetään sähköisesti eteenpäin toimistolle, jossa laskutus hoidetaan.
- Laskutusohjelmistot tarjoavat sähköisen laskunkäsittelyn, jolloin työmaalla tarkistetaan laskujen oikeellisuus ja laitetaan sitten eteenpäin toimistolle hyväksyttäväksi ja maksuun.

Kasvanut käyttäjien ja tietoliikenteen määrä on monissa toimipaikoissa ahtauttanut nykyiset kaistat. Tähän kun lisää TO1:n (Tietoliikenneoperaattori 1) kasvavat toimitusvaikeudet ja huonontuneen asiakaspalvelun, alkoi suunnittelu parempaan tilanteeseen pääsemisestä kehittyä tietohallinnon ytimessä. Toimistokohtaiset nopeuksien kasvattamisetkin olisi kätevä tehdä ilman lisäkustannuksia samalla kun operaattori vaihtuu. Alaluvussa 4.2 käsitellään ongelmatilanteita, jotka osaltaan helpottivat päätöstä uuden operaattorin hankintaan ryhtymiseksi.

4.2 Palvelun parantaminen

Hyvä asiakas, liittymän nopeus on nyt nostettu

Vuonna 2007 alkoi Hämeenlinnan piirikonttorin yhteysnopeus 2 Mbit/s / 512 Kbit/s käydä ahtaaksi. Päätettiin tilata operaattorilta yhteysnopeuden nosto symmetriseksi liittymäksi 2 Mbit/s. Aikaa kului noin viikko, jonka jälkeen operaattorilta tuli sähköpostitse ilmoitus nopeuden onnistuneesta nostosta. Uusi laskukin tuli ja hinta oli uuden nopeuden mukainen. Kaikki näytti menneen niin kuin piti.

Lemminkäisen tietohallinto vastaanotti kuitenkin edelleen Hämeenlinnan toimiston valituksia yhteyden hitaudesta. Mietittiin, josko symmetrinen liittymä 2 Mbit/s ei ole sittenkään riittävä. Päätettiin kuitenkin testata yhteysnopeus erilaisilla Internetistä löytyvillä nopeustesteillä. Luotettavammaksi osoittautui Speedtest.net [12], jonka testitulokset antoivat seuraavanlaisia tuloksia:

- latausnopeus (download) parhaimmillaan 1960 kbit/s
- lähetysnopeus (upload) parhaimmillaan 635 kbit/s.

Yhteys ei ollut nopeutunut tilauksen ja laskun mukaiselle tasolle. Asiasta lähetettiin reklamaatio TO1:lle, josta usean päivän jälkeen kuitattiin asia vastaamalla viestiin asian olevan kunnossa. Nopeus ei kuitenkaan ollut kasvanut. Tämän jälkeen asiasta on tehty kaksi uutta vikailmoitusta, joihin molempiin TO1 on vastannut ”vikaa ei ole”. Missään vaiheessa lähetysnopeus ei kuitenkaan kasvanut tasolle 2 Mbit/s.

Fyysinen media ja paikan sijainti vaikuttavat suuresti tietoliikenneyhteyden nopeuteen. Toisinaan ei ole edes mahdollista tarjota nopeampaa yhteyttä nykyisen tilalle ilman fyysisiä muutostöitä, kuten valokaapelin rakentamista talojakamoon. Kuitenkin tietoliikenneoperaattorin vastuulle jää selvittää suurin mahdollinen nopeus, jonka se voi asiakkaalleen tarjota. Harvoin teoreettisiin maksiminopeuksiin päästään ja 635 kbit/s on nopeampi kuin 512 kbit/s, mutta se ei silti vastaa tilattua ja maksettua lähetysnopeutta 2 Mbit/s.

Käsittämättömät laskut työllistävät

Liittymiä avataan ja suljetaan samassa tahdissa työmaiden kanssa. Toisinaan Lemminkäisen tietohallintoa kuormittavat työmaajohtajien kyselyt laskuista, joita TO1 on lähettänyt vielä useiden kuukausien jälkeen liittymän irtisanomisesta. Asia on useasti edennyt samalla kaavalla, eli työmaa on purettu, liittymä irtisanottu ja TO1 on myös purkanut yhteydet. Jostain syystä TO1:n sisäinen viestintä ei tunnu toimivan ja laskuja lähetetään edelleen työmaan nimellä ja osoitteella emoyhtiölle. Tällaisista tilanteista on useimmiten päästy yhteisymmärrykseen reklamoimalla TO1:lle ja ylimääräiset kuukausimaksut on palautettu. Samankaltaiset tilanteet uudelleen ja uudelleen läpikäytynä kuitenkin kuormittavat työmaiden johtajia ja tietohallintoa täysin turhaan.

Valitettavasti nämä ovat vain niitä tilanteita, jolloin asia on huomattu ja siihen on otettu kantaa. Suuressa organisaatiossa voi helposti käydä niin, että tarpeetonta ja irtisanottua liittymää maksetaan useita kuukausia, jopa vuosia, ennen kuin asiaan huomataan puuttua ja taloudelliset tappiot ovat aina todellisuutta. Mielestäni tietoliikenneoperaattorin asiakkaan ei tulisi joutua palkkaamaan henkilöä tekemään työtä korjatakseen operaattorin virheitä, vaan ideaali tilanne olisi se, että operaattori olisi selvillä omista asioistaan ja asiakas voisi luottaa siihen.

Vikoja ja viankorjausta

TO1:n ongelma on jo useita vuosia ollut asiakaspalvelun heikkous. Puhelimitse on ollut hankala päästä asiakaspalvelijalle asti ja sähköpostitse on vaikea lähettää vikailmoitusta, jos tietoliikenneyhteydet ovat poikki. Paras tilanne olisi se, että operaattorilla olisi organisaatiolle oma yhteyshenkilö, jolle voi soittaa suoraan, niin ongelmien, kuin tilausten tai irtisanomistenkin kanssa. Yhteyshenkilön ei toki tarvitsisi olla jokaisen asian huipputekijä, vaan voisi kirjata ongelman ja ohjata asian oikealle henkilölle eteenpäin.

Asiakas on valmis maksamaan paremmasta palvelusta

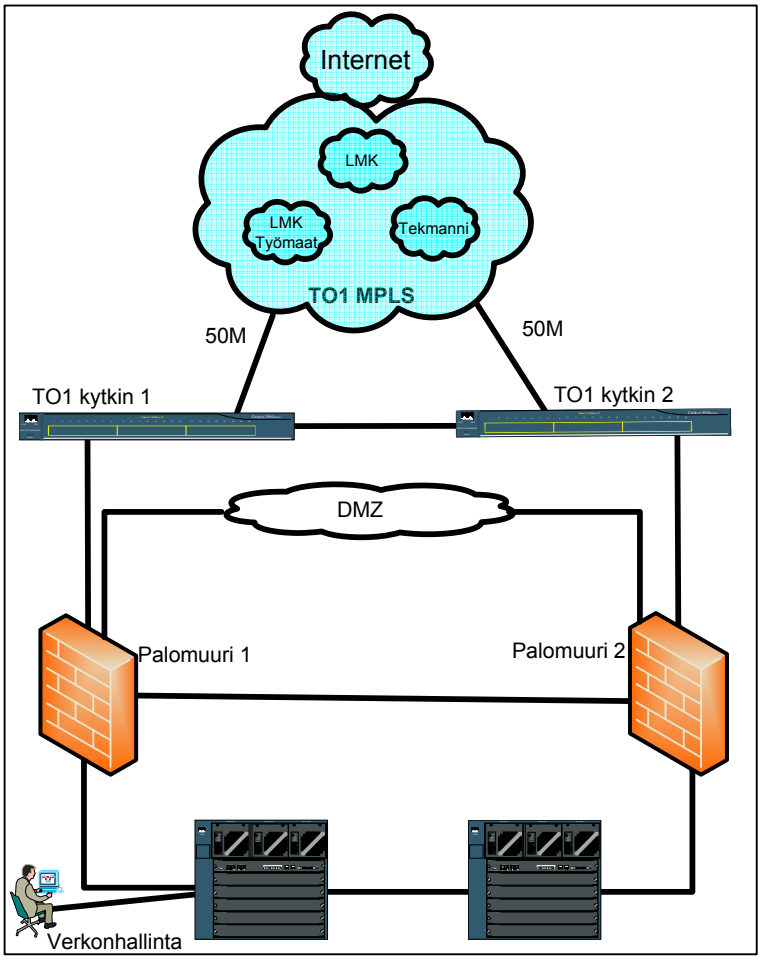
Kun alkoi näyttää siltä, että Lemminkäinen olisi lähdössä vaihtamaan tietoliikenneoperaattoria, kysyttiin mielipiteitä eri yksiköiden työntekijöiltä ja johtajilta. Kaikkia jotka olivat olleet itse TO1:n kanssa tekemisissä, yhdisti yksimielisyys siitä, että yksikkö on valmis maksamaan toisen operaattorin palvelukseen siirtymisen aiheuttamat kulut ja jopa ylimääräistä, kunhan palvelun laatua parannetaan.

