Jussi Kujala

Palomuurin ja L3-kytkimen L2VPN yhteensopivuus operaattoriverkossa

Opinnäytetyö

Tietotekniikka / Tietoverkkotekniikka

Toukokuu 2016

KYAMK
University of Applied Sciences

Tekijä/Tekijät	Tutkinto	Aika
Jussi Kujala	Insinööri	Toukokuu 2016

Opinnäytetyön nimi

Palomuurin ja L3-kytkimen L2VPN yhteensopivuus operaattoriverkossa

33 sivua

Toimeksiantaja

Suomen Datasafe Oy

Ohjaaja

Yliopettaja Martti Kettunen

Tiivistelmä

Palveluntarjoajien verkoissa ei ole vain yhtä suurta laitevalmistajaa, jolla olisi monopoliasema. Palveluntarjoajan on tunnettava laaja kirjo eri laitevalmistajia ja löydettävä yhtäläisyydet laitevalmistajien välillä. Palveluntarjoajan on myös pystyttävä reagoimaan vikatilanteisiin nopeasti ja tehokkaasti.

Opinnäytetyö käsittelee erilaisia L2VPN-siirtoteitä ja niiden yhteensopivuutta eri laitevalmistajien välillä. L2VPN-siirtoteissä keskityttiin VLL Martini -moodiin ja VPLS Martini -moodiin, koska molemmat moodit käyttävät OSPF- ja LDP-protokollia reititykseen MPLS-verkossa. L2VPN-siirtoteitä tutkittiin palomuurien ja L3-kytkinten välillä. Lisäksi työssä käytettiin IPsec VPN -siirtotietä LTE-verkon ylitse.

Opinnäytetyön tavoitteena oli tutkia yhteensopivuutta laitteiden välillä. Työssä rakennettiin toimiva MPLS-verkon osa ja verkon sisälle toimivat L2VPN-tiedonsiirtotiet, jotka toimivat testattavia yhteyksiä ja Internetiä varten. Työn tarkoituksena on löytää käyttökelpoinen L2VPN toteutus ja hyödyntää sitä vanhoilla yhteyksillä.

Tuloksena yrityksellä on toimiva MPLS-verkko ja valmiudet luoda tarvittavia L2VPN-siirtoteitä tarpeidensa mukaan. L2VPN-siirtoteitä hyödynnettiin testattaviin yhteyksiin. Yrityksellä on myös valmius käyttää IPsec VPN -tiedonsiirtotietä palomuurien välillä ja reitittää liikennettä IPsec VPN -tiedonsiirtotien sisällä.

Asiasanat

MPLS, VPLS martini mod, VLL martini mod, CCC, IPsec VPN

Author (authors)	Degree	Time
Jussi Kujala	Bachelor of Engineering	May 2016

Thesis Title

The Provider's L2VPN Compatibility between Firewall and L3-Switch

33 pages

Commissioned by

Suomen Datasafe Oy

Supervisor

Martti Kettunen, Principal Lecturer

Abstract

In the service providers' networks, no major device manufacturer has a monopoly. The service provider must have knowledge on a wide spectrum of different device manufacturers, as well as to find the similarities between the devices manufacturers. The service providers also have to react quickly and effectively in fault situations.

The thesis work deals with different data transmission paths between different device manufacturers, L2VPN as well as their compatibility. In L2VPN data transmission paths, the focus was on the VLL Martini mode as well as VPLS Martini mode, because both of them are using OSPF as well as LDP protocols for the routing in the MPLS networks. L2VPN data transmission paths were examined between firewalls as well as L3 switches. Furthermore, (in the thesis work) IPsec VPN was used over the LTE network as a transmission path.

The objective of the thesis was to examine compatibility between the devices. As a part of the thesis process, the functional part of the MPLS network and L2VPN data transmission paths inside the network were built for the Internet as well as for the testing of connections. The purpose of the thesis work was to find a practicable L2VPN implementation and to utilise it with the old connections.

As a result of this thesis work, the company gained a functional MPLS network as well as readiness to configure L2VPN data transmission paths fulfilling its requirements. L2VPN data transmission paths were utilised for connections tested. The company also has readiness to use IPsec VPN data transmission paths between firewalls as well as to route traffic inside the IPsec VPN data transmission path.

Keywords

MPLS, VPLS martini mod, VLL martini mod, CCC, IPsec VPN

SISÄLLYS

1 SANASTO JA LYHENTEET

CCC	Circuit Cross-Connect: *siirtokerroksen yhteys alkupisteestä loppupisteeseen. Toimiakseen MPLS-verkon sisällä se tarvitsee RSVP-lähetyslipun.*
C-VLAN	Customer Virtual Local Area Network: *asiakkaan 802.1q kehys.*
GRE	Generic Routing Encapsulatin: *ciscon kehittämä tunnelointiprotokolla. Tämän avulla voidaan tehdä alkupisteestä loppupisteeseen olevia linkkejä esimerkiksi ISP:n läpi.*
IPSEC	Internet Protocol Security: *protokollan avulla voidaan autentikoida ja suojata jokainen IP-paketti. IPsec on liikenteen loppupäiden turvaava protokolla.*
IKE	Internet Key Exchance: *avaintenvaihtoprotokolla.*
ISP	Internet Service Provider: *organisaatio, joka tarjoaa Internet-yhteyden palveluna omien laitteidensa läpi.*
LDP	Label Distribution Protocol: *protokolla jakaa liput käyttäen pohjalla olevaa reititysprotokollaa useimmiten OSPF tai BGP.*
LSP	Label Switched Path: *toimii siirtotienä MPLS-verkossa.*
MPLS	Multiprotocol Label Switching: *ip-pakettien kuljettamiseen kehitetty menetelmä, jolla voidaan kuljettaa liikennettä solmukohtien läpi ilman reititystä. MPLS toimii siirtokerroksella ja verkkokerroksella.*
OSPF	Open Shortest Path First: y*leisesti tunnettu reititysprotokolla.*
PW	Pseudo Wire: *kuviteltu kaapeli kahden reunareittimen välillä.*
QinQ	IEEE 802.1Q-in-Q VLAN tunneling mechanism: *802.1q koteloitu kehys koteloidaan toisella 802.1q kehyksellä.*
RSVP	Resource Reservation Protocol: *RSVP toimii kuljetuskerroksella. Tämän protokollan avulla määräytyvät oikeat liput paketeille.*
S-VLAN	Service Virtual Local Area Network: *palveluntarjoajan 802.1q kehys.*
VLL	Virtual Leased Line: *protokolla toimii ethernet-pohjaisen liikenteen MPLS-verkossa, kun alku- ja loppupisteitä on vain yksi.*

VPLS	Virtual Private LAN Service: *protokolla yhdistää ethernet-pohjaisen liiketeen MPLS-verkossa, kun alku- ja loppupisteitä on monia.*
VPN	Virtual Private Network: *virtuaalinen yksityinen verkko, jonka avulla voidaan yhdistää kaksi lähiverkkoa toisiinsa julkisen verkon ylitse.*
VSI	Virtual Switching Instance: *VPLS:ssä käytettävä alue, johon voidaan liittää useampi portti tai VLAN.*

2 JOHDANTO

Tämän opinnäytetyön tarkoituksena on selvittää L3-tasoisten kytkinten ja palomuurien L2-tason VPN-yhteensopivuutta operaattoriverkossa. Tarkoituksena on keskittyä pelkästään siirtokerroksen virtuaalisiin yksityisiin verkkoihin. Tutkinnan kohteena ovat etenkin VLL (Virtual Leased Line) Martini -moodi ja VPLS (Virtual Private LAN Service) Martini -moodi. Martini-moodi mahdollistaa saman LSP-siirtotien käyttämistä moneen alueeseen. Huomiotavia asioita ovat myös palomuurin yhteensopivuus MPLS-verkkoon ja reitityksen tietoturva.

2.1 Yleistä

Nykypäivän tietoverkkoratkaisuissa ei ole enää yhtä laitevalmistajaa, joka olisi monopoliasemassa. Palveluntarjoajan on tunnettava laaja kirjo eri laitevalmistajia, koska laitteet vaihtelevat palveluntarjoajan ja asiakkaan rajapinnalla. Laitteiden erilaisuus voi tuoda haasteita etenkin yhteensopivuuden osalta, vaikka yleisesti tunnetut standardit ja tekniikat ovat kaikissa laitteissa samankaltaisia.

