

Marko Marttinen

# MPLS-tekniikan soveltuminen yrityksen käyttöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

Toukokuu 2013



Tekijä Otsikko	Marko Marttinen MPLS-tekniikan soveltuminen yrityksen käyttöön
Sivumäärä Aika	23 sivua 15.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	tietoliikennetekniikka
Ohjaajat	yliopettaja Matti Puska Director, Operations Tommi Kemppainen
<p>Insinöörityössä etsittiin tehokkaampaa verkkoteknologiaa Innofactor Oyj:n käyttöön tarjouskilpailuttamalla operaattoreita toimittamaan dynaamisempi ja kustannustehokkaampi verkkoratkaisu. Työssä kuvattiin yrityksen alkuperäinen verkkotopologia ja ylläpidolliset haasteet. Operaattorien tarjoamien ratkaisujen perusteella työssä esitettiin MPLS-tekniikan tarjoamat edut sekä kuvattiin teoriassa MPLS:n toimintaperiaate tukemaan valittua ratkaisua.</p> <p>MPLS-verkon käyttöönottamiseksi työssä tehtiin alustava projektisuunnitelma. Suunnitelmassa määritettiin projektin tavoitteet ja tulokset, projektityömalli, hyväksymiskäytännöt sekä eri vaiheet.</p> <p>Työssä esitellyn teorian perusteella organisaatiolle löydettiin toimivampi verkkoratkaisu, sekä operaattoreilta saatujen tarjousten perusteella oli havaittavissa saavutettavia kustannussäästöjä yksittäisissä verkkoliitännöissä.</p>	
Avainsanat	monipalveluverkko, tietoliikenneverkko, MPLS, leimakytkentä, VPN

Author Title Number of Pages Date	Marko Marttinen MPLS-technology and its applicability for company's use 23 pages 5 May 2010
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications technology
Instructors	Matti Puska, Principal Lecturer Director, Operations Tommi Kemppainen
<p>The goal of the project described in this thesis was the renewal of the telecommunications network of Innofactor Plc. The main purpose of the project was to search for more dynamic and pervasive network technology by sending requests for tender to Internet service providers. The company wanted to reduce administrative work and achieve cost efficiency in network services with the new technology.</p> <p>This thesis describes the existing network topology of the company with its administrative challenges. Based on the service providers' offers, the thesis introduces the basic principles of the MPLS technology to support the desired solution selection procedure.</p> <p>A tentative project plan was made for the implementation of the MPLS technology. The project plan defined objectives and goals, schema, acceptance criteria and phases for the project.</p> <p>New suitable network technology could be determined based on the theoretical section of the thesis and it could be seen that individual network services with solutions offered by the service providers could bring potential cost savings.</p>	
Keywords	integrated services network, telecommunication network, MPLS, Label Switching, VPN

## Sisällys

1	Johdanto	1
2	Multi-Protocol Label Switching	2
2.1	MPLS-tekniikan kehitys	2
2.2	MPLS:n toiminta	3
2.2.1	MPLS-reititys	4
2.2.2	MPLS VPN	7
2.2.3	MPLS:n tarjoamat edut	10
3	MPLS:n soveltuminen organisaation käyttöön	11
3.1	Organisaation nykyinen verkko	12
3.2	Tarjotut MPLS-ratkaisut	14
3.3	Mahdollisia haasteita tai ongelmia	16
4	Projektisuunnitelma MPLS tekniikkaan siirtymisestä	17
4.1	Projektin tavoitteet, malli ja kriteerit	17
4.2	Projektin ositus, vaiheistus, aikataulu ja työmäärät	19
4.3	Projektin käynnistys	20
4.4	Määrittäminen	20
5	Yhteenveto	233
	Lähteet	24

## Lyhenteitä ja käsitteitä

AS	<i>Autonomous System</i> . Internetin hallinnon mukaan jaettujen verkkojen yksilöllinen tunnusnumero, autonominen järjestelmä.
ATM	<i>Asynchronous Transfer Mode</i> . Asynkroninen runkoverkkoteknologia.
BGP	<i>Border Gateway Protocol</i> . TCP/IP-verkkojen reititysprotokolla.
CoS	<i>Class of Service</i> . Luokitukseen perustuva palvelunlaatu.
FEC	<i>Forwarding Equivalence Class</i> . Arvo, joka määrittelee ryhmän paketteja, joilla on kaikilla jokin yhteinen nimittäjä.
FICIX	<i>Finnish Communication and Internet Exchange ry</i> . Rekisteröity yhdistys, joka toimii neutraalina osapuolena operaattorien välissä tarjoten jäsenilleen toimivan ja luotettavan, mutta samalla kustannustehokkaan tavan vaihtaa IP-liikennettä Internetin verkkojen välillä.
IANA	<i>Internet Assigned Numbers Authority</i> . Organisaatio, joka valvoo maailmanlaajuisesti muun muassa IP-osoitteiden ja autonomisten järjestelmien jakoa.
IETF	<i>Internet Engineering Task Force</i> . Internet-protokollien standardoinnista vastaava organisaatio.
L3VPN	<i>Layer3 Virtual Private Networks</i> . Mekanismi, jolla operaattorit voivat siirtää VPN-reittejä BGP-protokollaa hyödyntäen.
LDP	<i>Label Distribution Protocol</i> . Protokolla, joka määrittää leimattujen pakettien lähetystavan.
LER	<i>Label Edge Router</i> . MPLS-verkon reunareitityslaite.
LFIB	<i>Label Forward Information Base</i> . Reitittimien leimatitokanta.

LSP	<i>Label Switched Paths.</i> MPLS-verkon sisällä oleva siirtotie.
LSR	<i>Label Switching Routers.</i> MPLS-verkon runkoreitityslaite.
MPLS	<i>Multi-Protocol Label Switching.</i> Moniprotokollainen leimakytkentä.
PE	<i>Providers Edge.</i> Operaattorin reunareitityslaite.
QoS	<i>Quality of Service.</i> Palvelunlaatu.
RD	<i>Route Distinguisher.</i> Menetelmä, jolla yksilöidään MPLS verkossa IPv4 prefiksejä.
VPLS	<i>Virtual Private LAN Service.</i> Menetelmä, jolla voidaan luoda VLAN emuloimalla LAN-verkkoa.
VPN	<i>Virtual Private Network.</i> Virtuaalinen erillisverkko.
VRF	<i>Virtual Routing and Forwarding.</i> MPLS-verkossa käytetty virtuaalinen reititystaulu.

## 1 Johdanto

Insinööriytyö on tehty Innofactor Oyj:lle, joka on suurin suomalainen Microsoft-ratkaisuihin keskittynyt toimittaja. Innofactor Oyj toimii systeemi-integraattorina ja kehittää omia ohjelmistotuotteita. Innofactor Oyj:llä on toimipisteitä Tampereella, Turussa, Kuopiossa, Kajaanissa, Savonlinnassa, Kööpenhaminassa ja pääkonttori Espoossa.

Innofactor on organisaationa kasvanut voimakkaasti usean vuoden ajan ja sijoittui sijalle 24 vuoden 2012 Deloitte Technology Fast 50 -listalla, joka kokoaa 50 eniten viimeisen viiden vuoden kuluessa kasvanutta teknologiayritystä Suomessa [1]. Innofactor oli listan ainoa pörssiyritys 310 prosentin kasvullaan. Yrityksen kasvun, jonka osuus esimerkiksi vuoden 2011 liikevaihdon kasvun osuudesta oli 53,1 prosenttisyyskoko [2], ja yritysjärjestelyiden myötä on tietojärjestelmille ja etenkin tietoliikennejärjestelmille tullut tilausta yhtenäistämiseksi ja yksinkertaistamiseksi.

Työn tavoitteena on etsiä kasvaneelle organisaatiolle paremmin tarpeita vastaava kokonaisvaltainen tietoverkkoratkaisu. Työssä haetaan ratkaisuun soveltuvaa teknologiaa ja tehdään alustava suunnitelma valitun teknologian käyttöönotolle. Tietoverkkouudistuksen halutaan yksinkertaistavan organisaation epäorganisen kasvun myötä tullutta tietoliikennejärjestelmien monimuotoisuutta ja parantaa myös ylläpidettävyyttä. Lisäksi verkkouudistuksella halutaan parantaa vikasetoisuutta palvelinympäristöjen tietoverkkoihin ja uudistuksen toivotaan tuovan myös kustannussäästöjä. Välittömät säästöt eivät ole pääkriteerinä, vaan niitä pyritään tarkastelemaan kokonaisuutena, myös ylläpidon helpottumisen kautta, eli välillisiä kustannuksia halutaan vähentää.