5 Kahden operaattorin rinnakkaiskäyttö

5.1 Toimintavarmuuden parantaminen

Kuvasta 10 nähdään pääkonttorin verkkojärjestelyt ja se kuinka pääkonttori on varmistettu kahdella TO1:n kytkimellä, joista molemmista on 50 Mbit/s yhteys TO1:n MPLS:ään ja julkiseen Internettiin. Molemmat kytkimet ovat asetettu toimimaan samalla tavalla ja liikenne jakautuu niiden kesken. Jos toinen kytkimistä hajoaa, kaikki liikenne siirtyy toimimaan toisen kytkimen läpi.

Mikäli TO1:n runkoverkko lakkaa toimimasta tai molemmat kytkimet rikkoutuvat yhtä aikaa, vaikuttaisi se kaikkeen pääkonttorin läpi kulkevaan, huomattavaan määrään liikennettä ja koko konsernin liiketoimintaan, tytäryhtiöiden toimipaikasta tai maasta riippumatta.



Kuva 10. Pääkonttorin verkkojärjestelyt

Toimintavarmuuden parantamiseksi Pasila halutaan varmistaa toisen operaattorin MPLS verkolla ja samanlaisella verkkoasetelmalla, kuin TO1:llä kuvassa 10 jo on. Tällä tavoin liikenne saataisiin kahdennettua eri operaattoreilla, joilla molemmilla olisi kaksi kytkintä ja kaksi 50 Mbit/s linjaa omaan MPLS-verkkoonsa ja julkiseen Internetiin. Sisä- ja ulkoverkon liikenteen jakaminen kahden operaattorin kesken ja parantaisi myös huomattavasti verkon suorituskykyä.

Tämän lisäksi uusi yhteys rakennetaan kulkemaan toisen toimittajan DSLAMin (Digital Subscriber Line Access Multiplexer) kautta, sekä fyysisesti eri puolelta rakennusta, kuin edellinen yhteys kulkee. Näin saadaan maksimoitua yhteyksien toimintavarmuus.

5.2 Kilpailuttaminen

Jos organisaatiolla olisi kaksi tietoliikenneoperaattoria samaan aikaan käytössään, se mahdollistaisi kilpailuttamisen uusien liittymien hankinnassa ja nykyisten ylläpidossa. Kun saataisiin tieto uudesta toimipaikasta tai työmaasta, voitaisiin lähettää molemmille operaattoreille tarjouspyyntö ja valita tilanteen mukaan nopeimman toimituksen, halvimman hinnan tai jopa parhaan palvelun tarjoava operaattori. Tämä tietysti vaatii sen, että organisaation sisäiset järjestelmät mahdollistavat kahden eri operaattorin sekä kahden MPLS-verkon rinnakkaiskäytön.

5.3 Päätös aloittaa kahden eri operaattorin asiakkaana

Alun perin oli tarkoitus vaihtaa kaikki konsernin toimipaikat ja työmaat uuden operaattorin, TO2:n verkkoon ja jättää TO1 toimimaan vain pääkonttorin ulkoyhteyksien varmistuksessa. Suunnitteluvaiheessa kuitenkin huomattiin kahden operaattorin asiakkaana toimimisen tuomat edut ja päätettiin siirtää uuteen TO2 verkkoon noin puolet toimipisteistä. Mikäli toimipaikka muuttaa uuteen osoitteeseen, otetaan uusi liittymä TO2:lta. Mikäli toimipaikka niin haluaa, vaihdetaan liittymä TO2:lle. Pääkonttori tullaan varmistamaan uudella TO2:n liittymällä ja edellä suunnitellulla ratkaisulla.

Uuden operaattorin valinta

Lemminkäinen Konsernilla on ollut käytössään erilaisia operaattorin tarjoamia yritysverkon malleja. Kaksipiste -tyyppinen X.25 oli näistä ensimmäinen, jonka jälkeen käytössä oli Frame Relay ennen VPN:ää [2, s. 41–43]. Aina yhteystekniikan vaihtuessa on operaattorit kilpailutettu ja jokaisella kerralla kilpailu on tiivistynyt kahden operaattorin kaupaksi, jossa nykyinen TO1 oli aina vienyt voiton. Toiseen tilaan aiemmin taipunut operaattori oli kuitenkin hinta-laatusuhteeltaan reilusti edellä seuraavia, jolloin se tuli luonnollisena valintana uudeksi operaattoriksi. Ongelmat nykyisen operaattorin asiakaspalvelun kanssa yhdistettynä uuden operaattorin viime aikojen ”Vuoden Help Desk” -palkintoon myös edesauttoi valintaa omalta osaltaan.

6 Uuden operaattorin käyttöönotto

6.1 Aloituspalaveri

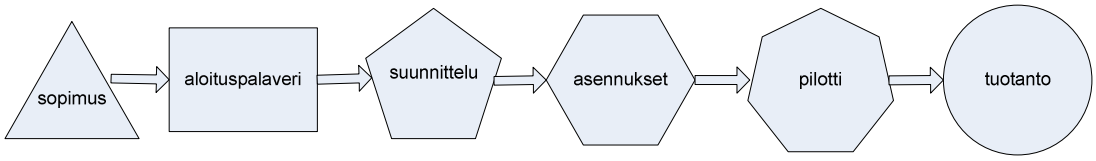
Kun sopimus saatiin neuvoteltua molempia osapuolia tyydyttäväksi, alettiin suunnitella uuden operaattorin käyttöönottoa. Aloituspalaveri pidettiin TO2:n tiloissa 3. maaliskuuta 2008, jossa kolmen Lemminkäisen edustajan ja kolmen TO2:n edustajan kesken mietittiin projektin vaatimia toimenpiteitä molempien osapuolten osalta ja rajattiin projekti. Taulukosta 4 selviää aloituspalaverin tärkeimmät päätökset ja lähiaikoina selvitettävät asiat.

Taulukko 4. Aloituspalaverin muistio [13]

Asia	**Vastuu**	**Kalmanlinja**	**Huomioita**
Pääkonttorin nielu tulee rakentaa kuntoon ensimmäisenä.	LMK TO2	-	-
Onko pääkonttorilla vapaita sisäkuituja talojakamosta laitetilaan.	LMK	14.3.2008	Ilmoitus TO2:lle
Pilotti, Elannontie 5, Vantaa, 4/4M (nyt 2/2M).	LMK TO2	-	Tehdään muistio
Verkkosuunnitelman toimitus TO2:lle	LMK	14.3.2008	-
Tekninen piirustus TO2 osalta.	TO2	28.3.2008	-
IP-osoitesuunnitelma, SNMP, DHCP ja DNS osoitteet TO2:lle.	LMK	14.3.2008	
DNS- ja sähköpostipalvelut toimivat Lemminkäisellä itsellään, eikä vaadi toimenpiteitä TO2:lta.	LMK	-	Tiedoksi
Selvitetään pääkonttorin palomuurin määritykset StoneGatelta.	TO2 LMK	14.3.2008	-
TO2:lle siirrettävien toimipisteiden yhteyshenkilöt ja puhelinnumerot on selvitettävä.	LMK	mahd. nopeasti	Lähetys TO2:lle
Selvitys TO1 BGP:n käytöstä.	LMK	14.3.2008	-
Pääkonttorin muutto.	LMK TO2	Kesä 2009	Tiedoksi

6.2 Aloitusprojekti

Projektissa valmistellaan kaikki toimenpiteet, jotka TO2:n ja Lemminkäisen tulee tehdä ennen kuin on mahdollista ottaa TO2:n yhteydet käyttöön ja yliheittää pilottina toimiva toimipaikka uuteen verkkoon. Pilotista tehdään dokumentti, joka mahdollistaa tuotantovaiheeseen siirtymisen, eli useampien toimipaikkojen turvallisen ja tehokkaan yliheiton ja uusien toimipaikkojen avaamisen TO2:n verkkoon. Projektin päätarkoituksena on minimoida työmäärä ja ongelmakohdat tulevassa tuotantovaiheessa. Projektin toteutuminen voidaan pelkistää kuvassa 11 esitettyyn malliin.

