SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

ETHERNET VPN

TEKIJÄ: Mikko Väätäinen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Mikko Väätäinen	
Työn nimi Ethernet VPN	
Päiväys 20.11.2015	Sivumäärä/Liitteet 44/1
Ohjaaja(t) Lehtori Veijo Pitkänen / Savonia-ammattikorkeakoulu	
Toimeksiantaja/Yhteistyökumppani(t) Savonia-ammattikorkeakoulu	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutustua Ethernet VPN (EVPN) -tekniikkaan, joka on hiljattain standardoitu tekniikka Layer2 VPN -palveluiden toteuttamiseen. Standardin esittelyn lisäksi työn tavoitteena oli testata Ethernet VPN:n toimintaa Savonia-ammattikorkeakoulun tietoverkkolaboratoriossa.

Teoriaosuudessa on esitelty keskeiset operaattoritasoisten VPN-palveluiden taustalla olevat tekniikat, kuten Multiprotocol Label Switching (MPLS) ja Multiprotocol BGP (MP-BGP). Ethernet VPN on esitelty RFC 7432 -standardin mukaisesti. Kokeellisessa osuudessa konfiguroitiin Ethernet VPN -toteutus Savonia-ammattikorkeakoulun tietoverkkolaboratoriossa.

Työlle asetetut tavoitteet saavutettiin, ja tuloksena syntynyt opinnäytetyö toimii johdantona uuteen tekniikkaan ja sen ominaisuuksiin. Kokeellisessa osuudessa tuotettuja konfiguraatioita voidaan hyödyntää tulevaisuudessa suunniteltaessa uusia laboratorioverkkoja VPN-palveluiden simuloimiseksi.

Avainsanat
BGP, MPLS, VPN

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Mikko Väätäinen			
Title of Thesis Ethernet VPN			
Date	20 November 2015	Pages/Appendices	44/1
Supervisor(s) Mr. Veijo Pitkänen, Principal Lecturer / Savonia University of Applied Sciences			
Client Organisation /Partners Savonia University of Applied Sciences			

Abstract

The subject of this thesis was Ethernet VPN (EVPN), a newly standardized MPLS / BGP based Layer2 VPN technology. The purpose was to introduce the new technology, and verify its operation by configuring a sample EVPN topology in Savonia UAS's network laboratory.

The first part of the work was to get familiar with fundamental building blocks of carrier grade VPN services. EVPN features defined by Internet Engineering Task Force (IETF) were researched. The last step of the theoretical part was to research the RFC 7432 internet standard that defines the EVPN operation.

In the experimental part of the thesis, the EVPN configuration was tested at Savonia UAS's network laboratory. Two different types of service interfaces were evaluated on Juniper MX series routers.

The result of the thesis was an introduction to carrier VPN technologies and the Ethernet VPN standard, and configuration examples of two types of EVPN service instances.

Keywords
BGP, MPLS, VPN

ESIPUHE

Haluan kiittää erityisesti opinnäytetyön ohjaajaa, lehtori Veijo Pitkästä opinnäytetyön ohjauksesta ja kannustavasta tietoverkkotekniikan opetuksesta koko opintojen ajalta.

Kuopiossa 21.11.2015

Mikko Väätäinen

SISÄLTÖ

TERMIT JA LYHENTEET

AS	Autonomous System, verkkoalue, joka on saman hallinnollisen tahon alla.
ASIC	Application Specific Integrated Circuit, piiri, joka on suunniteltu tiettyä käyttötarkoitusta varten.
BGP	Border Gateway Protocol, Käytännössä ainoa käytössä oleva EGP-protokolla.
EGP	Exterior gateway protocol, autonomisten järjestelmien väliseen reititykseen käytetty protokolla.
IETF	Internet Engineering Task Force, työryhmistä koostuva avoin organisaatio joka tuottaa internet-standardeja.
IGP	Interior Gateway Protocol, yleisnimitys saman autonomisen järjestelmän sisällä käytetyistä reititysprotokollista.
IS-IS	Intermediate System-to-Intermediate System, IGP-reititysprotokolla.
OSPF	Open Shortest Path First, IGP-reititysprotokolla.
QoS	Quality of Service, liikenteen luokittelu ja priorisointi, jonka avulla voidaan taata esimerkiksi viiveelle alttiille liikenteelle suurempi prioriteetti.
RADIUS	Remote Authentication Dial In User Service, autentikointiin ja kirjanpitoon käytetty protokolla.
RIP	Routing Information Protocol, ensimmäinen, jo teknisesti vanhentunut dynaaminen reititysprotokolla.
SNMP	Simple Network Management Protocol, verkkolaitteiden hallintaan ja valvontaan käytetty protokolla.
SSH	Secure Shell, salattuun tiedonsiirtoon tarkoitettu protokolla jota voidaan käyttää esimerkiksi etähallintaan tai tiedostonsiirtoon.
VRF	Virtual Routing and Forwarding, tekniikka, jonka avulla reitittimeen voidaan muodostaa useita erillään olevia reititystauluja.

1 JOHDANTO

Opinnäytetyössä tutustutaan uuden sukupolven Layer2 VPN -toteutukseen, Ethernet VPN:ään. Työ on tehty kesän ja syksyn 2015 aikana Savonia-ammattikorkeakoululle.

Teoriaosuudessa esitellään toteutuksen kannalta oleelliset käsitteet ja tekniikat, jotka mahdollistavat EVPN:n toteutuksen. Lisäksi tutustutaan EVPN:ää edeltäviin ratkaisuihin. Protokollan tärkeimmät ominaisuudet esitellään RFC 7432 –standardin mukaisesti.

Lopuksi tutkitaan tekniikan konfigurointia käytännössä Savonian tietoverkkolaboratoriossa, johon on hankittu syksyn 2014 aikana uutta laitteistoa, joka mahdollistaa operaattoritasoisten VPN-palveluiden testaamisen käytännössä.

2 HALLINTATASO, KONTROLLITASO JA DATATASO

Hallintataso, kontrollitaso ja datataso ovat verkkolaitteiden toimintaa kuvaavia käsitteitä. Tasoja voidaan kuvata kerroksisella mallilla, jossa ylimpänä on kontrollikerroksen toimintaan vaikuttava hallintataso ja alimpana nopeasta liikenteenvälityksestä vastaava datataso. Liikenne saapuu aina datatasolle, ja sitä voidaan tarvittaessa ohjata ylempien tasojen käsiteltäväksi. (Ranjbar 2005, 437, 438.)

2.1 Hallintataso (management plane)

Verkkolaitteen hallintaan ja valvontaan liittyvät protokollat ja toiminnot sijaitsevat hallintatasolla. Hallintatasolla määritetään kontrollikerroksen toteuttamat toiminnot, esimerkiksi konfiguroidaan käytettävät reititysprotokollat. Hallintatason protokollia ovat esimerkiksi SSH, SNMP ja RADIUS. (Pepelnjak 2013.)

2.2 Kontrollitaso (control plane)

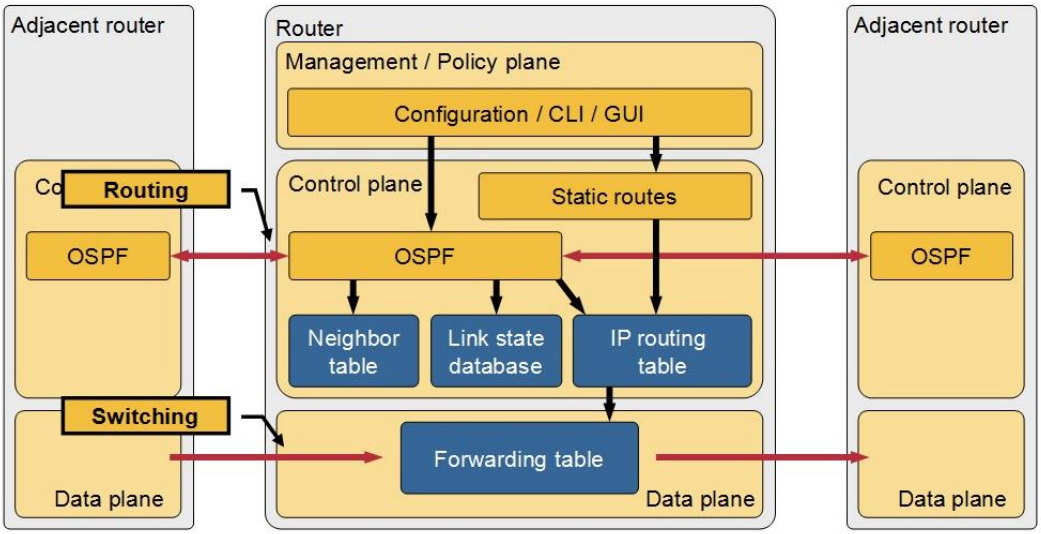
Kontrollitason tehtävänä on muodostaa liikenteenvälitykseen käytetyt tietorakenteet ja välittää tarvittavat tiedot datakerrokselle. Kontrollitaso käsittelee mm. reititysprotokollien päivitysviestit ja laskee parhaimmat mahdolliset reitit keräämiensä tietojen perusteella. (Pepelnjak 2013.)

MPLS/IP-verkoissa kontrollikerroksen tietorakenteita ovat esimerkiksi Routing Infromation Base (RIB) ja Label Information Base (LIB) -taulut. Näistä tauluista muodostetaan datakerroksella sijaitsevat, nopeaan liikenteenvälitykseen käytetyt tietorakenteet, kuten Forwarding Information Base (FIB) ja Label Forwarding Information Base (LFIB) -taulut. (Ine Inc. 2015.)

2.3 Datataso (data plane)

Datatason (data plane, forwarding plane) tehtävänä on välittää liikennettä verkkolaitteen läpi mahdollisimman tehokkaasti käyttäen kontrollitason muodostamia tietorakenteita. Liikenteenvälitys tapahtuu usein nopeilla ASIC-piireillä, eikä datatasolla tapahtuva liikenteenvälitys kuormita laitteen suoritinta (CPU). (Pepelnjak 2013.)

Konvergoituneessa verkossa suurin osa reitittimien käsittelemästä liikenteestä virtaa datakerroksen läpi saavuttamatta koskaan ylempiä kerroksia. Reititysprotokollien päivitysviestit tai esimerkiksi reitittimen hallintaosoitteeseen kohdistettu SSH-liikenne ohjataan datakerrokselta kontrollikerroksen suoritinpohjaiseen käsittelyyn. Kuvassa 1 on havainnollistettu, kuinka esitellyt kerrokset toimivat keskenään. (Pepelnjak 2013.)



KUVA 1. Verkkolaitteen toimintaa kuvaava tasomalli (Pepelnjak 2013.)

3 REITITYSPROTOKOLLAT

Reititysprotokollan tehtävä on muodostaa optimaalinen, silmukoista vapaa reititys sekä reagoida mahdollisiin topologian muutoksiin. Reititysprotokollat voidaan jakaa Interior Gateway (IGP) ja Exterior Gateway (EGP) –protokolliin. IGP-protokollia käytetään yleensä autonomisen järjestelmän sisäisessä reitityksessä ja EGP-protokollia autonomisten järjestelmien väliseen reititykseen. IGP-protokollia ovat esimerkiksi OSPF, IS-IS ja RIP. On olemassa käytännössä vain yksi käytössä oleva EGP-protokolla, Border Gateway Protocol (BGP). (Teare 2010, 26, 27, 472.)

