Joel Honkanen

SD-WAN MPLS-yritysverkon korvaavana ratkaisuna

Opinnäytetyö
Tieto- ja viestintätekniikan koulutus

Kyberturvallisuus

2021

Tekijä/Tekijät	Tutkinto	Aika
Joel Honkanen	Insinööri (AMK)	Elokuu 2021
Opinnäytetyön nimi SD-WAN MPLS-yritysverkon korvaavana ratkaisuna		43 sivua
Toimeksiantaja Elisa Oyj		
Ohjaaja Vesa Kankare		

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli selvittää, olisiko Multi-protocol Label Switching (MPLS) vai Software-defined Wide Area Networking (SD-WAN) käytettävä verkkotekninen ratkaisu tulevaisuuden yritysverkoissa. Tutkimuksen pohja perustuu opinnäytetyön aiheeseen kuuluvien tekniikoiden teoriapohjaiseen materiaaliin, jonka pohjalta työn käytännön tutkimusosa toteutettiin. Tekniikoiden topologinen toteutus tapahtui rakentamalla hypoteettisia ratkaisuja, jotka kuvaavat tämän hetken mahdollisia yritysverkkopohjaisia toteutuksia. Näiden hypoteettisten ratkaisujen tavoitteena ei kuitenkaan ollut antaa tarkkaa kuvausta parhaasta mahdollisesta tavasta toteuttaa kyseisiä yritysverkkoratkaisuja.

Tulevaisuudessa toteutettavien yritysverkkoratkaisujen on oltava toiminnaltaan luotettavia, sekä kykeneviä laajenemaan yritysten IT-strategian vaatimalla tasolla. Tämä tuo erilaisten ratkaisujen kehityksen ja niitä ylläpitävien tahojen asiantuntevan osaamisen tärkeyden uudelle tasolle. Tietoturvan tärkeyttä ei myöskään tule unohtaa, kun kehitetään optimaalisinta ratkaisua yritysverkoille.

Tutkimuksen alussa keskityttiin aiheena olleiden teknologioiden perusominaisuuksien tutkimiseen, jotta tarvittavat tekninen tieto voitiin sisällyttää käytännöntutkimuksessa näytettyihin topologioihin. Esimerkki topologioiden tukemat tulokset voitiin sisällyttää teoriaosassa läpikäytyjen ominaisuuksien kanssa tutkimustuloksiin.

Opinnäytetyön tutkimuskysymyksiin vastattiin ja asetetut tavoitteet saavutettiin riittävällä tasolla. Näiden vastauksien pohjalta voitiin todeta tulevaisuuden verkkotekniikoiden toteutusten paremmuuden ja käytettävyyden perustuvan täysin palveluntarjoajan palveluita ostavan yrityksen tarpeisiin. Tutkimukseen lisättiin tietoturvan puolesta tarvittavaa keskustelua, ja mahdollisia ehdotettuja toimintatapoja toteuttaa näiden ratkaisujen ohella toimivia tietoturvaa parantavia ratkaisuja.

Asiasanat

tietoverkko, saatavuus, tietoturva

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Joel Honkanen	Bachelor of Engineering	August 2021

Thesis title

SD-WAN as a replacement for MPLS in corporate networks

43 pages

Commissioned by

Elisa Oyj

Supervisor

Vesa Kankare

Abstract

The objective of this thesis was to determine whether Multiprotocol Label Switching or Software-defined Wide Area Network could be a viable solution for future corporate networks. The study is based on theory-based material, which was used to construct the hypothesis-based network typologies of these corporate network solutions. The purpose was not to establish an accurate picture of how these hypothetic solutions would be implemented in the future.

In the future, corporate network solutions are required to be reliable and expandable at the level required by the IT strategy of the company. This brings the development of various solutions and the importance of the expertise of those who maintain them to a new level. Importance of security should not be forgotten, when developing optimal solution for corporate networks.

At the beginning of the study, the focus was on the basic features of the technologies in question, so that the necessary technical information could be included in the topologies shown in the hypothesis field study. The results supported by the example topologies could be included in the theoretical part with the results of the properties reviewed in the study.

The research questions of the thesis were answered and the set objectives were achieved at a sufficient level. Based on these results, it could be concluded that the superiority and usability of future network technology implementations were based entirely on the needs of the company purchasing the services of the service provider. The necessary debate on information security was added to the study, and possible proposed courses of action to implement security-enhancing solutions alongside these solutions.

Keywords

network, availability, security

SISÄLLYS

LYHENTEET JA TERMIT

ATM	Asynchronous Transfer Mode
CPE	Customer Provider Edge
DPS	Dynamic Path Steering
FEC	Forwarding Equivalence Class
GRE	Generic Routing Encapsulation
IPS	Intrusion Prevention System
IP-SEC	IP-Security Architecture
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Base
LSP	Label Switch Paths
LSR	Label Switching Router
MPLS	Multiprotocol Label Switching
MP-BGP	Multiprotocol BGP
NGFW	Next Generation Firewall
OSI	Open Systems Interconnection
P	Provider (Router)
PE	Provider Edge
PHP	Penultimate Hop Popping
RD	Route Distinguisher
SaaS	Software as a Service
SD-WAN	Software-defined Wide Area Network
SLA	Service Level Agreement
TC	Traffic Class
TTL	Time-to-live
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VoIP	Voice over IP

1 JOHDANTO

Verkkotekniikoiden innovaatio maailmalla on johtanut tilanteeseen, jossa ohjelmallisten verkkojen markkinointi on lisännyt kysymyksiä nykyisten yritysverkoissa käytettävien ratkaisujen tarpeellisuudesta. Lisääntynyt tarve integroida pilvipalveluita osaksi yritysten IT-strategiaa on lisännyt tarvetta entistä paremmille tavoille tuottaa palveluita WAN-yhteyksiä tarjoaville operaattoreille. Näiden palveluiden tulee olla luotettavia, kohtuuhintaisia toteuttaa, sekä verkon kapasiteetin on tarjottava asiakkaalle vakaa yhteys.

Tutkimuksen kohteena on ohjelmallisten verkkojen WAN-osuutta edustava Software-defined Wide Area Network tai SD-WAN. Vertailu kohtana käytetään Multiprotocol Label Switching- tai MPLS-verkkoa, joka on laajalti käytössä oleva verkkotekniikka yritysverkkojen WAN-ratkaisuiden toteutukseen. Työssä keskitytään tutkimaan edellä mainittujen kahden tekniikan hyödyllisyyttä tilanteessa, jossa Suomessa toimiva yritys tilaa palveluntarjoajalta heidän tarpeisiinsa sopivimman ratkaisun. Näin voidaan vertailla yritysten kannalta, onko nykyisellä MPLS-verkolla paikkaa tulevaisuuden verkkoratkaisuissa ohjelmallisten verkkoratkaisujen yleistyessä.

Opinnäytetyön toimeksiantaja on Kaakkois-Suomen ammattikorkeakoulu, XAMK. Vuodesta 2017 XAMK-nimellä toiminut Kaakkois-Suomen ammattikorkea koulu on korkeamman asteen koulutuksesta vastaava instituutti. Vaikka toimeksiantajana työlle toimii XAMK, ei työtä tehdä suoranaisesti esimerkiksi tietotekniikan koulutuksen kehittämistä varten.

1.1 Opinnäytetyön tavoitteet

Tämän opinnäytetyön tavoitteena on hankkia tietoa ja tutkia sekä vertailla näiden pohjalta kahden nykypäivän ja tulevaisuuden tekniikkaa, joilla toteutetaan yritysverkkoratkaisuja. Teoriapohjan avulla pyritään saamaan tarvittu pohjatieto, jotta käytännön tutkimuksen aikana tehtävät topologiat edustaisivat mahdollisimman tarkasti työhön valittujen tekniikoiden toteutustapaa esimerkkeinä annetuille yritysverkkototeutuksille. Toteutusten erilaisten variaatioiden määrä

on kuitenkin hyvin suuri, joten työssä joudutaan rajaamaan tarkastelu mahdollisesti muutamiin erilaisiin kokoonpanoihin.

Tarkoituksena on käydä läpi tekniikoiden vahvuudet erilaisissa toteutuksissa, sekä tarkastella tietoturvapuolta ja koota näistä hypoteettisella tasolla toimiva topologia. Työn aikana näytettävät topologiat eivät tule vastaamaan parasta mahdollista toteutusta, vaan perustuvat täysin tavoitteeseen saada suuntaa antava tulos tutkimukselle. Saatujen tuloksien pohjalta tullaan toteamaan työn tutkimuskysymyksiin liittyvät vastaukset ja mahdolliset ongelmat, joita tutkimuksen aikana ja ennen tutkimusta havaittiin.

Opinnäytetyön yhtenä tutkimusongelmista on SD-WAN-teknologiasta löytyvän tiedon huomattava vähäisyys. Tämä vähäisyys aiheuttaa kerättävän materiaalin perustumisen suurelta osin eri laitetoimittajien myyntiin käytettävään materiaaliin, eikä niinkään tekniseen tietoon, jolla saataisiin tarkempaa teoriapohjaista tietoa näistä ratkaisuista. Löytyvä materiaali perustuu myös yleisesti yhden tietyn laitetoimittajan ominaisuuksiin, joten työn aikana tehtävien havaintojen aikana tulee ottaa huomioon laitetoimittajista aiheutuvat erot.

1.2 Opinnäytetyön tutkimusmenetelmät

Tämän opinnäytetyön tutkimusmenetelmäksi valittiin tapaustutkimuksen (case study) piiriin kuuluva tutkimusmenetelmä. Valinta tehtiin työn suunnitteluvaiheessa, sillä perusteella, että työssä tulisi olemaan myös pieni osa numeropohjaista tarkastelua, joka liittyy mahdollisiin yritykselle aiheutuviin kuluihin. Kun työssä tutkitaan konkreettisia havaintoja analysoimalla, mittaamalla ja tarkastelemalla, sitä kustannusten näkökulmasta voidaan tutkimuksesta käyttää kvantitatiivista ja kvalitatiivisen tutkimuksen määritelmää. (Jyväskylän yliopisto 2015.) Työn kvalitatiivinen suuntaus perustuu työn toteutustapaan, jossa pyritään löytämään tutkimuskohteille historiallisesti yksityiskohtainen ja tarkka kuva käyttötarkoituksista sekä yhdistämään tutkimus yhteyskunnallisiin yhteyksiin. (ks. Eskola & Suoranta 1999.) Laadullisen ja määrällisen tutkimuksen eroja korostetaan, vaikka molempia suuntauksia voidaan käyttää myös samassa tutkimuksessa, kuten tässä työssä sovelletaan. (Jyväskylän yliopisto 2015.)

2 YRITYSVERKOT

Opinnäytetyö keskittyy tulevaisuuden ja tämän hetken yritysverkoissa käytettäviin kahteen eri tekniikkaan. Tämän luvun tarkoituksena on kertoa olennainen pohjatieto yritysverkkojen historiasta ja Suomen yritysverkkoista. Luvussa käsitellyn tieto antaa paremman tietopohjan tutkittaville tekniikoille, ja niiden mahdollisille käyttötarkoituksille.

Tulevaisuuden yritysten luotettavan tiedonsiirron tarve lisääntyy kovaa tahtia, jolloin tarve vaihtoehtoisille ratkaisuille kasvaa. Myös yritysten käyttämien palveluiden siirtyminen pilveen vaikuttaa tarpeeseen kehittää uusia turvallisempia ratkaisuja korvaamaan ja tukemaan jo olemassa olevia ratkaisuja.
Tämän työn tavoitteena on vertailla, testata ja todeta tämänhetkisen tiedon pohjalta, kuinka SD-WAN ja MPLS soveltuvat tulevaisuuden yritysverkkoratkaisuksi.

2.1 Yritysverkkoratkaisujen historia

Yritysverkoissa käytettävät ratkaisut ovat kehittyneet vuosien aikana nopeasti. 1990-luvun alkupuolella verkkoratkaisuissa käytettiin suurelta osin vuokralinjoja (eng. Leased line), joiden välityksellä yrityksen eri toimipisteet olivat yhteydessä toisiinsa. Linjat olivat yksityisiä, jolloin ne olivat vain kyseisen yrityksen tai operaattorin käytettävissä.

Isoin harppaus yritysverkoissa käytettävissä teknologioissa palveluntarjoajille, lähinnä operaattoreille, tuli Asynchronous Transfer Mode -ratkaisun (ATM) myötä. ATM-teknologiaa pidettiin, jopa ratkaisuna internetin kapasiteettiongelmaan, sillä se kykenee käsittelemään paketteja muutetussa pienemmässä koossa. Tämä poikkeaa normaalista tavasta siirtää paketteja, jossa tiedonsiirtolinjalla voi aiheutua merkittävää viivettä, kun paketit kuljetetaan aina täysikokoisena. (Techopedia 2020.)

Ennen MPLS:n käyttöönottoa yritykset käyttivät ratkaisuja, kuten esimerkiksi ATM:ää, Frame Relayta tai ethernetiä. Nykypäivän tiedonsiirtokapasiteetin lisääntymisen ja tietoturvan tarpeen kasvaminen pakottaa yritykset siirtymään uusiin, entistä tehokkaampiin tapoihin siirtää tietoa. Tälle hetkellä yritykset nojautuvat täysin MPLS-ratkaisuihin mahdollistaakseen turvallisen ja luotettavan tiedonsiirron. Vaikka MPLS on mullistava teknologinen harppaus edeltäjiinsä, on tarve kapasiteetille, tietoturvalle ja hallittavuudelle lisääntynyt. Esimerkiksi yritysten siirtyminen pilvipalveluihin lisää kapasiteetin ja hallittavuuden tarvetta verkossa. MPLS-verkkojen rinnalle ehdotetaan SD-WAN-pohjaisia verkkoja, joissa edellä mainitut ominaisuudet ovat edeltäjäänsä huomattavasti kehittyneempiä ja joustavampia.

2.2 Yritysverkot suomessa

Suomessa yritysverkkoja ylläpitävät operaattorit, jotka toimivat palveluntarjoajina. Näitä operaattoreita ovat Telia, Elisa ja DNA. Nämä kolme suurinta toimijaa Suomessa tarjoavat yrityksille tässäkin työssä käsiteltävien MPLS:n ja SD-WANin lisäksi Ethernet-WAN-ratkaisuja, jotka soveltuvat niille yrityksille tai toimijoille, joiden tavoitteena on ylläpitää IP-verkkojaan itse. Suomeen verkkonsa hankkivilla yrityksillä on saatavilla siis mihin tahansa tarpeeseen sopiva ratkaisu, joita käsitellään tarkemmin tässä työssä.

Perinteinen yritysverkko Suomessa pohjautuu yleensä MPLS-tekniikkaan, jolla luodaan esimerkiksi konesalin- ja yritysten toimipisteiden välillä käytettävä yhteys. Kasvava tarve pilvipalveluille on kuitenkin huomattu myös Suomessa. Tämän tarpeen kasvaessa tarvitaan mahdollisesti uusia joustavampia vaihtoehtoja tukemaan nykyisiä ratkaisuja. Myös mahdollisuus käyttää yritysten palveluja missä vain, on kasvattanut tarvetta joustaville ratkaisuille. (Telia 2018.)