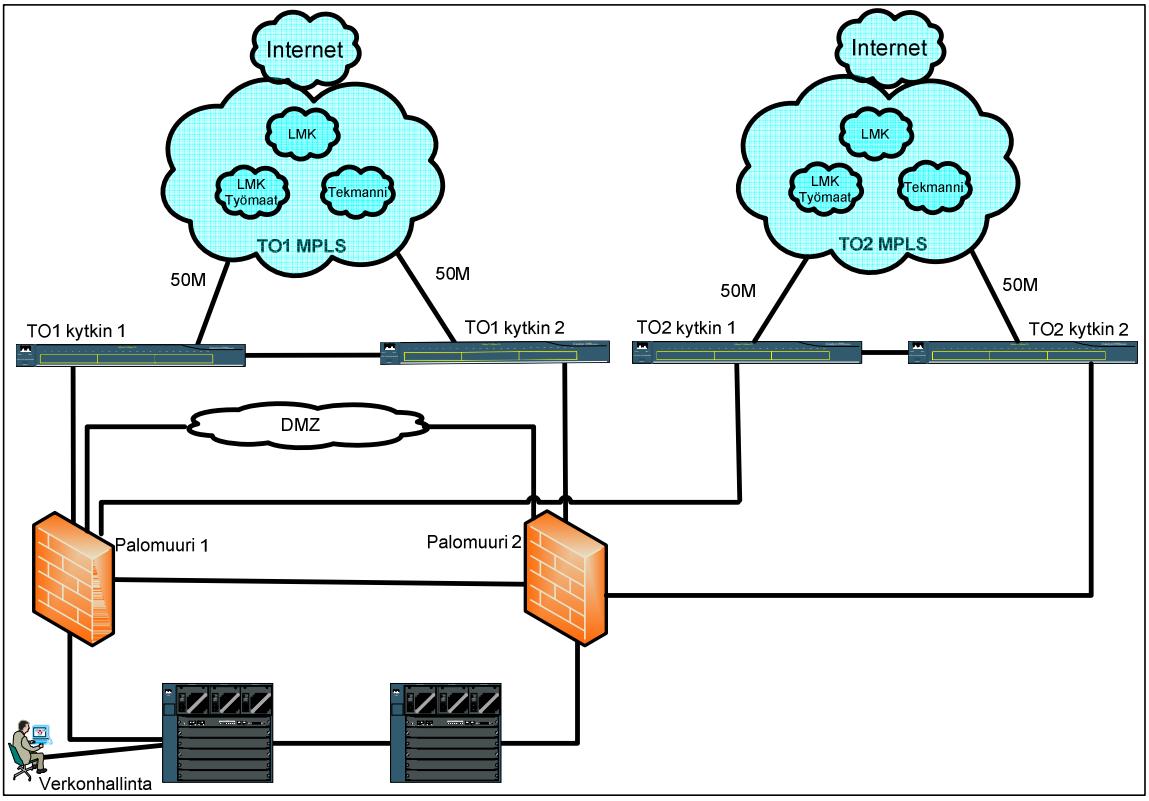


Kuva 11. Sopimuksesta tuotantoon.

Ensimmäisenä rakennetaan pääkonttorin uusi liittymä kuntoon, tarkoituksena jakaa liikenne pääkonttorilta ulkomaailmaan kahden operaattorin kautta (katso kuva 12).

Pääkonttorin uuden yhteyden valmistuminen on edellytys TO2:n verkkoon siirrettävien toimipisteiden MPLS-yhteyksien toiminnalle, koska kaikki liikenne kulkee pääkonttorin kautta.

Seuraavaksi selvitetään perinpohjaisesti oman verkon rakenne ja mietitään miten toisen operaattorin rinnakkaiskäyttö vaikuttaa siihen. Vaikka suunniteltuna lopputuloksena ei olisi ollut kahden operaattorin yhteiskäyttö, niin yliheiton aikana tultaisiin joka tapauksessa käyttämään kahta operaattoria rinnakkain.



Kuva 12. Pääkonttorin verkkoratkaisu kahdennettuna.

6.3 Tuotantovaihe

Projekti antaa tiedot ja määrittelee yhteiset toimintamallit jatkon suhteen niin operaattorille kuin Lemminkäisellekin. Tämän jälkeen siirrytään tuotantovaiheeseen, jolloin yliheittojen tulee olla rutiininomaista työtä molemmille osapuolille.

Tuotantovaiheessa prosessi liittymän tilauksesta yliheittoon voidaan suorittaa saman kaavan mukaan, yhteisiä toimintamalleja käyttäen. Lisää tuotantovaiheesta on kerrottu luvussa 10.

7 Yliheitto

7.1 Järkevin yliheittotapa

Koska kyseessä on usean toimipisteen organisaatio, on täysin mahdotonta yliheittää koko konserni toisen operaattorin verkkoon yhdellä kertaa. Uudet liittymät voivat ja kannattavat tilata samalla kertaa kaikkiin yliheitettäviin toimipisteisiin ja sitä mukaa kun niitä valmistuu, voidaan yliheittoja tehdä. Uusi liittymä rakennetaan jo olemassa olevan rinnalle, jolloin yliheitto voidaan suorittaa mahdollisimman kivuttomasti. Esimerkkitapauksessa tilattiin aluksi kahdeksan liittymää ja niiden valmistuttua lisää. Vaikka liittymiä tilattiin useampia ja niitä valmistuisi nopeaa vauhtia, ei yliheittoja olisi tarpeen kiirehtiä, sillä laskutus sovittiin alkamaan vasta liittymän käyttöönoton jälkeen.

Ennen pilottipaikan yliheittoa määriteltiin kolme asiaa, jotka korostavat yliheiton suunnittelun tärkeyttä.

- Yliheitot on pystyttävä tekemään tietohallinnon toimesta etäisesti, toimipisteessä paikanpäällä olevan yhteyshenkilön avulla. Tämä vaatii hyvää yhteistyötä ja kommunikointia yhteyshenkilön kanssa mutta helpottaa huomattavasti tietohallinnon työskentelyä, kun ei tarvitse yliheittojen takia matkustaa ympäri Suomea. Yhteyshenkilön toimenkuvasta yliheiton aikana on kerrottu lisää alaluvussa 8.2.
- Yliheitot tehdään virka-aikana (klo 8–16), mieluiten keskipäivällä, ruokatunnin yhteydessä ja yliheitettävän toimipisteen haluamana viikonpäivänä.
- Yliheiton aiheuttama tietoliikennekatkos saa kestää pisimmillään yhden tunnin.

7.2 Ennen yliheittoa

Ennen kuin uusi liittymä valmistuu, valmistellaan toimipistekohtainen verkko mahdollisimman pitkälle uutta liittymää varten, jotta yliheitto on mahdollista toteuttaa etäisesti yhden tunnin aikana.