3.1 Border Gateway Protocol

Border Gateway Protocol (BGP) on autonomisten järjestelmien väliseen reititykseen käytetty reititysprotokolla, joka on suunniteltu erityisen skaalautuvaksi ja monikäyttöiseksi. BGP käyttää kuljetuskerroksella TCP-protokollaa, se mahdollistaa luotettavan tiedonsiirron ja osittaisten päivitysten lähettämisen yhteyden alustuksen jälkeen. (Teare 2010, 46, 47.)

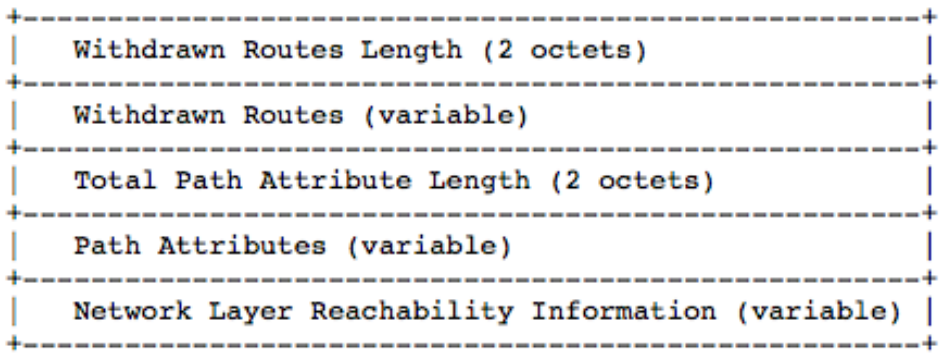
BGP-reitittimien välille muodostuvaa naapuruussuhdetta voidaan kutsua internal (iBGP) tai external (eBGP) –tyyppiseksi. Samaan autonomiseen järjestelmään kuuluvien BGP-reitittimien välille muodostuva naapuruussuhde on iBGP-tyyppinen. Naapuruussuhteen tyyppi määrittää, kuinka BGP-naapureilta vastaanotettuja reittejä välitetään eteenpäin. (Teare 2010, 498, 499.)

iBGP estää reitityssilmukoiden syntymisen määrittämällä säännön, jonka perusteella iBGP-naapurilta opittua reittiä ei välitetä eteenpäin muille iBGP-naapureille. Toteutus vaatii siis naapuruussuhteet full mesh –periaatteella kaikkien iBGP-reitittimien välille. Verkon kasvaessa naapuruussuhteiden määrä kasvaa nopeasti. Skaalautuvuutta voidaan parantaa merkittävästi käyttämällä Route Reflector –reitittimiä tai konfederaatioita, jolloin full mesh –vaatimusta ei tarvitse toteuttaa. (Teare 2010, 501.)

Reittitietojen mainostus tapahtuu Update-viesteillä, joiden rakenne on esitetty kuvassa 2. Attribuutit ovat kyseistä polkua kuvaavia muuttujia, ja ne voivat olla Well Known tai Optional-tyyppisiä. (Teare 2010, 510.)

Kaikkien BGP-toteutuksien tulee tunnistaa Well Known –attribuutit, ja ne voidaan jaotella edelleen pakollisiin (Mandatory) ja harkinnanvaraisiin (Discretionary), sen mukaan, tuleeko niiden olla läsnä jokaisessa lähetettävässä Update-viestissä. (Teare 2010, 511, 512.)

Optional-attribuutit ovat valinnaisia attribuutteja, joita ei ole pakko tunnistaa kaikissa BGP-toteutuksissa. Attribuutin flags-kentässä määritetään mitä attribuutille tehdään tilanteessa, jossa BGP-toteutus ei ymmärrä attribuutin merkitystä. Transitive-attribuutti tulee lähettää edelleen muille BGP-naapureille partial-bitillä merkittynä, nontransitive-attribuuttia ei saa välittää edelleen. (Teare 2010, 511, 512.)



KUVA 2. Update-viestin rakenne (Rekhter et al. 2006.)

3.2 Multiprotocol BGP

Alkuperäinen BGP:n toteutus tuki ainoastaan IPv4-unicast tyyppisiä reittejä. Myöhemmin BGP:n toiminnallisuutta on laajennettu Multiprotocol-laajennuksilla, jotka mahdollistavat useiden erilaisten osoiteperheiden (address family) yhtäaikaisen kuljettamisen.

Multiprotocol BGP (MP-BGP) on toteutettu määrittämällä kaksi uutta optional nontransitive –tyyppistä attribuuttia, MP_REACH_NLRI ja MP_UNREACH_NLRI. Molemmat attribuutit sisältävät Address Family Identifier (AFI) ja Subsequent Address Family Identifier (SAFI) –kentät, jotka määrittävät NLRI-viestiin liittyvän protokollan ja Next-hop osoitteen toteuttamat toiminnallisuudet. Standardoimalla uusia osoiteperheitä voidaan MP-BGP:n avulla kuljettaa aina uusia protokollia. (Bates et al. 2007.)

4 MULTIPROTOCOL LABEL SWITCHING

Multiprotocol label switching (MPLS) on tekniikka, jossa liikenteenvälitys tapahtuu IP-osoitteiden sijaan paketteihin liitettyjen leimojen (label) perusteella. MPLS-verkossa paketin kohdeosoitteen perusteella tehtävä IP-reitityspäätös suoritetaan ainoastaan MPLS-verkon reunareitittimillä, runkoverkossa sijaitsevat reitittimet välittävät liikennettä vain leimoihin perustuen. Reunareitittimien välille muodostuvaa polkua, jolla liikenteenvälitys suoritetaan MPLS-leimoihin perustuen, kuvataan termillä Label Swithced Path (LSP). (Minei ja Lucek 2013, 6.)

4.1 Laitteiden roolit MPLS-verkossa

MPLS-verkkojen yhteydessä laitteita kuvataan usein termeillä Customer Edge, Provider Edge (PE) ja Provider Core (P). Yleisnimitys leimakytkentää käyttävälle reitittimelle on Label Swiching Router (LSR). (Minei ja Lucek 2013, 6.)

Customer edge –laite on yhteydessä asiakkaan omaan verkkoon ja palveluntarjoajan PE-laitteeseen. Käytettävien palveluiden mukaan CE-laite voi olla esimerkiksi kytkin tai reititin. (Minei ja Lucek 2013, 576.)

Provider edge -reititin toimii asiakkaan verkon ja palveluntarjoajan MPLS-verkon reunalla. Reunareititin määrittää asiakkaalta tulevan liikenteen Forwarding Equivilance Class (FEC) -luokan ja luo leimakytkentäisen polun toiselle PE-reitittimelle asettamalla FEC-luokkaa vastaavan leiman paketteihin. Leimausoperaatiota kutsutaan PUSH-operaatioksi. (Minei ja Lucek 2013, 6.)

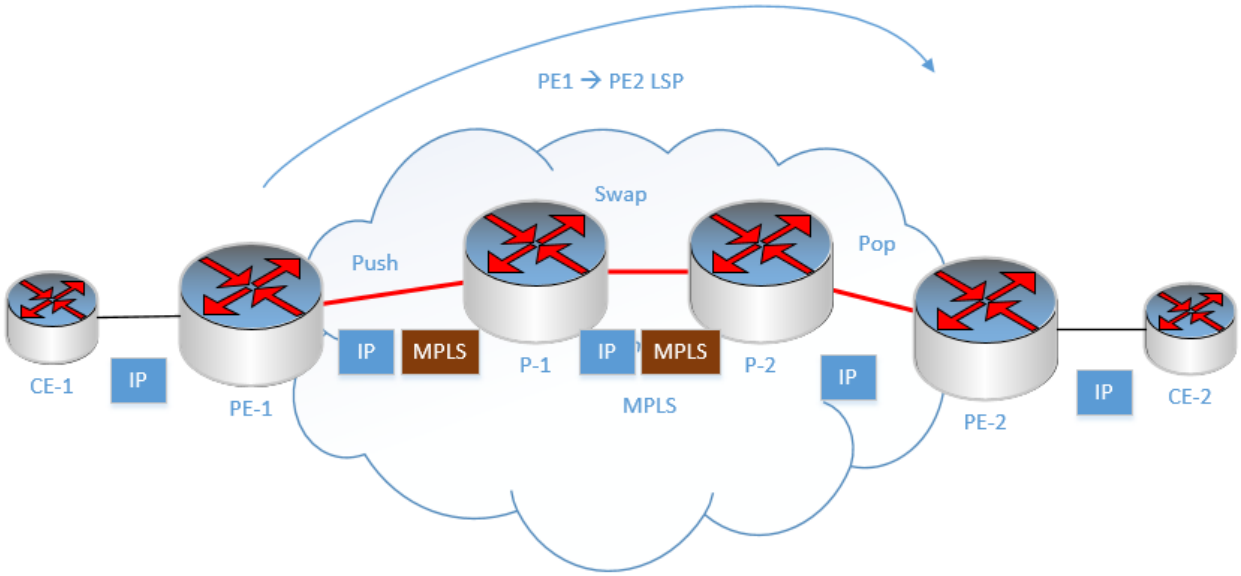
Pakettien katsotaan kuuluvan samaan FEC-luokkaan, jos ne välitetään samalle reunareitittimelle samaa LSP:tä pitkin, samalla Qos-kohtelulla. Samaan FEC-luokkaan kuuluvia paketteja voidaankin kuvata samalla leimalla. (Minei ja Lucek 2013, 6.)

Provider core (P) –reititin on yhteydessä toisiin PE– tai P-reitittimiin. P-reititin välittää liikennettä vain leimoihin perustuen, sen ei tarvitse siis pitää yllä koko internetin kattavaa BGP-taulua tai asiakkaiden VPN–reittejä. P-reititin tarkastaa saapuvan liikenteen leiman, suorittaa leimaa vastaavan operaation ja ohjaa liikenteen kohti polun seuraavaa reititintä. Tyypillisesti P-reititin voi suorittaa leimalle vaihto- (SWAP) tai poisto (POP) -operaation. (Minei ja Lucek 2013, 6, 7.)

Mikäli Provider Core –reititin on LSP:n toiseksi viimeinen reititin, se voi poistaa päällimmäisen leiman valmiiksi. Tällöin LSP:n viimeinen reititin (eli PE-reititin) voi lukea suoraan VPN-leiman tai suorittaa IP-reitityspäätöksen, eikä sen tarvitse ensin määrittää päällimmäiselle leimalle suoritettavaa operaatiota. Leimanpoisto-operaatiota kutsutaan POP-operaatioksi ja LSP:n toiseksi viimeisen reitittimen suorittamana siitä käytetään nimitystä Penultimate Hop Popping (PHP). PE-reitittimet määrittävät

FEC-luokalle suoritettavan PHP–toiminnon mainostamalla kohdeosoitetta varatulla implicit null –leimalla. (Minei ja Lucek 2013, 8.)

Kuvassa 3 on esitetty tyypillinen tilanne, jossa PE-1 -reititin asettaa liikenteelle leiman PUSH-operaatiolla, P-reititin suorittaa SWAP-operaation ja LSP:n toiseksi viimeinen reititin suorittaa PHP-toiminnon.



