Jere Kataja

Ethernet-siirtotekniikoiden vertailu

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 17.5.2013.

Työn valvoja:

Prof. Raimo Kantola

Työn ohjaaja:

TkL Marko Luoma

Aalto-yliopisto
Sähkötekniikan
korkeakoulu

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Jere Kataja

Työn nimi: Ethernet-siirtotekniikoiden vertailu

Päivämäärä: 17.5.2013 Kieli: Suomi Sivumäärä:9+83

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Raimo Kantola

Ohjaaja: TkL Marko Luoma

Tässä diplomityössä on tutkittu erinäisiä ratkaisuja, joiden avulla Ethernet-tekniikkaa voidaan hyödyntää palveluntarjoajien verkoissa. Tutkitut ja vertaillut tekniikat ovat PB, PBB, PBB-TE, VPLS, H-VPLS, MPLS-TP sekä PBB-VPLS. Tämän lisäksi työssä tutustuttiin optisiin siirtojärjestelmiin. Tekniikoihin tutustuttiin kirjallisuustutkimuksen avulla. Tietoa löytyi artikkeleista, standardeista sekä laitevalmistajien teknisistä dokumentaatioista. Optisia siirtojärjestelmiä tutkittaessa tutkimusmetodit olivat samat kuin verkkotekniikoita tutkittaessa. Kirjallisuustutkimuksen lisäksi rakennettiin PBB-VPLS -tekniikkaan pohjautuva testiverkko, jonka avulla varmennettiin ratkaisun ominaisuuksia.

Verkkotekniikoiden osalta kirjallisuustutkimuksen tulokseksi saatiin, että parhaiten palveluntarjoajien käyttöön soveltuvat PBB-TE, MPLS-TP sekä PBB-VPLS -tekniikat. Se mikä tekniikka sopii tietylle palveluntarjoajalle parhaiten riippuu muun muassa käytetystä verkkotopologiasta, olemassa olevasta laitteistosta sekä verkossa siirretyn liikenteen liikenneprofiilista. Optisten siirtojärjestelmien suhteen havaittiin, että todennäköisimmin tulevaisuudessa hyödynnetty tekniikka on aallonpituuksien multipleksointiin (WDM) pohjautuva optinen siirtojärjestelmä tai mahdollisesti aallonpituuksiin ja aikajaksoisuuteen (WDM ja TDM) pohjautuva järjestelmä.

Käytännön testeissä havaittiin, että PBB-VPLS -tekniikka on toteutettavissa ja tekniikka soveltuu hyvin MAC-osoitteiden piilottamiseen VPLS-tekniikkaan pohjautuvasta runkoverkosta. Samalla havaittiin kuitenkin se, että PBB-VPLS -tekniikkaan pohjautuvan verkon toteuttaminen laitteilla, jotka eivät suoraan tue kyseistä yhdistelmätekniikka, ei ole käytännöllistä. Itse PBB-VPLS -tekniikan havaittiin kuitenkin olevan erittäin potentiaalinen.

Avainsanat: Carrier Ethernet, PB, PBB, PBB-TE, VPLS, H-VPLS, MPLS-TP, PBB-VPLS, Optiset siirtojärjestelmät

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Jere Kataja

Title: Comparision of Ethernet transport technologies

Date: 17.5.2013 Language: Finnish Number of pages:9+83

Department of Communications and Networking

Professorship: Networking Engineering Code: S-38

Supervisor: Prof. Raimo Kantola

Instructor: Lic.Sc. (Tech.) Marko Luoma

In this Master's Thesis we have studied various technologies that enable the use of Ethernet within the networks of service providers. The compared technologies were PB, PBB, PBB-TE, VPLS, H-VPLS, MPLS-TP and PBB-VPLS. In addition to these technologies also optical transport technologies were evaluated. The research method was literature study. Information was found in journals, standards and technical documentations of networking device manufacturers. In addition to literature study a test network based on PBB-VPLS was built. This test network was used to verify the properties of the technology.

It was found, that the most suitable networking technologies to be used within the networks of service providers are PBB-TE, MPLS-TP and PBB-VPLS. The most suitable technology for a specific service provider depends on issues such as, network topology, existing hardware and the profile of transported traffic. Moreover, it was discovered that the optical technology most likely to be utilized in the future is to be based on wavelength multiplexing (WDM) or a technology that combines wavelength multiplexing with time-division multiplexing (TDM).

In practical tests, it was noticed that PBB-VPLS technology is feasible and it is very suitable for masking customer MAC addresses from the VPLS core network. However, it was also discovered that building a PBB-VPLS network, without devices that specifically support the technology, is not practical. Regardless, it was concluded that the PBB-VPLS technology has a great amount of potential.

Keywords: Carrier Ethernet, PB, PBB, PBB-TE, VPLS, H-VPLS, MPLS-TP, PBB-VPLS, Optical transport

Esipuhe

Haluan kiittää kaikkia jotka ovat edesauttaneet tämän työn valmistumista.

Otaniemi, 17.5.2013

Jere Kataja

Sisältö

Lyhenteet

ATM	Asynchronous Transfer Mode
BCB	Backbone Core Bridge
BEB	Backbone Edge Bridge
BGP	Border Gateway Protocol
BMAC	Backbone Media Access Control
BVLAN	Backbone Virtual LAN
CE	Customer Edge
CMAC	Customer Media Access Control
CP	Control Plane
CRC	Cyclic redundancy check
CWDM	Coarse Wavelength-division Multiplexing
CVLAN	Customer Virtual LAN
DST	Destination
DWDM	Dense Wavelength-division Multiplexing
EPON	Ethernet Passive Optical Network
FDB	Forwarding Database
FIB	Forwarding Information Base
GMPLS	Generalized Multiprotocol Label Switching
GPON	Gigabit Passive Optical Network
H-VPLS	Hierarchical Virtual Private LAN Service
IVL	Independent VLAN Learning
LAN	Local Area Network
LDP	Label Distribution Protocol
MAC	Media Access Control
MP	Management Plane
MPLS	Multiprotocol Label Switching
MPLS-TP	Multiprotocol Label Switching: Transport Profile
MTU	Multi-Tenant Unit
MSTP	Multiple Spanning Tree Protocol
OAM	Operations, administration and management
PB	Provider Bridging
PBB	Provider Backbone Bridging
PBB-TE	Provider Backbone Bridging: Traffic Engineering
PE	Provider Edge
PEB	Provider Edge Bridge
PLSB	Provider Link State Bridging
PON	Passive Optical Network
PWE	Pseudo Wire Encapsulation
RR	Route Reflector
RSTP	Rapid Spanning Tree Protocol
RTF	Route Target Filtering

SRC	Source
STP	Spanning Tree Protocol
SVLAN	Service Virtual LAN
TDM	Time Division Multiplexing
TVL	Type-length-value
VLAN	Virtual LAN
VOIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WDM	Wavelength Division Multiplexing

1 Johdanto

Ethernet-tekniikka on kehittynyt yksinkertaisesta lähiverkkotekniikasta käytännössä kaikkialla läsnä olevaksi verkkotekniikaksi, jota käytetään niin yritysten kuin yksityisasiakkaidenkin ympäristöissä. Ethernetin tarkat määrittelyt sekä sen käyttämisen yksinkertaisuus on mahdollistanut tekniikan yleistymisen laajemmin kuin minkään muun verkkotekniikan. Pääosa palveluntarjoajien verkoista on kuitenkin rakennettu aikana, jolloin virtuaalipiirikytkentäiset verkkotekniikat kuten Frame relay ja Asynchronous transfer mode (ATM) olivat pääasialliset keinot toteuttaa liikenteen siirto. Nämä seikat ovat johtaneet tilanteeseen, jossa palveluntarjoajien on tuettava useaa tekniikkaa, mikä johtaa suuriin kustannuksiin sekä mahdollisiin yhteensopivuusongelmiin. Yksi merkittävä keino, jonka avulla palveluntarjoavat voivat pienentää kustannuksiaan on Ethernet-tekniikan hyödyntäminen palveluntarjoajien siirtoverkoissa. Kustannussäästö muodostuu siitä, että palveluntarjoajien ei tarvitse enää tukea useaa eri tekniikkaa, jolloin operatiiviset kustannukset pienenevät. Sellaisenaan perinteinen Ethernet ei kuitenkaan ole riittävän hyvä palveluntarjoajien käyttöön, koska tekniikan hallittavuus ja valvottavuus ovat heikkoja ja palveluntarjoajan kannalta tekniikka skaalautuu huonosti. [1]

Useita tekniikoita on kehitetty, jotta Ethernetia voidaan hyödyntää palveluntarjoajien verkoissa nykyistä tehokkaammin. Tässä diplomityössä esitetään merkittävimmät tällaiset tekniikat. Lisäksi näitä ratkaisuja verrataan kirjallisuustutkimuksen perusteella keskenään. Optiset siirtoverkot tarjoavat monia etuja perinteisiin elektronisiin siirtoverkkoihin verrattuna. Tästä syystä myös osaa näistä optisista siirtojärjestelmistä käsitellään tässä työssä. Työn pääpaino on kuitenkin Ethernetin käytössä pakettisiirrossa, joten optisia siirtojärjestelmiä ei käsitellä yhtä laajalti. Kirjallisuustutkimuksen lisäksi suoritettiin kokeellinen tutkimus hyödyntämällä työn yhteydessä rakennettua testiverkkoa. Diplomityö on tehty Aalto-yliopiston Sähkötekniikan korkeakoulun Tietoliikenne- ja tietoverkkotekniikan laitoksella.

1.1 Tutkimuskysymykset ja tutkimusalueen rajaus

Tutkittavat tekniikat valittiin niiden yleisen merkityksen perusteella. Kirjallisuusselvityksen tutkimustavoitteina olivat seuraavat asiat:

1. Eri siirto- ja välitystekniikoiden perusteiden esittäminen
2. Näiden tekniikoiden vertailu
3. Erinäisten yhdistelmätekniikoiden perusteiden esittäminen.