Työ aloitetaan määrittelemällä organisaation tavoitteet uudistukselle, valitsemalla kaksi luotettavaa palveluntarjoajaa, jotka pystyvät toteuttamaan asetetut tavoitteet nykyisten toimipisteiden alueilla kuin myös laajemmin Euroopassa ja tarjouskilpailuttamalla heidät. Työssä esitellään myös valitun teknologian pääpiirteet teoriassa.

## 2 Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS), voitaisiin suomentaa esimerkiksi moniprotokollaiseksi leimakytkennäksi. MPLS on leimoihin perustuva pakettien välitysmenetelmä, joka koostuu useista RFC-dokumenteista, standardiluonnoksista ja standardeista.

### 2.1 MPLS-tekniikan kehitys

MPLS-tekniikan kehitys alkoi 1990-luvun puolen välin aikaan, kun Internet-protokollien standardoinnista vastaava organisaatio Internet Engineering Task Force (IETF) alkoi kehittää menetelmää, joka ratkaisisi IP-protokollan skaalautumisongelmia ATM-verkkoja (Asynchronous Transfer Mode) käytettäessä. IETF perusti MPLS-työryhmän, jonka päämääränä oli standardisoida leimakytkennän käyttöön vaadittu teknologia ja implementoida kyseiset menetelmät runkoverkossa käytettävien teknologioiden (Sonet, Frame Relay, ATM) sekä lähiverkkoteknologioiden (Ethernet-tekniikat, Token Ring jne.) kanssa [3.]

Alun perin yksi MPLS-työryhmän tavoitteista oli poistaa hitaiden reitittimien aiheuttama pullonkaula ATM-runkoverkkojen tiedonsiirtonopeudessa. Käytännössä tarkoituksena oli korvata monimuotoiset ATM- ja IP-reititysoperaatiot yksinkertaisella tietopaketin leimaan perustuvalla välityksellä.

MPLS-tekniikan suhteellisen pitkän kehitystyön aikana ovat kehittyneet myös tietolaitteet sekä muut verkkotekniikat, jolloin monet alkuperäiset MPLS:llä haetut tavoitteet ovat menettäneet merkitystään [4, s. 354–358]. Kehitystyön aikana on kuitenkin havaittu, että MPLS tarjoaa alkuperäisiä tavoitteitaan tärkeämpiä etuja ja mahdollisuuksia. Jos alun perin MPLS kehiteltiin verkko-operaattorien tietoverkkojen teknologiaksi, on se nykyisin yleistynyt operaattorien yksityisille organisaatioille tarjotuksi palveluksi.

Davien ym. [4, s. 368] ja Minein & Lucekin [5, s. 4] MPLS-tekniikkaan keskittyvien kirjojen mukaan nykyisin merkittävimmät MPLS:n tarjoamat edut organisaatioille ovat kolmannen tason (OSI Layer 3) VPN (Virtual Private Network) -palvelut ja MPLS:n eks-



plisiittisen tietopakettien reitittämisen hyödyntäminen. Tämä tarkoittaa käytetyn verkkopolun etukäteen määrittämistä tietyntyyppiselle liikenteelle, tai tietyntyyppisen liikenteen palveluluokittelun (CoS, Class of Service) myötä saatu palvelunlaadun parantaminen (QoS, Quality of Service). Tai myös nopean varayhteyden määrittämistä alkuperäisen verkkopolun vikaantumisen varalle (Fast reroute). Kokonaisuudessaan MPLS-verkon leimojenvaihtoparadigman tuoman verkon kapasiteetin optimoinnin voidaan ajatella parantavan tietoverkon suorituskykyä ja kasvattavan palvelunlaatua. Minei & Lucek [5] käyttääkin jo esipuheessaan nykyisestä MPLS-teknologiasta nimeä "Multi-Purpose Label Switching", joka voitaisiin suomentaa monikäyttöinen leimakytkentä.

## 2.2 MPLS:n toiminta

Perinteisessä tietoverkossa tieto kulkee paketteina, joihin lähettäjä laittaa vastaanottajan osoitteen. Paketti lähetetään lähimmälle reitittimelle, joka tutkii vastaanottajan osoitteen ja päättelee omien sisäisten taulukkojensa avulla, mille naapurireitittimelle paketti kannattaa lähettää. Sama toistuu jokaisella reitittimellä, ne päättelevät itsenäisesti määränpään osoitteen perusteella paketin matkan seuraavan etapin.

MPLS on uudempi ja tehokkaampi liikennöinti-protokolla, joka yhdistää OSI-3 (Open Systems Interconnection Reference Model) -reititystason ja OSI-2 -kytkentätason vahvuudet tehokkaiksi tietoverkoiksi. Se perustuu valmiiksi viitoitettuihin reitteihin verkon kaikkien sisääntulo- ja uloslähtöpisteiden välillä. Kun paketti saapuu MPLS-verkon reunalle, sen alkuun liitetään paikallinen leima. Matkan varrella jokainen reitin tietää, mikä on kunkin reitin seuraava etappi. Paketin ohjaaminen eteenpäin reittitunnuksen avulla on paljon yksinkertaisempaa kuin ohjaus vastaanottajan osoitetta tutkimalla. Paketin alussa oleva reittitunnuksen luku ja kirjoitus sekä paketin edelleen ohjaus voidaan tehdä laitteistotasolla, mikä on paljon nopeampaa kuin ohjelmallisesti tehty ohjaus. Valmiiksi viitoitetuilla reiteillä voidaan muodostaa yhteyksiä, joiden siirtonopeutta ja siirron laatua voidaan hallita. MPLS-verkossa voidaan esimerkiksi teräväpiirtotelevision kaltaiselle multimediyhteydelle taata sen vaatima suuri siirtonopeus ja pieni viive samaan aikaan, kun staattisten Internet-sivustojen selaamiseen käytetään pienempää kaistaa [6.]

MPLS-tekniikan keskeinen ominaisuus on se, että sitä voi käyttää joustavasti siirtämään useaa erityyppistä liikennettä ympäri runkoverkkoa. MPLS-verkon sisällä olevista siirto-  
teistä käytetään nimitystä Label Switched Paths (LSP), ja yleisesti MPLS-tekniikan ky-  
kyä välittää paketteja ympäri verkkoa verkkolaitteiden tietämättä määränpäättä, voi-  
daan kutsua MPLS-tunneloinniksi [5, s. 42].

Paketin siirtyessä MPLS-verkkoon ja MPLS-verkosta takaisin perinteiseen järjestelmään  
vain liityntäkohtien täytyy ymmärtää alkuperäisen liikenteen reititystietoja tai käytettyjä  
protokollia. MPLS-verkon sisällä reitittimet voivat siirtyä MPLS-kapseloituihin paketteihin  
eikä niiden tarvitse enää huomioida alkuperäisen verkon kontekstia. Tämän ansiosta  
yhteen LSP:iin voidaan limittää kaikäntyyppistä liikennettä välittämättä verkkolaitteiden  
tukemista menetelmistä tai protokollista. [5, s. 42.]

MPLS-tunnelit tai LSP tarjoavat seuraavanlaisia etuja [5, s. 6]:

- Liikenne voidaan välittää eksplisiittisesti kulkemaan eri siirtoteitä, normaalista reiti-  
tyspäättöksistä poiketen, esimerkiksi käytetyn signalointimenetelmän perusteella.
- Tunneleita voi olla tunneleiden sisällä.
- Ainoastaan MPLS-tunnelin päässä voidaan syöttää dataa tunneliin, minkä ansiosta  
saavutetaan datan eheys. Toisaalta dataa voidaan syöttää tunneliin mistä tahansa  
lähteestä, jolla on yhteysrajapinta verkkoon jossa tunneli sijaitsee.
- Kapseloinnissa on pieni otsakedata (overhead), neljä tavua jokaisessa MPLS-  
otsakkeessa.

### 2.2.1 MPLS-reititys

MPLS-verkko koostuu reunareitityslaitteista (LER, Label Edge Routers) ja runkoreititti-  
mistä (LSR, Label Switching Routers). Reunareitittimet muodostavat yksisuuntaisia tie-  
toliikennepolkuja (LSP, Label Switched Path) MPLS-verkon sisääntulo- ja ulosmenolait-  
teiden välille. Kun paketti saapuu MPLS-verkon reunareitittimelle, reititin päättää, mihin  
FEC-luokkaan (Forwarding Equivalence Class) paketti kuuluu. FEC-luokitus määrittelee  
ryhmän paketteja, joilla on kaikilla jokin yhteinen nimittäjä. FEC-luokkia voidaan muo-  
dostaa useiden syiden perusteella. Esimerkiksi paketit, jotka reititetään samalle reititti-  
melle samaa polkua pitkin ja samanlaisella käsittelyllä, kuuluvat samaan FEC-luokkaan.