KUVA 3. MPLS-verkon reunareitittimien välille muodostuva leimakytkentäinen polku. P2-reititin suorittaa PHP-toiminnon poistamalla MPLS-otsikon ennen polun viimeistä reititintä

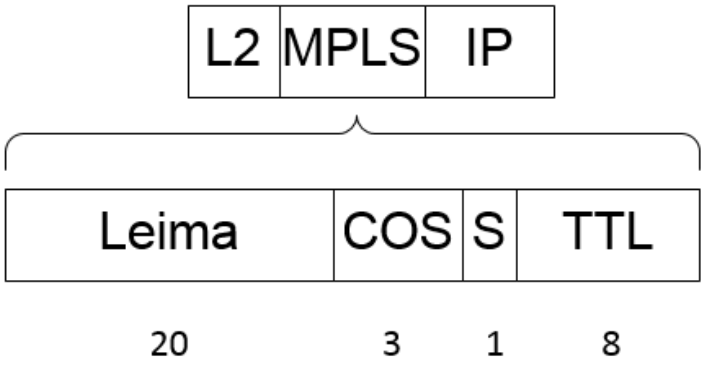
4.2 Historia

MPLS-tekniikan kehittäminen aloitettiin vuonna 1997 Internet Engineering Task Forcen (IETF) toimesta. Kehitystyön tavoitteena oli luoda Layer 2 –tason toteutuksesta riippumaton, yhtenäinen tekniikka suorituskykyiseen liikenteenvälitykseen. Uuteen standardiin haluttiin yhdistää IP-tekniikan joustavuus, ATM-tekniikan edistyneet liikenteensuunnittelumahdollisuudet ja kytkentäisen tekniikan nopeus. (Kaario 2002, 126.)

Nykyään kehittyneiden ASIC-piirien myötä nopeus ei ole MPLS-tekniikan suosion kannalta oleellinen tekijä, vaan se perustuu pitkälti tekniikan mahdollistamiin palveluihin ja edistyneisiin liikenteensuunnitteluominaisuuksiin. Siitä onkin tullut olennainen osa palveluntarjoajien liiketoimintaa. (Minei ja Lucek 2013, 4.)

4.3 MPLS-otsikon rakenne

MPLS:n kuvataan usein toimivan OSI-mallin tasojen 2 ja 3 välillä, koska MPLS-otsikko (header) sijoitetaan kuvan 4 mukaisesti siirtoyhteyskerroksen ja verkkokerroksen otsikoiden väliin.



KUVA 4. MPLS-otsikon rakenne

32-bittinen MPLS-otsikko koostuu itse leimasta (20), traffic class -biteistä (3), bottom of the stack -bitistä (1) ja Time to Live -osasta (8).

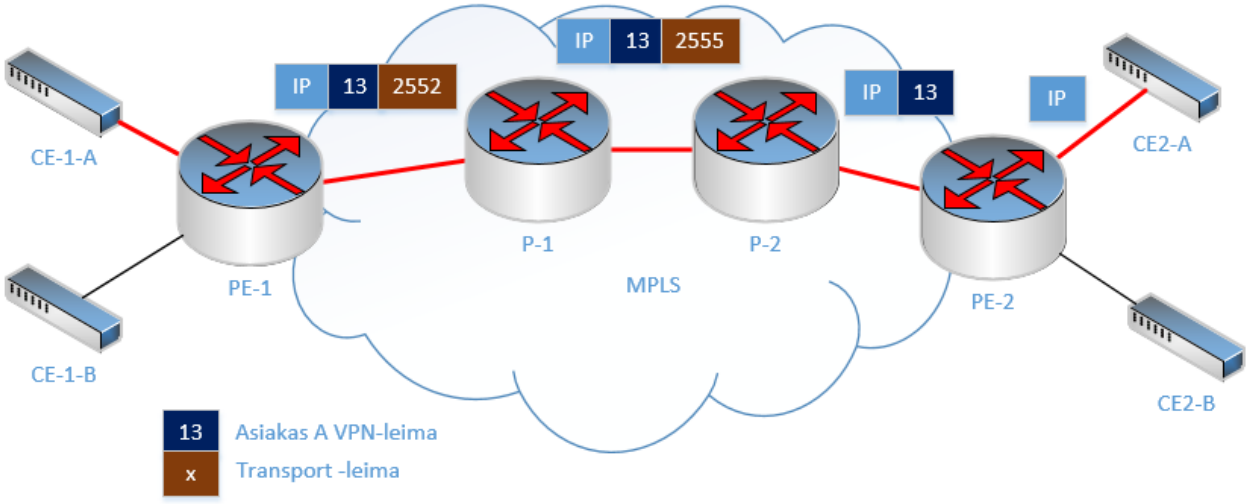
Traffic class -bittejä käytetään liikenteen luokitteluun. Luokittelulla voidaan erotella liikennettä sen tarvitsemien vaatimusten mukaan. Luokittelun avulla voidaan esimerkiksi sijoittaa viiveelle altis liikenne omaan korkeamman prioriteetin jonoon kuin tavallinen dataliikenne. (Minei ja Lucek 2013, 7.)

MPLS-leimoja voidaan pinota päällekkäin. Pinoamista käytetään esimerkiksi erilaisissa MPLS-pohjaisissa VPN-ratkaisuissa. MPLS-verkon reunareitittimet merkkaavat erillisiin VPN-instansseihin kuuluvaa liikennettä yksilöllisillä VPN-leimoilla. VPN-leiman päälle pinotaan toinen leima, jonka perusteella liikenne välitetään MPLS-verkossa. Päällimmäistä leimaa voidaan kutsua myös transport-leimaksi. (Minei ja Lucek 2013, 9.)

Bottom of the stack –bitillä ilmaistaan leiman olevan pinon alimmainen. VPN-ratkaisuissa reunareitittimet tunnistavat VPN-leiman Bottom of the stack –bitin avulla ja välittävät liikenteen VPN-leimaa vastaavaan VRF-instanssiin. (Minei ja Lucek 2013, 9.)

Kuvassa 5 on esitetty tilanne, jossa liikenne välitetään päällimmäisen transport –leiman perusteella, ja ohjataan MPLS-verkon reunalla oikeaan VRF-instanssiin VPN-leiman perusteella.

TTL-arvoa (0-255) käytetään IP-protokollan kaltaisesti silmukoiden estoon. MPLS-verkon reunareititin määrittää verkon reunalla TTL-kentän arvoksi 255, ja jokainen hyppy LSP:n varrella pienentää TTL-arvoa yhdellä. TTL-arvon laskiessa nollaan paketit pudotetaan. (Minei ja Lucek 2013, 8.)



KUVA 5. MPLS-leimojen pinoutuminen

4.4 Tietorakenteet

Reitittimet rakentavat leimatietojen perusteella Label Information Base (LIB) ja Label Forwarding Information Base (LFIB) –taulut.

Label Information Base –taulu sisältää paikallisen reitittimen asettamat leimatiedot sekä kaikki viereisiltä reitittimiltä leimanvälitysprotokollan kautta vastaanotetut leimat vastaaville reiteille. LIB –taulun ja reititystaulun perusteella muodostetaan Label Forwarding Information Base –taulu, joka sisältää paikallisen leiman ja siihen liittyvän operaation (PUSH / POP / SWAP) sekä next-hop interfacen, johon taulun riviä vastaava liikenne välitetään. (Ine Inc. 2015.)

5 LEIMANVÄLITYSPROTOKOLLAT

MPLS-verkkoon kuuluvat reitittimet vaihtavat tietoja FEC-luokille asettamistaan leimoista leimanvälitysprotokollan avulla. IETF kehitti leimanvaihtoa varten Label Distribution –protokollan (LDP). Leimanvaihtoon voidaan käytää myös Resource Reservation (RSVP) –protokollan tai BGP:n laajennuksia. RSVP on suunniteltu varaamaan verkon resursseja ennalta määriteltyjen sovellusten tarpeisiin ja sitä käytetäänkin usein liikenteensuunnitteluun. LDP on ainoa pelkästään leimanvaihtoa varten kehitetty protokolla. (Minei ja Lucek 2013, 12.)

5.1 Label Distribution Protocol

Label Distribution Protocol (LDP) on IETF:n kehittämä protokolla, jonka avulla MPLS-verkon reitittimet vaihtavat tietoja FEC-luokille asettamistaan leimoista.

5.1.1 LDP-istunto

Protokollan perustana on reitittimien välille muodostuva LDP-istunto, joka voidaan muodostaa automaattisesti suoraan kytkettyjen reitittimien välille lähettämällä Hello-viestejä kaikkien aliverkon reitittimien multicast-osoitteeseen (224.0.0.2), LDP:n käyttämään porttiin 646. Jos LDP-naapuruussuhde halutaan muodostaa muiden kuin suoraan kytkettyjen reitittimien välille, käytetään istunnon muodostamisessa kohdennettuja Hello-viestejä (targeted hello), joiden kohdeosoitteeksi asetetaan halutun naapurin osoite. (Minei ja Lucek, 12.)

Hello-pakettien lähdeosoitteena on aina liitännän ip-osoite, josta LDP-viesti lähetettiin, ja LDP-istunto pyritäänkin muodostamaan Hello-paketin lähdeosoitteen perusteella, mikäli viestistä puuttuu valinnainen Transport Address –kenttä. RFC 5036 –standardissa määritetään Hello-viestiin liitetty valinnainen Transport address –kenttä, joka määrittää osoitteen, johon varsinainen LDP-istunto tulisi muodostaa. Transport-osoite voi olla esimerkiksi loopback-liitännän osoite.

Istunnon muodostus voi jatkua, mikäli molempien reitittimien reititystaulusta löytyy reitti transport-osoitteeseen. LDP vaatii siis taustalle toimivan reitityksen, joka on voitu muodostaa esimerkiksi IGP-protokollalla. (Andersson et al. 2007.)

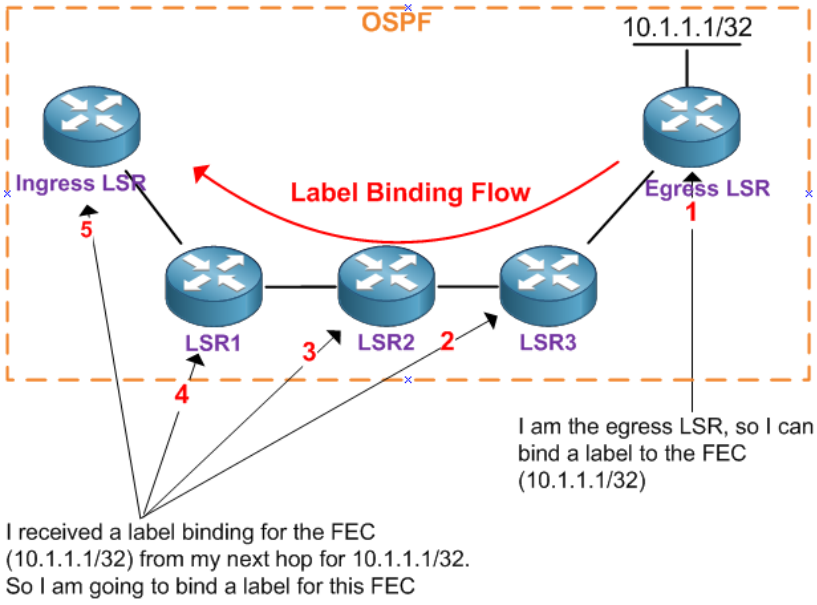
LDP-istunnon muodostamisessa suuremman transport-osoitteen omaava reititin omaksuu aktiivisen roolin, ja aloittaa TCP-yhteyden muodostamisen passiiviseen reitittimeen. Kolmivaiheisen TCP-yhteyden kättelyn jälkeen reitittimet neuvottelevat istunnon parametrit LDP-alustusviesteillä, jotka mm. sisältävät KeepAlive-viestien lähetystiheyden, protokollan version ja muita istuntoon liittyviä parametreja. Istunnon avaustoimenpiteiden jälkeen LDP-naapurit vaihtavat päivitysviesteillä tietoja FEC-luokille asettamistaan leimoista. Istuntoa pidetään yllä ajoittaisilla keepalive-viesteillä. Kuljetus-

kerroksen toteutus TCP-protokollalla mahdollistaa viestien luotettavan siirron, ja istunnon aloittamisen jälkeen voidaan päivityksiä lähettää vain muuttuneiden tietojen osalta tarvittaessa. (Andersson et al. 2007.)