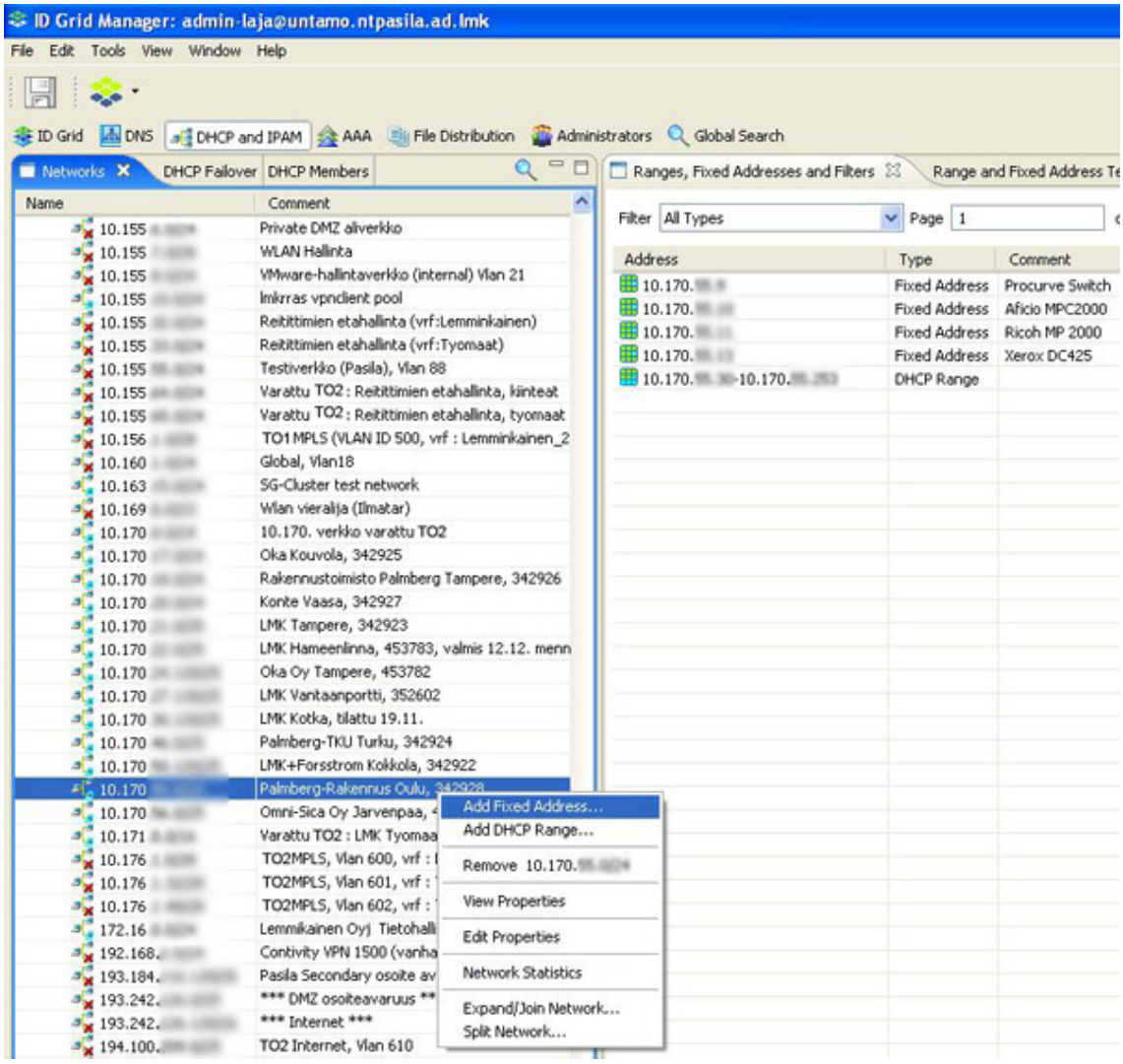
DHCP-palvelin ja verkkolaitteet

Lemminkäisellä on käytössään Infobloxin DHCP-palvelin, jonka asetuksia pääsee tarkastelemaan ja muuttamaan ID Grid Manager -hallintasovelluksen kautta (kuva 13). Periaatteena on, että verkkolaitteet on asetettu noutamaan IP-osoitteen automaattisesti verkosta, ja mikäli laite tarvitsee kiinteän IP-osoitteen, se määritetään DHCP-palvelimelle laitteen MAC-osoitteen perusteella.

Aluksi on hyvä listata toimipaikan nykyisen verkon kaikki laitteet joille on varattu kiinteä osoite DHCP-palvelimelta ja tarkastaa ping-kyselyllä, onko kyseinen laite verkossa. Tällaisia laitteita ovat verkkotulostimet, palvelimet, toimialueen ohjauskoneet, hallittavat kytkimet ja esimerkiksi IP-valvontakamerat. Jos laite vastaa ping-kyselyyn, tarkastetaan, saako siihen muodostettua hallintayhteyden. Hallintayhteys voidaan muodostaa selaimella (tulostimet, IP-valvontakamerat) tai Telnetillä (hallittavat kytkimet) ja asetuksista tarkastetaan, onko laitteelle itselleen määritetty kiinteää IP-osoitetta. Mikäli laitteelle itselleen on asetettu kiinteä IP-osoite, se tulee yliheiton yhteydessä vaihtaa vastaamaan uutta verkkoa. Mikäli automaattinen IP-osoitteen haku on toiminnassa, riittää yliheiton aikana pelkkä laitteen uudelleenkäynnistys.

Seuraavaksi luodaan uusi verkko DHCP-palvelimelle (Infoblox) käyttäen ID Grid Manager -hallintaohjelmistoa (kuva 13). Uusi verkko luodaan niin, että laiteosoitteet (host) säilyvät ja vain osoitteen toinen kenttä muuttuu. Kiinteissä toimipisteissä TO1:n verkko on 10.**150**.x.y / 25 (tai /24) ja uusi TO2:n verkko tulee olemaan 10.**170**.x.y /25 (tai /24). Työmailla 10.**151**.x.y vaihtuu vastaavasti 10.**171**.x.y:ksi.

Uusi verkko ilmoitetaan TO2:lle, jotta he osaavat konfiguroida toimipisteeseen tulevan reitittimen oikein. TO2:lle riittää tieto verkon ensimmäisestä osoitteesta, verkkomaskista ja reitittimen IP-osoitteesta.



Kuva 13. Uuden verkon luonti DHCP-palvelimelle, ID Grid Manager -hallintaohjelmiston avulla.

Kuten kuvasta 13 voi huomata, ID Grid manager on hyvin monipuolinen mutta selkeä ohjelma verkonhallintaan. Vanhasta verkosta kopioidaan kiinteiksi määritetyt osoitteet uuteen verkkoon, IP-osoitteen kakkoskentän muutoksella varustettuna. Useissa verkoissa on määritetty kiinteitä osoitteita laitteille, joita ei ole enää käytössä, joten kopioidaan vain ne laitteet, jotka vastaavat ping-kyselyyn. Tällä tavoin saadaan puhdistettua DHCP-palvelin turhista kiinteistä osoitteista.

Palomuurin määritykset

Palomuurille määritetään uusi verkko ja sallitut yhteydet samalla tavalla kuin toimipaikan edelliselle verkolle on määritetty. Ainoana erona vanhan verkon määrityksiin on se, että aikaisemmin TO1:n verkoista on sallittu yhteydet kaikkiin muihin toimipisteisiin. Kun operaattori vaihtuu TO2:ksi ja samalla verkko vaihtuu (10.**170**.x.y), pitää kaikki yhteydet TO1:n verkkoon sallia erikseen palomuurilta. On siis otettava selvää kaikista yliheitettävän toimipaikan yhteystarpeista palomuurin asetuksia varten.

Palomuurin konfiguroinnissa käytetään pienimpien mahdollisten oikeuksien mallia ja sallitaan vain välttämättömät yhteydet. Samalla tietoturva paranee, kun ylimääräiset yhteydet karsitaan pois.

Liittymän testaus

Kun TO2 on ilmoittanut valmistuneesta liittymästä ja tietohallinnon puolesta on tehty asetukset DHCP-palvelimelle, palomuurille ja Active Directoryyn, voidaan toimipisteen yhteyshenkilölle antaa ohjeet liittymän testauksesta.

Yhteyshenkilön tulee kytkeä tietokoneensa kiinni uuteen reitittimeen ja testata toimivatko seuraavan listauksen mukaiset asiat:

- IP-osoiteavaruus muuttuu 10.**150**.x.y → 10.**170**.x.y
- sähköposti
- internet (intra, ulkoinen)
- levylinkki (esim. Y-asema)
- Metaframe-sovellus (esim. Basware Invoice Processing)
- liittymän nopeus osoitteessa www.speedtest.net [12] (työasemassa ei saa olla proxy päällä).

Kun testit on suoritettu, raportoi yhteyshenkilö tuloksista tietohallinnolle. Ongelmat selvitetään yhdessä TO2:n kanssa ja korjataan ennen kuin yliheitto suoritetaan.

Yliheiton sopiminen

Yhteyshenkilön kanssa sovitaan yliheiton päivämäärä ja kellonaika. Päivämäärän valintaa pitää miettiä siltä kannalta, että useimmiten ongelmia esiintyy yliheittopäivänä ja sitä seuraavana päivänä. Perjantai on huono päivä, sillä ongelmat jäävät viikonlopuksi ja silloin tietohallinnossa ei ole ketään auttamassa. Jäljelle jää päivät maanantaista torstaihin. Yleisesti käytössä oleva ruokatunti kello 11:00–12:00 on hyvä yliheiton kellonajaksi, koska se on aamun ja iltapäivän kiireellisten tuntien välissä. Tämä kellonaika mahdollistaa aamulla tehtävät testaukset ja jättää iltapäivälle aikaa selvittää yliheiton aiheuttamia ongelmia.

Ajankohdan kannalta on hyvä miettiä toimenpiteitä, joita yliheiton aiheuttamat ongelmat eivät ole tervetulleita viivyttämään. Huonoksi ajankohdaksi voidaan todeta mm. palkanmaksun katkopäivä, jolloin palkat maksetaan keskitetysti. Myös palkanmaksua edeltävä päivä on hyvä jättää yliheitolta rauhaan.

Kun yliheiton ajankohta on päätetty, tiedotetaan kaikkia toimipisteen ja sen lähialueen käyttäjiä tunnin tietoliikennekatkoksesta kyseisenä päivänä. Käyttäjiä myös opastetaan, että katkoksen jälkeen henkilökohtainen työasema on hyvä käynnistää uudelleen. Tämän jälkeen päästään itse asiaan, jota käsittelee alaluku 7.3.

7.3 Yliheiton aikana

Ensimmäiseksi ilmoitetaan puhelimitse yhteyshenkilölle yliheiton aloittamisesta ja varmistetaan, että tiedotus tietoliikennekatkoksesta on mennyt perille sekä yhteyshenkilö on valmiina toimimaan, kun saa siihen luvan puhelimitse. Seuraavat toimenpiteet tehdään alla olevassa numerojärjestyksessä.

1. Luodaan etäyhteys kiinteillä IP-osoitteella varustettuihin laitteisiin yksi kerrallaan ja vaihdetaan IP-osoitteet vastaamaan uutta verkkoa. On tärkeää huomioida, että uusien IP-asetusten käyttöönoton jälkeen asetukset jäävät voimaan ja etäyhteys laitteeseen menetetään. Osoitteiden vaihdon kanssa on siis noudatettava erityistä

tarkkuutta. Tämän vaiheen voi mennä läpi tärkeimmästä vähiten tärkeään ja aloittaa palvelimista, jonka jälkeen siirtyä hallittavaan kytkimeen, valvontakameroihin ja verkkotulostimiin.