Paketit jotka kuuluvat tietylle asiakkaalle, voivat muodostaa FEC-luokan [4, s. 358]. Saman FEC-luokan paketit reititetään yhtenäisellä MPLS-leimalla.

MPLS-tekniikkaan perustuvassa tietoliikenteessä siirrettävään dataan lisätään yksi tai useampi leimakenttä. MPLS-paketin leima on 32 bitin eli neljän tavun mittainen ja muodostuu seuraavista kentistä (kuva 1):

- Leima  
20 bitin mittainen leimakenttä. Kenttää käytetään MPLS-pakettien välittämiseen.
- TC / EXP  
3 bitin mittainen liikenteen luokittelu kenttä (TC = Traffic Class), jota aiemmin kutsuttiin EXP-biteiksi. Näiden bittien avulla MPLS-verkon reititys laitteet, LSR (Label Switching Routers) ja LER (Label Edge Routers), määrittävät, mihin jonoon kukin paketti ohjataan, tai miten paketti käyttäytyy kussakin jonossa.
- Stack  
MPLS-järjestelmässä paketissa voi olla päällekkäin useita leimoja, ja Stack-bitti kertoo paketin sisällä sijaitsevan leimapinon hierarkiassa, onko kyseessä alimmainen leima vai ei.
- TTL (Time-to-live)  
Kenttä kertoo paketin elinajan MPLS-verkossa. Paketin TTL-arvoa vähennetään aina yhdellä sen siirtyessä reititinlaitteelta toiselle. Kun arvo on nolla, paketti hylätään. TTL-kentän avulla ehkäistään liikennettä haittaavien reitityssilmukoiden (loop) muodostumista ja sitä käytetään myös paketin reitin jäljittämiseen. IP TTL tuodaan tai poistetaan MPLS-verkon reunoilla. [7, s. 415.]

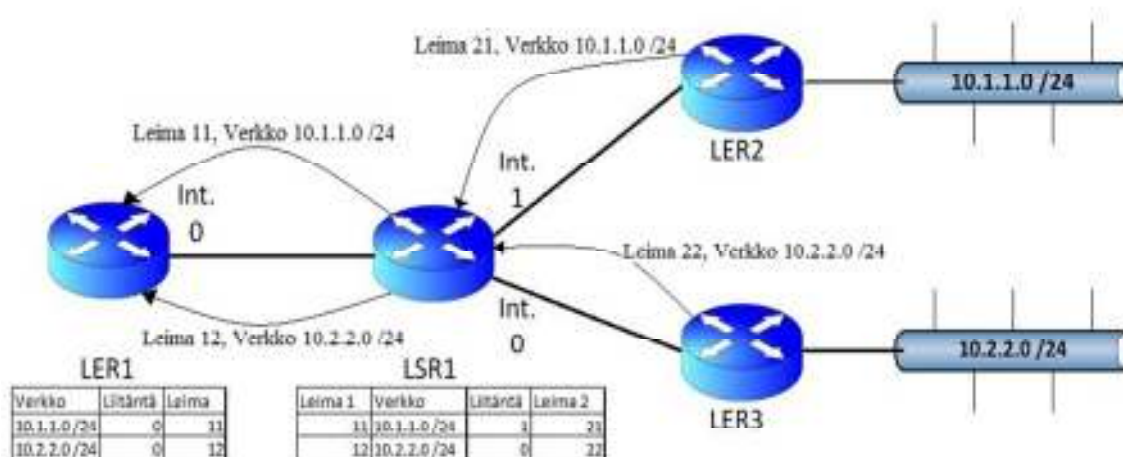
Leima 20 bittiä	TC EXP 3 bit- tiä	Stack 1 bitti	MPLS-TTL 8 bittiä
--------------------	----------------------------	---------------------	----------------------

Kuva 1. MPLS-leiman rakenne.

Joissain yksinkertaisimmissa reititystapauksissa yksi MPLS-otsikko paketissa riittää, kuten siirrettäessä julkista IP-liikennettä MPLS-verkossa, jolloin reititys perustuu pitkälti tavalliseen IP-osoitetietojen hakuun (IP-Lookup). Esimerkkinä tällaisesta tapauksesta voisi kohdeosoitteen perusteella reitittäminen (Destination-Based Forwarding).

Kuvassa 2 on havainnollistettu yhden MPLS-otsikon tapausta, jossa oikean puoleisilla reunareitittimillä LER1 ja LER2 on yhteys IP-verkkoihin 10.1.1.0 /24 ja 10.2.2.0 /24. LSR1 -reitittimellä ja vasemmanpuoleisella LER1-reitittimellä on taas reititystauluissa tieto, mitä reitittimen fyysistä liitäntää (interface) käytetään kullekin IP-verkolle.

MPLS-verkossa reitittimet allokoivat leiman kullekin IP-verkolle reititystaulussaan ja mainostavat näitä naapurireitittimilleen. Kun tietopaketti, jonka kohde IP-osoitteena on 10.1.1.15, saapuu LER1-reitittimelle, se suorittaa IP-Lookup-toiminnon ja tämän perusteella lisää pakettiin otsikon. Reititin LER1 huomaa että IP-osoite 10.1.1.15 täsmää verkon 10.1.1.0 /24 prefiksiin leimatietokannassaan (LFIB, Label Forward Information Base), jossa on myös tieto käytettävästä liitännästä (interface = Int 0) ja halutun verkon otsikosta. LER1 lisää siis pakettiin otsikon arvon 11 ja lähettää sen eteenpäin liitännästä (interface) 0. Kun paketti saapuu reitittimelle LSR1, se katsoo ainoastaan paketin otsikkoa, ja LFIB:n avulla LSR1 tietää, että tietoliikennepaketti otsikolla 11 pitää lähettää eteenpäin liitännästä 1 otsikolla 21 (Otsikko 2), kuten reunareititin LER2 on sille mainostanut. Tällöin LSR1-reitittimen ei koskaan tarvitse tarkastaa paketin IP-osoitetta, vaan se operoi pelkästään saapuvan paketin leimatiedolla. LER2-reititin ohjatussaan paketin kohdeverkkoon 10.1.1.0 /24 poistaa paketista otsikon ja jäljelle jää vain alkuperäinen IP-paketti. LDP-protokolla (Label Distribution Protocol) määrittää leimattujen pakettien lähetystavan. [8.]



Kuva 2. Destination-Based Forwarding [9, s. 62.]

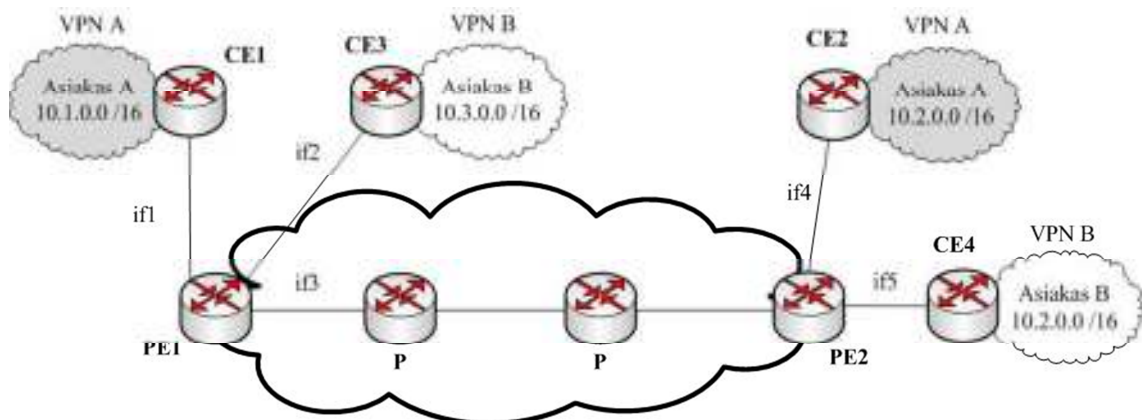
## 2.2.2 MPLS VPN

Kakkostason virtuaalilähiverkkopalvelu (VPLS Virtual Private LAN Service) on ollut yksi jatkuvasti kasvavista sovelluksista MPLS-verkoissa. VPLS:n avulla operaattorit voivat yhdistää asiakkaiden maantieteellisesti erillään olevia Ethernet-verkkoja toimimaan yhden lähiverkon (LAN, Local Area Network) tavoin [5, s. 5].

BGP/MPLS IP VPN (BGP, Border Gateway Protocol), jota kutsutaan myös MPLS L3VPN:ksi tai lyhyesti L3VPN:ksi (Layer3 Virtual Private Networks), on myös kasvanut yhdeksi MPLS:n laajimmin käytetyksi sovellukseksi. Tässä palveluntarjoaja siirtää verkossaan usean asiakkaan VPN-reitit BGP-reititysprotokollalla ja rajoittaa VPN-reititystietojen jakelun omille reunareitittimilleen [10, s. 375].