5.1.2 Leimojen asettaminen

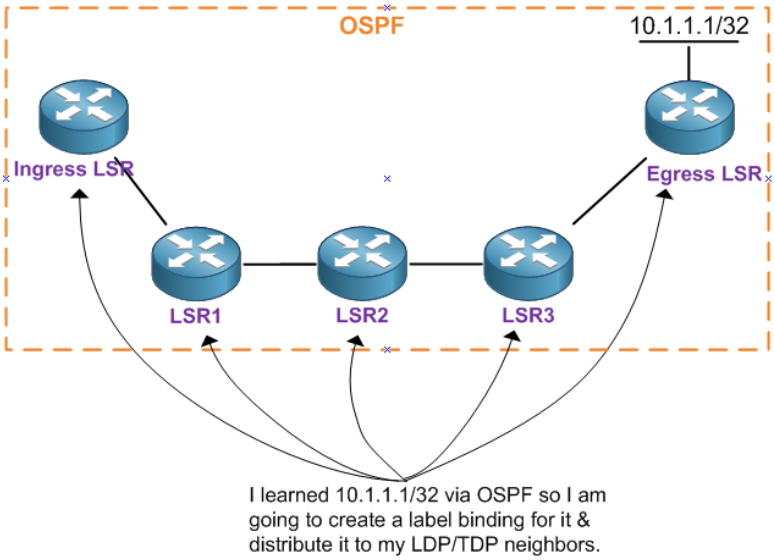
LDP-standardi määrittää leimatietojen asettamiselle kaksi tilaa, ordered control ja independent control –tilat.

Ordered control –tilassa reitittimet noudattavat sääntöä, jonka perusteella FEC-luokalle voidaan asettaa leima vain, jos kyseessä on LSP:n viimeinen reititin, tai FEC-luokalle on vastaanotettu leima liitännästä, jossa sijaitsee reititystaulun next-hop osoite kyselle FEC-luokalle. Ordered control-tilassa LSP:n reunalla olevat reitittimet asettavat FEC-luokkaa vastaavan leiman ja leimatieto etenee reunalta kohti verkon runkoa. Leimatietojen asettaminen ordered control –menetelmällä on esitetty kuvassa 6. (Minei ja Lucek 2013, 17.)



KUVA 6. Ordered control –tilassa verkon reunareitittimet määrittävät FEC-luokille asetettavat leimat (CCIE R&S Study blog 2012.)

Independent –tilassa reitittimet voivat asettaa reititystaulun reiteille leiman itsenäisesti, muilta reitittimiltä opituista leimatiedoista riippumatta. Tilannetta on havainnollistettu kuvassa 7. (Minei ja Lucek 2013, 18.)

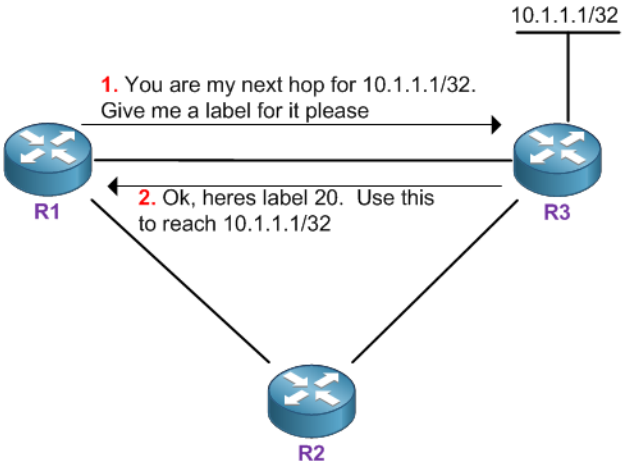


KUVA 7. Independent control (CCIE R&S Study blog 2012.)

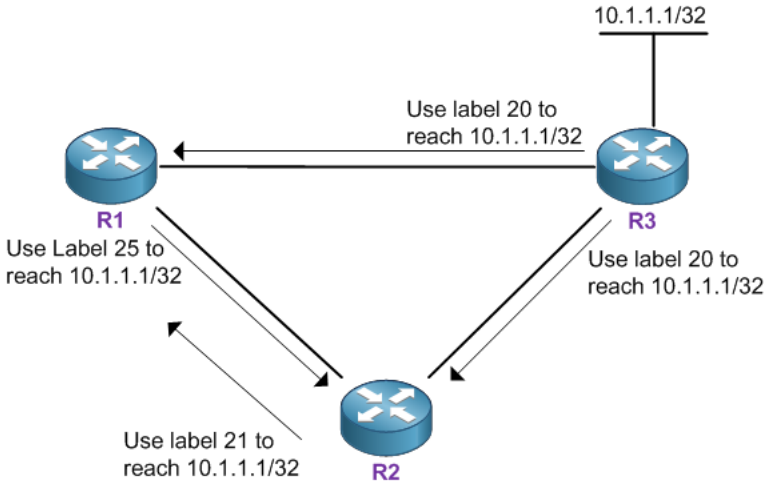
5.1.3 Leimojen mainostaminen

FEC-luokille asetettujen leimojen mainostamiselle on määritetty kaksi tapaa, unsolicited ja on demand. Kuvassa 8 esitetyssä On demand –tilassa FEC-luokkaan liitettyä leimatietoa jaetaan LDP-naapurille vasta sen pyytäessä sitä. Kuvan 9 mukaisessa Unsolicited –tilassa kaikille LDP-naapureille mainostetaan kaikkia paikallisesti asetettuja leimatietoja. Reitittimet odottavat vastaanottavansa FEC-luokkaan kuuluvaa liikennettä valitsemallaan leimalla, leimat asetetaan siis ns. alavirtaan (downstream). (Minei ja Lucek 2013, 16.)

LDP-standardi ei ota kantaa mille FEC-luokille tulisi oletuksena määrittää leima, vaan päätös jätetään vapaasti konfiguroitavaksi. Oletusasetuksissa on valmistajakohtaisia eroja. (Bhasin, 2013.)



KUVA 8. Leimanjakelu on demand -menetelmällä (CCIE R&S Study blog 2012.)



KUVA 9. Leimanjakelu unsolicited -menetelmällä (CCIE R&S Study blog 2012.)

5.1.4 Leimatietojen säilytys (retention)

Standardi määrittää LDP-naapureilta vastaanotetuille leimatiedoille kaksi erilaista säilytysmahdollisuutta (engl. retention), liberal ja conservative. Conservative retention –tilassa säilytetään vain liikenteenvälitykseen käytettävät leimatiedot. Liberal label retention –tilassa sälytetään kaikki viereisiltä reitittimiltä vastaanotetut leimatiedot, vaikka niitä ei käytettäisikään liikenteenvälitykseen. Liberal label retention –tila on hyödyksi tilanteessa, jossa reititys muuttuu. Tällöin Label information Base –taulussa voi olla valmiiksi uutta reittiä vastaava leima, jota ei aikaisemmin käytetty liikenteenvälitykseen esimerkiksi IGP:n huonomman metriikan takia. Conservative –tilassa uusi käytettävä leima täytyy vastaanottaa naapurilta ennen liikenteenvälityksen jatkumista. (Minei ja Lucek 2013, 21.)

6 VIRTUAL ROUTING AND FORWARDING

Virtual Routing and Forwarding (VRF) on tekniikka, joka mahdollistaa useiden erillisten reititystaulujen ylläpitämisen samassa reitittimessä. Palveluntarjoaja voi esimerkiksi määrittää reunareitittimen jokaiselle asiakkaalle oman VRF-instanssin. Ratkaisu eristää asiakkaiden verkot omiin reititystauluihinsa ja mahdollistaa myös päällekkäisten osoitealueiden käyttämisen eri asiakkailla. Liikennöinti VRF-instanssien välillä ei ole oletuksena mahdollista, vaan se vaatii aina erillistä konfigurointia. Oletusreitiystaulua (joka ei kuulu yhteenkään VRF-instanssiin) kutsutaan globaaliksi reititystauluksi, asiakkaiden ollessa omissa VRF-instansseissaan globaalia reititystaulua voidaan käyttää liikennöintiin palveluntarjoajan verkossa. (Minei ja Lucek 2013, 206.)

VRF-tekniikka on keskeisessä roolissa VPN-palveluiden toteutuksessa. VPN-palveluita toteutettaessa erillisiin VRF-instansseihin kuuluvat reitit yksilöidään Route Distinguisher –arvolla, joka on osa Network Layer Reachability Information –viestiä. (Minei ja Lucek 2013, 208.)

Route distinguisher –arvo koostuu kahdeksasta tavusta, ensimmäiset kaksi tavua määrittävät esitystavan ja seuraavat arvot sisältävät esitystavasta riippuen ASN-numeron tai IP-osoitteen. Route distinguisherin tehtävä on vain tehdä VPN-reiteistä yksilöllisiä. (Rosen ja Rekhter 2006.)

Route target –arvo on update-viestiin liitetty extended community -attribuutti, jonka perusteella reittitietoja tuodaan ja viedään VRF-instanssien välillä. Kun VRF-instanssiin kuuluvaa reittiä mainostetaan muille BGP-reitittimille, lisätään viestiin määritetty export Route Target -arvo. Update-viestin saapuessa PE-reitittimelle, se tutkii Route Target -arvon, ja mikäli kyseinen arvo on määritetty VRF-instanssin Import Targetiksi, viedään reittitieto kyseisen instanssin reititystauluun. Import –ja export target- arvojen konfiguroinnilla voidaan vaikuttaa muodostettavan VPN-instanssin topologiaan, tai tarvittaessa jakaa reittitietoja useampien VPN-instanssien kesken. (Rosen ja Rekhter 2006.)

7 MPLS-POHJAISET VPN-PALVELUT

7.1 Layer 2 VPN

Layer 2 VPN -ratkaisussa luodaan palveluntarjoajan MPLS-verkon kautta Layer 2 –tason yhteys asiakkaan CE-laitteiden välille. Palveluntarjoaja käyttää samaa MPLS-verkkoa useiden eri asiakkaiden palveluiden tarjoamiseen. Asiakkaiden liikenne pidetään erillään asiakaskohtaisten VRF-instanssien ja VPN-tunnisteiden avulla. Layer 2 VPN –palveluita käytettäessä asiakas vastaa itse reitityksen rakentamisesta VPN-ratkaisun päälle, palveluntarjoaja tarjoaa vain Layer 2 –siirtoyhteyden. (Minei ja Lucek 2013, 344.)

MPLS-verkossa VPN-tunniste on käytännössä MPLS-leima, jonka perusteella PE-reitittimet tunnistavat leimaan liitetyn VPN-instanssin ja ohjaavat liikenteen oikeaan VRF-instanssiin. PE–reititin sijoittaa VPN–leiman leimapinon alimmaiseksi, ja pinoaa sen päälle transport–leiman, jonka perusteella liikenne välitetään MPLS-verkon läpi toiselle PE-reitittimelle. (Rosen ja Rekhter 2006.)