3 SOFTWARE-DEFINED WIDE AREA NETWORK

Software-defined wide area network (SD-WAN) on tulevaisuuden yritysverkoissa käytettävä tekniikka. SD-WAN perustuu Software-Defined Networkingiä (SDN) käytettävään tekniikkaan, jossa hyödynnetään verkkojen keskitettyä hallintaa toimipisteiden välillä ohjelmallisesti. SD-WAN yksinkertaistaa toimi-

pisteiden väliset WAN-yhteydet yhdistämällä nämä verkot yhdeksi isoksi kokonaisuudeksi, jossa keskitetyn hallinnan kautta mahdollistetaan optimoitu verkko esimerkiksi sovelluksille Internetin ja hybridilaajakaistojen yli. (What is SD-WAN 2020.)

Ohjelmallisten verkkojen perusperiaate on erottaa verkko erillisiksi ominaisuuksiksi, jossa verkon aluskerroksen päälle luodaan ohjelmallinen hallinnoitava kerros. Tuloksena on verkossa käytettävien sovellusten vähenevä tarve tietää tarkkoja tietoja verkkolaitteista. SD-WAN tuo siis ohjelmallisen eristetyn verkon päällyskerroksen, joka erottaa palvelut pohjalla olevista WAN-laitteista. Tällä verkon uudella kerroksella verkon ylläpito helpottuu IT-ammattilaisten näkökulmasta, sillä sen sijaan, että heidän tarvitsisi hallita jokaista erillistä pohjalla olevaa WAN-verkkoa erikseen, tuo SD-WAN mahdollisuuden keskitettyyn hallintaan. (Uppal, ym. 2018, 6.)

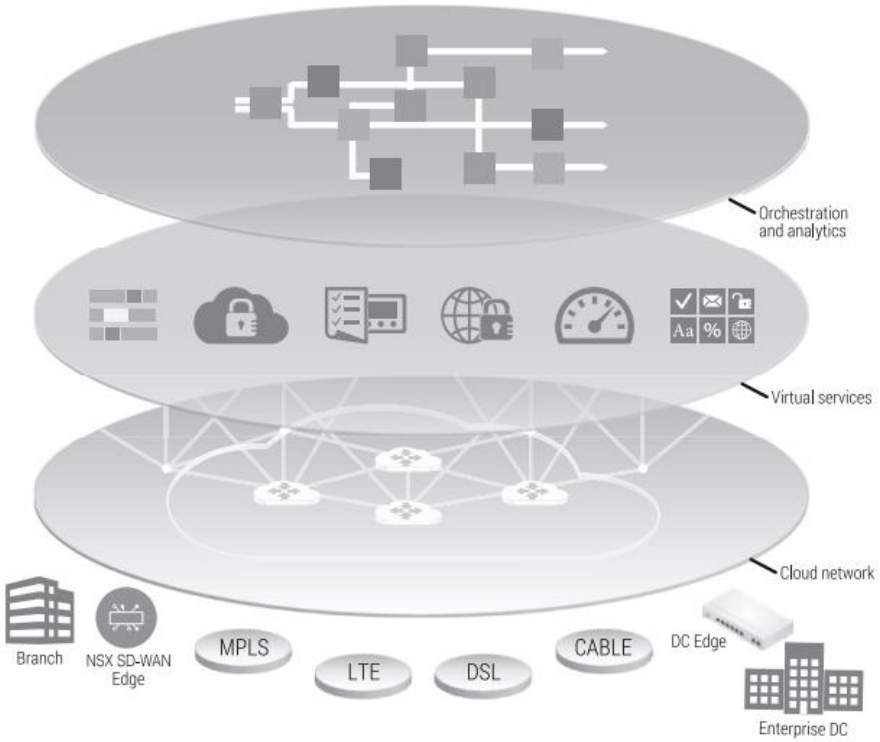
Teknologian evoluutio on muokannut liikenteen käyttöä organisaatioiden sisällä. Pelkästään kaistan käytön suuri kasvu käyttäjäkohtaisesti, esimerkiksi videokokouksissa, varaa huomattavan määrän kaistaa. Software as a service (SaaS) palvelut ovat myös suurelta osin syynä kapasiteetin, hallittavuuden ja tietoturvan tarpeen lisääntymiseen yrityksissä. Office 365 ja Salesforce ovat vain muutamia yritysten käytössä olevia sovelluksia.
(Uppal ym. 2018, 9.)

SD-WAN tarjoaa tässä tapauksessa yrityksille mahdollisuuden palveluiden siirtämiseen esimerkiksi kokonaan pilvipalveluiksi, sillä kaistan käytön rajoituksia ei ole. Yritystoiminnan jatkuva kehitys vaatii käyttöön otettavien palveluiden helpon ja nopean implementoimisen. Uusien toimipisteissä käytettävien verkkojen tai jo olemassa olevien päivittäminen SD-WAN-ratkaisuksi parantaa tietoturvan näkökulmasta yrityksen toimintaa ja mahdollistaa nopeiden muutoksien tekemisen tarpeen vaatiessa. (Uppal ym. 2018, 10.)

Tämän hetken jo käytössä olevien verkkotekniikoiden (esim. kupari, valokuitu, radioverkko) saatavuus on suurelta osin hyvä. Tämä mahdollistaa normaalin WAN-pohjaisen yhteyden käytön SD-WAN-verkkoratkaisussa.

3.1 SD-WAN-verkon rakenne

Ohjelmallinen verkko rakentuu kolmesta kerroksesta. Nämä kerrokset voivat koostua esimerkiksi MPLS, LTE(4G) tai kaapeliverkon pohjaratkaisuista. Myös 5G:n tuleminen markkinoille edistää radioteitse käytettävien ratkaisujen käyttämistä SD-WAN-ratkaisuissa.
Virtuaaliset palvelut luovat toisen kerroksen, jotka on liitetty SD-WAN-verkkoratkaisuun. Viimeisenä on näiden kaikkien yhdistävä kerros, joka koostuu analytiikasta ja SD-WAN-verkon keskitetystä hallinnasta. Kuten kuvasta 1 voidaan huomata SD-WAN koostuu näistä kolmesta kerroksesta.



Kuva 1. SD-WAN-verkon arkkitehtuuri (Uppal ym. 2018), 19)

SD-WAN keskittyy korjaaman ongelmia, joihin esimerkiksi MPLS tai normaali WAN-ratkaisu ei kykene yritysverkkomaailmassa. Näistä huomattavin on SD-WANin kyky tuoda tietoturvallista ja luotettavaa palvelua erilaisten toimipisteiden välillä, jossa käytössä voi olla esimerkiksi henkilökohtaisia, hybridi tai internet toteutuksia. SaaS-ohjelmat, kuten myös reaaliaikaista yhteistyötä vaativat projektit vaativat vikasietoisen verkkoratkaisun, jonka SD-WAN tuo dynamic path forwarding -tekniikalla. (Uppal ym. 2018, 19.)

Ennen kuin toimipisteessä sijaitseva SD-WAN-laite voi liittyä osaksi verkkoa, on sen ensin varmennettava itsensä SD-WAN-hallintakerroksen (eng. management-plane) kanssa. Tässä käytetään esimerkiksi AES-salaustekniikkaa, jonka avulla luodaan IP-SEC-tunneli minkä tahansa verkkomedian yli.

3.2 Data ja Control Plane

SD-WAN erottaa verkon kahteen tärkeään osaan, joita ovat control plane ja data plane. Nämä kaksi tärkeää ominaisuutta yhdessä luovat verkolle toimivan pohjan. Control plane ohjaa verkossa liikkuvia paketteja ja on täysin vastuussa, mihin paketit päätyvät. Ominaisuus sisältää myös järjestelmien konfiguraation ja hallinnan. Data plane taas huolehtii verkossa sovellusten ja käyttäjien tiedoista. On tärkeää ymmärtää, että yksi control planen looginen instanssi sisältää ja palvelee monia data plane -instansseja, jotka ovat yleensä reitittimiä ja kytkimiä. Normaaleissa verkoissa jokainen data plane -instanssi sisältää oman control planen, joka tekee verkon ohjelmoinnista mahdotonta. Tämä SD-WAN:in tapa erotella nämä kaksi ominaisuuta sisältää monia hyötyjä. Verkon kerrosten erottamisella on seuraavia hyötyjä (Uppal ym. 2018, 6):

- Protokolla kuten OpenFlow mahdollistaa controlin ja data planen välisen kommunikaation. Tätä protokollaa kutsutaan myös nimellä Southbound Interface (SBI). Nimi protokollalle tulee siitä, että se sijaitsee ”etelän” puolella control planesta verkkojen arkkitehtuurisessa diagrammissa.

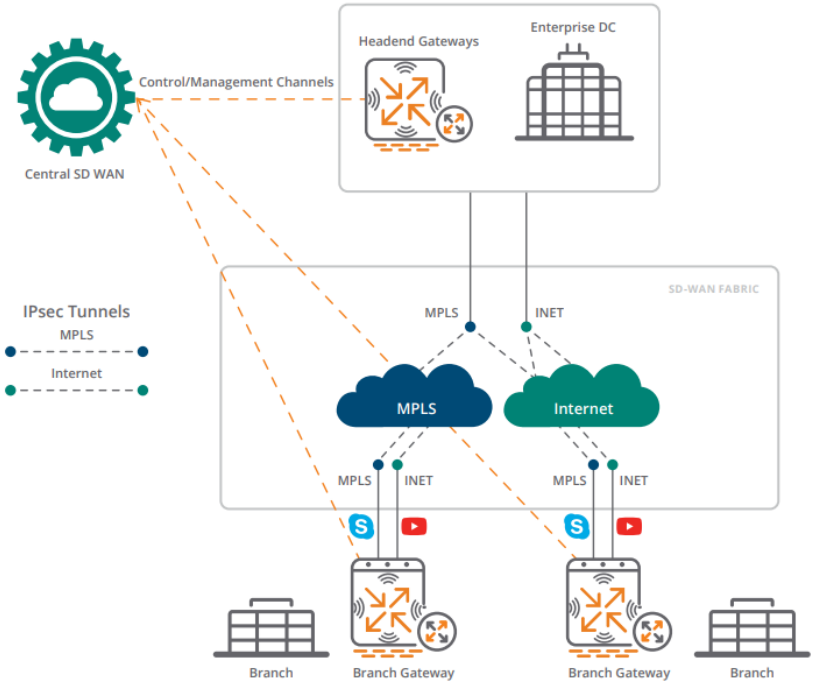
- Ohjelmointirajapinta tai API (Application-programming interface) on toinen ominaisuus, joka mahdollistaa verkon ohjelmoimisen ohjelma tasolla. Tätä kutsutaan nimellä Northbound Interface (NBI) samasta syystä kuin OpenFlow-protokollaa.

3.3 Dynamic Path Steering

DPS tai Dynamic Path Steering on laajalti käytössä oleva ratkaisu SD-WAN-pohjaisissa verkoissa, joskin tälle on toimittajasta riippuen käytössä eri nimellä samanlaisia toteutuksia. Tämä ominaisuus mahdollistaa tällä hetkellä käytössä olevien WAN-yhteyksien hallinnoimisen ja mahdollistaa hyvän näkyvyyden sille mitä verkossa tapahtuu. Lisääntynyt perinteisten Internet-liittymien käyttö yritysmaailmassa on luonut tarpeen tuoda näkyvyyttä ja mahdollisuutta

kontrolloida näissä verkoissa liikkuvaa liikennettä. (Aruba SD-WAN Dynamic Path Steering with Service Level Agreements 2019.)

DPS-ominaisuuksia ovat mahdollisuus mitata esimerkkinä kahden erillisen WAN-linkin välillä esiintyvää pakettien pudotuksia (packet loss), viivettä, viiveen vaihtelua (jitter) ja WAN-linkissä esiintyvää kuormaa. Tämä mahdollistaa WAN-linkkien valvonnan perustuen kerättyyn tietoon, jolla voidaan optimoida ja mahdollistaa hyvän tason SLA-asiakkaille (Service Level Agreement) ja sovelluksille ohjaamalla linkeissä liikkuvaa dataa älykkäästi. Ohjelmien toimivuus parantuu näin huomattavasti, sillä dataa ohjataan aina tarpeeseen sopivan yhteyden kautta.



Kuva 2. Dynamic Path Switching VoIP/Video (Aruba SD-WAN Dynamic Path Steering with Service Level Agreements 2019)

Kuvassa 2 havainnollistetaan tilannetta, jossa käytettävät palvelut ovat Voice over IP tai VoIP (Skype) ja Video (Youtube). Koska VoIP-liikenteelle on tärkeää palvelun luotettavuus, ohjataan liikenne aina parhaan mahdollisen saatavan yhteyden läpi. Tässä tilanteessa voidaan huomata, että Skype-sovelluksen liikenne ohjataan MPLS-yhteyden läpi, kun taas Youtube käyttää normaalia Internet yhteyttä. Jos MPLS-yhteydessä esiintyy esimerkiksi epävakautta, ohjaa DPS VoIP-liikenteen älykkäästi käyttäen normaalia internet-yhteyttä.

(Aruba SD-WAN Dynamic Path Steering with Service Level Agreements 2019.)

Dynamic Path Steering parantaa huomattavasti yleistä redundanssia ja WAN-ympäristön laatua. Käyttäjät verkossa hyötyvät tästä, sillä jatkuva pakettien ohjaus tasoittaa kuormaa ja ohjaa tärkeimmät, kuten esimerkiksi VoIP-liikenteen parhainta reittiä pitkin, mikäli se on määritetty DPS-asetuksissa. Käytännössä tämä tuo verkon ylläpitäjälle tarvittavat työkalut, jotta verkko voidaan optimoida asiakkaan tarpeiden mukaisesti. Ylläpitäjä voi tarkastella kerättyä dataa ja määritellä mitkä WAN-linkit sopivat parhaiten mihinkin tarkoitukseen. (Aruba SD-WAN Dynamic Path Steering with Service Level Agreements 2019.)

SD-WAN-toimipisteiden laitteet muodostavat kohteessa sijaitsevien WAN-yhteyksen yli jokaiseen oman IP-SEC-tunnelin, joiden kautta liikenne ohjataan. DPS-ominaisuus vaatii SD-WAN-Branch-laitteen dynaamisen reitinvalitsemisasetuksen käyttöön ottamista. Ylläpitäjä määrittää näiden kolmen komponentin perusteella liikenteen ohjauksesta (Configuring Policies for Dynamic Path Steering 2021):

- perinteinen liikenteen ohjaus listaus
- Service Level Agreement (SLA), ja niille määritetyt rajat
- optimaalisten WAN-linkkien määrittäminen.

Fortinet tutki tämän ominaisuuden vaikutusta omassa ratkaisussaan, jossa Fortinet adoptoi omassa yritysverkossaan käyttöönsä Fortinet Secure SD-WAN ratkaisun. Uusien toimipisteiden liittäminen verkkoon paransi verkon laatua noin 80 % sekä nopeutti verkon konfigurointia käyttöä varten. Automaattisella verkon ohjauksella applikaatiotasolla on huomattava vaikutus verkon yleiseen laatuun, sillä yleisesti esimerkiksi normaalit 4G:tä käyttävät WAN-toteutukset, eivät takaa luotettavinta tiedonsiirtotietä. (Fortinet Optimizes Network Performance With Secure SD-WAN 2020.)

