KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / tietoliikennetekniikka

Tuomo Korja

CARRIER ETHERNET -PALVELUT

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Elektroniikan koulutusohjelma

KORJA, TUOMO	Carrier Ethernet -palvelut
Opinnäytetyö	37 sivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	Kymen Puhelin Oy
Huhtikuu 2011	
Avainsanat	Ethernet, VPLS, MPLS, carrier, metro

Tämä on Kymen Puhelimen toimeksiantama opinnäytetyö, jossa on hyödynnetty Kymenlaakson ammattikorkeakoulun ja lähialueen palveluntarjoajien yhteisen EAKR-rahoitteisen SimuNet-hankkeen testiverkkoa.

Työn keskeinen tavoite oli perehtyä Carrier Ethernet -palveluihin, ja esittää perusteellisesti yksi vaihtoehto palvelun toteuttamiseksi. Lisäksi tarkoituksena oli perehtyä käytännössä SimuNet-laboratorion reititinlaitteiden palveluinstansseihin ja niiden käyttömahdollisuuksiin valitun vaihtoehdon toteuttamisessa.

Carrier Ethenet -palvelun idea on, että palveluntarjoaja pystyy tarjoamaan Ethernetin asiakkaalle palveluna. Carrier Ethernet -konseptista vastaava Metro Ethernet Ethernet Forum on määritellyt Ethernet-palveluiden toimintaidean ja erilaisia vaihtoehtoja niiden toteuttamiseksi. Palvelutyypit jaetaan kolmeen tyyppiin: E-Line, E-LAN ja E-Tree.

Työssä syvennyttiin erityisesti E-LAN -palvelutyyppiä edustavaan VPLS-tekniikkaan, jolla voidaan yhdistää asiakkaan maantieteellisesti eri paikoissa sijaitsevat yrityksen toimipisteet samaan törmäysalueeseen. Palveluntarjoajan MPLS-runkoverkko näyttää asiakkaan näkökulmasta normaalilta lähiverkkokytkimeltä, joka välittää asiakasliikenteen verkon läpi koskematta sen sisältöön.

Opinnäytetyössä käytiin läpi VPLS-tekniikka niin teorian kuin käytännön tasolla. Työssä esitellään SimuNet-verkon VPLS-toteutus konfiguraatioiden osalta. SimuNet-verkossa VPLS on konfiguroitu Cisco 7600 -sarjan reitittimen ja siihen kiinnitetyn SIP-lisäkortin mahdollistavassa palveluinstanssien määritystilassa. Jokaiselle VPLS-instanssille muodostettiin oma erillisten VLAN- ja MAC-osoiteavaruuksien omaava palveluinstanssi verkon molempiin runkoreitittimiin, joiden välille saatiin lopulta muodostettua toimivat VPLS-yhteydet.

Toimivien VPLS-määritysten lisäksi opinnäytetyön tuloksena syntyi ohjeet palveluinstanssien määrittelytilan käskyistä ja niiden käytöstä. Ohjeita voidaan myöhemmin käyttää apuna niin VPLS-tekniikan kuin muidenkin palveluiden konfiguroinnissa.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Electronics

KORJA, TUOMO	Carrier Ethernet Services
Bachelor’s Thesis	37 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Kymen Puhelin Oy
April 2011	
Keywords	Ethernet, VPLS, MPLS, carrier, metro

This thesis work was commissioned by Kymen Puhelin Oy and it utilized the test network of The SimuNet project, which is a co-project of Kymenlaakso University of Applied Scienses and local Internet service providers. The SimuNet project is funded by The European Regional Development Fund.

The main objective of this thesis work was to inspect Carrier Ethernet services and present one way of deploying one in practice. Another goal was to study in practice the service instances of the SimuNet routers and find out how they could be utilized for the implementation of the chosen Carrier Ethernet service type.

The principle of a Carrier Ethernet Service is that the service provider can provide Ethernet for a customer as a service. Metro Ethernet Forum, which is the organization that manages the standardization of Carrier Ethernet services, has specified three standardized service types: E-Line, E-LAN and E-Tree.

The main focus of this thesis was on the VPLS protocol, which is a type of E-LAN service. VPLS is mainly used for connecting the customer's geographically dispersed networks to the same broadcast domain. From the customer's point of view, the MPLS core network of the service provider seems like a normal Ethernet switch with a role of transporting the customer traffic from edge to edge untouched. This study presents the VPLS configurations in the SimuNet environment. VPLS is configured under the service instance configuration mode, which is a feature provided by the SIP modules that have been added to the modular Cisco 7600 series core routers. In both routers, a separate service instance was created for each VPLS instance, each having its own VLAN and MAC address space. Finally, the VPLS connections were built successfully between the core routers.

Besides yielding working VPLS configurations, this thesis work resulted in instructions for using the commands of the service instance configuration mode. The configuration guide can later be used as helpful reference when configuring VPLS or other services.

SISÄLLYS

LYHENNELUETTELO

AC	Attachment Circuit; liityntäpiiri
ATM	Asynchronous Transfer Mode; tiedonsiirtoprotokolla
AToM	Any Transport over MPLS; MPLS-sovellus
C	Customer; asiakkaan reititin
CE	Customer Edge; asiakkaan reunareititin
CWDM	Coarse Wavelength-Division Multiplexing; optinen multipleksaustekniikka
DWDM	Dense Wavelength-Division Multiplexing; optinen multipleksaustekniikka
EoMPLS	Ethernet over MPLS; siirtoyhteyskerroksen VPN-tekniikka
EPL	Ethernet Private Line; Ethernet-palvelun alatyyppi
ES	EtherSwitch; reitittimeen asennettava lisämoduuli
EVC	Ethernet Virtual Connection; Metro Ethernet -verkon läpi kulkeva tunneli
EVPL	Ethernet Virtual Private Line; Ethernet-palvelun alatyyppi
FDDI	Fiber Distributed Data Interface; optinen verkkotekniikka
GRE	Generic Routing Encapsulation; tunnelointiprotokolla
HDLC	High-Level Data Link Control; siirtoyhteyskerroksen protokolla
H-VPLS	Hierarchical VPLS; VPLS-tekniikan hierarkinen versio
IETF	Internet Engineering Task Force; Internet-protokollien standardointiorganisaatio
IP	Internet Protocol; verkkokerroksen protokolla

IPsec	IP Security Architecture; tietoliikenneprotokollanippu
LAN	Local Area Network; lähiverkko
LFIB	Label Forwarding Information Base; lippunvälitystietokanta
LIB	Label Information Base; lipputietokanta
LSP	Label Switced Path; kehtysten reitti MPLS-verkon läpi
LSR	Label Switching Router; MPLS-verkon reititin
MAC	Media Access Control; siirtoyhteyskerroksen alakerros
MEN	Metro Ethernet Network; Ethernet-pohjainen kaupunkiverkko
MinM	Mac in Mac; MAC-osoitteiden kerrostustekniikka
MP-BGP	Multiprotocol-BGP; BGP-protokollan moniprotokollalaajennukset
MPLS	Multiprotocol Label Switching; lippujen vaihtoon perustuva runkoverkkoprotokolla
NG-SDH	Next Generation Synchronous Optical Networking; multipleksausprotokolla
P	Provider; palveluntarjoajan reititin
PE	Provider Edge; palveluntarjoajan reunareititin
PPP	Point-to-Point Protocol; siirtoyhteyskerroksen protokolla
PVC	Permanent Virtual Circuit; ennaltamääritetty pysyvä yhteys
PW	Pseudowire; virtuaalinen point-to-point -yhteys palveluntarjoajan verkon yli
PWE3	Pseudowire Emulation Edge to Edge; pseudojohdoista vastaava työryhmä

QinQ	.1q in .1q; VLAN-tunnisteiden kerrostustekniikka
QoS	Quality of Service; palvelun laatu
RD	Route Distinguisher; BGP:ssä tunniste, jolla erotellaan asiakkaat toisistaan
RT	Route Target; määrää BGP:ssä, mitkä reitit otetaan vastaan ja mitkä lähetetään eteenpäin
SIP	reitittimeen asennettava lisämoduuli
SVI	Switch Virtual Interface; VLAN-portti
TE	Traffic Engineering; MPLS-sovellus
TDM	Time-division multiplexing; aikajakojärjestelmä
UNI	User-Network Interface: asiakkaan ja palveluntarjoajan välinen rajapinta Metro Ethernet -verkossa
VC	Virtual Circuit/Channel; virtuaalikanava
VFI	Virtual Forwarding Interface; PE-laitteen sisällä oleva looginen komponentti
VLAN	Virtual LAN; virtuaalinen lähiverkko
VPLS	Virtual Private LAN Service; siirtoyhteyskerroksella toimiva VPN-tekniikka
VPN	Virtual Private Network; yksityinen suojattu verkko
VRF	VPN Routing and Forwarding; virtuaalinen reititysinstanssi
VSI	Virtual Switch Interface; PE-laitteen sisällä oleva looginen komponentti (sama kuin VFI)

1 JOHDANTO

Ethernet-tekniikasta on vuosien saatossa tullut johtava lähiverkkotekniikka sen kustannustehokkuuden ja yksinkertaisen rakenteen vuoksi. Nykyajan suuntaus tietoverkkomaailmassa on antaa entistä enemmän roolia Ethernetille korvaamalla sillä mahdollisimman paljon muita monimutkaisempia tekniikoita. Verkko on silloin yksinkertainen ja tehokas, kun se alkaa Ethernet-portista ja päättyy Ethernet-porttiin.

Metro Ethernet -verkolla tarkoitetaan verkkoa, joka yhdistää maantieteellisesti eri paikoissa sijaitsevat yrityksen lähiverkot toisiinsa laaja-alueverkon tai palveluntarjoajien omistaman runkoverkoston läpi. Ethernet-pohjaista kaupunkiverkkoa kutsutaan Metro Ethernet -verkoksi.

Metro Ethernet Forumin määritelmän mukaan Carrier Ethernet on kaikkialla saatavissa oleva palvelu tai verkko, jolla on viisi ominaisuutta: standardoidut palvelut, skaalautuvuus, luotettavuus, hallinta ja palvelun laatu. Nämä ominaisuudet erottavat Carrier Ethernetin perinteisestä lähiverkkopohjaisesta Ethernetistä. Carrier Ethernet -palvelun keskeinen idea on, että palveluntarjoaja pystyy tarjoamaan Ethernetin palveluna asiakkaalle. Tässä työssä esitellään Metro Ethernet Forumin määrittelemät Carrier Ethernet -palvelutyypit: E-Line, E-LAN ja E-Tree.

