KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Riku Oinonen

MPLS L2VPN ja operaattoriverkon kahdennetut palvelut

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

OINONEN, RIKU	MPLS L2VPN ja operaattoriverkon kahdennetut palvelut
Opinnäytetyö	52 sivua + 10 liitesivua
Työn ohjaaja	yliopettaja Martti Kettunen
Toimeksiantaja	KYMP Oy, SimuNet-hanke
Maaliskuu 2011	
Avainsanat	SimuNet, MPLS, VPN, L2VPN, VPLS, EoMPLS

Nykyään yritykset ostavat entistä enemmän tietoverkkoratkaisuja palveluna verkko-operaattorilta. Näiden palveluiden tarjoaminen riittävän korkealla saatavuudella ajaa verkko-operaattoreita verkkojen virtualisointiin ja järjestelmien kahdentamiseen maantieteellisesti erilleen sijoitettuihin laitetiloihin.

Kymenlaakson ammattikorkeakoulun tiloissa toimii tietoverkkopalveluiden testaus- ja kehitysympäristö nimeltä SimuNet. SimuNet-verkko simuloi nykyaikaisen verkko-operaattorin tuotantoverkkoa useine laitetiloineen ja virtualisointia hyödyntävine järjestelmineen. SimuNet-verkkoon oli asennettu HA-palvelinklusteri ja sen edustapalomuurit, jotka on kahdennettu eri laitetiloihin. Tämän työn tarkoituksena oli toteuttaa näitä järjestelmiä varten tarvittavat yhteydet SimuNetin eri laitetilojen välille, jotta niiden tarjoama toiminnallisuus saadaan käyttöön. Lisäksi verkkoon oli tarkoitus toteuttaa valmiiksi vastaavat yhteydet myös verkkoon tulossa olevia kahdennettuja WLAN-ohjaimia varten.

Tarvittavat yhteydet toteutettiin VPLS- ja EoMPLS–palveluiden avulla. Ne molemmat ovat Layer 2 –tasolla toimivia virtuaalisia lähiverkkopalveluita. Näiden palveluiden avulla SimuNetin laitetilojen lähiverkkoja voitiin virtuaalisesti jatkaa Layer 2 –tasolla, niiden välissä sijaitsevan pakettikytkentäisen IP/MPLS-runkoverkon yli. Työn alussa kerrotaan teoriaa käytetyistä protokollista ja sen jälkeen SimuNet-verkkoon toteutetut ratkaisut esitetään laitteiden konfiguraatioiden kera.

Tuloksena SimuNetin HA-palvelinklusteri ja palomuurit saatiin tuotua toimintakuntoon ja myös kahdennettuja WLAN-ohjaimia varten saatiin luotua valmius odottamaan niiden lisäämistä verkkoon. VPLS- ja EoMPLS-palvelut todettiin tehokkaiksi ratkaisuiksi toteuttaa kahdennettujen järjestelmien tarvitsemat yhteydet pakettikytkentäisen verkon yli, ja ne on helppo ottaa käyttöön, jos IP/MPLS-verkko on jo olemassa.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

OINONEN, RIKU	MPLS L2VPN and Redundant Carrier Services
Bachelor's Thesis	52 pages + 10 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	KYMP Oy, SimuNet Project
March 2011	
Keywords	SimuNet, MPLS, VPN, L2VPN, VPLS, EoMPLS

Today, companies are buying more and more network solutions as a service from their network operators. Providing such services with sufficient availability drives network operators to virtualization, and to duplicating their systems in geographically separate equipment rooms.

In the premises of Kymenlaakso University of Applied Sciences there operates a data network testing and development environment called SimuNet. The SimuNet network simulates the production network of a modern network operator, with several equipment rooms and virtualized systems. High-availability cluster and its representative firewalls had already been installed in SimuNet network with their physical equipment are duplicated in geographically separate equipment rooms. The purpose of this work was to implement necessary connections between the equipment rooms for those redundant systems so that the functionality what they offer would become available. In addition, similar connections were also premade for the duplicated WLAN controllers to wait for their upcoming installation to the SimuNet network.

Necessary connections were made by using EoMPLS and VPLS services. They both are virtual private network services that offer Layer 2 connectivity over packet switched networks. Using these services, it was possible to virtually extend local area networks from one equipment room to another over the IP/MPLS network, which lies between them. At the beginning of this work, the used protocols are explained theoretically, and then the solutions implemented for SimuNet network are presented with all the necessary configurations.

As a result of this work, SimuNet's high-availability cluster and firewalls are now fully functional and there is network readiness waiting for the installation of the WLAN controllers. VPLS and EoMPLS services were found to be effective solutions to implement the required connections for redundant carrier services over packet switched network, and they are easy to deploy, if the IP/MPLS network is already available.

SISÄLLYS

LYHENNELUETTELO

BGP	Border Gateway Protocol; *Autonomisten alueiden välinen reititysprotokolla*
DHCP	Dynamic Host Configuration Protocol; *Verkkoon kytkeytyville laitteille osoitetietoja jakava protokolla*
EAKR	Euroopan aluekehitysrahasto
EoMPLS	Ethernet over MPLS; *Tunnelointitekniikka Ethernet-kehysten kuljettamiseen MPLS-verkon yli*
FEC	Forwarding Equivalance Class; *Ryhmä paketteja, joita kohdellaan MPLS-verkossa yhdenmukaisesti*
HSRP	Hot Standby Router Protocol; *Redundanttisen oletusyhdyskäytävän tarjoava protokolla*
H-VPLS	Hierarchical VPLS; *Hierarkinen versio VPLS-palvelusta*
iBGP	Internal BGP; *Autonomisen alueen sisäinen BGP-reititys*
IETF	The Internet Engineering Task Force; *Internet-protokollien standardoinnista vastaava organisaatio*
IGP	Interior Gateway Protocol; *Yleisnimitys autonomisen alueen sisällä toimivista reititysprotokollista*
IOS	Internetwork Operating System; *Cisco Systemsin kytkin- ja reititinlaitteiden käyttöjärjestelmä*
IPv4	Internet Protocol version 4; *Internet-protokollan versio 4*
IPv6	Internet Protocol version 6; *Internet-protokollan versio 6*
iSCSI	Internet Small Computer System Interface; *IP-verkon yli toimiva verkkolevyjärjestelmä*

LDP	Label Distribution Protocol; *Protokolla lipputietojen vaihtoon MPLS-verkossa*
LER	Label Edge Router; *MPLS-verkon reunalaite*
LIB	Label Information Base; *MPLS-verkon laitteiden ylläpitämämä tietokanta lippumerkinnöistä*
LSP	Label Switched Path; *Polku, jota pitkin paketit kulkevat MPLS-verkossa*
LSR	Label Switch Router; *MPLS-verkon runkolaite*
MAC-osoite	Media Access Control; *Ethernet-verkon laitteita yksilöivä Layer 2 –tason osoite*
MPLS	Multiprotocol Label Switching; *Lippumerkintöihin perustuva pakettien kytkentätekniikka*
MTU	Maxium Transmission Unit; *Suurin paketti, joka voidaan välittää eteenpäin kokonaisena*
OSPF	Open Shortest Path First; *Autonomisen alueen sisäinen reititysprotokolla*
P-laite	Provider; *Operaattoriverkon runkolaite*
PE-laite	Provider Edge; *Operaattoriverkon reunalaite*
QoS	Quality of Service; *Palvelun laatu*
SVI	Switch Virtual Interface; *Virtuaalinen portti, joka edustaa yhtä VLAN-aluetta*
VLAN	Virtual Local Area Network; *Virtuaalinen lähiverkko*
VPLS	Virtual Private LAN Service; *Tekniikka Ethernet-kehysten kuljettamiseen ja kytkemiseen MPLS-verkon yli*

1 JOHDANTO

Tietoverkoista ja Internetistä on niiden kasvun myötä tullut myös erittäin tärkeä osa yritysmaailmaa. Tieto on tallennettu verkkoon ja suurilla yrityksillä on monia toimipisteitä yhteydessä toisiinsa. Sen sijaan että yritykset itse kehittäisivät ja ylläpitäisivät omia järjestelmiään ja verkkojaan, pyritään useat tietoverkkoratkaisut nykyään ostamaan palveluna verkko-operaattorilta. Suuret asiakasmäärät ja palveluna myytävät toiminnot ajavat verkko-operaattoreita laitteiden ja verkkoinfrastruktuurin virtualisointiin. Virtualisoinnin avulla tarvittavien laitteiden lukumäärää voidaan vähentää ja se mahdollistaa esimerkiksi lähiverkkojen jatkamisen virtuaalisesti verkko-operaattorin pakettikytkentäisen runkoverkon yli. Lähiverkon jatkaminen runkoverkon yli voi jo itsessään olla asiakasyritykselle myytävä palvelu, mutta verkko-operaattori voi käyttää niitä myös hyödyksi muiden tarjoamiensa palveluiden tuottamiseen ja kuljettamiseen asiakkaan luokse.

Yritykset osaavat myös nykyään vaatia verkko-operaattorilta hyvin korkeaa saatavuutta, eli verkon ja sen palveluiden tulisi olla lähes katkottomasti saatavilla (Kettunen 2009, 5). Verkon laitteet ovat kuitenkin alttiita laite- ja ohjelmavioille, sähkönsyöttöhäiriöille ja muille, niiden toiminnan estäville ongelmatilanteille. Virtualisoiduissa verkoissa verkon laitteiden redundanttisuus kohoaa entistä tärkeämpään asemaan, kun yhden fyysisen laitteen hajoaminen saattaa aiheuttaa koko asiakaskuntaa koskevia ongelmia. Tämän takia tärkeä osa virtualisoidun verkon saatavuutta parannettaessa on laitteiden kahdentaminen. Laitteiden kahdennuksella mahdollistetaan niiden katkoton tai lähes katkoton toiminta myös tilanteissa, joissa toinen laitteista vikaantuu. Kahdennusratkaisuissa, joissa kahdennetun laitteen molemmat osapuolet halutaan pitää aktiivisina, tarvitaan laitteiden virtualisointia myös itse kahdennuksen toteutukseen.

Verkko-operaattorin tarjoamille palveluille riittävää saatavuutta tavoiteltaessa on kuitenkin otettava huomioon myös suuremmat kuin yhtä laitetta koskevat uhat. Tällaisia uhkia ovat esimerkiksi sähkönsyötön tai ilmastoinnin pettäminen, tulipalo tai tulva. Nämä koskevat kokonaisia laitetiloja, joten verkon palvelujen turvaaminen myös tällaisissa uhkatilanteissa vaatii kahdennettujen laitteiden sijoittamisen maantieteellisesti toisistaan erilleen. Toimiakseen täytyy aktiivisesti kahdennetut laitteet kuitenkin usein sijoittaa samaan verkon Layer 2 -segmenttiin. Lähiverkkoja on siis jatkettava maantie-

teellisesti erillään sijaitsevien laitetilojen välillä. Tämä on mahdollista tehdä esimerkiksi varaamalla kuidusta dedikoitu kanava, jonka kautta lähiverkot laajennetaan laitetilojen välille, tai kuten tässä työssä, jatkamalla lähiverkkoja virtuaalisesti yhteisen pakettikytkentäisen verkon yli. Nämä Layer 2 -tason virtuaaliset lähiverkkopalvelut tunnetaan nimellä L2VPN (Layer 2 Virtual Private Network).

Alustana työn käytännön toteutuksille toimii Kymenlaakson ammattikorkeakoulun ja alueellisten yritysten yhteinen testi- ja T&K-ympäristö, SimuNet. Verkkolaitteina SimuNetissä käytetään lähes kokonaan Cisco Systemsin laitteistoa, ja siksi tässä työssä esiintyvä termistö on osaltaan Cisco Systemsin omaa sanastoa.

2 TYÖN RAJAUS JA LÄHTÖTILANNE

Työssä on tarkoitus tutustua MPLS-verkon L2VPN -tekniikoihin ja hyödyntää niitä operaattoriverkon sisäisessä toiminnassa kahdennettujen palveluiden tarpeisiin. Työssä käytetään EoMPLS- ja VPLS-ratkaisuja, joiden avulla lähiverkkoja jatketaan SimuNetin laitetilojen välillä, niiden välissä sijaitsevan IP/MPLS-runkoverkon yli. Työtä tehdessä pyritään pitämään mielessä myös palvelujen saatavuus, toteuttamalla ratkaisut niin ettei SimuNet-verkkoon jäisi yhden pisteen vian mahdollisuutta.

Työtä aloittaessa SimuNetin runkoverkko koostui kahdesta P- ja PE-laitteesta ja niiden välinen IP/MPLS-verkko oli jo toimintakunnossa. SimuNetiin oli asennettu HA-palvelinklusteri sekä kahdennetut palomuurit palvelimien liikennettä varten. Näiden järjestelmien tarvitsemia yhteyksiä ei kuitenkaan runkoverkkoon ollut luotu, joten ne eivät vielä tuoneet toiminnallisuutta SimuNetiin. Tässä työssä on tarkoitus liittää nämä palvelut SimuNet-verkkoon luomalla niiden tarvitsemat Layer 2 -tason yhteydet virtuaalisesti SimuNetin laitetilojen välille. Työn ohessa SimuNetin runkoverkkoa on tarkoitus laajentaa ottamalla mukaan uusia PE-laitetta. Lisäksi SimuNetiin on tulossa kahdennetut WLAN-ohjaimet, joita varten luodaan valmius toteuttamalla niiden vaatimat Layer 2 –tason yhteydet valmiiksi verkkoon.

Työn alussa esitetään teoriaa työhön liittyvistä protokollista, sen jälkeen esitellään SimuNet-verkko ja siihen tehdyt käytännön toteutukset näyttämällä verkon laitteisiin tehdyt konfiguraatiot vaihe vaiheelta. Työssä keskitytään kokonaan Layer 2 –tason VPN-ratkaisuihin ja Layer 3 –tason VPN-ratkaisut on rajattu työstä pois, vaikka myös ne ovat tärkeä osa tämän päivän operaattoriverkkojen virtualisointia.

3 MULTIPROTOCOL LABEL SWITCHING (MPLS)

MPLS on yleisesti käytetty protokolla liikenteen kuljettamiseen runkoverkoissa. Tässä työssä käsitellään RFC 3031 -dokumentin määrittelemää MPLS/IP -tekniikka, eli Layer 3 -tason protokollana käytetään IP-protokollaa.

3.1 Yleistä

MPLS on protokolla, joka yhdistää kytkentäisten verkkojen suorituskyvyn ja reititettyjen IP-verkkojen skaalautuvuuden (Darukhanawalla & Bellagamba 2009, 19). Erona puhtaisiin IP-verkkoihin, MPLS mahdollistaa liikenteen välittämisen verkon läpi ilman, että se on reititettävä jokaisella hypyllä. Keskeinen ominaisuus MPLS-verkoissa on myös mahdollisuus tunneloida eri protokollien liikenne ja kuljettaa ne saman verkkoinfrastruktuurin yli. Tunnelointi on tehokas työkalu, sillä vain verkon reunalaitteiden tarvitsee osata käsitellä liikenne sen natiivimuodossaan. Muut verkon laitteet vain välittävät liikennettä, eikä niiden tarvitse ymmärtää tunnelien sisällä kulkevaa liikennettä. (Minei & Lucek 2008, 6.)

3.2 MPLS-verkon toiminta

Normaalissa IP-verkossa saapuvan paketin Layer 3 –otsikko tutkitaan ja paketin reitittämiseen liittyvien kenttien perusteella selvitetään seuraavan hypyn IP-osoite. Kaikkein tavanomaisimmassa tapauksessa ainoa merkityksellinen kenttä otsikkotiedoissa on kohde IP-osoite, mutta joissain tapauksissa myös muut kentät ovat merkityksellisiä. IP-reitityksessä Layer 3 –otsikko täytyy analysoida jokaisessa reitittimessä, jonka läpi paketti kulkee.

MPLS-verkossa IP-paketin Layer 3 -otsikko analysoidaan vain kerran ja sen jälkeen sille annetaan lukuarvo, jota kutsuntaan lipuksi (label). Reitittimissä matkan varrella reitityspäätökset tehdään perustuen tähän lippumerkintään. Lippu on linkkikohtainen ja ennen liikenteen edelleenvälittämistä MPLS-verkon reitittimet voivat tarvittaessa lisätä, poistaa tai uudelleenkirjoittaa lipun seuraavaa linkkiväliä varten. (Darukhanawalla & Bellagamba 2009, 19-20.) MPLS ei kuitenkaan poista muiden reititysprotokollien tarvetta, sillä normaali IP-reititys vaaditaan edelleen toimimaan taustalle.

MPLS-verkko koostuu reunalaitteista, jotka tunnetaan LER- tai PE-laitteina, ja runkolaitteista, jotka tunnetaan LSR- tai P-laitteina. PE-laitteiden välille muodostetaan verkosto yksisuuntaisia Label Switched Paths (LSP) –polkuja, joita pitkin liikenne kulkee. PE-laitteen vastaanottaessa liikennettä MPLS-verkon kuljetettavaksi, ensimmäiseksi se määrittää, mihin Forwarding Equivalence Class (FEC) -ryhmään liikenne kuuluu. Kaikki samaan FEC-ryhmään kuuluva liikenne kulkee samaa LSP-polkua pitkin vastaanottavalle laitteelle. MPLS lippumerkintä kertoo, mihin FEC-ryhmään liikenne kuuluu, ja se lisätään mukaan liikenteeseen ennen sen välittämistä MPLS-verkon kuljetettavaksi. P-laitteet LSP-polun varrella tekevät vain liikenteen edelleenvälittämistä kytkemällä liikennettä perustuen pakettien lippumerkintään. P-laite lukee paketin mukana kulkevan lippumerkinnän sekä sen perusteella valitsee oikean lipun käytettäväksi seuraavalle hypylle ja ohjaa liikenteen ulos oikeasta portista. (Minei & Lucek 2008, 6-8.)

3.3 MPLS-otsikko

Ennen liikenteen välittämistä MPLS-verkon kuljetettavaksi PE-laite enkapsuloi liikenteen MPLS-paketiksi. MPLS-enkapsuloinnissa paketin Layer 2 ja Layer 3 –kehyksen väliin lisätään 32 bitin pituinen MPLS-otsikko (ks. kuva 1).

Kuva 1. MPLS-otsikkon rakenne (Minei & Lucek 2008, 7)

MPLS-otsikko koostuu neljästä kentästä. Alussa on 20 bitin pituinen lippumerkintä, jonka perusteella paketteja kytketään. EXP (Experimental) -kenttä on 3 bitin pituinen, ja sitä hyödynnetään QoS-priorisoinnin yhteydessä. MPLS-otsikoita voidaan pinota päällekkäin, sen takia mukana otsikossa kulkee S-bitti, joka kertoo onko kyseessä pinon alimmainen otsikko. Viimeistä TTL-kenttää käytetään estämään, ettei paketti jää pyörimään silmukkaan loputtomiksi ajoiksi. Jokaisella hypyllä reititin vähentää tämän kentän arvoa yhdellä ja paketti pudotetaan pois verkosta, jos kentän arvo laskee nollaan. MPLS-verkon yli siirrettävällä liikenteellä on aina yksi tai useampi MPLS-otsikko. (Minei & Lucek 2008, 7.)

Jossain tapauksissa, kuten julkisen IP-liikenteen kuljettamisessa MPLS-verkon läpi, yksi MPLS-otsikko on riittävä. Perille päästyään liikenteen Layer 3 –otsikko tutkitaan ja paketti reititetään eteenpäin tavanomaisen IP-reitityksen keinoin. Kuitenkin esimer-

kiksi VPN-palveluita MPLS-verkon päällä ajettaessa PE-laitteilla täytyy olla tieto, mihin palveluun ja mihin sen palvelun instanssiin vastaanotettu liikenne kuuluu. Tämä tieto voidaan kuljettaa liikenteen mukana lisäämällä toinen MPLS-otsikko mukaan paketteihin. Päällimmäistä lippua käytetään liikenteen ohjaamiseen oikealla PE-laitteelle ja alempaa lippua käytetään palvelujen erotteluun. (Minei & Lucek 2008, 8.)