Vertailtaviksi tekniikoiksi valittiin Ethernet-alueverkkovälitys (Provider Bridging, PB), Ethernet-runkoverkkovälitys hajautetulla hallinnalla (Provider Backbone Bridging, PBB), Ethernet-runkoverkkovälitys keskitetyllä hallinnalla (Provider Backbone Bridging: Traffic Engineering, PBB-TE), Ethernet-leimakytkentä (Virtual Private Lan Service, VPLS), Hierarkkinen Ethernet-leimakytkentä (Hierarchical VPLS,

H-VPLS) ja Leimakytkentä keskitetyllä hallinnalla (MPLS: Transport Profile, MPLS-TP). Lisäksi päätettiin, että valittuja tekniikoita verrataan kirjallisuustutkimuksen perusteella seuraavien osa-alueiden suhteen:

- Skaalautuvuus: verkko, liitännät, palvelut ja asiakkaat
- Hallittavuus: palvelu, laatu ja verkko
- Toimintavarmuus: vikasietoisuus, toipuvuus
- Tietoturvauhkat: palvelunestot ja kuuntelu, protokollat ja tilakoneet
- Liitettävyys: kyky liittyä ulkoisiin verkkoihin ja palveluihin tai kyky hyödyntää ulkoisia verkkoja osana palvelua

Lisäksi päätettiin tehdä lyhyt kirjallisuusselvitys optisista siirtojärjestelmistä. Optisten siirtojärjestelmien merkitys kiinteässä tiedonsiirrossa kasvaa jatkuvasti. Kirjallisuusselvityksen pohjalta pyritään esittämään arvio siitä, mikä optinen siirtojärjestelmä yleistyy tulevaisuudessa.

Kaikkia verkkotekniikoita ei ollut mielekästä testata käytännössä diplomityön yhteydessä. Kirjallisuustutkimuksen pohjalta testattavaksi rajautui PBB-VPLS -tekniikka, koska ratkaisulla on potentiaalia parantaa olemassa olevien verkkojen suorituskykyä, ja se ei ole niin laajalti tutkittu kuin MPLS-TP tai PBB-TE -tekniikat. Tämän tekniikan testaamisen suhteen tutkimuskysymyksiksi muodostuivat seuraavat kaksi asiaa:

1. Pystytäänkö PBB-VPLS -tekniikalla toteutettu verkko rakentamaan ilman erityisesti tämän tekniikan toteuttamiseen kehitettyjä laitteita?
2. Toimiiko tekniikan MAC-osoitteiden skaalautuvuuden parantaminen käytännössä tällaisessa verkossa?

Tekniikan tarkempi tutkiminen rajattiin ainoastaan MAC-osoitteiden skaalautuvuuteen, kuten yllä on mainittu. Tämä rajaus oli tarpeellinen, koska tutkimukseen tarvitut Extreme Networksin BlackDiamond-kytkimet olivat lainassa laitevalmistajalta vain rajallisen ajan.

1.2 Työn rakenne ja tutkimusmenetelmät

Luvussa 2 esitetään kirjallisuustutkimuksen tulokset. Kyseisessä luvussa esitetään ensin eri verkkotekniikoiden perusteet, jonka jälkeen eri tekniikoita verrataan keskenään siten, että samaan käyttötarkoituksiin kehitettyjä tekniikoita verrataan keskenään. Runkoverkkoon tarkoitettua tekniikka ei siis verrata pääsyverkkoon tarkoitetun tekniikan kanssa. Luvussa esitetään myös tekniikoita, jotka on kehitetty yhdistämällä aiemmin esiteltyjä tekniikoita yhteen. Luvussa 2 esitetään myös optisten siirtojärjestelmien perusteet, niiden nykytila ja niiden todennäköinen tulevaisuus. Luvussa 3 käsitellään kokeellisen tutkimuksen eteneminen. Samaisessa luvussa esitetään tehdyt

testit sekä testien aikana havaitut ongelmat. Luvussa 4 esitetään teknisen tutkimuksen pohjalta saadut tulokset. Tuloksista esitetään tärkeimmät asiat eli lukijan ei tarvitse itse yrittää tulkita tuloksia. Luvussa 5 arvioidaan näiden tulosten oikeellisuutta sekä esitetään mahdollisia jatkotutkimuskohteita. Luvussa 6 luodaan yhteenveto työstä.

Kirjallisuustutkimus toteutettiin hyödyntämällä kolmea erityyppistä dokumenttiluokkaa. Pääasiallinen painoarvo oli tieteellisillä julkaisuilla, jotka on julkaistu alan lehdissä. Näiden lähteiden sisältöä pidettiin erittäin luotettavana, koska kyseiset artikkelit on seulottu tarkkaan ennen niiden julkaisemista alan julkaisuissa. Toinen dokumenttityyppi oli erilaiset standardit sekä tekniset määritelmät. Näidenkin luotettavuutta voitiin pitää erittäin hyvänä, koska nämä dokumentit kokevat tarkan arvioinnin ennen niiden hyväksymistä standardiksi. Kolmas dokumenttityyppi oli eri laitevalmistajien julkaisemat tekniset dokumentaatiot sekä laitteiden ohjeet. Näitä dokumentteja arvioitiin kriittisesti ennen kuin niiden ilmoittamia tietoja käytettiin hyväksi. Tämä johtuu siitä, että laitevalmistajat eivät noudata standardeja täysin. Lisäksi laitevalmistajat ovat subjektiivisia esittäessään suosimiaan tekniikoita. Teknisessä tutkimuksessa hyödynnettiin sekä liikenteen kaappausta että komentoliittymien ilmoittamia tietoja siitä, miten MAC-osoitteet leviävät, sekä miten niitä opitaan. Näin kyettiin todentamaan tulosten oikeellisuus.

2 Teoreettinen tutkimus

Tässä luvussa käsitellään tutkittuja tekniikoita kirjallisuuden perusteella. Luvussa käsitellään aluksi Ethernet-siirtotekniikat, jonka jälkeen kerrotaan optisista siirtojärjestelmistä. Ethernet-siirtotekniikoiden käsittely on jaettu osiin siten, että aluksi esitetään tekniikoiden perusteet. Tämän jälkeen vertaillaan samoihin käyttötarkoituksiin suunniteltuja tekniikoita keskenään. Lisäksi käydään läpi tekniikoita, jotka on kehitetty yhdistämällä yksittäisiä tekniikoita keskenään. Optisista siirtojärjestelmistä annetaan aluksi lyhyt esittely, jonka jälkeen kerrotaan optisten tekniikoiden nykytilasta. Lopuksi tehdään katsaus optisten siirtojärjestelmien lähitulevaisuuteen.

2.1 Perinteinen Ethernet

Perinteinen Ethernet suunniteltiin käytettäväksi lähiverkoissa mahdollisimman yksinkertaisesti. Tästä syystä Ethernetin toiminnan kannalta oleellisia ovat sekä MAC-osoitteiden oppiminen että Spanning Tree -protokollan käyttäminen. MAC-osoitteiden oppimisen ansiosta laitteet voidaan kytkeä verkkoon ilman konfigurointia. Spanning Tree -protokolla puolestaan huolehtii siitä, että verkkoon ei muodostu silmukkaa.

MAC-osoitteiden oppiminen johtaa kuitenkin skaalautuvuusongelmiin. Välitystaulut joihin opitut osoitteet tallennetaan, eivät kestä kuormitusta kun verkon koko kasvaa erittäin suureksi. MAC-osoitteiden oppiminen edellyttää myös sitä, että tuntemattomiin osoitteisiin suunnatut kehykset on yleislähetettävä koko verkkoon. Tästä seuraa se, että tietyissä tapauksissa yleislähetysliikenne voi kuormittaa verkkoa erittäin voimakkaasti. Pahimmassa tapauksessa koko verkko voi kaatua.

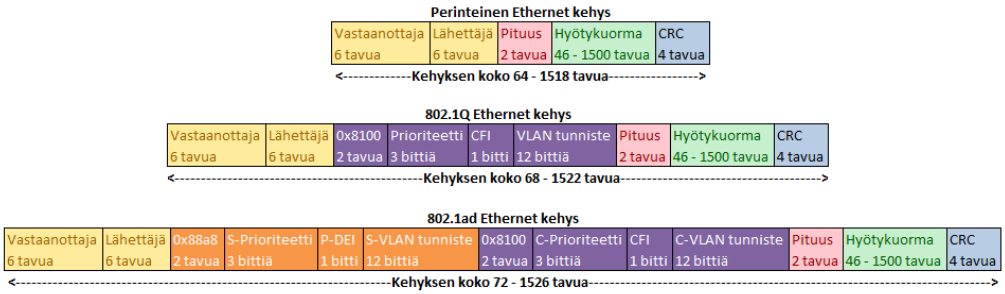
Toimintavarmuutta Ethernetiin saadaan käyttämällä yhtä kolmesta Spanning Tree -protokollasta. Vaihtoehdot ovat Spanning Tree (STP), Rapid Spanning Tree (RSTP) ja Multiple Spanning Tree -protokollat (MSTP). Kaikkien ratkaisujen tehtävänä on poistaa verkon silmukat sekä mahdollistaa redundanssin lisääminen verkkoon. Protokollien toimintaperiaatteet eivät eroa merkittävästi toisistaan. RSTP-protokolla kehitettiin nopeuttamaan STP-protokollan konvergenssiä. Tämä toteutettiin hienosäätämällä muun muassa »Hello»-viestien käyttämistä. MSTP-protokolla puolestaan laajentaa RSTP-toteutusta siten, että verkossa ajetaan useaa RSTP-instanssia VLAN-tunnistekohtaisesti. Tällä tavoin kyetään lieventämään yksittäisen instanssin laskutoimitusten raskautta. Tästä huolimatta kaikkien toteutusten konvergenssiajat ovat liian suuria käytettäväksi suurissa verkoissa. [2]

2.2 Provider Bridging

Ethernet-tekniikassa eri loogiset verkot erotetaan toisistaan käyttämällä tähän tarkoitukseen suunniteltua Virtual LAN -tunnistetta (VLAN-tunniste). Palveluntarjoaja ei voi kuitenkaan hyödyntää tätä tunnistetta, mikäli asiakkaana on esimerkiksi yritys, joka on jakanut eri osastot omiin loogisiin levitysalueisiinsa käyttäen VLAN-tunnistetta. Tässä aliluvussa esitellään tekniikka, joka kehitettiin ratkaisemaan tämä ongelma.