Palveluntarjoajan runkoverkot on nykyään toteutettu pääsääntöisesti lippukytkentäisellä MPLS-tekniikalla, joten nykyaikaisten Carrier Ethernet -palveluiden ymmärtäminen vaatii vähintään perustason tietämyksen tekniikasta. MPLS-tekniikkaan on ajan saatossa kehitetty erilaisia suureen suosioon päässeitä sovelluksia, joista tämän aiheen kannalta merkittävin on Metro Ethernet Forumin määrittelemää E-LAN -palvelutyyppiä edustava VPLS-tekniikka, joka on yksi tapa yhdistää eri paikoissa sijaitsevat lähiverkot yhdeksi virtuaaliseksi lähiverkoksi palveluntarjoajan runkoverkon läpi. Asiakkaan näkökulmasta VPLS-toteutus saa verkon näyttämän siltä, että yhdistettyjen lähiverkkojen välissä olisi normaali L2-kytkin.

SimuNet-verkko on Kymenlaakson ammattikorkeakoulun ja lähialueen palveluntarjoajien yhteisen EAKR-rahoitteisen SimuNet-hankkeen tulos. Verkko on tietoliikennelaboratorioon rakennettu opetus- ja testiverkko, joka mallintaa perinteistä palveluntar-

joajan tuotantoverkkoa. SimuNet-verkon runkoverkossa käytetään MPLS-protokollaa ja runkoverkon yli vedetyt virtuaaliset yhteydet on toteutettu VPLS-tunneleina.

Tässä työssä teoria ja käytäntö yhdistyvät osiossa, jossa käydään läpi eräs vaihtoehto VPLS-tekniikan toteuttamiseksi SimuNet-verkkoa hyödyntäen. Carrier Ethernet -palveluiden ja VPLS-tekniikan esittelyn lisäksi kolmas työn päätavoitteista on reitittimien palveluinstanssien konfigurointitilaan tutustuminen VPLS-tekniikan kannalta.

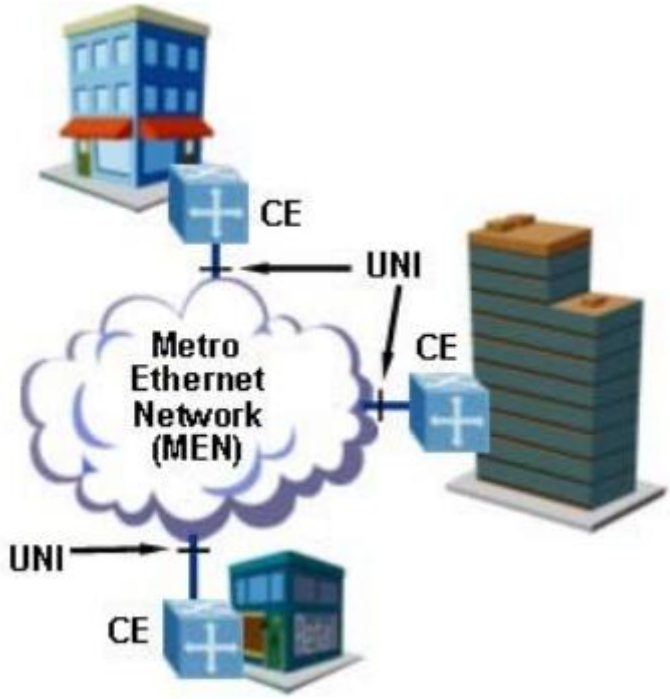
2 METRO ETHERNET

Ethernet-pohjaista kaupunkiverkkoa (Metropolitan Area Network) kutsutaan yleisesti Metro Ethernet -verkoksi eli lyhennettynä MEN:ksi (Metro Ethernet Network). Ethernet mahdollistaa kaupunkiverkossa suuremman kapasiteetin sekä erinäisiä palveluita joustavasti, yksinkertaisesti ja helposti laajennettavasti. (1, 1)

Ethernet on vuosien varrella jättänyt varjoonsa vanhempia lähiverkkotekniikoita, kuten Token Ring, ATM ja FDDI. Ethernetin suuria etuja ovat muun muassa vastaavia tekniikoita parempi hinta-suorituskykysuhde ja yksinkertaisuus. Nykyään 98 % kaikesta yritysverkkojen dataliikenteestä alkaa ja päättyy Ethernet-porttiin, joten Metro Ethernet on luonnollinen valinta viemään yhteydet yrityksen omien toimipisteiden lähiverkkojen ulkopuolelle. (1, 2)

2.1 Metro Ethernet -verkon komponentit

Metro Ethernet -verkon perinteinen malli on esitetty kuvassa 1. Verkon runkona toimii varsinainen Metro Ethernet -verkko, johon asiakkaat kytkeytyvät. Metro Ethernet -verkon tärkeimpiä komponentteja ovat UNI-rajapinta (User-Network Interface) ja EVC-tunneli (Ethernet Virtual Connection).



Kuva 1. Ethernet-palvelun malli (2, 1).

2.1.1 User-Network Interface -rajapinta

Asiakkaan CE-laitteen ja Metro Ethernet -verkon välistä rajapintaa kutsutaan User-Network Interface -rajapinnaksi, jossa fyysisenä liitäntänä toimii normaali 10 Mbps, 100 Mbps, 1 Gbps tai 10 GBps Ethernet-liityntäportti. UNI-rajapinnassa on kaksi puolta: UNI-C (asiakkaan puoli) ja UNI-N (palveluntarjoajan verkon puoli). Asiakkaan ja palveluntarjoajan hallittavien alueiden jako tapahtuu UNI-rajapinnassa siten, että asiakas on vastuussa UNI-C-puolesta ja vastaavasti UNI-N kuuluu palveluntarjoajan vastuualueeseen. (2, 1)

2.1.2 Ethernet Virtual Connection -tunneli

Metro Ethernet Forumin määritelmän mukaan Ethernet Virtual Connection yhdistää kahden tai useamman UNI-rajapinnan keskenään, jotta niiden välillä voidaan lähettää Ethernet-palveluun kuuluvia paketteja. EVC-tunnelin toinen tärkeä rooli on estää tilaajaverkkojen välinen tiedonsiirto, elleivät ne kuulu samaan EVC-tunneliin. (2, 2)

Yksinkertaistettuna EVC on asiakkaiden verkkojen välinen looginen tunneli, joka yhdistää toimipisteet siten, että niiden välillä voidaan kommunikoida. EVC-tunneli kuljetetaan palveluntarjoajan verkon läpi. Kuljetusmekanismeiksi on useita vaihtoehtoja:

Ethernet (QinQ, MinM), MPLS (PWE3, L2VPN), NG-SDH ja Lambada (CWDM, DWDM). Tässä työssä käsitellään kuljetusmekanismeista vain MPLS-vaihtoehto. (3, 6)

Ethernet-kehysten kuljetusta EVC-tunnelin läpi rajoittaa kaksi tärkeää sääntöä:

1. Palvelukehys (service frame) ei koskaan saa palata samaan UNI-rajapintaan, mistä se on alun perin saapunut Metro Ethernet -verkkoon.

2. Palvelukehyhyksen sisältö ja MAC-osoite eivät saa muuttua kuljetuksen aikana, eli Ethernet-kehyksen pitää olla sama sekä lähtö- että kohdeportissa. (2, 2)

2.2 Carrier Ethernet -palvelut

Carrier Ethernet -palvelun ideana on, että palveluntarjoaja pystyy tarjoamaan Ethernetin palveluna asiakkaille. Metro Ethernet Forum on asettanut standardoiduille palveluille kriteerit, jotka niiden on täytettävä:

1. Niiden tulisi olla saatavissa standardoidulla laitteistolla maantieteellisestä sijainnista riippumatta.

2. Ne eivät saa vaatia muutoksia asiakaslaitteistossa.

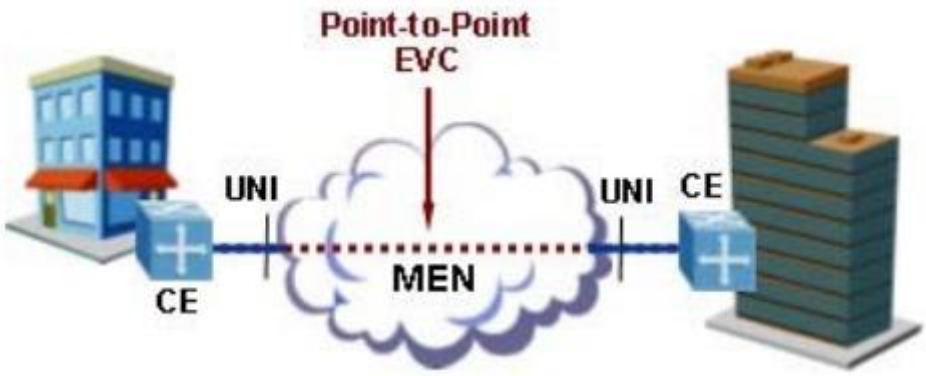
3. Niiden täytyy pystyä kuljettamaan konvergoidun verkon liikennettä (ääni, video, data).

4. Niiden pitää mahdollistaa erilaiset kaistanleveydet ja QoS-luokat.

EVC voi olla joko point-to-point- tai multipoint-to-multipoint -tyyppiä, ja sillä rakennetaan joko L2 private line tai VPN-ratkaisuja. Point-to-point -tyypin EVC-tunnelia kutsutaan E-Line -palveluksi, kun taas multipoint-to-multipoint -tunnelia kutsutaan E-LAN -palveluksi. (2, 3)

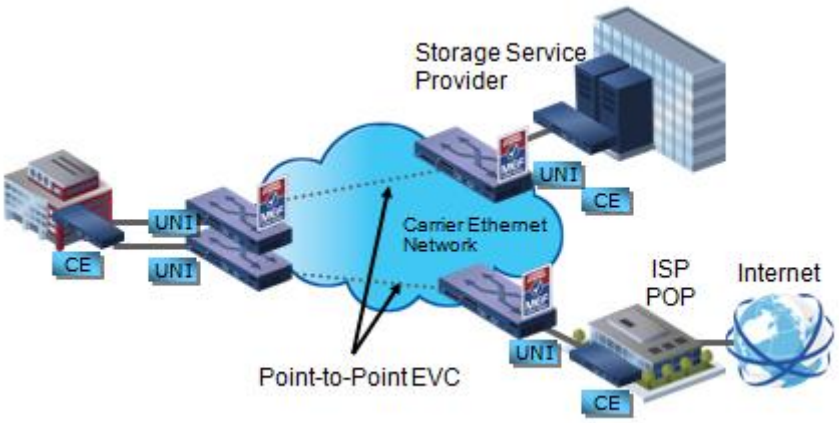
2.2.1 E-Line -palvelu

E-Line -palvelu tarjoaa point-to-point -tyyppisen EVC-tunnelin kahden UNI-rajapinnan välille (kuva 2). E-Line -palvelu voidaan rakentaa esimerkiksi vastaamaan Frame Relay -verkkoa tai yksityistä vuokrattua linjaa tarjoten kuitenkin enemmän mahdollisia vaihtoehtoja kaistan leveydelle ja liitettävyydelle. Yksinkertaisimmillaan E-Line -palvelussa kaistan leveys on symmetrinen molempiin suuntiin eikä palvelun laatua taata mitenkään. (2, 3)

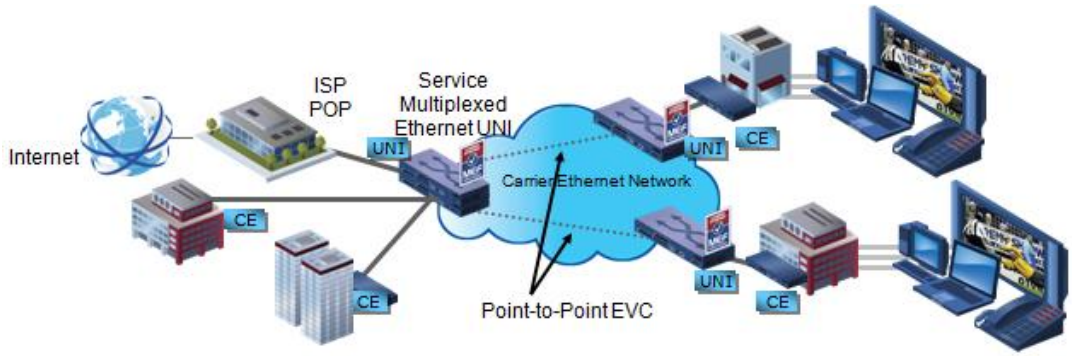


Kuva 2. E-Line -palvelun malli (2, 3).