Perinteisistä VPN-yhteyksistä poiketen L3VPN-tunneloinnissa jokainen tunnelin päätepiste liitetään suoraan palveluntarjoajan reunareitittimellä (PE, Providers Edge) runkoverkkoon. Jokainen palveluntarjoajan reunareititin voi sisältää usean asiakkaan VPN-yhteyksiä [4, s. 363–365]. Vaikka asiakkailla, jotka jakavat saman verkkoyhteyden, voi olla toistensa kanssa päällekkäin meneviä osoitealueita, voidaan jokaisen VPN-liikenne reitittää toisilta eriteltynä vain kunkin VPN-yhteyteen määritettyjen päätepisteiden välil-

lä. Tämä toiminta perustuu virtuaalisten reititystaulujen (VRF, Virtual Routing and Forwarding) käyttöön. VRF on tekniikka, joka mahdollistaa PE:llä usean yksittäisen reititystaulun käytön. VRF kertoo reititystiedot vain saman VPN-yhteyden käyttöön, piilottaen sisäverkkojen tiedot ja paketit tunnelin ulkopuolisilta tahoilta. VRF-taulu liitetään kullekin asiakkaalle niiden liityntäpisteessä, jolloin kyseisestä liitynnästä tulevat paketit voidaan reitittää oman VRF-taulun mukaisesti runkoverkon läpi kohdeosoitteeseen [10]. Kuvassa 3 on havainnollistettu yksinkertaista kahden asiakkaan MPLS VPN-verkkoa, jossa palveluntarjoajan reunareititin PE1 on yhdistetty if1 -nimisen liitynnän kautta asiakkaan A reunareitittimeen CE1 ja johon on liitetty VRF-taulu "VPN A". Vastaavasti PE1:n liitettä if2 yhdistää asiakas B:n reunareitittimen CE3, johon on liitetty VRF-taulu "VPN B". Kun CE1-reititin lähettää PE1:lle IP-paketin if1-liitynnän yli, PE1 valitsee käytettävän polun reititystaulu VPN A:n mukaan, ja kun asiakkaan B reunareititin CE3 liikennöi if1:n kautta, PE1 tarkastaa reitityksen VPN B -reititystaulun mukaan.



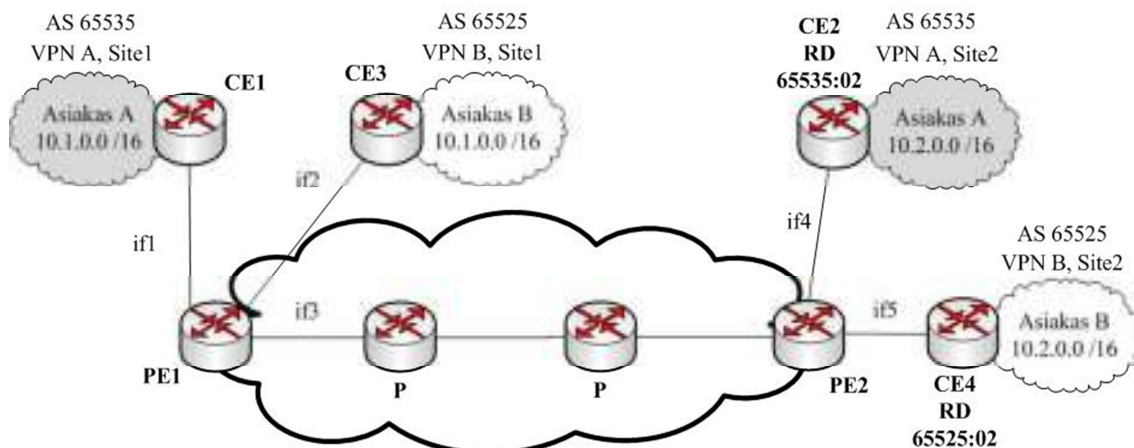
Kuva 3. MPLS-VPN verkko [12, s. 115.]

Kuten esimerkissä havainnollistettiin, usean reititystaulun käyttö estää päällekkäisten verkkojen aiheuttamat konfliktit reitityksissä, mutta se ei vielä välttämättä riitä estämään sitä, ettei liikennettä ohjata VPN:stä toiseen, joten reititystietojen näkyvyyttä täytyy rajoittaa. Jotta perinteisen VPN-tunneloinnin ylläpidon määrältä välttyttäisiin, voidaan kaikki VPN-reitit kuljettaa palveluntarjoajan verkossa yhden reititysprotokollan, BGP:n (Border Gateway Protocol) avulla. BGP pystyy ylläpitämään vain yhtä reittiä an-

netulle osoiteprefiksille, ja MPLS VPN vaatii toimiakseen jokaisen asiakkaan käyttä omia osoitealueitaan, joten BGP pakotetaan reitittämään useita reittejä yhdelle IP-osoiteprefiksille lisäämällä reititykseen Route Distinguisher (RD). Eli kun VPN:n sisällä oleva laite liikennöi PE -reunareitittimelle, se lisää IPv4 (Internet Protocol version 4) prefiksiin RD:n, muuntaen osoitteen VPN-IPv4 (Virtual Private Network version 4) prefiksiksi. BGP:n multiprotocol (MP) -kyvykyys sallii useantyyppisten prefiksien reitityksen. PE-reunareititin tunnelin ulostulo päässä poistaa RD:n, palauttaen reitityksen perinteiseksi IP-reititykseksi, jolloin asiakkaan tai VPN-tunneliin kuuluvien sisäverkon laitteiden ei tarvitse tietää VPN-IP-osoitteita. VPN-IPv4 osoite muodostuu 12 tavusta, jonka kahdeksan ensimmäistä tavua sisältävät RD:n ja loput neljä tavua IPv4-osoitteen. Koska RD tekee IP-osoitteista ainutkertaisia, täytyy myös RD:n olla ainutkertainen. [13, s. 225.]

Jokainen palveluntarjoaja hallitsee omaa numerointialuetta eli voi allokoida RD:eita siten, etteivät ne aiheuta konflikteja muiden palveluntarjoajien RD-allokointien kanssa. RD koostuu kahden tavun tyyppikentistä, administrator- ja määritetty numero (assigned number) -kentistä. Tyyppikentän arvo määrittää kahden muun kentän pituuden sekä administrator-kentän merkityksen. Administrator-kenttä identifioi omistajan määritellylle numerolle, määritetyn numeron kenttä sisältää numeroarvon, joka on saatu yleisesti luotettavalta taholta. Esimerkiksi RD voisi muodostua administrator -kentästä, jossa olisi AS-numero (Autonomous System) ja sen neljä tavuinen numerokenttä sisältäisi IANA:n (Internet Assigned Numbers Authority) palveluntarjoajalle osoittaman AS-numeron. [14.]

Kuvassa 4 on havainnollistettu, kuinka AS-numerointia voidaan käyttää RD:n yksilöivänä tekijänä. Kuvan asiakkaalla A on AS-numero 65535 ja B:llä AS-numero 65525, jotka molemmat kuuluvat yhteiselle palveluntarjoajalle. CE2-reitittimellä VPN A Site2:lla Route Distinguisher on 65535:02 ja CE4-reitittimen VPN B Site2:lla RD on 65525:02. Kun reunareititin PE2 saa reitin CE2-reitittimeltä, se muuntaa asiakkaan IPv4-osoitteen 10.2.0.0 VPN-IPv4 muotoon 65535:02:10.2.0.0, kun taas CE4-reitittimen VPN B IPv4-osoite muutetaan VPN-IPv4-osoitteeksi 65525:02:10.2.0.0.



Kuva 4. AS Route Distinguisher. [4. s, 318.]

### 2.2.3 MPLS:n tarjoamat edut

Verkkopalvelujen uudistusta tarjouskilpailuttamalla saadaan haastettua operaattorit tarjoamaan ajankohtaisesti taloudelliset sekä kilpailukykyiset verkkopalvelut. Samalla saatetaan heidän intresseihinsä Internet- ja verkkoliitöntöjen infrastruktuurin päivittäminen esimerkiksi kuparitekniikasta kuitutekniikkaan sekä mahdollisten verkkolaitteiden uudenaikaistaminen. Yhdenmukaistamalla ja uudistamalla kerralla koko organisaation tietoverkkojärjestelmän ottaa palveluntarjoaja vastuulle koko verkon päästä päähän-toimituksen aina yrityksen lähiverkkoliitintään saakka sekä verkon ongelmatilojen selvittämisen ja korjaamisen. Operaattorin toimittaessa verkkopalvelut lähiverkkoon saakka verkkoa on helppo laajentaa lisäpisteillä Suomessa ja kansainvälisesti, etenkin jos palveluntarjoajaksi on valittu operaattori jolla on kattava kansainvälinen kumppaniverkosto.