3.4 SD-WAN Tietoturva

Suurin haaste perinteisille SD-WAN-toimittajille on riittämätön tietoturva palveluille, joita ovat esimerkiksi pilvi- ja SaaS-ratkaisut. SD-WAN-kehitys on alun perin pohjautunut täysin verkkotekniseen kehitykseen, mutta tulevaisuuden suunta on ennustettu menevän vahvasti tietoturvapainotteisiin ratkaisuihin. SD-WAN-ratkaisujen tapana on suojata verkon liikennettä Layer-3-verkkokerroksen tasolla, ja ne eivät usein tue Layer 4–7 tason hallittavuutta, joka on vaatimuksena luotettaviin ratkaisuihin. (Secure SD-WAN: Integrated NGFW Security with WAN Transformation 2017.)

Yleisesti käytössä on SD-WAN ratkaisuihin sisällytettyjä tietoturvaratkaisuja, hoWAN-yhteyden päällä. Turvallisen yhteyden luomiseksi suositellaan käytettävän Secure Web Gateway (SWG)- tai Next Generation Firewall (NGFW) -ratkaisuja suojaamaan käytettävää SD-WANia. (Secure SD-WAN: Integrated NGFW Security with WAN Transformation 2017.)

Perinteinen SD-WAN voi sisältää Stateful-tyylisen palomuurin, jossa suojaus luodaan käyttämällä sääntöpohjaista (Policy based) suodatusta ja sovellusten liikenteen estämistä IP-osoitteita käyttäen. Tämän kaltaiset ratkaisut tuovat suojaa perinteiselle SaaS-ratkaisulle, jossa yhteys luodaan vain kohteen ja pilvipalvelun välille. Mikäli yritys vaatii pääsyn laajempaan internetin tarjontaan, on hyvä käyttää edellä mainittuja Layer 4–7 kerroksissa löytyviä ratkaisuja, kuten NGFW. (The 4 SD-WAN architectures for network security 2017.)

Yleinen SD-WAN toimittajien käytössä oleva termi ”Secure SD-WAN” merkitsee vain liikenteen suojaamista esimerkiksi IP-sec-tunneloidulla yhteydellä, jossa liikkuva data salataan AES-256-salausmetodia käyttäen. Hyvin suojattu verkko tarvitsee yritykseltä kokonaisvaltaisen kartoituksen, jossa otetaan huomioon muut verkon ulkopuoliset uhat. Näitä uhkia ovat ulkopuolisten yhteys/murtautumisyritysten estot, malware-tartunnat ja muut kehittyneet kyberuhat. (Complete guide to SD-WAN 2018.)

SD-WAN-ratkaisujen tulisi ideaalitilanteessa sisältää esimerkiksi NGFW-ratkaisu jo sisäänrakennettuna. Ohjelmalliset WAN-ratkaisut, jotka sisältävät

Next Generation Firewall -ominaisuudet sisään rakennettuna, ovat esimerkiksi Fortinet, Barracuda, sekä Cisco Meraki. Huomattavia ominaisuuksia NGFW SD-WAN -ratkaisuissa ovat:

- SSL Inspection, jossa esimerkiksi palomuuri purkaa HTTPS-paketin, jotta sitä voidaan tutkia ennen sen siirtymistä sisäverkkoon.
- IPS tai Instrusion Prevention System toimii tavalla, jossa järjestelmän älykkyys pystyy tunnistamaan tiedossa olevat sekä ei aikaisemmin havaitsemattomat uhat.
- Antivirus, joka ajantasaisella tietokannalla pystyy torjumaan mahdolliset haitalliset virustartunnat.

SD-WAN-toteutuksista voidaan myös käyttää hyväksi mahdollisuutta korvata normaalit WAN-reitittimet toimittajien omilla reitittimillä, joissa on sisäänrakennettu tietoturvaratkaisu. Tämä parantaa toimipisteiden, päätoimipisteiden ja etäisten kohteiden tietoturvaa tavalla, jossa kaikilla kohteilla on yhteinen ja salattu tapa kommunikoida julkisen Internetin yli. Liikenteen salaaminen ja segmentointi perustuen tietoon käyttäjästä ja laiteryhmästä mahdollistaa julkisen verkon yli kulkevan tiedon perille pääsyn koskemattomana. (Gartner 2019.)

4 MULTI PROTOCOL LABEL SWITCHING

Multi Protocol Label Switching tai MPLS on tietoverkoissa käytettävä tekniikka, joka mahdollistaa pakettien nopean ja tietoturvallisen kuljetuksen erilaisten käytössä olevien verkkomediaanien yli. Esimerkkinä voidaan ajatella MPLS-tekniikkaa vastaavana maailman postiyritysten käyttämään postin priorisointiin, jossa paketit voidaan jakaa tietynlaiseen tärkeysjärjestykseen. Paketit saavat MPLS-verkossa liikkuessaan leiman, joka määrittää mihin paketti liikkuu verkon eri reitittimien välillä, sekä määrittää paketin tärkeyden siirtotiellä. Reitittimet päättävät nämä rakentamalla lajittelukenttiä ja tietokantoja, jolloin paketeille on aina tiedossa mahdollinen reitti verkon läpi.

Perinteisessä IP-verkossa pakettien lajittelua ei ole ja näin ollen niiden kuljetuksessa käytetään parasta saatavilla olevaa reittiä (eng. Best effort route), jossa jokainen reititin tekee oman päätöksensä siitä, mihin paketti tulisi ohjata.

Reitittimet tarkastelevat IP-paketin otsaketta (header), minkä jälkeen reititysalgoritmi vertaa kohdeosoitetta ja tekee päätöksen siitä, mille reitittimelle seuraava hyppy (next hop) suuntautuu. Next hop on reitittimien itsensä päätettävissä. Päätös perustuu paketin kehyksessä oleviin tietoihin, sekä käytettyyn reititysprotokollaan. (DeGeest 2001.)

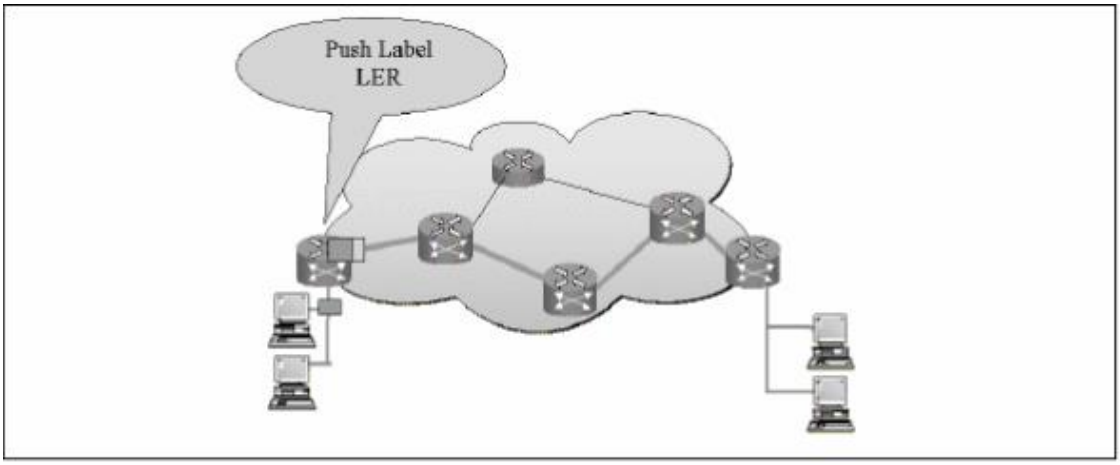
4.1 MPLS FEC

MPLS-verkoissa pakettien verkon otsake tarkistetaan vain kerran, ja tämä tapahtuu vain silloin, kun paketti siirtyy MPLS-verkkoon. Forwarding Equivalence Class (FEC) lisätään pakettiin samalla tavalla kuin normaaleissa IP-verkoissa, mutta tässä tapauksessa jokaisella FEC:lla on oma MPLS-leimansa (Label). FEC on MPLS-verkon keskeinen konsepti, jonka ymmärtäminen on tärkeä osa MPLS-verkon osaamista. Kun MPLS-reitittimet, joita kutsutaan label switch router -nimellä (LSR) tulevat osaksi MPLS-verkkoa, ne rakentavat itselleen tietokentän, josta selviää, mihin leimaan FEC kuuluu. Jokaisella FEC:llä on tiedossa oma seuraava pisteensä (Next hop). (DeGeest 2001.)

Verkossa vierekkäin olevien MPLS-reitittimien (LSR) välillä käytetään leimojen tiedon välittämiseen LDP:tä (label distribution protocol). MPLS:ia varten on kehitetty lisäominaisuuksia, jotta LDP:tä voidaan ajaa verkossa käytettävien reititysprotokollien päällä. Paketin kulkiessa MPLS-verkossa reitittimien välillä, ei ensimmäisen kerran jälkeen tehtyä otsakkeen tarkistusta enää tehdä, vaan MPLS-leimoja käytetään määrittämään mihin paketti ohjataan seuraavaksi. MPLS forwarding -termiä käytetään, kun paketti on saanut FEC-ohjauksen, jonka jälkeen jäljellä olevat reitittimet eivät tee otsakeanalyyseja paketeille. Tämä tarkoittaa sitä, että leimat määräävät kaikki tehtävät reitityspäätökset. (DeGeest 2001.)

4.2 MPLS-verkon rakenne

Ensimmäistä reititintä MPLS-verkossa kutsutaan nimellä label edge router (LER), jonka tehtävä on suorittaa pakettien muuntaminen IP-paketeista MPLS-paketeiksi ja toisinpäin (Gallaher 2004, 3).

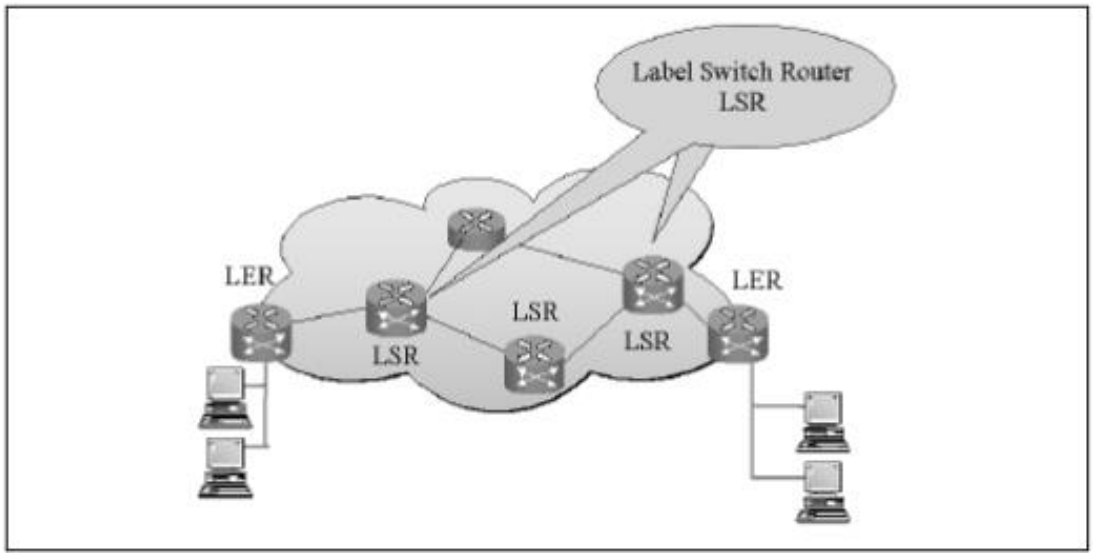


Kuva 3. Label Edge Router IP-verkossa (Gallaher 2004, 3)

Esimerkkinä kuvassa 2 LER etsii, löytyykö sen tietokannasta paketin saajan IP-osoitetta, ja lisää siihen sille osoitetun MPLS-tiivistekehyksen (frame). Kun paketti siirtyy label edge routerilta MPLS-verkkoon, sen seuraava piste on label switch router (LSR), joka on mikä tahansa MPLS-leimoja käsittelemään kykenevä reititin. Leimojen käsittelyyn liittyviä toimenpiteitä ovat PUSH, POP ja SWAP. PUSH-operaatio lisää uuden leiman kehykseen, POP poistaa leiman kehyksestä esimerkiksi silloin, kun paketti poistuu MPLS-verkosta, ja SWAP vaihtaa leiman. (Gallaher 2004, 3.)

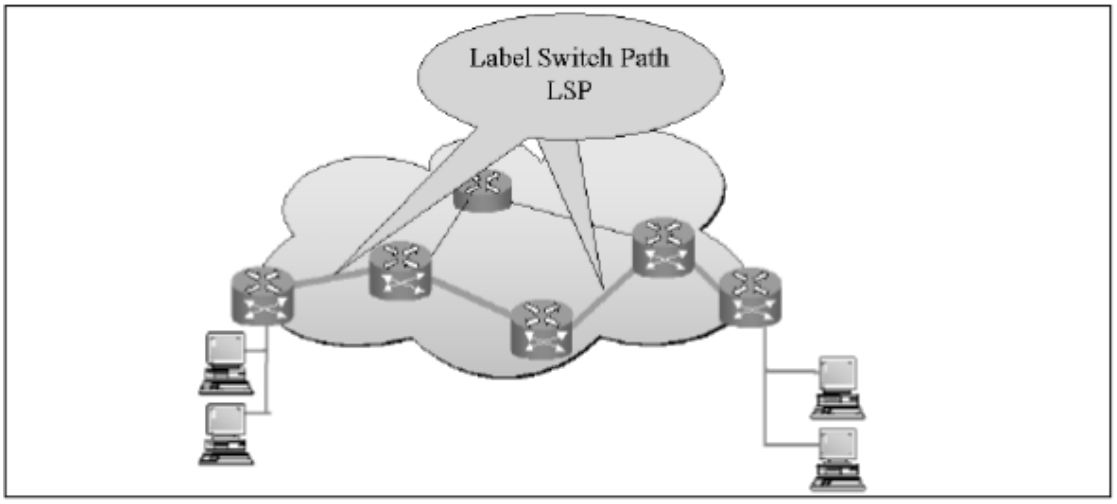
MPLS-verkossa tapahtuvan liikenteen reitittämisen vastuuta hoitavat LSR-reitittimet, jotka ottavat hoitaakseen verkossa tapahtuvien pakettien ohjauksen sen jälkeen, kun LER-reititin on liittänyt MPLS-leiman pakettiin. Huomionarvoista on käsitellä näitä silti vain normaaleina reitittiminä, sillä pakettien analysointi määrittää sen, toimivatko ne LSR-laitteina vai reitittiminä. (Gallaher 2004, 4.)

LSR:n tarkoituksena on analysoida sille tulevat paketit, ja mikäli paketti sisältää MPLS-leiman, LSR tarkistaa ja seuraa sen leimassa näkyviä reittitietoja, jonka perusteella se lähettää paketin eteenpäin seuraavalle reitittimelle. Yleisesti LSR tehtävänä on siis suorittaa leimalle SWAP toiminto, jossa kuten aikaisemmin on mainittu, reititin vaihtaa leiman uuteen. Kuvassa 3 havainnollistetaan MPLS-verkossa esiintyvät LSR-laitteet.