E-Line palveluja on kahden tyyppisiä: Ethernet Private Line (EPL) ja Ethernet Virtual Private Line (EVPL). TDM Private Line -palvelun korvaajaksi suunnitellussa EPL-palvelussa on yksi EVC-tunneli jokaista UNI-rajapintaa kohden (kuva 3), kun taas EVPL-toteutuksessa on useita EVC-tunneleita (kuva 4). Toisin sanoen EVPL mahdollistaa yhden fyysisen linkin (UNI) yhdistämisen useaan virtuaaliseen asiakkaan puolen linkkiin, jolloin EVPL vastaa perinteisiä Frame Relay- ja ATM-palveluita. (4, 12–13)



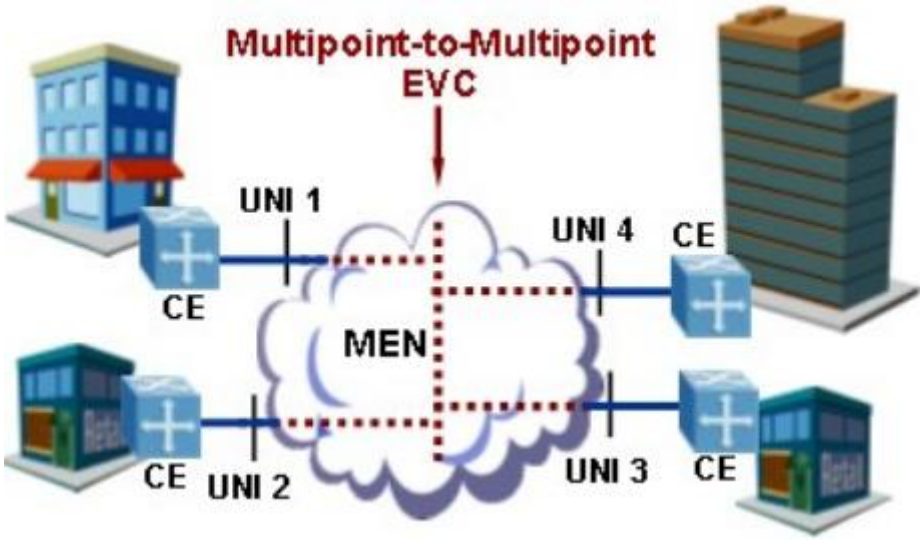
Kuva 3. Ethernet Private Line (4, 12).



Kuva 4. Ethernet Virtual Private Line (4, 13).

2.2.2 E-LAN -palvelu

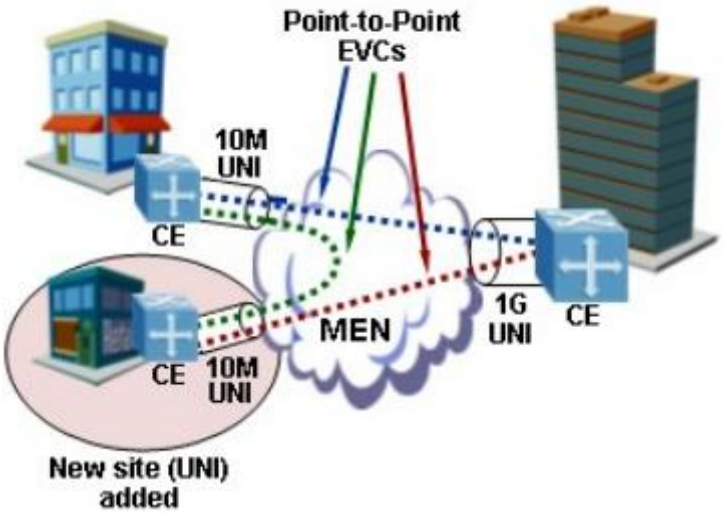
E-LAN -palvelu toimii multipoint-to-multipoint periaatteella, eli sillä voidaan kytkeä useampia UNI-rajapintoja yhteen (kuva 5). Asiakkaan toimipisteet kytketään samaan multipoint-EVC-yhteyteen, jolloin Metro Ethernet -verkko näyttää tavalliselta lähiverkolta. E-Line -palvelun tapaan myös E-LAN -palvelusta on olemassa Ethernet Private- ja Ethernet Virtual Private LAN -versiot, joista EVPL-tyypissä voidaan multipleksoida useita EVC-yhteyksiä yhteen UNI-rajapintaan. (2, 3–4)



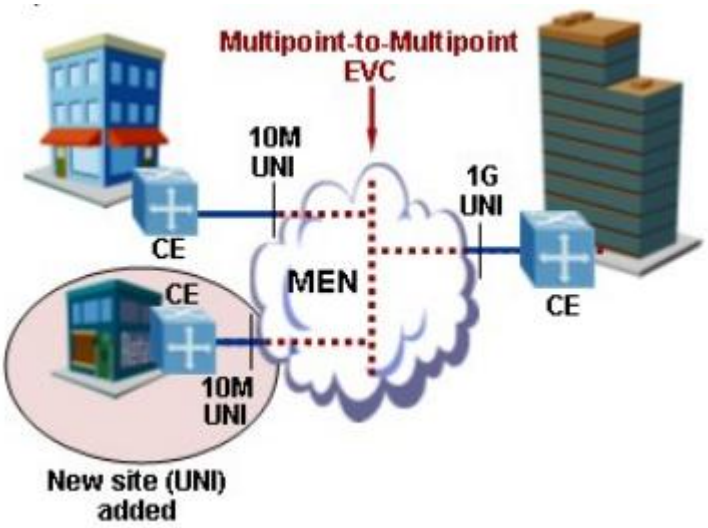
Kuva 5. E-LAN -palvelun malli (2, 4).

Yhdessä UNI-rajapinnassa voi olla samanaikaisesti käytössä sekä E-LAN- että E-Line -palvelu esimerkiksi siten, että E-LAN kytkee UNI-rajapinnan asiakkaan muihin toimipisteisiin, kun taas E-Line-palvelu kytkee UNI-rajapinnan Internetiin. (2, 3–4)

E-Lan -palvelulla voidaan kytkeä myös vain kaksi toimipistettä yhteen E-Line -palvelun tapaisesti. Toteutusten eroavaisuudet tulevat kuitenkin esiin jos Metro Ethernet -verkkoon lisätään toimipisteitä myöhemmin. Koska E-Line toimii point-to-point periaatteella, uudelta toimipisteeltä pitää luoda erilliset EVC-tunnelit jokaiselle jo verkossa olevalle toimipisteelle ja vastaavasti muilta toimipisteiltä täytyy määrittää EVC uutta toimipistettä varten, jotta täysverkko toteutuisi (kuva 6). E-Lan-palvelussa uusi toimipiste kytketään yksinkertaisesti samaan multipoint-EVC-tunneliin, jossa muutkin toimipisteet ovat (kuva 7). (2, 5)



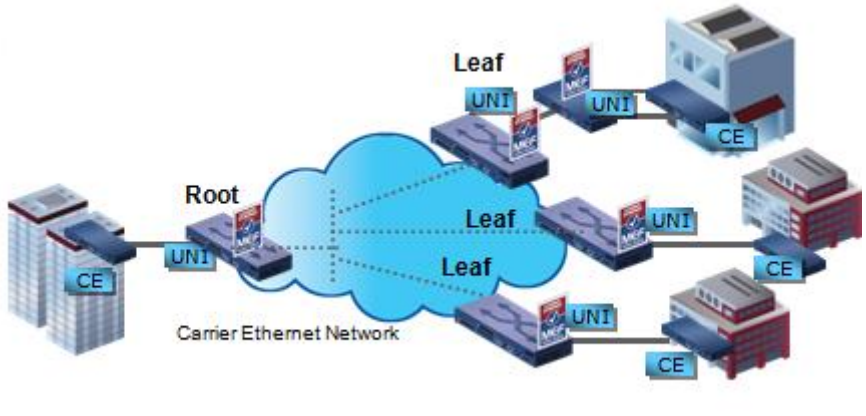
Kuva 6. Uuden toimipisteen lisääminen käyttäen E-Line palvelua (2, 6).



Kuva 7. Uuden toimipisteen lisääminen käyttäen E-LAN -palvelua (2, 6).

2.2.3 E-Tree -palvelu

Kolmas Carrier Ethernet -palvelustandardi on E-Tree, jonka ideana on mahdollistaa hub-and-spoke -tyyppinen Point-To-Multipoint -verkko (kuva 8). E-Tree verkossa lehdet (leaf) voivat keskustella yhden tai useamman juuren (root) kanssa, mutta lehdet eivät voi keskustella keskenään. Lehtien takana olevat käyttäjät eivät siis näe toisiaan, koska juuri ei välitä lehdiltä tulevaa liikennettä muille lehdille. E-Tree soveltuu hyvin esimerkiksi IPTV-palvelun jakamiseen, joka voitaisiin toteuttaa esimerkiksi H-VPLS -tekniikan (hierarkinen VPLS) avulla. (4, 16)



Kuva 8. E-Tree -palvelun malli (4, 16).