Kuten luvussa 2 on esitetty, MPLS-tekniikan suuri etu on sen kyky siirtää ennalta määritetyillä reiteillä nopeasti ja tehokkaasti lähes mitä tahansa dataa, kuten esimerkiksi IPv6-paketteja, yhden ja saman runkoverkon läpi. MPLS-tekniikkaan siirryttäessä saadaan yrityksen verkko suljetuksi sekä tarvittaessa täysin eristetyksi julkisesta verkosta, jolloin verkosta tulee immuuni Internetissä liikkuville uhille, sekä tehden luvaton verk-



koon liittyminen mahdottomaksi. Toimipisteiden välisiä salattuja VPN-tunneleita ei enää tarvita, jolloin vapaudutaan erillisten tietoliikennelaitteiden ylläpidosta ja hankinnoista. Tarvittaessa liikenteen salausta asiakasreitittimessä ja tunnelointi yritysverkon sisällä on kuitenkin toteutettavissa. MPLS:n virtuaalisten reititystaulujen avulla suljetun yritysverkon sisällä voidaan luoda uusia suljettuja yhteyksiä esimerkiksi yksittäisten toimipisteiden tai palvelujen välille, mikä mahdollistaa entistä rajatumpien palveluiden tarjoamisen.

Kolmannen tason VPN-ratkaisussa vain verkkojen reunalaitteet käsittelevät IP-osoitteita, jolloin liikennettä voidaan luokitella ja priorisoida joustavammin käyttämällä hyväksi FEC-luokkia. Lisäksi leimakytkentäinen reititys mahdollistaa yksityisten IP-osoitteiden käytön MPLS-verkon alueella ja poistaa perinteisessä ratkaisussa vaadittujen julkisten IP-osoitteiden tarpeen, jolloin verkon ylläpito yksinkertaistuu. Koko organisaation Internet-yhteydet voidaan hoitaa keskitetyn palomuurin tai väylän kautta, jolloin saadaan yhtenäistettyä myös organisaation tietoturvaliikettä ja kaikkien verkon yhteyspisteiden nopeuksia voidaan nostaa tai laskea tarpeiden muuttuessa. Operaattoreilla on myös tarjota kattavat verkonvalvonta- ja raportointipalvelut, joiden avulla yrityksen verkosta saadaan poistettua mahdollisia ongelmakohtia sekä optimoitua verkon suorituskykyä. Dynaamisen reititysominaisuutensa ansiosta MPLS-verkon viansietoisuus kasvaa, eikä tietopakettien kulku esty yhden verkkolaitteen tai jonkin verkon alueen virheellisestä toiminnasta.

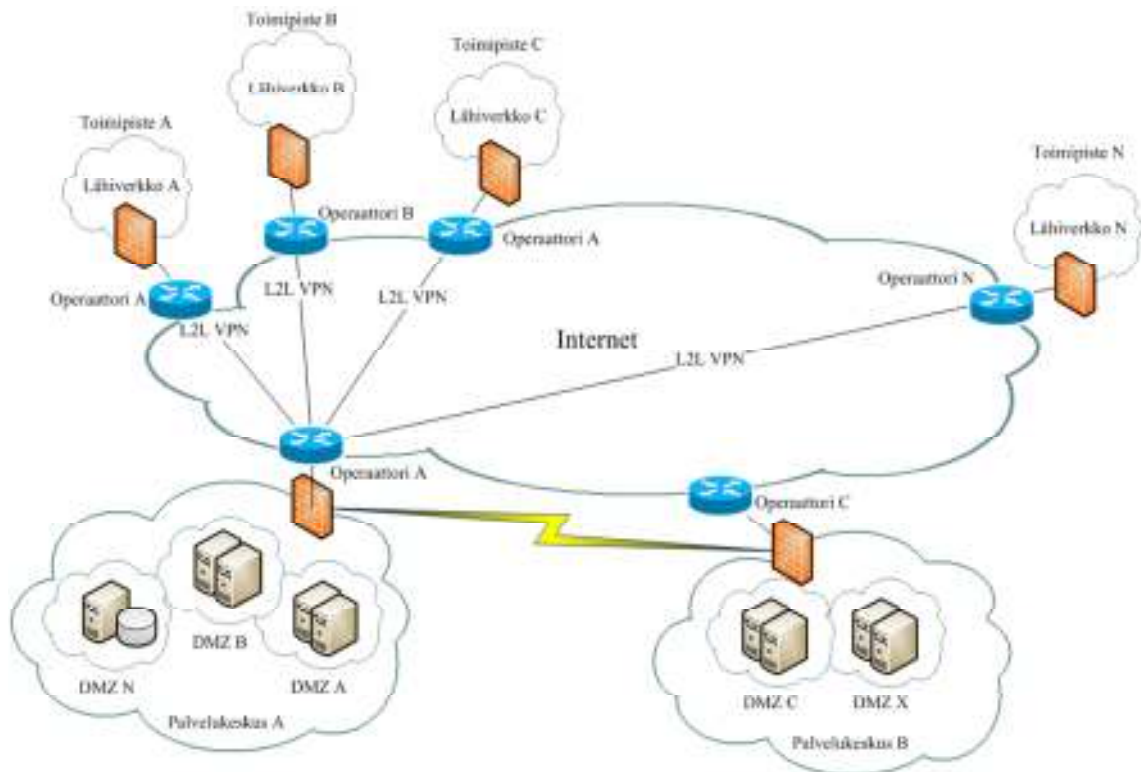
### **3 MPLS:n soveltuminen organisaation käyttöön**

Yrityksen epäorganisaation kasvun myötä tapahtunut eri organisaatioiden tietojärjestelmien yhteen sulautuminen on tuonut kompleksisuutta nykyisen verkon ylläpitoon. Perinteisiä ratkaisumalleja käytettäessä pienetkin muutokset verkossa vaativat ylläpitoa useilla eri verkkolaitteilla ja vaativat verrattain paljon aikaa. Lisäksi monen organisaation oman toimipisteen verkkoyhteydet ovat usean eri alueellisen toimijan tarjoamia, minkä vuoksi esimerkiksi mahdollisissa ongelmatilanteissa kontaktipisteitä ja vastuunkantajia on useita.

Innofactorin alkuperäinen erillisiä verkkoja yhdistävä L2L VPN (LAN-to-LAN Virtual Private Network) -tekniikkaan pohjautuva toteutusmalli ei enää vastaa kasvaneita tarpeita verkon dynaamisuudesta, etenkin yrityksen kasvaessa ulkomailla. Tällöin MPLS tarjoaa joustavan ratkaisun verkon yhdenmukaistamiseen ja yksinkertaistamiseen.

### 3.1 Organisaation nykyinen verkko

Innofactorin nykyisessä verkkomallissa toimipisteiden erillisiä lähiverkkoja ja palvelukeskusten palveluita yhdistetään toisiinsa VPN-päätelaitteilla kuvan 5 esittämän periaatteen mukaisesti. Jokaisella toimipisteellä on oma VPN-päätelaite eli palomuuuri, jolla luodaan salattu tunneli keskitetyn VPN-päätelaitteen ja toimipisteen välille. VPN-tunnelit yhdistävät toimipisteiden paikalliset lähiverkot palvelukeskusten demilitarisoi-tuihin (DMZ, demilitarized zone) vyöhykkeisiin sekä mahdollistavat toimipisteiden väli-sen liikenteen salattuna. Toimipisteiden, DMZ-alueiden sekä Internetin julkisen liikenteen kulkua suodatetaan palvelukeskusten ja toimipisteiden palomuuureilla. Jokainen toimipiste tarvitsee omalta paikalliselta operaattoriltaan Internet-yhteyden, julkisen IP-osoitteen ja mainitun VPN-päätelaitteen yhdistämään verkkoja.



Kuva 5. VPN-verkko.

Toimipisteiden määrän kasvettua organisaation verkon ylläpitoon vaadittavien verkkolaitteiden määrä on kasvanut, kuten myös omien lähiverkkojen määrä on kasvanut. Koska jokaiselle toimipisteelle on toimitettu verkkoyhteys usealta paikalliselta operaattorilta, verkon kokonaishallittavuuteen tulee useita erilaisia käytäntöjä sekä verkkoyhteyksien hinnoittelussa voi olla huomattavia paikkakuntakohtaisia eroja.