On tärkeää hallita perusteet, jotta voi soveltaa tietoa muissa laitevalmistajissa. Liian heikko pohjatieto voi johtaa virhepäätelmiin. Palveluntarjoajan on kyettävä reagoimaan vikatilanteisiin nopeasti ja tehokkaasti. Hyvää pohjatietoa perusteiden omaksumiselle tarjoavat esimerkiksi Cisco Systems Inc ja Juniper Networks.

2.2 Työn rajaus

Yhteensopivuutta lähdettiin tutkimaan, jotta ymmärrys kehittyisi eri laitteiden ja protokollien välillä. Tällä tavalla hahmottuu eri laitteiden toimintatavat ja löydetään yhtäläisyyksiä, joita voidaan hyödyntää. On tärkeää löytää yhtäläisyydet laitteiden väliltä, jotka auttavat vian rajauksessa haastavimmissakin tilanteissa.

Opinnäytetyön tavoitteena on rakentaa MPLS-verkon osa ja siihen toimivat L2VPN-siirtotieyhteydet. Vanhat yhteydet siirrettäisiin myöhemmin käyttämään uusia L2VPN-siirtotieyhteyksiä. Uusia L2VPN-siirtotieyhteyksiä suunniteltaessa on huomioitava vanhojen yhteyksien toimintatavat ja yhteyden käyttäytyminen siirryttäessä uuteen siirtotiehen.

Palomuureissa hyödynnettäisiin IPsec VPN -siirtotietä tarpeiden mukaisesti. IPsec VPN -siirtotieyhteys käyttäisi LTE-verkkoa. Tätä siirtotietä käytettäisiin varayhteyksien ja muiden sekundääristen yhteyksien pohjana. On huomattava, että LTE-verkko on myös kasvava ja kehittyvä siirtotievaihtoehto yhteyksille.

3 TEKNIIKAT JA STANDARDIT

Tekniikat ja standardit kohdassa käydään tarkemmin läpi käytettyjä tekniikoita ja standardeja, joita on hyödynnetty opinnäytetyössä. Työ pohjautuu L2VPN ratkaisuihin, jotka käyttävät LDP-signaloitumiseen OSPF-protokollaa. L2VPN:stä käytettiin VLL Martini -moodi ja VPLS Martini -moodi protokollia. VLL Martini -moodi protokollaa käytettiin *point-to-point* tiedonsiirtoteihin ja VPLS Martini -moodi protokollaa käytettiin *point-to-multipoint* tiedonsiirtoteihin. Molempia protokollia voidaan käyttää joko suoraan liitäntäporttiin tai virtuaalisen paikallisen osoitteen liitäntään. IPsec VPN toimi työssä varayhteyksien siirtotienä.

3.1 MPLS

Multiprotocol Label Switching yhdistää suorituskyvyn ja saatavuuden siirtokerroksella ja yhdistää skaalautuvuuden ja reitityksen verkkokerroksella. MPLS mahdollistaa yritysten ja palveluntarjoajien muodostaa seuraavan sukupolven infrastruktuureja. MPLS mahdollistaa myös tuottaa uusia tapoja palvella monia yrityksiä suoritustehoista tinkimättä. Yhteyksiä tilaavien asiakkaiden ei tarvitse muuttaa omia laitteitaan, kunhan ne tukevat MPLS-teknologiaa, koska MPLS on riippumaton asiakkaiden käyttämistä teknologioista.(Darukhanawalla & Bellagamba 2009, 19-20.)

MPLS sisältää verkkokerroksen virtuaalisia yksityisiä verkkoja, siirtokerroksen virtuaalisia yksityisiä verkkoja, liikenteen suunnittelua, palvelujen laadun määrittelemistä, keskitettyä IP-pakettien kuljettamiseen kehitettyä menetelmää ja se tukee IPv6:tta. MPLS:n avulla saavutetaan suuri saatavuus, eriytettävyys, loppupään IP palveluita yksinkertaisilla konfiguraatioilla, hallin-

taa, paljon erilaisia palveluita yrityksille säästämällä palveluntarjoajan omaisuutta. (Darukhanawalla & Bellagamba 2009, 19-20.)

3.2 VPLS Martini -moodi

Virtual Private LAN Service tarvitsee Martini moodissa LDP-etänaapuruuden (remote LDP session) ja reititysprotokollan - esimerkiksi OSPF-protokollan toimiakseen. *Pseudo Wiren* aktivoituessa tarvitaan yhteydelle tietyt PWID:t eli identiteettinumerot. Identiteettinumeroiden avulla tietyt portit tai virtuaaliset paikalliset alueelliset verkot tunnistautuvat kuuluvansa tiettyyn virtuaaliseen osa-alueeseen eli virtuaaliseen ethernet-liitäntään. (Hangzhou H3C Technologies Co. 2008; Apcar 2006.)

VPLS Martini -moodi on helppo implementoida. LDP ei kuitenkaan aina luo automaattista naapuruuden etsintämekanismia, joten reunareitittimet joudutaan konfiguroimaan manuaalisesti aina kun reunalle liitetään uusi reunareititin. (Hangzhou H3C Technologies Co. 2008; Apcar 2006.)

3.3 VLL Martini -moodi

Virtual Leased Line Martini -moodi käyttää LDP-yhteyskäytäntöä signaloitumiseen virtuaalisten osa-alueiden tietojen lähettämiseen. Martini-moodi tarvitsee LDP-etänaapuruuden (remote LDP session) toimiakseen. Reunareitittimet löytävät reitin virtuaalisen osa-alueen läpi pidennetyllä LDP-naapuruuden avulla. (Huawei Technologies Co. 2012.)

Kuva 1: L2VPN Martini -moodi

3.4 CCC

Circuit Cross-Connect on perinteinen pisteestä pisteeseen oleva L2-tiedonsiirtotie. MPLS-verkon yli käytettynä se tarvitsee uniikin RSVP LSP:n jokaista aluetta ja kohdetta vasten, koska LSP ei sisällä tässä tapauksessa VC:n sisäistä lippua. Jokainen LSP:tä käyttävä kehys kuuluu tiettyyn alueeseen. (O'Connor, D. 2014.)

Erisuuntiin kulkevat asiakkaan lähettämät tietokehykset edelleen kapseloidaan toiseen L2-tason kehykseen. Tässä ulommassa kehyksessä on mukana RSVP-lippu, joka kertoo aluetiedon kehyksen saapuessa vastaanottavaan päähän tiedonsiirtoyhteydellä. (O'Connor, D. 2014.)

Kuva 2: Circuit Cross-Connect

3.5 IPsec VPN

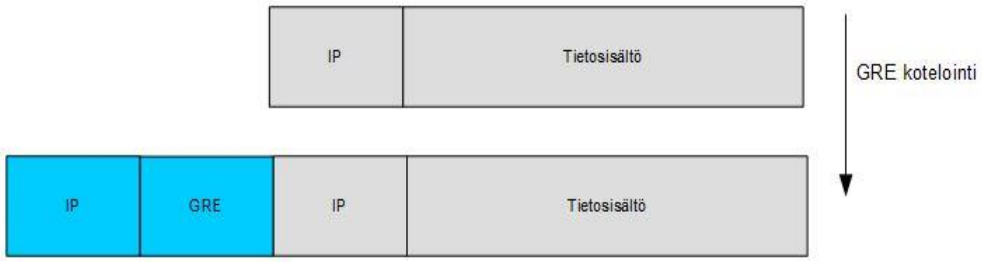
IPsec VPN:stä on tullut keskeinen osa nykypäivän tietoverkkoliikenteessä. IPsec VPN:n avulla suojataan lähetettävä tieto eri paikkojen ja etäkäyttäjien välillä. Tietoliikenne sisältää paljon enemmän arkaluontoista tietoa, joka täytyy pitää salassa. Tämä taas on kasvattanut tietoturvan kehittämistä. IPsec VPN:n tarkoituksena on autentikoida ja suojata salattu informaatio kolmannelta osapuolelta. (Cameron & Woodberg, 2013; Juniper Networks Inc, 2014a; Juniper Networks, Inc, 2015.)

SRX-sarjan palomuureihin voidaan konfiguroida muun muassa kahden tyyppisiä IPsec VPN -tiedonsiirtotievaihtoehtoja. Vaihtoehdot ovat *policy-based* ja *route-based*. Molempien vaihtoehtojen tarkoituksena on suojata liikenne. (Cameron & Woodberg, 2013; Juniper Networks Inc, 2014a; Juniper Networks, Inc, 2015.)