3 MPLS-TEKNIIKKA

MPLS on IETF-järjestön standardisoima runkoverkkotekniikka, jossa paketit kytketään eteenpäin IP-osoitteiden sijasta MPLS-lipuilla. Lippukytkentäisyyttä on perinteisesti pidetty monimutkaista IP-kytkentäisyyttä nopeampana ratkaisuna, mikä ei varsinkaan enää pidä paikkaansa. Tekniikan kehityksen ansiosta IP-pakettien kytkeminen on nykyään yhtä nopeaa kuin lipuilla varustettujen pakettien kytkeminen. (5, 7)

Yksi suurimmista MPLS-tekniikan hyödyistä on runkoverkon kevyt rakenne. Hallintoalueiden välillä käytettävä raskas reititysprotokolla BGP (Boarder Gateway Protocol) pitäisi olla konfiguroituna runkoverkon jokaisessa reitittimessä, jos verkon liikenteen ohjaus perustuisi IP-osoitteisiin. MPLS-verkossa riittää, että BGP on päällä vain verkon reunareitittimissä, mikä vähentää verkossa liikkuvaa kuormaa eikä sisemmissä reitittimissä tarvita niin paljoa muistia suurta reititystaulua varten. (5, 10)

3.1 MPLS-tekniikan toiminta

LSR (Label Switching Router) on MPLS-verkon reititin, joka pystyy lisäämään, poistamaan ja vaihtamaan MPLS-lippuja. MPLS-verkon yksittäisestä lippujenvaihtoreitistä käytetään nimitystä LSP (Label Switched Path). Yksittäisen LSP-reitin ensimmäinen LSR lisää paketin eteen MPLS-lipun. Keskimmäiset LSR-reitittimet korvaavat vanhat liput uusilla, ja reitin toisessa reunassa oleva LSR (tai reitin toiseksi viimeinen LSR) poistaa lipun lopulta ennen kehyksen lähettämistä MPLS-verkosta IP-verkkoon. (5, 29–32)

Suosituin tapa lipputietojen jakamiseen laitteiden välillä on LDP-protokolla (Label Distribution Protocol). LSR valitsee jokaiselle IP-reititystaulunsa reitille lipputunnisteen, ja mainostaa valintojaan omille LDP-naapureille. Sekä omat että naapurin mainostamat lipputiedot kirjataan ylös reitittimen lipputietokantaan (LIB, Label Information Base). Eri reitittimien tiettyyn kohdeverkkoon mainostamista lipuista valitaan yksi. Tämä valittu lippu lisätään LFIB-tauluun (Label Forwarding Information Base), josta LSR katsoo, minkä lipun asettaa ulos lähetettävään pakettiin. (5, 33–36)

3.2 MPLS-sovellukset

Joustavan ja monipuolisen MPLS-tekniikan ympärille on vuosien varrella kehitetty erilaisia sovelluksia, joista merkittävimmät ovat AToM (Any Transport over MPLS), MPLS TE (Traffic Engineering), MPLS L3VPN ja L2VPN-tyyppiä edustava VPLS (Virtual Private LAN Service). Tässä kappaleessa käydään läpi pääpiirteittäin kolme ensimmäistä sovellusta, ja VPLS-tekniikka käsitellään myöhemmin perusteellisesti omassa kappaleessaan.

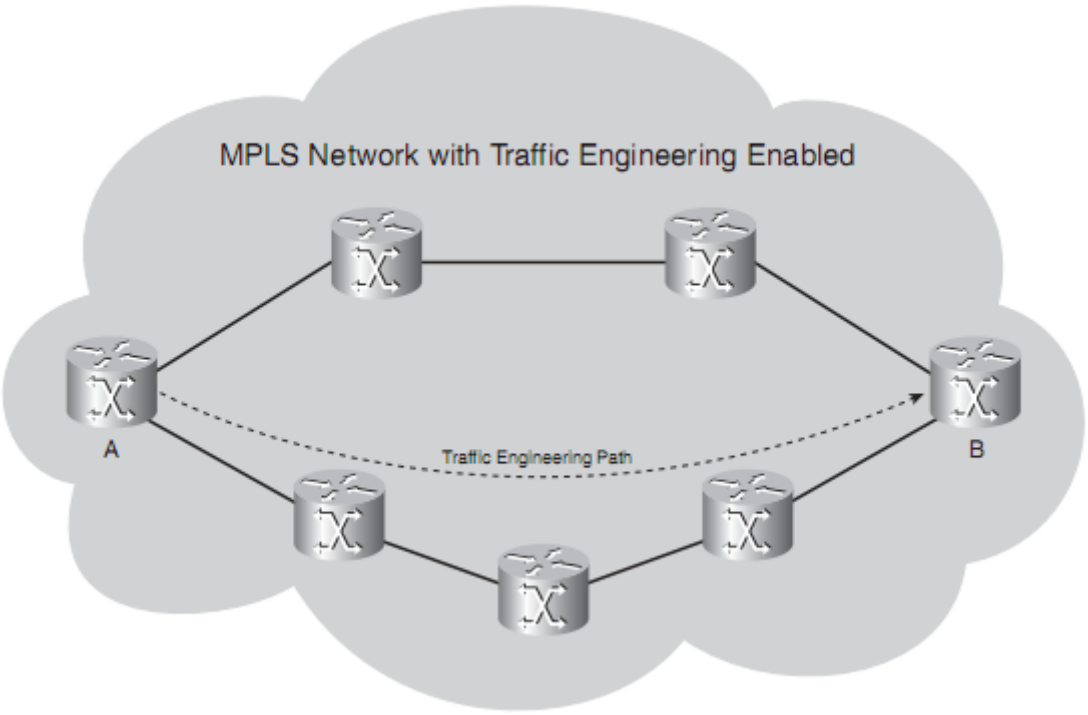
3.2.1 Any Transport over MPLS

Yksi suurimmista syistä IP:n valta-aseman saavuttamiselle on, että sen yli voidaan kuljettaa lukuisia eri tekniikoilla toteutettuja yhteyksiä. Kuljetusmahdollisuudet vain laajentuvat kun käytetään IP:n rinnalla MPLS-tekniikkaa, sillä MPLS-lipuilla varustettuihin paketteihin voidaan mahduttaa IPv4, IPv6, Ethernet, HDLC, PPP ja muita siirtoyhteyskerroksen tekniikoita. Tämä ominaisuus tunnetaan nimellä AToM.

Erinäisten siirtoyhteyskerroksen protokollien kuljettamisen mahdollistaa se, että reitittimien ei tarvitse tietää mitään MPLS-pakettien sisällöstä, vaan ne katsovat paketeista ainoastaan sen MPLS-lipun, jonka perusteella ne kytketään eteenpäin. Palveluntarjoaja pystyy kuljettamaan kaiken tyyppistä asiakasliikennettä yhdessä ainoassa verkkoinfrastruktuurissa. (5, 7)

3.2.2 MPLS Traffic Engineering

MPLS-verkossa oletusreitit määräytyvät reititysprotokollan laskutoimitusalgoritmien (esim. shortest path first) mukaisesti. Seurauksena voi olla tiettyjen yhteysvälien ruuhkautuminen liikenteen kulkiessa aina reititysprotokollan ilmoittamaa lyhintä reittiä pitkin. MPLS-tekniikan Traffic Engineering -sovelluksella voidaan määritellä haluttu liikenne kulkemaan alihyödynnettyjä reittejä pitkin, jolloin saadaan jaettua liikennettä tasaisemmin ja hyödynnettyä verkkoinfrastruktuuria tehokkaammin. Kuvan 9 esimerkissä ylempi reitti on reititysprotokollan mukaan nopein, koska matkalla on vähemmän hyppyjä, mutta TE-sovelluksen avulla liikenne ohjataan kulkemaan alempaa reittiä pitkin, koska siellä on vähemmän ruuhkaa. (5, 18)



Kuva 9. MPLS TE -sovelluksen toimintaperiaate (5, 18).

3.2.3 MPLS L3VPN

VPN (Virtual Private Network) on julkisessa verkkoinfrastruktuurissa toimiva verkko, joka toimii yksityisen verkon tavoin. VPN-verkon keskeisin vaatimus on, että asiakkaan toimipisteet voivat kommunikoida keskenään julkisen verkon läpi, mutta eivät näe muiden yritysten vastaavia samassa julkisessa infrastruktuurissa toimivia VPN-verkkoja. MPLS L3VPN on palveluntarjoajalle nykyaikainen verkkokerroksella toimiva VPN-vaihtoehto, jolla voidaan esimerkiksi korvata vanhat Frame Relay- ja ATM-verkot. Tekniikan etuja ovat muun muassa skaalautuvuus ja mahdollisuus jakaa suuri verkko pienempiin osiin. (5, 173)

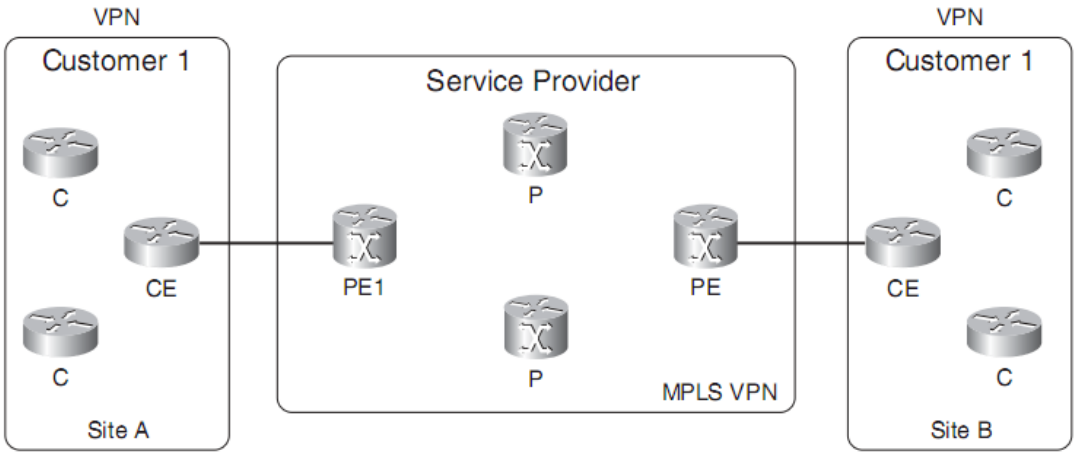
MPLS L3VPN -verkossa (Kuva 10) on neljän tyyppisiä laitteita:

PE (Provider Edge): palveluntarjoajan reunalaitteet

P (Provider): palveluntarjoajan verkon runkolaitteet

CE (Customer Edge): asiakkaan reunalaitteet

C (Customer): asiakkaan reunalaitteen takana olevat laitteet, jotka eivät osallistu VPN-tunnelin muodostukseen mitenkään.



Kuva 10. MPLS L3VPN -verkon topologia (5, 174).