Ethernet-alueverkkovälityksessä (Provider Bridging, PB, myös 802.1ad, Q-in-Q) hyödynnetään 802.1Q-standardissa määritettyä VLAN-tunnistemerkintää. Sitä

käytetään asiakkaan VLAN-tunnisteen (CVLAN-tunniste) ilmaisemiseen. Tämän tunnisteen eteen lisätään toinen VLAN-tunnistemerkintä, joka tunnetaan palveluntarjoajan VLAN-tunnisteena (SVLAN-tunniste). Tekniikka perustuu siis siihen, että Ethernet-kehyksiin merkataan kaksi tai useampi VLAN-tunniste, joka mahdollistaa sen, että asiakkaiden ja palveluntarjoajien loogiset verkot kyetään erottamaan toisistaan. Tekniikka on mahdollista toteuttaa siten, että asiakkaan ei tarvitse tehdä muutoksia omaan verkkoonsa, koska SVLAN-tunnisteet voidaan lisätä ja poistaa kehyksistä palveluntarjoajien laitteilla. Kuvasta 1 nähdään perinteisen Ethernetin, 802.1Q-tunnisteella merkatun sekä 802.1ad-tunnisteilla merkatun kehysten rakenne. Huomioitavaa on se, että vaikka kehysten kokonaiskoko on kasvanut laajennusten myötä, ei hyötykuormalle määritettyjä kokorajoja ole muutettu. [1], [3]–[5]

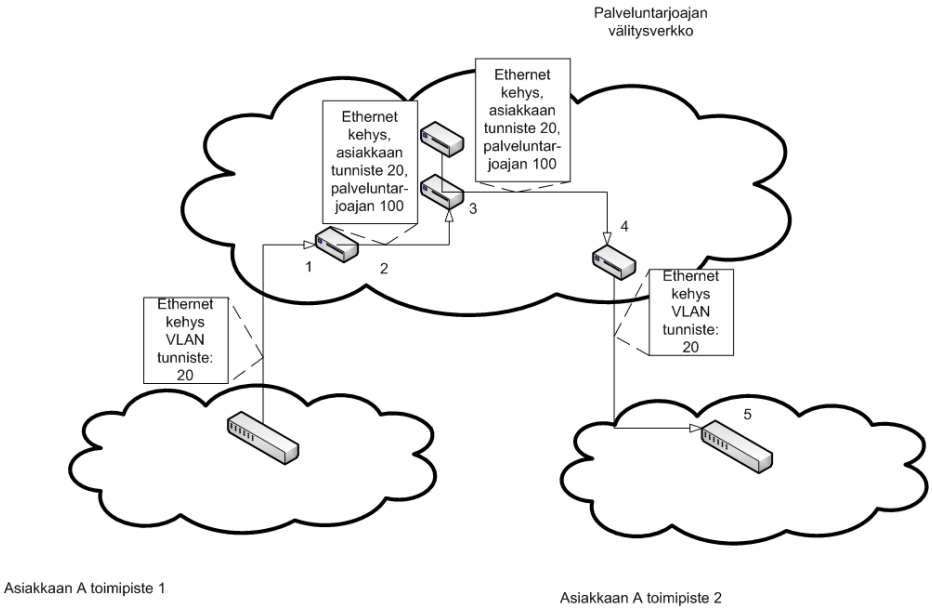


Kuva 1: Ethernet-kehysten rakenne.

Ethernet-alueverkkovälitys mahdollistaa sen, että asiakkaat voivat käyttää CVLAN-tunnisteita omien käytäntöjensä mukaisesti, riippumatta muiden asiakkaiden tai palveluntarjoajien käytännöistä. Esimerkiksi asiakas *A* voi käyttää tunnisteita 10–20 ja asiakas *B* voi käyttää CVLAN-tunnisteita 15–30. 802.1Q-tekniikkaan pohjautuvassa verkossa tämä ei olisi mahdollista, koska asiakkaiden käyttämät tunnisteet 15–20 ovat päällekkäisiä. Ethernet-alueverkkovälitystä käyttämällä palveluntarjoajien ei tarvitse kertoa omia VLAN-tunnisteiden merkitsemiskäytäntöjään asiakkaille, eikä asiakkaiden tarvitse tietää niistä. [1], [3]–[5]

Kuvassa 2 esitetään PB-tekniikalla kapseloidun kehyksen välitys PB-tekniikkaan pohjautuvassa verkossa. Vaiheessa **1** asiakkaan kytkin toimipisteessä *1* lähettää VLAN-tunnisteella *20* merkatun kehyksen palveluntarjoajan kytkimelle. Vaiheessa **2** palveluntarjoajan kytkin lisää kehykseen palveluntarjoajan VLAN-tunnisteen *100*. Jos palveluntarjoajan kytkimen SVLAN-tunnisteen *100* välitystaulussa (Forwarding database, FDB) on tieto rajapinnasta, jota käyttämällä kehyksen vastaanottaja voidaan saavuttaa, välittää kytkin kehyksen ainoastaan siihen rajapintaan. Mikäli kytkin ei tiedä, mitä rajapintaa tulisi käyttää vastaanottajan saavuttamiseksi, välitetään kehys kaikkiin rajapintoihin, jotka välittävät SVLAN-tunnisteella *100* merkittyjä kehyksiä. Vaiheessa **3** palveluntarjoajan toisen kytkimen ei tarvitse tehdä muutoksia kehykseen. Kytkin välittää kehyksen eteenpäin samalla periaatteella kuin palveluntarjoajan ensimmäinen kytkin. Vaiheessa **4** palveluntarjoajan kolmas kytkin poistaa kehyksestä SVLAN-tunnisteen ja välittää kehyksen asiakaskytkimelle, joka on toimipisteessä *2*. Vaiheessa **5** asiakkaan kytkin välittää asiakkaan VLAN-tunnisteella *20* eteenpäin. Kehysten välitys perustuu siis siihen, että palveluntarjoajan kytkimillä

on jokaista SVLAN-tunnistetta kohden oma välitystaulu. Välitystauluissa on tieto siitä, mitkä MAC-osoitteet ovat saavutettavissa mistäkin rajapinnasta. Välitys tapahtuu siis SVLAN-tunnistekohtaisesti. Asiakkaiden käyttämät VLAN-tunnisteet eivät vaikuta palveluntarjoajien kytkimien muodostamiin välitystauluihin.



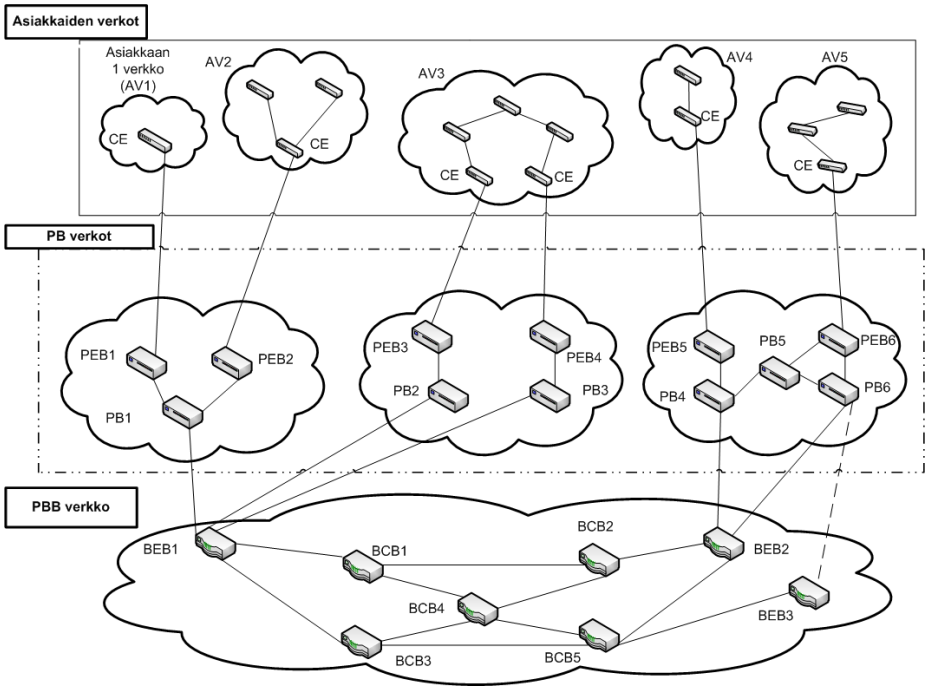
Kuva 2: PB-tekniikan kehyksen kulku välitysverkossa.

2.3 Provider Backbone Bridging

Ethernet-runkoverkkovälitys hajautetulla hallinnalla (Provider Backbone Bridging, PBB, 802.1ah, MAC-in-MAC) kehitettiin pääasiallisesti parantamaan PB-tekniikkaa. Parannus perustui malliin hierarkkisesta verkkoarkkitehtuurista. Tämän arkkitehtuurin pohjana on eri verkkojen ryhmittäminen. PBB-tekniikka voi siirtää sekä PB- että 802.1Q-tekniikan liikennettä. Tällöin voidaan 802.1Q-tekniikan liikenne ensin aggregoida PB-tekniikalla ennen liikenteen siirtämistä PBB-tekniikalla toteutetun verkon lävitse, mikäli se on verkon kannalta järkevää. Mikäli verkko ei saavuta etua tästä aggregoinnista, siirretään 802.1Q-tekniikan liikenne suoraan PBB-tekniikalla toteutetun verkon lävitse. [5]

Kuvassa 3 esitetään PBB:n hierarkkisuutta. Asiakkaiden verkkoihin ei tarvitse tehdä päivityksiä tai määritysten muokkaamista. Asiakaslaitteet (CE) eivät siis ole tietoisia kuvan esimerkissä muista verkkotekniikoista. PB-tekniikalla toteutettujen verkkojen kytkimet (PEB, PB) eivät ole tietoisia PBB-tekniikalla toteutetusta verkossa, joten nämäkin laitteet toimivat kuvan esimerkissä ilman muutoksia. Palveluntarjoajan runkoverkon kytkinten (BCB, BEB) on kuitenkin tuettava PBB-tekniikkaa. PB-tekniikalla toteutetun verkon asiakasreunan kytkin (PEB) muuntaa kehykset PB-tekniikan kehysmuotoon. Runkoverkon reunakytkin (BEB) muuttaa kehykset PBB-tekniikan kehysmuotoon. Runkoverkon runkokytkin (BCB) on samanlainen laite kuin runkoverkon reunakytkin. Ero näiden laitteiden välillä on se, että runkoverkon

runkokytkimen ei tarvitse muuntaa kehysmuotoa. Tämä hierarkkisuus mahdollistaa sen, että kun PBB-tekniikka otetaan käyttöön, asiakkaan laitteissa eikä PB-tekniikan toteuttavissa kytkimissä tarvitse tehdä muutoksia.