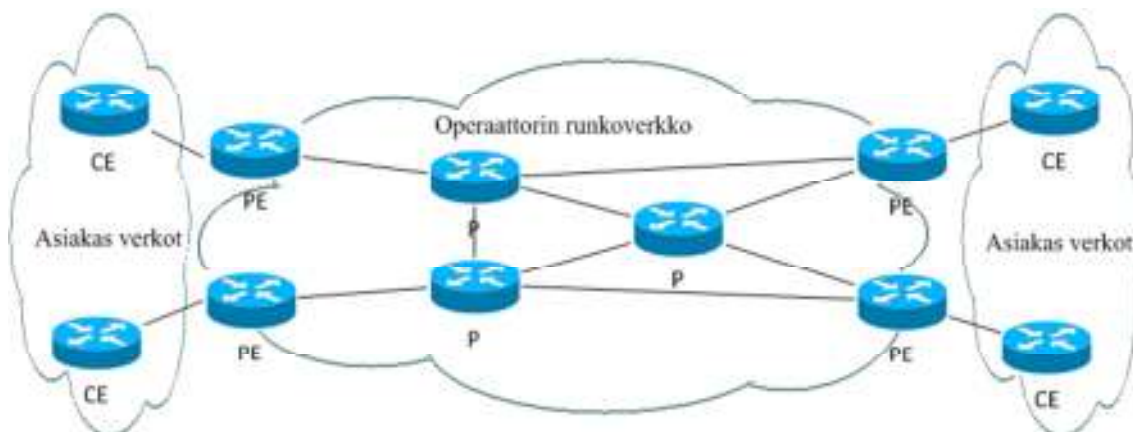
Lisäksi tarjottujen palveluiden lisääntymisen myötä asiakas- tai palvelukohtaiset verkkoratkaisut ovat laajentuneet sekä monimutkaistuneet. Jos esimerkiksi oletetaan jonkin uuden palvelun vaativan oman rajatun DMZ-verkkoalueen, haluttuihin protokoliin suodatetun Internetyhteyden sekä jokaiselta toimipisteeltä yhteyden kyseisen palvelun resursseihin, tarvitaan jokaisen toimipisteen omalla palomuurilla sekä palvelua rajaavalla palomuurilla määrittelyt kyseiselle verkolle. Lisäksi laajentuminen ulkomailla luo paikallisten toimipisteiden integroimisen VPN-tunnelointiin perustuvaan verkkokokonaisuuteen haasteita. Näistä syistä myös verkon ylläpidollisten resurssien tarve on kasvanut niin työmäärällä kuin taloudellisilla mittareilla mitattuna.

### 3.2 Tarjotut MPLS-ratkaisut

Tarjouskilpailun valittiin mukaan operaattori, joka toimittaa suurimman osan organisaation nykyisistä verkkoliitännöistä ja jolla on merkittävä osa käytettyjen asiakasverkko-segmenttien toimituksissa. Toiseksi kilpailutetuksi tarjoajaksi valittiin operaattori, jonka palvelunlaatu oli aiemmin hyväksi todettu organisaation yrityskauppojen myötä ja jolla on myös riittävät yhteistyökumppanit ulkomailla.

Tarjousten perusteella verkon uudistaminen ei yritykselle ole taloudellisesti kovinkaan mittava panostus ja kuukausittaisista kuluissa voi saada jopa säästöjä keskittämällä verkkoyhteyksiä yhteen toimittajaan. Molemmat kilpailutuksessa mukana olleet palveluntarjoajat pitivät verkkouudistuksen tarpeista keskusteltaessa luontevimpana ratkaisuna MPLS-verkkoa. Tekniseltä toteutukseltaan tarjoukset olivat käytännössä identtisiä. Myös taloudellisesti tarjoukset olivat erittäin lähellä toisiaan, josta voisi päätellä MPLS-ratkaisujen olevan molemmilla mukana olleilla palveluntarjoajilla hyvin prosessoituja sekä kilpailutettuja. Verkkouudistuksen toimittajaksi valittiin operaattori, joka toimittaa suurimman osan yrityksen verkkoliitännöistä sekä palveluista. Tästä katsottiin olevan hyötyä projektin etenemisessä, ja kyseinen tarjous oli yksityiskohtaisempi, kattavampi niin palveluiden kuin lisäpalveluiden esittelyssä ja taloudellisesti edullisempi.

Kumpikin operaattori oli halukas tarjoamaan muilta operaattoreilta hankittujen verkkoyhteyksien korvaamista omalla kuitutekniikkayhteydellään. Tarjotuissa malleissa toimipisteet ja niiden lähiverkot yhdistettäisiin operaattorin runkoverkossa MPLS-tekniikalla, kuten kuvassa 6 on havainnollistettu.

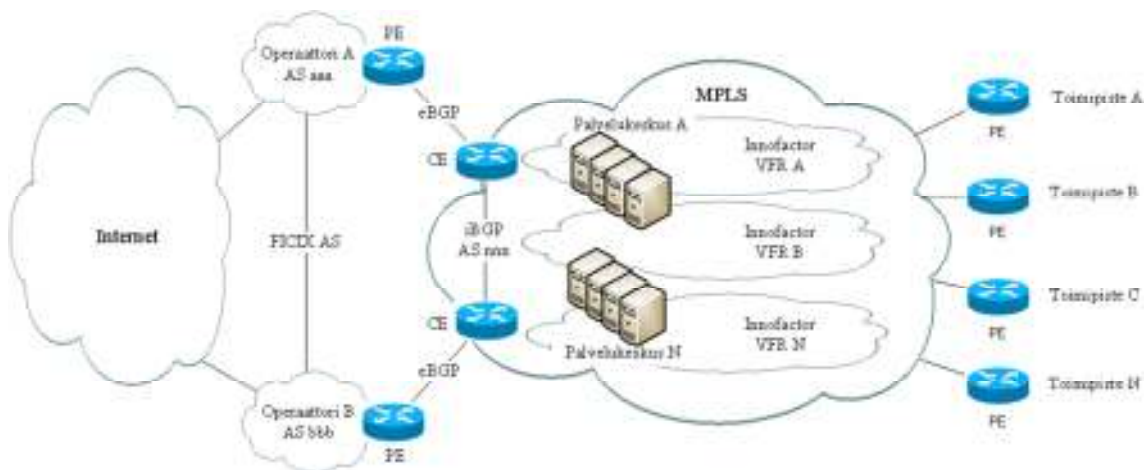


Kuva 6. Suljettu MPLS-arkkitehtuuri.

Kahteen Innofactorin nykyiseen palvelukeskukseen tehtäisiin Internet yhteyspiste eli niin sanottu nielu. Palvelukeskuksiin tarjoutuksissa luotaisiin kuvan 7 mukaisesti BGP-protokollaa ja Innofactorin jo olemassa olevaa AS-numeroa hyväksikäyttäen kahdennettu ja vikasietoinen Internetyhteys, joka on toteutettavissa kahden eri operaattorin yhteydellä, jota kutsutaan yleisesti BGP-multihomingiksi.

Kahden operaattorin multihoming -Internet-palvelussa valittu palveluntarjoaja voi toimia pääoperaattorina, joka hallinnoi kokonaisuutta, toimittaa yhden Internet-liittymän ja vastaa rajapinnasta toisen operaattorin liittymään, toteuttaen BGP-reitityksen oman verkkonsa sekä toisen operaattorin verkon suuntaan. Ratkaisulla saadaan asiakkaan Internet-liikenne vikasietoiseksi yhden operaattorin mahdollisesta vikatilanteesta sekä ohjattua liikenne automaattisesti lyhyimmän AS-polun mukaan.

Toteutuksessa asiakkaan CE-reitittimet vaihtavat reititystietoja reititysalueen sisällä toimivalla iBGP (internal BGP) -mekanismilla käyttäen asiakkaan omaa autonomista järjestelmää (AS, Autonomous System) sekä asiakkaan operaattorista riippumattomia julkisia IP-osoitteita. Operaattorien PE-reitittimet käyttävät eBGP (external BGP) eli reititysalueiden välillä toimivaa BGP-protokollaa ja operaattorien omaa FICIX:lle (Finnish Communication and Internet Exchange ry) rekisteröityä verkkotunnusnumeroa.



Kuva 7. Innofactorin MPLS-verkkoratkaisu.

### 3.3 Mahdollisia haasteita tai ongelmia

Siirryttäessä operaattorin toimittamaan MPLS-verkkoon tulee organisaatiosta enemmän riippuvainen yhdestä palveluntarjoajasta tai yhdestä palvelusopimuksesta, etenkin jos tarjottu palvelu on sovittu määräaikaiseksi. Verkon hallinnoinnin ulkoistaminen tekee joistain ylläpitotöistä, joita yrityksessä on perinteisesti voitu tehdä itse, tilattavia ja mahdollisesti lisämaksullisia palveluita, joiden toteutumisaikataulu ei ole omissa käsissä. Lisäksi organisaation ulkopuolisen tahon vastaaminen verkkopalveluista lisää tarvetta organisaation tai verkon hallinnollisen tietoturvan tai riskienhallintaprosessien uudelleenarvioinnille.