Moni laitevalmistaja ei välttämättä tue molempia vaihtoehtoja. Vaihtoehtojen yhteensopivuus ei kuitenkaan ole ongelma. On olemassa kuitenkin yksi poikkeus: käyttäessä dynaamista reititysprotokollaa (RIP, OSPF, IS-IS), niin on käytettävä *route-based* VPN -tiedonsiirtotietä. (Cameron & Woodberg, 2013; Juniper Networks Inc, 2014a; Juniper Networks, Inc, 2015.)

3.6 GRE

GRE koteloi (encapsulation) datapaketit ja uudelleenohjaa ne laitteeseen, joka purkaa koteloinnin ja reitittää datapaketit päämääräänsä. Protokolla mahdollistaa laitteiden välille virtuaalisen suoranlinkin, vaikka laitteet olisivatkin monen kilometrin päässä toisistaan. GRE-tunneli mahdollistaa eri protokollien viennin tunnelin läpi esimerkiksi OSPF, LDP ja MPLS. (Juniper Networks Inc, 2014b; Cameron ym. 2010.)



Kuva 3: GRE kotelointi

4 JUNIPER NETWORKS JA PALOMUURIT

Palomuurit ovat tärkein osa nykypäivän tietoverkoissa. Palomuurit suojaavat sisäverkkoja sekä DMZ-alueita verkkohyökkäyksiltä ja haittaohjelmilta. Palomuurit ovat kuitenkin muuttuneet vuosien myötä. Palomuurit ja palomuurien tarve on kasvanut tietoverkkojen laajentuessa vuosien myötä. Palomuurien tarvitsee myös toimia osittain myös reitittiminä. Palomuurien tarvitsee myös tutkia tietoliikenteessä liikkuvia paketteja yhä tarkemmin ja tarkemmin. Tärkeää on myös, ettei pakettien tarkastelu rasita muun liikenteen kulkua, vaan kaiken pitää toimia mahdollisimman nopeasti ja tarkasti. (Cameron & Woodberg, 2013; Cameron ym. 2010.)

4.1 Palomuurin sijoittaminen

Palomuurien sijoittaminen riippuu pitkälti suojattavan verkon koosta. Pienemmissä verkoissa riittää, että palomuuri sijaitsee asiakasverkon ja internetin rajalla. Suuremmissa verkoissa tulee miettiä tarkemmin palomuurien sijoittamista. Mitä suuremmat ovat suojattavat verkot ja alueet sitä enemmän tarvitaan palomuureja suojaamaan verkkoja. Suuremmissa verkoissa on otettava huomioon kuormanjako ja priorisoida liikenne oikein. Todella suurissa yritysverkoissa on otettava huomioon palomuurien kahdennus hyvän suorituskyvyn ylläpitämiseksi. (Cameron & Woodberg, 2013; Cameron ym. 2010.)

4.2 Vahvuudet

Juniper Networksin informaatio on tarpeeksi laajaa ja kattavaa. Se on hyvä lähtökohta suunnittelulle. Juniper Networksin sivuilta saatavassa informaatiossa on myös eritelty eri osa-alueita verkkojen suuruudesta. Juniperin laitteet taipuvat lähes minkälaiseen konfiguraatioon tahansa, joten erilaisia ratkaisuja eri tarpeisiin löytyy useita. Palomuurit on nimetty eri luokkiin, jotka vastaavat eri käyttötarkoitusta. Nykypäivän organisaatiot tarvitsevat mahdollisimman monipuolista palvelua ja yksityiskohtaisia ratkaisuja eri ongelmatilanteisiin.

4.3 Heikkoudet

Juniper Networksin sivuilta saatavan informaation laajuus on hieman liian suuri aloittelijoille. Verrattuna Cisco Systemsin ohjeisiin ja esimerkkeihin ovat ne vaikealukuisia ja moniselitteisiä. Toiminnollisuus ja ratkaisujen suuri kirjo tuovat ehkä ongelmia hahmottaa ratkaisuja lopullisiin ongelmatilanteisiin. On tärkeää, että hahmottaa kokonaiskuvan, ennen kuin lähtee hakemaan ratkaisuja Juniper Networksin laitteilla. Komentorivi johtaa usein harhaan, koska konfiguraatio on puumainen ja useita komentoja voi asettaa useisiin paikkoihin.

5 TYÖN TAVOITELTAVA KOKONAISUUS

Tavoitteena on löytää hyviä tapoja toteuttaa MPLS-verkon osa pienelle kasvavalle palveluntarjoajalle ja suunnitella verkko niin, että verkko vastaisi tulevaisuuden kasvu tarpeita. Suunnittelussa on otettava myös huomioon L2-tasoisten tiedonsiirtoteiden helppo liittäminen MPLS-verkkoon. Liityntärajapinta on myös suunniteltava tarkasti ja otettava huomioon eri laitteiden yhteensopivuusongelmat. Pääyhteydelle on myös joissakin tilanteissa suunniteltava varayhteys, jotta toteutuksessa säilyy toimiva verkkoyhteys.

5.1 Palomuuri MPLS-verkon reunalla

Palomuuri voisi toimia MPLS-verkon palveluntarjoajan rajapinnalla, jolloin se suojaisi liikenteen molempiin suuntiin. Reitittimessäkin voi tehdä palomuurausta, mutta palomuurin sijoittaminen reunalle toisi enemmän tietoturvaa. Palomuuri ei tosin pystyisi samaan reititystehoon kuin reititin. Riippuen asiakkaan tarpeista voisi palomuurikin toimia MPLS-verkon reunalla.

5.1.1 Vahvuudet

Palomuurin vahvuuksia olisivat tietoturvan kasvu ja liikenteen vahvempi valvominen. Juniper Networksin palomuurit voivat toimia kuten tilalliset palomuurit (stateful) ja eri liitäntäportit voidaan jakaa kuulumaan eri alueisiin. Palomuureista löytyy myös ohjelmistopohjainen palomuuritoiminto, mutta käytimme työssä tilallista toimintoa. Palomuurin tilallisuustoiminto tutkii paketin tilan ja paketille avatun yhteyden. Ominaisuus muistaa paketit, joille on jo valmiiksi avattu yhteys. Eri alueille voidaan määrittää erilaisia sääntöjä tarpeiden mukaisesti. On parempi avata uudessa alueessa tarvittavia palveluita ja protokollia, kuin lisätä liitäntäportti suoraan alueeseen, jossa on kaikki sallittua. Tällöin tietoturvariskit ovat pienemmät.

5.1.2 Heikkoudet

Palomuuri ei kykene samoihin reititystehoihin kuin reititin ja liikenteen pakettien tarkistaminen voi viedä suoritustehoja. Palomuurin skaalautuvuus ei välttämättä ole yhtä riittävä kuin reitittimellä. Palomuurin reititystauluun ei välttä-

mättä mahdu yhtä paljon reititystietoja kuin reitittimen reititystaulussa. Internetin reititystaulu on parempi sijaita reitittimessä. Palomuurissa voi tulla muistiongelmia, jos siinä pitää Internetin reititystaulun.

5.2 L3-tasoinen kytkin MPLS-verkon reunalla

L3-tasoinen kytkin pystyisi myös toimimaan MPLS-verkon reunalla. Monet L3-tasoisista kytkimistä tukevat MPLS-teknologioita. Kytkimet pystyvät myös reitittämään paketteja.

Kytkinten vahvuuksina ovat liitäntäporttien suuri määrä. Fyysisten liitäntäporttien lisäksi kytkimeen pystytään tekemään loogisia aliliitäntäportteja. L3-tasoisten kytkinten suoritusteho on myös riittävä toimiakseen MPLS-verkon reunalla.

Kytkinten tietoturva rajoittuu pitkälti pääsylistoihin. Kytkinten reititystaulu ei ole yhtä suuri kuin reitittimillä. Kytkimiä konfiguroidessa on oltava tarkkana portin moodista. L2-tasoisissa porteissa voi syntyä *switching loop* laitteiden välillä. L3-tasoisten porttien konfiguroiminen on turvallisempaa.

6 TOTEUTUS

Toteutuksessa käydään tehtyjä asioita yksityiskohtaisesti läpi. Testatut asiat jakautuvat L2VPN tiedonsiirtoteihin L3-kytkinten ja palomuurien välille ja IPsec VPN -tiedonsiirtoteihin palomuurien välille. Osassa toteutuksissa on myös käytetty GRE-tiedonsiirtotietä. Eräässä toteutuksessa käytettiin QinQ-tunnelointia.

6.1 L2VPN-tiedonsiirtotiet

Tarkoituksena on käyttää Juniperin SRX-sarjan palomuureja ja mahdollisesti eri valmistajan L3-kytkintä. Tarkoituksena on löytää mahdollisimman helppo ja yksinkertainen L2VPN-tiedonsiirtotie kasvavalle yritykselle. Reititysprotokollista OSPF toimisi LDP:tä varten.