Seuraavaksi on listattu vaihdettavat osoitteet:

- IP-osoite ja oletusyhdyskäytävä muuttuu aina (10.**150**.x.y → 10.**170**.x.y).
- Aliverkon peite muuttuu, mikäli yliheiton yhteydessä aliverkkoa suurennetaan. (Esim. /25 → /24 = 255.255.255.**128** → 255.255.255.**0**).
- Ensisijainen DNS-palvelin muuttuu, mikäli toimipaikassa on käytössä oma toimialueen ohjauskone (10.**150**.x.z → 10.**170**.x.z).
- Vaihtoehtoinen DNS-palvelin on pääkonttorin toimialueen ohjauskone ja sen IP-osoite säilyy samana.

Mikäli toimipaikassa ei ole omaa toimialueen ohjauskonetta, ensisijainen DNS-palvelin on pääkonttorin toimialueen ohjauskone ja sen IP-osoite ei muutu.

2. Tehdään muutokset IP-osoitteisiin pääkonttorin nimipalvelujärjestelmään (DNS-palvelin). Nimipalveluun on liitetty palvelimet, verkkotulostimet ja muut kiinteällä IP-osoitteella varustetut laitteet. Nimipalvelujärjestelmän muutokset tehdään pääkonttorin toimialueen ohjauskoneelle ja sieltä tieto kahdentuu automaattisesti kaikille muille toimipaikoille.

Seuraavaksi on listattu toimintaohjeet nimipalvelujärjestelmän muutoksiin.

- Kirjaudutaan etäyhteydellä pääkonttorin nimipalvelujärjestelmään ja käynnistetään DNS-työkalu.
- Avataan ruudulle auki kaikki nimipalveluun liitetyt IP-osoitteet ja listataan IP-osoitteen perusteella. (DNS-työkalussa ne löytyvät ”Forward Lookup Zones – ntpasila.ad.lmk”).
- Etsitään listasta toimipaikan vanhan verkon mukainen osoiteväli (10.150.x.y – 10.150.x.z).
- Muutetaan osoitevälin kaikkien kiinteillä IP-osoitteilla varustettujen laitteiden IP-osoitteet vastaamaan uutta verkkoa (10.**150**.x.y → 10.**170**.x.y).

Työasemien (listassa esimerkiksi työasema3) IP-osoitteita ei tarvitse muuttaa, sillä ne päivittyvät automaattisesti viimeistään uudelleenkäynnistyksen yhteydessä. Nimipalvelujärjestelmän muutoksissa on huomioitava, että uusien asetusten kahdentuminen muihin toimipisteisiin saattaa viedä aina muutamista minuuteista kymmeniin.

3. Ilmoitetaan yhteyshenkilölle, että hän valmistautuu siirtämään TO1:n reitittimen ja kytkimen yhdistävän verkkokaapelin TO1:n reitittimestä TO2:n reitittimeen. Ennen siirtoa on kuitenkin hyvä tehdä kytkimen uudelleenkäynnistys. Jos kytkin on hallittavaa mallia, voidaan uudelleenkäynnistys tehdä etäyhteydellä Telnetin tai selaimen avulla. Useimmiten helpoin tapa on ottaa virrat pois kytkimestä fyysisesti. Kytkimen uudelleen käynnistyksen aikana siirretään verkkokaapeli reitittimestä toiseen.

4. Yhteyshenkilön tehtävänä on uudelleenkäynnistää kaikki toimipaikan verkkotulostimet. Uudelleenkäynnistyksen tulee olla fyysinen, eli laitteesta on otettava virrat pois, sillä ohjelmallinen uudelleenkäynnistys ei välttämättä päivitä laitteen IP-osoitteita.

5. Käyttäjät käynnistävät itse omat työasemansa uudestaan ja ovat velvollisia testaamaan käyttämiensä sovellusten toimivuuden. Ongelmat raportoidaan yhteyshenkilön kautta tai suoraan tietohallinnon yliheitosta olevalle vastuuhenkilölle.

7.4 Yliheiton jälkeen

Yliheiton jälkeen ollaan yhteydessä yhteyshenkilön kanssa ja varmistetaan laitteiden toimivuus. Mikäli ongelmia tulee, ne selvitetään ja korjataan välittömästi.

7.5 Ongelmia

Laite ei näy verkossa

Ongelmia yliheiton aikana ja jälkeen voivat aiheuttaa laitteet, joille on määritetty kiinteä IP-osoite mutta joille ei ole huomattu vaihtaa uutta osoitetta. Tällaiset laitteet eivät enää näy uuteen verkkoon siirryttäessä. Laitteet ovat kuitenkin kytkettynä edelleen samaan kytkimeen, joten niihin saa yhteyden asettamalla omaan työasemaan kiinteäksi vanhan verkon IP-osoite ja tällä tavoin työasema on ongelmia tuottavan laitteen kanssa samassa verkossa. Näin laite saadaan hallintaan ja päästään vaihtamaan IP-osoitteet uuden verkon mukaiseksi. Useissa laitteissa (mm. verkkotulostimet) on myös mahdollista vaihtaa IP-osoite ja muita asetuksia suoraan laitteen hallintapaneelista.

Ohjelma ei toimi

Monet Lemminkäisen käyttämistä ohjelmista käyttää tietokantapalvelimia muualta kuin omalta toimipaikaltaan. Tällaiset ohjelmat voivat ottaa yhteyttä suoraan toiseen toimipaikkaan, joka saattaa olla TO1:n verkossa. Yliheiton jälkeen liikenne toisen operaattorin verkkoon kulkee pääkonttorin kautta ja palomuuri estää sen. Palomuurille on siis kerrottava, että liikenne haluttuun paikkaan sallitaan.

Tällaiset ongelmat ovat hyvin yleisiä yliheiton jälkeen. Tietohallinnolla ei ole kuitenkaan mahdollisuutta selvittää kaikkien toimipaikkojen käyttämiä sovelluksia ja niiden toimintaa, joten käyttäjien omien ohjelmien testaaminen ja ongelmien raportointi on erittäin tärkeää.

Uusi yhteys on hidas

Jossain tapauksissa uusi reititin voi neuvotella kytkimen kanssa liikennöintinopeuden hitaammalle kuin on tarkoitus. On ollut muutamia tapauksia, joissa kytkin ja reititin pystyvät 100/100 Mbit/s kaksisuuntaiseen (full-duplex) yhteyteen, mutta ovat neuvotelleet nopeudeksi yksisuuntaisen (half-duplex) 100/100 Mbit/s tai jopa yksisuuntaisen 10/10 Mbit/s. Yksisuuntaisessa tilassa liikennöinti tapahtuu vain yhteen

suuntaan kerrallaan, kun taas kaksisuuntaisessa tilassa voidaan liikennöidä samanaikaisesti molempiin suuntiin. Tämä vaikuttaa oleellisesti yhteysnopeuteen. [14]

Jossain tapauksissa on auttanut kytkimen tai reitittimen uudelleenkäynnistys, joissain tapauksissa operaattorin on täytynyt asettaa reitittimen portti pakotettuun kaksisuuntaiseen 100/100 Mbit/s tilaan.

8 Pilotti

8.1 Ennen pilottipaikan yliheittoa

Jotta pilottipaikan yliheitto olisi mahdollinen, on pääkonttori saatava toimimaan TO2:n verkossa. TO2 toimitti pääkonttorille laitteet, jotka asennettiin TO1:n liittymän rinnalle, työssä jo aiemmin esitetyn kuvan 12 mukaisesti. Tarkoitus olisi jakaa liikenne pääkonttorilta ulkoverkkoon kahden operaattorin kesken aina nopeinta reittiä pitkin. Operaattoreiden välistä MPLS-liikennettä hallitaan pääkonttorin palomuurilla.

Pilottipaikaksi valittiin Vantaanportin toimipiste, jossa työskentelee noin 20 työntekijää. Pilottipaikan valintaan vaikutti suurelta osin toimipaikan sijainti, sillä ennen yliheittoa paikanpäällä saattaa joutua käymään useita kertoja ja Pasilasta Vantaanporttiin on riittävän lyhyt matka. Myös toimipisteen pieni koko vaikutti valintaan positiivisesti. Vantaanporttiin tilattiin TO2:lta 4/4 M:n yritysverkon MPLS-liittymä entisen TO1:n 2/2 M:n liittymän tilalle ja se asennettiin edellisen liittymän rinnalle.

Liittymän testaus

Kun uudet liittymät oli asennettu TO2:n toimesta pääkonttorille, samoin kuin pilottipaikkaan, aloitettiin testaus. Pääkonttorin liikenteen jako toimi kahdennettuna TO1:n ja TO2:n yhteyksillä hyvin. Liikenteen jako ulkoverkkoon suoritetaan operaattoreiden välillä pääkonttorin palomuurilla. Palomuuri lähettää pyynnön molempien operaattoreiden reitittimiin ja se, kummalta vastaus tulee nopeammin, saa kyseisen liikenteen reititettäväkseen. Liikenteen jaon operaattoreiden välillä voi todeta

julkisten IP-osoitteiden perusteella, kun ottaa selaimella yhteyden osoitteeseen whatismyip.com [15] tai whatismyip.org [16]. Kun whatismyip-verkkosivuston avaa selaimella, se kertoo nimensä mukaisesti, mistä julkisesta IP-osoitteesta siihen yhteys muodostetaan. Tässä testitapauksessa com-päätteinen osoite antoi TO1:n julkisen IP-osoitteen, kun taas org-päätteinen osoite antoi TO2:n julkisen IP-osoitteen. Kun testin uusii, antaa se samat tulokset. Palveluiden maantieteellisestä sijainnista ei ole tietoa mutta voidaan päätellä, että TO1:llä on paremmat yhteydet whatismyip.com:in palvelimelle, kun taas TO2:lla on paremmat yhteydet whatismyip.org:in palvelimelle.