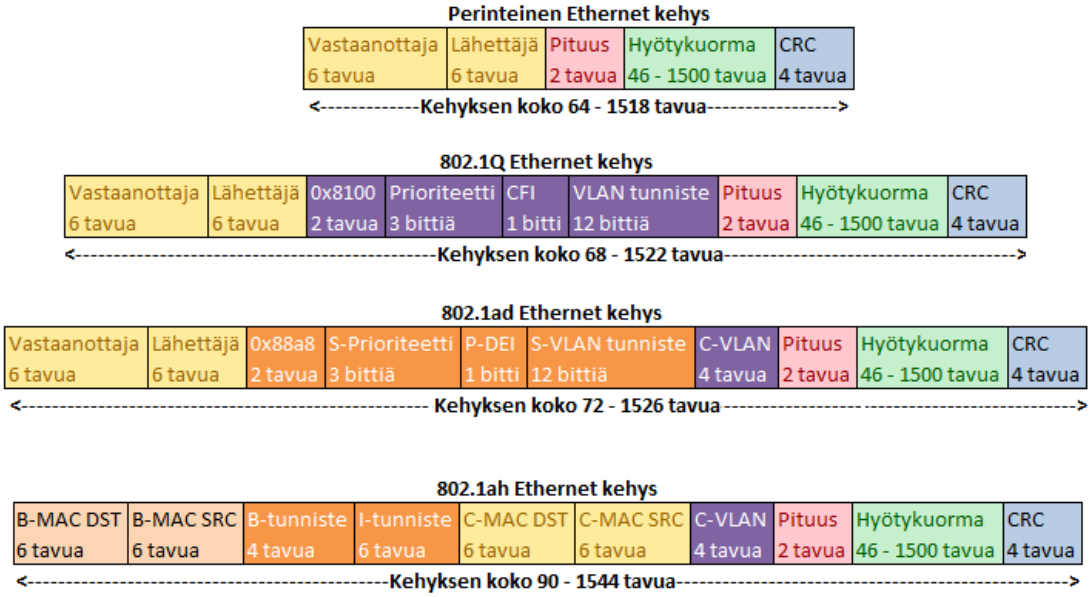


Kuva 3: PBB-verkon hierarkkisuus [5].

Vaikka tällainen hierarkkisuus parantaa PB-tekniikalla rakennettujen verkkojen skaalautuvuutta, ei se ratkaise asiaa täysin. Esimerkiksi asiakaslaitteiden MAC-osoitteiden oppimisesta johtuva välitystaulujen täyttyminen ei ratkea pelkästään verkon hierarkkisuudella. Tästä syystä PBB-tekniikassa otetaan käyttöön myös uusi kehysformaatti. Uudessa kehysmallissa PBB-verkkoon saapuvat kehykset kapseloidaan uudelleen siten, että kehyksiin lisätään muun muassa palveluntarjoajan runkoverkon kytkimen MAC-osoite. Näin asiakaslaitteiden MAC-osoitteita ei tarvitse käyttää PBB-tekniikan runkoverkossa.Tämä ratkaisu tunnetaan myös nimellä MAC-in-MAC, ja sen takia asiakaslaitteiden MAC-osoitteita ei näy PBB-verkon keskuskytkimien välitystauluissa. Välitys PBB-tekniikan verkossa tapahtuu runkoverkon MAC-osoitteiden (BMAC) lisäksi runkoverkon VLAN-tunnisteen (BVLAN-tunniste) avulla. Runkoverkon MAC-osoitteet opitaan siis BVLAN-tunnistekohtaisiin välitystauluihin. BVLAN-tunnisteiden käyttäminen mahdollistaa myös runkoverkon jakamisen tehokkaasti useaan loogiseen verkkoon, jotta laitteiden välisten linkkien hyötysuhde olisi mahdollisimman suuri. Yhteistä PBB-tekniikalla ja perinteisellä Ethernet-tekniikalla on siinä, että molemmissa käytetään Spanning Tree -protokollaa (STP) välityspolkujen määrittämiseen ja kehysten tulvitusta, mikäli vastaanottajan sijainti ei ole tiedossa. [3]–[6]

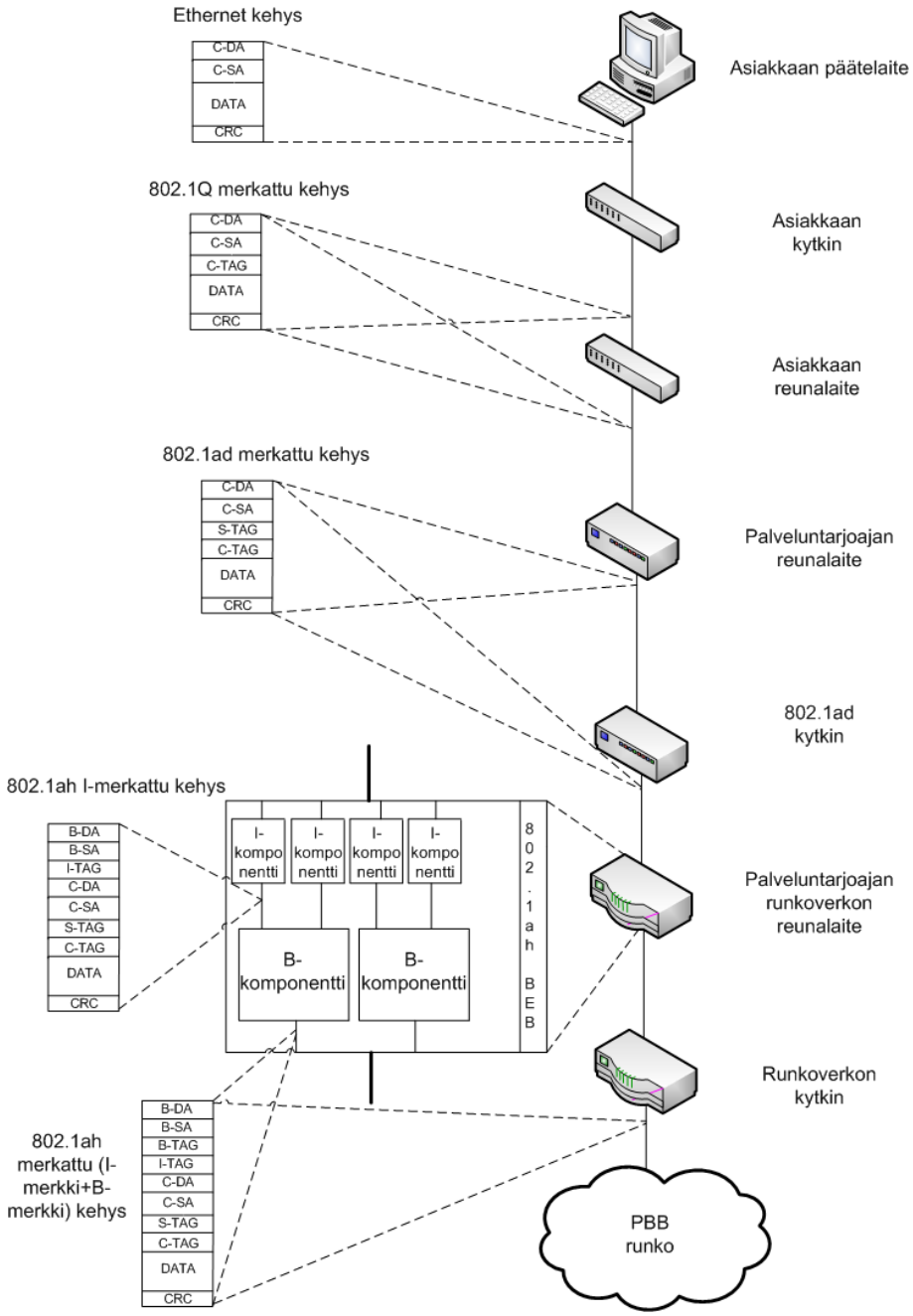
Kuvassa 4 esitetään perinteisen Ethernetin, 802.1Q-tunnisteella merkatun kehyksen, PB-tekniikan kehyksen sekä PBB-tekniikan kehyksen kehysrakenteet. PBB- ja PB-tekniikan kehysrakenteissa esitetty CVLAN-solu pitää sisällään 802.1Q-tekniikan

kehysrakenteessa laajemmin esitetyt tiedot. Runkoverkossa käytettäviä MAC-osoitteita kuvataan termeillä *B-MAC DST* ja *B-MAC SRC*. Kun Ethernet-kehys saapuu PBB-verkon reunakytkimelle, lisää reunakytkin kehykseen runkoverkon MAC-osoitteiden lisäksi ISID-komponentin (I-komponentin) ja B-komponentin. Mikäli saapuvassa kehyksessä on SVLAN-tunniste, ISID-komponentin tiedot määrittyvät yleensä sen perusteella, mutta komponentin tiedot voidaan määrittää myös muilla perusteilla. ISID-komponentti sisältää Ethertype-kentän, jonka arvo on »0x88E7», prioriteettikentän sekä kolmen tavun mittaisen ISID-tunnisteen. ISID-tunniste on verkonlaajuinen uniikki tunniste, jonka avulla tunnistetaan asiakas, asiakkaan palvelu tai molemmat, minkä johdosta sitä hyödynnetään ainoastaan PBB-verkon reunakytkimillä. Tunnisteen koko, kolme tavua, tarkoittaa että verkossa voi olla samanaikaisesti 2^{24} eli noin 16 miljoonaa asiakaspalveluinstanssia. ISID-komponentin lisäämisen jälkeen kehykseen lisätään B-komponentti. B-komponentin sisällä olevan runkoverkon VLAN-tunnisteen (BVLAN-tunniste) avulla siirtoverkko jaetaan loogisesti useaksi siirtoverkoksi. Yhteen BVLAN-tunnisteeseen, eli loogiseen siirtoverkkoon, voidaan assosioida useita ISID-tunnisteita, mutta ISID-tunniste voidaan assosioida ainoastaan yhteen BVLAN-tunnisteeseen. PBB-tekniikan kytkimet muodostavat välitystaulut BVLAN-tunnistekohtaisesti, ja niihin opitaan ainoastaan runkoverkossa käytössä olevia MAC-osoitteita. [3], [5], [6]



Kuva 4: PBB-tekniikan kehys verrattuna muihin Ethernet-tekniikoiden kehyksiin.