3.4 Label Distribution Protocol (LDP)

Label Distribution Protocol (LDP) -protokollan avulla MPLS-verkon laitteet sopivat lippujen merkityksestä. LDP on yksi yleisimmistä protokollista MPLS-verkon signalointiin, muttei ainoa (Minei & Lucek 2008, 11). LDP-protokollan avulla jokainen laite jakaa paikallisesti määritellyt lippumerkinnät muille laitteille ja ylläpitää LIB Label Information Base (LIB) –taulua, johon tiedot lippumerkintöjen merkityksistä tallennetaan.

LDP-prokolla ei itse yritä suorittaa reititystoimintoja, vaan nojaa IGP-reititysprotokollan toimintaan reitityksen liittyvissä päätöksissä. LSP-polut noudattavat käytössä olevan IGP-protokollan ilmoittamia lyhyimpiä reittejä ja mukautuvat verkon mukaan, jos IGP:n reittitiedot muuttuvat. (Minei & Lucek 2008, 11-13.)

Lippumerkintöjen vaihto tapahtuu LDP-istunnon avulla. LDP-istunto on aina kaksisuuntainen. LDP-käyttää viestien välittämiseen LDP PDU -paketteja, jotka välitetään käyttäen UDP- ja TCP-protokollaa. LDP-tarvitsee siis toimiakseen IP-yhteyden laitteiden välille. LDP PDU -paketti koostuu LDP-otsikosta ja sitä seuraa yksi tai useampi LDP-viesti, joiden avulla laitteet keskustelevat. (Luo, Pignataro, Bokotey & Chan 2005, 116.)

4 MPLS L2VPN

MPLS L2VPN –palvelut mahdollistavat Layer 2 –tason liikenteen kuljettamisen IP/MPLS-runkoverkon yli. Liikenne kuljetetaan PE-laitteiden välille muodostettujen virtuaalisten Pseudowire-linkkien sisällä. Tärkeimpänä ominaisuutena tämän työn kannalta Ethernet-lähiverkkoja voidaan laajentaa Pseudowire-emulointiin perustuvien tekniikoiden avulla IP/MPLS-verkon yli.

4.1 Yleistä

Natiiveja Layer 2 -tason palveluita, kuten Frame Relay tai ATM, on ollut käytössä jo useita vuosia ja usein näitä palveluita on käytetty yhdistämään yritysten toimipisteitä toisiinsa. MPLS L2VPN -palveluiden avulla operaattorit voivat siirtää nämä palvelut kuljetettavaksi MPLS-verkon yli. Palveluiden siirtäminen MPLS-verkkoon säästää kustannuksissa, kun Layer 2 ja Layer 3 -tason palvelut voidaan kuljettaa samassa runkoverkossa yksilöityjen verkkojen sijasta. Asiakkaan näkökulmasta tällainen migraatio on täysin läpinäkyvä. (Luo, Pignataro, Bokotey & Chan 2005, 8-11.)

Kasvava palvelu, jota halutaan kuljettaa MPLS-verkon yli, on Ethernet. Ethernet kiinnostaa tekniikkana sen tarjoaman suuren nopeuden ja alhaisen hinnan takia. Nykyään käytännössä kaikki lähiverkot alkavat olla Ethernet-verkkoja. Ethernet-tekniikan kuljettaminen myös WAN-verkon yli VPN-palveluna on luonnollinen valinta, koska tällöin voidaan samaa tekniikkaa käyttää verkon päästä päähän. (Minei & Lucek 2008, 314.) MPLS L2VPN –palveluiden avulla verkon yhtä Ethernet-verkon segmenttiä voidaan jatkaa niin kauas, kuin IP/MPLS-runkoverkkoa riittää.

Erona Layer 3 -tason VPN-tekniikoihin, operaattoriverkon laitteet eivät tee liikenteen reititystä, vaan liikenteen ohjaaminen perustuu Layer 2 –tason kytkentään. Jokaista VPN-instanssia kohden ei tarvitse siis ylläpitää erillistä reititystaulua, vaan liityntärajapintaan saapuva Layer 2 -tason liikenne vain yksinkertaisesti kytketään oikeaan tunneliin. Asiakasyrityksen ostaessa L2VPN-palvelu operaattorilta jää reititys asiakkaan omien laitteiden hoidettavaksi. Operaattorin näkökulmasta tämä yksinkertaistaa verkkoa ja sen hallintaa.

4.2 Pseudowire-emulointi

Pseudowire-emulointi luo pohjan Layer 2 -tason liikenteen siirtämiseen IP/MPLS-pohjaisen verkon yli. Verkon PE-laitteiden välille muodostetaan virtuaalinen Pseudowire-linkki. Pseudowire-linkki on tunneli, jolla on L1-tason yhteyden kaltaiset ominaisuudet, joten se tarjoaa läpinäkyvän siirtotien Layer 2 –tason tekniikoille.

Pseudowire-linkki yhdistää liityntärajapinnat kahden PE-laitteen välillä. Rajapinta voi olla esimerksi: Ethernet-portti tai –VLAN, PPP-istunto, Frame Relay DLCI, ATM VPI/VCI ja niin edelleen. Pseudowire-linkin läpi liikenne kulkee palvelukohtaisina

Protocol Data Unit (PDU) -paketteina. PE-laite enkapsuloi liityntärajapintaan saapuvan liikenteen PDU-paketeiksi ja ohjaa ne oikean Pseudowire-linkin läpi toiselle PE-laitteelle. Vastaanottava PE-laite muuntaa liikenteen PDU-paketeista takaisin natiiviin muotoonsa ja ohjaa oikeaan liityntärajapintaan. Verkon P-laitteet vain kytkevät paketteja, eivätkä ole tietoisia Pseudowire-linkeistä tai niiden sisällä kulkevasta liikenteestä. (Luo, Pignataro, Bokotey & Chan 2005, 16-17.)

Pseudowire-emuloinnin avulla voidaan kuljettaa saman pakettikytkentäisen verkon yli palveluita, jotka normaalisti pitäisi tehdä rinnakkaisilla verkoilla. Keskittyminen yhteen runkoverkkoon vähentää kustannuksia ja lisäksi pakettikytkentäinen verkko tarjoaa tehokkaan konvergoitumisen vikatilanteissa. (Luo, Pignataro, Bokotey & Chan 2005, 15.)

5 ETHERNET OVER MPLS (EOMPLS)

EoMPLS on yksi Any Transport over MPLS (AToM) –perheen tekniikoista. Sen avulla voidaan kuljettaa Ethernet-liikennettä kahden PE-laitteen välillä IP/MPLS-verkossa. Konfigurointi tavasta riippuen, EoMPLS-palvelun avulla on mahdollista emuloida fyysistä Ethernet-kaapelia kahden PE-laitteen portin välillä tai ottaa mukaan myös pakettien kytkentä ja useampi liityntärajapinta.

5.1 Yleistä

EoMPLS on Pseudowire-emulointi –tekniikka Ethernet-liikenteen kuljettamiseen IP/MPLS-verkon yli. EoMPLS-yhteydet ovat topologialtaan Point-to-point –tyyppisiä, eli niihin voi osallista vain kaksi MPLS-verkon reunalaitetta kerrallaan. PE-laitteiden välille muodostetaan kaksisuuntainen tunneli, joka koostuu parista yksisuuntaisia LSP-polkuja (Luo, Pignataro, Bokotey & Chan 2005, 34).

PE-laiteessa Ethernet-kehykset enkapsuloidaan MPLS-paketeiksi ja siirretään Pseudowire-linkin kuljetettavaksi toiselle PE-laitteelle. Tavanomaisessa käytössä EoMPLS-liikenne merkitään kahdella lipulla. Päällimmäinen lippu ohjaa paketit verkon läpi oikealle PE-laitteelle ja alempi lippu kertoo vastaanottavalle PE-laitteelle oikean liityntärajapinnan. Kumpikin lippu on neljän tavun pituinen ja lisäksi ainakin Cisco Systemsin laitteet lisäävät mukaan neljän tavun Control Word –kentän, jossa

mukana kulkee muun muassa pakettien sekvenssinumero, jonka avulla varmistetaan pakettien oikea järjestys. (Luo, Pignataro, Bokotey & Chan 2005, 140.)

5.2 Porttipohjainen EoMPLS

Yleisin muoto EoMPLS-palvelusta on porttipohjainen EoMPLS. Se on tuettu useimmissa Ciscon Systemsin reititinlaitteissa. Porttipohjaisen EoMPLS-palvelun liityntärajapinta on fyysinen portti tai aliliityntäportti. Laitteet eivät opettele MAC-osoitteita, eivätkä tee paikallista kytkentää liikenteelle. (Tassos 2009.) Yhtä instanssia kohden voi liityntärajapintoja olla vain yksi kappale kummassakin PE-laitteessa. Kaikki liityntärajapintaan saapuva liikenne ohjataan suoraan Pseudowire-linkkiin ja vastaavasti kaikki Pseudowire-linkistä saapuva liikenne ohjataan suoraan ulos liityntärajapinnasta. Porttipohjainen EoMPLS emuloi siis fyysistä Ethernet-kaapelia liityntäpisteiden välillä ja palvelu tunnetaan myös nimellä Virtual Private Wire Service (VPWS). (Darukhanawalla & Bellagamba 2008, 14.)

5.3 VLAN-pohjainen EoMPLS

VLAN-pohjaisessa EoMPLS-palvelussa liityntärajapintana on laitteen samaan Bridge Domain –alueeseen liitetyt kytkinportit. Liityntärajapintoja voi siis yhdessä PE-laitteessa olla useita. PE-laitteet oppivat liikenteestä MAC-osoitteet ja kytkevät paketteja CAM-taulun merkintöihin perustuen Pseudowire-linkin ja liityntärajapintojen välillä. VLAN-pohjainen EoMPLS-palvelu tarjoaa siis kytkinlaitteen kaltaisen toiminnan molempien PE-laitteiden liityntärajapintojen välille. Palvelu on kuitenkin vain Point-to-point –tyyppinen, eli siihen voidaan liittää vain kaksi PE-laitetta, jotka yhdistää yksi Pseudowire-linkki. VLAN-pohjainen EoMPLS-palvelu ei onnistu Cisco Systemsin perustason reititinlaitteilta, sillä laitteesta täytyy löytyä SIP- tai ES/ES+ -moduuli. (Tassos 2009.)

6 VIRTUAL PRIVATE LAN SERVICE (VPLS)

VPLS-palvelun avulla voidaan kuljettaa Ethernet-liikennettä usean PE-laitteen välillä IP/MPLS-verkossa. Loogisesti VPLS-instanssi toimii kuin kytkinlaite PE-laitteiden liityntärajapintojen välillä. VPLS-palvelua voidaan toteuttaa kahdella eri topologialla ja toinen toteutustapa on saanut nimen H-VPLS. Tässä kappaleessa esitellään lyhyesti myös VPLS-palvelun kehitetty versio, A-VPLS. Sitä ei tässä työssä kuitenkaan kokeiltu käytännön tasolla.

6.1 Yleistä

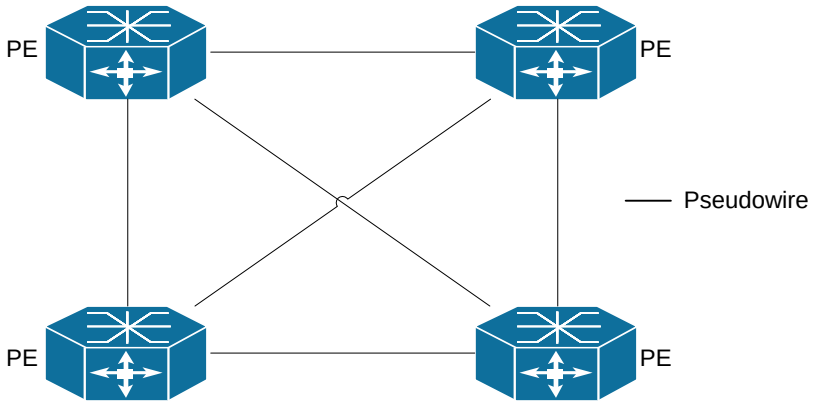
Virtual Private LAN Service (VPLS) on Layer 2 -tason VPN-palvelu IP/MPLS-runkoverkon yli. VPLS-palvelun avulla voidaan yhdistää useita eripuolella MPLS-verkkoa sijaitsevia verkkoja yhteen ja emuloida kytkinlaitetta niiden välillä. Kaikki samaan VPLS-instanssiin liitetyt verkot muodostavat yhden loogisen lähiverkon. (Xu 2010, 464.)

Kuten EoMPLS-palveluissa, liikenteen kuljettamiseen käytetään Pseudowire-linkkejä. VPLS kuitenkin mahdollistaa liityntärajapintojen yhdistämisen Multipoint-to-multipoint tai Point-to-multipoint -topologialla erillisten Point-to-point -yhteyksien sijasta. Jos mukaan osallistuvia PE-laitteita on enemmän kuin kaksi kappaletta, on yhteydet järkevämpi ja helpompi toteuttaa VPLS-palvelun avulla kuin erillisillä EoMPLS-tunneleilla, jos vain tuki laitteista löytyy. VPLS yksinkertaistaa myös konfigurointia tilanteissa, joissa uusi liityntärajapinta pitää ottaa mukaan VPN-palveluun. Jos Pseudowire-linkit PE-laitteiden välille on jo luotu, riittää vain uuden portin liittäminen osaksi VPLS-instanssia. Point-to-point arkkitehtuurilla toteutetuissa ratkaisuissa tämä vaatii jokaisen kyseiseen VPN-palveluun osallistuvan PE-laitteen konfiguroimista. (Luo, Pignataro, Bokotey & Chan 2005, 570.)

6.2 VPLS (Full Mesh)

VPLS-palvelun perusta on Full Mesh – topologian mukaisesti luodut Pseudowire-linkit laitteiden välillä. Yksi Pseudowire-linkki yhdistää aina kahden samaan VPLS-instanssiin kuuluvan PE-laitteen Bridge Domain -alueet keskenään. Full Mesh – topologian saavuttamiseksi jokaisesta PE-laitteesta on Pseudowire-linkki jokaiseen muuhun samaan VPLS-instanssiin kuuluvaan PE-laitteeseen. Full Mesh –topologian saa-

vuttamiseksi Pseudowire-linkkejä tarvitaan N * (N – 1) / 2 kappaletta, missä *N* on VPLS-instanssiin osallistuvien PE-laitteiden lukumäärä. (Xu 2010, 511-512.) Kuva 2 esittää miten Pseudowire-linkit muodostetaan neljän PE-laitteen välille Full Mesh -topologiassa.



Kuva 2. Full Mesh -topologia

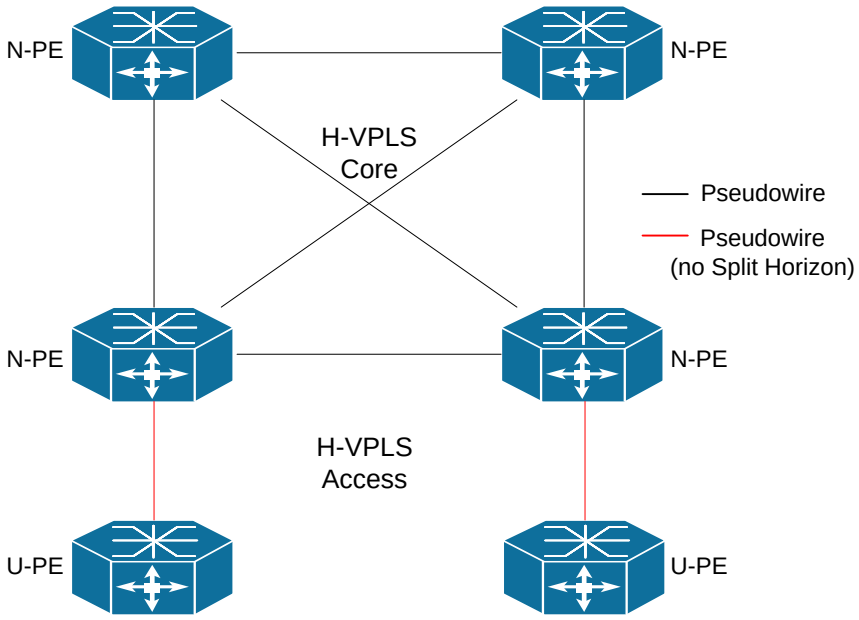
Ethernet-kytkimet monistavat Broadcast- ja tuntemattomat Unicast-lähetykset kaikista kytkinporteista, paitsi siitä josta paketti vastaanotettiin. Tästä toimintatavasta johtuen voi verkossa oleva silmukka aiheuttaa levitysviestimyrskyn. Levitysviestimyrskyssä paketit jäävät pyörimään silmukkaan loputtomiin, kun kytkin kytkee vastaanottamiaan paketteja toisesta portista takaisin lähettäneelle laitteelle ja päinvastoin. Silmukka syntyy jos liikenne pääsee kahta eri reittiä samalle laitteelle, eli esimerkiksi jos kytkimet halutaan kytkeä redundanttisesti toisiinsa. Silmukoiden estämiseksi Ethernet-verkoissa käytetään Spanning Tree (STP) -protokollaa. Spanning Tree –protokolla estää silmukan syntymisen estämällä liikennöinnin ylimääräisestä linkistä. Käytössä olevan linkin vikaantuessa Spanning Tree –protokollan algoritmi laskee uuden reitin ja aiemmin estetty linkki otetaan käyttöön.

Full Mesh –topologian mukaisesti toteutetuissa VPLS-verkoissa Spanning Tree -protokollan tarve voidaan poistaa, koska tiedetään, että jokainen laite kytkeytyy loogisesti suoraan jokaiseen samaan VPLS-instanssiin kuuluvaan laitteeseen. Levitysviestimyrskyjen estämiseksi VPLS-instanssiin kuuluvat Pseudowire-linkit noudattavat oletusarvoisesti Split Horizon –sääntöä. Split Horizon -sääntö estää PE-laitetta lähettämästä Pseudowire-linkistä vastaanottamiaan paketteja toiseen Pseudowire-linkkiin. Kaikki Pseudowire-linkit voidaan siis ajatella löytyvän saman kytkinportin takaa ja Ethernet-kytkimen toiminnan tavoin se ei monista liikennettä porttiin, josta se vastaanotti paketin. (Xu 2010, 511-512.)

6.3 H-VPLS (Hub-Spoke)

H-VPLS (Hierarchical-VPLS) mahdollistaa VPLS-palvelun topologian jaottelun kahteen tasoon, VPLS -runkoon ja alempaan liityntätasoon. VPLS-runko omaa perinteisen Full Mesh –topologian mukaisesti muodostetut Pseudowire-linkit PE-laitteiden välillä. Liityntätasolta voidaan tarttua kiinni yhdellä Pseudowire-linkillä mihin vain osana H-VPLS -runkoa olevaan PE-laitteeseen. Tästä topologiasta käytetään nimitystä *Hub-Spoke*. H-VPLS -palvelussa runkoon osallistuvista laitteista käytetään nimitystä N-PE (Network-facing PE) ja liityntätasolla olevista laitteista nimitystä U-PE (User-facing PE). Full mesh -topologiassa käytettävä Split Horizon –sääntö on Hup-Spoke –topologiassa poistettava N-PE –laitteista U-PE –laitteisiin osoittavista Pseudowire-linkeistä. Muuten N-PE –laite ei lähetä muilta PE-laitteilta vastaanottamaansa liikennettä U-PE –laitteille.