Toistaiseksi käytetyin tekniikka MPLS-pohjaisten Layer2 VPN -palveluiden toteuttamiseen on ollut RFC4761 ja RFC4762 –standardiesityksissä määritetty VPLS.

VPLS:n avulla voidaan toteuttaa point-to-multipoint –tyylinen Layer2 VPN, jolloin kaikki samaan VPN-instanssiin kuuluvat CE-laitteet näyttävät olevan samassa Layer2 –domainissa. Palveluntarjoajan PE-reitittimet pitävät kytkimen tavoin MAC-osoitetaulukkoa VPN-instanssiin kuuluvista MAC-osoitteista. (Minei ja Lucek 2013, 375.)

VPLS-tekniikan toiminta perustuu PE-reitittimien välille muodostettaviin loogisiin pseudowire –yhteyksiin, jotka muodostetaan full mesh –periaatteella jokaista VPN-instanssia varten. Full mesh –verkon muodostamiseen tarvittavien linkkien määrä on $n * \frac{n-1}{2}$, jossa n on verkkoon kuuluvien reitittimien määrä. Tilannetta on havainnollistettu kuvassa 10, jossa kuuden toimipisteen välisen VPLS –verkon muodostamiseksi tarvitaan 15 pseudowire-linkkiä.

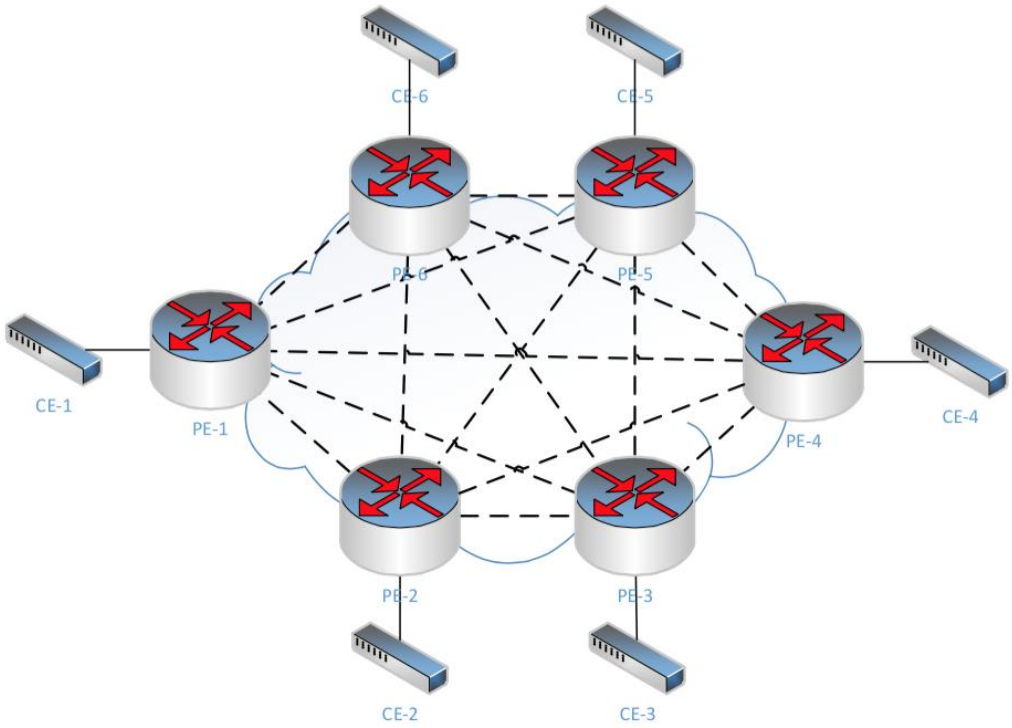
PE-reitittimet välittävät asiakkaalta saapuvaa liikennettä vertaamalla kehyksien kohde-MAC –osoitetta pitämiinsä MAC-osoitetauluihin, joissa on MAC-osoitetta vastaavan liitännän nimi (paikallisen liitännän osalta), tai MAC-osoitteen sijaitessa toisella PE-reitittimellä, pseudowire-linkin tunniste. Mikäli osoitetta ei löydy MAC-taulusta, lähetetään liikenne kytkimen tavoin kaikille muille samaan VPN-instanssiin kuuluville liitännöille. Verkon toisessa päässä olevat PE-laitteet tunnistavat VPLS-instanssin pseudowire–tunnisteen avulla ja tarvittaessa lähettävät liikenteen edelleen kohti paikallisia CE-laitteita. (Lasserre ja Kompella 2007.)

Silmukoiden esto on toteutettu VPLS:ssä noudattamalla Split Horizon –sääntöä, jonka mukaan pseudowire-linkin kautta vastaanotettua liikennettä ei koskaan välitetä muille VPLS-instanssin pseudowireille. (Lasserre ja Kompella 2007.)

Olennainen ero VPLS:n ja myöhemmin esiteltävän Ethernet VPN:n välillä on tapa, jolla MAC-osoitteiden oppiminen on toteutettu PE-laitteiden välillä. VPLS muodostaa MAC-osoitetaulukot data-kerroksella tapahtuvan liikenteen tulvittamisen perusteella. Ethernet VPN käyttää MAC-osoitteiden oppimiseen MP-BGP:llä toteutettua kontrollikerrosta. (Sajassi et al. 2015.)

RFC4761 määrittää VPLS:n MP-BGP-pohjaisen autodiscovery-ominaisuuden, jolloin samaan VPN-instanssiin kuuluvat PE-reitittimet tunnistavat toisensa MP-BGP:n avulla ja neuvottelevat topologiaan tarvittavat pseudowire-linkit automaattisesti. (Kompella ja Rekhter 2007.)

PE-reitittimen liittäminen tai poistaminen VPN-instanssiin ei vaadi konfigurointeja muille samaan instanssiin kuuluville reitittimille. VPLS-instanssiin kuuluvien PE-reitittimien määrän kasvaessa pseudowire-linkkien määrä kuitenkin alkaa aiheuttaa skaalautumisongelmia. (Ine Inc. 2010.)



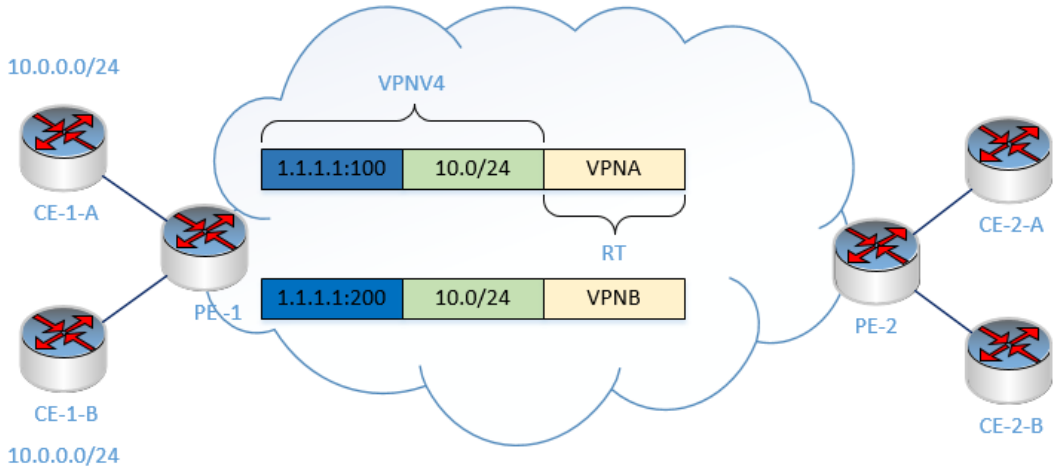
KUVA 10. VPLS vaatii full mesh –periaatteella toteutetut pseudowire-yhteydet samaan instanssiin osallistuvien PE-reitittimien välille

7.2 Layer 3 VPN

Layer 3 VPN –palveluissa CE-reititin muodostaa naapuruussuhteen palveluntarjoajan PE-reitittimen kanssa ja mainostaa paikallisia reittejään reititysprotokollan välityksellä PE-reitittimelle. Asiakkaan reitit kuljetetaan kontrollikerroksella MP-BGP:n avulla palveluntarjoajan MPLS-verkon läpi muille samaan VPN-instanssiin kuuluville PE-reitittimille, jotka mainostavat reittejä edelleen paikallisille CE-reitittimille. PE-reitittimet hoitavat asiakkaan toimipisteiden välisen liikenteen reitityksen MPLS-verkon yli. (Minei ja Lucek 2013, 200.)

Asiakaskohtaiset reitit eristetään toisistaan käyttämällä asiakaskohtaisia VRF-instansseja. Ratkaisu mahdollistaa päällekkäisten osoitealueiden käyttämisen eri asiakkailla. Palveluntarjoajan verkossa kaikkien VPN-instanssien reittitiedot kuljetetaan samassa BGP-instanssissa. Route distinguisher -arvolla yksilöityjä IPV4-reittejä kutsutaan VPNV4-reiteiksi. Muuntaessaan asiakkaalta saapuvia reittejä VPNV4-reiteiksi PE-reitittimet liittävät community-attribuuttina myös yhden tai useamman route target (RT) –arvon, joilla hallitaan reittitietojen tuomista muille PE-laitteille. Import ja export– arvoja muuttamalla voidaan vaikuttaa muodostuvan VPN:n topologiaan. (Minei ja Lucek 2013, 206, 207.)

Kuvassa 11 on esitetty tilanne, jossa PE-1 reitittimeen on kytketty kaksi asiakasta, jotka käyttävät samaa osoiteavaruutta omissa verkoissaan. PE-reititin muodostaa VPNV4-reitin liittämällä prefikseihin reitin yksilöivän route distinguisher –arvon.



KUVA 11. VPNV4-reitti koostuu route distinguisherista ja prefiksistä. Route target liitetään extended community-arvona

8 ETHERNET VPN

Ethernet VPN (EVPN) on uusi L2VPN-standardi, joka julkaistiin helmikuussa 2015. Ethernet VPN:n kehitystyössä ovat olleet mukana mm. IETF, Juniper Networks, Cisco, AT&T ja Verizon Wireless. (Sajassi et al 2015.)

Layer2 VPN –palveluiden kysyntä on kasvanut mm. Data Center Interconnect –ratkaisujen myötä. Virtualisointitekniikat asettavat MAC-osoitteiden liikkuvuudelle ja toteutuksen skaalautuvuudelle uusia vaatimuksia, joihin VPLS-tekniikalla ei pystytä vastaamaan. Kasvaneet liikennemäärät vaativat tehokkaampia keinoja kuormantasaukseen ja nopeaan virhetilanteista toipumiseen. (Sajassi et al. 2014.)

VPLS:n vaatimus pseudowire-linkkien muodostamiseen full mesh –periaatteella ja datakerroksella tapahtuva MAC-osoitteiden oppiminen flood and learn –tyyliin kuormittaa huomattavasti palveluntarjoajan reitittimien resursseja.

Ethernet VPN pyrkii vastaamaan kasvaneisiin vaatimuksiin siirtämällä PE-reitittimien välisen MAC-osoitteiden oppimisen kontrollikerroksen tehtäväksi ja esittelemällä joukon uusia ominaisuuksia, jotka mahdollistavat edistyneen kuormantasauksen sekä L2 ja L3- palveluiden tarjoamisen samasta liitännästä. (Hankins, 2014.)