Kuvassa 5 näytetään, miten asiakaslaitteen kehys välittyy eri tekniikoissa sekä miten kehys kapseloidaan. Alkutilanteessa asiakkaan päätelaite lähettää normaalin Ethernet-kehyksen. Kun kehys saapuu ensimmäiselle 802.1Q-kytkimelle, tämä lisää kehykseen CVLAN-tunnisteen kytkimen ylläpitäjän tekemien määritysten mukaisesti. Normaalissa tilanteessa tätä CVLAN-tunnistetta ei muokata 802.1Q-tekniikalla toteutetussa verkossa. Kun kehys saapuu PB-tekniikalla toteutetun verkon reunakytkimelle, lisää kytkin kehykseen palveluntarjoajan VLAN-tunnisteen. SVLAN-tunnisteen arvo määrittyy kytkimen ylläpitäjän määrittämien asetusten perusteella. Tällöin kehysrakenne vastaa PB-tekniikan standardin määrittämää kehysrakennetta, jota ei muuteta kehyksen liikkuessa PB-verkon sisällä. Seuraavassa vaiheessa kehys saapuu PBB-tekniikalla toteutetun verkon reunakytkimelle. Saapuva kehys käsitellään kytkimen sisällä ensin ISID-komponentissa, joka lisää kehykseen ISID-komponentin ja runkoverkon MAC-osoitteet. Mikäli runkoverkon MAC-kohdeosoite ei ole tiedossa, merkitään vastaanottajaksi yleislähetysosoite. Tämän jälkeen kehys siirtyy kytkimen sisällä B-komponentin käsiteltäväksi. Tämän jälkeen kehys vastaa PBB-tekniikan standardin määrittämää kehysstandardia. [3]–[6]



Kuva 5: Ethernet-kehyksen välitys ja kapselointi eri tekniikoissa.

2.4 Provider Backbone Bridging Traffic Engineering

Ethernet-runkoverkkovälitys keskitetyllä hallinnalla (Provider Backbone Bridging Traffic Engineering, PBB-TE, 802.1Qay) on usean vuoden kehitystyön tulos, jota Institute of Electrical and Electronics Engineers (IEEE) ja ITU Telecommunication Standardization Sector (ITU-T) -organisaatiot tekivät yhteistyössä. Tekniikan tarkoitus on parantaa ja tehostaa Ethernet-tekniikan käyttöä siirtoverkoissa. PBB-TE -tekniikka

mahdollistaa sen, että palveluntarjoajat voivat luoda verkon, joka pohjautuu täysin Ethernet-tekniikkaan niin ettei muita tekniikoita, kuten SDH- tai MPLS-tekniikkaa, tarvita verkossa. PBB-TE -tekniikka hyödyntää muita Ethernet-tekniikoita. 802.1Q- ja PB-tekniikkoita hyödynnetään täysin ja PBB- ja 802.1ag-tekniikoita hyödynnetään lähes täysin. PBB-TE -tekniikan ja muiden Ethernet-tekniikoiden merkittävin ero on se, että PBB-TE -tekniikka käyttää välityspolun rakentamiseen perinteisistä Ethernet-verkoista poiketen joko staattisia konfiguraatioita tai reititysalgoritmeja. [3]

PBB-TE -tekniikan toiminta on hallittua sekä determinististä. Tämä on suoraan verrannollista olemassa olevien siirtotekniikoiden, kuten SDH-tekniikan, käyttäytymiseen. PBB-TE -tekniikan toimintamalli eroaa siis selvästi PBB-tekniikan toimintamallista, joka ei ole deterministinen tai hallittu. PBB-tekniikassa BVLAN-tunnisteella verkko jaetaan loogisiin siirtoverkkoihin. PBB-TE -tekniikassa BVLAN-tunniste yhdessä runkoverkon MAC-kohdeosoitteen kanssa määrittää tietyn tarkan polun PBB-TE -verkon lävitse. [3]

PBB-tekniikassa kytkimet välittävät kehykset BVLAN-tunnisteiden ja runkoverkon MAC-kohdeosoitteiden muodostamien 60-bittisten tunnisteiden perusteella. PBB-TE -tekniikassa MAC-osoitteiden oppiminen ei ole käytössä, joten ohjaustason tai hallintajärjestelmän on lisättävä nämä 60-bittiset tunnisteet kytkinten välitystauluihin. Verkon sisällä 60-bittiset tunnisteet ovat globaaleja sekä uniikkeja, jonka johdosta verkon päästä-päähän operointi on yksinkertaisempaa kuin muissa Ethernet-tekniikoissa. [3]

PBB-TE -tekniikassa MAC-kohdeosoitteisiin liitetyt polut tunnistetaan 12-bittisen BVLAN-tunnisteen avulla. Tämä mahdollistaa varayhteyksien muodostamisen verkkoon ennen vikatilanteiden tapahtumista. Varayhteydelle siirtyminen on myös erittäin nopeaa, koska vikatilanteen sattuessa, kytkimien tulee vaihtaa ainoastaan ensisijaisen polun BVLAN-tunniste varayhteyden BVLAN-tunnisteeseen. Vikatilanteet havaitaan käyttämällä Connectivity Fault Management -tekniikan (802.1ag) toimintoja. Vikatilanne voidaan kiertää käyttämällä täysin erillistä polkua tai ohjaamalla liikenne vain vikaantunen kohdan ohitse. Lisäksi OAM-tekniikan kehykset siirtyvät verkossa normaaliliikenteen käyttämää polkua pitkin, kun ne käyttävät samaa BVLAN-tunnistetta. Yhteydellisyys saadaan hallittua ainoastaan lisäämällä kytkimien välitystauluihin haluttujen polkujen mukaiset tiedot. [3]

PBB-TE -tekniikka mahdollistaa myös sen, että kaikkia BVLAN-tunnisteita ei määritetä PBB-TE -tekniikan käyttöön. Tällöin näitä BVLAN-tunnisteita voidaan käyttää hyödyntäen Spanning Tree -tekniikaa PBB-TE -tekniikan kanssa rinnakkain. Välitystaulut voidaan täyttää usealla eri tavalla. Yksi vaihtoehto on käyttää GMPLS-tekniikkaa välitystaulujen täyttämiseksi. Toinen keino tietojen lisäämiseksi välitystauluihin on käyttää Provider Link State Bridging -tekniikkaa (PLSB). Tässä tekniikassa käytetään IS-IS -protokollaa muodostamaan näkymä verkon topologiasta ja laskemaan optimaalinen polku verkon eri pisteiden välille. Kolmas keino, tietojen lisäämiseksi välitystauluihin, on käyttää erillistä hallintajärjestelmää. [3]

Ethernet-runkoverkkovälitys keskitetyllä hallinnalla muistuttaa voimakkaasti perinteisiä piirikytkentäisiä verkkoja, kuten SDH-verkkoja. Perinteisissä tekniikoissa käytettiin myös ulkoista hallintajärjestelmää palveluiden provisiointiin, mikä on myös mahdollista PBB-TE -tekniikassa. PBB-TE -tekniikan arkkitehtuurissa ei myös-

kään ole määriteltynä raskasta ja kompleksista ohjaustasoa, toisin kuin esimerkiksi IP/MPLS-tekniikassa. Onkin siis selvää, että perinteisiä piirikytkentäisiä verkkojen toteutustapoja on käytetty hyödyksi, kun PBB-TE -tekniikkaa on suunniteltu. [3], [8]

2.5 Virtual Private LAN Service

Ethernet-leimakytkennällä (Virtual Private LAN Service, VPLS) palveluntarjoajat voivat tarjota L2 Virtual Private Network -palveluita (L2 VPN) asiakkailleen. VPLS-tekniikka pohjautuu MPLS-tekniikkaan, ja asiakkaiden näkökulmasta VPLS-verkko on yksi kytkin toimipisteiden välissä. Jokaisella VPLS-palveluinstanssilla on oma välitystaulu, johon palveluntarjoajan verkkolaitteet oppivat asiakkaiden MAC-osoitteet. VPLS-tekniikka voidaan toteuttaa kahdella tavalla. RFC 4761 -standardin mukaisessa toteutuksessa hyödynnetään Border Gateway Protocol -protokollaa (BGP) signaloimaan ohjaustietoja sekä muiden VPLS-palveluinstanssiin osallistuvien laitteiden löytämiseen. RFC 4762 -standardin mukaisessa toteutuksessa ei ole toisten reitittimien automaattista löytämistä ja ohjaustietojen signalointiin käytetään Label Distribution -protokollaa (LDP). Kumpikin toteutustapa edellyttää, että palveluntarjoajan verkossa käytetään MPLS-tekniikkaa. [9]–[11]

RFC 4761 -standardin mukaisessa toteutuksessa ohjaustasolla on kaksi pääasiallista toimintoa: toisten VPLS-palveluinstanssiin osallistuvien reitittimien löytäminen ja ohjausliikenteen signalointi. Molemmat toiminnot toteutetaan yhdellä BGP Update -viestillä. Samaan VPLS-palveluinstanssiin osallistuvien laitteiden automaattinen havaitseminen on hyödyllinen toiminallisuus, koska kaikkien saman palveluinstanssin reunakytkinten välillä pitää olla MPLS-yhteys. Tämä tarkoittaa sitä, että jos käytössä ei ole toisten reitittimien automaattista havaitsemista, tulee jokaiselle VPLS-palveluinstanssiin osallistuvalle reitittimelle määrittää tieto kaikista muista reitittimistä, joissa on käytössä sama palveluinstanssi. Mikäli reitittimien automaattinen havaitseminen on käytössä, muutokset tulee tehdä ainoastaan laitteeseen, joka lisätään tai poistetaan VPLS-palveluinstanssista. RFC 4761 -standardin käyttäminen edellyttää kuitenkin sitä, että BGP-protokolla on otettu verkossa käyttöön. [9], [11]

Ohjausliikenteen signaloinnin tehtävä on sama riippumatta siitä onko käytössä RFC-standardin 4761 vai 4762 mukainen toteutus. Kun MPLS-verkon reunalaite (PE) havaitsee toisen PE-laitteen, joka on samassa VPLS-palveluinstanssissa, tulee näiden laitteiden kyetä luomaan, ja myöhemmin poistamaan, instanssin palveluleima laitteiden välille. Nämä instanssien palveluleimat ovat MPLS-leimoja, joiden avulla tunnistetaan, mikä PE-laite on lähettänyt kehyksen ja mihin VPLS-palveluinstanssiin kehys kuuluu. VPLS-instanssin palveluleima mahdollistaa liikenteen multipleksoinnin toteuttamisen. Kuitenkin riippumatta käytetystä standardista, VPLS-tekniikan vaatima looginen täyskytkentäisyys VPLS-palveluinstanssiin osallistuvien reitittimien välillä aiheuttaa skaalautuvuusongelmia suurissa verkoissa. [9]–[11]