H-VPLS parantaa VPLS-palvelun skaalautuvuutta, sillä tarvittavien Pseudowire-linkkien määrää voidaan vähentää (Luo, Pignataro, Bokotey & Chan 2005, 578). H-VPLS:n avulla on myös mahdollista liittää edullisempia laitteita mukaan VPLS-instanssiin, koska yksikätisenä tarttuvilta liityntätason laitteilta vaaditaan vain tuki EoMPLS-palvelulle. H-VPLS:n huonona puolena voidaan pitää N-PE –laitteiden kasvavaa kuormitusta, kun kaikki U-PE –laitteiden liikenne kierrätetään niiden kautta. Kuva 3 esittää miten Pseudowire-linkit PE-laitteiden välille muodostetaan Hub-Spoke –topologiassa.



Kuva 3. Hub-Spoke -topologia

6.4 A-VPLS

A-VPLS (Advanced-VPLS) on Cisco Systemsin kehitetty versio VPLS-palvelusta. A-VPLS on palveluna sama kuin VPLS, mutta se tuo mukaan joitakin lisäominaisuuksia. Suurimpina muutoksina A-VPLS muuttaa konfigurointitapaa ja lisää liikenteeseen mukaan Flow Label –kentän paketin enkapsuloinnin yhteydessä. (Singh 2011.)

Tavallisen VPLS-palvelun konfiguroinnissa jokainen VPLS-instanssi luodaan laitteeseen erikseen. A-VPLS:n uusi konfigurointitapa tuo mukanaan *virtual-ethernet* –konfigurointitilan, joka vähentää tarvittavien komentojen määrää, koska useampi VPLS-instanssi, johon osallistuvat samat naapurilaitteet, voidaan määritellä saman konfigurointitilan alla. (Singh 2011.)

Flow Label –kentän avulla parannetaan VPLS-liikenteen kuormanjako-ominaisuuksia. Yhden Pseudowire-linkin kuljettamaa kuormaa voidaan jakaa maksimissaan kahdeksan eri LSP-polun kuljetettavaksi. Kuormanjakoa tehdään paketin Layer 2, 3 ja 4 –kenttien perusteella. (Singh 2011.)

7 EVC FRAMEWORK

EVC eli Ethernet Virtual Connection tarkoittaa Ciscon kehittämiä Carrier Ethernet infrastruktuurin ohjelmistoratkaisuja. Sitä ei pidä sekoittaa MEF:n (Metro Ethernet Forum) termistöön, jossa EVC:llä tarkoitetaan Ethernet-liikenteen kuljettamiseen käytettäviä virtuaalisia tunneleita, joista tässä työssä on puhuttu Pseudowire-linkkeinä.

Operaattorille yksi EVC:n suuri etu on mahdollisuus käyttää laitteen samassa fyysisessä portissa Layer 2 ja Layer 3 -tason palveluita samanaikaisesti. Saman fyysisen portin alla voidaan käyttää mitä tahansa yhdistelmää näistä palveluista:

- Layer 2 access
- 802.1Q trunk
- 802.1Q tunneli
- Paikallinen silmukka
- EoMPLS
- VPLS
- L3-liikenteen terminointi

(Tassos 2009.)

EVC-porttiin luodaan jokaista virtuaalista palvelua varten *Service Instance*, johon liikenne ohjataan saapuvan liikenteen VLAN-merkinnän perusteella. Service Instance ei oletusarvoisesti tee liikenteelle mitään, vaan liikenteen käsittelytapa on manuaalisesti määriteltävä. EVC framework mahdollistaa pakettien VLAN-merkintöjen vapaan uudelleenkirjoittamisen ennen niiden ohjaamista eteenpäin. L3-tason liikenteen terminoinnin voi hoitaa joko konfiguroimalla aliliityntäportin muiden palveluiden rinnalle tai ohjaamalle liikenne ensin Service Instancesta Bridge Domain –alueeseen ja terminoimalla liikenne SVI-rajapintaan. (Moskal 2008, 4-16.)

L2VPN-palveluita luodessa VLAN-merkinnöillä on kahdenlaista merkitystä. PE-laitteiden liityntärajapinnoissa niillä erotellaan esimerkiksi saman palvelun tai asiakkaan eri verkkoja, jotka jakavat saman fyysisen median. Samaa Layer 2 –segmenttiä voidaan jatkaa toisen PE-laitteen liityntärajapinnassa käyttäen siinä eri VLAN-merkintää. Näillä VLAN-merkkinöillä on siis siinä mielessä vain paikallista merkitystä ja niistä käytetään nimitystä Service-Delimiting VLAN. Toinen VLAN-tyyppi on Internal VLAN, joka edustaa PE-laitteen Bridge Domain –aluetta. (Luo, Pignataro, Bokotey & Chan 2005, 581-582.)

Tavallinen 802.1Q trunk -kytkinportti ohjaa liikenteen aina Service-Delimiting VLAN –merkinnän osoittamaan Bridge Domain –alueeseen. Eli Internal VLAN –merkkinnän täytyy vastata Service-Delimiting VLAN –merkintää. Tämä ei ole aina haluttu toimintatapa. Service Instancen avulla liikenne voidaan ohjata eri Bridge Domain –alueeseen, kuin liikenteeseen merkitty Service-Delimiting VLAN -merkintä osoittaa. Näin pystytään liittämään samaan Bridge Domain –alueeseen useita liityntärajapintoja, joissa käytetään eri Service-Delimiting VLAN –merkintää.

8 SIMUNET

SimuNet on osittain EAKR-rahoitteinen hanke, jossa vuonna 2009 Kymenlaakson ammattikorkeakoulun ICT-laboratorion tiloihin perustettiin SimuNet-verkko. SimuNet simuloi useista laitetiloista koostuvaa verkko-operaattorin tuotantoverkkoa, jossa laitetiloja yhdistää IP/MPLS-pilvi. SimuNet-verkko toimi alustana tämän työn kaikille käytännön toteutuksille.

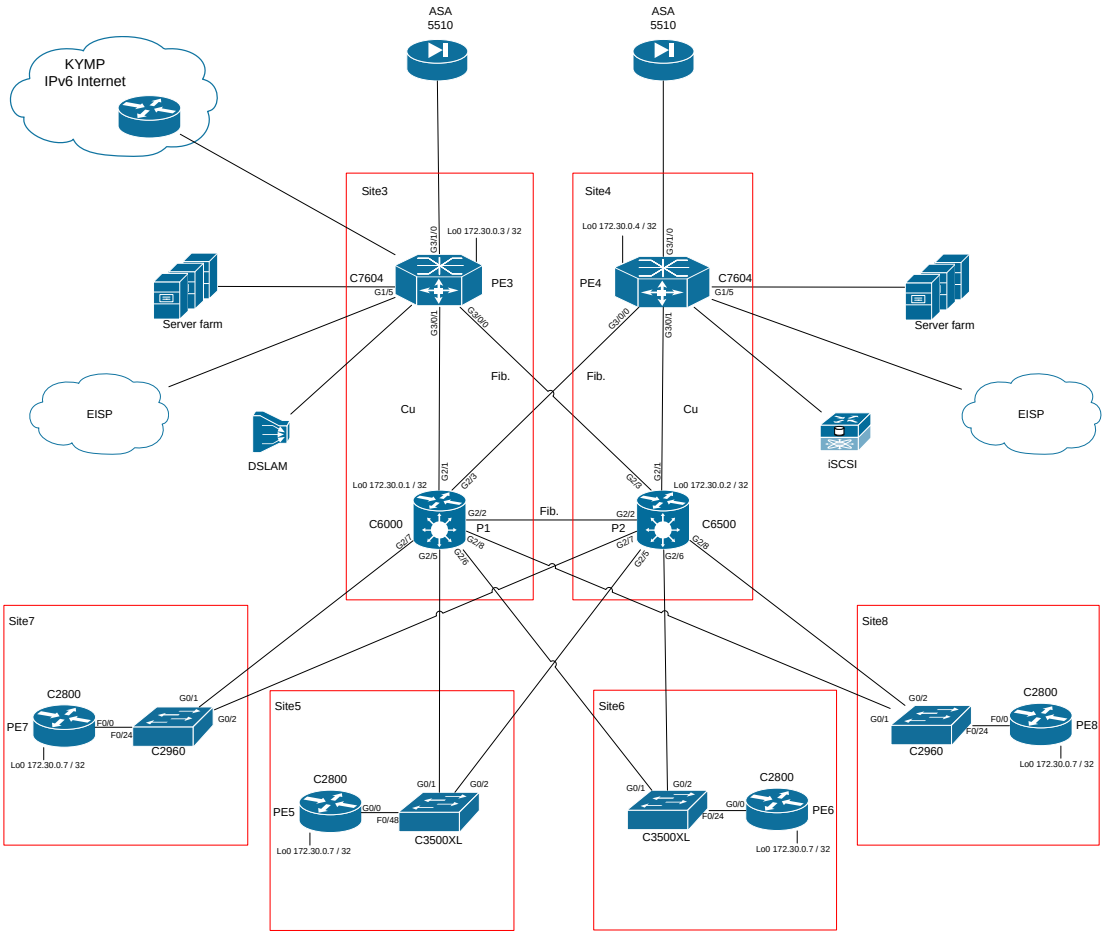
8.1 Yleistä

SimuNet on testi- ja T&K-verkko, joka simuloi nykyaikaista verkko-operaattorin tuotantoverkkoa. SimuNetin avulla tietoverkkotekniikan opiskelijat pääsevät tekemään harjoitustöitä operaattoriverkon kaltaisessa ympäristössä, ja sitä voidaan käyttää erinäisissä harjoitustöissä simuloimaan Internet-palveluntarjoajaa. SimuNet-verkkoon liittyvissä projekti- ja opinnäytetöissä oppilaat itse miettivät ja kehittävät verkon topologiaa ja tuovat verkkoon lisää palveluja. Eniten SimuNet-verkkoa on käytetty juuri alustana tietoverkkotekniikan projektitöissä. SimuNetin on myös tarkoitus palvella tilanteissa, jossa paikallisen verkko-operaattorin verkkoon on syytä toteuttaa omaan verkkoonsa jokin suurempi muutos. Muutos voidaan ensin toteuttaa turvallisesti SimuNet-verkossa ennen muutoksen toteuttamista oikeassa tuotantoverkossa. (Kettunen 2009, 11.)

8.2 Topologia

SimuNet-verkko on koulun tuotantoverkosta eristetty ympäristö. Ainoastaan sen hallintayhteydet on kuljetettu koulun ICT-laboratorion tuotantoverkon puolelle. Verkkolaitteiden hallinta on toteutettu tuotantoverkon puolelle kytkettyjen Cisco Systemsin etäkäyttö-palvelimien avulla. Laitteiden konsoliportit on kytketty näihin palvelimeen, ja ne muuntavat tuotantoverkosta otetut Telnet-yhteydet konsolimuotoon ja ohjaavat ne oikealle laitteelle käytetyn porttinumeron perusteella. Palvelinklusterin hallintaportti kytkeytyy myös tuotantoverkon puolelle mahdollistaakseen sen graafisen ja web-pohjaisen hallinnan.

SimuNetin verkko koostuu kuudesta laitetilasta. Laitetilat on numeroitu niissä sijaitsevan PE-laitteen järjestysnumeron mukaan (*Site3-8*) ja kuvitteellisesti nämä laitetilat on hajautettu maantieteellisesti erilleen. Oikeassa operaattorikäytössä laitetiloja yhdistäisi esimerkiksi valokuiduin toteutettu rengas, jossa liikenteen erotteluun käytetään optista aallonpituuskanavointia. SimuNet-verkon fyysinen kytkentä selviää kuvasta 4 ja suurempana liitteestä 1.



Kuva 4. SimuNet-verkon fyysinen topologia

Varsinaista runkoverkko-osaa SimuNetissä edustaa kaksi P-laitetta ja kuusi PE-laitetta. Näitä yhdistää jokaisen laitetilan kattava IP/MPLS-pilvi. Fyysisesti kaikki PE-laitteet tarttuvat IP/MPLS-pilveen laitetiloissa *Site3* ja *Site4* sijaitsevien P-laitteiden kautta. Yhden pisteen vian mahdollisuuden poistamiseksi tarttuu jokainen PE-laite kumpaankin P-laitteeseen. Jos laitetiloja yhdistää valokuiturengas, kuljetaan nämä linkit sen eri reunoja pitkin, jottei kuidun katkeaminen yhdestä pisteestä katkaise molempia yhteyksiä. IGP-reititysprotokollana SimuNetin rungossa toimii OSPF.

PE-laitteet ovat operaattorin reunalaitteita, joihin muun muassa kaikki tarvittavat MPLS L2VPN –yhteydet terminoidaan. Suurin osa verkon toiminnallisuudesta ja palveluista sijaitsee PE3- ja PE4-reitittimissä, sillä nämä laitteet ovat huomattavasti muita PE-laitteita järeämpiä ja muut PE-laitteet lisättiin verkkoon vasta tämän työn yhteydessä. SimuNet kytkeytyy myös PE3-reitittimen kautta IPv6-Internetiin. SimuNetin käyttöön rekisteröity globaali IPv6-osoiteavaruus on 2a00:1dd0:100::/48 (Leinonen 2011).

P-laitteet runkoverkon ytimessä tekevät vain liikenteen kytkentää perustuen MPLS-lippumerkintöihin. Ne eivät ota kantaa läpi kulkevaan liikenteeseen, vaan niiden tarkoitus on tehokkaasti kytkeä PE-laitteiden välillä kulkevaa liikennettä.

SimuNet-verkko eroaa sen loogisilta toiminnallisuuksiltaan paljon fyysisestä topologiastaan, sillä melkein kaikki verkon palvelut ovat jollain tasolla virtualisoitu ja palvelut eivät ole sidoksissa yhteen fyysiseen laitteeseen tai sijaintiin, vaan niiden looginen toiminta voidaan siirtää eri laitteen käsiteltäväksi.

8.3 Laitteisto

Laitteistona SimuNetissä käytetään pääasiallisesti Cisco Systemsin laitteita. PE3 ja PE4 laitteet ovat Cisco 7600 -sarjan reitittimiä. Ne on varustettu SUP32-moduulilla ja SIP400-lisämoduulilla, jolla saadaan laitteisiin lisäominaisuuksia, kuten tuki VPLS- sekä VLAN-pohjaiselle EoMPLS -palvelulle. Muut PE-laitteet ovat huomattavasti pienempiä Cisco Systemsin 2800 –sarjan reitittimien eri versioita. P-laitteista eli SimuNetin runkokytkimistä P1 on Cisco Catalyst 6000-sarjan ja P2 Cisco Catalyst 6500-sarjan kytkin. Työn käytännön toteutuksia tehdessä PE3- ja PE4-laitteiden IOS-ohjelmistoversio oli 15.1(1)S1.

9 PE-LAITTEIDEN LISÄÄMINEN VERKKOON

SimuNet-verkkoa kasvatettiin lisäämällä verkkoon uusia PE-laitteita. Uudet PE-laitteet ovat Cisco 2800 –sarjan reitittimiä ja jokaisella on oma edustakytkin, jonka avulla niiden porttimäärää laajennetaan.

9.1 Yleistä

Tätä työtä aloitettaessa SimuNet-runko koostui kahdesta P-laitteesta ja kahdesta PE-laitteesta, jotka nykyisellä nimeämistavalla ovat P1, P2, PE3 ja PE4. SimuNetiin lisättiin neljä uutta PE-laitetta kuvaamaan jokainen omaa uutta maantieteellistä sijaintiaan. Uudet PE-laitteet nimettiin juoksevalla numerolla: PE5, PE6, PE7 ja PE8. Laitteiden fyysinen kytkentä selviää kuvasta 4 tai suurempana liitteestä 1.

Uusia PE-laitteita on tarkoitus käyttää muun muassa H-VPLS -palvelun kokeiluun. Käytetyt Cisco Systemsin 2800-sarjan laitteet ovat kevyemmän sarjan reitittimiä ei-

vätkä ne tue VPLS-palvelua. Tuki kuitenkin löytyy porttipohjaiselle EoMPLS-palvelulle, joten ne saadaan mukaan VPLS-palveluun H-VPLS liityntätason laitteina. Uudet PE-laitteet on tarkoitus jättää pysyvästi osaksi SimuNet-verkkoa, jolloin niitä voidaan jatkossakin käyttää hyödyksi SimuNet-verkkoon liittyvissä projekteissa.

9.2 Toteutus

Redundanttisuutta ajatellen kukin PE-laite on järkevä kytkeä kumpaankin P-laitteeseen. Käytetyissä reitittimissä ei kuitenkaan ole kuin kaksi Ethernet-porttia kussakin ja jos nämä molemmat käytetään runkoverkon puolelle, ei laitteisiin olisi jäänyt vapaita portteja asiakaskäyttöön. Tämän takia PE-laitteiden alle asennettiin edustakytkimet, jotka toimivat reitittimien lisäportteina. Näin vältyttiin kalliiden lisämoduulien hankinnalta. Suurta kaistanleveyttä tarvittaessa tämä ei ole hyvä ratkaisu, mutta ajaa asiansa hyvin testiympäristössä. Edustakytkimien ansiosta vapaita portteja asiakasyhteyksiä varten jäi käytetyistä kytkin malleista riippuen joko 23 tai 47 kappaletta PE-laitetta kohden.

Edustakytkimiin tehtiin yksinkertainen konfiguraatio, jossa jokainen portti yhtä lukuun ottamatta konfiguroitiin portin järjestysnumeroa vastaavaan VLAN-alueeseen. Yksi jäljelle jäänyt portti on 802.1Q trunk –portti, jossa muiden porttien liikenne kuljetetaan reitittimelle. Liikenne voidaan päättää reitittimen päässä aliliityntäportteihin, joista jokainen vastaa omaa fyysistä porttiaan edustakytkimessä. Kytkimien viimeinen Fast Ethernet -portti kytkettiin PE-reitittimeen ja Gigabit Ethernet -portit kytkettiin P-laitteisiin. Loput portit jäivät asiakasyhteyksien käyttöön.

Konfigurointi aloitettiin liittämällä PE-laitteet osaksi SimuNet-verkon IP/MPLS-pilveä, käynnistämällä niihin MPLS sekä OSPF-reititys. Myöhemmin Tolosen (2011) opinnäytetyössä laitteisiin käynnistettiin myös iBGP-reititys, mutta sitä ei tämän työn virtuaaliyhteyksien toteutukseen tarvita, koska niiden signalointiin käytettiin LDP-protokollaa. Jokaisen PE-laitteen konfigurointi on miltein samanlainen, alla esiintyvissä esimerkeissä on siksi esitetty vain PE5-laitteen konfigurointia.