Kuva 4. Label Switching Router (Gallaher 2004, 5)

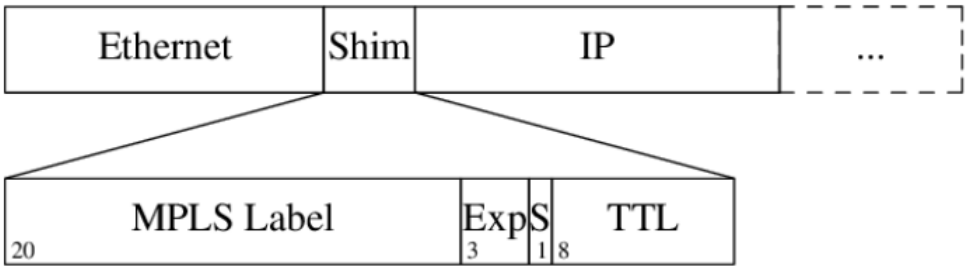
LER-reitittimen ja LSR:n välistä reittiä kutsutaan nimellä label switch paths tai LSP. Nämä reitit on suunniteltu hyvin samalla tavalla kuin ATM-verkoissa käytettävä tekniikka reittivalintoja varten. Liikenteen käsittelyn kapasiteetti lasketaan jokaiselle LSP-linkille erikseen. Nämä voivat sisältää esimerkiksi dataa maksimikuormasta linkissä, pakettien välisiä eroja ja siirron välillä tippuneiden pakettien prosentuaalista määrää verrattuna kaikkiin siirrettyihin paketteihin. Kuten kuvasta 4 voidaan huomata, LSP:t rakennetaan osaksi MPLS-verkkoa laitteiden väliin, koska MPLS toimii kerroksena (eng. overlay) IP-protokollalle voivat kumpikin toimia samassa verkossa ilman, että ne häiritsevät toisiaan. (Gallaher 2004, 5.)



Kuva 5. Label Switch Paths (Gallaher 2004, 5)

4.3 MPLS-otsake

MPLS-verkon läpi kulkevan datan on mahdollista sisältää yksi tai useampi MPLS-otsake, jotta sen reititys verkon läpi onnistuisi. Tämän rakenne voidaan havainnollistaa kuvasta 5, jossa MPLS-otsake sisältää MPLS-leiman. Tämä leima koostuu 20 bitistä, jotka määrittävät reitityssäännöt paketille. Loput yhteensä 32 bitistä sisältävät Traffic Class (TC) kentän (3 bittiä), bottom of stack bitin (1 bitti) ja Time-to-live (TTL) kentän, joka on 8 bitin kokoinen. (Minei & Lucek 2011, 6.)



Kuva 6. MPLS header (Thimmaraju ym. 2016.)

Kuvasta 6 voidaan myös huomata Open Systems Interconnectionin kerroksen (OSI) eri osia. Ethernet-osa paketista on Layer 2:ta edustava osa, kun taas IP-osa koostuu Layer 2- ja Layer 3 -kerroksista. Kun IP-paketti saapuu LER-reitittimelle, lisätään siihen kuvassa 5 esitettävä tiivistekehys (Shim) Ethernetin (Layer 2) ja IP (Layer 3) väliin. Vaikka kyseinen tiiviste ei kuulu Layer 2- tai Layer 3 -kerroksiin, on sen tehtävänä silti välittää näiden kerrosten välillä tietoa. (Gallaher 2004, 4.)

On tapauksia, joissa yksi MPLS-otsake riittää toimittamaan paketti oikeaan paikkaan esim. julkisen IP-liikenteen kuljettaminen. Tilanteessa, jossa paketti saapuu LER-laitteelle, suorittaa se normaalin IP:n tarkastelun määrittääkseen mihin linkkiin paketti ohjataan. Yleensä MPLS-verkoissa käytetään Penultimate Hop Popping tai PHP:ta. PHP-ominaisuus yksinkertaistaa MPLS-verkon rajalla olevan LER-laitteen kuormaa tavalla, jossa verkossa ennen LER-laitetta sijaitseva LSR-laite tekee POP-operaation paketille. Tämän jälkeen LSR ohjaa paketin normaalina IP-pakettina LER-reitittimelle, jolloin tämän ei tar-

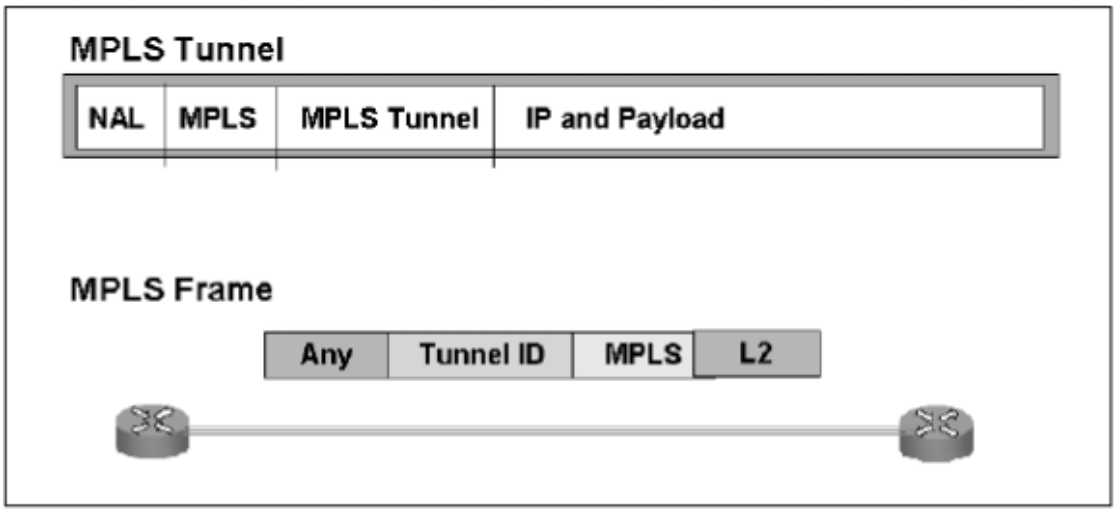
vitse POP-operaatiota tai paketin analysointia. Tämä operaatio ei ole pakollinen, mutta se on implementoitu useimmissa ratkaisuissa. (Minei, Lucek 2011, 8.)

Normaaleissa tapauksissa yksi MPLS-otsake ei riitä, vaan paketilla on oltava kaksi otsaketta tai enemmän, jotta verkko toimisi oikein. Tämä johtuu usein siitä, että kyseinen verkko voi sisältää monenlaisia palveluita. Esimerkkejä näistä palveluista ovat Layer-3 VPN, Layer-2 VPN, VPLS (virtual private LAN service).
LER siis tarvitsee enemmän kuin yhden otsakkeen, jotta se pystyy määrittelemään mihin palveluun ja instanssiin (esimerkiksi eri asiakkaan) paketti kuuluu.

4.4 MPLS Virtual Private Network

Virtual Private Network, tai VPN, on verkko, joka muistuttaa ominaisuuksiltaan normaalia sisäverkkoa, mutta sen sijaan se toimii julkisessa verkossa. VPN estää julkisessa verkossa datan erilaisen tarkastelun ja muokkaamisen, sekä denial of service -hyökkäykset (DoS). Turvallisen VPN-yhteyden luomiseksi tarvitaan ohjelma, joka kykenee luomaan turvallisen salatun tunneloidun yhteyden kahden eri kohteen välille.

VPN-yhteyksien toteutukseen on olemassa erilaisia vaihtoehtoja myös ilman salausta. Esimerkkejä erilaisista VPN-tunneleista ovat Generic Routing Encapsulation tai GRE, IP to IP (IP-IP), IP Security (IPSec), Layer-2 Tunnel Protocol (L2PT) ja MPLS. (Gallaher 2004, 144–145.)



Kuva 7. MPLS Tunnel (Gallaher 2004, 148.)

MPLS-tunneleita voidaan käyttää yhdessä edellä mainittujen tunnelointitekniikoiden kanssa. Suurelta osin käytössä ovat MPLS ja GRE. MPLS:ää itsessään voidaan kutsua siis tunnelointitekniikaksi, joka mahdollistaa end to end - ja edge to edge -ratkaisuiden toteuttamisen. Kuva 7 havainnollistaa MPLS end to end -tunnelin rakenteen.

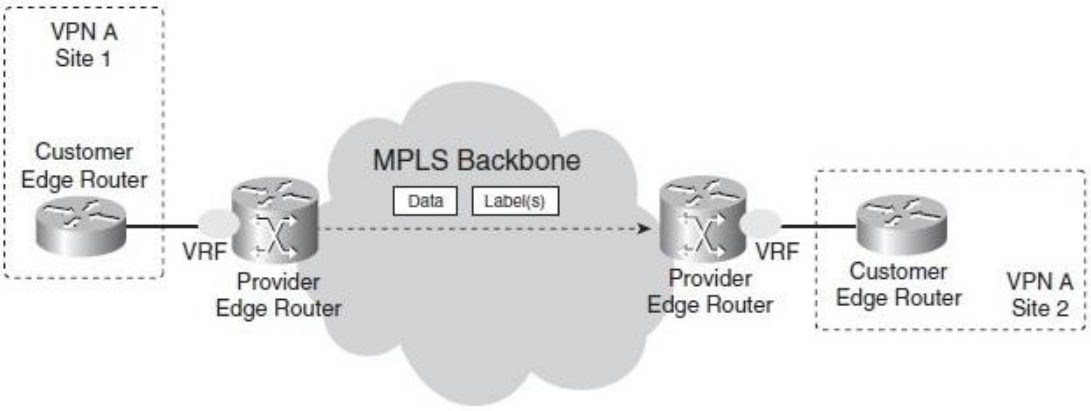
MPLS-verkkojen yleistymisen myötä, MPLS VPN-ratkaisut yleistyivät ja oli selvää, että ne pystyivät tarjoamaan joustavan ratkaisun esimerkiksi operaattoreille. Tämän ratkaisun mahdollistamiseksi kehitettiin Layer-3 MPLS VPN. (Gallaher 2004, 154.)

MPLS Layer 3 VPN reititys tapahtuu palveluntarjoajan reitittimillä, jossa kyseiset reitittimet hoitavat tunneloidun liikenteen ohjausta transit-verkon sisään ja ulos pisteissä. Nämä voivat esimerkiksi olla operaattorien runkoverkkoja. Palveluntarjoajan verkko vastaa IP-osoitteiden oppimisesta niille laitteille, jotka lähettävät liikennettä VPN-tunneloidun yhteyden yli. Tässä ratkaisussa verkon reititystiedot on mainostettava ja suodatettava palveluntarjoajan verkossa. Tämä aiheuttaa sen, että Layer-3 VPN:t tarvitsevat tietoa asiakkaan verkon reitityksen reittitiedoista. Ratkaisu vaatii myös kattavamman virtual routing and forwarding (VRF) -määrityksen konfiguroinnin, kun tätä verrataan Layer-2 VPN-ratkaisuun. Tätä tietoa käytetään jakamiseen ja suodatukseen reiteillä, jotka ovat peräisin VPN:stä tai päättyvät VPN:n sisällä. (MPLS VPN Overview 2019.)

Provider Edge (PE) reititin on nimensä mukaan palveluntarjoajan ja loppuasiakkaan rajalla oleva laite, joka vastaa reititystietojen ja asiakkaan pään liikenteen ohjauksesta. Tämä laite tarvitsee paljon prosessointikapasiteettia sillä reititystietojen ja liikenteen ohjauksesta aiheutuva kuormitus johtuu suurelta osin Layer-3 VPN suurista reititystietokentistä. (MPLS VPN Overview 2019.)

4.5 MPLS VPN virtual routing forwarding

Tämä ratkaisu on yleisesti palveluntarjoajien käytössä oleva, sillä se mahdollistaa hyvin yksityistetyn MPLS VPN ratkaisun implementoinnin. Tässä konseptissa virtual routing forwarding (VRF) erottaa esimerkiksi eri asiakkaiden reititystiedon toisistaan ja MPLS runkoverkko hoitaa leimojen avulla pakettien ohjauksen. Esimerkiksi normaalissa peer-to-peer-tyyppisessä VPN-ratkaisussa paketit ohjataan runkoverkossa käyttämällä paketista löytyvää IP-otsaketta (IP-header). (Peer to Peer VPN overlay 2019.)



Kuva 8 MPLS VPN operaattoriverkoissa (Tutorzine 2019)

Kuvassa 8 havainnollistetaan, miten yleinen MPLS VPN-ratkaisu toteutetaan operaattoriverkoissa. Ratkaisusta hyödytään monella tapaa, sillä yhden asiakkaan toimipisteen lisääminen ei vaadi kuin normaalin BGP-peering konfiguraation lisäämisen palveluntarjoajan reitittimen (PE) ja asiakkaan reuna reitittimen (CE tai Customer Edge) väliin.

Operaattoreiden transit-verkko on konfiguroitu tukemaan monia VPN-instansseja samanaikaisesti, jolloin myös nämä voivat sisältää monia VRF-instansseja. Tämä voi aiheuttaa sen, että yleisesti käytettävä BGP-protokollan reitti tiedot voivat sisältää monia samanlaisia reittejä saman kohdeosoitteeseen. BGP tarvitsee keinon erottaa mahdolliset samanlaisuudet verkon kerrosten

saatavuustietoviesteistä (eng. network layer reachability information tai NLRI), jotka eri VPN-instanssit lähettävät. (Juniper Networks 2019.)

4.5.1 BGP Route Distinguisher ja Route Target

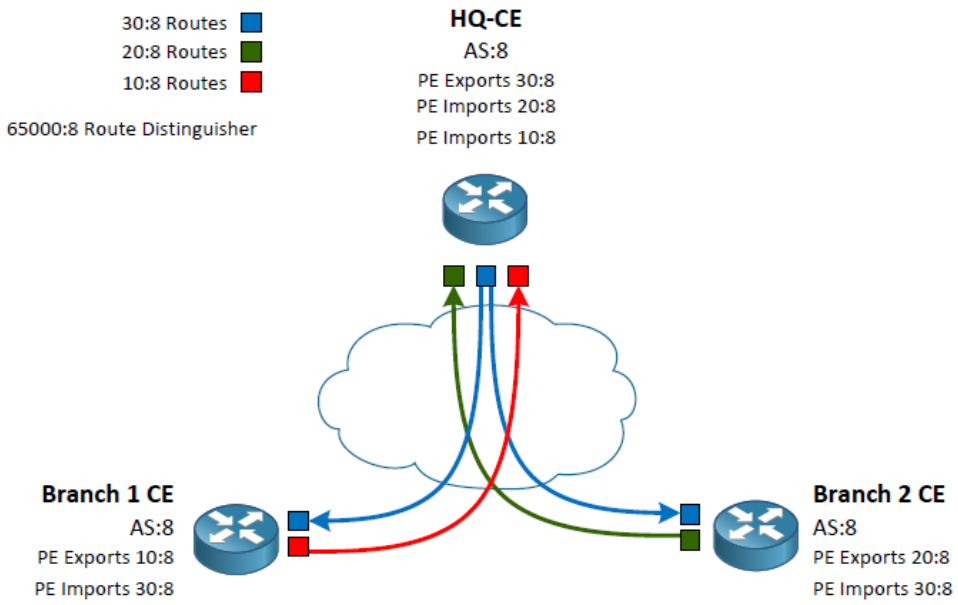
Route Distinguisher (RD) on paikallisesti uniikki numero, jolla tunnistetaan mihin VPN-instansseihin tiedot kuuluvat. Tämä mahdollistaa ongelman poissulkemisen, jossa verkosta löytyy identtisiä BGP reittejä. PE-reititin sisältää jokaiselle reittiinstanssille uniikin RD:n kahdenlaisessa eri formaatissa.