Välitystasot ovat sekä RFC 4761 että RFC 4762 -standardiin pohjautuvassa toteutuksessa lähes identtiset. Välitystasolla on kaksi päätehtävää: kehysten välittäminen VPLS-palveluinstanssissa ja kehysten kapselointi MPLS-verkossa kuljetettavaksi. Kapseloinnissa asiakkailta saapuneisiin kehyksiin lisätään kaksi MPLS-leimaa. Pääl-

limmäinen leima leimapinossa on välitysleima ja pohjimmainen VPLS-instanssin palveluleima. Jokaiselle VPLS-palveluinstanssille luodaan oma välitystaulu (Forwarding Information Base, FIB). Tämän välitystaulun ja instanssin palveluleiman perusteella reitittimet kykenevät määrittämään, mille VPLS-palveluinstanssin reitittimelle niiden on välitettävä tiettyyn MAC-osoitteeseen suunnattu kehys. [9]–[11]

Kun asiakaslaite siirtyy yhdeltä reitittimeltä toiselle reitittimelle, MAC-osoitteiden uudelleenoppimisen nopeus on merkittävää, jotta asiakasliikenteen välitys keskeytyisi mahdollisimman lyhyeksi aikaa. RFC 4762 -standardissa on esitetty uusi MAC List TLV -elementti, jonka avulla voidaan poistaa tiettyjä MAC-osoitteita toisten laitteiden välitystauluista. Laitteet, jotka eivät ymmärrä kyseistä elementtiä, eivät välitä siitä. Vastaanotettua elementtiä ei myöskään lähetetä edelleen. Tämä toiminnallisuus nopeuttaa MAC-osoitteiden uudelleenoppimista, ja sitä voidaan käyttää myös VPLS-palveluissa, joissa on reitittimiä, jotka eivät tue toiminnallisuutta. [10]

Kun verkkoon ollaan luomassa VPLS-palvelua, on tärkeää huomioida standardien erot. RFC 4761 -standardin mukainen toteutus vaatii enemmän konfigurointia, mutta skaalautuu helpommin johtuen muun muassa muiden laitteiden automaattisesta tunnistamisesta. RFC 4762 -standardin mukainen toteutus voidaan toteuttaa pienemmällä konfigurointimäärällä, mutta toteutuksessa joudutaan määrittämään kaikki VPLS-palveluinstanssiin osallistuvat naapurit kaikille palveluun osallistuville reitittimille. Tämän lisäksi on tärkeää huomioida se, mikä on käytettävissä olevien verkkolaitteiden valmistajan suosima toteutus. Esimerkiksi Juniper Networks suosittaa RFC 4761 -standardin mukaista toteutusta käytettäväksi, kun taas Extreme Networks suosittelee standardin RFC 4762 mukaista toteutusta. [11], [12]

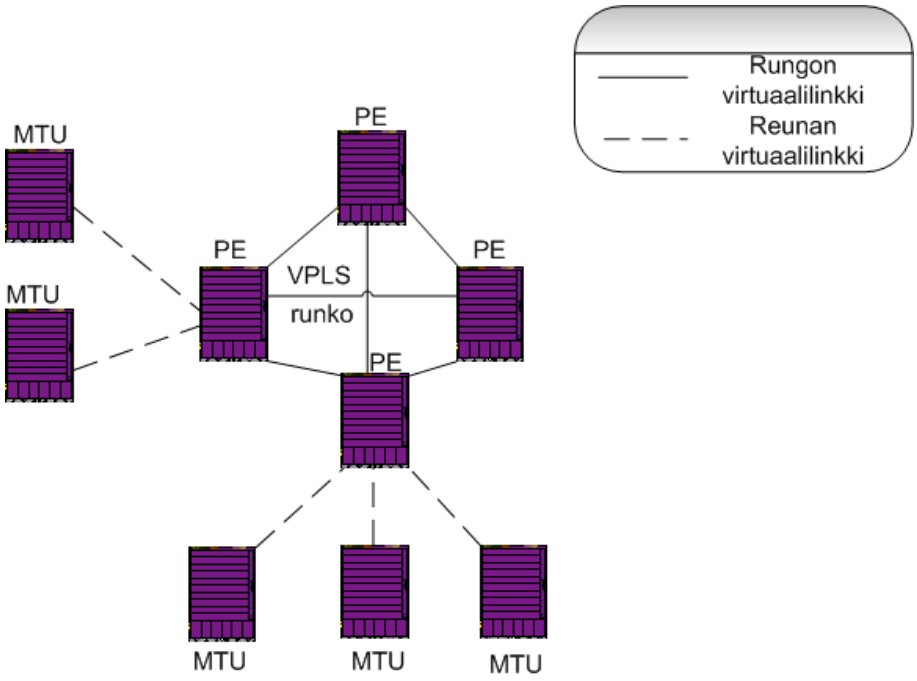
2.6 Hierarkkinen Virtual Private LAN Service

Hierarkkisella Ethernet-leimakytkennällä (H-VPLS) viitataan tekniikkaan, jonka avulla on mahdollista parantaa RFC 4762 -standardin mukaisen VPLS-toteutuksen skaalautuvuutta. RFC 4761 -standardin mukaista toteutusta voidaan parantaa hierarkkisella BGP VPLS -mallilla. Tässä hierarkkisessa BGP VPLS -tekniikassa hyödynnetään BGP-tekniikan reittien peilausta (Route Reflector, RR) ja reittien suodatusta (Route Target Filtering, RTF). Näitä ominaisuuksia hyödyntämällä hierarkkisessa BGP VPLS -tekniikassa voidaan yksinkertaistaa laitteiden lisäämistä tai poistamista VPLS-palveluinstanssiin, toteuttaa palvelu ilman täysikytkentäisyyttä ja rajoittaa viestien välitys ainoastaan vaadituille laitteille. Saman palveluinstanssin sisällä pitää kuitenkin edelleen olla MPLS-tason yhteys kaikkien verkkolaitteiden välillä. [9], [10]

H-VPLS -tekniikka määritetään LDP-protokollaa hyödyntävän VPLS-tekniikan kanssa samassa standardissa RFC 4762. H-VPLS -tekniikkaa käytettäessä täydellistä täysikytkentäisyyttä ei vaadita, ohjausliikenteen määrä pienenee sekä kehysten monistaminen vähenee. Nämä parannukset perustuvat siihen, että H-VPLS -tekniikassa verkon reunalla olevat laitteet (Multi-tenant unit, MTU tai spoke) ovat yhdistettyinä ainoastaan yhteen, tai redundanssin vuoksi useaan, VPLS-palveluinstanssin runkolaitteeseen. Nämä runkolaitteet ovat edelleen täysin kytkettyinä toisiinsa. Tällä tavalla saadaan muodostettua kaksitasoinen hierarkkisuus verkkoon ja saavute-

taan muun muassa seuraavat edut: täysikytkentäisyyttä ei vaadita kaikkien VPLS-palveluinstanssissa olevien laitteiden välillä, kytkinkohtainen signalointikuorma vähenee ja hierarkkisuudesta johtuen on mahdollista luoda usean palveluntarjoajan verkon lävitse kulkevia VPLS-palveluja. [10]

H-VPLS -tekniikassa käytetty verkkorakenne johtaa kuitenkin siihen, että kehysten välityssäännöt eivät ole samoja kaikilla laitteilla. VPLS-palveluinstanssissa olevat reitittimet eivät saa välittää toiselta reitittimeltä vastaanotettua yleislähetysliikennettä muille reitittimille johtuen verkon täysikytkentäisyydestä. Tämä välityssääntö on voimassa myös H-VPLS -tekniikalla toteutetuissa verkoissa. Sääntö kuitenkin eroaa siten, että yleislähetysliikenne on välitettävä kaikille reunalaitteille, jotka ovat yhteydessä runkoreitittimeen. Reunalaitteiden on puolestaan välitettävä yleislähetysliikenne aina kaikille laitteille, joihin sillä on yhteys. Kuvassa 6 on esimerkki hierarkkisesta VPLS-verkosta. VPLS-palveluinstanssin runkoverkon laitteita kuvataan termillä »PE» ja reunalaitteita termillä »MTU». Termillä »virtuaalilinkki» kuvataan välitysleimojen muodostamaa kokonaisuutta. [10], [13]



Kuva 6: Esimerkki H-VPLS -verkosta. [13]

2.7 Multiprotocol Label Switching: Transport Profile

Leimakytkentä keskitetyllä hallinnalla (Multiprotocol Label Switching: Transport Profile, MPLS-TP) on MPLS-tekniikkaan luotu uusi profiili. Tämän profiilin avulla voidaan parantaa MPLS-tekniikan siirtoverkko-ominaisuuksia. Parannus toteutetaan siten, että hyödynnetään osaa MPLS- ja GMPLS-ominaisuuksista sekä lisätään tekniikkaan uusia ominaisuuksia laajennusten avulla. Näiden laajennusten ansiosta MPLS- ja GMPLS-tekniikoiden protokollakokoelma laajenee niin, että tekniikkaa