Loopback-portti pitää konfiguroida IP-osoitteella ja /32 verkkomaskilla. Tätä osoitetta käytetään muun muassa laitteen ID-tunnisteena LDP-signaloinnissa. Käytetyissä IP-osoitteissa viimeinen luku määräytyy PE-laitteen järjestysnumeron mukaan:

PE5(config-if)#interface loopback0
PE5(config-if)#ip address 172.30.0.5 255.255.255.255

Runkoverkkoa kohti osoittavat portit konfiguroitiin linkkiverkon IP-osoitteella. Konfiguraatio syötettiin aliliityntäportteihin *GigabitEthernet 0/0.49* ja *0/0.50*. Nämä vastaavat edustakytkimen fyysisiä GbE-portteja GBIC-modulipaikoissa 1 ja 2:

PE5(config)#interface GigabitEthernet 0/0.49
PE5(config-if)#encapsulation dot1q 49
PE5(config-if)#ip address 192.168.15.5 255.255.255.255

PE5(config-if)#interface GigabitEthernet 0/0.50
PE5(config-if)#encapsulation dot1q 50
PE5(config-if)#ip address 192.168.25.5 255.255.255.255

SimuNetin IGP-reititysprotokollana toimii OSPF. Laitteisiin luotiin OSPF-prosessi numerolla 1. Osaksi prosessia lisättiin runkoverkkoa kohti osoittavat portit ja myös loopback-rajapinta:

PE5(config)#router ospf 1
PE5(config-router)#network 192.168.0.0 0.0.255.255 area 0
PE5(config-router)#network 172.31.0.0 0.0.255.255 area 0

MPLS käynnistettiin runkoverkkoa kohti osoittavissa porteissa ja portin MTU-arvo asetettiin riittävän suureksi, jotta MPLS-otsikot mahtuvat mukaan liikenteeseen:

PE5(config)#interface GigabitEthernet 0/0.49
PE5(config-subif)#mpls ip
PE5(config-subif)#mtu 1600

PE5(config-subif)#interface GigabitEthernet 0/0.50
PE5(config-subif)#mpls ip
PE5(config-subif)#mtu 1600

SimuNetin P-laitteissa oikea MTU-arvo sekä MPLS on asetettu oletusarvoisesti käyttöön jokaisessa portissa, joten niissä riitti portin käynnistäminen ja selitykset lisääminen oikeiden porttien asetuksiin. MPLS:n ja LDP:n toiminnan voi todeta esimerkiksi komennolla *show mpls interfaces:*

```
PE5#show mpls interfaces
Interface                IP         Tunnel   Operational
GigabitEthernet0/0.49    Yes (ldp)  No       Yes
GigabitEthernet0/0.50    Yes (ldp)  No       Yes
```

9.3 Asiakasyhteyksien käyttöönotto

Asiakasyhteydet laitteissa PE5 - PE8 kytketään niiden edustakytkimeen. Asiakasyhteyksiä varten kytkimistä on varattu Fast Ethernet –portit ensimmäisestä toiseksi viimeiseen, eli F0/1 - 23 tai F0/1 - 47, kytkinmallista riippuen. Konfigurointi tehdään PE-reitittimen nolla portin aliliityntäportteihin ja ensimmäiseksi sille määritetään liikenne enkapsuloitavaksi 802.1Q VLAN –merkinnällä, käytettyä kytkimen porttinumeroa vastaavaan VLAN-alueeseen. Esimerkiksi jos asiakasyhteys kytketään PE-laitteen edustakytkimen porttiin F0/5 konfiguroidaan PE-laite ensin alla esitetyllä tavalla:

```
PE5(config)#interface GigabitEthernet 0/0.5
PE5(config-if)#encapsulation dot1q 5
```

Tämän jälkeen voidaan portti konfiguroida esimerkiksi haluttu IP-osoite tai MPLS L2VPN –palvelu.

10 CASE HA-PALVELINKLUSTERI

SimuNetissä toimii HA-palvelinklusteri, jossa fyysisiä palvelinlaitteita on kaksi kappaletta. Palvelinlaiteet on sijoitettu SimuNetin eri laitetiloihin ja niiden tarvitsemat yhteydet toteutettiin VLAN-pohjaisen EoMPLS-palvelun avulla.

10.1 Yleistä

High-availability (HA) eli korkean saatavuuden palvelinklustereista on tullut yksi IT-strategioiden pääkomponentti haluttaessa parantaa muun muassa tarjottavien palveluiden saatavuutta (Darukhanawalla & Bellagamba 2008, xvi). HA-palvelinklusterit koostuvat kahdesta tai useammasta fyysisestä palvelinlaitteesta, joihin voidaan virtualisoida suuri määrä palvelimia virtuaalikoneiksi. Palvelinlaitteiden todelliset fyysiset resurssit eivät näy suoraan virtuaalikoneille, vaan palvelinklusterin ohjelmisto emuloi

niistä määritetyn osan jokaiselle. Tämä mahdollistaa niiden resurssien tehokkaan hallinnan tarpeen mukaan.

Palvelinlaitteisiin kohdistuviin vikatilanteisiin HA-palvelinklusterin laitteet reagoivat käynnistämällä vikaantuneessa laitteessa toimineet virtuaalikoneet toisessa palvelinlaitteessa. HA-palvelinklusteri havaitsee sekä rauta- että ohjelmistoviat ja virtuaalikoneiden siirto toiselle klusterin palvelinlaitteelle tapahtuu ilman ylläpitäjän toimenpiteitä.

HA-palvelinklusterit on tyypillisesti rakennettu käyttäen kahta erillistä verkkoa: Tuotantoverkko virtuaalikoneisiin liikennöintiä varten ja yksityinen verkko palvelinlaitteiden keskinäistä liikennöintiä varten. Yksityisen verkon kautta palvelinlaitteet myös lähettävät toisilleen heartbeat-viestejä, joiden avulla ne tarkkailet toistensa tilaa. Yksityinen verkko on reitittämätön ja se jakaa saman Layer 2 –alueen palvelinlaitteiden välillä. (Darukhanawalla & Bellagamba 2008, 2-4.)

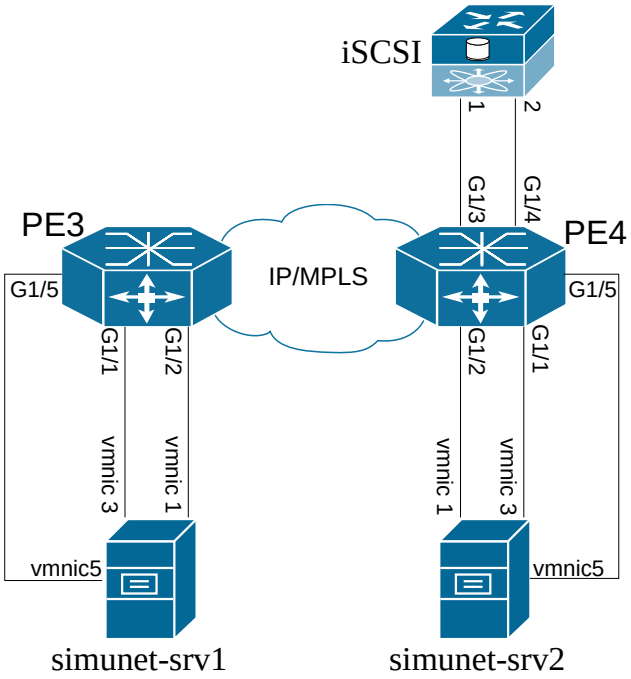
HA-palvelinklusterin avulla kasvatetaan SimuNetin palvelujen redundanttisuutta, poistamalla yhden pisteen vian mahdollisuus palvelinkoneista. Käyttöjärjestelmänä palvelinlaitteissa on VMware ESX 4.1.0. Tarkempaa tietoa itse palvelinklusterista ja sen perustamisesta SimuNetiin löytyy Aholan (2010) opinnäytetyöstä.

HA-palvelinklusteri vaatii toimiakseen jokaisen siihen kuuluvan palvelinlaitteen virtuaalikoneille pääsyn samaan verkon Layer 2 –segmenttiin, jotta ne pystyvät liikennöimään käyttäen samoja IP-osoitteita riippumatta kummassa klusterin palvelinlaitteessa ne sijaitsevat. SimuNetin palvelinklusterin käyttämiä VLAN-alueita jatkettiin MPLS L2VPN-palveluiden avulla MPLS -verkon yli. Näin saadaan HA-palvelinklusteri toimimaan myös maantieteellisesti erillään sijaitsevien laitetilojen välillä.

SimuNetin palvelinlaitteissa on käytössä myös VMware VMotion. VMotion mahdollistaa virtuaalikoneen migraation lennosta palvelinlaitteiden välillä ilman minkäänlaista downtime-aikaa. VLAN-alue erillään käyttäjien liikenteestä vaaditaan VMotionin liikenteelle, jotta virtuaalikoneiden siirto ei vaikuta käyttäjiin. Lisäksi myös VMotion vaatii, että virtuaalikone pysyy samassa verkon Layer 2 -segmentissä migraation jälkeen, koska IP-osoite ei voi vaihtua siirron aikana. (Darukhanawalla & Bellagamba 2008, xv.)

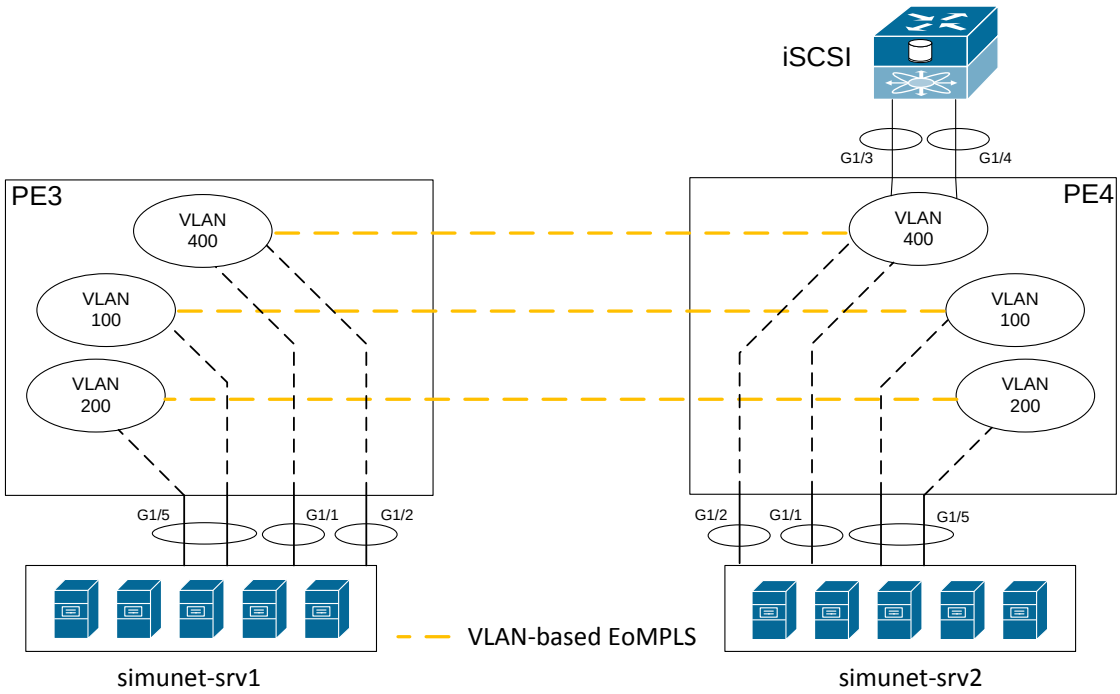
10.2Topologia

SimuNetin kahdennettu palvelinklusteri on toteutettu kahdella fyysisellä palvelinlaitteella ja ne on nimetty *simunet-srv1:ksi* ja *simunet-srv2:ksi*. Palvelinlaitteet on sijoitettu omiin laitekaappeihin, jotka SimuNet-verkossa simuloivat eri laitetiloja. Virtuaalikoneiden liikennöintiä varten kumpikin palvelinlaite tarttuu PE-laitteeseen yhdellä fyysisellä kaapelilla. Lisäksi keskinäistä kommunikointia ja iSCSI-tietovarastoon liikennöimistä varten ne tarttuvat PE-laitteisiin kahdella kaapelilla. Palvelin laitteiden sijainti SimuNet-verkossa selviää kuvasta 4 ja suurempana liitteestä 1. Tarkka fyysinen kytkentä selviää kuvasta 5.



Kuva 5. Palvelimien fyysinen topologia

Palvelinklusterin virtuaalikoneet on sijoitettu kahteen eri verkkoon, ja nämä verkot kattavat kummankin laitetilan. Loogisesti tarkasteltuna verkossa näyttäisi olevan kaksi erillistä Layer 2 –tason kytkintä, johon virtualisoituja palvelimia voidaan liittää niiden sijainnista riippumatta. Lisäksi palvelinlaitteiden omaa liikennöintiä varten on oma kytkin irrallaan tuotantoliikenteestä. Kuva 6 esittää palvelinklusterin käyttämiä virtuaaliyhteyksiä SimuNet-verkkon laitetilojen välillä.

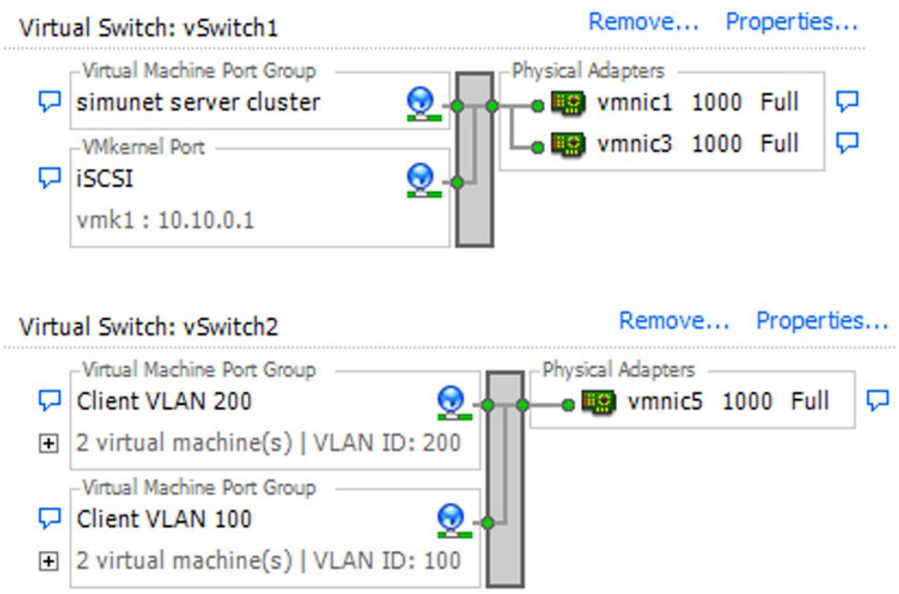


Kuva 6. Palvelimien looginen topologia

Palvelinklusteriin saapuva liikenne kulkee SimuNetin palomuurien läpi verkkoihin VLAN 100 ja VLAN 200. Näihin verkkoihin liitetään SimuNetin virtualisoidut palvelimet. VLAN 100 on tarkoitettu *simunet-srv-1* -palvelinlaitteen virtuaalikoneille ja VLAN 200 vastaavasti *simunet-srv2* -palvelinlaitteen virtuaalikoneille. Molempien palvelinlaitteiden virtuaalikoneilta on kuitenkin pääsy kumpaankin VLAN-alueeseen, vikatilanteesta tai muusta syystä johtuvaa palvelinlaitteiden välillä tapahtuvaa virtuaalikoneen migraatiota varten. VLAN 400 on varattu klusterin palvelinlaitteiden väliseen kommunikointiin ja VMotion liikenteelle. VLAN 400 -verkon kautta palvelimet myös tarttuvat iSCSI-tietovarastoon.

10.3Toteutus

Virtuaalikoneiden tuotantoverkkoa varten VMware ESX:n verkkoasetuksista laitteisiin luotiin virtuaalinen kytkin ja siihen VLAN-alueet 100 ja 200. Niiden liikenteeseen lisätään 802.1Q VLAN -merkintä liikenteen poistuessa ulos palvelinlaitteesta PE-laitteelle. Lisäksi palvelinlaitteisiin oli jo luotu virtuaalikytkin palvelinlaitteiden välistä kommunikointia varten. Tämän verkon liikenne lähetetään ulospäin ilman VLAN-merkintää (ks. kuva 7).



Kuva 7. Virtuaalikytkimet VMware ESX –palvelinlaitteen verkkoasetuksissa

PE-laitteissa VLANien 100, 200 ja 400 Bridge Domain -alueet yhdistettiin VLAN-pohjaisen EoMPLS-palvelun avulla. Tämä mahdollistaa VPLS-palvelun kaltaisen toiminnan kahden PE-laitteen välillä. PE-laitteet oppivat liikenteestä lähde MAC-osoitteet ja kytkevät paketteja sen perusteella oikealle palvelinlaitteelle. Samaan verkkoon liitettyjen virtuaalikoneiden näkökulmasta näyttää, että niitä yhdistää sijainnista riippumatta Layer 2 –tason kytkin. VLAN-pohjainen EoMPLS luodaan *xconnect*-komennolla ja parametreiksi sille annettiin toisen PE-laitteen IP-osoite ja enkapsulointitapa. PE-laitteiden konfiguraatio eroaa vain naapurilaitteen IP-osoitteiden osalta. Alla esiintyvissä esimerkeissä esitetään PE3-laitteen konfigurointia:

PE3(config)#interface vlan 100
PE3(config-if)#xconnect 172.30.0.4 100 encapsulation mpls

PE3(config-if)#interface vlan 200
PE3(config-if)#xconnect 172.30.0.4 200 encapsulation mpls

PE3(config-if)#interface vlan 400
PE3(config-if)#xconnect 172.30.0.4 400 encapsulation mpls

PE-laitteiden ja palvelinlaitteiden välinen yhteys on 802.1Q trunk –linkki. Portti PE-laitteiden päästä asetettiin 802.1Q trunk -kytkinportiksi ja sallituiksi VLAN-verkoiksi määriteltiin 100 ja 200:

```
PE3(config)#interface GigabitEthernet1/5
PE3(config-if)#switchport
PE3(config-if)#switchport trunk encapsulation dot1q
PE3(config-if)#switchport trunk allowed vlan 100,200
PE3(config-if)#switchport mode trunk
```

Palvelinklusterin keskinäistä kommunikointia sekä iSCSI-verkkolevylle liikennöintiä varten palvelinlaitteet tarttuvat PE-laitteisiin kahdella Ethernet-linkillä. Nämä PE-laitteiden portit määritettiin access-kytkinporteiksi, eli liikenne kulkee palvelin- ja PE-laitteiden välillä ilman VLAN-merkintää:

```
PE3(config)# interface GigabitEthernet1/1
PE3(config-if)#switchport
PE3(config-if)#switchport access vlan 400
PE3(config-if)#switchport mode access
```

EoMPLS-tunnelit aktivoituvat vasta kun käytettävä rajapinta on ylhäällä, eli tässä tapauksessa SVI-portti. SVI-portti nousee ylös vasta, kun samaan Bridge Domain –alueeseen on lisätty fyysinen liityntärajapinta. EoMPLS-tunneleiden tila voidaan tarkastaa esimerkiksi komennolla *show mpls l2transport vc.*Tulosteen viimeisestä kentästä voidaan tarkistaa, että tunneli laitteiden välillä on ylhäällä. Alla komennon antama tuloste PE3-laitteesta:

```
PE3#show mpls l2transport vc | include Status | 100 | 200 | 400
Local intf     Local circuit            Dest address    VC ID      Status
Vl100          Eth VLAN 100             172.30.0.4      100        UP
Vl200          Eth VLAN 200             172.30.0.4      200        UP
Vl400          Eth VLAN 400             172.30.0.4      400        UP
```

10.4Virtuaalikoneiden verkkoasetukset

SimuNetin palvelinklusteriin virtuaalikonetta luodessa voidaan kone liittää joko verkkoon *Client VLAN 100* tai *Client VLAN 200.* Valinta määrittää sen, kumpaan verkkoon palvelin tarttuu ja sitä kautta kumpaa SimuNet-verkon reunaa pitkin sen liikenne kulkee. SimuNetin *Site3*-laitetilan palomuuri oletusarvoisesti hoitaa VLANin 100 liikenteen ja vastaavasti *Site4*-laitetilan palomuuri hoitaa oletusarvoisesti VLANin 200 liikenteen. Tämän takia *simunet-srv1* -palvelinlaitteeseen virtuaalikoneita luodessa tulisi ne liittää verkkoon *Client VLAN 100* ja *simunet-srv2* -palvelinlaitteen virtuaalikoneet

liittää verkkoon *Client VLAN 200.* Tämä siis sen takia, että SimuNetin laitetiloilla voidaan ajatella olevan jonkin verran maantieteellistä välimatkaa ja näin saadaan liikenne kulkemaan lyhyintä ja järkevintä reittiä. Yhteydet kyllä toimivat täysin vaikka valinnan tekisikin ristiin, johtuen verkon redundanttisesta toteutuksesta. IP-osoiteasetukset virtuaalikoneille tulee asettaa taulukon 1 mukaisesti. Parhaaksi tavaksi IPv6-osoitteiden käytön kanssa todettiin määrittää palvelimen oma osoite käsin, mutta antaa IPv6-protokollan autokonfiguraation löytää oikea oletusyhdyskäytävä.