- Ensimmäinen vaihtoehto on käyttää RD:n tunnisteena autonomous system (AS) -numeroa, joka voi olla välillä 1-65535.
- Toinen vaihtoehto, joka on yleisemmin käytössä, on normaali IP-osoite, joka yleisesti on RD:n virkaa hoitavan reitittimen router-id-tunniste.

Yksi tärkeistä osista tässä kokonaisuudessa on ymmärtää myös ero Route Distinguisherin ja route-targetin välillä. Route-target muistuttaa ja voi olla samankaltainen, kuin RD, vaikka niiden tarkoitus on silti täysin erilainen. Kuten aiemmin mainittu, RD on uniikki numero MPLS verkossa, kun taas route target määrää, mitkä prefix-määritykset tuodaan ja lähetetään PE reitittimille. (Roger Perkin 2013.)

PE-reititin lähettää määritykset CE-laitteille, jotka ovat yhdistyneenä suoraan PE-reitittimiin. Asiakkaan puolen reititin (CE) kättelee VRF läpi käyttäen eBGP:tä (external BGP), ja VRF konfiguraatio PE-reitittimellä merkitsee tälle route-targetit lähetettäväksi. (Route-Targets Explained 2015.)

Kuvassa 9 havainnollistetaan yksinkertaista ratkaisua, jossa päätoimipisteen (HQ) CE-reitittimen route-target konfiguraatio sisältää määritykset, ja jossa vain sen omat reitit näkyvät toimipisteiden välillä. Tämä ratkaisu konfiguraatiossa estää toimipisteitä näkemästä toisiansa (paitsi HQ), jolloin voidaan esimerkiksi erotella toisistaan riippumattomat yrityksen haarat.



Kuva 9. Route-targets (Packet Pilot 2015)

Tarkemmin tarkasteltuna tämän konseptin ymmärtäminen on helpompaa, kun ymmärretään Route Distinguisherin rooli. RD ei määrää, mitkä reitit reititin sisällyttää tai lähettää eBGP-reititys prosessiin PE-CE-reitittimien välille. RD:n tehtävänä on lisätä kerros prefixeille, joka mahdollistaa aiemmin mainittujen-päällekkäisten osoitteiden olemassaolon. Kuvassa 9 oleva RD 65000:8 sisällyttää kaikkien esimerkiksi asiakkaan VRF-instanssissa sijaitsevat reitit. Mikäli verkossa löytyy samoja reittejä, joilla on sama IP-osoite, mutta niillä on eri RD, mahdollistaa se niiden olemassaolon samanaikaisesti. (Packet Pilot 2015.)

4.5.2 Multiprotocol BGP

Multiprotocol BGP tai MP-BGP on perinteisen BGP-protokollan kehittyneempi versio. Perinteisesti palveluntarjoajat käyttävät BGP:tä IPv4-reititystietojen vaihtamiseen asiakkaiden CPE-laitteiden välillä. Moderni BGP on erittäin joustava ja kykenevä käsittelemään paljon enemmän, kuin normaalia IP-liikennettä. Tätä kyvykkyyttä kutsutaan Multiprotocol BGP nimellä, jolle on olemassa standardi RFC 4760. Tämä standardi sisältää tiedot BGP-protokollaan lisätyistä ominaisuuksista. MP-BGP:n vahvuuteena on kyky kuljettaa useita eri osoiteperheitä samanaikaisesti. Esimerkkinä IPv4, IPv6 Multicast ja Unicast, sekä L2VPN tietoa. (Network Direction 2021.)

4.6 MPLS Tietoturva

MPLS-verkoissa tietoturvaa ei ole otettu alusta asti huomioon, ennen viimevuosina esille otettua tarvetta parantaa yleistä tietoturvaa julkisissa verkoissa. MPLS tietoturvaa pidetään verrannollisena yleiseen VPN ratkaisuun. Isoin ongelma näissä verkoissa, on tiedon kulkeminen koskemattomana, hyvin säilytettynä, sekä alkuperän varmennuksella. Tämä tarkoittaa käytännössä sitä, että MPLS verkoissa siirrettävällä tiedolla on riski joutua luetuksi tai tieto voi korruptoitua matkalla kohteeseen. Tiedonsiirrolla MPLS-runkoverkossa asiakas luottaa täysin palveluntarjoajan lupaukseen pitää verkossa siirrettävä tieto koskemattomana, vaikka palveluntarjoajalla on mahdollisuus teoriassa tutkia kaikkea siirrettävää dataa. MPLS verkkoa käyttävä asiakas voi myös käyttää esimerkiksi IPSEC tunnelointia salatakseen yhteyden MPLS-verkon yli. (Alouneh, Abed 2010, 134.)

Koskemattomuudella voidaan MPLS-verkoissa viitata useaan eri osa-alueeseen. Näitä ovat esimerkiksi Label Information Base (LIB) koskemattomuus ja yleinen liikenteen koskemattomuus MPLS tiedonsiirtotiellä. LIB-tietokanta sisältää MPLS-runkoverkossa käytettävien leimojen tiedot. Mikäli kyseiseen MPLS-verkon kannalta tärkeään tietokantaan kohdistuu hyökkäys verkon ulkopuolelta, voi se mahdollisesti aiheuttaa koko verkon toimimattomuuden. Tämä voi tapahtua tilanteessa, jossa LSR hyväksyy runkoverkon ulkopuolisten isäntien leimapaketteja. LIB-listaukseen kohdistuva hyökkäys voi esimerkiksi täyttää koko tietokannan väärällä tiedolla verkossa sijaitsevista leimoista. Tämän vuoksi MPLS-ratkaisussa ei tule sallia ulkopuolisten pääsyä runkoverkkoon tietoturvariskien vuoksi. MPLS-VPN ratkaisussa liikenteelle ei siis luoda minkäänlaista salausta, jolloin asiakas ei voi olla varma lähettämänsä tiedon koskemattomuudesta. Tekniikka kehitettiin mahdollistamaan nopein mahdollinen pakettien siirto verkossa, joka on pääsyynä siihen, miksi MPLS ei sisällä minkäänlaista tietoturvan näkökulmasta kehitettyä ominaisuutta. Yleisen tietoturvan parantaminen vaatisi runkoverkon reitittimiltä paketin otsakkeiden salauksen prosessointia, joka itsessään hidastaisi MPLS-verkon toimintaa. (Alouneh & Abed 2010, 136.)

Toinen tärkeä osa tietoturvaa on kuljetettavan tiedon eheys. Tämä mahdollistetaan MPLS-verkossa tavalla, jossa aiemmin mainittu LIB-tietokanta sisältää liikenteen ohjaukseen käytettävät tiedot. Näiden tietojen, kuten esimerkiksi LDP:n on oltava luotettavista lähteistä. Sääntöjen toteutumiseksi on olemassa kaksi hyvää sääntöä, jotka parantavat MPLS-verkon eheyttä. Esimerkkinä LDP päivitystietoja ei tulisi sallia rajapinnoista (interface), mikäli takana ei sijaitse toista LSR laitetta. MPLS-runkoverkossa voi esiintyä tapauksia, joissa runkoverkon laitteeseen tai laitteisiin ei luoteta tai ne on todettu haavoittuviksi. Näissä tilanteissa verkkoon tulee lisätä todentamismekanismi. (Alouneh & Abed 2010, 136.)

Mikäli runkoverkon eheys ei ole taattu, sen saatavuus, joka on yksi tärkeä osa minkä tahansa verkon toimivuutta voi myös vaarantua. Saatavuus voi esimerkkinä edellä mainitulla tavalla vaarantua, jos ulkoinen taho onnistuu lähettämään runkoverkkoon virheellistä tietoa sisältäviä LDP-päivityksiä. Nämä haitalliset päivitykset voivat aiheuttaa liikenteen ohjautumista väärään osoitteeseen. Tämän vuoksi mitkä tahansa verkossa liikkuvat päivitykset tulisi sallia vain luotetuilta tahoilta. (Alouneh & Abed 2010, 137.)

5 SD-WAN JA MPLS YRITYSVERKOISSA

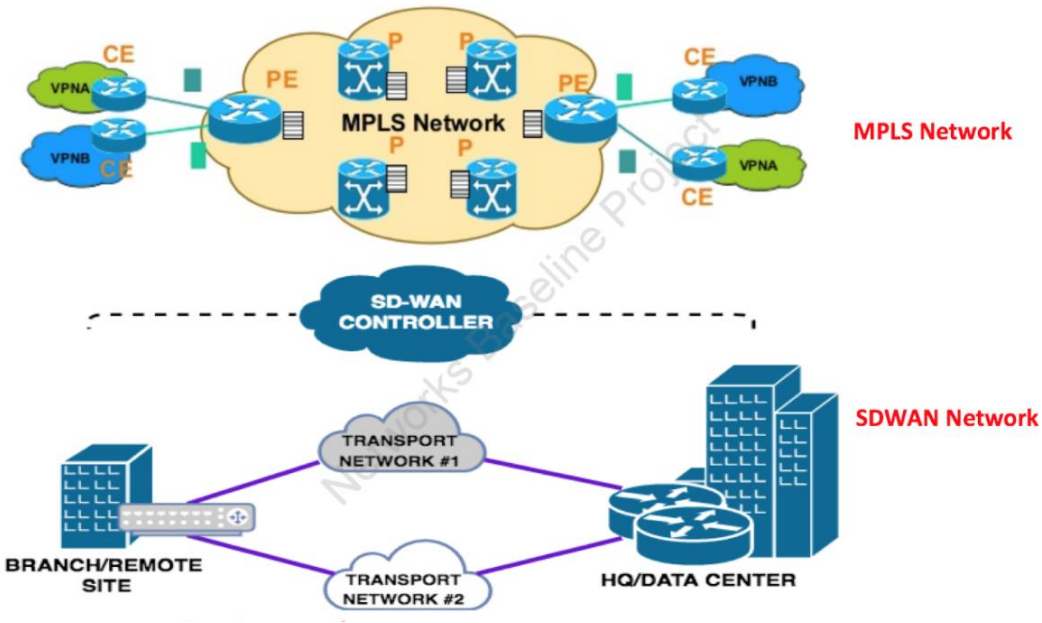
Tutkimuksen käytännön osassa keskitytään tutkimaan teoriaosassa käsiteltyjen ratkaisujen kokonaisvaltaista hyötyä yrityksille, sekä onko SD-WAN mahdollinen korvaaja perinteiselle MPLS-pohjaiselle ratkaisulle Suomessa toimiville yrityksille. Tutkimuksen alussa kerättiin tarvittavat tekniset, sekä yleistä käyttötapaa koskevat tiedot, jotka auttoivat tutkimuksen edetessä määrittelemään, minkälainen suunta Suomessa käytettävillä yritysverkoilla on tekniikkatoteutuksen osalta. Seuraavassa vaiheessa tutkitaan teoriassa yritysten näkökulmasta näiden tekniikoiden implementoimista kokonaan uutena rakenneituihin ratkaisuihin. Tämän vaiheen tavoitteena on keskittyä vastaamaan kysymykseen, onko yritysten kannattavaa rakentaa SD-WAN-pohjainen ratkaisu vai valita ratkaisuksi MPLS-verkko sekä ottaa huomioon kulut, joita tämä ai-

heuttaa. Käytännön tutkimuksen vaiheet tulevat yhdessä vastaamaan kysymykseen, onko paljon puhuttu SD-WAN tekniikkana kannattava ratkaisu, ja voisiko se korvata perinteiset MPLS-ratkaisut.

Tutkimus perustuu kerättyyn tietoon kirjallisista lähteistä, jotka pohjautuvat SD-WAN tapauksessa erityisesti markkinoita johtaviin laitetoimittajiin. Ohjelmallisten verkkojen osalta teknisen tiedon kerääminen on huomattavan hankalaa, sillä SD-WAN-toteutuksia on monenlaisia sekä tekniikka on huomattavasti uudempaa. Tämä hankaloittaa esimerkiksi kirjoista löytyvän tiedon määrää. MPLS-verkoista kerätty tieto on yleisesti saatavilla olevaa tietoa, jossa käytetään Internet Engineering Task Forcen (IETF), sille antamaa standardia RFC 3031.

5.1 Erot tekniikoissa

Teoriaosassa käsiteltyjä SD-WAN- ja MPLS-verkkoja vertailtaessa tulisi ottaa huomioon se, että nämä kaksi tekniikkaa ovat hyvin erilaisia toisistaan, eivätkä ne ole suoraan teknisesti vertailtavissa. MPLS-verkkoa kutsutaan yleisesti yksityiseksi yhteydeksi (eng. private connection), joka muodostetaan yleisesti datakeskusten ja toimipisteiden välille. Tätä voidaan siis ajatella hyvin samanlaisena ratkaisuna, kuin normaalia VPN-yhteyttä, mutta ilman minkäänlaista erityistä salausta. MPLS on myös alusverkkona (underlay) toimiva tekniikka erottaen sen SD-WAN-tekniikasta, joka toimii päällysverkkona (overlay). SD-WAN ratkaisu vaatii siis toimiakseen pohjalle aina verkon pohjakerroksen (esim. Internet). Käytännössä tämä tarkoittaa sitä, että MPLS voi toimia ohjelmallisen verkon pohjana ratkaisua luotaessa. Esimerkkinä yritys voi tarvittaessa ottaa käyttöön SD-WAN-ratkaisun, jossa se hyödyntää, jo olemassa olevaa MPLS-ratkaisua.



Kuva 10. SD-WAN vs. MPLS (MPLS vs SD-WAN: Which suits your organization 2020.)

Kuva 10 havainnollistaa hyvin, kuinka MPLS-verkko on oma pohjansa verkolle, kun taas SD-WAN tarvitsee esimerkiksi MPLS:n tai Internet-pohjaker-roksen (kuvassa Transport Network 1/2).

Hallittavuus on myös iso ero MPLS-verkkojen ja ohjelmallisten verkkojen välillä, sillä verkon konfigurointimuutosten teko ylläpidollisesti MPLS-verkossa vie enemmän aikaa. Ohjelmallisten verkkojen etuna on siis niiden hallittavuus, jossa keskitetysti hallinnasta vastaa SD-WAN Controller. Controlleri hallitsee kaikkea SD-WAN-verkossa tapahtuvaa, joka on huomattava etu MPLS-verkossa käytettävään hallintamalliin, jossa verkkoon tehtävät muutokset tulee tehdä jokaiselle laitteelle erikseen, mikäli ylläpitävällä taholla ei ole omaa automaatiota tämän luomiseksi. On kuitenkin otettava huomioon näistä tekniikoista se, että tietyillä toimenpiteillä ja ominaisuuksien lisäyksellä MPLS, sekä SD-WAN-verkoista ja niiden laitteista voidaan tehdä ohjelmallisia tai automatisoituja konfiguraation osalta.