PE-laitteilla on IP-tason yhteys CE-laitteiden kanssa, joten niiden välillä pitää olla joko reititysprotokolla tai staattinen reititys. P-laitteet ovat MPLS-verkon runkolaitteita, jotka eivät ole tekemisissä asiakkaan laitteiden kanssa, vaan niiden ainoa tehtävä on välittää MPLS-paketteja eteenpäin. (5, 174–175)

Asiakkaat erotellaan MPLS L3VPN -verkossa VRF-instanssien (VPN Routing and Forwarding) avulla. PE-laitteissa jokaiselle VPN-yhteydelle on oma erillistä reititystaulua ylläpitävä VRF-instanssi, joka on yhteydessä asiakkaan CE-laitteen kanssa. Asiakkaiden omat reititystiedot kulkevat VRF-instanssien välillä, eikä palveluntarjoajan verkon tarvitse tietää niistä mitään. (5, 177)

VPN-reitit kuljetetaan MPLS L3VPN -verkon läpi BGP-reititysprotokollan multiprotokolla-laaajennusten (MP-BGP) avulla. Jotta eri asiakkaiden mahdolliset päällekkäiset IP-osoitteet eivät aiheuttaisi ongelmia, reitteihin lisätään RD-tunnisteet (Route Distinguisher), jolloin IPv4-osoitteet muuttuvat VPNv4-osoitteiksi. Toinen MPLS L3VPN -tekniikan käyttämä MP-BGP -laajennus on RT (Route Target), jolla määritellään, mitkä VPN-reitit otetaan vastaan VRF-instanssiin ja mitkä lähetetään eteenpäin. (5, 179–182)

MPLS L3VPN on palveluntarjoajan kannalta edeltäjiinsä verrattuna helppohoitoinen VPN-verkon toteutustapa. Asiakkaan toimipisteen lisäyksen yhteydessä palveluntarjo-

ajan ei tarvitse lisätä uusia virtuaalipiirejä overlay-tyyppisten VPN-ratkaisujen tapaan eikä IP-verkon yli rakennetuista VPN-yhteyksistä tuttuja paketti- ja reittisuodattimia tarvita, vaan IP-yhteyden määritys yhden PE-laitteen kanssa riittää. (5, 15)

4 VIRTUAL PRIVATE LAN SERVICE -TEKNIIKKA

VPLS (Virtual Private LAN Service) on VPN-tekniikka, jota käytetään asiakkaan eri toimipisteiden yhdistämiseen OSI-mallin toisella kerroksella. Toimipisteiden lähiverkot, jotka voivat olla maantieteellisesti kaukana toisistaan, yhdistetään toisiinsa virtuaalisesti palveluntarjoajan IP/MPLS-runkoverkon läpi. Asiakkaan näkökulmasta katsottuna verkko näyttää siltä, että lähiverkkojen välillä olisi vain normaali L2-kytkin. Jokaisella asiakkaalla on yksi tai useampi VPLS-instanssi, eli virtuaalinen lähiverkko, eivätkä ne näy toisilleen. VPLS lukeutuu Metro Ethernet Forumin määrittelemistä palvelutyypeistä E-LAN -kategoriaan.

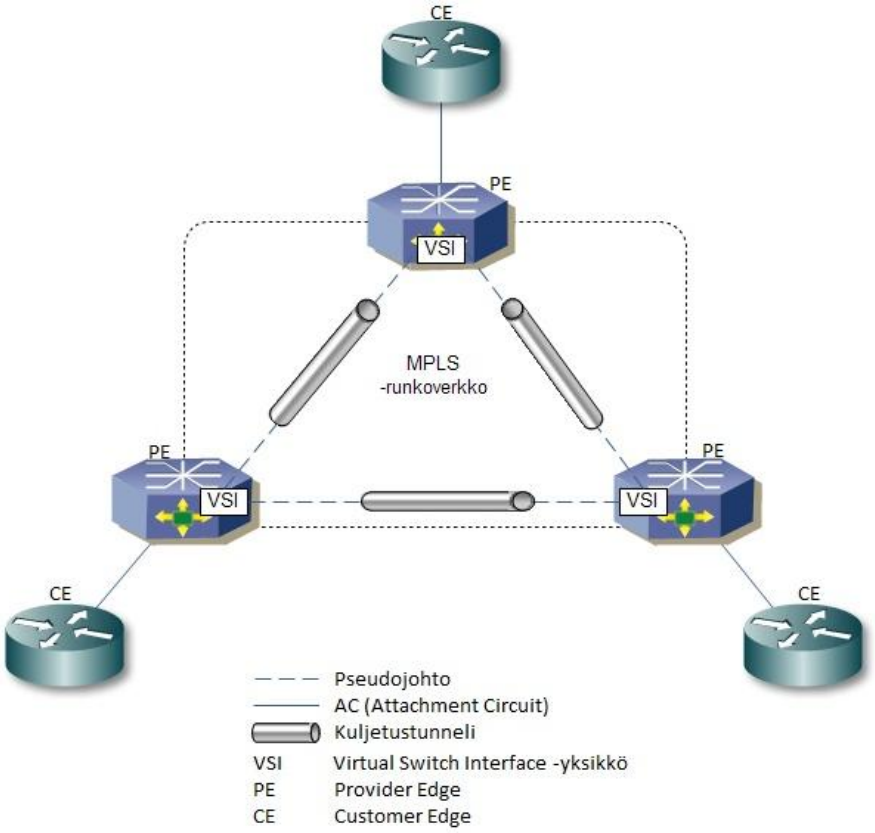
VPLS-tekniikka tuli tarpeelliseksi muiden MPLS-pohjaisten sovellusten puutteiden vuoksi. MPLS VPN tukee verkkokerroksen osalta vain IP-protokollaa. AToM pystyy kuljettamaan mitä tahansa verkkokerroksen protokollaa runkoverkon yli, mutta AToM-tekniikan ongelmana on, että se pystyy vain point-to-point -tyyppiseen tiedonsiirtoon. Sama puute koskee myös vastaavaa Ethernet over MPLS -tekniikkaa. (5, 435)

VPLS on yritysten it-tukihenkilöiden kannalta yksinkertainen tekniikka, sillä yrityksen jokaisessa toimipisteessä tarvitsee olla käytännössä vain yksi normaali Ethernet-kytkin kytkettynä yrityksen tarjoamaan Ethernet-liitäntään. Asiakkaan ja palveluntarjoajan välillä ei ole ip-yhteyttä, vaan se muodostetaan asiakkaan omien toimipisteiden välille. Virtuaalisen lähiverkon emulointi on täysin palveluntarjoajan vastuulla eikä asiakkaan tarvitse tietää siitä mitään. (6, 315–316)

4.1 VPLS-verkon komponentit

VPLS-tekniikan toiminnan ymmärtäminen vaatii siihen liittyvän termistön tuntemista. Fyysiseltä kannalta laitteisto on tuttu jo muun muassa MPLS VPN -tekniikasta, sillä myös VPLS-tekniikassa laitteet jaetaan PE, P, CE ja C -tyyppeihin. Pääpiirteittäin laitteiden roolit ovat samanlaiset tekniikasta riippumatta, mutta niiden loogiset kom-

ponentit niin laitteiden sisällä kuin yhteysväleillä vaihtelevat. Kuvassa 11 on perinteinen VPLS-verkko rakennettuna PE-laitteiden välille MPLS-runkoverkon yli. Tässä kappaleessa käydään läpi pääpiirteittäin mitä laitteiden välillä on.



Kuva 11. VPLS-verkon loogiset komponentit.

4.1.1 Pseudojohto

Yksittäistä siirtoyhteyskerroksen point-to-point -yhteyttä MPLS-verkon yli kutsutaan pseudojohdoksi. Yksi pseudojohto muodostuu kahdesta yksisuuntaisesta LSP:stä, jotka yhdessä muodostavat kaksisuuntaisen parin. Jokaisella on omat PW- ja VC-liput. PE-reitittimet vaihtavat PW-lippuja toistensa kanssa kohdistetun LDP-signaloinnin avulla. Mukana lähetetään myös VPLS-tunniste, jolla määritellään mihin VPLS-instanssiin pseudojohdot kuuluvat. Pseudojohtojen standardointiin perustuvan Pseudowire Emulation Edge To Edge -tekniikan (PWE3) ideana on, että kaikki mahdollinen pystytään kapseloimaan MPLS-pakettiin, ja lähettämään näkymättömänä verkon läpi. (7, 3)

4.1.2 Attachment Circuit -liityntä

AC (Attachment Circuit) on palveluntarjoajan PE-laitteen ja asiakkaan CE-laitteen välinen liityntä. AC-liityntänä käytetään yleensä fyysistä Ethernet-porttia, mutta muita vaihtoehtoja on muun muassa looginen Ethernet-portti tai Ethernet-kehyksiä kuljettava ATM PVC. (8, 4)

4.1.3 Virtual Switch Interface -yksikkö

Virtual Switch Interface (VSI) on PE-laitteen sisällä oleva looginen komponentti, johon AC-liitynnät ja pseudojohtot kytkeytyvät. VSI-yksikön voidaan nimensä mukaisesti ajatella olevan virtuaalinen kytkin, joita on PE-laitteessa yksi jokaista VPLS-instanssia kohden. Jokaisella VSI-yksiköllä on VSI-tunniste, jonka on oltava sama molemmissa päissä, jotta pseudojohto voidaan muodostaa niiden välille. Virtual Switch Interface tunnetaan myös nimellä Virtual Forwarding Interface (VFI). (3, 85)

4.2 VPLS-verkon muodostus

Samaan VPLS-instanssiin kuuluvat PE-reitittimet muodostavat keskenään täysverkon (full-mesh) pseudojohdoilla. Toisin sanoen kahden PE-laitteen välillä on yksi pseudojohto jokaista asiakasta kohden, eli jos jommankumman PE-laitteen takana on kahden eri asiakkaan toimipisteet, tarvitaan molemmille asiakkaille oma pseudojohto. Vastaanottava PE-laite tunnistaa pseudojohtotunnisteen perusteella, mihin VPLS-instanssiin paketti kuuluu. Pseudojohtojen lisäksi PE-laitteiden välillä on oltava myös läpinäkyvä kuljetustunneli, jonka sisällä pseudojohtojen liikenne kulkee. Kuljetustunneli voi olla esimerkiksi LDP- tai RSVP-signaloinnilla varustettu LSP-tunneli, mutta myös GRE- ja IPsec-tunneleita voidaan käyttää. (6, 319)

Pelkkä VPLS-instanssien määritys PE-laitteeseen ei vielä riitä, vaan PE-laitteen on tiedettävä, missä muut samaan instanssiin kuuluvat PE-laitteet sijaitsevat. PE-laitteet voivat löytää toisensa ja muodostaa tarvittavat pseudojohdot keskenään automaattisesti, jos signalointimenetelmänä käytetään BGP-protokollaa, mutta VPLS-tekniikan LDP-versiota käytettäessä pseudojohdot pitää määrittää manuaalisesti kertomalla VPLS-instanssille muiden instanssiin kuuluvien laitteiden IP-osoitteet. Tässä työssä käsitellään VPLS-tekniikan LDP-versiota. (6, 319)