Seuraavaksi aloitettiin yhteyden testaaminen Vantaanportista pääkonttorille. Kun luvussa 7 käsitellyt vaiheet oli saatu tehtyä ja palomuurilta avattu riittävästi yhteyksiä, alkoi yhteys toimia.

Ainoaksi ongelmaksi muodostui pääkonttorin uuden yhteyden kahdennus TO2:n reitittimien läpi. Kun Vantaanportissa yhteys oli muodostettu ja pääkonttorilla otettiin toisesta TO2:n kytkimestä virrat pois, ei yhteys alkanut toimia pelkästään toisen TO2:n reitittimen läpi. Asia saatiin selvitettyä operaattorin kanssa yhteistyössä, ja lopulta vika löytyi TO2:n reitittimien ja pääkonttorin palomuurin konfiguraatioista. Laitteiden konfiguroinnin jälkeen yhteys alkoi toimia halutulla tavalla ja pilottipaikka oli valmis yliheitettäväksi.

8.2 Yliheitto

Kun yliheitto oli valmisteltu luvun 7 mukaisilla toimenpiteillä ja yliheiton aiheuttamasta tietoliikennekatkoksesta oli tiedotettu toimipaikkaa, mentiin paikan päälle suorittamaan yliheittoa. Pilottipaikassa toimittiin itse yhteyshenkilön roolissa mutta samalla tavalla kuin oltaisi pääkonttorilla etäyhteyden varassa.

Aluksi testattiin TO2:n linja kytkemällä työaseman suoraan TO2:n reitittimeen. Tämän jälkeen kytkeydyttiin toimipaikan entiseen verkkoon, jossa otettiin yhteydet palvelimiin (tiedostopalvelin, nimipalvelu, toimialueen ohjauskone) ja tehtiin luvussa 7 kerrotut muutokset. Tämän jälkeen uudelleenkäynnistettiin ohjelmallisesti toimipaikan hallittava

kytkin ja vaihdettiin verkkokaapeli TO1:n reitittimestä TO2:n reitittimeen. Tämän jälkeen uudelleenkäynnistettiin kaikki toimipaikan verkkotulostimet ja kehotettiin työntekijöitä testaamaan käyttämänsä sovellukset ja kertomaan mahdollisista ongelmistaan suoraan meille.

8.3 Ongelmia ja ratkaisuita

Tiedostopalvelin ei vastaa

Toimipaikan tiedostopalvelin ei vastannut ping-kutsuihin nimellä, vaan se yhdisti nimen entiseen IP-osoitteeseen 10.**150**.x.y. Aluksi ajateltiin nimipalvelun päivittymisen kestävän tavallista pidempään, mutta hetken odottelun jälkeen päätettiin käynnistää palvelimen uudestaan. Tämäkään ei auttanut asiaan, joten kirjauduttiin paikallisesti palvelimella ja tarkastettiin IP-asetukset, josta vika lopulta löytyi. Oletusyhdyskäytävän IP-osoite oli unohtunut vaihtaa. IP-asetukset vaihtaminen vastaamaan uutta verkkoa korjasi tilanteen ja palvelin alkoi vastata.

Tässä tilanteessa ei olisi pystytty kirjautumaan palvelimelle etänä yliheiton jälkeen. Koska IP-osoite ja oletusyhdyskäytävä olivat ristiriidassa keskenään, ei palvelinta olisi saanut kiinni edes vanhasta verkosta. Vaihtoehdoksi olisi siis jäänyt paikallisen yhteyshenkilön avulla palvelimelle kirjautuminen tietohallinnon henkilön tunnuksilla ja oletusyhdyskäytävän korjaaminen. Todettiin, että tulevaisuudessa IP-osoitteiden vaihtoon liittyvät virheet on vähintäänkin minimoitava.

Tulostin ja sähköposti eivät toimi

Toimipaikalla oli kolme verkkotulostinta, jotka hakivat uuden IP-osoitteen DHCP-palvelimelta, kun ne käynnistettiin uudelleen. Kuitenkin muutama käyttäjä ei pystynyt tulostamaan laitteisiin. Pienen selvityksen jälkeen huomattiin, etteivät käyttäjien työasemat olleet hakeneet uusia IP-osoitteita ja tästä syystä oli sähköposti mennyt yhteydettömään tilaan, eikä tulostaminen onnistunut. Käyttäjät opastettiin

käynnistämään työasemansa uudestaan, koska se on helpompi kertoa suurelle joukolle kuin opettaa uusimaan IP-osoitteet komentokehoitteen kautta.

Samantyylisistä ongelmista käyttäjät saattavat soitella Lemminkäisen helpdeskiin, joten myös helpdeskiä on ohjeistettava useimmiten esiintyvistä ongelmista.

Kalustohallinnan ohjelmisto KALTSU ei toimi

Käyttäjän yrittäessä kirjautua palveluun herjaa ohjelma yhteysvirhettä. Kone oli saanut uuden verkon IP-osoitteen, ja kaikki muut verkkoa käyttävät sovellukset toimivat.

Ongelma johtui siitä, että ohjelma muodostaa kirjautuessa yhteyden toisessa toimipisteessä olevaan tietokantapalvelimeen, joka on TO1:n verkossa. Yliheiton jälkeen pääkonttorin palomuuri ei sallinut yhteyttä TO1:n MPLS-verkkoon ja ohjelma antoi virheilmoituksen. Ongelma korjattiin sallimalla liikenteen tästä toimipisteestä kyseisen tietokantapalvelimen omaavan toimipisteen verkkoon.

9 Tuotantovaihe

9.1 Tuotantovaiheeseen siirtyminen

Onnistuneen pilotin jälkeen projekti päätetään ja siirrytään tuotantovaiheeseen, jolloin seuraavat yliheitot muodostavat rutiinin, jota noudattamalla piirikonttoreiden yliheitot voidaan suorittaa kuin liukuhihnalta.

Projektin päättämisen jälkeen TO2:lle lähetetään tarjouspyyntö, johon on listattu tilattavat toimipaikat osoitteineen ja uusien liittymien nopeudet. Kun vaihdettavat liittymät ovat selvillä, ilmoitetaan toimipaikalle tulevasta operaattorin vaihdosta ja valitaan sopiva yhteyshenkilö, joka ilmoitetaan TO2:lle. TO2 käyttää aliurakoitsijoita päätelaitteiden asennuksissa, jolloin aliurakoitsija ottaa yhteyttä yhteyshenkilöön ennen asennusta. Kun linja on asennettu, testataan se alaluvun 8.2 mukaan ja edetään itse yliheittoon.

9.2 Parannusta vian paikannukseen

Pilotin jälkeen pohdittiin, miten tulevaisuudessa tietoliikennekatkosten vian paikannus saataisiin paremmalle tasolle. Jos toimipisteessä olevat tietokoneet eivät kytkeydy verkkoon, voi tämän aiheuttaa moni asia ja usein vika ei ole operaattorin puolella vaan sisäverkossa. Ratkaisu vian paikantamiseksi ulko- tai sisäverkkoon löytyy operaattorin päätelaitteesta. Mikäli operaattori mahdollistaa päätelaitteen virtuaalisen liitännän (loopback) osoitteen testaamisen ping-pyynnöllä, voidaan yhteys todeta toimivaksi ja paikallistaa vika toimipaikan sisäverkkoon.

Tämän jälkeen päätettiin yhdessä TO2:n kanssa lisätä operaattorin päätelaitteiden konfigurointeihin myös loopback-osoite käyttöön. Osoite ilmoitetaan uuden liittymän tilauksen yhteydessä ja se päätetään Lemminkäisen toimesta.

9.3 Yhteyshenkilön valinta

Tuotantovaiheessa yliheitot tehdään pääkonttorilta käsin yhteyshenkilön avulla. Kun yliheitto on järjestetty ja suunniteltu oikein, ei yhteyshenkilölle jää muuta tehtävää kuin siirtää verkkokaapeli vanhasta reitittimestä uuteen ja uudelleenkäynnistää verkkotulostimet. Kuitenkin jo pilottipaikassa todettiin mahdollisten ristiriitojen ja ongelmakohtien määrän olevan yliheiton aikana ja sen jälkeen hyvin mahdollisia, joten yhteyshenkilön valinnassa on hyvä ottaa muutama asia huomioon.