5.2 Ratkaisujen implementointi

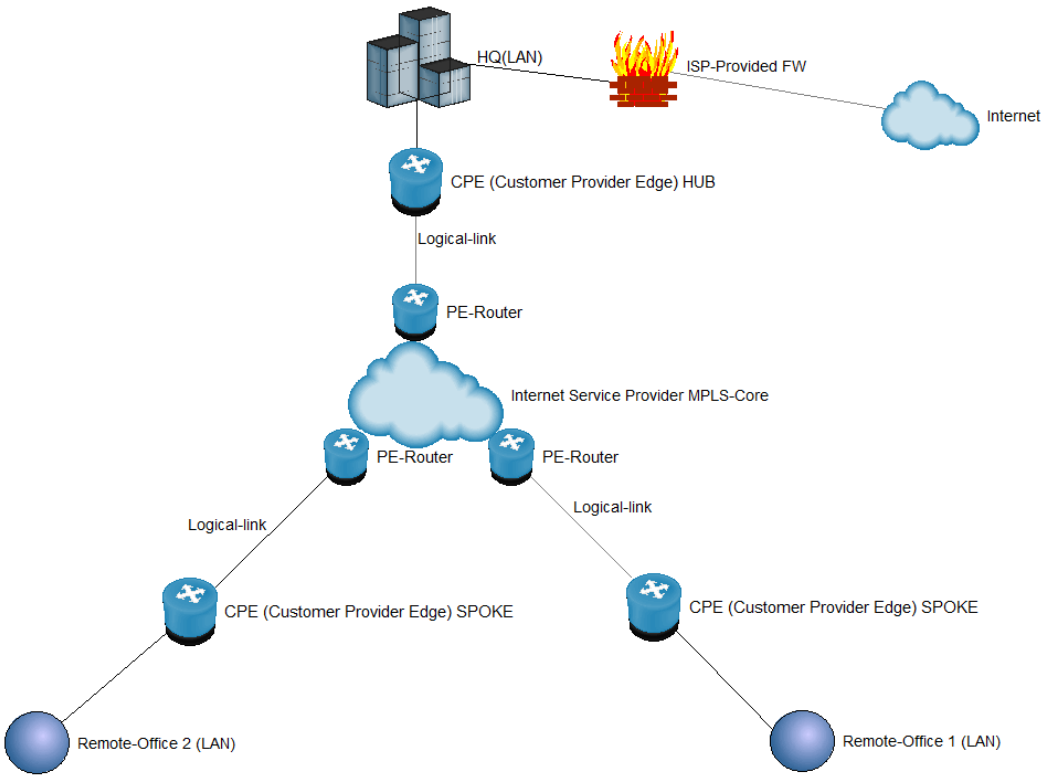
Tämä osa käytännön tutkimusta käsittelee teoriatasolla SD-WAN- ja MPLS-ratkaisujen implementointia Suomessa toimiville yrityksille. Tällä hetkellä yrityksillä on lisääntyvä tarve pilvipalveluiden saatavuudelle, ja siksi luotettava

verkkoyhteys on palveluntarjoajien tavoitteissa asiakaskokemuksen parantamiseksi. Suomessa toimivien yritysten yleinen ratkaisu verkkoyhteyksille on MPLS-verkon läpi toteutettu verkkoratkaisu, jossa teleoperaattori yhdistää asiakkaan toimipisteet yhdeksi isoksi verkoksi käyttämällä hyväksi MPLS Layer-3 VPN-mallia. Tässä toteutuksessa asiakas hyötyy esimerkiksi, jos asiakkaan palvelut sijaitsevat konesalissa, johon kaikki MPLS-VPN-tunnelit terminoidaan. Palveluntarjoaja, joka Suomessa on yleisesti teleoperaattori, ylläpitää MPLS-runkoverkkoa, johon asiakkaat liitetään muodostamalla VRF-instansseja. Kuvassa 8 kuvataan hyvin tapaa, jolla Suomessa teleoperaattorit muodostavat MPLS-pohjaisen verkon.

5.2.1 MPLS-ratkaisun toteutus yritykselle

Tämä osa ei tule käsittelemään koko MPLS-runkoverkon rakentamista, vaan keskittyy suurelta osin asiakkaan liittämistä osaksi operaattoriverkoissa tapahtuvaa MPLS-reititystä. Asiakkaalle kasataan lähtötilanteessa hypoteettinen ratkaisu, jossa asiakkaalla ei ole entuudestaan minkäänlaista tietoverkkototeutusta. Lähtökohtaisesti myös voidaan olettaa, että asiakkaalla on jonkin tason IT-osaamista yrityksen sisällä, sillä kyseessä voi esimerkiksi olla keskisuuri yritys. Yritys ostaa siis kaikki palvelut operaattorilta, paitsi päätelaitteiden ylläpidon.

Esimerkki yritys tutkimuksessa on ollut yhteydessä palveluntarjoajaan ja on perustamassa Suomeen kolmea toimipistettä, jossa yksi on päätoimipisteenä toimiva kohde. Kaksi muuta toimipistettä toimivat sivutoimipisteinä. Yrityksen toiveena on, että palveluntarjoaja ehdottaa yritykselle sopivaa ratkaisua. Kuvitteellinen toteutus tulee olemaan Hub and Spoke -tyylinen MPLS-VPN, jossa päätoimipiste esittää Hubia, jonka kautta kaikki liikenne ohjataan.



Kuva 11. MPLS VPN Hub and Spoke

Kuvassa 11 havainnollistetaan tätä topologiaa. Mikäli asiakas päätyy tähän toteutukseen, on se Suomen operaattorien näkökulmasta helppo toteuttaa, sillä MPLS-runkoverkko on suomessa hyvälle pohjalle rakennettu, ja se vaikuttaa MPLS-verkon yleiseen kannattavuuteen yrityksille implementoinnin ja hinnan näkökulmasta. Toinen vaihtoehtoinen topologia yritykselle olisi käyttää Full Mesh-tyylistä MPLS VPN-ratkaisua, jossa liikennettä ei ohjattaisi yhden toimipisteen läpi. Hub and Spoke -topologia on suunnittelultaan hiukan monimutkaisempi konfiguroida, sillä HUB-toimipisteen reititin, joka toimii reitityksen ohjauspisteenä, vaatii VRF-instanssien välisten reititystietojen levitykseen käytettävän konfiguraation oikeaoppista luomista monimutkaisuuden lisääntyessä. Kuvassa 11 näkyvät loogiset linkit (logical-link) sisältävät palveluntarjoajan access-laitteet, joita voivat esimerkiksi olla ADSL-, VDSL- ja SHDSL-tekniikoista vastaavat DSLAM-laitteet tai kuitupäätteet. Tutkimuksessa tässä tilanteessa ei otettu huomioon tarvitseeko yrityksen rakentaa fyysisiä linkkiverkkoja toimipisteiden välille, joten tässä tilanteessa oletetaan yrityksellä olevan jokaisessa toimipisteessä valokuituratkaisu, sekä mahdollisuus käyttää mobiiliverkkoa va-

rayhteytenä. Varayhteyden käyttämisestä myös sivutoimipisteille aiheutuu kuitenkin huomattava määrä lisäkuluja, joten yrityksen tulee harkita, onko sivutoimipisteillä tarvetta yhteyden varmentamiselle.

MPLS-verkkoon tarvittavat laitteet tähän kokoonpanoon ilman varmentavaa CPE WAN -yhteyttä näkyvät koostetussa taulukossa. Esimerkkitoimittaja tässä käytetty Elisa Oyj:tä, vaikka tällä ei lopputulokseen tutkimuksen kannalta ole vaikutusta, sillä hinnat suomen markkinoilla ovat hyvin tasaisia.

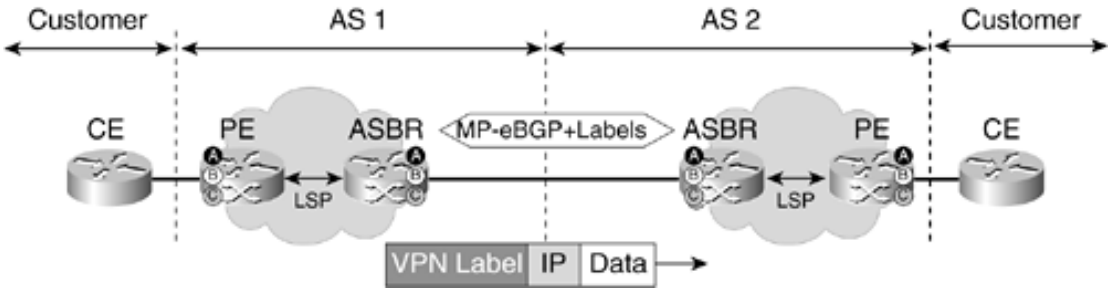
Taulukko 1. MPLS-operaattorinverkon CPE ja palomuurilaitteet

Verkon laitteet	Kappale määrä	Toimittaja
Firewall	1	Elisa
CPE GW	3	Elisa

CPE laitteet ovat toteutuksessa operaattorin vuokraamia reitittimiä esimerkkinä Cisco tai Huawei. Tutkimuksessa on kuvitteellisesti kuitenkin käytössä Ciscon toimittama laite, sillä se on yleisesti käytetty laitetoimittaja Suomessa sekä maailmalla, mikäli kyseessä on yritysverkkoon tarkoitettu etähallittava laite. Reititin-laitteet päätoimipisteissä, sekä sivutoimipisteissä sisältävät asiakkaan reititykseen tarvittavat lokaalit VRF-konfiguraatiot. Operaattori luo tässä tilanteessa asiakkaalle suunnitellun konfiguraation laitteeseen, joka yleensä määräytyy ennalta määritettyjen pohjien perusteella. Tällä hetkellä automaation kehittäminen on kyseisiä laitteita ylläpitäville operaattoreille tärkeää, sillä se helpottaa prosessin läpiviemistä, ja näin ollen sen toimittamista asiakkaalle mahdollisimman nopeasti. Mikäli esimerkiksi MPLS L3 VPN konfiguraatiot CPE, PE ja P laitteille luotaisiin käsin, olisi yhden uuden asiakkaan liittäminen MPLS runkoverkkoon hyvin työlästä ja kallista asiakkaan näkökulmasta.

Tutkimuksen aikana selvitettiin myös MPLS tapauksessa verkon yleistä kattavuutta ja sen vaikutusta yritysten valitsemaan ratkaisuun. Maailmalla yleisesti MPLS-runkoverkon pohja on huono tai se menettelee. Tämä aiheuttaa sen, että hintatasojen erot MPLS ratkaisujen tarjonnassa ovat korkeat. Tutkimus keskittyi vain Suomen tilanteeseen, joka on hyvä. Suomessa teleoperaattorit

toimivat suurelta osin palveluntarjoajina ja, jo alusta asti hyvin rakennetut MPLS-runkoverkot tuovat luotettavuutta verkon toiminnassa, sekä yleisessä hinta tasossa verrattuna muuhun maailmaan. Mikäli asiakkaana oleva yritys vaatii MPLS-verkon toteutusta kohteeseen, jossa palveluntarjoajalla ei ole mahdollisuutta käyttää omaa verkkoaan, on palvelua tarjoavan operaattorin mahdollisuus luoda Inter-AS-mallia käyttämällä yhteys kohteeseen vuokraamalla toisen operaattorin MPLS-runkoverkkoa. Inter-AS-ratkaisussa on erilaisia toteutustapoja, joista malli-B on varteen otettava ratkaisu.



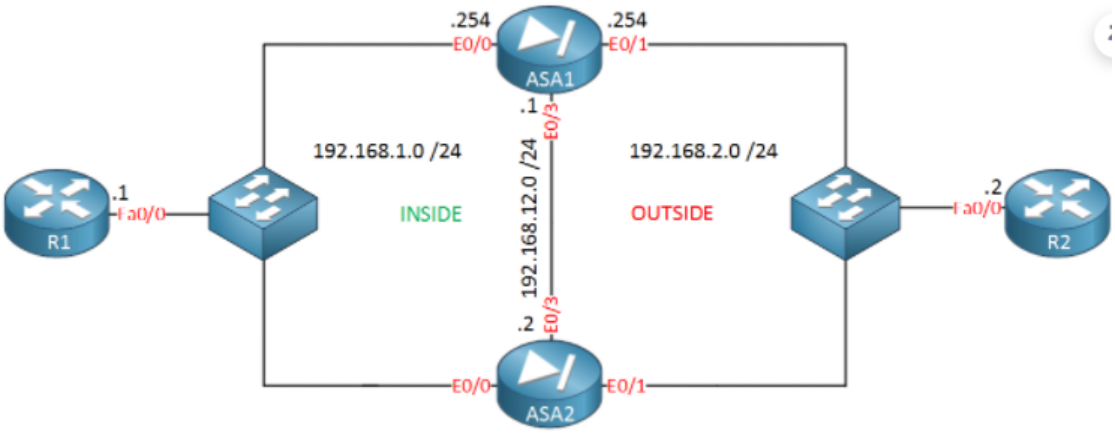
Kuva 12. Malli-B Inter-AS (Analyzing MPLS VPN Security 2005.)

Kuva 12 kuvaa B-mallin toteutusta, jossa Multi-Protocol-eBGP (MP-eBGP) reitittää VPN-IPv4 reitit, ja ne jaetaan esimerkiksi kahden operaattorin välillä. Käytännössä asiakas ei huomaa mitään eroa verkon toiminnassa verrattuna tilanteeseen, jossa VPN-IPv4-yhteydet kulkisivat pelkästään yhden palveluntarjoajan verkon sisällä. Ainoa mitä asiakkaan tulee ottaa huomioon, on datan eheys kahta palveluntarjoajaa käytettäessä. Mikäli asiakkaalla on tarvetta tälle ratkaisulle, voi se luoda huomattavia lisäkuluja, jotka otetaan huomioon tutkimuksen tuloksissa.

5.2.2 MPLS-ratkaisun tietoturva toteutus

Kuten kuvassa 11 huomataan, on MPLS-ratkaisulle integroitu operaattorin toimittama ja ylläpitämä palomuuri ratkaisu. Palomuurin ideana tässä ratkaisussa, on suojata yrityksen verkkoa tilanteessa, jossa liikennöidään Internetin suuntaan. MPLS verkossa on monia ratkaisuja tämän toteuttamiseksi. Tässä ratkaisussa on käytössä keskitetty palomuuri yrityksen päätoimipisteellä. Tämä tekee helpoksi suodattaa koko yrityksen ulkomaailmaan kohdistuva liikenne yhden keskitetyn pisteen kautta. Yrityksen on myös mahdollista ottaa

käyttöön ratkaisu, jossa konfiguroidaan niin sanottu ”Failover” pari palomuurille, joka tuo redundanssin yhteydelle. Näissä tilanteissa ja ratkaisuissa on kuitenkin huomattavan paljon kustannuseroja sekä toteutuksen kannalta huomioon otettavia seikkoja.