MPLS-verkon implementoinnissa mahdollisia haasteita ovat palveluiden saatavuuden varmistaminen mahdollisimman pienillä vaikutuksilla palveluita käyttäville tahoille. Etenkin jos organisaatiolla on rajattuja rajapintoja kolmansille osapuolille esimerkiksi suoraan toimipisteiden tai palveluiden nykyisillä julkisilla IP-osoitteilla, voi palveluiden käyttö estyä IP-osoitteiden vaihtuessa, kunnes mahdolliset muutokset on tehty myös kolmansien tahojen puolesta. Myös MPLS-verkkoon siirrettyjen palveluiden testaaminen loppukäyttäjän näkökulmasta on haasteellista.

## 4 Projektisuunnitelma MPLS-tekniikkaan siirtymisestä

Tässä osiossa esitetään alustava projektisuunnitelma MPLS-verkon toteuttamiseksi yrityksen käyttöön. Toimittaja laatii toimituksesta yhdessä asiakkaan kanssa varsinaisen projektisuunnitelman projektin käynnistämisen yhteydessä. Projektisuunnitelma sisältää projektin tavoitteet ja vaatimukset sekä rakenteen työn ositukselle. Toimittajalla on kokonaisvastuu järjestelmän toteutuksesta sekä uusittavista verkkolaitteista. Järjestelmän testaus, dokumentointi sekä projektinhallinta toteutetaan yhteistyössä toimittajan ja asiakkaan toimesta. Toimittaja tukee asiakasta järjestelmän käyttöönoton suunnittelussa ja käyttöönotossa. Asiakas vastaa tarvittavien tietojen antamisesta, hyväksymistestauksesta sekä käyttöönotosta niiltä osin, kun se ei kuulu toimittajan vastuulle, esimerkiksi tiedottamisesta verkossa toimivien palveluiden käyttäjille. Projektiin liittyy riippuvuussuhde kolmannen tahon toteuttamaan Internet-yhteyden kahdennukseen, jota ei käsitellä vielä tässä suunnitelmassa, koska se ei ole esteenä toimivan verkkopalvelun tuottamiselle.

### 4.1 Projektin tavoitteet, malli ja kriteerit

#### Projektin tavoitteet ja tulokset

Toimitusprojektin tavoitteena on toteuttaa määritetyssä aikataulussa ja käytettävissä olevien resurssien puitteissa asiakkaan tarjouspyyntöä ja alustavaa määritystä vastaava, toimittajan toteutusmallin mukaisesti toteutettu ja asiakkaan toimintaa mahdollisimman hyvin tukeva järjestelmä.

#### Projektin tuloksena syntyy

- tarjouspyyntöä vastaava ja käyttöönotettavissa oleva verkkokokonaisuus
- yritykselle palvelukuvaus muutos- ja palvelupyyntöjä varten
- projektidokumentaatio
- käytön, ylläpidon ja kehityksen edellyttämä dokumentaatio.

## Projektityömalli

Järjestelmän onnistunut määrittely, suunnittelu, toteutus, stabilointi ja käyttöönotto edellyttävät onnistunutta toimitusprojektia. Toimittaja tarjoaa projektipäällikön sovittamaan projektimallia asiakkaan tarpeisiin ja nykyiseen ympäristöön soveltuvaksi. Projektissa toimittaja edellyttää asiakkaan kanssa yhteistyötä, jota johdetaan, ohjataan ja tuetaan yhteistyössä eri vaiheissa. Mallissa toimittaja jakaa projektin seuraaviin vaiheisiin:

- määrittely- ja tiedonkeruuvaihe
- projektin käynnistys
- projektin suunnittelu ja toteutus.

## Hyväksymiskäytännöt ja projektin päätöskriteerit

Asiakas osallistuu projektiin tarjoamalla toimittajan tarvitsemat tiedot tarpeita vastaavan järjestelmän luomiseksi. Onnistuneen tuloksen varmistamiseksi palvelun toteuttamista varten luotava dokumentaatio katselmoidaan aina toimittajan ja asiakkaan projektiryhmässä. Katselmointikierrroksia toistetaan, kunnes dokumentaatio on valmis hyväksyttäväksi. Tavoiteltavana määränä voidaan pitää 2–3 katselmointikierrrosta. Aikataulu on suunniteltu tämän mukaiseksi, siten että kummallakin osapuolella on aina viikko aikaa dokumentin läpikäymiseen ja muokkaamiseen.

Kun dokumentaatio on sekä asiakkaan että toimittajan näkökulmasta valmis toteutuksen pohjaksi, asiakkaan ja toimittajan projektiryhmät esittävät ohjausryhmälle dokumentaation hyväksymistä, jonka jälkeen ohjausryhmä voi hyväksyä dokumentaation. Myös muutokset jo hyväksytyyn dokumentaatioon on hyväksyttävä ohjausryhmällä.

Asiakas katselmoi toteutetun järjestelmän suorittamalla hyväksymistestauksen. Kun hyväksymistestaus on suoritettu ja sen aikana ilmenneet puutteet on korjattu ja testattu, ohjausryhmä hyväksyy testausraportin ja sen myötä verkkopalvelun toteutuksen.



Käyttöönottovaihe hyväksytään sopimuksen mukaisesti, kun tuotantonsiirto on tehty. Ohjausryhmä hyväksyy käyttöönoton ja projekti voidaan päättää, kun määritysten mukainen järjestelmä on asiakkaalla tuotantokäytössä.

#### 4.2 Projektin ositus, vaiheistus, aikataulu ja työmäärät

Projekti on alustavasti ositettu ja vaiheistettu seuraavasti:

- määrittely
- suunnittelu
- toteutus
- käyttöönotto.

Varsinainen projektiaikataulu muodostetaan yhdessä asiakkaan kanssa projektin käynnistämisen yhteydessä ottaen huomioon asiakkaan omat aikataulutarpeet ja -suunnitelmat. Toimittajan näkemys projektin vaatimista työmääristä henkilötyöpäivinä (hpt) täytetään taulukoon 1 asiakkaan omien työmääräarvioiden kanssa. Työmääriä tarkennetaan vaiheittain kunkin projektin vaiheen jälkeen.

Taulukko 1. Työmääräarviot.

Vaihe	Toimittajan arvioitu työmäärä	Asiakkaan arvioitu työmäärä
Määrittely		
Suunnittelu		
Toteutus		
Käyttöönotto		
Yhteensä		

### 4.3 Projektin käynnistys

Aloittamisen edellytyksenä on, että sopimus on hyväksytty ja allekirjoitettu.

Toimittajan vastuut ovat

- projektisuunnitelman ja sen liitteiden valmistelu
- projektiryhmän aloituskokouksen koolle kutsuminen
- projektisuunnitelman ja sen liitteiden muokkaaminen projektin aloituskokouksessa sovitun mukaisesti.

Asiakkaan vastuut ovat osallistuminen projektiryhmän aloituskokoukseen ja dokumentaation katselmointi ja hyväksyminen.

Projektisuunnitelma voidaan hyväksyä, kun todetaan, että se on riittävän laaja ja yksityiskohtainen projektin onnistuneen läpiviennin varmistamiseksi. Projektisuunnitelma hyväksytään ohjausryhmässä.

### 4.4 Määrittäminen

Määrittämissivun tavoitteena on että asiakas ja toimittaja ymmärtävät ja hahmottavat yhteisesti tulevan järjestelmän ominaisuudet, toiminnan ja laajuuden. Toimittaja pystyy arvioimaan tarkasti suunnittelun vaatiman työmäärän, varaamaan tarvittavat resurssit sekä vahvistamaan aikataulun suunnittelun osalta. Määrittämissivussa tuotetaan riittävän laaja dokumentaatio, joka on molemminpuolisesti ymmärretty ja jonka pohjalta tarkempi suunnittelu voidaan toteuttaa. Määrittämissivudokumentti sisältää käyttäjäryhmien ja -roolien kuvaukset sekä teknisen arkkitehtuurin yleiskuvauksen, jonka pohjalta tarkempi tekninen suunnittelu voidaan tehdä.

Toimittajan vastuulla on

- tutustua olemassa oleviin järjestelmiin ja määrittämissivudokumenttaatioon
- kutsua koolle määrittämissivuryhmä, ja johtaa sitä

- laatia tarvittavat määrittäydokumentaatit.

Asiakkaan vastuulla on

- toimittaa toimittajalle tarvittavat dokumentaatit tarvittaviin järjestelmiin
- osallistua määrittäydyryhman työpajoihin
- katselmoida määrittäydokumentit.