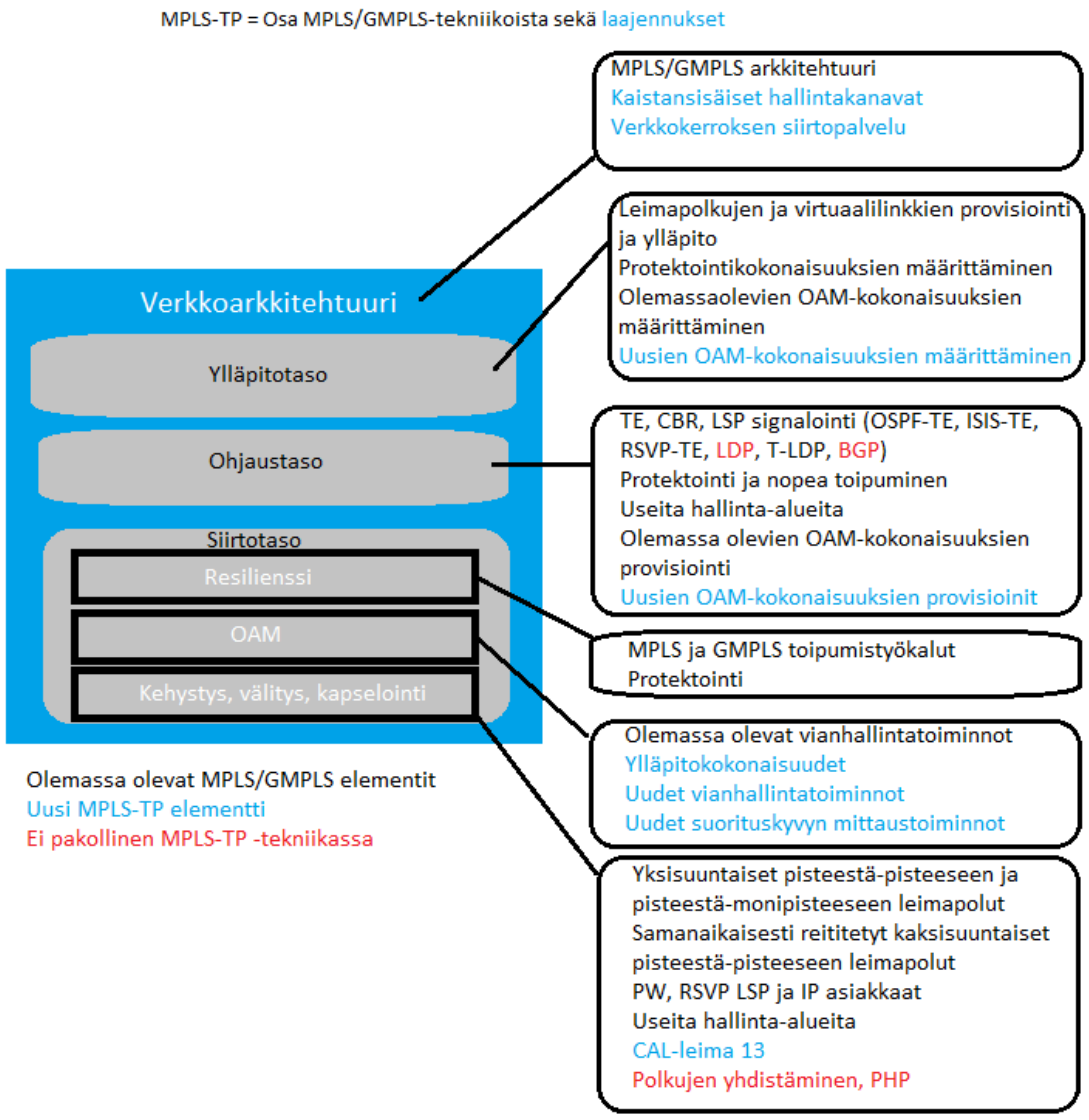
voidaan hyödyntää sekä palvelu- että siirtoverkoissa. IETF- ja ITU-T -organisaatiot ovat molemmat osallistuneet MPLS-TP -tekniikan standardointiin. [14]

Puhuttaessa MPLS-TP -tekniikasta, todellisuudessa viitataan kokonaisuuteen, joka muodostuu useasta protokollasta ja MPLS-protokollakokoelman laajennuksesta. Nämä laajennukset ja protokollat voidaan jakaa kategorioihin seuraavalla tavalla:

- Verkkoarkkitehtuuri, joka sisältää useiden funktioiden määritykset sekä näiden vuorovaikutukset
- Siirtotaso, joka sisältää protokollat ja mekanismit, joita käytetään kehysten välittämiseen ja joka jakautuu edelleen
  - Kehystys, siirto ja kapselointi
  - Kunnossapito eli Operations, administration and management -toiminnallisuus (OAM)
  - Toipuvuus
- Ohjaustaso (Control Plane, CP), joka sisältää protokollat ja mekanismit joilla signaloidaan välitysleimat
- Hallintataso (Management Plane, MP), joka sisältää protokollat ja mekanismit joiden avulla hallitaan verkkoa. [14]

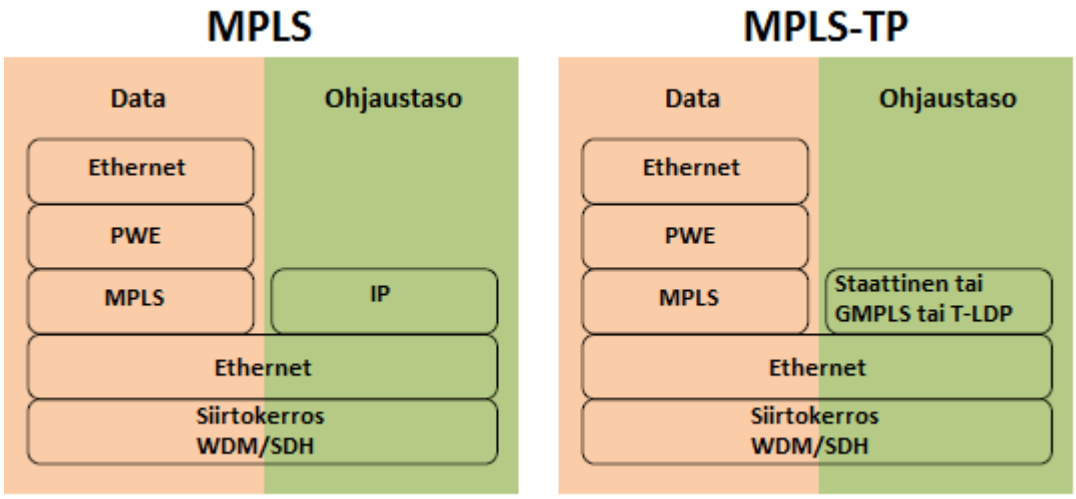
Siirtoverkoissa palvelutasosopimusten tarjoaminen ja valvominen on kriittistä. Toisin kuin MPLS-tekniikassa, perinteisissä siirtoverkoissa on käytössä laajat, vakiintuneet työkalut siirtoverkkojen valvontaan ja hallintaan. Tästä syystä merkittävä osa MPLS-TP -tekniikan esittämistä uudistuksista liittyy OAM-toiminnallisuuteen. OAM-toiminnallisuuksista on hyötyä myös niissä MPLS-verkoissa, joita ei käytetä siirtoverkkopalvelun tuottamiseen. Lisättävät OAM-toiminnallisuudet mahdollistavat vikojen havaitsemisen, vikojen paikallistamisen sekä suorituskyvyn valvonnan. Nämä toiminnallisuudet toteutetaan laajentamalla olemassa olevien MPLS-tekniikan työkalujen, kuten LSP Ping ja LSP Trace, ominaisuuksia.

Kuvassa 7 esitetään protokollia ja mekanismeja jaoteltuna yllä listattuihin kategorioihin. Kuvasta nähdään, mitkä toiminnallisuudet tulevat MPLS- tai GMPLS-tekniikasta, mitkä ovat uusia MPLS-TP -tekniikassa sekä mitä ei MPLS-TP -tekniikassa vaadita.



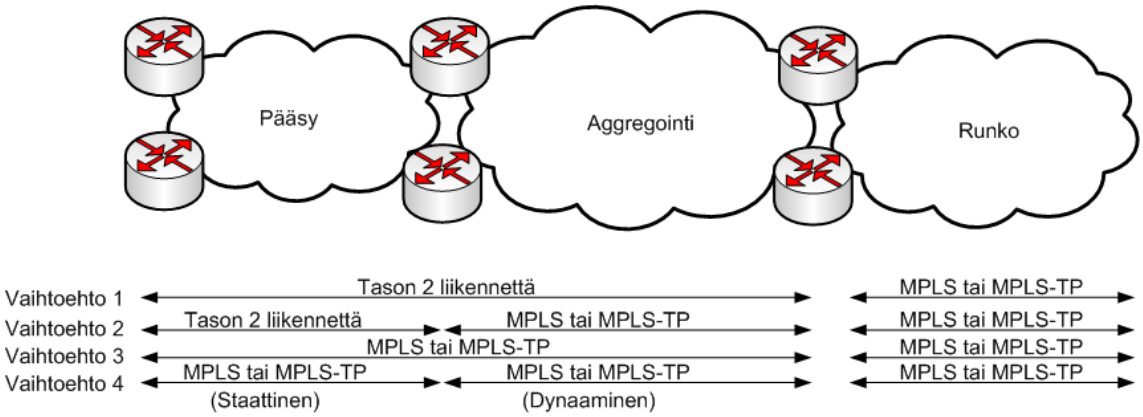
Kuva 7: MPLS- ja MPLS-TP -tekniikoiden komponentit. [14]

MPLS-tekniikassa ohjaustaso on vastuussa välitysleimojen signaloinnista. Ohjaustaso on dynaaminen ja sen toteuttamisessa on hyödynnetty IP-tekniikkaa. MPLS-TP -tekniikan ohjaustaso on kuitenkin toteutettu ilman IP-tekniikkaa. Merkittävä syy tähän on se, että nykyiset siirtoverkot hyödyntävät pääasiallisesti staattisia ohjaustasoja, joissa älykkään verkonhallintajärjestelmän avulla provisioidaan yhteydet piirikytkentäisesti. MPLS-TP -tekniikassa voidaan käyttää joko staattista tai dynaamista ohjaustasoa. Dynaaminen ohjaustaso skaalautuu paremmin kuin staattinen ja sen kanssa voidaan hyödyntää edistyneitä linkkien suojausmekanismeja. Dynaaminen ohjaustaso voidaan toteuttaa käyttämällä joko GMPLS- tai T-LDP -tekniikkaa. Kuvassa 8 esitetään MPLS- ja MPLS-TP -tekniikoiden siirto- ja ohjaustasojen rakenne. Siirtotasot (data) ovat keskenään yhteensopivia toisin kuin ohjaustasot. [14]



Kuva 8: MPLS- ja MPLS-TP -tekniikoiden ohjaustasojen erot. [15]

MPLS-tekniikka sisältää tehokkaat mekanismit liikenteen luotettavuuden varmistamiseksi. Näitä mekanismeja ovat muun muassa nopea uudelleenreititys ja polkujen suojaaminen. MPLS-TP -tekniikkaan lisätyillä OAM-viesteillä luotettavuutta voidaan parantaa edelleen, erityisesti pääsy- ja aggregointiverkoissa. Nämä OAM-viestit mahdollistavat sen, että reitittimet voivat ottaa vaihtoehtoisen välitysleiman käyttöön aiempaa nopeammin. Vaikka MPLS- ja MPLS-TP -tekniikoiden ohjaustasot eivät ole yhteensopivia, siirtotasojen yhteensopivuuden takia tekniikoita voidaan käyttää yhdessä. Erilaisia vaihtoehtoja tekniikoiden käyttämiseen yhdessä esitetään kuvassa 9. [14]



Kuva 9: Esimerkkejä MPLS- ja MPLS-TP -tekniikoiden käyttämiseen yhdessä. [14]

2.8 PB- ja VPLS-tekniikoiden vertailu

Tässä luvussa esitetään tekniikoiden PB ja VPLS vertailu. Tekniikat soveltuvat ominaisuuksiltaan parhaiten välityspalvelun toteuttamiseen ja vertautuvat esitetyistä

tekniikoista parhaiten keskenään. Luvussa esitetyt tiedot pohjautuvat mainittujen lähteiden lisäksi lukujen 2.2 ja 2.5 sisältöön sekä näiden lähteisiin.