Kuva 13. High Availability (HA) palomuuri toteutus Cisco ASA (Cisco 2013.)

Kuvassa 13 on esimerkki toteutuksesta, jossa R1 kuvaa kuvassa 11 nähtyä HQ-toimipisteen reititintä. Mikäli kokopanoon halutaan lisätä lisävarmennusta, voidaan reitittimen R1, sekä viereisen kytkimen pariksi lisätä varmentava linkki, jotta saadaan lisää redundanssia Internetin suuntaan kulkevaan liikenteeseen.

Palomuuri on asiakkaalle MPLS-toteutuksessa tärkeä, mikäli liikenne ohjataan MPLS-runkoverkosta suoraan Internetiin. Vaikka asiakkaalle aiheutuu tästä kuluja, on yrityksen tietoverkon eheys tärkeää tilanteessa, jossa yhteys muodostuu MPLS-verkon ulkopuolelle. Tilanteessa, jossa asiakkaalla olisi hub and spoke MPLS L3 VPN sijasta käytössä full mesh-topologia voitaisiin harkita käytettävän paikallisia palomuureja, jos jokaisella toimipisteellä olisi oma Internet ”exit”-piste.

Tutkimuksessa otettiin myös huomioon aiemmin esitellyn keskitetyn palomuuriratkaisun huonoja ominaisuuksia perinteisessä MPLS-verkossa. Esimerkiksi tietoturvan kannalta internetin rajapinnassa sijaitseva palomuuri ei suojaa yritystä sen sisälle kohdistuvilta tietoturvauhilta. Tähän tutkittiin myös nykypäiväistä vaihtoehtoa suojaamaan yrityksen verkkoa mahdollisilta uhilta. Kyber-

turvallisuudessa käytettävästä Zero Trust -arkkitehtuurista tehtiin tutkimuksessa vertailukohta perinteiselle palomuuriratkaisulle. Zero Trust perustuu nimensä mukaisesti siihen, että kehenkään tai mihinkään ei tulisi luottaa. Tässä tutkimuksessa yrityksen olisi mahdollista toteuttaa tämän arkkitehtuurin kuvaama tavoite, mikäli yritys suostuu implementoimaan tarvittavat toimenpiteet sisä- ja ulkoverkon suojaamiseksi. (Zero Trust Architecture. 2020.)

5.2.3 SD-WAN-toteutus yritykselle

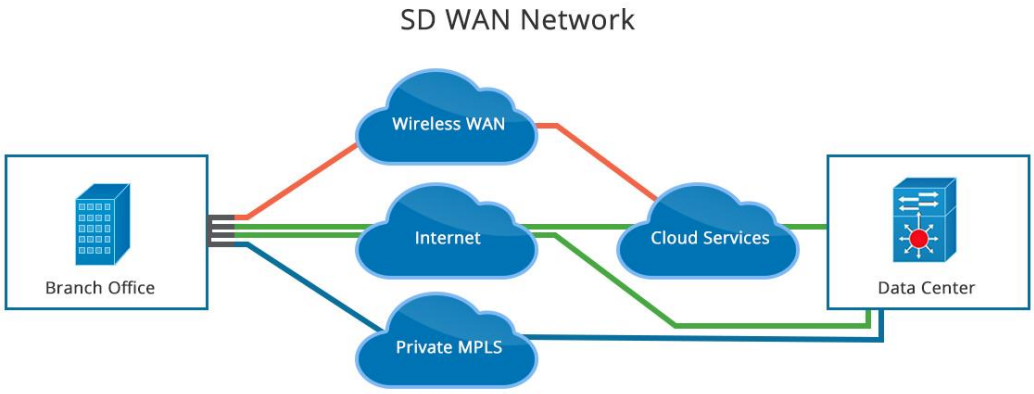
Tutkimuksessa pyrittiin vertailemaan SD-WAN ja MPLS mahdollisimman samanlaisista lähtökohdista sekä topologian osalta. SD-WAN toteutuksessa yrityksellä on myös toiveena kahden sivutoimipisteen ja yhden päätoimipisteen liittäminen SD-WAN-ratkaisuun, jotta vertailukohta MPLS-ratkaisuun säilyy. SD-WAN toteutuksessa lähdettiin siitä olettamuksesta, että yritys tulisi käyttämään kahden eri operaattorin/palveluntarjoajan underlay-ratkaisua, jotka olisivat suomen tilanteessa esimerkiksi Telia ja Elisa. Fortinet valittiin toimittajaksi, ja sen SD-WAN-ratkaisun toimittaisi toinen näistä operaattoreista. Kahden eri operaattorin käyttäminen lisää redundanssia verkon aluskerrokseen, sillä yrityksen ratkaisu on yhden operaattorin runkoverkkoon kohdistuvasta viasta riippumaton.

Topologiaan tarvittavat laitteet redundanttisen SD-WAN-verkon luomiseksi määrittyvät asiakkaalle sillä oletuksella, että jokaiseen toimipisteeseen halutaan aiemmin mainitut kaksi WAN-linkkiä. Tämän suunnan voi perustella SD-WAN-tekniikan hyödyillä, jotka tulevat esille vasta tilanteessa, jossa redundanssi ja verkon yleinen konfiguroitavuus otetaan huomioon. Tämä aiheuttaa asiakkaalle kuluja, sillä vaikka asiakas hyötyisi SD-WAN-tekniikasta jossain määrin ilman redundanssia, on vertailukohtana tärkeä ottaa huomioon tekniikasta löytyvät ominaisuudet, joiden takia tekniikka voisi olla korvaava ratkaisu puhtaalle MPLS-ratkaisulle.

Taulukko 2. SD-WAN-laitteet

Verkon laitteet	Kappale määrä	Toimittaja
Fortigate SD-WAN GW	3	Elisa
CPE Underlay GW	6	Telia 3 / Elisa 3
SD-WAN Controller	1	Elisa

Yrityksellä voi olla tarvetta luotettavaan tiedonsiirtoon, kuten suoralle yhteydelle datakeskukseen, joka sijaitsee päätoimipisteessä tai maantieteellisesti samassa kohteessa. Tämän kaltaisen yhteyden verkon pohjakerros voidaan luoda käyttäen MPLS-verkkoa. Kuten teoriaosan kuvasta 2 voidaan huomata, on yrityksillä selvä tarve turvautua vanhaan ja luotettavaan MPLS-ratkaisuun, mikäli kyseessä ovat esimerkiksi video- tai puheyhteydet.



Kuva 13. SD-WAN-yhteys pilvipalveluihin ja konesaliin (FS-community 2018)

Kuva 13 kuvaa hyvin tässä tutkimuksessa käytettyä ratkaisua SD-WAN-verkolle, jossa redundanssi mahdollistaa ohjelmallisen liikenteen ohjauksen optimaalisinta reittiä kohti konesalia sekä pilvipalveluita. Kuvassa näkyy kolme vaihtoehtoista WAN-yhteyttä, joista luotettavin tiedonsiirtotie on edelleen MPLS. Tämä on tutkimukseen tuloksellisesti tärkeä osa, sillä vaikka SD-WAN tulisi suosituksi ratkaisuksi yrityksille suomessa, on MPLS-verkolle edelleen suuri tarve sen luotettavuuden takia.

Tutkimuksen teoriaosaa tarkastelemalla voidaan todeta ohjelmistopohjaisten verkkojen ominaisuuksien olevan hyvin toimittajariippuvaisia, ja tekniikalle ei ole olemassa minkäänlaista standardia, kuten esimerkiksi MPLS-tekniikalla (RFC3031). Tutkimukseen on siis valittu toimittaja sen perusteella, minkälaiset arvostelut toteutus on saanut eri tahoilta sekä kuinka ominaisuudet sopivat tutkimukseen vertailukohdiltaan.

5.2.4 SD-WAN-tietoturvatoteutus

Tietoturva on iso huolenaihe nykypäivänä, minkä vuoksi tarvittavien tietoturvaominaisuuksien määrä yrityksille on suuri. SD-WAN keskittyy tähän osa-alueeseen tarkasti, ja siksi esimerkiksi tässä tutkimuksessa käytettävissä Fortinet Secure SD-WAN-Branch -laitteissa on käytössä NGFW-ominaisuus sisäänrakennettuna. Tämä poistaa keskitetyn palomuuriratkaisun tarpeen yhteyksien luomiseksi internettiä kohti, koska jokaisen toimipisteen WAN-LAN-rajapinnan välissä on SD-WAN-reititin, joka sisältää palomuuriominaisuuden. Ylläpidollisesti jokaisen toimipisteen palomuuriratkaisu kuulostaa monimutkaiselta ja hankalalta ylläpitää. Ohjelmallisen verkon hyödyt on kuitenkin huomattu tutkimuksen aikana vaikuttavan tähän tavalla, jolla konfiguroitavuus on helppoa, sillä kuten ohjelmallisten verkkojen muut ominaisuudet, on kaikki asetukset ennalta määritetty SD-WAN-controllerille. Tällöin toimipisteiden provisiointi ja ylläpito helpottuu myös tietoturvan näkökulmasta.

Ohjelmalliset verkot tuovat siis, kuten aiemmin on mainittu, hyvän näkyvyyden ja ohjattavuuden verkon resursseihin. Tämä hyöty on SD-WAN-verkkojen suurin ero perinteisiin MPLS-yritysverkkoratkaisuihin, sillä esimerkiksi verkossa liikkuvan turvaluokitellun datan siirtäminen voidaan sovelluskohtaisesti ohjata turvallista WAN-yhteyden päälle luotavaa IP-SEC-tunnelia pitkin. Tutkimuksessa otettiin tämä huomioon erityisenä hyötynä yrityksille tietoturvan kannalta, sillä vaikka liikenne ohjattaisiin suoraan toimipisteistä internetin suuntaan kohti pilvipalveluja, on liikenne mahdollista salata koko matkalta. Salauksesta vastaavan SD-WAN-reitittimen tehtävä on siis käytännössä huolehtia End to End -salauksesta, josta on yritykselle hyötyä, mikäli pilvipalveluihin tarvittavat yhteydet kulkevat internetin yli.

Valittuna laitetoimittajana Fortinet Secure SD-WAN tuo monia ominaisuuksia yrityksen käyttöön, ja ne otettiin myös huomioon toimittajan valintaa tehtäessä. Uuden sukupolven palomuuriratkaisu mahdollistaa normaalia palomuuria enemmän erilaisten uusien uhkien suodattamista yrityksen käyttöön, ja tämä katsottiin hyötynä normaaliin keskitettyyn palomuuriin. Aiemmin käsitellyssä MPLS-Tietoturva-kappaleessa mainittu Zero Trust -arkkitehtuuri soveltuu hyvin ohjelmistopohjaisten tietoturvaratkaisuiden implementointiin. Tätä voidaan perustella sillä, että SD-WAN-reitittimet sisältävät kattavan uuden sukupolven palomuuriratkaisun sisään rakennettuna. Tämä on yksi kriittinen osa Zero Trust-arkkitehtuurissa mainituista vaatimuksista suojatun kerroksen luomiseksi. (Computer Security Resource Center 2020.)

6 JOHTOPÄÄTÖKSET

Suomessa yritysverkkojen luotettavuuden, joustavuuden ja tietoturvan tarve kasvaa kovaa tahtia. Tämä johtaa tilanteeseen, jossa palveluntarjoajat kilpailevat parhaiden ratkaisuiden implementoinnista ja uusien innovaatioiden tuomisesta markkinoille. Asiakkaina olevat yritykset tarvitsevat huomattavan paljon enemmän kapasiteettia verkkoihin laitteiden lisääntyessä. OSI-mallin fyysisen kerroksen perinteiset kupari- tai 4G-mobiiliratkaisut, eivät nykypäivänä kykene tuomaan tarvittavaa kapasiteettia yritysten tarpeisiin implementoida laitemäärällisesti entistä monimutkaisempia verkkoja. Tämä tarkoittaa käytännössä sitä, että yritysverkoissa implementoitavien yhteyksien tulee tulevaisuudessa sisältää tarvittavaan kapasiteettiin kykeneviä fyysisiä ratkaisuja, jotka tukevat MPLS:n ja SD-WANin kaltaisia verkkotekniikoita. Verkostoitumisen lisääntyminen tuo myös mukanaan tietoturvan kannalta varteenotettavia kehityskohteita tietoverkoissa. Palveluntarjoajat tarjoavat yleensä yritysverkkoliittymiin perinteisten palomuuriratkaisuiden lisäksi ohjelmistopohjaisten verkkojen tuomia vaihtoehtoisia ratkaisuja.

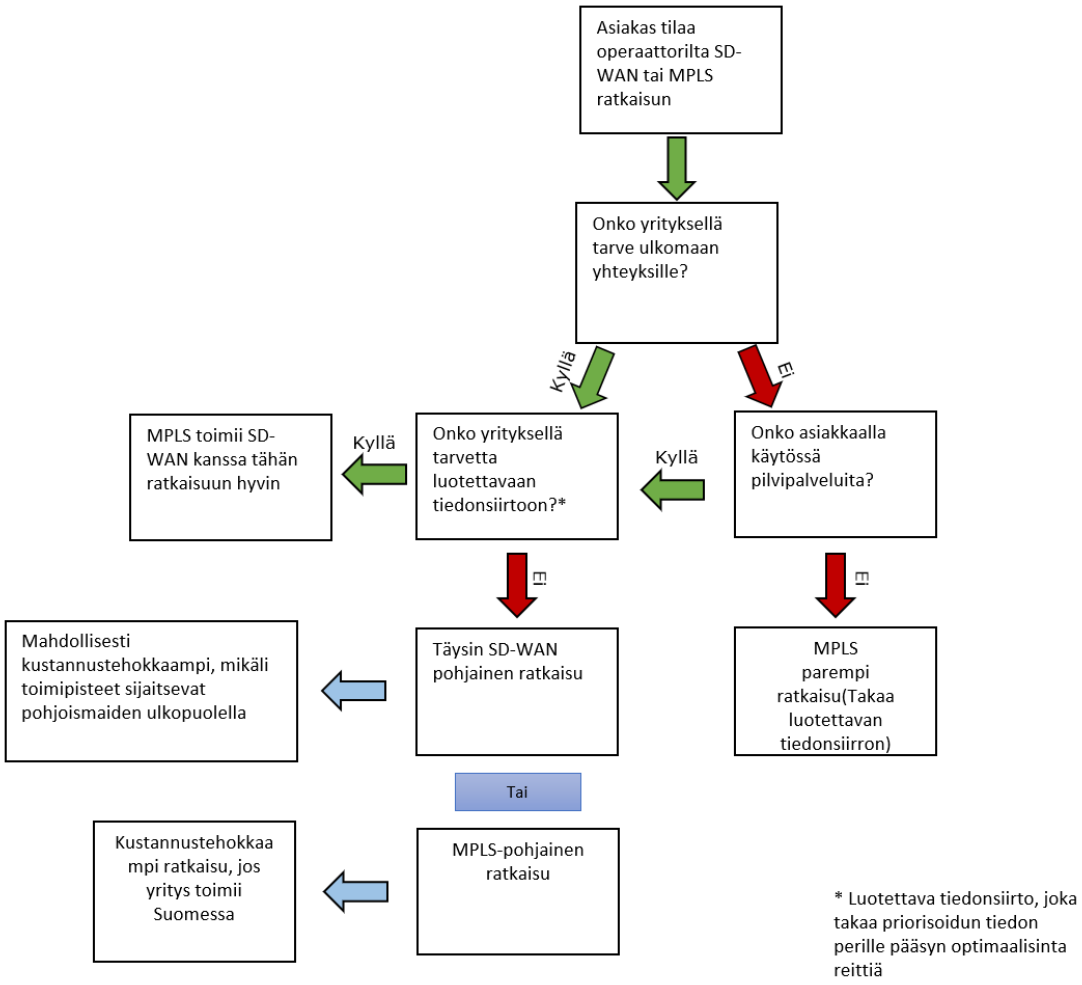
Tämän opinnäytetyön tavoitteena, oli tutkia olisiko SD-WAN mahdollinen korvaaja perinteisille MPLS-toteutuksille yritysverkoissa. Lähtökohtana käytiin teoriaosuudessa läpi näitä kahta tekniikkaa, minkä avulla saataisiin tietopohja käytännön tutkimukselle. Teoriapohjan ja käytännöntutkimuksen avulla selvi-

tettiin näiden tekniikoiden heikkouksia ja vahvuuksia, kun niitä implementoidaan yritysverkkoratkaisuiksi. Ratkaisuiden tutkiminen suoritettiin luomalla hypoteettisia tilanteita, jossa asiakkaana oleva yritys ostaa palveluna SD-WAN- tai MPLS-ratkaisun palveluntarjoajalta. Kuvitteellisesti luoduilla ratkaisuilla pyrittiin tuomaan esille asiakkaalle mahdollisesti aiheutuvia haasteita, hyötyjä ja kuluja. Nämä kuvitteelliset topologiat sisälsivät myös ehdotettuja ratkaisuja tietoturvan parantamiseksi lisäämällä palomuuri osaksi toteutusta.