Taulukko 1. Virtuaalikoneiden IP-osoitteet verkkoille VLAN 100 ja VLAN 200.

	VLAN 100	**VLAN 200**
Virtuaalikoneiden osoiteavaruus (IPv4)	172.30.2.0 /24	172.31.2.0 /24
Virtuaalikoneiden oletusyhdyskäytävä (IPv4)	172.30.2.1	172.31.2.1
Virtuaalikoneiden osoiteavaruus (IPv6)	2a00:1dd0:100:b1:: /64	2a00:1dd0:100:b2:: /64
Virtuaalikoneiden oletusyhdyskäytävä (IPv6)	fe80:b1::1	fe80:b2::1

11 CASE PALOMUURIT

SimuNetin palvelimien edustalle on asennettu Active/active –tyyppisesti kahdennetut palomuurit. Palomuurien tarvitsemien yhteyksien toteutukseen käytettiin VPLS- sekä porttipohjaista EoMPLS-palvelua.

11.1 Yleistä

Verkkolaitteiden virtualisointi ei rajoitu pelkästään kytkimien ja reitittimien virtualisointiin. Myös palomuurit voidaan virtualisoida. Toisin sanoen yhdessä fyysisessä palomuurilaitteessa voidaan ajaa useaa loogista palomuurilaitetta. Näin saadaan kustannustehokkaasti esimerkiksi verkko-operaattorin usean eri asiakkaan palomuurit samaan fyysiseen laitteeseen, mutta pidettyä liikenne kuitenkin loogisesti erillään. (Moreno & Reddy 2006, 64-65.) Toinen syy palomuurien virtualisointiin voi olla Active/active –kahdennuksen toteutus, jossa kumpikin laite on yhtäaikaisesti aktiivisena eli välittää dataa.

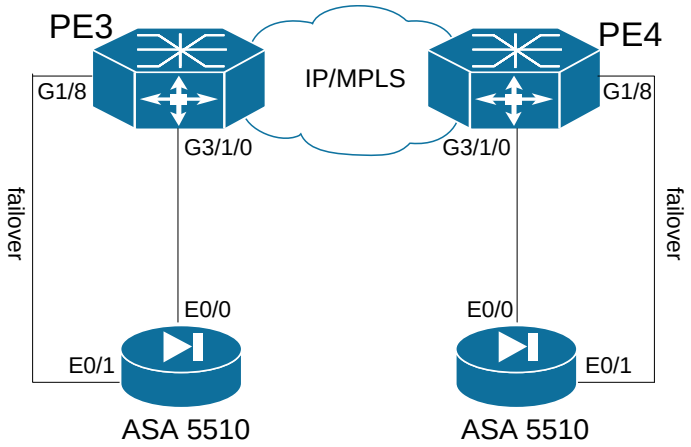
Active/active –kahdennuksessa virtuaaliset palomuurit sijaitsevat molemmissa fyysisissä laitteissa samanaikaisesti, mutta jokainen on kuitenkin vain toisessa laitteessa kerrallaan aktiivisena. Palomuurilaitteen vikaantuessa siinä aktiivisena pyörineet pa-

lomuurit käynnistetään toisessa laitteessa. Palomuurien Active/active –kahdennuksen toteutus oli SimuNetin tapauksessa syy palomuurien virtualisointiin.

Cisco Systems käyttää virtuaalisesta palomuurista termiä *context*. Jokainen palomuuri-context muodostaa itsenäisen loogisen palomuurilaitteen, jolla on omat säädökset, suodatuslistat ja portit tulevalle sekä lähtevälle liikenteelle. Useaa palomuuri-contextia käytettäessä tarjoavat ne saman toiminnallisuuden kuin yhtä monta fyysistä palomuurilaitetta. Tässä työssä käytetyt Cisco ASA 5510 -palomuurilaitteet eivät kuitenkaan tue dynaamisia reititysprotokollia tai VPN-ratkaisuja, silloin kun ne on konfiguroitu oletusarvoisesta *single context* –tilasta useita contexteja tukevaan *multiple context* -tilaan. Multiple context -tilassa palomuuri tutkii saapuvan paketin VLAN-merkinnän tai kohde IP-osoitteen ja päättää sen perusteella, mille palomuuri-contextille paketti ohjataan. Jokaisella palomuuri-contextilla tulee siis olla yksilöllinen VLAN-numerointi ja/tai IP-osoiteavaruus.

11.2 Topologia

SimuNet-verkossa on kaksi fyysistä palomuurilaitetta sijoitettuna laitetiloihin *Site3* ja *Site4* (ks. kuva 4). Kumpikin on kytketty oman laitetilan PE-laitteeseen kuvan 8 mukaisesti.

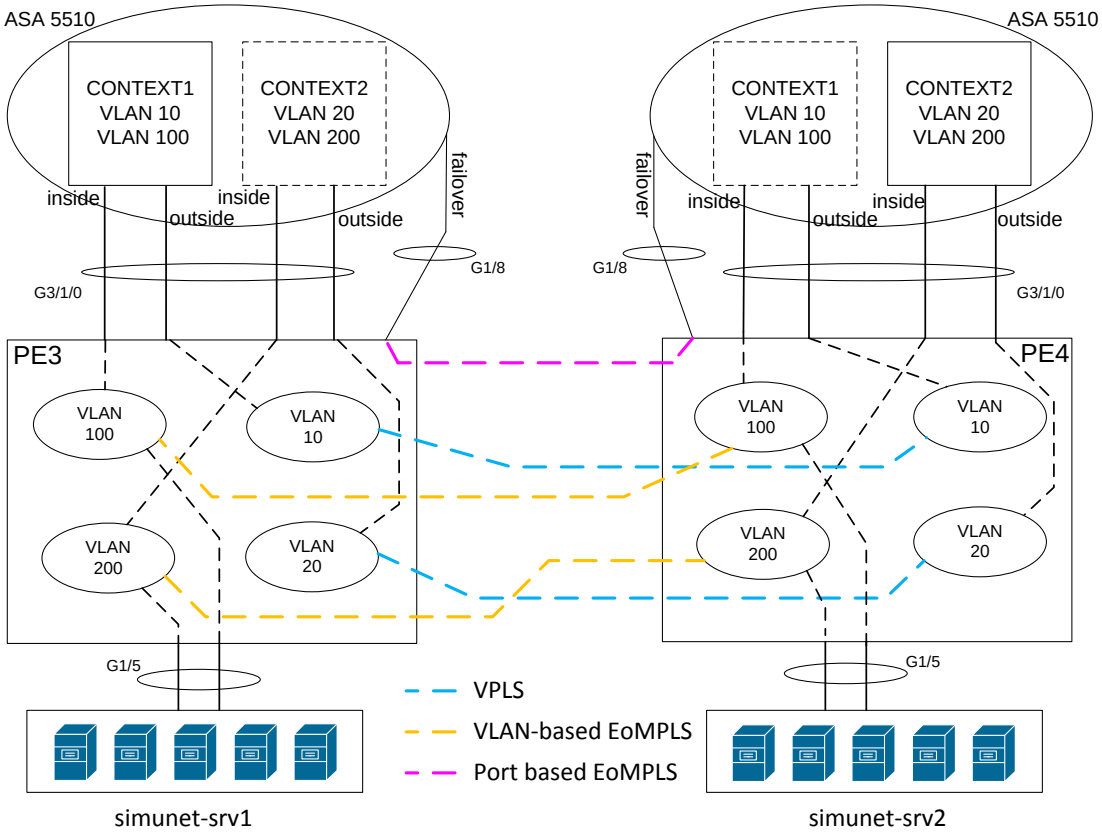


Kuva 8. Palomuurien fyysinen topologia

Loogisesti palomuurit sijaitsevat palvelinklusterin virtuaalikoneiden ja muun verkon välissä. Laitteissa toimii kaksi palomuuri-contextia, joista toinen käsittelee *simunet-srv1*- ja toinen *simunet-srv2* -palvelinlaitteen liikenteen. Kummassakin palomuuri-contextissa on sisäverkon ja ulkoverkon portti, jotka kaikki jakavat saman fyysisen

median palomuurin ja PE-laitteen välillä. Liikenne ohjataan oikeaan palomuuri-contextiin ja porttiin VLAN-merkinnän perusteella.

Palomuuri-contextien ulkoverkon reunan käyttämät Bridge Domain –alueet PE-laitteissa on yhdistetty käyttämällä VPLS-palvelua ja palomuuri-contextien sisäverkon reuna tarttuu palvelinklusterin virtuaalikoneiden verkkoihin. Kumpikin palomuuri-contexti on aktiivinen yhdessä laitteessa kerrallaan ja toisessa se odottaa passiivisena. Kuva 9 kuvastaa miten palomuurit loogisesti ovat yhteydessä palvelinlaitteisiin ja toisiinsa. Kuvassa aktiivinen palomuuri-contexti on rajattu yhtenäisellä viivalla ja katkoviivalla rajattu esittää standby-tilassa odottavaa.



Kuva 9. Palomuurien looginen topologia

VLAN 100 ja VLAN 200 ovat palvelinklusterin virtuaalikoneiden verkkoja. VLAN 10 ja VLAN 20 ovat palomuuri-contextien ulkopuolen verkot ja niiden SVI-rajapinnoissa on myös IP-osoitteet ulkoverkkoon liikennöintiä varten. Palomuurit ovat reitittävässä tilassa ja toimivat oletusyhdyskäytävänä palvelinklusterin virtuaalikoneille. Vastaavasti PE-laitteiden VLAN 10 ja VLAN 20 Bridge Domain –alueiden SVI-rajapinnat toimivat oletusyhdyskäytävinä palomuureille.

Active/active -failover vaatii lisäksi palomuurilaitteiden välille failover-kaapelin, jonka avulla ne keskustelevat keskenään. Failover-kaapelia varten täytyy käytetyissä palomuurilaitteissa varata oma fyysinen portti. Failover-kaapeli kytkeytyy PE-laitteeseen ja sen liikenne kuljetetaan porttipohjaisen EoMPLS-palvelun avulla laitetilasta toiseen.

11.3 Toteutus

Toteutus alkoi konfiguroimalla porttipohjainen EoMPLS-palvelu palomuurien failover-liikenteen kuljettamista varten. Porttipohjaista EoMPLS-palvelua käytettäessä *xconnect*-komento konfiguroidaan suoraan käytettävään liityntärajapintaan ja sille annetaan parametreiksi naapurilaitteen IP-osoite, instanssien erottelemiseen käytettävä VPN ID ja enkapsulointitapa. Portin MTU-arvoksi on asetettava molempiin päihin sama arvo ja vähintään 1504 tavua, jotta mahdollinen VLAN-merkintä mahtuu kulkemaan pakettien mukana. Laitteet eivät ilmoita mitään, jos MTU-arvo on liian pieni, mutta tunnelin tila ei vaihdu aktiiviseksi ennen kuin se on asetettu riittävän suureksi. PE3- ja PE4-laitteiden konfiguraatiot eivät eroa kuin IP-osoitteiden osalta. Alla esiintyvissä esimerkeissä esitetään PE3-laitteen konfigurointia:

```
PE3(config)#interface GigabitEthernet1/8
PE3(config-if)#mtu 1600
PE3(config-if)#xconnect 172.30.0.4 300 encapsulation mpls
```

Palomuuri-contextien ulkopuolen verkot VLAN 10 ja VLAN 20 yhdistettiin samaksi Layer 2 –alueeksi VPLS-palvelun avulla. VPLS käyttää omaa VSI-konfigurointitilaa, jonka alle naapurilaitteet määritetään. Ensiksi VFI:lle annetaan VPN ID, jonka avulla tunnistetaan samaan VPLS-toimialueeseen kuuluvat PE-laitteet. VPN ID lisätään jokaisen saman VFI:n alle luodun Pseudowire-linkin ID-kenttään. Se ei siis saa mennä päällekkäin Point-to-point -ratkaisuissa käytettyjen ID-numeroiden kanssa. *Neighbor*-komennoilla VFI:hin lisätään jokainen samaan VPLS-instanssiin osallistuvan PE-laitteen IP-osoite ja kerrotaan liikenteen enkapsulointitapa. Näiden perusteella VPLS luo laitteiden välille Pseudowire-linkit. Tässä tapauksessa VPLS-intanssiin osallistuu vain kaksi laitetta, joten vain yksi naapurilaite lisätään kummallekin laitteelle. Bridge Domain alue liitetään tähän luotuun instanssiin konfiguroimalla *xconnect*-komento SVI-rajapintaan ja antamalla sen parametriksi luodun instanssin nimi:

```
PE3(config)#l2 vfi VFI FW_OUT_10 manual
PE3(config-vfi)#vpn id 10
PE3(config-vfi)#neighbor 172.30.0.4 encapsulation mpls
PE3(config-vfi)#exit
PE3(config)#interface vlan 10
PE3(config-if)#xconnect vfi FW_OUT_10
PE3(config-if)#exit

PE3(config)#l2 vfi VFI FW_OUT_20 manual
PE3(config-vfi)#vpn id 20
PE3(config-vfi)#neighbor 172.30.0.4 encapsulation mpls
PE3(config-vfi)#exit

PE3(config-if)#interface vlan 20
PE3(config-if)#xconnect vfi FW_OUT_20
```

Palomuurit ovat yksikätisinä kiinni PE-laitteissa ja VLAN-alueet jakavat saman fyysisen median. Palomuurin päässä liikenne erotetaan VLAN-merkinnän perusteella oikeaan palomuuri-contextiin ja se terminoituu aliliityntäportteihin. PE-laitteiden päässä liikenne ohjataan haluttuun Bridge Domain -alueeseen EVC framework -portin avulla. Porttiin konfiguroitiin jokaista VLAN-merkintää kohden Service Instance. Service Instanceja käytettäessä porttiin saapuvan liikenteen VLAN-merkinnöillä on vain porttikohtaista merkitystä. Tässä tilanteessa ei ollut kuitenkaan estettä käyttää samoja VLAN-numeroita alusta loppuun saakka, joten niin tehtiin selkeyden vuoksi. Jokaista VLANia kohden luotiin oma Service Instance. Komennolla *encapsulation* saadaan kerättyä liikenne VLAN-merkinnän perusteella kyseiseen Service Instanceen. *Rewrite*-komennon avulla porttiin tulevista kehyksistä poistetaan VLAN-merkintä ja *bridge-domain* –komennon avulla ohjataan liikenne haluttuun Bridge Domain -alueeseen. *Rewrite*-käskyn parametri *symmetric* määrittää Service Instancen tekemään portista lähtevälle liikenteelle päinvastaisen toimenpiteen, eli *encapsulation* komennon määrittelemä VLAN-tagi lisätään jokaiseen portista ulospäin lähtevään kehykseen. Portti on siis konfiguroitu käsittelemään liikenne trunk-tilassa toimivan kytkinportin tavoin:

```
PE3(config-if)#interface gigabitethernet 3/1/0
PE3(config-if)#service instance 1 ethernet
PE3(config-if-srv)#encapsulation dot1q 10
PE3(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE3(config-if-srv)#bridge-domain 10
PE3(config-if-srv)#exit
```

```
PE3(config-if)#service instance 2 ethernet
PE3(config-if-srv)#encapsulation dot1q 20
PE3(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE3(config-if-srv)#bridge-domain 20
PE3(config-if-srv)#exit

PE3(config-if)#service instance 3 ethernet
PE3(config-if-srv)#encapsulation dot1q 100
PE3(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE3(config-if-srv)#bridge-domain 100
PE3(config-if-srv)#exit

PE3(config-if)#service instance 4 ethernet
PE3(config-if-srv)#encapsulation dot1q 200
PE3(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE3(config-if-srv)#bridge-domain 200
```

VPLS- ja EoMPLS-palveluiden tila voidaan tarkistaa esimerkiksi komennolla *show mpls l2transport vc*. Tulosteen viimeisestä kentästä nähdään, että kyseinen tunneli on ylhäällä. Alla komennon antama tuloste PE3-laitteesta:

```
PE3#show mpls l2transport vc | include Status | 10 | 20 | 300
Local intf     Local circuit   Dest address    VC ID      Status
VFI FW_OUT_10  VFI             172.30.0.4      10         UP
VFI FW_OUT_20  VFI             172.30.0.4      20         UP
Gi1/8          Ethernet        172.30.0.4      300        UP
```

PE-laitteisiin konfigurointiin Hot Standby Router Protocol (HSRP) tarjoamaan redundanttisen oletusyhdyskäytävän palomuureille. HSRP on Cisco Systemsin kehittämä protokolla, joka vastaa toiminnallisuudeltaan IETF:n kehittämää Virtual Router Redundancy (VRRP) -protokollaa. PE3- ja PE4-laitteet muodostavat parin, missä toinen laite hoitaa reititystä ja toinen laite odottaa varalla. HSRP-prosessi muodostaa laitteille yhteisen virtuaalisen IP-osoitteen. Laitteen liikennöidessä tähän virtuaaliseen osoitteeseen liikenne terminoidaan HSRP:n aktiivisen reunan laitteen SVI-rajapintaan ja reititetään eteenpäin.