Uuden standardin tavoitteiksi asetettiin mm. VPLS:n kaltainen provisionnin helppous (mm. autodiscovery-ominaisuus), Active – Active –multihoming- mahdollisuus ja multicast-liikenteen optimaalisempi välitys. Lisäksi standardin vaatimuksiin määritettin nopea, MAC-osoitteiden määrästä riippumaton konvergenssiaika vikatilanteissa. Uuden toteutustavan tuli myös minimoida tarpeeton BUM (Broadcast, Unkown Unicast, Multicast) –liikenteen lähettäminen VPN:n ylitse. (Sajassi et al. 2014.)

8.1 Toteutus

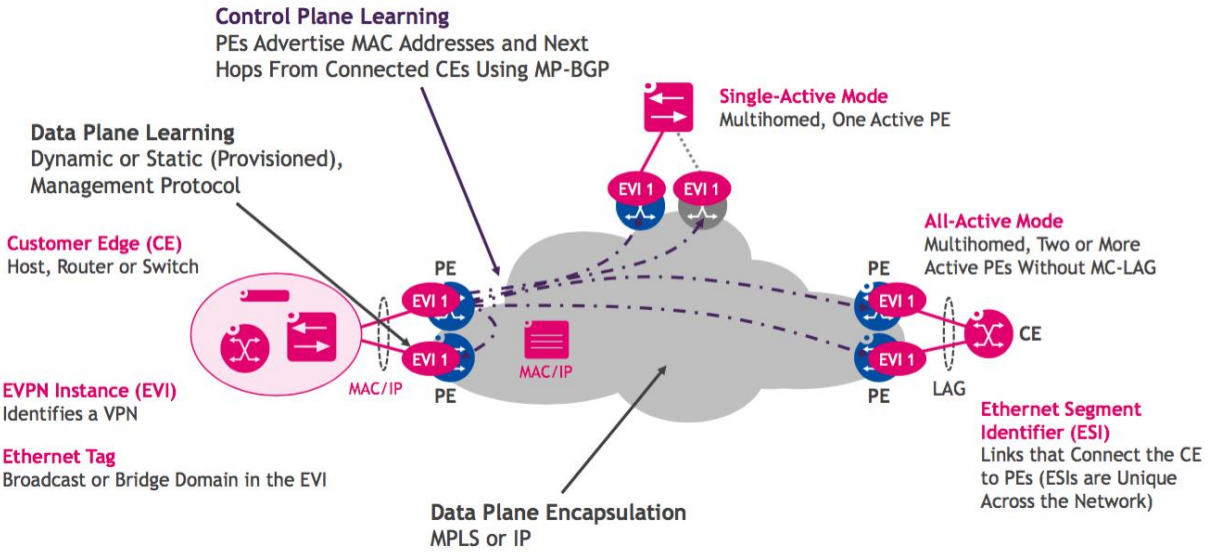
EVPN –toteutuksessa PE-reitittimet mainostavat saavutettavissa olevia MAC-osoitteita MP-BGP:n avulla. Reittitietojen kontrollointi on mahdollista BGP:n perinteisillä työkaluilla. (Sajassi et al. 2015)

8.1.1 EVPN Instance

EVPN Instance (EVI) tarkoittaa PE-reitittimillä pidettävää asiakaskohtaista VPN-instanssia, jolle on määritetty instanssikohtainen Route Distinguisher –arvo ja yksi tai useampia Route target –arvoja. (Sajassi et al. 2015.)

8.1.2 Multihoming

Multihoming toteutetaan EVPN-ratkaisuissa yhdistämällä CE-laite kahteen tai useampaan PE-reitittimeen Link Aggregation Group (LAG) –liitännän avulla. LAG-liitännän muodostama alue yksilöidään määrittämällä sille verkon laajuinen tunniste, Ethernet Segment Identifier (ESI). Multihoming voidaan toteuttaa active – active –mallilla, jolloin kaikki samaan Ethernet-segmenttiin kytketyt PE-reitittimet voivat väittää liikennettä samanaikaisesti. Tilannetta on havainnollistettu kuvassa 12. (Sajassi et al. 2015.)



KUVA 12. EVPN-standardissa määritettyjen termien esitys (Hankins 2014.)

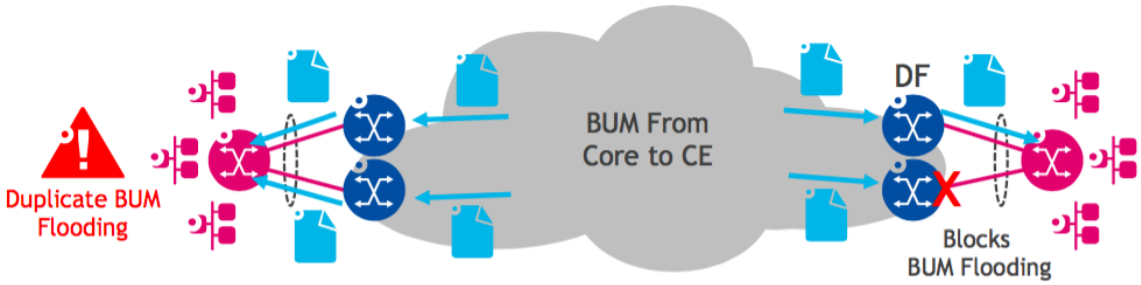
8.1.3 Aliasing

Aliasing tarkoittaa sääntöä, jonka perusteella samaan Ethernet-segmenttiin kuuluvat MAC-osoitteet voi tavoittaa kaikista saman segmentin PE-reitittimistä, vaikka MAC-osoitetta olisi mainostanut ainoastaan yksi segmentin PE-reititin. Toiminto mahdollistaa Ethernet-segmenttiä kohti suuntautuvan liikenteen kuormantasauksen usean PE-reitittimen välille. Sääntöä tarvitaan, koska osa liikenteestä voi kulkea LAG-ryhmästä huolimatta vain yhtä linkkiä pitkin. (Sajassi et al. 2015.)

8.1.4 Broadcast, unkown unicast ja multicast –liikenteenvälityksen optimointi

Kuvan 13 kaltaisessa multihoming-tilanteessa Ethernet-segmenttiä kohti saapuvan BUM-liikenteen tarpeeton monistaminen estetään valitsemalla segmenttiin kuuluvista PE-reitittimistä designated forwarder, joka välittää liikenteen kohti segmenttiä. Muut segmenttiin kytketyt PE-reitittimet eivät välitä BUM-liikennettä kohti segmenttiä.

Samasta Ethernet-segmentistä lähtöisin olevan liikenteen kiertäminen takaisin on estetty noudattamalla split horizon –sääntöä. (Sajassi et al. 2015.)



KUVA 13. Vain Designated forwarder –reititin välittää liikennettä kohti Ethernet-segmenttiä (HANKINS 2014.)

8.1.5 MAC Mobility

MAC-reittimainokseen extended community –arvona liitetty sekvenssinumero mahdollistaa eri VPN-toimipisteiden välillä siirtyvän MAC-osoitteen nopean tunnistamisen. PE-reititin lähettää MAC-osoitetta koskevan withdrawal-viestin, kun se näkee paikallista MAC-osoitetta vastaavan reittimainoksen korkeammalla sekvenssinumerolla. Virhetilanteita varten standardissa määritetään konfiguroitavissa oleva ajastin, joka sallii oletuksena viisi MAC-osoitteen siirymää 180 sekunnin sisällä. Mikäli ajastimella määritetty aika ylittyy, jätetään sillä hetkellä korkeimman sekvenssinumeron omaava reitti käyttöön ja seuraavat saman MAC-osoitteen reittimainokset jätetään huomiotta. (Sajassi et al. 2015.)

8.1.6 Mass withdrawal

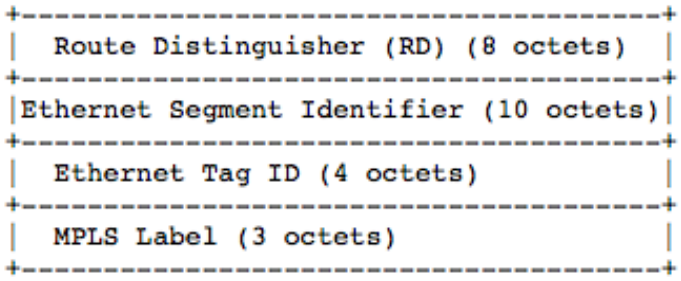
Mass withdrawal -ominaisuus mahdollistaa nopean virhetilanteista toipumisen, kun yhdellä reittimainoksella voidaan poistaa kaikki kyseisen PE-reitittimen takana olevat MAC-osoitteet liikenteenvälitystaulukoista. PE–CE linkin virhetilanteessa PE-reititin lähettää koko Ethernet-segmenttiä koskevan withdraw–viestin ja muut PE-reitittimet poistavat kaikki vikaantuneen linkin takana olevat MAC-osoitteet liikenteenvälitystauluistaan. (Sajassi et al. 2015.)

8.2 EVPN-reittityypit

RFC 7432 määrittää uuden MP-BGP-reittityypin, jonka Address Family Identifier –arvo on 25 (L2VPN) ja Subsequent Address Family Identifier –arvo on 70 (EVPN). EVPN NLRI –viesti koostuu yhden oktetin pituisista tyyppi- ja pituus- kentistä sekä reittityypin mukaisista vaihtuvista osioista. (Sajassi et al. 2015.)

8.2.1 Ethernet autodiscovery

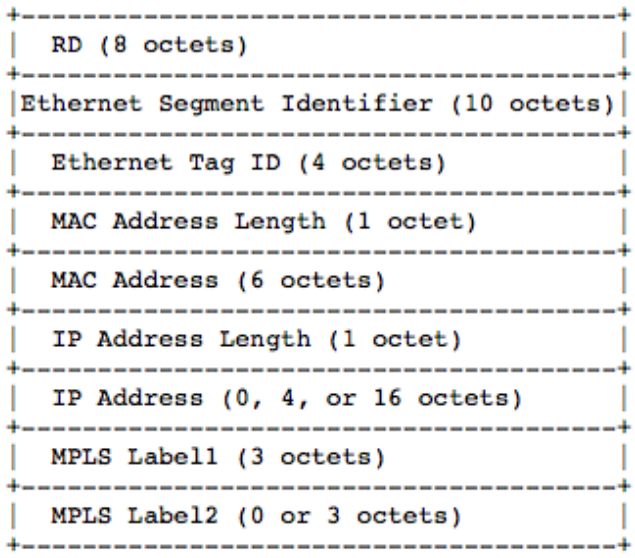
Ethernet autodiscovery –reittityyppiä käytetään aliasing- ja mass withdraw -ominaisuuksiin sekä split horizon –säännön toteuttamiseen. Autodiscovery-reitit voivat olla instanssikohtaisia (Ethernet A-D per EVI) tai segmenttikohtaisia (A-D per ESI). Reittityypin rakenne on esitetty kuvassa 14. (Sajassi et al. 2015.)



KUVA 14. Ethernet autodiscovery-reitin rakenne (Sajassi et al. 2015.)

8.2.2 MAC / IP Advertisement

Kuvassa 15 havainnollistettujen MAC / IP Advertisement –reittien avulla mainostetaan saavutettavissa olevia MAC-osoitteita. IP-osoitekentän sisällyttäminen MAC / IP Advertisement –reittiin mahdollistaa L2- ja L3 -palveluiden tarjoamisen samasta liitännästä. Reittiin kuuluvat MPLS-leimakentät välitetään attribuuttina. Ratkaisu mahdollistaa datakerroksen toteuttamisen myös muulla kuin MPLS-tekniikalla. (Sajassi et al. 2015.)