Määrittäyvaihe voidaan hyväksyä, kun määrittäydokumentatio on toteutettu tässä projektisuunnitelmassa kuvattujen menetelmien mukaisesti ja katsotaan sovitun mukaiseksi.

Suunnittelu

Suunnitteluvaiheen aloittamisen edellytyksenä on, että määrittäys on hyväksytty. Suunnitelmien tulee olla dokumentoitu sillä tasolla, että järjestelmä ja integraatiot voidaan toteuttaa suunnitelman pohjalta. Dokumentaation tulee kuvata vähintään toteutuksen edellyttämän arkkitehtuurin, konfiguroinnin ja integraatiot. Suunnitelmassa täytyy selvittää toteutuksen, stabiloinnin ja toteutuksen vaatimat työmäärät, resurssit sekä aikataulu. Toimittaja tukee asiakasta käyttöönoton suunnittelussa.

Suunnitteluvaiheessa toimittajan vastuulla on vaadittavien suunnitelmien laadinta, dokumentointi ja katselmointi sekä tarvittavien työryhmien järjestäminen asiakkaan ja mahdollisten kolmansien osapuolten kanssa.

Asiakkaan vastuulla on

- pyydettyjen lisätietojen toimittaminen
- osallistuminen mahdollisiin työpajoihin
- dokumentaation katselmointi ja hyväksyminen niiltä osin kuin se on tarpeen
- luoda toimittajan kanssa suunnitelma palvelun käyttöönotosta.

Suunnitteluvaihe voidaan hyväksyä, kun suunnitteludokumentit on toteutettu projektisuunnitelmassa kuvattujen menetelmien mukaisesti ja katsotaan sovitun mukaiseksi.

## Toteutus

Toteutusvaihe voidaan aloittaa kun kaikki suunnitelmat ovat hyväksytyt. Vaiheessa toimittajan vastuulla on

- verkkopalveluiden ja integraatioiden toteutus
- toteutuksen dokumentointi
- välivaiheiden esittäminen asiakkaalle, niiltä osin kuin on tarpeen tai on sovittu.

Asiakas tarkentaa tarvittaessa suunnitelmia tai välivaiheita. Toteutus voidaan hyväksyä kun kaikki vaiheeseen liittyvät tehtävät dokumentteineen on tehty ja järjestelmän testaus on suoritettu.

## Käyttöönotto

Käyttöönotto voidaan aloittaa, kun ohjausryhmä on hyväksynyt toteutuksen ja sen testauksen sekä asiakas on valmis siirtämään palveluita järjestelmään. Käyttöönotossa asiakas siirtää toimittajan tukemana palveluita toteutettuun verkkopalveluun suunnitelmien ja testausten perusteella, sekä seuraa siirrettyjen palveluiden toimintaa uudessa ympäristössä. Käyttöönotossa toimittajan vastuulla on asiakkaan tukeminen käyttöönotossa suunnitelmien mukaisesti, sekä tarvittavan koulutuksen järjestäminen järjestelmien käyttöönottoa ja ylläpitoa varten. Asiakas vastaa käyttöönoton koordinoimisesta sekä huolehtii tarvittavasta tiedottamisesta. Käyttöönottovaihe voidaan hyväksyä, kun on todettu, että järjestelmä testattu ja otettavissa käyttöön ja että järjestelmä toimii seurantavaiheen perusteella teknisesti oikein.

## Projektin lopetus

Projektin lopettamisen edellytyksenä on, että järjestelmä on otettu käyttöön. Toimittaja ja asiakas pitävät projektin lopetuskokouksen, jossa todetaan projekti päättyneeksi sekä sovitaan käytännöistä liittyen ylläpitovaiheeseen. Asiakas siirtyy toimittajan asia-

kastuen piiriin. Viimeistään projektin lopetusvaiheessa tehdään järjestelmän jatkuvan asiakaspalvelun ja ylläpidon sopimus sekä dokumentoidaan näihin liittyvät käytännöt. [15.]

## **5 Yhteenveto**

Työn tavoitteena oli etsiä organisaation kasvaneisiin tarpeisiin sopivampaa verkkoratkaisua, yksinkertaistaa verkon ylläpitoa sekä mahdollisesti saavuttaa kustannussäästöjä uudistuksen myötä. Tehtyjen tarjousten perusteella operaattorit ovat halukkaita tarjoamaan kokonaisvaltaisia verkkoratkaisuja, joihin sisältyy verkkoliittynät tarvittavine laitteistoineen sekä lisäpalveluineen. Vaikka saadut tarjoukset olivat vasta alustavia, eikä lopullisia kustannuksia voitu ilman perusteellista määrittelyä laskea johtuen projektin määrittelyn keskeneräisyydestä, oli keskitettyjen palveluiden myötä havaittavissa saavutettavia kustannussäästöjä yksittäisiin verkkoliittäntöihin tai palveluihin verrattuna.

Työn puitteissa saatiin muodostettua tarvittava tekninen käsitys MPLS-verkosta tukemaan tarjouskilpailuttamista, toteutuksen valintaperusteita sekä alustamaan tulevia määrittely- sekä suunnitteluvaiheita. Insinööri työ vastasi tavoitteisiin löytää tehokkaampi verkkojärjestelmä tukemaan organisaation kasvua etenkin ulkomailla sekä tuottaa alustava suunnitelma uuden järjestelmän käyttöönottamiseksi. Lisäksi kustannussäästöjä ylläpitotyöstä sekä verkkopalveluista oli saavutettavissa, joten näiltä osin työ oli onnistunut.

## Lähteet

- 1 Deloitte Technology Fast 50 vuoden 2012 listaus Verkkodokumentti. <[http://www.deloitte.com/view/fi\\_FI/fi/ajankohtaista/](http://www.deloitte.com/view/fi_FI/fi/ajankohtaista/)> Päivitetty 2012. Luettu 6.1.2013.
- 2 Innofactor Oyj WWW-sivut. Verkkodokumentti. <[http://www.innofactor.fi/media/uutiset/0/0/innofactor\\_oyj\\_n\\_tilinpaatostiedote\\_2011\\_2](http://www.innofactor.fi/media/uutiset/0/0/innofactor_oyj_n_tilinpaatostiedote_2011_2) Päivitetty> 28.2 2012. Luettu 6.1.2013.
- 3 IETF. Multiprotocol Label Switching. 1997. Verkkodokumentti. <<http://datatracker.ietf.org/doc/charter-ietf-mpls>> Päivitetty 3.3.1997. Luettu 6.1 2013.
- 4 Davie, Bruce S., Peterson, Larry L. 2012. Computer Networks a system approach, fifth edition. Boston: Morgan Kaufmann.
- 5 Minei, Ina, Lucek, Julian. 2005. MPLS Enabled Applications, Emerging Developments and new Technologies. West Sussex: John Wiley & Sons Ltd.
- 6 Ash, Gerald R. Traffic Engineering and QoS Optimization of Integrated Voice and Data Networks. 2006. Burlington: Morgan Kaufmann.
- 7 Minoli, Daniel. 2003. Telecommunications Technology Handbook. Norwood, MA, USA: Artech House.
- 8 IETF. RFC 5036. LDP Specification 2007. Verkkodokumentti. <<http://tools.ietf.org/html/rfc5036>> Päivitetty 2007. Luettu 13.5.2013.
- 9 Tatipamula, Mallikarjun Oki, Eiji Rojas-Cessa, Roberto. 2012. Advanced Internet Protocols, Services, and Applications. Hoboken: Wiley.

- 10 Herrero, Gonzalo Gomez, Van der Ven, Jan Anton Bernal. 2010. Network Mergers and Migrations: Junos Design and Implementation. Hoboken, NJ, USA: Wiley.
- 11 Cisco Active Network Abstraction Reference Guide. 2013. Verkkodokumentti. <[http://www.cisco.com/en/US/docs/net\\_mgmt/active\\_network\\_abstraction/3.7/reference/guide/vrf.html](http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/reference/guide/vrf.html)> Luettu 15.5.2013.
- 12 Metsälä, Esa. Salmelin, Juha. 2012. Mobile Backhaul. Hoboken: Wiley.
- 13 Apcar, Jeff. Guichard, Jim Pepelnjak, Ivan. 2003. MPLS and VPN Architectures Volume II. Indianapolis USA: Cisco Press.
- 14 IETF. RFC4364. BGP/MPLS VPNs. 1999. Verkkodokumentti. <<http://tools.ietf.org/html/rfc2547>> Päivitetty 1999. Luettu 2.2 2013.
- 15 Karlsson, Åke, Marttala Anders. 2001. Projekti kirjja Onnistuneen projektin toteuttaminen Helsinki: Kauppakaari.