Laitteiden SVI-rajapintaan määritetään paikalliset IP-osoitteet ja sen lisäksi yhteinen virtuaalinen IP-osoite. Tähän yhteiseen virtuaaliseen osoitteeseen palomuurien ulkoverkkoon päin kulkeva liikenne reititetään. PE-laitteet laitteet ohjaavat liikenteen HSRP-aktiivisen laitteen SVI-rajapintaan ja liikenne välitetään eteenpäin käyttäen ra-

japinnan paikallista IP-osoitetta. HSRP:n prioriteetti määritettiin Site3-laitetilan puolella suuremmaksi VLAN 10:n liikenteelle ja Site4-laitetilan puolella suuremmaksi VLAN 20:n liikenteelle. Näin varmistetaan, että normaalitilanteessa HSRP:n aktiivinen reuna on samassa laitetilassa kuin siihen liikennöivän palomuuri-contextin aktiivinen reuna. Laitteissa käynnistettiin myös HSRP:n preempt-toiminto. Se sallii standby-laitteen omaksua aktiivisen laitteen rooli heti, jos sen prioriteetti kasvaa sen hetkistä aktiivista laitetta suuremmaksi. Ensin laitteisiin konfiguroitiin HSRP-prosessit kummankin palomuuri-contextin IPv4-liikennettä varten:

```
PE3(config)#interface vlan 10
PE3(config-if)#ip address 172.30.1.3 255.255.255.248
PE3(config-if)#standby 10 ip 172.30.1.5
PE3(config-if)#standby 10 priority 150
PE3(config-if)#standby 10 preempt

PE3(config-if)#interface vlan 20
PE3(config-if)#ip address 172.31.1.3 255.255.255.248
PE3(config-if)#standby 20 ip 172.30.1.5
PE3(config-if)#standby 20 preempt
```

IPv6-liikennettä varten tehtiin omat HSRP-prosessit. IPv6-osoitetta käytettäessä on HSRP:n versio kaksi ensin otettava käyttöön. Virtuaalinen IP-osoite on link local –osoite ja se voidaan määrittää itse tai generoida automaattisesti. Ennen virtuaalisen osoitteen asettamista tai generoimista täytyy SVI-rajapinnalla olla paikallinen IPv6 link local –osoite. Se generoituu automaattisesti, kun IPv6 käynnistetään porttitasolla tai sille annetaan julkinen osoite. Paikalliset ja virtuaaliset link-local -osoitteet määritettiin käsin lyhyemmän osoitteen tarjoaman selkeyden vuoksi:

```
PE3(config)#interface vlan 10
PE3(config-if)#ipv6 address 2a00:1dd0:100:a1::3/64
PE3(config-if)#ipv6 address fe80:a1::3 link-local
PE3(config-if)#standby version 2
PE3(config-if)#standby 110 ipv6 fe80::1
PE3(config-if)#standby 110 priority 150
PE3(config-if)#standby 110 preempt

PE3(config-if)#interface vlan 20
PE3(config-if)#ipv6 address 2a00:1dd0:100:a2::3/64
PE3(config-if)#ipv6 address fe80:a2::3 link-local
PE3(config-if)#standby version 2
PE3(config-if)#standby 120 ipv6 fe80::2
PE3(config-if)#standby 120 preempt
```

HSRP:n tilan voi tarkistaa esimerkiksi komennolla *show standby brief*. Tulosteesta nähdään, että HSRP on havainnut naapurilaitteen ja asettanut paikallisen laitteen aktiiviseksi HSRP-ryhmille 10 ja 110. Alla komennon antama tuloste PE3-laitteesta:

PE3#show standby brief

Interface	*Grp*	*Pri*	*P*	*State*	*Active*	*Standby*	*Virtual IP*
Vl10	*10*	*150*	*P*	*Active*	*local*	*172.30.1.4*	*172.30.1.5*
Vl10	*110*	*150*	*P*	*Active*	*local*	*FE80:A1::4*	*FE80::1*
Vl20	*20*	*100*	*P*	*Standby*	*172.31.1.4*	*local*	*172.31.1.5*
Vl20	*120*	*100*	*P*	*Standby*	*FE80:A2::4*	*local*	*FE80::2*

Palomuuri-contexteihin konfiguroitiin IPv4- ja IPv6-oletusreitit osoittamaan kohti virtuaalista oletusyhdyskäytävän osoitetta. Alla Site3-laitetilan palomuuri-contextin konfigurointi:

ciscoasa/KOTKA(config)#route outside 0.0.0.0 0.0.0.0 172.30.1.5 1
ciscoasa/KOTKA(config)#ipv6 route outside ::/0 fe80::1

Palomuureissa ei ole mahdollista käyttää dynaamisia reititysprotokollia multiple context –tilassa. PE-laitteille täytyy kuitenkin saada reitti palomuurien takana sijaitseviin verkkoihin, jotta liikenne osataan reitittää ulkoverkosta palomuurin sisäverkkoon. PE3 ja PE4 –laitteisiin konfiguroitiin staattiset reitit liikenteelle kohti palvelimien verkkoa. Äkkiseltään voisi luulla, että nämä staattiset reitit rikkovat verkon redundanttisuuden, koska ne eivät ota huomioon verkon muutoksia. Näin ei kuitenkaan ole, koska reittimäärityksessä osoitetaan virtuaalisen palomuurin osoitteeseen. Palomuurin vikaantuessa tämä palomuuri-contexti vaihtaa paikkaa toisen laitetilaan, mutta sen MAC- ja IP-osoitetiedot säilyvät ennallaan ja se sijaitsee vieläkin loogisesti samassa Layer 2 -segmentissä. Reittitieto verkkoa kohti pysyy siis täsmälleen samana. Staattiset reitit konfiguroitiin SimuNetin IPv4- ja IPv6-palvelinverkoille. PE3- ja PE4-laitteet konfiguroitiin samalla tavalla. Alla PE3-laitteen konfigurointi:

PE3(config)#ip route 172.30.2.0 255.255.255.0 172.30.1.1
PE3(config)#ip route 172.31.2.0 255.255.255.0 172.31.1.1

PE3(config)# ipv6 route 2a00:1dd0:100:b1::/64 vlan10 fe80:a1::1
PE3(config)# ipv6 route 2a00:1dd0:100:b2::/64 vlan20 fe80:a2::1

Reitit palvelimien IPv4-verkkoihin levitetään muille SimuNetin PE-laitteille tuomalla staattiset reitit mukaan OSPF-prosessiin. Runkoyhteydet vain toimivat IPv4-protokollalla, joten IPv6-verkot täytyy levittää BGP:n avulla lisäämällä ne BGP:n IPv6 address-family –ryhmän alle. Työtä tehdessä vain PE3- ja PE4-laitteisssa on IPv6 käytössä, mutta kun se otetaan myöhemmin mukaan myös muihin verkon PE-laitteisiin, mainostaa BGP-protokolla palvelimien IPv6-verkot myös niille. Alle PE3-laitteen konfigurointi:

PE3(config)#router ospf 1
PE3(config-router)#redistribute static subnets

PE3(config)#router bgp 65001
PE3(config-router)#address-family ipv6
PE3(config-router-af)#network 2a00:1dd0:100:b1::/64
PE3(config-router-af)#network 2a00:1dd0:100:b2::/64

11.4 Palomuurien ohitus

11.4.1 Yleistä

Palvelinklusterin virtuaalikoneille huomattiin myös tarve päästä liikennöimään ulkoverkkoon suoraan ohittamalla niiden edustapalomuurit. Palvelinklusteriin luotiin uusi virtuaaliverkko, jonka liikennettä ei ohjata palomuurilaitteiden läpi, vaan liikenne päätetään suoraan PE-laitteiden SVI-rajapintaan. Tämän verkon avulla päästää kokeilemaan, ettei jonkin palvelun toimimattomuus johdu palomuurien suodatussäännöksistä. Ohitusta ei ole tarkoitus käyttää lopullisena ratkaisuna, vaan pikemminkin väliaikaiseen yhteyksien testaukseen.

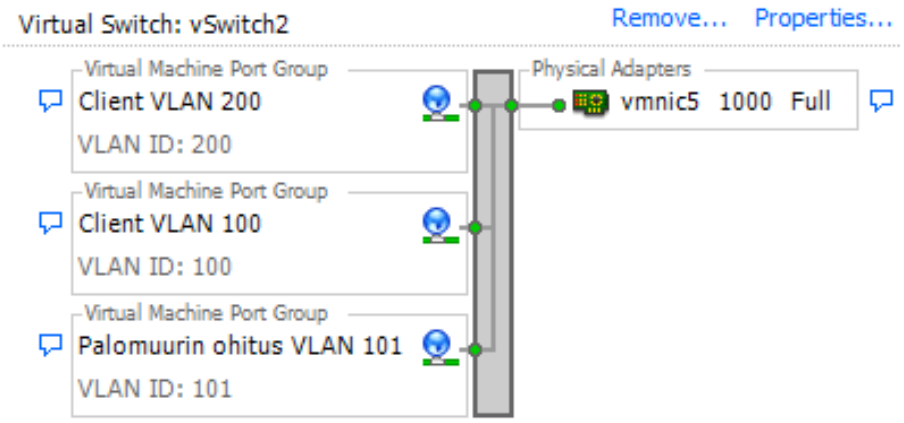
Virtuaalikoneen saa liitettyä tähän verkkoon valitsemalla sen asetuksista käyttöön *Palomuurin ohitus VLAN 101* virtuaaliverkon. Palomuurien ohitukseen oli ollut tarvetta vain IPv6-puolella, joten tähän verkkoon konfiguroitiin vain IPv6-osoiteavaruus. Osoitteet tähän verkkoon liitetyille virtuaalikoneille annetaan taulukon 2 mukaisesti.

Taulukko 2. Virtuaalikoneiden IP-osoitteet verkkoon VLAN 101.

	VLAN 100
Virtuaalikoneiden osoiteavaruus	2a00:1dd0:100:c1:: /64
Virtuaalikoneiden oletusyhdyskäytävä	fe80:c1::1

11.4.2 Toteutus

Palvelinklusteriin tehtiin uusi virtuaaliverkko saman virtuaalikytkimen alle, josta muukin tuotantoliikenne kulkee ja asetettiin sen liikenteeseen merkattavaksi 802.1Q VLAN-merkintä 101 (ks. kuva 10).



Kuva 10. Virtuaalikytkin VMware ESX –palvelinlaitteen verkkoasetuksissa

PE-laitteisiin luotiin VLAN 101 ja se sallittiin kuljetettavaksi PE-laitteiden ja palvelinklusterin välistä linkkiä pitkin VLANien 100 ja 200 lisäksi. Alla esiintyvissä esimerkeissä esitetään PE3-laitteen konfigurointia:

PE3(config)#vlan 101
PE3(config-vlan)#name Palomuurin_ohitus
PE3(config-vlan)#exit

PE3(config)#interface GigabitEthernet1/5
*PE3(config-if)#switchport trunk allowed vlan 100,**101**,200*

PE-laitteiden VLAN 101 Bridge Domain –alueet laitteiden välillä yhdistettiin VLAN-pohjaista EoMPLS-palvelua käyttäen, konfiguroimalla *xconnect* SVI-rajapintaan:

PE3(config)#interface vlan 101
PE3(config-if)#xconnect 172.30.0.4 101 encapsulation mpls

EoMPLS-tunnelin tila tarkistettiin komennolla *show mpls l2transport vc.* Alla komennon antama tuloste PE3-laitteesta*:*

```
PE3#show mpls l2transport vc | inc Status | 101
Local intf     Local circuit      Dest address    VC ID      Status
Vl101          Eth VLAN 101       172.30.0.4      101        UP
```

HSRP konfigurointiin tarjoamaan oletusyhdyskäytävän osoite suoraan tähän verkkoon liitetyille virtuaalikoneille. HSRP konfiguroitiin vain IPv6-osoitteille, mutta jos tarvetta tulee, IPv4-osoitteet voidaan lisätä helposti rinnalle luomalla toinen HSRP-prosessi. HSRP virtuaalista IP-osoitetta käytetään oletusyhdyskäytävänä virtuaalikoneille:

```
PE3(config)#interface vlan 101
PE3(config-if)#ipv6 address 2a00:1dd0:100:c1::3/64
PE3(config-if)#ipv6 address fe80:101::3 link-local
PE3(config-if)#standby version 2
PE3(config-if)#standby 101 ipv6 fe80:c1::1
PE3(config-if)#standby 101 priority 150
PE3(config-if)#standby 101 preempt
```

HSRP:n toiminta tarkistettiin komennolla *show standby brief.* Alla komennon antama tuloste PE3-laitteesta*:*

```
PE3#show standby bri | inc State | 101
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl101       101  150 P Active  local           FE80:101::4     FE80:c1::1
```

12 CASE WLAN-OHJAIMET

SimuNet-verkkoon asennetaan myöhemmin kahdennetut WLAN-ohjaimet. WLAN-ohjaimia varten verkkoon luotiin valmius toteuttamalla niiden vaatimat yhteydet valmiiksi laitetilojen välille. Yhteydet toteutettiin käyttäen VPLS- ja H-VPLS –palveluita.

12.1 Yleistä

Langattomat lähiverkot ovat yleistyneet yritysverkoissa ja myös niitä on alettu myydä palveluna yritysasiakkaille. Yritysasiakkaan kannalta langattomien lähiverkkojen käyttöönotto saadaan näin vaivattomaksi. Operaattorin verkkoon sijoitetaan keskitetyt ohjainlaitteet, johon yrityksen verkkoon sijoitettavat LWAPP (Lightweight Access

Point Protocol) -tukiasemat ottavat yhteyden ja muodostavan tunnelin. Kaikki loppukäyttäjien liikenne kulkee LWAPP-tunnelin läpi WLAN-ohjaimiin ja siitä edelleen muualle verkkoon. WLAN-ohjaimet kannattaa ehdottomasti kahdentaa riittävän palvelun saatavuuden tavoittamiseksi.

Tukiaseman takana olevien loppukäyttäjien täytyy pysyä samassa verkossa, vaikka toinen WLAN-ohjain vikaantuisi, ettei niiden osoitetietoja tarvitse uusia yhteyden palauttamiseksi. Yhteydet pitää siis toteuttaa niin, että molempien WLAN-ohjaimien kautta on pääsy samaan Layer 2 –segmenttiin.

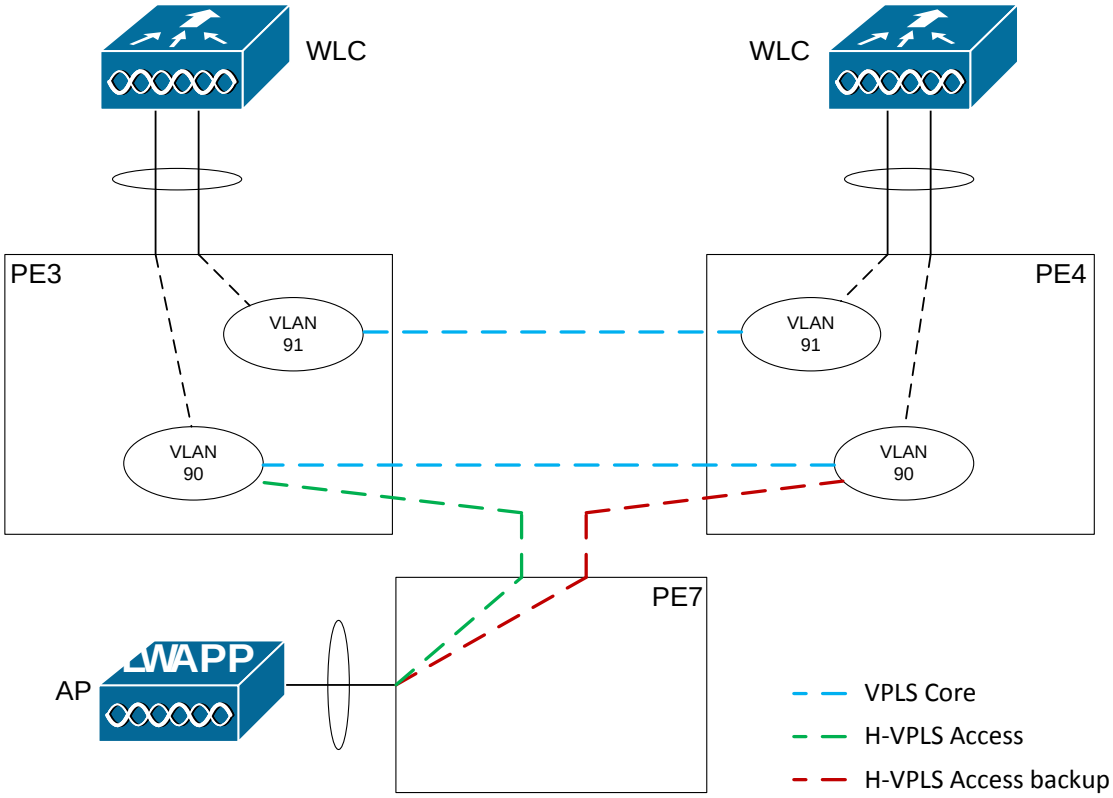
SimuNetiin tulevia kahdennettuja WLAN-ohjaimia varten luotiin valmiiksi pohjaksi niiden tarvitsemat yhteydet käyttäen VPLS- ja H-VPLS -palvelua. Kahdennettuja WLAN-ohjaimia käyttävää toteutusta tutkittiin Hakkaraisen ja Vanhalan (2011) opinnäytetyössä, ja ne on jatkossa tarkoitus siirtää SimuNet-verkkoon. SimuNetiin siirtoa varten WLAN-ohjaimien ja LWAPP-tukiasemien välinen fyysinen verkko toteutettiin loogisesti SimuNetin PE-laitteiden välille. Tarkoituksena oli säilyttää sama verkkotopologia ja VLAN-numerointi, jotta WLAN-ohjaimet voitaisiin lisätä SimuNet-verkkoon suoraan niiden konfiguratioon puuttumatta. Kuva Hakkaraisen ja Vanhalan (2011) opinnäytetyössä toteutetusta verkosta löytyy liitteestä 2.

WLAN-ohjaimet on tarkoitus kytkeä PE3- ja PE4-laitteisiin ja LWAPP-tukiasema verkon toiselle reunalle PE7-reitittimen taakse. Lisäksi LWAPP-tukiaseman takana olevia asiakaslaitteita varten palvelinklusteriin asennetaan jatkossa DHCP-palvelin.

Verkkoon tarvitaan VLAN-alue, johon LWAPP-tukiasemat sijoitetaan sekä oma VLAN-alue jokaisen asiakkaan loppukäyttäjiä varten, jotta eri asiakkaiden liikenne saadaan pidettyä toistaan erillään. Tehdyssä projektityössä WLAN-ohjaimet ja LWAPP-tukiasemat ovat kommunikoineet keskenään käyttäen VLAN 10 –verkkoa ja asiakkaan loppukäyttäjät ovat sijainneet VLAN 50 –verkossa. Nämä VLAN-numerot olivat kuitenkin jo käytössä molemmissa PE-laitteissa, joten kyseistä VLAN-numerointia käytettiin vain PE-laitteiden ja WLAN-ohjaimien välillä ja PE-laitteen rajapinnassa liikenne ohjataan eri Bridge Domain –alueeseen, kuin mihin saapuvan liikenteeen Service-Delimiting VLAN -merkintä osoittaa. Lisäksi loppukäyttäjille piti mahdollistaa liikennöinti Internettiin ja ohjata niiden DHCP-kyselyt palvelinklusteriin tulevaan DHCP-palvelimeen.

12.2 Topologia

WLAN-ohjaimia varten PE3- ja PE4-laitteissa on kaksi VPLS-instanssia. VLAN 90 on WLAN-ohjaimien ja LWAPP-tukiasemien välistä kommunikointia ja VLAN 91 on ensimmäisen asiakkaan loppukäyttäjien liikennettä varten. Kuva 11 esittää WLAN-ohjaimia varten tehtyjä loogisia yhteyksiä.



Kuva 11. WLAN-ohjaimien looginen topologia

PE3- ja PE4-laitteiden VLAN 90 Bridge Domain –alueet on yhdistetty Full Mesh VPLS-palvelun avulla ja PE7-laite tarttuu samaan instanssiin mukaan H-VPLS liityntätason laitteena. Oletusarvoisesti PE7-laitteen yhteys on muodostettu PE3-laitteeseen, mutta linkin vikaantuessa otetaan varayhteys PE4-laitteeseen. VLAN 91 Bridge Domain –alueet on myös yhdistetty VPLS-palvelun avulla ja mukaan tähän instanssiin liittyvät vain WLAN-ohjaimet. Siihen kuuluvissa SVI-rajapinnoissa on myös IP-osoitteet ulkoverkkoon liikennöintiä varten sekä loppukäyttäjien DHCP-kyselyjen välittämiseen eri verkossa sijaitsevalle DHCP-palvelimelle.