VPLS-verkossa liikkuvat kehykset on varustettu kahdella MPLS-lipulla: tunnelilipulla ja VC-lipulla. Ulompi tunnelilippu kertoo, mihin kuljetustunneliin (eli mille PE-laitteelle) kehys tulisi lähettää. VC-lippu kantaa VC-tunnisteen, joka ilmaisee, mihin VPLS-instanssiin LDP-viesti kuuluu. Jokaisella VPLS-instanssilla on oma VC-tunniste, jonka on oltava sama jokaisessa instanssiin kuuluvassa PE-laitteessa. VPLS-tekniikan LDP-versiossa VC-tunnisteet on määritettävä itse (Ciscon laitteessa komennolla *vpn id*). (6, 327–328)

4.3 Liikenteen ohjaus

VSI muodostaa virtuaalisen kytkentätaulun (virtual switching table) aivan kuin normaalit Ethernet-kytkimet. Liikennettä tarkkailemalla VSI ottaa ylös, mitkä MAC-osoitteet ovat kunkin pseudojohdon ja AC-liitännän takana. Tiedot kirjataan kytkentätauluun, jonka perusteella VSI tekee myöhemmin päätökset, mihin saapuneet paketit lähetetään. Jokaisella PE-reitittimellä on erilliset taulut eri VPLS-instansseille. (3, 86)

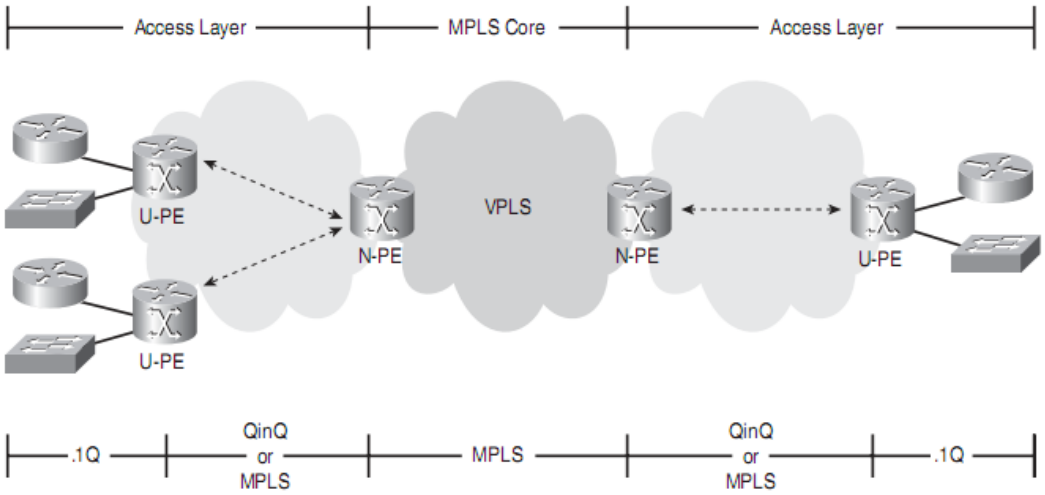
Jos kehyksen kohde-MAC-osoite löytyy kytkentätaulusta, VSI lähettää sen oikeaan pseudojohtoon tai AC-liityntään. Tuntemattomilla osoitteilla varustetut kehykset lähetetään jokaiseen pseudojohtoon ja AC-liityntään, paitsi sinne, mistä kehys saapui VSI-yksikköön. Multicast- ja broadcast-kehyksiä käsitellään täysin samalla tavalla, kuin tuntemattoman kohdeosoitteen omaavia unicast-kehyksiä. (3, 86)

VPLS-palvelussa silmukat pidetään kurissa Split Horizon -säännön avulla, eli pseudojohdosta tulevia kehyksiä ei lähetetä muihin pseudojohtoihin, vaan pelkästään AC-yhteyksien kautta CE-laitteille. Spanning Tree Protocol -silmukanestoprotokollaa ei tarvita, koska pseudojohtojen muodostamassa täysverkossa kehykset voidaan lähettää suoraan PE-laitteelta toiselle ilman välikäsiä. Täysverkossa reitit ovat täysin kahden laitteen välisiä, joten silmukoita ei pääse syntymään. (6, 322)

4.4 Hierarkinen VPLS

Suurissa verkoissa perinteisen VPLS-tekniikan ongelmaksi muodostuu ylläpidettävien pseudojohtojen ja liikkuvien pakettien määrä PE-laitteiden välillä. E-Tree -palvelutyypiksi lukeutuva H-VPLS -tekniikka parantaa tilannetta jakamalla verkon pienempiin osiin lisäämällä PE-laitteiden ja asiakkaan väliin uuden kerroksen.

H-VPLS -verkossa PE-laitteet on jaettu kahteen tyyppiin: N-PE ja U-PE (kuva 12). MPLS-runkoverkko toimii N-PE laitteiden välillä. N-PE laitteet kytketään verkon ulkoreunalla sijaitseviin U-PE laitteisiin joko dot1q-tunneloinnilla (QinQ) tai MPLS-tekniikalla, jolloin runkoverkon ulkopuolelle muodostuu uusi liityntäkerros. (5, 450)



Kuva 12. Hierarkisen VPLS-verkon malli (5, 450).

5 PALVELUINSTANSSIT

Tässä kappaleessa käsitellään Cisco Systemsin ES- ja SIP-linjakorttien mahdollistamaa palveluiden määrittelytilaa, eli palveluinstanssia (Service Instance). Aihe on olennainen osa tässä työssä myöhemmin käsiteltävää SimuNet-verkon VPLS-toteutusta, joten palveluinstanssit on hyvä käydä läpi perusteellisesti varsinkin kun palveluinstansseista on niukasti virallista dokumentaatiota saatavissa.

Palveluinstanssi reitittimessä on Ethernet-palveluiille suunniteltu ominaisuus, jossa haluttu liikenne otetaan mukaan palveluun käsiteltäväksi. Palveluinstanssien avulla yhteen fyysiseen porttiin saadaan useita toisistaan riippumattomia palveluita, joista jokaisella on oma MAC-osoite- ja VLAN-avaruus.

Palveluinstanssin konfigurointitilaan mennään komennolla *service instance [ID] ethernet*, jossa ID:llä erotellaan palveluinstanssit toisistaan ja sillä on merkitystä vain paikallisen liityntäportin kannalta.

Esimerkki:

```
Router(config)# interface GigabitEthernet3/1/0
Router (config-if)#  service instance 1 ethernet.
```

5.1 Liikenteen siirtäminen palveluinstanssiin

Instanssiin mukaan otettava liikenne määritellään *encapsulation dot1q [VLAN-ID]* käskyllä. Komennon nimestä huolimatta instanssiin tulevia kehyksiä ei tässä vaiheessa kapseloida mitenkään, vaan komento määrittää, millä VLAN-tunnisteilla varustetut paketit otetaan instanssiin tarkasteltavaksi ja käsiteltäväksi. Instanssiin voidaan ottaa myös kahdella VLAN-tunnisteella varustettuja kehyksiä komennolla *encapsulation dot1q [VLAN-ID]second-dot1q [VLAN-ID]*, jossa ensimmäisen VLAN-ID:n on oltava yksittäinen, mutta toisen ID:n paikalle voidaan asettaa VLAN-alue tai lista. Palveluinstanssissa voi olla vain yksi *encapsulation*-käsky.

Esimerkkejä:

```
Router (config-if-srv)# encapsulation dot1q 10
  ! hyväksyy instanssiin kehykset, joissa uloin tunniste on 10
Router (config-if-srv)# encapsulation dot1q 10-12
  ! hyväksyy jos uloin tunniste on 10, 11 tai 12
Router (config-if-srv)# encapsulation dot1q 10,12
  ! hyväksyy jos uloin tunniste on 10 tai 12
Router (config-if-srv)# encapsulation dot1q 10 second-dot1q 12
  ! hyväksytään kehykset, joissa uloin VLAN-tunniste on 10 ja toiseksi uloin 12
Router (config-if-srv)# encapsulation dot1q any
  ! hyväksyy millä tahansa tunnisteella varustetut kehykset
Router (config-if-srv)# encapsulation dot1q untagged
  ! hyväksyy kehykset, jotka eivät sisällä VLAN-tunnisteita
Router (config-if-srv)# encapsulation dot1q default
  ! ottaa mukaan kaikki loput kehykset, jotka eivät tule hyväksytyksi minkään saman
portin toisen instanssin encapsulation-lauseen perusteella.
```

Jos saman portin alla on useita palveluinstansseja, niin liikenne siirretään oikeaan instanssiin täsmällisimmän osuman mukaan. Kahdella VLAN-tunnisteella kehys menee aina ensisijaisesti instanssiin, jossa encapsulation-käskyn hyväksyntäkriteeri täsmää kehyksen molempien tunnisteiden kanssa.

Esimerkki:

Reitittimen GE3/1/0-porttiin on määritetty kolme palveluinstanssia:

```
Router(config)# interface GigabitEthernet3/1/0
Router (config-if)# service instance 1 ethernet
Router (config-if-srv)# encapsulation dot1q 10 second-dot1q 12
!
Router (config-if)# service instance 2 ethernet
Router (config-if-srv)# encapsulation dot1q 10
!
Router (config-if)# service instance 3 ethernet
Router (config-if-srv)# encapsulation dot1q default
```

1. Porttiin saapuu kahdella VLAN-tunnisteella varustettu kehys, jossa ulompi tunniste on 10 ja sisempi 12. Kehyksen uloin tunniste täsmää sekä palveluinstanssi 1:n että palveluinstanssi 2:n *encapsulation*-kriteerien kanssa, mutta koska kehyksen toiseksi uloin tunniste täsmää vain palveluinstanssi 1:n *encapsulation*-kriteerin kanssa, kehys siirretään sinne. Jos ensimmäistä palveluinstanssia ei olisi määriteltynä porttiin, kehys siirtyisi palveluinstanssi 2:een.

2. Porttiin saapuu kahdella VLAN-tunnisteella varustettu kehys, jossa ulompi tunniste on 10 ja sisempi 20. Tässäkin tapauksessa ulompi tunniste täsmää kahden ensimmäisen palveluinstanssin kanssa. Ensimmäisessä palveluinstanssissa kuitenkin vaaditaan myös VLAN 12 -tunnisteen olemassaoloa, mutta koska kehyksessä ei sitä ole, palveluinstanssi 1 on poissa pelistä. Toisessa palveluinstanssissa ei uloimman kehyksen lisäksi ole muita vaatimuskriteereitä, joten kehys siirretään palveluinstanssi 2:een.