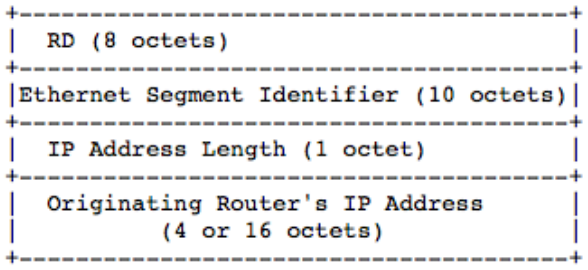
KUVA 15. MAC / IP Advertisement –reitin rakenne (Sajassi, et al, 2015.)

8.2.3 Inclusive multicast route

Inclusive multicast –reittityyppiä käytetään silloin kun liikenteenvälitykseen PE-reitittimien välillä käytetään Point – to multipoint tai multipoint –to multipoint tyylisiä LSP-polkuja. (Sajassi et al. 2015.)

8.2.4 Ethernet segment route

Ethernet segment –reittityyppiä käytetään multihoming-tapauksissa samaan segmenttiin kytkettyjen PE-reitittimien tunnistamiseen ja designated forwarder –reitittimen valintaan. Reittiin kuuluva Ethernet Segment Identifier –arvo voidaan määrittää konfiguraatiossa tai generoida automaattisesti CE-PE linkin LACP- tai BPDU-kehyksistä. Reittityypin rakenne on havainnollistettu kuvassa 16. (Sajassi et al. 2015.)



KUVA 16. Ethernet segment -reitin rakenne (Sajassi et al. 2015.)

8.3 Service interface –tyypit

EVPN voidaan toteuttaa useammalla erilaisella liitäntätyypillä (service interface), jotka määrittävät kuinka CE-laitteelta saapuvat VLAN ID:t määritetään kuulumaan EVPN-instansseihin. (Sajassi et al. 2015.)

8.3.1 VLAN Based Service Interface

VLAN-pohjaisessa EVPN-instanssissa (VLAN Based Service Interface) jokainen VLAN kuuluu omaan EVPN-instanssiinsa. VLAN ID –arvojen uudelleenkirjoitus (translation) on mahdollista PE-laitteiden välillä ja instansseissa voi olla päällekkäisiä MAC-osoitteita. (Sajassi et al. 2015.)

8.3.2 VLAN Bundle Service Interface

VLAN Bundle –tyyppinen liitäntä mahdollistaa useiden VLANien kuljettamisen samassa VPN-instanssissa. Instanssiin kuuluvat VLANit ovat samassa bridge domainissa, joten päällekkäisten MAC-osoitteiden käyttäminen tai VLAN-ID arvojen uudelleenkirjoitus ei ole mahdollista. (Sajassi et al. 2015.)

8.3.3 VLAN Aware Bundle Service Interface

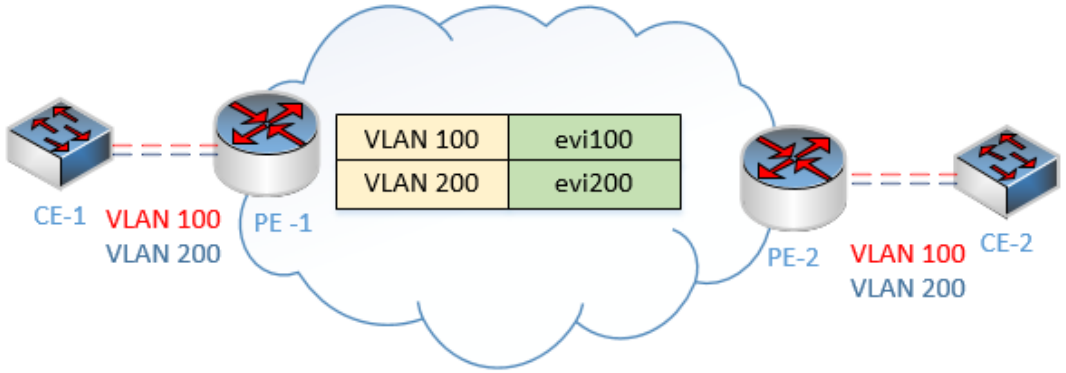
VLAN Aware Bundle –liitännässä VLANit kuuluvat samaan instanssiin, mutta jokaiselle VLANille luodaan erillinen bridge domain, se mahdollistaa VLAN ID –arvojen uudelleenkirjoituksen ja päällekkäiset MAC –osoitteet VLANien välillä. (Sajassi et al. 2015.)

8.4 EVPN:n konfigurointi

Savonian tietoverkkolaboratoriossa on käytettävissä kaksi Juniper Networksin MX-sarjan reititintä, joilla EVPN-konfiguraatiota on mahdollista testata. Konfiguroidaan VLAN-pohjainen EVPN-instanssi ja VLAN Aware Bundle –tyyppinen EVPN-instanssi.

8.4.1 VLAN-pohjainen EVPN-instanssi

VLAN-pohjaisessa EVPN-instanssissa VLAN-ID –arvot liitetään 1:1 –menetelmällä omiin EVPN-instansseihinsa. Konfiguroidaan kuvan 17 kaltainen verkko.



KUVA 17. Testausverkon rakenne

Taustalle vaaditaan toimiva MPLS-verkko ja mahdollisuus BGP-istunnon muodostamiseen PE-reitittimien välillä. Testausverkossa IGP-protokollana käytettiin OSPF:ää ja leimanjakeluun LDP-protokollaa. Lisäksi hyödynnettiin Juniperin Logical Systems –tekniikkaa, jonka avulla yhteen fyysiseen reitittimeen voidaan konfiguroida useita loogisia reitittimiä. Koko testausverkon konfiguraatio on esitetty liitteessä 1.

EVPN:n kannalta oleellista on ottaa käyttöön MP-BGP -osoiteperhe ja konfiguroida EVPN-instanssi jokaista kuljetettavaa VLANia varten.

8.4.2 EVPN-osoiteperheen konfigurointi

EVPN-osoiteperhe otetaan Junosissa käyttöön konfiguroimalla *family evpn signaling* iBGP –konfiguraation alle.

```
root@PE1# show protocols bgp group internal
type internal;
local-address 1.1.1.1;
family evpn {
    signaling;
}
neighbor 2.2.2.2;
```

8.4.3 PE-CE-liitännän konfigurointi

Konfiguroidaan CE-laitteen suuntainen liitäntä *ge0/0/4* käytetyillä VLAN ID –arvoilla ja oikealla enkapsuloinnilla.

```
root@PE1# show interfaces ge0/0/4
flexible-vlan-tagging;
encapsulation flexible-ethernet-services;
unit 100 {
    encapsulation vlan-bridge;
    vlan-id 100;
}
unit 200 {
    encapsulation vlan-bridge;
    vlan-id 200;
}
```

8.4.4 Reititysinstanssien konfigurointi

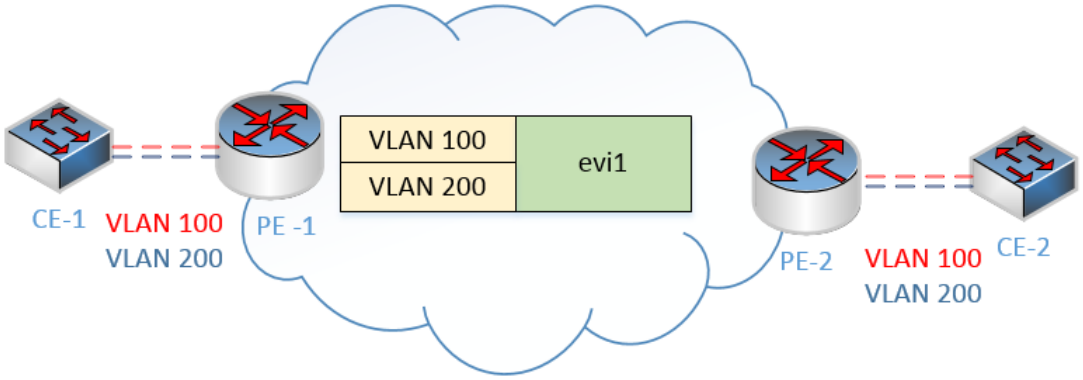
Seuraavaksi konfiguroidaan VLANeja vastaavat EVPN-instanssit evpn100 ja evpn200. Instansseihin määritetään käytetty VLAN ID ja liitäntä, sekä VPN-reitit yksilöivä route-distinguisher ja instanssikohtainen VRF-target –arvo. Esimerkissä määritetään import –ja export arvot kerralla *target:* -avainsanalla.

```
root@PE1# show routing-instances
evpn100 {
    instance-type evpn;
    vlan-id 100;
    interface ge-0/0/4.100;
    route-distinguisher 1.1.1.1:100;
    vrf-target target:100:100;
    protocols {
        evpn;
    }
}
evpn200 {
    instance-type evpn;
    vlan-id 200;
    interface ge-0/0/4.200;
    route-distinguisher 1.1.1.1:200;
    vrf-target target:200:200;
    protocols {
        evpn;
    }
}
```

VLAN-pohjaisten instanssien määritys on nyt valmis, ja konfiguraatiota voidaan testata tuottamalla liikennettä CE-laitteiden välille.

8.5 VLAN Aware Bundle Service Interface

VLAN Aware Bundle -tyyppisen instanssin konfiguraatiossa CE-laitteen suuntainen liitäntä konfiguroidaan trunk-tyyppiseksi. Kaikilla VLAN Aware Bundle interfacen VLANeilla on oma bridge domaininsa. Konfiguroidaan kuvan 18 mukainen evi1-instanssi ja liitetään siihen VLAN-ID:t 100 ja 200.



KUVA 18. VLAN Aware Bundle Interface –tyypissä VLAN-ID:t kuuluvat samaan instanssiin.

8.5.1 PE – CE–liitännän konfigurointi

Konfiguroidaan PE–CE-liitäntä trunk-tyyppiseksi ja määritetään siihen VLAN-ID:t 100 ja 200.

```
root@PE1# show interfaces ge-0/0/4
flexible-vlan-tagging;
encapsulation flexible-ethernet-services;
unit 0 {
    family bridge {
        interface-mode trunk;
        vlan-id-list [ 100 200 ];
    }
}
```

8.5.2 Reititysinstanssin ja bridge domainien konfigurointi

VLAN Aware Bundle –tyyppisessä konfiguraatiossa samaan instanssiin voidaan määrittää useita VLANeja ja jokaiselle VLANille muodostetaan lisäksi oma bridge domaininsa. Reititysinstanssi konfiguroidaan *virtual-switch*–tyyppiseksi, ja määritetään siihen kuuluvat bridge domainit ja EVPN-protokollaan kuuluvat VLAN ID-arvot.

```
root@PE1# show routing-instances evpn1
instance-type virtual-switch;
interface ge-0/0/4.0;
route-distinguisher 1.1.1.1:100;
vrf-target target:100:100;
protocols {
    evpn {
        extended-vlan-list [ 100 200 ];
    }
}
```

```
bridge-domains {
    vl100 {
        domain-type bridge;
        vlan-id 100;
    }
    vl200 {
        domain-type bridge;
        vlan-id 200;
    }
}
```

Instanssin ja liitäntöjen konfiguraatio on nyt valmis, ja sitä voidaan testata tuottamalla liikennettä CE-laitteiden välille.