12.3 Toteutus

Toteutus aloitettiin luomalla Layer 2 -tason yhteydet WLAN-ohjaimien ja LWAPP-tukiasemien väliseen kommunikointiin. LWAPP-tukiasema sijoitetaan PE7-laitteen taakse. Tämä PE-laite ei tue VPLS-tekniikoita, mutta se voidaan liittää osaksi samaa VPLS-instanssia H-VPLS:n Hub-Spoke -topologiaa käyttäen. VLAN 90 Bridge Domain –alueita PE3- ja PE4 –laitteiden välillä yhdistämään luotiin VPLS-instanssi ja PE7 tarttuu samaan instanssiin mukaan EoMPLS-tunnelin avulla. PE7-laitteen Pseudowire-linkki päätetään oletusarvoisesti PE3-laitteeseen, mutta sen vikaantumisen varalle PE7-laitteesta on Pseudowire-linkki myös PE4-laitteeseen. Tämä linkki on oletusarvoisesti alhaalla ja nousee ylös, jos ensisijainen linkki vikaantuu. PE7-laitteeseen päin osoittavasta Pseudowire-linkistä poistettiin Split Horizon -sääntö, jotta muiden Pseudowire-linkien kautta vastaanotettu liikenne voidaan kytkeä sinne. Tämä on tarpeellista, koska PE7-laite tarttuu VPLS-instanssiin vain yhdellä Pseudowire-linkillä Full Mesh –topologian sijasta, joten kaikki liikenne ei muuten kulkisi perille asti. Alla PE3- ja PE7-laitteen konfigurointi:

```
PE3(config)#l2 vfi WLC manual
PE3(config-vfi)#vpn id 90
PE3(config-vfi)#neighbor 172.30.0.4 encapsulation mpls
PE3(config-vfi)#neighbor 172.30.0.7 encapsulation mpls no-split-horizon

PE3(config)#interface vlan 90
PE3(config-if)#mtu 1600
PE3(config-if)#xconnect vfi WLC

PE7(config)#interface fastethernet 0/0.13
PE7(config-subif)#description WLAN AP
PE7(config-subif)#encapsulation dot1q 13
PE7(config-subif)#xconnect 172.30.0.3 90 encapsulation mpls
PE7(config-subif-xconn)#backup peer 172.30.0.4 90
```

Asiakkaan loppukäyttäjien liikennettä varten luotiin toinen VPLS-instanssi. Jos asiakkaita halutaan myöhemmin lisätä, luodaan jokaiselle uudelle asiakkaalle vastaavasti uusi oma VPLS-instanssi, jotta asiakkaiden liikenne saadaan pidettyä erillään. Tämä instanssi toimii vain WLAN-ohjaimien välillä. VPLS-instanssiin kuuluviin SVI-rajapintoihin määriteltiin lisäksi IP-osoitteet ulkoverkkoon liikennöintiä varten. Alla PE3-laitteen konfigurointi:

```
PE3(config)#l2 vfi WLC_C1 manual
PE3(config-vfi)#vpn id 91
PE3(config-vfi)#neighbor 172.30.0.4 encapsulation mpls
PE3(config-vfi)#exit

PE3(config)#interface vlan 91
PE3(config-if)#mtu 1600
PE3(config-if)#xconnect vfi WLC
PE3(config-if)#ip address 172.30.91.3 255.255.255.0
```

PE3- ja PE4-laitteisiin konfiguroitiin portti WLAN-ohjaimien liittämistä varten. Portissa käytettiin Cisco EVC Framework –tekniikkaa. Tämän avulla voitiin käyttää PE-laitteissa liikenteen Service-Delimiting VLAN -numeroinnista riippumatonta Bridge Domain –aluetta. PE7-laitteen EoMPLS-tunnelista saapuvaan liikenteeseen jää VLAN-merkintä 13. Tämä VLAN-merkintä vaihdetaan *rewrite*-käskyn avulla WLAN-ohjaimien reunalla käytettävään arvoon, eli arvoon 10 ja päinvastoin. VLAN 50 –merkinnällä saapuvasta liikenteestä poistetaan vain VLAN-merkintä ennen sen ohjaamista Bridge Domain -alueeseen ja vastaavasti lisätään merkintä portista lähtevään liikenteeseen. Alla PE3-laitteen konfigurointi:

```
PE3(config)#interface GigabitEthernet3/1/3
PE3(config-if)#description WLC EVC
PE3(config-if)#mtu 1600
PE3(config-if)#service instance 1 ethernet
PE3(config-if-srv)#encapsulation dot1q 10
PE3(config-if-srv)#rewrite ingress tag translate 1-to-1 dot1q 13 symmetric
PE3(config-if-srv)#bridge-domain 90
PE3(config-if-srv)#exit

PE3(config-if)#service instance 2 ethernet
PE3(config-if-srv)#encapsulation dot1q 50
PE3(config-if-srv)#rewrite ingress tag pop 1 symmetric
PE3(config-if-srv)#bridge-domain 91
```

PE4- ja PE7-laitteiden välinen tunneli ei ole normaalitilassa toiminnassa, vaan se vaihtaa tilansa aktiiviseksi, jos PE3- ja P7-laitteiden välinen tunneli vikaantuu. Tunnelien tila voidaan tarkistaa *show mpls l2transport vc* komennolla. Alla komennon antama tuloste laitteista PE3, PE3 ja PE7:

PE3#show mpls l2transport vc | include Status | 90 | 91

Local intf	*Local circuit*	*Dest address*	*VC ID*	*Status*
VFI WLC	*VFI*	*172.30.0.4*	*90*	*UP*
VFI WLC_C1	*VFI*	*172.30.0.4*	*91*	*UP*
VFI WLC	*VFI*	*172.30.0.7*	*90*	*UP*

PE4#show mpls l2transport vc | include Status | 90 | 91

Local intf	*Local circuit*	*Dest address*	*VC ID*	*Status*
VFI WLC	*VFI*	*172.30.0.3*	*90*	*UP*
VFI WLC_C1	*VFI*	*172.30.0.3*	*91*	*UP*
VFI WLC	*VFI*	*172.30.0.7*	*90*	*DOWN*

PE7#show mpls l2transport vc | include Status | 90

Local intf	*Local circuit*	*Dest address*	*VC ID*	*Status*
Fa0/0.13	*Eth VLAN 13*	*172.30.0.3*	*90*	*UP*
Fa0/0.13	*Eth VLAN 13*	*172.30.0.4*	*90*	*DOWN*

HSRP-protokolla konfiguroitiin tarjoamaan virtuaalinen oletusyhdyskäytävän osoite loppukäyttäjille. Alla PE3-laitteen konfigurointi:

```
PE3(config)#interface vlan 91
PE3(config-if)#standby 91 ip 172.30.91.5
PE3(config-if)#standby 91 priority 150
PE3(config-if)#standby 91 preempt
```

HSRP:n toiminta tarkistettiin komennolla *show standby brief.* Alla tuloste PE3-laitteesta*:*

PE3#show standby brief | include State | 91

Interface	*Grp*	*Pri*	*P*	*State*	*Active*	*Standby*	*Virtual IP*
Vl91	*91*	*150*	*P*	*Active*	*local*	*172.30.91.4*	*172.30.91.5*

PE-laitteiden SVI-rajapinnat konfiguroitiin muuntamaan niihin saapuvat DHCP-kyselyt unicast-lähetyksiksi ja ohjaamaan ne palvelinklusteriin, johon DHCP-palvelin myöhemmin lisätään. Tässä olisi ollut paikallaan näiden komentojen liittäminen osaksi HSRP-prosessia HSRP redundancy group –toiminnon avulla. Näin komento olisi käytössä vain HSRP:n aktiivisella reunalla, eikä molemmissa laitteissa yhtä aikaa. Työn aikana käytössä olleesta IOS-ohjelmistoversiossa (15.1(1)S1) ei kyseistä ominaisuutta kuitenkaan löytynyt. Käytetyllä konfiguraatiolla DHCP-kyselyt lähetetään DHCP-palvelimelle turhaan kahteen kertaan. Komentoa ei kuitenkaan voi vain jättää

pois toisesta laitteesta, sillä silloin DHCP ei toimi, jos kyselyjä välittävä laite vikaantuu. Alla PE3-laitteen konfiguraatio:

PE3(config)#interface vlan 91
PE3(config-if)#ip helper-address 172.30.2.90
PE3(config-if)#ip dhcp relay information trusted

13 TULEVAISUUS

Työssä tehdyt ratkaisut pyrittiin tekemään niin, ettei verkkoon jää yhden pisteen vian mahdollisuutta. Työn ohessa yhteyksiä on testattu ja verkko vaikuttaisi konvergoituvan vikatilanteissa suunnitellusti. Jatkossa voitaisiin kuitenkin tehdä järjestelmällinen selvitys SimuNetin palveluiden ja verkon eri osien konvergoitumisnopeudesta ja viritää konvergoitumisajat optimaalisiksi.

WLAN-ohjaimia varten tehdyssä konfiguraatiossa DHCP-kyselyt välitetään DHCP-palvelimelle kahteen kertaan. Jos tämä sotkee DHCP-palvelimen toimintaa, täytyy sen estämiseksi kehittää jokin ratkaisu. HSRP redundancy group –toiminto olisi hyvä juuri tähän tarkoitukseen, jos sen käyttö tulee myöhemmin tehtävien ohjelmistopäivitysten myötä mahdolliseksi.

14 YHTEENVETO

14.1 SimuNet

SimuNet-verkossa on aina useita projektitöitä yhtä aikaa meneillään, ja ne ovat monesti riippuvaisia toisistaan. Montaa projektia on häirinnyt, kun palvelinklusteri ja sen edustapalomuurien kokonaisuus ei ole ollut valmis ja työtä on jouduttu muuttamaan tai miettimään väliaikaisratkaisuja sen toteuttamiseksi. Kaikki palvelinklusterin ja palomuurien tarvitsemat yhteydet laitetilojen välille saatiin nyt luotua, ja ne tarjoavat toimivan pohjan uusille projekteille. Myös kahdennettuja WLAN-ohjaimia varten saatiin luotua yhteydet, joiden avulla teoriassa palvelu pitäisi saada toimintakuntoon, lisäämällä vain itse WLAN-ohjainlaitteet ja DHCP-palvelin SimuNet-verkkoon. Käytännössä saattaa kuitenkin vielä ilmetä asioita, joita ei ole osattu tai pystytty ottamaan ennalta huomioon.

Työn pääasiallinen tavoite oli tuoda SimuNetin palvelut toimintakuntoon toteuttamalla kahdennettujen palveluiden tarvitsemat yhteydet laitetilojen välille. Tässä tavoitteessa onnistuttiin mielestäni hyvin ja palvelujen toiminnan myötä SimuNet-verkkoa saatiin kehitettyä eteenpäin. SimuNet-verkko myös laajeni testiympäristönä selvästi, kun uudet PE-laitteet lisättiin verkkoon ja verkon P-laitteiden merkitys verkossa näkyy nyt paremmin, kun SimuNet-verkko käsittää kuusi laitetilaa.

Työssä eniten käytettyjen PE-laitteiden lopulliset konfiguraatiot löytyvät työn liitteistä. PE3:n konfiguraatiot löytyvät liitteestä 3 ja PE4:n liitteestä 4.

14.2 MPLS L2VPN

EoMPLS- ja erityisesti VPLS-palvelut osoittautuivat tehokkaiksi tekniikoiksi toteuttaa yhteyksiä laitetilojen välille. Näiden Layer 2 –tason tekniikoiden etu tulee esiin hyvin eri laitetiloihin kahdennettujen palveluiden toteutuksessa, koska kahdennetut laitteet voidaan pitää samassa verkon Layer 2 –segmentissä niiden maantieteellisestä sijainnista riippumatta. Tämän takia IP-osoitteita tai muita parametreja ei tarvitse muuttaa yhteyksien ja verkon toiminnan palauttamiseksi vikatilanteen jäljiltä.

Tässä työssä MPLS L2VPN –palveluita käytettiin operaattorin sisäisessä käytössä yhdistämään runkoverkon erilaitetiloja. MPLS L2VPN –palvelut soveltuvat kuitenkin myös hyvin myytäväksi asiakasyritykselle sen toimipisteitä yhdistävänä palveluna. Operaattorin verkko jää tällöin läpinäkyväksi sillaksi toimipisteiden välille. Asiakkaan omien laitteiden tulee huolehtia reitityksestä, ja asiakas voi käyttää siihen haluamaansa reititysprotokollaa, sillä asiakaslaitteiden ei tarvitse keskustella reititystiedoista operaattorin PE-laitteiden kanssa.

Kun siirtyminen IPv4-osoitteista IPv6-osoitteisiin saadaan kohta vauhtiin, tullaan L2VPN-palveluista varmasti hyötymään entistä enemmän. Verkoissa tullaan todennäköisesti ajamaan molempia protokollia rinnakkain pitkäänkin, ennen kuin pikkuhiljaa voidaan alkaa pudottaa IPv4-osoitteita pois käytöstä. L2VPN-palvelut eivät ota kantaa käytettävään Layer 3 –protokollaan, joten IPv6-liikenteen kuljettaminen onnistuu olemassa olevien tunneleiden läpi ilman, että niihin vaaditaan mitään muutoksia.

Kaiken kaikkiaan MPLS L2VPN -palveluita on helppo ottaa käyttöön, jos MPLS-kykeneviä laitteita on käytettävissä. EoMPLS onnistuu nykyään perustason reittitti-

miltä, mutta VPLS-palvelun käyttöä saattaa joissain tapauksissa rajoittaa sen vaatimat lisäinvestoinnit verkkolaitteisiin. L2VPN-palveluiden käytön kanssa kannattaa myös olla maltillinen, sillä verkko monimutkaistuu ja vianpaikannus vaikeutuu, jos paljon Layer 2 ja Layer 3 –yhteyksiä kuljetetaan verkossa sekaisin.

LÄHTEET

Ahola, V. 2010. Palvelinklusteri ja verkkolevy. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/Opinnayte%20Ville%20Ahola.pdf [viitattu 8.4.2011]

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

Hakkarainen, J & Vanhala, P. 2011. Redundanttisuus kontrolleripohjaisessa langattomassa lähiverkossa. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Kettunen, M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/SimuNet%20artikkeliv6a.pdf. [viitattu 26.1.2011]

Leinonen, R. 2011. Palomuurien IPv6-migraatio. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Luo, W., Pignataro, C., Bokotey, D. & Chan, A. 2005. Layer 2 VPN Architectures. Indianapolis: Cisco Press.

Minei, I. & Lucek, J. 2008. MPLS-Enabled Applications. Chichester: John Wiley & Sons Ltd.

Moreno, V. & Reddy, K. 2006. Network Virtualization. Indianapolis: Cisco Press.

Moskal, M. 2008. Carrier Ethernet: EVC, OAM. Saatavissa: http://www.cisco.com/web/YU/events/expo_08/pdfs/Carrier_Ethernet_Marek_Moskal.pdf [viitattu 22.3.2011]

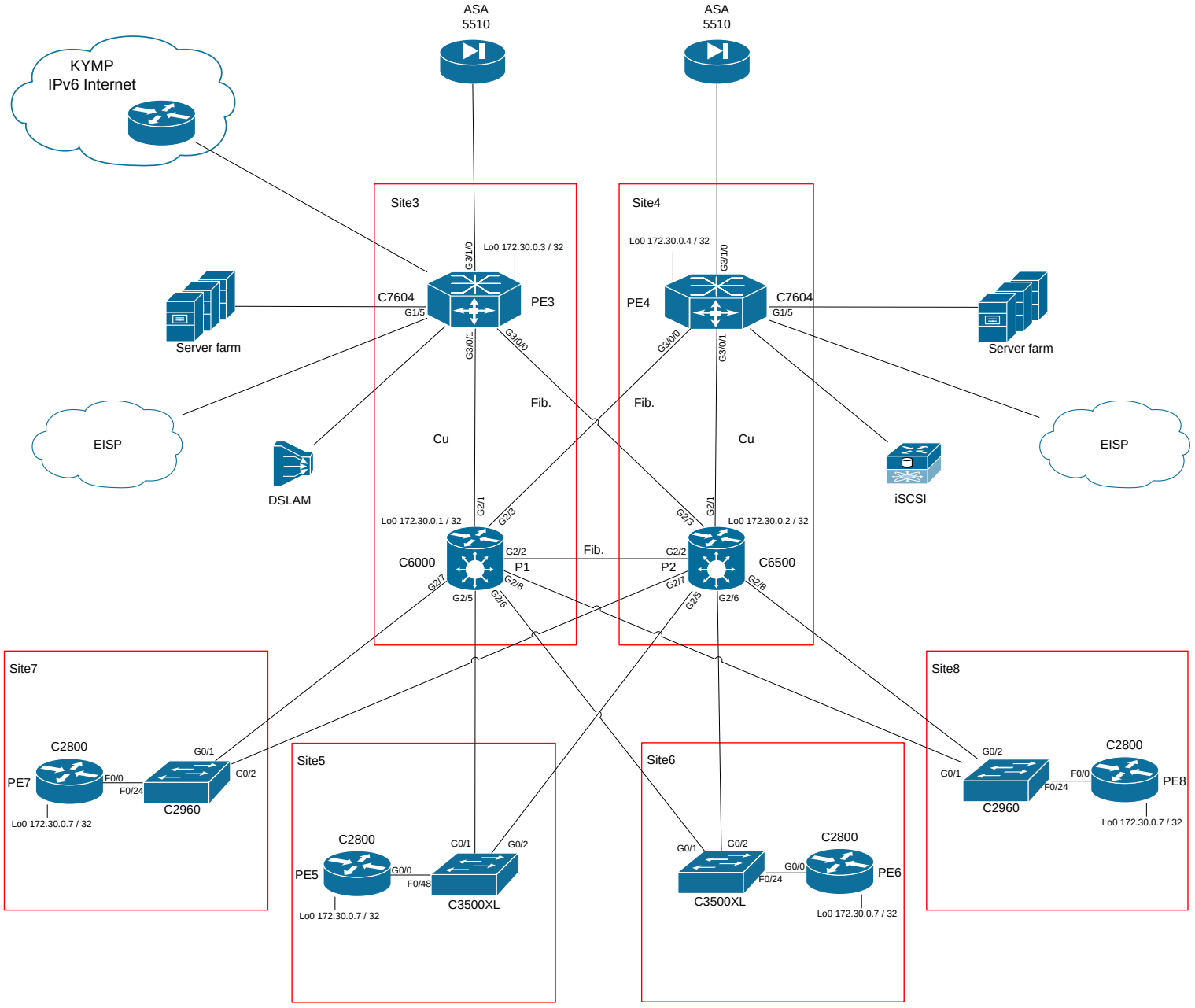
RFC 3031, Multiprotocol Label Switching Architecture. IETF. Saatavissa: http://www.ietf.org/rfc/rfc3031.txt [viitattu 3.2.2011.]

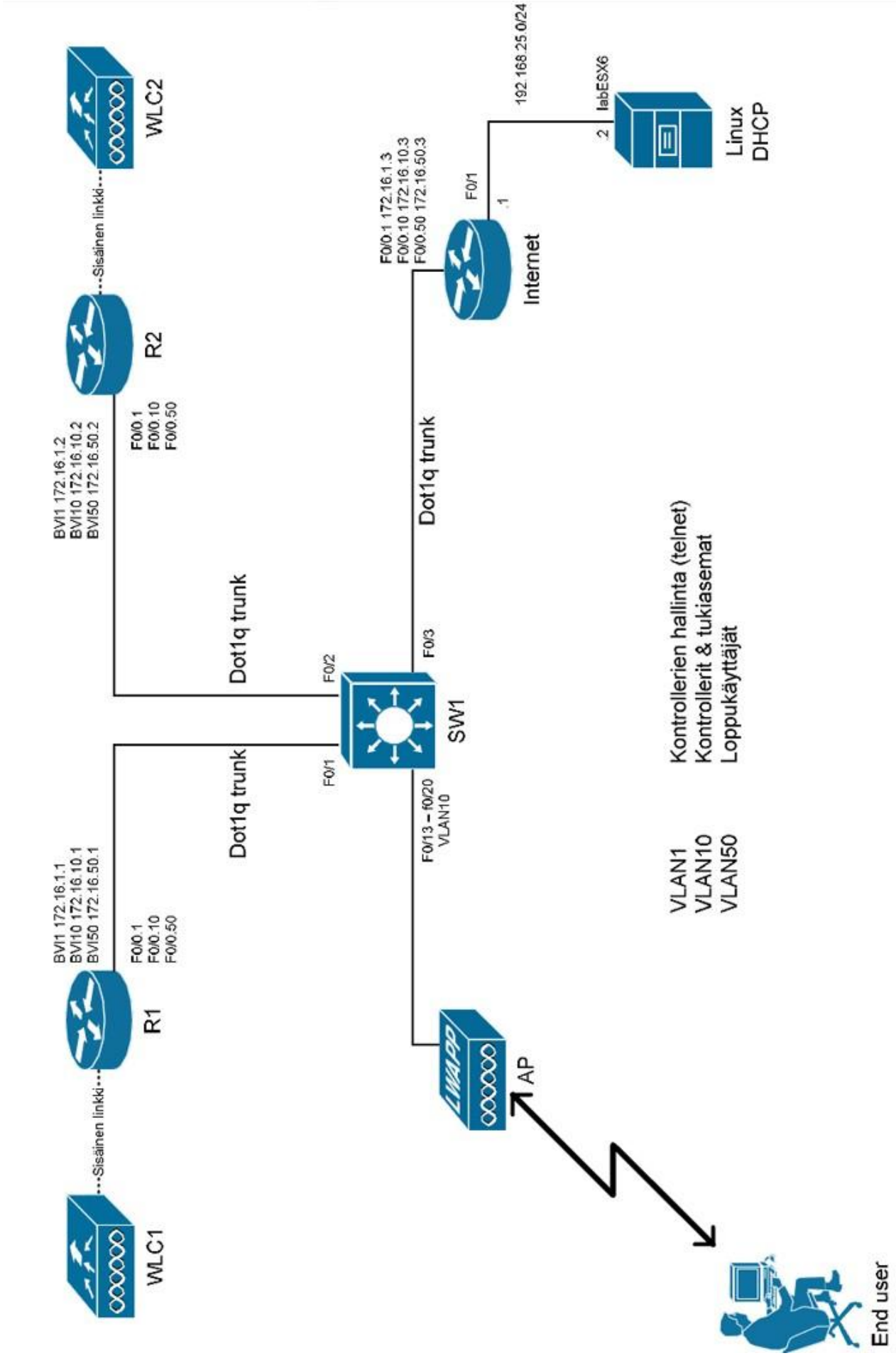
Singh A. 2011. Design and Deployment of Data Center Interconnects using Advanced VPLS (A-VPLS). Cisco Live 2011 tapahtuman kalvosarja.