3. Porttiin saapuu kahdella VLAN-tunnisteella varustettu kehys, jossa ulompi tunniste on 20 ja sisempi 10. Ulompi tunniste ei täsmää kahden ensimmäisen instanssin kriteereiden kanssa, joten kehys lähetetään palveluinstanssi 3:een, sillä *default*-parametri hyväksyy kaikki täsmällisimpiin instansseihin kelpaamattomat kehykset. Myös ilman VLAN-tunnistetta olevat kehykset kelpaavat default-instanssiin.

5.2 VLAN-tunnisteiden manipulointi

Palveluinstanssiin siirrettyjen kehysten VLAN-tunnisteita voidaan muokata *rewrite ingress tag* -komennolla. Käytännössä mitkä tahansa 0–2 tunnistetta voidaan korvata millä tahansa 0–2 tunnisteella. Käytettävissä on kolme operaatiota: push, pop ja translate, eli tunnisteita voidaan lisätä, poistaa ja muuttaa toiseksi. Komentoon on aina lisättävä perään pakollinen *symmetric* -parametri, sillä järkevää käyttöä epäsymmetriselle toiminnalle ei ole. Mitä tahansa operaatioita kehyksen VLAN-tunnisteelle suoritetaan sen tullessa sisään, samat operaatiot on tehtävä käänteisesti pakettien tullessa toisesta suunnasta. Tällöin *symmetric* -parametrin takia kehykseen lisätään *encapsulation*-käskyn osoittamat VLAN-tunnisteet, minkä jälkeen kehys otetaan pois palveluinstanssista. Yhdessä palveluinstanssissa voi olla korkeintaan yksi rewrite-komento.

Esimerkkejä:

```
PE3 (config-if-srv)# rewrite ingress tag pop 1 symmetric
  ! poistaa uloimman VLAN-tunnisteen
PE3 (config-if-srv)# rewrite ingress tag pop 2 symmetric
  ! poistaa kaksi ulointa VLAN-tunnistetta
PE3 (config-if-srv)# rewrite ingress tag push dot1q 10 symmetric
  ! lisää yhden VLAN-tunnisteen (10)
PE3 (config-if-srv)# rewrite ingress tag push dot1q 10 second-dot1q 12 symmetric
  ! lisää kaksi VLAN-tunnistetta (10 ja 12)
PE3 (config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 10 symmetric
  ! korvaa alkuperäisen tunnisteen 10:llä
PE3 (config-if-srv)# rewrite ingress tag translate 1-to-2 dot1q 10 second-dot1q 12
symmetric
  ! poistaa alkuperäisen tunnisteen ja lisää tilalle 2 tunnistetta (10 ja 12)
PE3 (config-if-srv)# rewrite ingress tag translate 2-to-2 dot1q 20 second-dot1q 30
symmetric
  ! korvaa alkuperäiset tunnisteet kahdella uudella tunnisteella (20 ja 30)
```

5.3 Palveluiden yhdistäminen

Palveluinstanssin määrittelyn jälkeen se pitää yhdistää jonnekin, jotta sillä olisi virkaa. Palveluinstanssi voidaan yhdistää muun muassa L2-kytkinporttiin, SVI-porttiin tai toiseen palveluinstanssiin muun muassa seuraavilla menetelmillä: local connect, xconnect, monipistesiltaus ja reititetty yhteys.

5.3.1 Point-To-Point local connect

Local connect -menetelmän avulla voidaan yhdistää kaksi palveluinstanssia toisiinsa L2-tasolla. Palveluinstanssit voivat olla joko saman tai eri portin alla. Jotta kehykset voisivat kulkea palveluinstanssista toiseen, niiden täytyy kelvata VLAN-tunnisteiden osalta kumpaankin palveluinstanssiin, eli mahdolliset erot on poistettava *rewrite*-käskyillä, jos *encapsulation*-käskyt ovat erilaisia. Koska local connect muodostuu tasan kahden pisteen välille, ei MAC-osoitteiden oppimista tai globaaleja VLAN-tunnisteita tarvita.

Esimerkki:

```
Router(config)# interface GigabitEthernet3/1/0
Router (config-if)# service instance 1 ethernet
Router (config-if-srv)# encapsulation dot1q 10
!
Router(config)# interface GigabitEthernet3/1/1
Router (config-if)# service instance 2 ethernet
Router (config-if-srv)# encapsulation dot1q 20
Router (config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 10 symmetric
   ! VLAN-tunnisteet muutetaan toisessa palveluinstanssissa vastaamaan ensimmäisen instanssin tunnisteita, jotta palveluinstanssit voidaan yhdistää keskenään. Jos molemmissa instansseissa olisi määriteltynä encapsulation dot1q 10, ei tunnistetta tarvisi vaihtaa.
!
Router(config)# connect lc-nimi GE3/1/0 1 GE3/1/1 2
   ! local connect muodostetaan GE3/1/0 portin palveluinstanssi 1:n ja GE3/1/1 portin palveluinstanssi 2:n välille, ja yhteyden nimeksi asetetaan "lc-nimi".
```

5.3.2 Point-To-Point xconnect

Point-To-Point xconnect -menetelmää käytetään EoMPLS-yhteyden muodostamiseen kahden eri laitteen välille. Jos xconnect muodostetaan reitittimen palveluinstanssista toisen reitittimen palveluinstanssiin, VLAN-tunnisteet on oltava identtisiä. Xconnect voidaan muodostaa myös toisen reitittimen aliliityntäporttiin, jolloin uloin tunniste on poistettava *rewrite*-käskyllä, sillä toisessa päässä oleva aliliityntäportti poistaa sen automaattisesti. Samoin kuin local connect -ratkaisussa, xconnect ei käytä globaalia VLAN-avaruutta eikä MAC-osoitteiden oppimista suoriteta.

Esimerkki:

```
Router1(config)# interface GigabitEthernet3/1/0
Router1(config-if)# service instance 1 ethernet
Router1(config-if-srv)# encapsulation dot1q 10
Router1(config-if-srv)# xconnect 198.168.10.2 1 encapsulation mpls
!
```

```
Router2(config)# interface GigabitEthernet3/1/0
Router2(config-if)# service instance 1 ethernet
Router2(config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Router2(config-if-srv)# rewrite ingress tag pop 1
  ! poistetaan ulompi tunniste (20), jotta palveluinstanssit olisivat yhteensopivia
Router2(config-if-srv)# xconnect 198.168.10.1 1 encapsulation mpls
```

5.3.3 Monipistesiltaus

Monipistesiltauksessa palveluinstanssi voidaan yhdistää laitteen globaaliin VLAN:iin L2-tasolla luomalla siltausalue (bridge-domain). Palveluinstanssin läpi kulkevaa liikenne voidaan siirtää siltausalueen kautta VLAN-porttiin, jossa voi olla määriteltynä esimerkiksi EoMPLS-yhteyden *xconnect*-käsky, joten palveluinstanssit soveltuvat hyvin esimerkiksi VPLS-verkon toteutustavaksi. Siltausalueita voidaan käyttää myös pelkästään palveluinstanssien yhdistämiseen kytkemällä ne samaan siltausalueeseen. Kehykseen lisätään *bridge-domain* -käskyn osoittama VLAN-tunniste sen liittyessä siltausalueeseen, joten tunnistemanipuloinnin kanssa on oltava tarkkana.

Esimerkki:

Palveluinstanssit yhdistetään keskenään siltausalueen avulla. Konfiguraatiossa poimitaan VLAN 10-, 20- ja 30 -kehykset omiin palveluinstansseihinsa, joissa niiden alkuperäiset VLAN-tunnisteet poistetaan, ja kukin instanssi kytketään siltausalue 40:een.

```
Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 40
!
Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# service instance 2 ethernet
Router(config-if-srv)# encapsulation dot1q 20
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 40
```

```
!
Router(config)# interface GigabitEthernet3/1/1
Router(config-if)# service instance 3 ethernet
Router(config-if-srv)# encapsulation dot1q 30
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 40
```

Esimerkki:

Tässä esimerkissä palveluinstanssi yhdistetään L2-trunk-porttiin. Trunk-porteissa VLAN-tunniste poistetaan automaattisesti, joten alkuperäinen tunniste on poistettava palveluinstanssissa *rewrite* -käskyllä, jotta siltausalueen molemmat puolet olisivat yhteensopivia.

```
Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 40
!
Router(config)# interface GigabitEthernet3/1/1
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport trunk allowed vlan 40
Router(config-if)# switchport mode trunk
```

5.3.4 Reititetty yhteys

Siltausaluetta voidaan käyttää myös liikenteen siirtämiseen palveluinstanssista L3-SVI-porttiin, josta se jatkaa eteenpäin verkkokerroksella. Alkuperäinen VLAN-tunniste on poistettava.

Esimerkki:

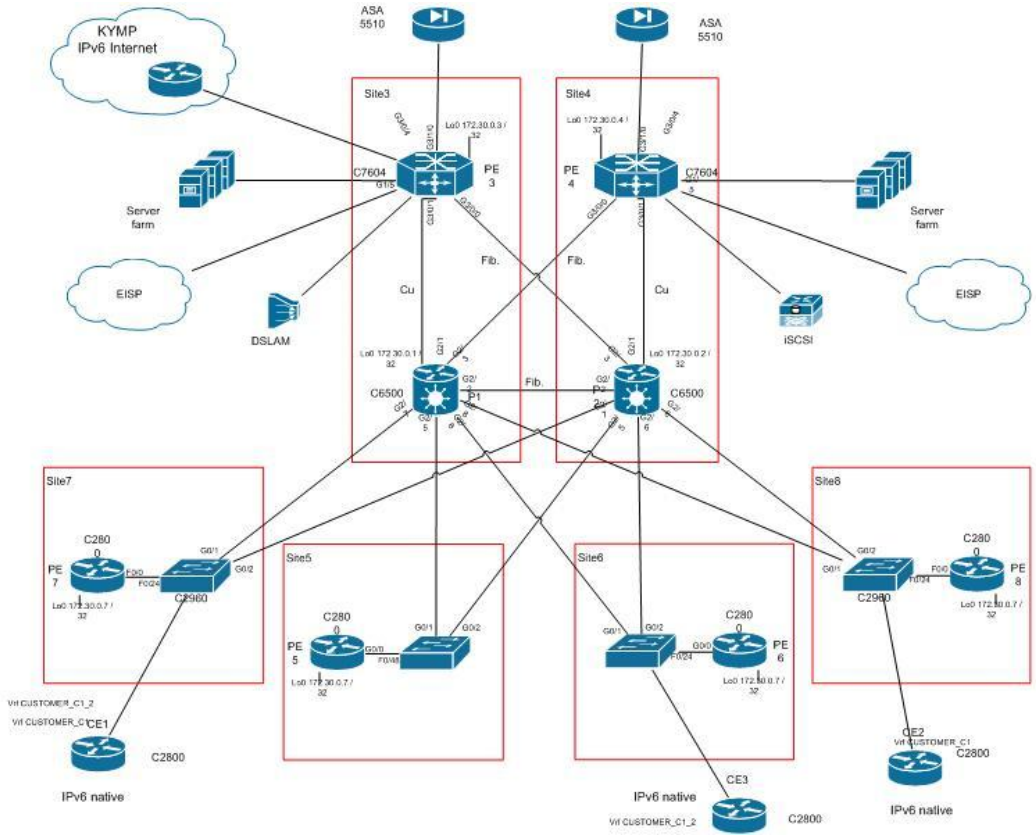
Esimerkissä palveluinstanssi yhdistetään L3-SVI-porttiin.

```
Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 20
!
Router(config)# interface Vlan 20
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

6 SIMUNET

SimuNet on Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorion ja alueen palveluntarjoajien yhteinen projekti, jossa rakennetaan palveluntarjoajan tuotantoverkkoa kuvaava testiympäristö opiskelijoiden projekteja ja palveluntarjoajien testejä varten. Palveluntarjoajan omaan verkkoon suunnittelemat muutokset voidaan testata etukäteen SimuNet-testiympäristössä, jotta migraatio menisi mahdollisimman sulavasti palveluntarjoajan oikean tuotantoverkon kanssa.

SimuNet-verkon ydin on sen runkoverkko, joka on jaettu kahteen eri maantieteellistä sijaintia simuloivaan laatekaappiin: site 3 ja site 4 kuvassa 13. Runkoverkko koostuu neljästä päälaitteesta: kahdesta Ciscon C6500-sarjan kytkimestä (P-laitteet) ja kahdesta C7604-reitittimestä (PE-laitteet), joihin VPLS-yhteydet terminoituvat. C7604-reitittimet ovat modulaarisia, joten niihin saa tarpeiden mukaan kiinnitettyä erillisiä lisäominaisuuksia tuovia moduuleja. Reitittimet eivät oletuksena tue esimerkiksi VPLS-tekniikassa vaadittavaa L2VPN-ominaisuutta, joten reitittimiin on asennettu SIP400-lisämoduulit mahdollistamaan VPLS-konfiguraatioiden luomisen.



Kuva 13. SimuNetin runkoverkon fyysinen topologia.

6.1 SimuNet-verkon VPLS-toteutus

Seuraavassa esitetään muutamia VPLS-toteutuksia. Toteutukset voitaisiin soveltaa esimerkiksi SimuNet-verkossa kahdessa eri laitetilassa olevien palomuurilaitteiden yhdistämisessä. Liikenne kulkee tunnelin päästä päähän PE- ja P-laitteiden muodostaman MPLS-runkoverkon läpi. Jokaiselle VLAN:lle on oma VPLS-instanssinsa, eivätkä ne näe toisiaan millään tavalla, vaikka eri instanssien päätepisteet ovat fyysisesti samoissa porteissa. Tässä kappaleessa käydään SimuNet-verkon VPLS-toteutus pala palalta läpi konfiguraatioiden ja toiminnan osalta.

VPLS-instanssit on konfiguroitu fyysisen portin alle palveluiksi, eli jokaiselle VLAN:lle on oma palveluinstanssinsa, jolla saadaan fyysinen portti jaettua useiksi erilliset VLAN- ja MAC-osoiteavaruudet omaaviksi loogisiksi porteiksi. Palveluinstanssit ovat käytössä, koska ilman palveluinstansseja rakennettu VPLS-toteutus ei toimisi kunnolla 7600-reitittimen SUP- ja SIP-korttien välisen L2-L3-rajapinnan takia. L2-protokollien tunnelointi VPLS-tunnelin läpi onnistuu vain palveluinstanssien avulla.

VPLS-instanssin eli VFI:n konfigurointitilaan mennään komennolla *l2 vfi [nimi] manual*, jossa *manual*-parametri tarkoittaa, että yhteys toisen pään kanssa muodostetaan käyttäjän antamien asetusten perusteella. Parametri on oltava komennossa käytännössä aina, sillä automaattiset mekanismit ovat vielä tulevaisuuden tekniikkaa.

```
PE3(config)# l2 vfi Palomuuri1 manual
PE3(config-vfi)# vpn id 10
PE3(config-vfi)# neighbor 172.30.0.4 encapsulation mpls
!
PE3(config)# l2 vfi Palomuuri2 manual
PE3(config-vfi)#  vpn id 20
PE3(config-vfi)#  neighbor 172.31.0.4 encapsulation mpls
!
```

VPLS-instanssin tunniste määritellään VFI:n konfigurointitilassa komennolla *vpn id [id]*. Tunnisteen on oltava kokonaisluku väliltä 1- 4 294 967 295. Tässä esimerkissä tunnisteet on selvyyden vuoksi määritetty vastaamaan VLAN:eja. Komennolla *neigh-*

bor [router ID] encapsulation mpls kerrotaan VFI:lle, missä instanssin muut PE -laitteet sijaitsevat ja mitä pseudojohtokapselointia käytetäään. IP-osoite 172.31.0.4 on PE4-laitteen loopback-osoite, eli LDP-signalointia varten konfiguroitu reitittimen ID.

```
PE3(config)# interface GigabitEthernet3/1/0
PE3(config-if)#  description Palomuurin trunk
PE3(config-if)#  mtu 1600
PE3(config-if)#  no ip address
PE3(config-if)#  no negotiation auto
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
```

SimuNet-verkossa PE3-laitteen palveluinstanssi 1:een otetuista kehyksistä poistetaan VLAN-tunniste 10 ennen lähettämistä VPLS-tunneliin. Tunniste on poistettava, koska VLAN 10-SVI-portista eteen päin liikenne jatkaa L3-tasolla. Vastaavasti toisesta suunnasta, eli VPLS-tunnelista palveluinstanssiin saapuviin ilman tunnistetta oleviin kehyksiin lisätään *encapsulation*-käskyn määräämä tunniste, eli 10.

Lopuksi palveluinstanssille on kerrottava, että mihin sen käsittelemät kehykset lähetetään. Komento *Bridge-domain 10* yhdistää instanssin VLAN 10:n kanssa samaan loogiseen verkkoon, eli käytännössä voidaan ajatella, että palveluinstanssi ja vlan 10 -portti kytketään samaan virtuaaliseen kytkimeen kiinni.

```
PE3(config)# interface Vlan10
PE3(config-if)# mtu 1600
PE3(config-if)# ip address 172.30.1.2 255.255.255.248
PE3(config-if)# xconnect vfi Palomuuri1
```

Komento *xconnect vfi Palomuuri1* kiinnittää aiemmin luodun Palomuuri1-nimisen VFI:n loogiseen VLAN 10 -porttiin. Reititin ei hyväksy komentoa, ellei VFI ole valmiiksi määriteltynä.

Kaikki VPLS-komennot ovat symmetrisiä runkolaitteissa, eli esitetyt komennot löytyvät myös PE4-laitteista toiseen suuntaan menevillä IP-osoitteilla. Komennot ovat symmetrisiä myös palveluinstanssien ja VLAN:ien välillä.

7 YHTEENVETO

Työn tavoitteet olivat Carrier Ethernet -palveluihin perehtyminen, E-LAN -palvelutyyppiä edustaman VPLS-tekniikan käsittely niin teoriassa kuin käytännössä ja reitittimien palveluinstanssien konfigurointitilaan tutustuminen. Keskeiset tavoitteet täyttyivät, ja lisäksi työssä esiteltiin teorian tasolla Metro Ethernet -verkon perusteet sekä MPLS-tekniikka.

Työn käytännön osiona oli olla mukana suunnittelemassa ja toteuttamassa VPLS-yhteyksiä SimuNet-verkkoon. Erilaisia toteutustapoja tuli kokeiltua useita, mutta suuressa osassa toteutuksista tuli vastaan rajoituksia, jotka pakottivat etsimään uusia toimintamalleja. Lopullinen toteutustapa löytyi Cisco 7600 -sarjan reitittimien ja niihin kiinnitettyjen SIP-lisäkorttien mahdollistamasta palveluinstanssien konfigurointitilasta. Palveluinstanssilla saatiin kierrettyä muun muassa siirtoyhteyskerroksen liikenteen estävät ongelmat. Lisäksi toteutustapa soveltuisi myös suuriin verkkoihin, koska jokaisella palveluinstanssilla on omat MAC-osoite- ja VLAN-avaruutensa.

Palveluinstanssien määritystilan komennoista muodostui oma kappale, jota voidaan myöhemmin käyttää ohjeena niin VPLS-tekniikan kuin muidenkin palveluiden toteutuksissa.

Opinnäytetyössä käsiteltiin EVC-tunnelin kuljetusmekanismeista vain MPLS-vaihtoehtoa. Koko työn aiheen kannalta käsittelyyn olisi voinut ottaa muista vaihtoehdoista ainakin puhtaat Ethernet-ratkaisut: QinQ ja MinM, mutta aika ei lopulta riittänyt laajentamiseen. Koko työn alkuperäinen idea oli erilaisten toteutusmallien vertailu, mutta lopputulos muotoutui enemmänkin yhden tavan perusteelliseksi esittelyksi. Myös VPN-maailma MPLS VPN -tekniikkaa lukuunottamatta ja Ethernet over MPLS jäivät lopulta työn ulkopuolelle.

LÄHTEET

1. Metro Ethernet Forum. 2002–2004. Metro Ethernet Networks - A Technical Overview. Saatavissa: http://metroethernetforum.org/PDFs/WhitePapers/metro-ethernet-networks.pdf [viitattu 26.10.2010].

2. Metro Ethernet Forum. Metro Ethernet Services - A Technical Overview. Saatavissa: http://www.metroethernetforum.org/PDF_Documents/metro-ethernet-services.pdf [viitattu: 19.8.2010].

3. Mamentor: Metro/Carrier Ethernet Services in Operator Networks. Luentomateriaalilehtiö. [viitattu 25.10.2010].

4. Metro Ethernet Forum. 2008. Carrier Ethernet Services Overview. Saatavissa: http://www.metroethernetforum.org/PPT_Documents/EthernetServicesOverview.ppt [viitattu 26.10.2010].

5. De Ghein, L. 2007. MPLS Fundamentals. Cisco Press.

6. Minei, I & Lucek, J. 2008. MPLS-Enabled Applications - Emerging Developments and New Technologies. John Wiley & Sons, Ltd.

7. Alcatel. 2004. VPLS Technical Tutorial. Saatavissa: http://www.exponentiale.com/PDF/whitepapers/VPLS-Technical-Primer.pdf [viitattu 26.03.2010].

8. Kompella, V. Lassarre, E. 2007. RFC 4762 Virtual Private Lan Service over LDP. Saatavissa: http://www.rfc-editor.org/rfc/rfc4762.txt [viitattu 5.11.2010].