Tutkimuksen aikana huomattiin, että alkuperäisessä suunnitelmassa mainittu fyysisen verkon rakentaminen ja konfigurointi ei toisi työlle tarvittavaa tulospohjaista hyötyä siihen käytettävään aikaan suhteutettuna. Työn tavoitteen saavuttaminen oli siis todennäköisempää tutkimalla tekniikoita ja niiden implementoimiseen yritysverkkoihin pintapuolisesti. Pintapuolisella tarkastelulla työssä tarkoitettiin esimerkkipohjaisen hypoteettisen ratkaisun luomista, jossa käytettiin hyödyksi MPLS ja SD-WAN-verkoissa käytettyjä ja ehdotettuja tapoja rakentaa kuvitellun yrityksen verkkoratkaisu. Opinnäytetyön aihe valikoitui kiinnostuksesta tutkia maailmalla paljon puhuttujen ohjelmallisten verkkojen tuloa markkinoille, ja miten ne mullistaisivat esimerkiksi pilvipalveluiden käytön yritysverkoissa. MPLS-verkko valittiin SD-WANin vertailukohdaksi sille perusteella, että sen erilaiset variaatiot ovat hallinneet yritysverkkomaailmaa jo pitkän aikaa. Näiden tekniikoiden välillä oltiin kuitenkin tarkkoja, jotta tekniikoiden erot siinä minkälaisia ne ovat teknisesti, eivät tuottaneet vääristyneitä tutkimustuloksia. Ohjelmalliset verkot tuovat markkinoille useita uusia ominaisuuksia sekä mahdollisuuksia yrityksille. Niiden lisääntyvä implementointi tukee niissä mainostettuja ominaisuuksia ja hyötyjä. On kuitenkin tärkeää vertailla näitä esille nostettuja ominaisuuksia suhteessa markkinoita suomessa hallitsevaan MPLS-ratkaisuun.

Tutkimuksessa tavoitteena oli saada vastaus, onko SD-WAN todellisuudessa se tekniikka, joka korvaisi perinteiset yritysverkkoratkaisut. MPLS:n korvaaminen uudella ohjelmallisella verkolla ei kuitenkaan pidä tutkimuksen aikana tehtyjen havaintojen ja tutkimustulosten perusteella paikkansa. Perusteluna tälle on tutkimuksen teoria- ja käytännöntutkimusvaiheessa nähtyjen SD-WAN-ratkaisujen topologiat ja niiden sisältävät MPLS-verkko-ratkaisut sekä MPLS-verkkotekniikan yleiset käyttötarkoitukset. On tärkeää muistaa, että nämä tek-

niikat eivät ole samanlaisia tai suoranaisesti vertailtavissa muuta kuin käyttötarkoitukseltaan. MPLS edustaa verkon aluskerrosta, joka tukee SD-WAN-tekniikan kaltaisia päällysverkkotekniikoita. Tätä voidaan käyttää perusteluna sille, että MPLS-verkkoa on suositeltavaa käyttää ratkaisuna yhdessä SD-WAN-verkon kanssa, mikäli tavoitteena on ohjelmallisten verkkojen asiakkaalle luvatun luotettavuuden saavuttaminen sitä tarvitseville kriittisille sovelluksille. Suomessa näiden tekniikoiden kannattavuus riippuu täysin asiakkaana olevan yrityksen tarpeista, johon verkkoa tullaan käyttämään. Tapauksia SD-WAN-verkon hyödyntämiseksi on monia, mutta Suomen yrityksille potentiaalisin vaihtoehto olisi hyödyntää tätä tekniikka, kun yrityksen toimipiste sijaitsee Pohjoismaiden tai Baltian ulkopuolella. Yrityksellä voi tässä tilanteessa olla monen toimipisteen kattava MPLS-verkko suomessa, ja tarpeen vaatiessa voidaan perustaa ulkomailla sijaitsevaan kohteeseen SD-WAN-yhteydet, jotka verkotetaan toimimaan yhdessä. Mutta kuten esimerkistä voidaan huomata, on kummankin tekniikan valitseminen täysin kiinni yrityksen käyttötarkoituksesta, tarpeista ja käyttöympäristöstä. Tekniikat sisältävät omat hyvät puolensa niissä osa-alueissa, joihin ne ovat alun perin suunniteltu. Tarkkaa lukua myöskään yritykselle aiheutuvista kuluista on mahdotonta todeta tarkasti, sillä kuten tekniikan valinta, myös kulut kulkevat käsikädessä yrityksen tarpeiden ja suunnitelmien kanssa. Taulukot 1 ja 2 antavat suuntaa yritykselle aiheutuvista kuluista, mutta tämäkin on täysin riippuvainen siitä, onko yritys minkälaisen ratkaisun tarpeessa.



Kuva 14. Tutkimuksen johtopäätöksiä havainnollistava kaavio

Tutkimuksessa saatiin haluttu vastaus kysymykseen, onko SD-WAN korvaava ratkaisu MPLS-tekniikalle yritysverkkoratkaisuissa. Aiheen käsittely saatiin rajattua siinä määrin, että tutkimustulosten tarkkuus riittää toteamaan tekniikoiden valinnan olevan täysin riippuvaisia tilanteesta. Tulevaisuudessa on mahdollista, että verkkotekniikoiden evoluutio muokkaa tässä työssä saadun tuloksen oikeellisuutta.

LÄHTEET

Alouneh, S. Abed, S. 2010. Fault tolerance and security issues in MPLS networks. PDF-dokumentti. Saatavissa: https://www.researchgate.net/publication/228850104_Fault_tolerance_and_security_issues_in_MPLS_networks [viitattu 14.1.2021].

Analyzing MPLS VPN Security. 2005. Cisco Press. WWW-dokumentti. Saatavissa: https://www.ciscopress.com/articles/article.asp?p=418656&seqNum=5 [viitattu 20.5.2021].

Aruba SD-WAN Dynamic Path Steering with Service Level Agreements. 2019. Hewlett Packard Enterprise. PDF-dokumentti. Saatavissa: https://www.arubanetworks.com/assets/tg/TB_SD-WAN-Dynamic-Path-Steering.pdf [viitattu 22.11.2020].

Brown, D. S. 2017. The IT Professional's guide to corporate networks. Blogi. Päivitetty 18.9.2017. Saatavissa: https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 [viitattu 26.9.2020].

Cisco ASA Firewall Active / Standby Failover. 2013. Networklessons. WWW-dokumentti. Saatavissa: https://networklessons.com/cisco/asa-firewall/cisco-asa-firewall-active-standby-failover [viitattu 15.5.2021].

Complete guide to SD-WAN. 2018. FirewallCX. WWW-dokumentti. Saatavissa: http://www.firewall.cx/general-topics-reviews/sd-wan/1210-sd-wan-networks-benefits-management-security-architecture.html#sd-wan-security-vpn-features [viitattu 25.12.2020].

Configuring Policies for Dynamic Path Steering. 2021. Aruba. WWW-dokumentti. Saatavissa: https://help.central.arubanetworks.com/latest/documentation/online_help/content/gateways/cfg/wan/dps.htm [viitattu 29.5.2021].

DeGeest, K. 2021. What is an MPLS anyway? SANS Institute. PDF-dokumentti. Saatavissa: https://www.sans.org/reading-room/whitepapers/vpns/mpls-vpn-anyway-718 [viitattu 16.11.2020].

Eskola, J & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Osuuskunta Vastapaino.

Fortinet Optimizes Network Performance With Secure SD-WAN. 2020. Fortinet. WWW-dokumentti. Saatavissa: https://www.fortinet.com/blog/business-and-technology/fortinet-optimizes-network-performance-with-secure-sd-wan [viitattu 25.12.2020].

Gallaher, R. 2004. MPLS Training Guide: Building Multiprotocol Label Switching Networks. Elsevier Science & Technology Books. ProQuest Ebook Central. E-kirja. Saatavissa: http://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=294347 [viitattu 7.11.2020]

In Search of the Right SD-WAN Solution. 2019. Gartner. PDF-dokumentti. Saatavissa: https://www.gartner.com/imagesrv/media-products/pdf/cisco/Cisco-1-5W2DWHZ.pdf [viitattu 20.2.2021].

Minei, I. & Lucek, J. MPLS-Enabled Applications: Emerging Developments and New Technologies, John Wiley & Sons, Incorporated, 2011. ProQuest Ebook Central. E-kirja. Saatavissa: http://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=644967 [viitattu 6.11.2020].

MPLS VPN Overview. 2019. Juniper Networks. WWW-dokumentti. Saatavissa: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-security-vpn-overview.html [viitattu 14.11.2020].

MPLS vs SD-WAN: Which suits your organisation. 2020. Route-xp. WWW-dokumentti. Saatavissa: https://www.routexp.com/2018/10/mpls-vs-sd-wan-which-suits-your.html [viitattu 25.4.2021].

MP-BGP. 2021. Network Direction. WWW-dokumentti. Saatavissa: https://networkdirection.net/articles/routingandswitching/mp-bgp/ [viitattu 27.5.2021]

Peer to Peer VPN overlay. 2019. Tutorzine. WWW-dokumentti Saatavissa: https://tutorzine.com/peer-to-peer-vpn-overlay-vpn/ [viitattu 14.11.2020].

Route Distinguisher and Route Target – MPLS Tutorial. 2013. Roger Perkin. WWW-dokumentti. Saatavissa: https://www.rogerperkin.co.uk/ccie/mpls/route-distinguisher-vs-route-target/ [viitattu 17.11.2020].

Route-Targets Explained. 2015. Packet Pilot. WWW-dokumentti. Saatavissa: https://www.packetpilot.com/route-targets-explained/ [viitattu 17.11.2020].

Secure SD-WAN: Integrated NGFW Security with WAN Transformation. 2017. Gartner. PDF-dokumentti. Saatavissa: https://www.itworld-canada.com/client/fortnite/pdf/en/Gatner_Secure%20SD%20WAN_Nov%202017.pdf [viitattu 28.11.2020].

Secure SD-WAN: The security vendors and their SD-WAN offerings. 2019. IDG Communications, Inc. WWW-dokumentti. Saatavissa: https://www.networkworld.com/article/3489480/secure-sd-wan-the-security-vendors-and-their-sd-wan-offerings.html [viitattu 26.12.2020].

SD-WAN vs MPLS: Pros and Cons. 2018. FS-Community. WWW-dokumentti. Saatavissa: https://community.fs.com/blog/sd-wan-vs-mpls-pros-and-cons.html [viitattu 20.5.2021].

Techopedia. 2020. Asynchronous Transfer Mode. WWW-dokumentti. Päivitetty 12.9.2020. Saatavissa: https://www.techopedia.com/definition/5339/asynchronous-transfer-mode-atm [viitattu 26.9.2020].

Telia. 2018. 5 yritysverkkojen trendiä – automaatio, käyttäjäystävällisyys ja ketteryys ovat nyt valttia. *Kauppalehti.* Verkkolehti. Saatavissa: https://studio.kauppalehti.fi/telia/5-yritysverkkojen-trendia-automaatio-kayttajaystavallisyys-ja-ketteryys-ovat-nyt-valttia [viitattu 29.5.2021].

Tutkimusstrategiat. 2014. Jyväskylän Yliopisto. WWW-dokumentti. Päivitetty 15.1.2014. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

The 4 SD-WAN architectures for network security. 2017. IDG Communications, Inc. WWW-dokumentti. Saatavissa: https://www.networkworld.com/article/3234790/the-4-sd-wan-architectures-for-network-security.html [viitattu 28.11.2020].

Thimmaraju, K. Shastry, B. Fiebig, T. Hetzelt, F. 2016. Reigns to the Cloud: Compromising Cloud Systems via the Data Plane. PDF-dokumentti. Saatavissa: https://www.researchgate.net/figure/The-Shim-header-is-placed-between-the-Ethernet-and-IP-headers-The-shim-header-MPLS_fig2_309484272 [viitattu 13.11.2020].

Understanding MPLS Header. 2009. GoMPLS. WWW-Dokumentti. Saatavissa: http://www.gompls.net/2009/08/understanding-mpls-header.html [viitattu 13.11.2020].

Understanding MPLS Layer 3 VPNs. 2019. Juniper Networks. WWW-dokumentti. Päivitetty 5.12.2019. Saatavissa: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-security-layer-3-vpn-understanding.html [viitattu 8.11.2020].

Uppal, S. Woo, S. Pitt, D. 2018. Software-Defined WAN For Dummies®, 2nd VMware Special Edition. New Jersey: John Wilei & Sons, Inc. PDF-dokumentti. Saatavissa: http://wan.velocloud.com/rs/098-RBR-178/images/SD_WAN_For_Dummies_VMware_2nd_SpecialEdition.pdf [viitattu 15.11.2020].

What is SD-WAN? 2020. VMware. WWW-dokumentti. Saatavissa: https://www.vmware.com/solutions/sd-wan.html [viitattu 8.11.2020].

Zero Trust Architecture. 2020. Computer Security Resource Center. WWW-dokumentti. Saatavissa: https://csrc.nist.gov/publications/detail/sp/800-207/final [viitattu 3.6.2021].