Tassos. 2009. EoMPLS on 7600: PFC-based, SVI-based, Scalable. Saatavissa: http://ccie-in-3-months.blogspot.com/2009/06/eompls-on-7600-pfc-based-svi-based.html. [viitattu 12.2.2011]

Tolonen, E. 2011. VPN-ratkaisut operaattorin siirtyessä IPv6 yhteyskäytäntöön. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Xu, Z. 2010. Design and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services. Indianapolis: Wiley Publishing, Inc.


ASA
5510
ASA
5510
KYMP
IPv6 Internet
Site3
Site4
Lo0 172.30.0.3 / 32
Lo0 172.30.0.4 / 32
G3/1/0
G3/1/0
C7604
G1/5
PE3
PE4
C7604
G1/5
Server farm
Server farm
G3/0/1
G3/0/0
G3/0/0
G3/0/1
Fib.
Fib.
EISP
EISP
Cu
Cu
DSLAM
iSCSI
G2/1
G2/3
G2/3
G2/1
Lo0 172.30.0.1 / 32
Lo0 172.30.0.2 / 32
C6000
G2/2
P1
Fib.
P2
G2/2
C6500
G2/7
G2/8
G2/5
G2/6
G2/7
G2/5
G2/6
G2/8
Site7
Site8
C2800
G0/1
G0/2
PE7
F0/0
F0/24
C2960
Lo0 172.30.0.7 / 32
G0/2
G0/1
C2800
F0/0
F0/24
PE8
C2960
Lo0 172.30.0.7 / 32
Site5
Site6
C2800
G0/1
G0/2
PE5
G0/0
F0/48
C3500XL
Lo0 172.30.0.7 / 32
G0/1
G0/2
C2800
G0/0
F0/24
PE6
C3500XL
Lo0 172.30.0.7 / 32


WLC2
Sisäinen linkki
R2
BVI1 172.16.1.2
BVI10 172.16.10.2
BVI50 172.16.50.2
F0/0.1
F0/0.10
F0/0.50
Dot1q trunk
F0/2
F0/3
SW1
F0/1
F0/13 – f0/20
VLAN10
Dot1q trunk
F0/0.1 172.16.1.3
F0/0.10 172.16.10.3
F0/0.50 172.16.50.3
Dot1q trunk
F0/1
.1
Internet
192.168.25.0/24
.2
labESX6
Linux
DHCP
BVI1 172.16.1.1
BVI10 172.16.10.1
BVI50 172.16.50.1
F0/0.1
F0/0.10
F0/0.50
R1
Sisäinen linkki
WLC1
LWAPP
AP
VLAN1
VLAN10
VLAN50
Kontrollerien hallinta (telnet)
Kontrollerit & tukiasemat
Loppukäyttäjät
End user

```
Current configuration : 9325 bytes
!
! Last configuration change at 12:14:12 UTC Tue Apr 12
2011
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
!
vrf definition CUSTOMER_C1
!
!
no aaa new-model
!
!
!
ip source-route
!
ip vrf INTERNET
 rd 1:80
 route-target export 1:80
 route-target import 1:80
!
no ip domain lookup
ip multicast-routing
!
!
ipv6 unicast-routing
!
!
vtp mode transparent
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 10
 name Area1FWout
!
vlan 20
 name Area2FWout
!
vlan 81
 name INTERNET_C1
!
vlan 90
 name WLC&APs
!
vlan 91
 name WLC_C1
!
vlan 100
 name Servers1
!
vlan 101
 name Palomuurin_ohitus
!
vlan 200
 name Servers2
!
vlan 300
 name Failover
!
vlan 400
 name iSCSI&ClusterVLAN
!
!
l2 vfi FW_OUT_10 manual
 vpn id 10
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi FW_OUT_20 manual
 vpn id 20
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi INTERNET_C1 manual
 vpn id 81
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi WLC manual
 vpn id 90
 neighbor 172.30.0.4 encapsulation mpls
 neighbor 172.30.0.7 encapsulation mpls no-split-horizon
!
l2 vfi WLC_C1 manual
 vpn id 91
 neighbor 172.30.0.4 encapsulation mpls
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.3 255.255.255.255
```

```
!
interface Loopback5
 no ip address
 ip pim sparse-mode
 ip igmp version 3
!
interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::3/128
!
interface GigabitEthernet1/1
 switchport
 switchport access vlan 400
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/2
 switchport
 switchport access vlan 400
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/3
 mtu 9216
 no ip address
!
interface GigabitEthernet1/4
 mtu 9216
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200
 switchport mode trunk
 mtu 9216
!
interface GigabitEthernet1/6
 switchport
 switchport access vlan 90
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/7
 mtu 1600
 ip address 172.16.50.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/8
 description Firewall failover
 mtu 1600
 no ip address
 xconnect 172.30.0.4 300 encapsulation mpls
!
interface GigabitEthernet1/9
 description KYMP-SIMUNET IPV6 CONNECTION
 mtu 9216
 no ip address
 speed 100
 duplex full
 ipv6 address 2A00:1DD0:0:200::2/64
!
interface GigabitEthernet3/0/0
 description P2-PE3 fiber
 mtu 1600
 ip address 192.168.23.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 negotiation auto
 mpls ip
!
interface GigabitEthernet3/0/1
 description P1-PE3 copper
 mtu 1600
 ip address 192.168.13.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 speed 1000
 no negotiation auto
 mpls ip
!
interface GigabitEthernet3/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet3/0/2.3
 description PE3-LAB_CONNECTION
 encapsulation dot1Q 3
 ip address 192.168.103.3 255.255.255.0
!
interface GigabitEthernet3/0/2.110
 encapsulation dot1Q 110
 ip address 150.100.1.10 255.255.255.252
!
interface GigabitEthernet3/0/2.120
 encapsulation dot1Q 120
 ip address 150.100.1.13 255.255.255.252
!
interface GigabitEthernet3/0/3
 mtu 1600
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0/4
 description 6VPE Customer1
 mtu 1600
 no ip address
 speed 100
 no negotiation auto
 ipv6 address 2A00:1DD0:100:F001::1/64
!
interface GigabitEthernet3/1/0
 description Firewall EVC
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
 service instance 2 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
```

```
bridge-domain 20
 !
 service instance 5 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 6 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
 !
!
interface GigabitEthernet3/1/1
 mtu 1600
 no ip address
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/1/2
 mtu 1600
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/1/3
 description WLC EVC
 mtu 1600
 no ip address
 speed 100
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag translate 1-to-1 dot1q 13 symmetric
  bridge-domain 90
 !
 service instance 2 ethernet
  encapsulation dot1q 50
  rewrite ingress tag pop 1 symmetric
  bridge-domain 91
 !
!
interface GigabitEthernet3/1/4
 mtu 1600
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Firewall context 1 outside
 mtu 1600
 ip address 172.30.1.3 255.255.255.248
 no ip redirects
 standby version 2
 standby 10 ip 172.30.1.5
 standby 10 priority 150
 standby 10 preempt
 standby 110 ipv6 FE80::1
 standby 110 priority 150
 standby 110 preempt
 ipv6 address FE80:A1::3 link-local
 ipv6 address 2A00:1DD0:100:A1::3/64
 xconnect vfi FW_OUT_10
!
interface Vlan20
 description Firewall context 2 outside
 mtu 1600
 ip address 172.31.1.3 255.255.255.248
 no ip redirects
 standby version 2
 standby 20 ip 172.31.1.5
 standby 20 preempt
 standby 120 ipv6 FE80::2
 standby 120 preempt
 ipv6 address FE80:A2::3 link-local
 ipv6 address 2A00:1DD0:100:A2::3/64
 xconnect vfi FW_OUT_20
!
interface Vlan81
 ip vrf forwarding INTERNET
 no ip address
 shutdown
 xconnect vfi INTERNET_C1
!
interface Vlan90
 description WLC
 mtu 1600
 no ip address
 xconnect vfi WLC
!
interface Vlan91
 mtu 1600
 ip dhcp relay information trusted
 ip address 172.30.91.3 255.255.255.0
 ip helper-address 172.30.2.90
 standby version 2
 standby 91 ip 172.30.91.5
 standby 91 priority 150
 standby 91 preempt
 standby 91 name WLC
 xconnect vfi WLC_C1
!
interface Vlan100
 description Firewall context 1 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.4 100 encapsulation mpls
!
interface Vlan101
 description Palomuurin_ohitus
 ip address 172.30.101.3 255.255.255.0
 standby version 2
 standby 101 ipv6 FE80:C1::1
 standby 101 priority 150
 standby 101 preempt
 ipv6 address FE80:101::3 link-local
 ipv6 address 2A00:1DD0:100:C1::3/64
 xconnect 172.30.0.4 101 encapsulation mpls
!
interface Vlan200
 description Firewall context 2 inside
 mtu 1600
```

```
no ip address
 xconnect 172.30.0.4 200 encapsulation mpls
!
interface Vlan400
 description ISCSI/Cluster-VLAN
 mtu 1600
 no ip address
 no ip redirects
 xconnect 172.30.0.4 400 encapsulation mpls
!
interface Vlan1100
 mtu 1600
 no ip address
!
router ospf 1
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 passive-interface GigabitEthernet1/7
 network 172.16.50.0 0.0.0.3 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
 neighbor 2A00:1DD0:0:200::1 remote-as 65000
 neighbor 150.100.1.9 remote-as 65100
 neighbor 150.100.1.9 version 4
 neighbor 150.100.1.14 remote-as 65200
 neighbor 150.100.1.14 version 4
 neighbor 172.30.0.4 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO
 !
 address-family ipv4
  network 20.20.0.0 backdoor
  network 172.30.0.0 mask 255.254.0.0
  neighbor 2A00:1DD0:0:200::1 activate
  neighbor 150.100.1.9 activate
  neighbor 150.100.1.14 activate
  neighbor 150.100.1.14 filter-list 1 in
  neighbor 172.30.0.4 activate
  neighbor 172.30.0.6 activate
 exit-address-family
 !
 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100::/48
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  neighbor SISAVERKKO send-label
  neighbor 2A00:1DD0:0:200::1 activate
  neighbor 172.30.0.4 activate
 exit-address-family
 !
 address-family ipv4 vrf INTERNET
  redistribute static
  redistribute connected
 exit-address-family
!
!
ip as-path access-list 1 deny _200_
ip as-path access-list 1 deny _400_
ip as-path access-list 1 permit .*
no ip http server
no ip http secure-server
ip pim ssm default
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1
!
logging esm config
access-list 1 permit 172.31.1.2
access-list 100 permit ip host 172.31.1.2 host 172.31.1.3
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100::/48 Null0
!
route-map PRED permit 10
 set as-path prepend 1
!
route-map International50 permit 10
 set local-preference 50
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 logging synchronous
line vty 0 4
 login
 transport input lat pad udptn telnet rlogin
!
!
!
end
```

```
Current configuration : 9467 bytes
!
! Last configuration change at 12:13:25 UTC Tue Apr 12
2011
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
mls ipv6 vrf
!
vrf definition CUSTOMER_C1
 rd 6:6
 !
 address-family ipv6
  route-target export 6:6
  route-target import 6:6
 exit-address-family
!
!
no aaa new-model
!
!
!
ip source-route
!
ip vrf INTERNET
 rd 1:80
 route-target export 1:80
 route-target import 1:80
!
no ip domain lookup
ip multicast-routing
!
!
ipv6 unicast-routing
!
!
vtp mode transparent
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 10
 name Area1FWout
!
vlan 20
 name Area2FWout
!
vlan 81
 name INTERNET_C1
!
vlan 90
 name WLC&APs
!
vlan 91
 name WLC_C1
!
vlan 100
 name Servers1
!
vlan 101
 name Palomuurin_ohitus
!
vlan 200
 name Servers2
!
vlan 300
 name Failover
!
vlan 400
 name iSCSI&ClusterVLAN
!
!
l2 vfi FW_OUT_10 manual
 vpn id 10
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi FW_OUT_20 manual
 vpn id 20
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi INTERNET_C1 manual
 vpn id 81
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi WLC manual
 vpn id 90
 neighbor 172.30.0.7 encapsulation mpls no-split-horizon
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi WLC_C1 manual
 vpn id 91
 neighbor 172.30.0.3 encapsulation mpls
!
!
!
!
```

```
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.4 255.255.255.255
!
interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::4/128
!
interface GigabitEthernet1/1
 switchport
 switchport access vlan 400
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/2
 switchport
 switchport access vlan 400
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/3
 switchport
 switchport access vlan 400
 switchport mode access
 mtu 9216
!
interface GigabitEthernet1/4
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/5
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200
 switchport mode trunk
 no keepalive
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 description IPTV-palvelin
 ip address 172.16.50.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/8
 description Firewall failover
 mtu 1600
 no ip address
 xconnect 172.30.0.3 300 encapsulation mpls
!
interface GigabitEthernet1/9
 switchport
 switchport access vlan 1100
 switchport mode access
!
interface GigabitEthernet3/0/0
 description P1-PE4 fiber
 mtu 1600
 ip address 192.168.14.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 negotiation auto
 mpls ip
!
interface GigabitEthernet3/0/1
 description P2-PE4 copper
 mtu 1600
 ip address 192.168.24.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 speed 1000
 no negotiation auto
 mpls ip
!
interface GigabitEthernet3/0/2
 no ip address
 speed 1000
 no negotiation auto
 ipv6 address 2A00:1DD0:100:F001::1/64
 ipv6 enable
!
interface GigabitEthernet3/0/3
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/0/4
 description 6VPE C1 Site4
 vrf forwarding CUSTOMER_C1
 mtu 1600
 no ip address
 speed 100
 no negotiation auto
 ipv6 address 2A00:1DD0:100:F310::1/64
!
interface GigabitEthernet3/1/0
 description Firewall EVC
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
 service instance 2 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
 service instance 5 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 6 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
```

```
 bridge-domain 200
 !
!
interface GigabitEthernet3/1/1
 no ip address
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/1/2
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/1/3
 description WLC EVC
 mtu 1600
 no ip address
 speed 100
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag translate 1-to-1 dot1q 13 symmetric
  bridge-domain 90
 !
 service instance 2 ethernet
  encapsulation dot1q 50
  rewrite ingress tag pop 1 symmetric
  bridge-domain 91
 !
!
interface GigabitEthernet3/1/4
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Firewall context 1 outside
 mtu 1600
 ip address 172.30.1.4 255.255.255.248
 no ip redirects
 standby version 2
 standby 10 ip 172.30.1.5
 standby 10 preempt
 standby 110 ipv6 FE80::1
 standby 110 preempt
 ipv6 address FE80:A1::4 link-local
 ipv6 address 2A00:1DD0:100:A1::4/64
 xconnect vfi FW_OUT_10
!
interface Vlan20
 description Firewall context 2 outside
 mtu 1600
 ip address 172.31.1.4 255.255.255.248
 no ip redirects
 standby version 2
 standby 20 ip 172.31.1.5
 standby 20 priority 150
 standby 20 preempt
 standby 120 ipv6 FE80::2
 standby 120 priority 150
 standby 120 preempt
 ipv6 address FE80:A2::4 link-local
 ipv6 address 2A00:1DD0:100:A2::4/64
 xconnect vfi FW_OUT_20
!
interface Vlan81
 ip vrf forwarding INTERNET
 no ip address
 shutdown
 xconnect vfi INTERNET_C1
!
interface Vlan90
 description WLC
 mtu 1600
 no ip address
 xconnect vfi WLC
!
interface Vlan91
 mtu 1600
 ip dhcp relay information trusted
 ip address 172.30.91.4 255.255.255.0
 ip helper-address 172.30.2.90
 standby version 2
 standby 91 ip 172.30.91.5
 standby 91 preempt
 standby 91 name WLC
 xconnect vfi WLC_C1
!
interface Vlan100
 description Firewall context 1 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.3 100 encapsulation mpls
!
interface Vlan101
 description Palomuurin_ohitus
 ip address 172.30.101.4 255.255.255.0
 standby version 2
 standby 101 ipv6 FE80:C1::1
 standby 101 preempt
 ipv6 address FE80:101::4 link-local
 ipv6 address 2A00:1DD0:100:C1::4/64
 xconnect 172.30.0.3 101 encapsulation mpls
!
interface Vlan120
 no ip address
 shutdown
!
interface Vlan200
 description Firewall context 2 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.3 200 encapsulation mpls
!
interface Vlan400
 description iSCSI&ClusterVLAN
 mtu 1600
 no ip address
 no ip redirects
 xconnect 172.30.0.3 400 encapsulation mpls
!
router ospf 1
```

```
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 network 172.16.50.0 0.0.0.3 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
 neighbor 150.100.1.1 remote-as 65300
 neighbor 150.100.1.1 version 4
 neighbor 150.100.1.5 remote-as 65100
 neighbor 150.100.1.5 version 4
 neighbor 172.30.0.3 peer-group SISAVERKKO
 neighbor 172.30.0.5 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO
 neighbor 172.30.0.7 remote-as 65001
 neighbor 172.30.0.7 update-source Loopback0
 neighbor 172.30.0.8 remote-as 65001
 neighbor 172.30.0.8 update-source Loopback0
 !
 address-family ipv4
  network 20.20.0.0 backdoor
  network 172.30.0.0 mask 255.254.0.0
  neighbor 150.100.1.1 activate
  neighbor 150.100.1.1 route-map PRED in
  neighbor 150.100.1.1 filter-list 1 in
  neighbor 150.100.1.5 activate
  neighbor 172.30.0.3 activate
  neighbor 172.30.0.5 activate
  neighbor 172.30.0.6 activate
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.8 activate
 exit-address-family
 !
 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  network 2A00:1DD0:100:100::/56
  neighbor SISAVERKKO send-label
  neighbor 172.30.0.3 activate
 exit-address-family
 !
 address-family vpnv6
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.7 send-community extended
  neighbor 172.30.0.8 activate
  neighbor 172.30.0.8 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf CUSTOMER_C1
  redistribute connected
  redistribute static
 exit-address-family
 !
 address-family ipv4 vrf INTERNET
  redistribute static
  redistribute connected
 exit-address-family
!
!
ip as-path access-list 1 deny _400?
ip as-path access-list 1 permit .*
no ip http server
no ip http secure-server
ip pim ssm default
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1
!
logging esm config
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100:100::/56 GigabitEthernet3/0/2
2A00:1DD0:100:F001::2
ipv6 route vrf CUSTOMER_C1 2A00:1DD0:100:10C3::/64
2A00:1DD0:100:F310::2
ipv6 router ospf 6
!
!
route-map PRED permit 10
 set as-path prepend 1
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 logging synchronous
line vty 0 4
 login
 transport input telnet
line vty 5
 no login
!
!
!
end
```