Ensimmäiseksi oli selvitettävä erilaisia L2VPN-vaihtoehtoja ja testattava niitä ensin L3-kytkinten välillä. Tämän jälkeen voitiin testata valittuja L2VPN-vaihtoehtoja palomuuria vasten. Tärkeää oli myös selvittää ensin mitä L2VPN-ominaisuuksia palomuuri tukee.

Vaihtoehtoina oli ottaa kantaa tiedonsiirtotien sisällä olevaan liikenteeseen tai vain tarjota tiedonsiirtotien alku- ja loppupiste ottamatta kantaa sisältöön.

Helpoin implementoitava L2-tason tiedonsiirtotie oli olla ottamatta kantaa tiedonsiirtotien sisällä kulkeviin paketteihin. Tässä toteutuksessa tarjotaan asiakkaalle tiedonsiirtotien alku- ja loppupiste. Tiedonsiirtotien siirtokapasiteettia voidaan kuitenkin rajoittaa halutuksi kuten konfiguraatio 1.

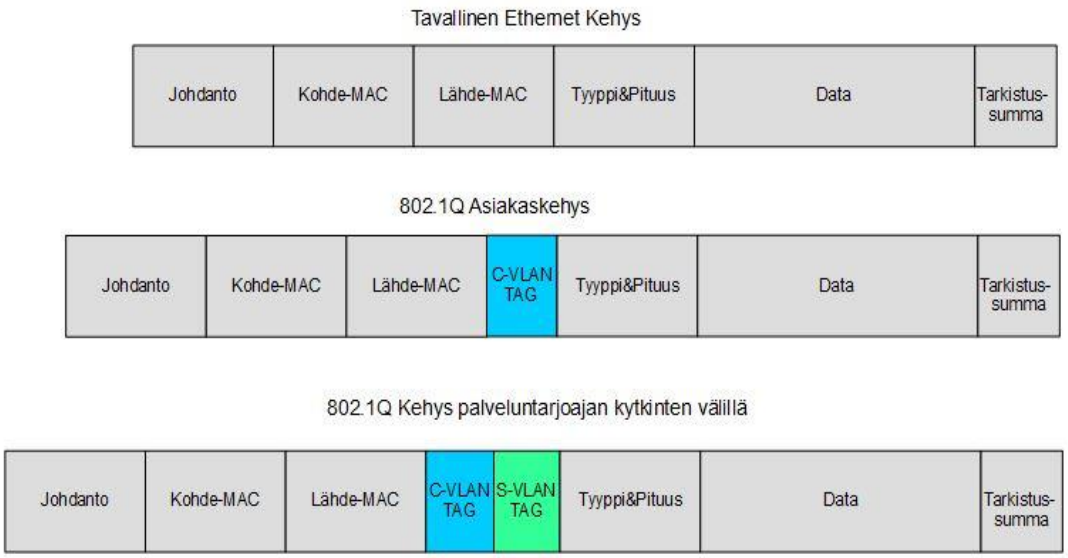
```
// Portin liikenteen rajoittaminen 10megaan                    (1)
 #
 Switch1
 #
 interface GigabitEthernet0/0/12
  undo portswitch
  mpls l2vc 10.11.12.1 pw-template pwtesti 12
  qos lr outbound cir 10240 cbs 2048000
  qos lr inbound cir 10240 cbs 2048000
 #
 Switch2
 #
 interface GigabitEthernet0/0/12
  undo portswitch
  mpls l2vc 10.11.12.2 pw-template pwtesti 12
  qos lr outbound cir 10240 cbs 2048000
  qos lr inbound cir 10240 cbs 2048000
 #
```

Haasteita tuotti QinQ-toteutus. Toteutuksessa käytettiin VLAN-manipulaatiota. Toteutuksessa otettiin kantaa L2-tason tiedonsiirtotien sisältöön. Tartuntarajapinnaksi tarjottiin S-VLAN. S-VLANin sisällä vietiin yksi tai useampi C-VLAN.

Toteutus tehtiin seuraavasti: Palomuurilta syötettiin halutut C-VLANit MPLS-verkon kytkimen porttiin, jossa suoritettiin *qinq stacking*-operaatio. Lopputu-

loksena saatiin palveluntarjoajan S-VLAN, jonka sisällä oli yksi tai useampi C-VLAN. Tämä iso S-VLAN kuljetettiin L2VPN-tiedonsiirtotietä pitkin toiselle MPLS-verkon kytkimen portille, jossa suoritettiin *qinq termination*-operaatio. Lopputuloksena saatiin palveluntarjoajan S-VLAN purettua C-VLANin ympäriltä.

Operaatiot oli suoritettava kytkimen aliliitäntäportissa. Pääliitäntäportin tuli olla L3-tilassa palomuuria vasten. Toteutus olisi onnistunut myös pääliitäntäportin ollessa L2-tilassa, mutta silloin olisi ollut vaarana silmukka (switching loop) kytkimen ja palomuurin välillä, mikä aiheuttaisi mahdollisesti verkon kaatumisen.



Kuva 4: Ethernet-kehykset

L3-kytkimen ja palomuurin välille osoittautui parhaimmaksi vaihtoehdoksi VLL, joka tunnetaan palomuurissa L2circuit nimellä. VPLS ei sopinut palomuuriin, koska se tarvitsee LDP-signalointiin BGP-protokollan ja tarkoituksena oli käyttää vain OSPF-protokollaa. Tässä malli L2circuit-protokollasta konfiguraatio 2.

// Switch (2)

interface GigabitEthernet0/0/10

undo portswitch

```
mpls l2vc 10.11.12.4 14


// Firewall

set protocols l2circuit neighbor 10.11.12.1 interface ge-0/0/3.0 virtual-circuit-id 14

set interfaces ge-0/0/3 encapsulation ethernet-ccc

set interfaces ge-0/0/3 unit 0 family ccc

set security zones security-zone trust interfaces ge-0/0/3.0
```

Vaihtoehdot toteutuksiin olivat tarjota liityntärajapinnaksi liityntäportti suoraan laitteesta tai laitteessa oleva VLAN-liitäntä. Haluttu vaihtoehto piti kuitenkin vielä liittää L2VPN-tiedonsiirtotiehen joko VLL Martini -moodissa tai VPLS Martini -moodissa. Moodit erottuivat siten, että VPLS Martini -moodissa käytettiin VSI (Virtual Switch Instance), jossa on tietyn alueen tunnistautumistiedot ja se mahdollistaa po*int-to-multipoint*-yhteydet liityntärajapintojen välillä. VLL Martini -moodissa taas tunnistetiedot liitetään suoraan haluttuun liitäntäporttiin tai VLAN-liitäntään, tämä mahdollistaa vain *point-to-point*-yhteydet liityntärajapintojen välillä.

6.2 IPsec VPN -tiedonsiirtotiet

Tarkoituksena on testata SRX-sarjan palomuureissa olevia IPsec VPN -tiedonsiirtotien vaihtoehtoja suojatulle yhteydelle. Keskeisenä testattavana asiana on *route-based* IPsec VPN -tiedonsiirtotie hyödyntäen staattisia reittejä sekä dynaamista reititysprotokollaa.

6.2.1 Site-to-Site IPsec VPN

IPsec VPN -ratkaisuja tutkittiin aluksi *site-to-site* IPsec VPN:n avulla. Ensimmäisessä toteutuksessa oli yksi palomuuri, jolla oli staattinen IP-osoite. Toinen palomuuri muodosti yhteyden dynaamisesta IP-osoitteesta. Tunnistautuminen tapahtui erikseen määritetyllä *preshared-keyn* ja *hostnamen* avulla. Palomuurien tunnistetiedot määriteltiin *IKE Gatewayssä*.