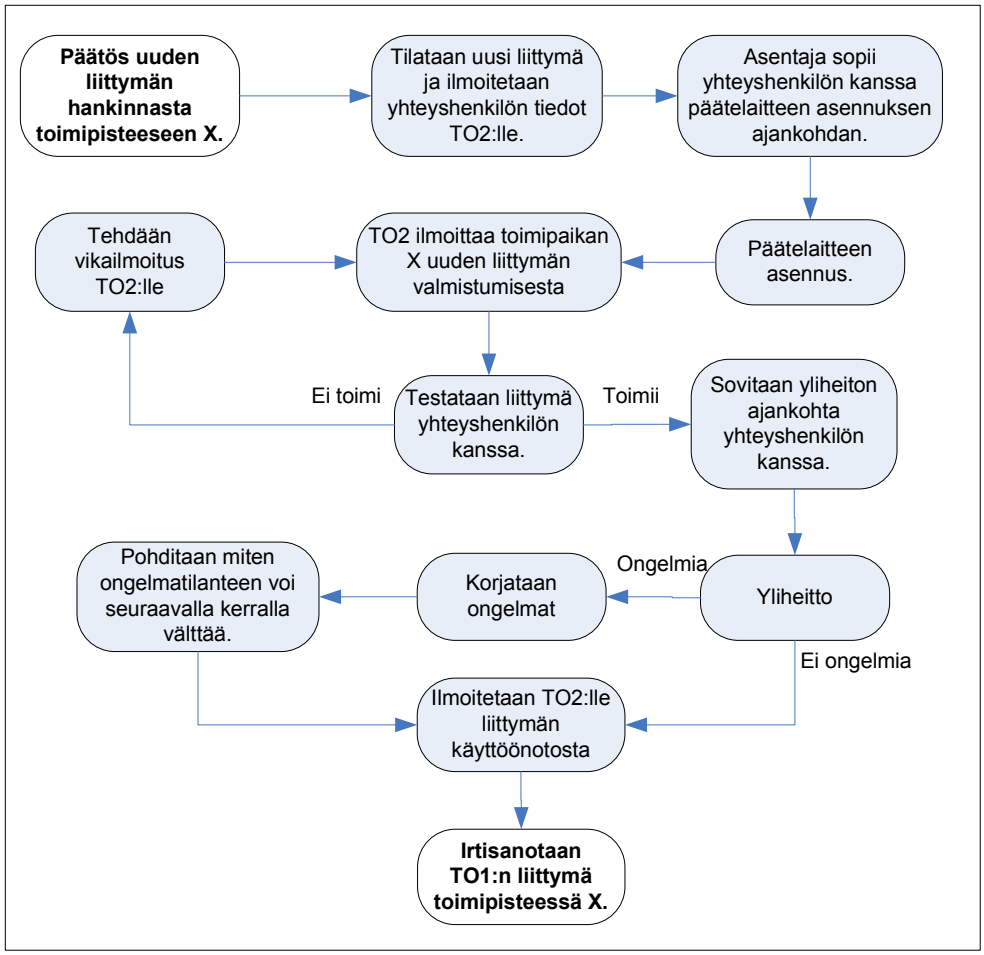
Yhteyshenkilön tulisi tuntea toimistotilat ja sen henkilökunta erittäin hyvin ja hänen tulisi pystyä irrottautumaan omista tehtävistään yliheiton, kuin myös mahdollisten ongelmien selvittelyn ajaksi. Yhteyshenkilöllä tulisi olla tietoteknisiltä taidoiltaan keskitasoa ja hänen tulisi olla valmis toimimaan tarkasti ohjeiden mukaan myös paineen alla.

Pienen pohdinnan jälkeen todettiin, että lähes täydellinen yhteyshenkilö on piirikonttorin toimistosihteeri, joka on usein tehnyt samoja töitä jo useamman vuoden

ajan, tuntee konttorin tilat ja henkilökunnan, on erittäin palvelualtis ja hyvähermoinen sekä lähes aina valmis irrottautumaan omista tehtävistään, jos häntä muuhun tarvitaan.

9.4 Prosessikuvaus tuotantovaiheesta

Tuotantovaiheessa yksittäisen toimipisteen siirtäminen toisen operaattorin MPLS-verkkoon tapahtuu kuvassa 14 olevan vuokaavion mukaan.



Kuva 14. Toimipaikan vaihtaminen uuden operaattorin verkkoon.

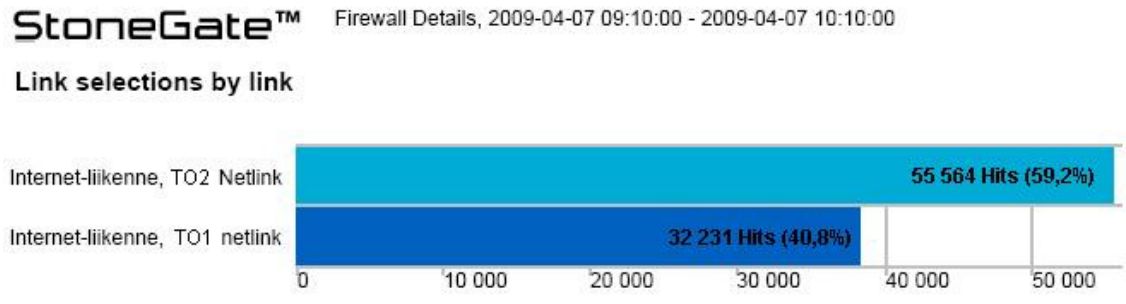
10 Seuranta ja palaute

10.1 Nykytilanne

Projekti käynnistettiin helmikuun lopussa 2008 ja suunnittelun sekä testauksen jälkeen otettiin toinen operaattori käyttöön pääkonttorilla kesällä 2008 ja päästiin yliheittämään pilottipaikka lokakuussa 2008. Pilotin jälkeen siirryttiin suunnitellusti tuotantovaiheeseen, jonka aikana vuoden 2009 huhtikuuhun mennessä on uusia liittymiä tilattu kaiken kaikkiaan 43 ja niistä noin puolet on yliheitetty.

Pääkonttorin liikenteen jako

Pääkonttorilta tietoliikenneyhteydet kahdennettiin toisella operaattorilla. Pääkonttorilta on siis kaksi symmetristä 50 Mbit/s linjaa Internetiin. Liikenteen jako kahden operaattorin välillä tapahtuu palomuurilla, joka vastaanottaa käyttäjän pyynnön ja välittää sen molempien operaattoreiden reitittimille. Nopeamman vastauksen antava reititin valitaan reitittämään kyseinen liikenne. Samalta työasemalta voi olla yhteys Internetiin kahden eri operaattorin yhteyden kautta samaan aikaan. Kuvassa 15 on esitetty palomuurin jakama liikenne operaattoreiden kesken tunnin ajalta normaalina työpäivänä 7.4.2009.



Kuva 15. Liikenteen jako operaattoreiden kesken.

Kuten kuvasta 15 nähdään, reitittyy noin 60% liikenteestä TO2:n kautta ja noin 40% TO1:n kautta. Suhde vaihtelee hieman vuorokauden aikojen ja ruuhkan mukaan, mutta pääasiassa näyttää siltä, että TO2:lla on yleisesti nopeammat yhteydet.

10.2 Miten asiat ovat muuttuneet operaattorin vaihdon myötä

Jo ensimmäisten suurempien toimipisteiden yliheittojen ja samalla TO1:n liittymien irtisanomisen jälkeen, alkoi TO1 kysellä, onko toimipaikkoja lakkautettu vai mitä on tapahtumassa. TO1:lle kerrottiin, että toimipaikka on edelleen täysin toiminnassa ja liittymä on siirretty toiselle operaattorille. TO1:lle annettiin myös selvä viesti, että Lemminkäinen ei ole tyytyväinen operaattorilta saamaansa palveluun, eikä sille maksamiinsa hintoihin. TO1:lle kerrottiin, että tästä lähtien Lemminkäinen tulee toimimaan kahden operaattorin asiakkaana, joista toinen on TO2. Se, mikä operaattori jää tai tulee olemaan toinen operaattori, on TO1:n päätettävissä.

Tämän jälkeen on TO1:n kanssa neuvoteltu uudet sopimukset, niin palvelun kuin hintojenkin osalta ja näillä näkymin TO1 tulee säilymään samana, ainakin toistaiseksi.

TO2 on toiminut tähän asti moitteettomasti. Jos jotain heikkouksia on operaattorista keksittävä, niin alkuvaiheessa asentajat eivät toimineet aloituspalaverissa sovittujen ehtojen mukaan. Aloituspalaverissa oli sovittu asentajan ottavan yhteyttä kohde-toimipaikkaan ennen sinne menoa mutta muutamia kertoja oli asentaja saapunut paikalle ilmoittamatta. Tästä ei ollut muuta ongelmaa, kuin että toimipaikan työntekijät soittelivat ihmeissään tietohallintoon tietämättä koko asiasta. Tietoturvasyistä tuntemattomia henkilöitä ei tietenkään ole sopivaa päästää tekemään asennustöitä mihinkään toimistoon.