8.5.3 Show-komennot

Reititysinstanssien tilaa voidaan tarkastella esimerkiksi kuvan 19 mukaisella *show evpn instance*-komennolla, jonka tulosteessa ilmoitetaan instanssiin kuuluvien MAC-osoitteiden lukumäärä ja niiden sijainti sekä instanssiin kuuluvat naapurit ja vastaanotettujen reittityyppien lukumäärä. Standardin mukaisesti single-homed -tyyppinen liitäntä saa ESI-arvoksi 0.

```
root@PE1> show evpn instance evpn100 extensive
Instance: evpn100
  Route Distinguisher: 1.1.1.1:100
  VLAN ID: 100
  Per-instance MAC route label: 299776
  MAC database status               Local  Remote
    Total MAC addresses:               1       1
    Default gateway MAC addresses:     0       0
  Number of local interfaces: 1 (1 up)
    Interface name  ESI                            Mode             Status
    ge-0/0/4.100    00:00:00:00:00:00:00:00:00:00  single-homed     Up
  Number of IRB interfaces: 0 (0 up)
  Number of bridge domains: 1
    VLAN ID  Intfs / up    Mode            MAC sync  IM route label
    100         1   1      Extended        Enabled   299888
  Number of neighbors: 1
    2.2.2.2
      Received routes
        MAC address advertisement:             1
        MAC+IP address advertisement:          0
        Inclusive multicast:                   1
        Ethernet auto-discovery:               0
  Number of ethernet segments: 0

root@PE1>
```

KUVA 19. EVPN100-instanssin tarkastelu

VLAN-pohjaisessa toteutuksessa jokaisella instanssilla on oma MAC-VRF –taulunsa, tässä tapauksessa *evpn100.evpn.0* ja *evpn200.evpn.0*. Taulujen sisältöä tarkastellaan *show route* –komennolla. Kuvassa 20 nähdään, kuinka PE1-reititin on asentanut MAC-reitin PE2-reitittimen takana sijaitsevalle osoitteelle *02:ce:22:22:22:22*.

```
root@PE1> show route table evpn100.evpn.0

evpn100.evpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2:1.1.1.1:100::100::02:ce:11:11:11:11/304
                   *[EVPN/170] 00:01:19
                      Indirect
2:2.2.2.2:100::100::02:ce:22:22:22:22/304
                   *[BGP/170] 00:01:11, localpref 100, from 2.2.2.2
                      AS path: I, validation-state: unverified
                    > to 10.0.0.2 via ge-0/0/3.0
3:1.1.1.1:100::100::1.1.1.1/304
                   *[EVPN/170] 00:01:23
                      Indirect
3:2.2.2.2:100::100::2.2.2.2/304
                   *[BGP/170] 00:01:11, localpref 100, from 2.2.2.2
                      AS path: I, validation-state: unverified
                    > to 10.0.0.2 via ge-0/0/3.0

root@PE1>
```

KUVA 20. Instanssikohtaisen reititystaulun tarkastelu

9 YHTEENTEVO

Opinnäytetyön tavoitteena oli esitellä EVPN-standardi ja sen taustalla olevat tekniikat. Uuden standardin esittelyn edellytys on ymmärtää VPN-palveluiden keskeisimmät rakennuspalikat ja datakerroksen ja kontrollikerroksen erilliset roolit verkkolaitteiden toiminnassa.

Työssä käsitellyt aiheet olivat suurelta osin uusia, mutta opinnoissa saatu pohja mahdollisti asioiden nopean omaksumisen. Uuden tekniikan konfigurointi käytännössä oli hyvin mielenkiintoista, ja tulevien ohjelmistoversioiden myötä mm. MAC mobility -ominaisuuden tai active–active multihomingin testaus on hyvin todennäköisesti mahdollista.

Opinnäytetyö toimii katsauksena verkkolaitteiden toimintojen havainnollistamiseen kerroksisella mallilla, sekä johdantona MPLS-tekniikan toimintaan ja sen mahdollistamiin palveluihin ja ominaisuuksiin. Savonian tietoverkkolaboratorion uudet laitteet tarjosivat erinomaisen alustan testata tekniikan konfigurointia käytännössä.

LÄHTEET JA TUOTETUT AINEISTOT

ANDERSSON, et al. 2007. RFC 5036 LDP Specification, IETF Network Working Group [Viitattu 2015-6-1.] Saatavissa: https://tools.ietf.org/html/rfc5036

BATES, et al. 2007. Multiprotocol Extensions for BGP-4 [Viitatttu 2015-9-15.] Saatavissa: https://tools.ietf.org/html/rfc4760

BHASIN, Nic 2013. BASIC LDP CONFIGURATION AND BEHAVIOR ON IOS AND JUNOS [Viitattu 2015-06-1.] Saatavissa: http://www.netcraftsmen.com/basic-ldp-configuration-and-behavior-on-ios-and-junos/

CCIE R&S STUDY BLOG, 2012. Downstream On Demand vs Unsolicited Downstream Label Distribution [Viitattu 2015-6-1.] Saatavissa: https://ccieblog.co.uk/mpls/downstream-on-demand-vs-unsolicited-downstream-label-distribution

HANKINS, Greg 2014. Ethernet VPN (EVPN) - Overlay Networks for Ethernet Services [Viitattu 2015-8-4.] Saatavissa: http://www.slideshare.net/Alcatel-Lucent/monday-general-hankinsvpn2

INE INC. 2010. Scaling Virtual Private LAN Services (VPLS) [Viitattu 2015-6-20.] Saatavissa: http://blog.ine.com/2010/11/26/scaling-virtual-private-lan-services-vpls/

INE INC. 2015. MPLS Control Plane and Forwarding Plane Interaction [Viitattu 2015-5-15.] Saatavissa: http://blog.ine.com/2010/02/28/mpls-control-plane-and-forwarding-plane-interaction/

KAARIO, Kimmo 2002. TCP / IP –verkot 1. Painos. Porvoo: WS Bookwell.

LASSERRE ja KOMPELLA 2007. RFC 4762 Virtual Private LAN Service over LDP, IETF Network Working Group [Viitattu 2015-6-20.] Saatavissa: https://tools.ietf.org/html/rfc4762

MINEI, Ina ja LUCEK, Julian 2011. MPLS Enabled Applications: Emerging Developments and New Technologies 3. painos. Yhdistyneet Kuningaskunnat: John Wiley & Sons.

PEPELNJAK, Ivan 2013. Management, control and data planes in network devices and systems [Viitattu 2015-5-15.] Saatavissa: http://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html

RABADAN-PALISLAMOVIC, et al. 2015. Usage and applicability of BGP MPLS based Ethernet VPN (expired) [Viitattu 2015-10-15.] Saatavissa: https://tools.ietf.org/html/draft-rp-l2vpn-evpn-usage-03

RANJBAR, Amir. 2010. Troubleshooting and maintaining Cisco IP Networks (TSHOOT) 1. painos. Indianapolis: CiscoPress.

REKHTER, et al. 2006. A Border Gateway Protocol 4 (BGP-4) [Viitattu 2015-9-15.] Saatavissa: https://www.ietf.org/rfc/rfc4271.txt

ROSEN JA REKHTER 2006. RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs), IETF Network Working Group [Viitattu 2015-6-13.] Saatavissa: https://tools.ietf.org/html/rfc4364

SAJASSI, et al. 2015. BGP MPLS based Ethernet VPN [Viitattu 2015-8-4.] Saatavissa: https://tools.ietf.org/html/rfc7432

SAJASSI, et al. 2014. Requirements for Ethernet VPN (EVPN) [Viitattu 2015-8-4.] Saatavissa: https://tools.ietf.org/html/rfc7209

TEARE, Diane 2010. Implementing Cisco IP Routing (ROUTE) 3. Painos. Yhdysvallat: CiscoPress.

LIITE 1: Testausverkon konfiguraatio:

MX1:

```
            system {
    host-name PE1;
    root-authentication {
        encrypted-password ""; ## SECRET-DATA
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
logical-systems {
    CE1 {
        interfaces {
            ge-0/0/0 {
                unit 100 {
                    vlan-id 100;
                    family inet {
                        address 192.168.100.1/24;
                    }
                }
                unit 200 {
                    vlan-id 200;
                    family inet {
                        address 192.168.200.1/24;
                    }
                }
            }
            lo0 {
                unit 1 {
                    family inet {
                        address 10.10.10.10/32;
                    }
```

```
                }
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        vlan-tagging;
    }
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
            family mpls;
        }
    }
    ge-0/0/4 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 100 {
            encapsulation vlan-bridge;
            vlan-id 100;
        }
        unit 200 {
            encapsulation vlan-bridge;
            vlan-id 200;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 1.1.1.1/32;
            }
        }
    }
}
routing-options {
    router-id 1.1.1.1;
    autonomous-system 65000;
}
protocols {
    mpls {
        interface ge-0/0/3.0;
```

```
    }
    bgp {
        group internal {
            type internal;
            local-address 1.1.1.1;
            family evpn {
                signaling;
            }
            neighbor 2.2.2.2;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/3.0;
        }
    }
    ldp {
        interface ge-0/0/3.0;
    }
}
routing-instances {
    evpn100 {
        instance-type evpn;
        vlan-id 100;
        interface ge-0/0/4.100;
        route-distinguisher 1.1.1.1:100;
        vrf-target target:100:100;
        protocols {
            evpn;
        }
    }
    evpn200 {
        instance-type evpn;
        vlan-id 200;
        interface ge-0/0/4.200;
        route-distinguisher 1.1.1.1:200;
        vrf-target target:200:200;
        protocols {
            evpn;
        }
    }
```

```
}
```

MX2:

```
system {
    host-name PE2;
    root-authentication {
        encrypted-password ""; ## SECRET-DATA
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
logical-systems {
    CE2 {
        interfaces {
            ge-0/0/0 {
                unit 100 {
                    vlan-id 100;
                    family inet {
                        address 192.168.100.2/24;
                    }
                }
                unit 200 {
                    vlan-id 200;
                    family inet {
                        address 192.168.200.2/24;
                    }
                }
            }
            lo0 {
                unit 2 {
                    family inet {
                        address 20.20.20.20/32;
                    }
                }
            }
```

```
        }
    }
}

interfaces {
    ge-0/0/0 {
        vlan-tagging;
    }
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 10.0.0.2/24;
            }
            family mpls;
        }
    }
    ge-0/0/4 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 100 {
            encapsulation vlan-bridge;
            vlan-id 100;
        }
        unit 200 {
            encapsulation vlan-bridge;
            vlan-id 200;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 2.2.2.2/32;
            }
        }
    }
}
routing-options {
    router-id 2.2.2.2;
    autonomous-system 65000;
}
protocols {
    mpls {
        interface ge-0/0/3.0;
    }
```

```
    bgp {
        group internal {
            type internal;
            local-address 2.2.2.2;
            family evpn {
                signaling;
            }
            neighbor 1.1.1.1;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/3.0;
        }
    }
    ldp {
        interface ge-0/0/3.0;
    }
}
routing-instances {
    evpn100 {
        instance-type evpn;
        vlan-id 100;
        interface ge-0/0/4.100;
        route-distinguisher 2.2.2.2:100;
        vrf-target target:100:100;
        protocols {
            evpn;
        }
    }
    evpn200 {
        instance-type evpn;
        vlan-id 200;
        interface ge-0/0/4.200;
        route-distinguisher 2.2.2.2:200;
        vrf-target target:200:200;
        protocols {
            evpn;
        }
    }
}
```