6.2.2 Hub-and-spoke IPsec VPN

Seuraavaksi tutkittiin *hub-and-spoke* IPsec VPN:iä. Tässä toteutuksessa *Hub*-puolena toimivalla palomuurilla oli staattinen osoite, johon *Spoke*-puolen palomuurit kiinnittyivät dynaamisella IP-osoitteella ja samalla periaatteella

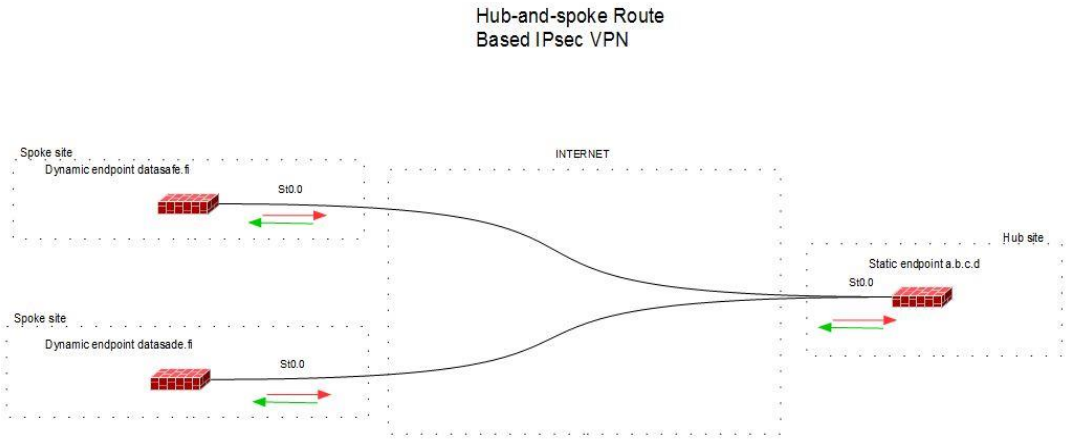
tehdyillä *preshared-keyn* ja *hostnamen* avulla. Tässä toteutuksessa oli huomioitavaa, että *preshared-key* ja *hostname* olivat molemmilla Spoke-puolen palomuureille erilaiset, mutta Hub-puolen palomuurin tuli vastata molemmille Spoke-puolen palomuureille.

Molemmissa testeissä käytettiin *route-based* IPsec VPN:iä. Reititys tapahtui staattisilla reiteillä, joissa hyppyosoitetta merkittiin joko *secure-tunnel*-liitännällä (st0.0) tai liitännän IP-osoitteella. IPsec VPN:n muodostus tapahtui LTE-verkon ylitse.

Palomuureissa oli huomioitava muutamia asioita, jotta *route-based* IPsec VPN toimi. Palomuureissa oli sallittava Internetiä vasten olevassa liitäntäportissa IKE-protokolla. Palomuureissa oli määritettävä sääntö, joka päästää molemmissa palomuureissa sisäverkon liikenteen läpi. Tärkeä huomioitava asia oli, että palomuurien *IKE Gateway*n tunnistetiedot olivat tarkalleen oikeat.

6.2.3 Oletusyhdyskäytävän reititys

IPsec VPN -toteutuksissa tutkittiin myös onnistuisiko oletusreitin (0.0.0.0/0) reititys IPsec VPN:n läpi. Tämä toteutus oli pohjimmillaan samanlainen kuin *site-to-site* IPsec VPN:n. Tässä toteutuksessa oli luotava dynaamisen puolen palomuurille staattinen reitti, joka johti palomuurille, jolla oli staattinen IP-osoite. Lisäksi palomuurille oli määritettävä staattinen IP-osoite liitäntäporttiin, joka oli vasten LTE-reititintä. Tämä esti LTE-reitittimen oletusreitin mainostuksen, koska tavoitteena oli saada oletusreitti IPsec VPN:n yli toiselta palomuurilta.



Kuva 5: Hub-and-spoke IPsec VPN

6.3 Reititetty kuituyhteys & reititetty varayhteys

Eräs testattava toteutus oli suora kuituyhteys ja varayhteydeksi teimme GRE-tunnelin, joka käytti IPsec VPN:n *secure tunnel*-liitännän osoitetta ja reitittimen VLAN-liitännän osoitetta alku- ja loppupisteenä. Suora kuituyhteys reititettiin L2VPN:n läpi OSPF-protokollaa hyödyntäen. Liityntärajapinnan reunalla toimi palomuuri, johon suora kuituyhteys ja varayhteys liitettiin.

6.3.1 Yleistä

Työssä oli monia eri vaiheita. Ensimmäisenä oli rajattava halutut osoitteet ja päätettävä tietty VLAN-liitäntä verkolle. Linkkiverkkoa varten oli myös varattava osoitteet ja määritettävä VLAN-liitäntä. Seuraavaksi oli palomuurille määritettävä peruskonfiguraatio, joka piti sisällään osoitteiden, tunnusten, nimipalvelimien konfiguroinnin. Tämän jälkeen palomuurissa oli määriteltävä liitäntäportit kuulumaan samaan VLANiin, jota käytettiin testattavassa toteutuksessa. Kaksi liitäntäporttia varattiin kuituyhteyttä ja varayhteyttä varten.

6.3.2 Tietoturva

Tietoturvaa varten oli määriteltävä oma alue VLAN-liitännälle ja sallia liikennöinti ulos. Halutut protokollat ja palvelut oli myös sallittava liitäntäporteista. Hallintaa varten oli tehtävä suodatin, jolla rajattiin pääsy laitteeseen. Hallintasuodatin oli myös muistettava konfiguroida loogiseen liityntäporttiin, joka esti kolmannen osapuolen pääsyn linkkiverkon kautta palomuuriin.

6.3.3 Varayhteys ja staattisen reitin merkitys

Varayhteyttä varten oli luotava IPsec VPN -tunneli palomuurien välille. Tässä toteutuksessa liityntärajapinnalle viety palomuuri ottaa tunnelin kautta yhteyttä palveluntarjoajan palomuuriin, josta on suora linkki reitittimelle. Liityntärajapinnan palomuuriin oli määritettävä staattiset reitit palveluntarjoajan palomuuria ja reititintä vasten. Palomuuria vasten olevassa reitissä oli huomioitava, että hyppyosoitteeksi määritettiin verkko, jolla liityntärajapinnalla oleva palomuuri otti yhteyden Internetiin. Lisäksi oli muistettava konfiguroida liityntärajapinnan palomuuriin osoite käsin, koska muuten Internetiin yhdistävä LTE-verkon reititin olisi ensisijainen vaihtoehto yhteydelle. Toisen staattisen reitin tarkoituksena oli kertoa liityntärajapinnalle viedylle palomuurille reitti palveluntarjoajan palomuurilta reitittimelle, jossa oli määriteltynä VLAN-liitäntä. Tätä VLAN-liitännän osoitetta kaikki liityntärajapinnan verkon laitteet käyttivät oletusyhdyskäytävänä.

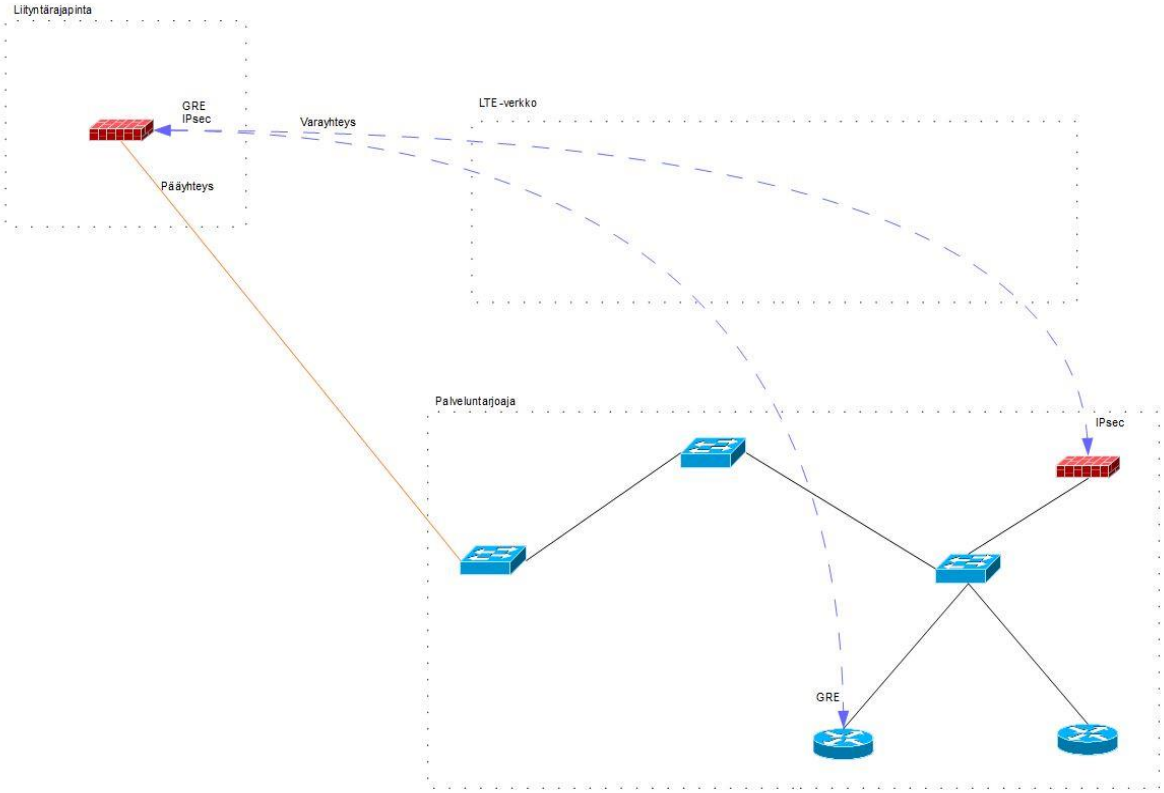
6.3.4 GRE-protokollan ja OPSF-protokollan merkitys

Varayhteyden reititystä varten oli luotava GRE-liitännät. Liityntärajapinnan palomuuria vasten alku- ja loppuosoitteina olivat liityntärajapinnan palomuurin *secure tunnel* –liitännän osoite ja palveluntarjoajan palomuurin linkkiverkon osoite palveluntarjoajan reitittimelle. Palveluntarjoajan palomuuria vasten osoitteet olivat määritelty toisinpäin. OSPF-protokolla loi naapuruudet GRE-liitännöiden välille ja reititys tapahtui GRE-siirtotien lävitse.