Toinen asia, mihin törmättiin muutamien yliheittojen yhteydessä, oli TO2:n konfigurointivirheet päätelaitteiden kanssa. Mikäli testausvaiheessa ei yhteyttä saatu muodostettua, löytyi vika useimmiten lopulta TO2:n konfiguraatioista. Toki inhimillisiä virheitä sattuu kaikille ja useimmiten TO2:een yhteydenoton jälkeen asia selvisi ja korjattiin, jos ei saman tien, niin muutaman tunnin sisällä.

10.3 Käyttäjien kokemuksia uuden operaattorin käyttöönoton jälkeen

Kymmeneen arpomalla valittuun, TO2:n verkkoon siirrettyyn toimipisteeseen lähetettiin lyhyt kysely koskien yliheittoa ja nykyisen yhteyden toimivuutta. Yhteyshenkilöiltä kysyttiin seuraavia asioita:

1 Miten yliheitto sujui, oliko ongelmia ja jos, niin millaisia?
2 Onko operaattorin vaihdos näkynyt käytännön työssä?
3 Onko yhteyksissä ollut ongelmia yliheiton jälkeen?
4 Oletteko olleet tekemisissä uuden operaattorin asiakastuen kanssa?

Seuraavanlaisia vastauksia saatiin: Yhdessä toimipisteessä oli yliheiton aikana ja sen jälkeen huomattu ongelmia ohjelmistojen toiminnan kanssa. Tämä oli korjaantunut pääkonttorin palomuurin määrittelyiden muuttamisella. Yhdessä toimipaikassa yliheitto oli kestänyt luvattua yhtä tuntia hieman pidempään, mikä johtui tulostinongelmista. Yhteydet olivat kuitenkin toiminnassa luvatun tunnin sisällä ja tulostimet toimivat toisen tunnin jälkeen. Lopuissa toimipisteissä ei yliheittoon liittyviä ongelmia ollut.

Puolet vastanneista oli sitä mieltä, että yhteyden nopeus oli parantunut, ja se näkyi käytännön työssä esimerkiksi sähköpostin lähetyksessä ja liitteiden avaamisessa. Neljä kymmenestä ei osannut sanoa eroa. Yhdellä toimipisteellä oli ollut aluksi ongelmia yhteyden hitauden kanssa mutta tämä oli korjaantunut tietohallinnon TO2:lle yhteydenoton jälkeen.

Millään toimipisteellä ei ole ollut ongelmia yhteyksien kanssa yliheiton jälkeen, eikä kukaan vastanneista myöskään ole ollut tekemisissä TO2:n asiakastuen kanssa.

Johtopäätökset

Palaute yliheitoista ja yhteyksien toiminnasta oli siis varsin hyvää, tosin jollain kyseisillä toimipaikoilla uusi yhteys oli ollut vasta muutamia viikkoja käytössään. Pidemmän aikavälin palaute yhteyksien toiminnasta pitää hankkia myöhemmin.

11 Yhteenveto

Tässä opinnäytetyössä dokumentoitiin projekti, jossa Lemminkäinen Oyj:lle suunniteltiin ja toteutettiin tietoliikenneoperaattorin käyttöönotto edellisen rinnalle. Projektia alkoivat alun perin suunnitella Lemminkäiseltä tietohallinnon kehityspäällikkö Mika Virtanen ja järjestelmäasiantuntija Heikki Strengell loppuvuodesta 2007. Itse tulin mukaan projektiin helmikuussa 2008, kun aloitin yrityksessä harjoittelijana. Tällöin valinta uudesta tietoliikenneoperaattorista oli jo tehty ja oli aika pitää aloituspalaveri.

Projektin alkuvaiheessa tutustuin Lemminkäisellä käytettyihin tietoteknisiin ratkaisuihin sekä olin mukana yhteistyössä TO2:n kanssa. Vietin projektin aikana paljon aikaa työn ohjaajan, Heikki Strengellin kanssa, jonka kymmenien vuosien kokemuksen pohjalta sain loistavat pohjatiedot Lemminkäisen tietojärjestelmistä, etenkin tietoliikenteen osalta. Projektista siirryttiin tuotantovaiheeseen, aloin tehdä yliheittoja itsenäisesti.

Projekti itsessään vei noin kuusi kuukautta, ennen kuin päästiin tekemään pilottipaikan yliheitto. Pitkä aika johtui pääasiassa siitä, että tietoliikenneoperaattorin vaihto oli Lemminkäisen osalta ensimmäinen laatuaan ja se vaati todella paljon ennakkoselvitystä ja testausta, ennen kuin uuden operaattorin käyttöönottoa voitiin turvallisesti alkaa tehdä. Valitettavan jotkin Lemminkäisen tietojärjestelmistä on heikosti dokumentoitu, joten kaikki ongelmat, joita uuden operaattorin käyttöönotto saattaisi tuottaa, oli testattava hyvin huolellisesti. Tämän takia tietoliikenneoperaattorin vaihto on dokumentoitu tässä työssä hyvin yksityiskohtaisesti, jotta vastaavassa tilanteessa on ohjeet projektin läpiviemiseen olemassa.

Nyt Lemminkäisen pääkonttori on varmistettu kahdella tietoliikenneoperaattorilla, kymmenien toimipaikkojen tietoliikennenopeuksia on nostettu ja uusien liittymien avaaminen voidaan kilpailuttaa kahden tietoliikenneoperaattorin välillä. Voidaan siis sanoa, että kokonaisuudessaan projekti onnistui erittäin hyvin ja onnistuu seuraavalla kerralla vielä paremmin ja helpommin tämän työn ansiosta.

Vaikeaa tämän insinöörityön tekemisessä oli projektin oleellisimpien asioiden tiivistäminen järkevästi. Mikäli kaikki tekniset yksityiskohdat olisi tässä työssä käyty perusteellisesti läpi, olisi työ niin sanotusti räjähtänyt laajuudessaan käsiin. Tämän takia työssä keskityttiin vain yrityksen kannalta oleellisiin yksityiskohtiin, jolloin työn tulevaisuuden arvo yritykselle maksimoidaan.

Lähteet

1 Lemminkäinen Oyj (WWW-dokumentti). Lemminkäinen konserni. <http://www.lemminkainen.fi/>. 2009. Luettu 3.3.2009.

2 Perimutter, Bruce & Zarkower, Jonathan. Virtuaaliset yksityisverkot VPN. Helsinki: Edita Oyj, 2001.

3 Kosiur, David. Building and Managing Virtual Private Networks. USA: John Wiley & Sons Inc, 1998.

4 Mitä tarkoittikaan VPN? (WWW-dokumentti). Sanoma Magazines Finland 2007. <http://www.tietokone.fi/lukusali/artikkelit/2001tk12/verkko_aloitus.htm>. 2001. Luettu 26.3.2009.

5 Adersson, Loa & Madsen, Tove. RFC 4026 - Provider Provisioned VPN Terminology (WWW-dokumentti). The Internet Society. <http://www.rfc-archive.org/getrfc.php?rfc=4026> 2005. Luettu 8.4.2008.

6 Jaakojuhta, Hannu. Lähiverkot – Ethernet. Helsinki: Edita Oyj, 2005.

7 Jansson, Kim. Etäkäyttö-VPN-laitteiden vertailu ja lähiverkkojen välisten VPN-yhteyksien toteutus. Espoo: Evtek ammattikorkeakoulu, 2001.

8 Lepistö, Tommi. MPLS-verkkojen liikenteenhallinta. Espoo: Evtek ammattikorkeakoulu, 2008.

9 Tuotekohtainen sopimusliite - palvelukuvaus ja erityisehdot. TO2 sisäinen dokumentti, 2008.

10 Hämäläinen, Pertti. Iäisyysprojekti MPLS (WWW-dokumentti). Sanoma Magazines Finland 2007 <http://www.tietokone.fi/lukusali/artikkelit/2000tk04/HAMALAINEN.HTM>. 2000. Luettu 3.4.2009.

11 MPLS Overview (WWW-dokumentti). Data Connection. <http://www.dataconnection.com/mpls/whatis.htm>. Luettu 15.4.2009.

12 The Global Broadband Speed Test (WWW-dokumentti). Ookla. <http://www.speedtest.net/> 2009. Luettu 2.2.2009.

13 Aloituspalaverin pöytäkirja 3.3.2009. Poytakirja Lemminkäinen - TO2

14 Wotel, Paul. The Difference Between Half and Full Duplex Explained (WWW-dokumentti). Hello Direct. <http://telecom.hellodirect.com/docs/Tutorials/DuplexExplained.1.080801.asp> Luettu 6.4.2009.

15 What Is My IP – The fastest, easiest way to determine your IP address (WWW-dokumentti). <www.whatismyip.com>. Luettu 18.11.2008.

16 IP-osoite 194.100.35.103. (WWW-dokumentti.) <www. whatismyip.org>. Luettu 18.11.2008.