Lopuksi oli liitettävä liityntärajapinnan verkko mainostukseen palveluntarjoajan reitittimessä OSPF-protokollalla. OSPF-protokollalle oli myös määritettävä *metric* arvot, joiden mukaan reititin osasi reitittää liityntärajapinnalta tulevan liikenteen ensisijaisesti kuituyhteyttä pitkin.

6.3.5 Toimivuuden todentaminen

Toteutuksen toimivuuden pystyi todentamaan liittämällä kannettavan liityntärajapinnan palomuuriin liityntärajapinnan verkon osoitteella. Kannettavaan oli määritettävä oletusyhdyskäytäväksi palveluntarjoajan reitittimen liityntärajapinnan VLAN-liitännän osoite.



Kuva 6: Reititetty kuituyhteys & reititetty varayhteys

6.4 L2 Circuit over MPLS over GRE over IPsec

IPsec VPN -tiedonsiirtotiet herättivät kiinnostusta, joten päädyin testaamaan pystyisikö SRX-sarjan palomuurien L2-tason *virtual circuit*-protokolla toimimaan LTE-verkon ylitse. Toteutusta testattaisiin DHCP-palvelimen avulla. Mielenkiintoista oli havaita miten MPLS käyttäytyy IPsec VPN –tiedonsiirtotien sisällä.

6.4.1 Yleistä

L2-tasoinen *virtual circuit* ei tarvitse BGP-protokollaa signaloitumiseen vaan se toimii OSPF-protokollan avulla. Protokollia varten oli muodostettava loogiset liitäntäportit palomuurien välille. Kaikki toteutuksessa käytettävät protokollat vaihtoivat tietoja niiden avulla. Palomuurien ollessa tilallisia palomuureja oli muodostettava suodatinsäännöt MPLS:lle ja CCC:lle. Säännöissä oli aktivoitava MPLS- ja CCC-liikenteelle *packet-mode*-toiminto. Tilallisissa palomuureissa oli myös huomioitava liikennöinti saman alueen sisällä ja sallittava liikennöinti alueista ulospäin.

6.4.2 IPsec VPN

Työn alussa täytyi konfiguroida *route-based* IPsec VPN -tiedonsiirtotie palomuurien välille. IPsec VPN muodostettiin samalla tavalla kuin edelliset samankaltaiset tiedonsiirtotiet. Ensimmäisellä palomuurilla oli staattinen IP-osoite ja toisella palomuurilla oli dynaaminen IP-osoite. Tunnistautuminen tapahtui IKE *Gatewayssä* määritetyillä *preshared-keyn* ja *hostnamen* avulla. Tunnelin ollessa aktiivinen voitiin siirtyä eteenpäin.

6.4.3 GRE

GRE-tiedonsiirtotie toimi tässä toteutuksessa protokollien keskusteluväylänä. GRE käytti tunnelin alku- ja loppupisteinä IPsec VPN -tiedonsiirtotien *secure tunnel* (st0.0) liitäntäportteja. GRE-tiedonsiirtotiessä oli huomioitava MTU:n arvo, jotta paketit mahtuivat kulkemaan sen lävitse. MTU-arvoa tuli nostaa 9000:een. *Secure tunnel* liitäntäporttien MTU arvo oli jo valmiiksi 9192.

6.4.4 MPLS

MPLS:n toimintaa varten oli aktivoitava OSPF-protokolla ja LDP-protokolla. Molemmat protokollat toimivat GRE-tiedonsiirtotien lävitse ja muodostivat naapuruudet GRE-liitäntäporttien avulla. Oletuksena SRX-sarjan palomuurit estävät MPLS:n liikennöinnin, joten sitä varten oli luotava suodatinsääntö.

6.4.5 L2 Circuit

L2 Circuit-protokollan aktivoimiseen tuli nostaa fyysisten liitäntäporttien MTU-arvoa 1600:een. Oletus MTU-arvo liitäntäporteilla on 1500. L2 Circuit-protokollassa tuli käyttää samaa *Virtual-Circuit-ID* numeroa laitteiden välillä ja kotelointi tyypiksi tuli valita ethernet. Fyysisille liitäntäporteille ei anneta IP-osoitetta, vaan niissä aktivoidaan CCC-toiminto. Toiminnon voi hahmottaa, ajattelemalla sen olevan looginen kaapeli palomuurien ja LTE-verkon välillä.

6.4.6 Lopputulos ja toiminnan todentaminen

Lopputuloksena saatiin L2-tasoinen silta LTE-verkon ylitse kahden palomuurin välille. Toteutuksen pystyi testaamaan liittämällä DHCP-palvelin ensimmäisen palomuurin fyysiseen liitäntäporttiin, johon oli aktivoitu CCC-toiminto. Toisen palomuurin fyysiseen liitäntäporttiin liitettiin kannettava, joka sai osoitteen DHCP-palvelimelta L2-tasoisen sillan kautta.

Seuraavasti pystyttiin varmentamaan protokollien toiminta komennoilla 3.

root@srx05# run show ospf neighbor (3)

Address Interface State ID Pri Dead

10.11.100.11 gr-0/0/0.0 Full 10.0.0.4 128 31

root@srx04# run show ospf neighbor

Address Interface State ID Pri Dead

10.11.100.10 gr-0/0/0.0 Full 10.0.0.5 128 36

root@srx05# run show ldp neighbor

Address Interface Label space ID Hold time

10.0.0.4 lo0.0 10.0.0.4:0 33

10.11.100.11 gr-0/0/0.0 10.0.0.4:0 11

root@srx04# run show ldp neighbor

Address Interface Label space ID Hold time

10.0.0.5 lo0.0 10.0.0.5:0 38

10.11.100.10 gr-0/0/0.0 10.0.0.5:0 13

root@srx05# run show ldp session

Address State Connection Hold time

10.0.0.4 Operational Open 23

root@srx04# run show ldp session

Address State Connection Hold time

10.0.0.5 Operational Open 26

root@srx05# run show l2circuit connections

Layer-2 Circuit Connections:

Legend for connection status (St)

EI -- encapsulation invalid NP -- interface h/w not present

MM -- mtu mismatch Dn -- down

EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down

CM -- control-word mismatch Up -- operational

VM -- vlan id mismatch CF -- Call admission control failure

OL -- no outgoing label IB -- TDM incompatible bitrate

NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration

BK -- Backup Connection ST -- Standby Connection

CB -- rcvd cell-bundle size bad SP -- Static Pseudowire

LD -- local site signaled down RS -- remote site standby

RD -- remote site signaled down XX -- unknown

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 10.0.0.4

Interface Type St Time last up # Up trans

ge-0/0/7.0(vc 10) rmt Up Nov 24 15:37:03 2015 1

Remote PE: 10.0.0.4, Negotiated control-word: Yes (Null)

Incoming label: 299776, Outgoing label: 299776

Negotiated PW status TLV: No

Local interface: ge-0/0/7.0, Status: Up, Encapsulation: ETHERNET

root@srx04# run show l2circuit connections

Layer-2 Circuit Connections:

Legend for connection status (St)

EI -- encapsulation invalid NP -- interface h/w not present

MM -- mtu mismatch Dn -- down

EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down

CM -- control-word mismatch Up -- operational

VM -- vlan id mismatch CF -- Call admission control failure

OL -- no outgoing label IB -- TDM incompatible bitrate

NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration

BK -- Backup Connection ST -- Standby Connection

CB -- rcvd cell-bundle size bad SP -- Static Pseudowire

LD -- local site signaled down RS -- remote site standby

RD -- remote site signaled down XX -- unknown

Legend for interface status

Up -- operational

Dn -- down

Neighbor: 10.0.0.5

Interface Type St Time last up # Up trans

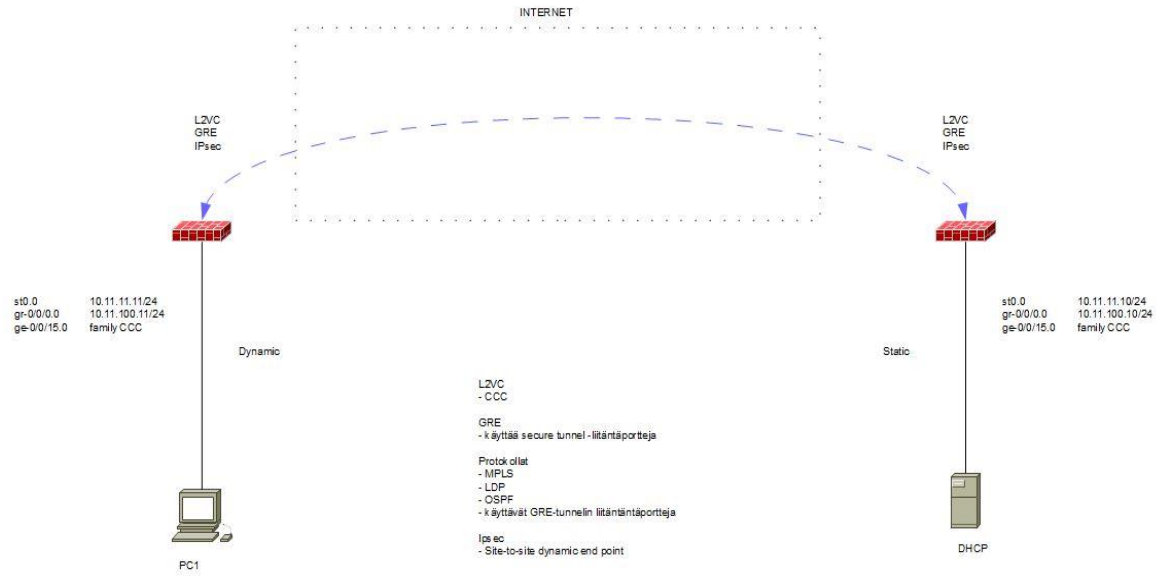
ge-0/0/15.0(vc 10) rmt Up Nov 24 06:08:06 2015 1

Remote PE: 10.0.0.5, Negotiated control-word: Yes (Null)

Incoming label: 299776, Outgoing label: 299776

Negotiated PW status TLV: No

Local interface: ge-0/0/15.0, Status: Up, Encapsulation: ETHERNET



Kuva 7: L2 Circuit over MPLS over GRE over IPsec

7 YHTEENVETO

Yhteenvedossa käydään läpi tuloksia ja havaintoja testatuista asioista. Työläin vaihe opinnäytetyössä oli suunnittelu ja toteutustapojen ymmärtäminen. Suurin osa ajasta kului suunnitteluun ja toteutustapojen pohdintaan. Konfiguraation tekeminen oli nopein vaihde työssä, mutta tehtävien toteutusten sisäistäminen vei aikaa.

7.1 Yleistä

Toteutukset toimivat lopulta hyvin. Tärkeintä oli huomioida muuttuvat tekijät eri toteutuksissa. Tärkeää oli myös koota tarvittavat asiat yhdeksi kokonaisuudeksi, jota lähdettiin toteuttamaan. Erityisesti asioiden suunnittelu ja pohdinta auttoivat havaitsemaan kokonaisuuksia paremmin.

Virtual Leased Line –protokollan voisi kuvitella loogisena kaapelina MPLS-verkon reunalta reunalle. *Virtual Private LAN Service* –protokollan voisi kuvi-

tella loogisena lähiverkkona MPLS-verkon sisällä. *Virtual Private LAN Service* –protokollan voisi myös kuvailla yhtenä loogisena kytkimenä, jossa jokainen VSI (Virtual Switching Instance) olisi kytkimen porttina.

7.2 L2VPN-tiedonsiirtotiet

Helpoin implementoitava toteutus oli VLL Martini -moodi, koska se oli suoraan verrattavissa aikaisemmin opiskelun yhteydessä tutustumaani Ciscon *xconnect ethernet over MPLS*- tekniikkaan. Siinä luotiin *point-to-point* linkki kahden reunan välille. VLL-tekniikka käyttää LDP- ja OSPF-protokollia löytääkseen reitin MPLS-pilvessä.

VPLS Martini –moodi oli myös helppo implementoida, koska se käyttää myös LDP- ja OSPF-protokollia reititykseen MPLS-pilven sisällä. VPLS Martini -moodin avulla pystytään luomaan monia eri päätepisteitä yhdelle lähtöpisteelle. Tekniikka tunnetaan *point-to-multipoint* termillä. VPLS Martini -moodi toimii yksinkertaisuudessaan tunnistautumismenetelmällä, jossa jokaiselle alueen jäsenelle annetaan sama tunnistetieto, jolla alueet yhdistyvät.

Molemmat VLL Martini -moodi ja VPLS Martini -moodi voidaan toteuttaa suoraan liitäntäporttiin tai VLAN-liitäntään. Molemmissa toteutuksissa voidaan myös manipuloida VLANin sisällä olevia VLANeja. Toteutuksissa voidaan myös olla ottamatta kantaa VLANin sisältöön tai liitäntäportin sisältöön.

Toteutuksina VLL Martini -moodi ja VPLS Martini -moodi ovat käytännöllisiä, koska ne ovat yleisesti tunnettuja tekniikkoja, joita käytetään ympäri maailmaa. Yhteensopivin L2VPN oli kuitenkin *Virtual Leased Line*, koska se ei tarvitse BGP-protokollaa signaloitumiseen Juniper Networks SRX -sarjan palomuurissa.

Tärkeimpinä asioina olivat eri L2VPN-tiedonsiirtoteiden toimintakuntoon saaminen. Tavoitteisiin päästiin ja löydettiin eri tapoja hyödyntää L2VPN-tiedonsiirtoteitä. Tarkastelussa olivat erityisesti pienille yrityksille tarkoitetut ratkaisut ja mahdollinen laajennusvara kasvulle.

7.3 IPsec VPN -tiedonsiirtotiet

IPsec VPN -toteutukset olivat alussa haastavia, koska perustieto kyseisistä toteutuksista oli puutteellinen. IPsec VPN -toteutukset vaativat tarkkaa ja täsmällistä tunnistetietojen asettelua. Juniper Networksin palomuureissa IPsec

VPN -mahdollisuuksia on useita, mutta päädyimme käyttämään *route-based* IPsec VPN -siirtoteitä. Niiden avulla pystytään reitittämään joko staattisilla reiteillä tai dynaamisella reititysprotokollalla useampia verkkoja IPsec VPN -siirtotien lävitse.

Tärkeimpänä asiana oli ymmärtää IPsec VPN:n toimintaperiaate ja hyödyntämismahdollisuudet. IPsec VPN- tiedonsiirtotie toimii kahdessa vaiheessa. Ensimmäisessä vaiheessa palomuurit vaihtavat sovitut tunnistetiedot keskenään. Seuraavassa vaiheessa muodostetaan suojattu tiedonsiirtotie palomuurien välille. Palomuureissa tiedonsiirtotien liitäntäportit tunnetaan nimellä *secure tunnel interface* (st0.0).

Tärkeä ymmärrettävä asia oli myös tajuta erot palomuurien välillä IPsec VPN -tiedonsiirtotietä tehdessä. Huomioitavaa oli kumpi palomuuri avaa suojatun yhteyden. Toteutuksissa käytettiin yhtä palomuuria, jolle annettiin kiinteä staattinen IP-osoite ja toiset palomuurit saivat osoitteensa dynaamisesti LTE-reitittimeltä. Tässä tilanteessa oli tunnistautuminen suoritettava joko *hostnamen* tai *user@hostnamen* avulla.

L2 Circuit over MPLS over GRE over IPsec -toteutuksessa muodostettiin L2-tason silta LTE-verkon ylitse. Pohjana toteutuksessa toimi *route-based* IPsec VPN. GRE toimi toteutuksessa tiedonsiirtotienä, jossa eri protokollat kommunikoivat keskenään. Reititystä varten käytettiin LDP- ja OSPF-protokollia. Toteutuksessa jouduttiin nostamaan fyysisten liitäntäporttien MTU arvoa 1600 ja GRE-tiedonsiirtotien liitäntäporttien MTU arvoa 9000, jotta paketit mahtuivat kulkemaan tiedonsiirtotietä pitkin. *Secure tunnel*-liitäntäporttien MTU arvo on oletuksena 9192.

Lopputuloksena pystyttiin lähettämään L2-sillan kautta sama yksityinen verkko palomuurilta toiselle ja toteutus toimi hyvin. Toteutuksen läpi toimi DHCP-palvelin. Eli ensimmäisen palomuurin porttiin liitettiin verkko, jossa toimi DHCP-palvelin ja toisen palomuurin porttiin liitettiin kannettava ja kannettava sai osoitteen L2-sillan ylitse.

8 LOPPUPÄÄTELMÄT

Loppupäätelmissä käydään läpi yhteenvedon asioita L2VPN-tiedonsiirtoteistä, IPsec VPN –tiedonsiirtoteistä. Loppupäätelmissä pohditaan myös omia kokemuksia tehdystä opinnäytetyöstä sekä mahdollista jatkokehitystä työlle. Huo-

mioitavia asioita ovat myös eri testattavien toteutusten toiminta tuotantoverkossa.

8.1 Yleistä

Toteutukset toimivat yleisesti odotetulla tavalla. Ongelmatilanteita aiheuttivat suurimmaksi osaksi inhimilliset virheet ja ajatusvirheet. Ongelmatilanteista kuitenkin opittiin paljon. Työssä helpoimmat osuudet olivat konfiguraatioiden tekeminen ja laitteiden asentaminen. Konfiguraatiot ovat pitkälti samankaltaisia kuin ajatusketjussa suunniteltu toteutus. Laitteiden asentaminenkaan ei tuottanut ongelmia, koska laitteille määriteltiin tietty paikka laitetelineessä ja varattiin tarvittava määrä kytkentäkuitua tai kytkentäkaapelia sekä varattiin tarvittavat moduulit portteihin. Haasteita työssä tuotti asioiden selvittäminen ja oikean ratkaisun löytäminen ongelmatilanteeseen. Tietoverkoissa ilmenevät ongelmat eivät ole läheskään aina yksiselitteisiä.

8.2 L2VPN & IPsec VPN -tiedonsiirtotiet

L2VPN-tiedonsiirtoteissä saatiin toimimaan *Virtual Leased Line* –protokolla, *Virtual Private LAN Service* –protokolla ja *L2 Virtual Circuit* –protokolla. Yhteensopivin protokollista oli Virtual Leased Line –protokolla. Virtual Leased Line –protokolla toimi Juniper SRX-sarjan palomuurin L2VC-protokollan kanssa. *Virtual Private LAN Service* –protokolla olisi toiminut myös, mutta Juniper SRX –sarjan palomuurien käyttämä Junos-käyttöjärjestelmä vaatii BGP-signaloinnin. Tarkoituksena opinnäytetyössä oli käyttää vain OSPF-protokollaa.

QinQ-toteutuksessa käytimme *Virtual Private LAN Service* –protokollaa, koska yhteyksiä oli useita. Kyseisellä protokollalla pystyttiin niputtamaan halutut CVLANit SVLANin sisälle. Tämä on yleinen tapa palveluntarjoajan verkossa. Tällä tavoin toteutus pysyi järkevänä kokonaisuutena. *L2 Virtual Circuit* –protokolla toimi Juniper SRX –sarjan palomuurien kesken ja L3-tasoisen kytkimen *Virtual Leased Line* –protokollaa vasten. *L2 Virtual Circuit* –protokolla tarvitsi signaloitumiseen MPLS-verkossa OSPF-protokollaan, joten kyseinen L2 Virtual Circuit –protokolla sopi hyvin toteutuksiin.

IPsec VPN -tiedonsiirtotiet toimivat oletetusti. Saimme testattua ja otettua käyttöön *route-based* IPsec VPN –tiedonsiirtotien palomuurien välille. Sen avulla pystyttiin reitittämään useampi verkko, joko staattisesti tai dynaamisesti,

tiedonsiirtotien sisällä. SRX-sarjan palomuurien IPsec VPN –siirtotien hyvänä puolena on varmuus siitä, että tiedonsiirtotie toimii varmasti.

8.3 Kehitys ja oma näkemys opinnäytetyöstä

Opinnäytetyö tarjoaa mahdollisuuksia jatkaa L2VPN-tiedonsiirteiden IPsec VPN -tiedonsiirtoteiden tutkimista operaattoriverkossa. Martini-moodi skaalautuu hyvin pienelle palveluntarjoajalle. Toteutuksia pystytään myöskin laajentamaan tarvittaessa.

Työtä tehdessä opin havainnoimaan asioita eri näkökulmista. Tärkein opittu asia oli hahmottaa syy ja seuraus konfiguraatioita ja liitäntöjä tehdessä. Oikeaan palveluntarjoajan verkkoon tutustuminen ja verkon toiminnan ymmärtäminen olivat myös avaintekijöitä opinnäytetyössä.

Kohokohtina työssä olivat verkkojen yliheittäminen ja yliheittoon valmistautuminen. Valmistautumisessa täytyi ottaa paljon asioita huomioon. Yliheiton tehtävälistan tuli olla yksiselitteinen, koska pienetkin virheet aiheuttavat paljon ajanhukkaa. Yliheittoon on varattu aina tietty huoltoikkuna eli tietty tuntimäärä asioiden toteuttamiseen. Kokonaisuudessaan työ oli mielenkiintoinen toteuttaa.

LÄHTEET

Apcar, J. Cisco Systems, Inc. 2006. An Introduction to VPLS. Powerpoint-esitys. Saatavissa: http://stor.balios.net/Divers/VPLS_Introduction.ppt [viitattu 12.10.2015]

Cameron, R. & Woodberg, B. 2013. O'Reilly Media, Inc. 2013. Juniper SRX Series. O'Reilly Atlas. Verkkojulkaisu. Saatavissa: http://chimera.labs.oreilly.com/books/1234000001633/index.html [viitattu 12.10.2015]

Cameron, R., Eberhard, T., Giecco, P., Quinn, J. & Woodberg, B. Juniper Networks, Inc. 2010. Junos Security. O'Reilly Media. Verkkojulkaisu. Saatavissa: http://subnets.ru/books/Junos_Security.pdf [viitattu 12.10.2015]

Darukhanawalla, N. & Bellagamba, P. 2009. Interconnecting Data Centers Using VPLS. Indianapolis: Cisco Press.

Hangzhou H3C Technologies Co. 2008. VPLS Technology White Paper. Verkkojulkaisu. Saatavissa: http://www.h3c.com.hk/products___solutions/technology/mpls/technology_white_paper/200804/602787_57_0.htm#_Toc189456057 [viitattu 12.10.2015]

Huawei Technologies Co., Ltd. 2012. VLL Technology White Paper. Verkkojulkaisu. Saatavissa: http://www.utopiatechnology.co.uk/UserFiles/Docs/Huawei/Switching/Whitepapers/VLL%20Technology%20White%20Paper.pdf [viitattu 12.10.2015]

Juniper Networks, Inc. 2014a. Configuring Branch SRX Series for MPLS over IPsec (1500-byte MTU). Verkkojulkaisu. Saatavissa: https://www.juniper.net/techpubs/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-140-srx-for-mpls-over-IPSec-1500byte-mtu-configuring.pdf [viitattu 12.10.2015]

Juniper Networks, Inc. 2014b. Understanding Generic Routing Encapsulation. Verkkojulkaisu. Saatavissa: http://www.juniper.net/documentation/en_US/junos13.2/topics/concept/gre-tunnel-services.html [viitattu 30.11.2015]

Juniper Networks, Inc. 2015. Configuring VPLS over GRE with IPsec VPNs. Verkkojulkaisu. Saatavissa:http://www.juniper.net/techpubs/en_US/junos15.1x49/topics/example/vpls-over-gre-ipsec.html [viitattu 12.10.2015]

Kamichoff, M. 2012. L2VPN over MPLS over GRE over IPsec on a Juniper SRX. Verkkojulkaisu. Saatavissa: http://prolixium.com/blog?id=976 [viitattu 12.10.2015]

O'Connor, D. 2014. L2VPN on Junos using CCC/Martini/Kompella. Verkkojulkaisu. Saatavissa: https://mellowd.co.uk/ccie/?p=4428 [viitattu 12.10.2015]