2.8.1 Skaalautuvuus

Ethernet-alueverkkovälityksessä asiakkaiden määrää rajoittaa pääasiallisesti asiakasinstanssit toisistaan erottava SVLAN-tunniste. SVLAN-tunnisteen kooksi on määritetty 12 bittiä, joka tarkoittaa, että asiakastunnisteita on käytettävissä 2^{12} eli 4096 kappaletta. Näistä tunnisteet 0 ja 4095 on standardissa varattu, joten tunnisteita voi olla käytössä enintään 4094 kappaletta. Käytännössä tunnisteita ei ole käytössä näinkään monta, koska kaikki laitteet eivät tue näin montaa samanaikaista SVLAN-tunnistetta. Toinen skaalautuvuutta rajoittava tekijä johtuu Ethernetin MAC-osoitteiden hallinnasta. PB-tekniikassa palveluntarjoajan verkkolaitteet joutuvat oppimaan kaikki asiakaslaitteiden MAC-osoitteet SVLAN-tunnistekohtaisiin välitystauluihin. Yleisesti käytössä olevat kytkimet kykenevät oppimaan keskimäärin 4000 – 64 000 MAC-osoitetta välitystaulua kohden [16]. Välitystauluja on tyyppillisesti käytettävissä 256 – 4096 [16]. Pienissä verkoissa tämä ei johda ongelmiin, mutta suurissa verkoissa välitystaulut voivat täyttyä. [1], [3], [17]

SVLAN-tunnistetta käytetään asiakasinstanssien tunnistamisen lisäksi myös välityspolun tunnisteena. Tunnisteen käyttäminen kahteen tarkoitukseen johtaa siihen, että mikäli samalle asiakkaalle halutaan määrittää kaksi palveluinstanssia, joudutaan käyttämään kahta eri SVLAN-tunnistetta.

PB:n skaalautuvuutta rajoittaa käsiteltyjen asioiden lisäksi se, että tekniikka hyödyntää Spanning Tree -protokollaa. Spanning Tree -ratkaisut muodostavat välityspuut aina koko loogisen levitysalueen sisällä. Tämä johtaa siihen, että kun loogisessa levitysalueessa olevien laitteiden määrä kasvaa suureksi, Spanning Tree -protokolla hidastuu, koska välityspuiden käsittely muodostuu erittäin raskaaksi. Rapid Spanning Tree -protokollassa verkon ylläpitäjä voi konfiguroida signalointiviestien voimassaoloaikaa, joka rajoittaa sitä, kuinka monen laitteen läpi signalointiviesti voidaan välittää. Tämä taas rajoittaa välityspuun syvyyttä, eli sitä, kuinka monta verkkolaitetta loogiseen levitysalueeseen voi kuulua. [2]

VPLS:n edellyttämä looginen täysikytkentäisyys rajoittaa tekniikan skaalautuvuutta merkittävästi. Kun VPLS-palveluinstanssiin osallistuvia laitteita on huomattava määrä, neuvoteltavien välitysleimojen ja instanssin palveluleimojen lukumäärä on erittäin suuri. Kaavalla 1 voidaan laskea neuvoteltavien instanssileimojen lukumäärä, kun tiedossa on VPLS-palveluinstanssiin osallistuvien laitteiden lukumäärä n. Esimerkiksi VPLS-palveluinstanssi, jossa on neljäkymmentä reititintä, vaatii yhteensä 1560 instanssileimaa. [9], [11], [12], [13]

$$N = n(n-1). \tag{1}$$

Myös VPLS-tekniikassa palveluntarjoajan verkon reunalaitteet joutuvat oppimaan asiakaslaitteiden MAC-osoitteet. VPLS-tekniikassa MAC-osoitteiden oppimisessa noudatetaan samaa periaatetta kuin Ethernet-tekniikassa. Mikäli tiettyä MAC-osoitetta ei havaita tietyn ajan sisällä, poistetaan kyseinen osoite VPLS-palveluinstanssin välitystaulusta, jotta laitteen suorituskykyä voidaan säästää. Toinen toiminto, joka

kuluttaa huomattavasti reitittimien resursseja, on kehysten monistaminen. VPLS-tekniikassa reitittimen on välitettävä asiakkaalta vastaanotettu kehys kaikille VPLS-palveluinstanssiin osallistuville reitittimille, mikäli vastaanottajan sijainti ei ole reitittimen välitystaulussa. [9], [11], [12], [13]

Molemmat tekniikat skaalautuvat heikosti. PB:n suurimmat heikkoudet ovat palveluntarjoajan VLAN-tunnisteen rajoitukset sekä asiakaslaitteiden MAC-osoitteiden oppiminen myös runkolaitteiden osalta. VPLS-tekniikassakin on heikkoutena asiakaslaitteiden MAC-osoitteiden oppiminen. Tämän lisäksi VPLS:n heikkous on VPLS-palveluun osallistuvien reitittimien välille vaadittu looginen täysikytkentäisyys.

2.8.2 Hallittavuus

Ethernet-tekniikka perustui alussa sen käytön yksinkertaisuuteen. Ylläpitäjän ei tarvitse tehdä mitään vaan tekniikassa hyödynnettävä Spanning Tree -protokolla määrittää verkossa käytettävät polut siten, että silmukoita ei ole. Ethernet-verkossa ei saa olla silmukoita, koska kytkimillä ei ole keinoa havaita sitä, onko kytkin jo välittänyt kehyksen. Tätä periaatetta noudattaen ei ylläpitäjän tarvitse PB-tekniikalla toteutetussa verkossa määrittää kuin SVLAN-tunnisteet. Tämä kuitenkin johtaa siihen, ettei verkon ylläpitäjällä ole hyödyllisiä työkaluja verkon hallinnointiin. Ainut tapa, jolla verkon ylläpitäjä voi vaikuttaa polkujen muodostumisiin, on määrittää rajapintojen painoarvoja sekä kytkimien tunnistetietoja [18]. Tämä ei ole kuitenkaan hyvä tapa hallita verkkoa, koska saavutettu hyöty suhteessa vaadittuun työmäärään on erittäin pieni.

PB:n kehysmallissa on määritetty 3 bittiä prioriteetin osoittamiseen ja 1 bitti kuvaamaan kehyksen pudotuskelpoisuutta. Näistä arvoista seuraa se, että käytettävissä on kahdeksan liikenneluokkaa, joissa jokaisessa on matalan ja korkean todennäköisyyden pudotusprofiili. Lisäksi on yleistä, että palveluntarjoajilla käytössä olevat laitteet osaavat merkitä nämä arvot IP-paketin DSCP-arvojen perusteella ja osaavat muuttaa kehyksessä jo olevia prioriteettiarvoja. [19], [20]

PB:n palveluiden hallittavuudessa toistuvat samat ongelmat kuin verkon hallittavuudessa. Palveluntarjoajan VLAN-tunnisteiden avulla tunnistetaan sekä asiakkaiden palveluinstanssit, että loogiset levitysalueet. Tämä johtaa muun muassa siihen, ettei kahta palvelua voida määrittää kulkemaan eri polkuja verkon lävitse, koska Spanning Tree -protokolla todennäköisesti luo saman polun molemmille palveluille. [8], [20]

VPLS:n hallittavuus on PB-tekniikkaa parempi. VPLS-tekniikka pohjautuu MPLS-verkkoihin, jotka voidaan toteuttaa käyttämällä RSVP-TE -tekniikkaa. Tässä tekniikassa palveluntarjoajat voivat määrittää tarkat polut verkkonsa lävitse, jolloin verkosta saadaan hyvin deterministinen. RSVP-TE -tekniikan avulla myös laatua voidaan hallita tehokkaasti. Asiakasliikenne on selkeämmin eriytetty palveluntarjoajan liikenteestä VPLS-tekniikassa, koska asiakkaiden liikenne tunnistetaan MAC-osoitteiden sekä palveluinstanssin leimojen perusteella ja liikenteen välitys tapahtuu välitysleimojen perusteella.

PB:n hallittavuus on heikkoa. Verkko rakentuu automaattisesti Spanning Tree -protokollan mukaisesti, tehden polkujen määrittämisestä lähes mahdotonta. VPLS-tekniikassa on puolestaan mahdollista määrittää verkon läpi kulkevat polut täysin.

2.8.3 Toimintavarmuus

Spanning Tree -protokollan toiminnallisuuteen kuuluu se, että kun protokolla havaitsee verkko-ongelman, etsii se uuden polun rikkoutuneen tilalle, mikäli sellainen on olemassa. Perinteistä Spanning Tree -protokollaa nopeampi toipuminen voidaan saavuttaa Rapid Spanning Tree -toteutuksella. Tällä protokollalla ollaan päästy kymmeniä millisekunteja kestävään toipumiseen, kun ajastimet ovat olleet oikein mitoitettuja. Liikenteen välitys ei kuitenkaan ole toipunut yhtä nopeasti. Tämä johtuu siitä, että toipumiseen vaikuttaa myös laitteiston aiheuttamat viiveet, johon kuuluu linkin katkeamisen havaitseminen, porttien ja välitystaulun muokkaaminen sekä MAC-osoitteiden uudelleenoppiminen. Näiden toimintojen takia Rapid Spanning Tree -protokollaa käytettäessä kokonaistoipumisaika nousee satoihin millisekunteihin tai jopa sekunteihin ja tämäkin hyvin deterministisessä verkkotopologiassa, jossa on hyvin rajallisesti redundanssia. [2]

Spanning Tree -protokolla kykenee parantamaan vikasietoisuutta ainoastaan siten, että kytkimet ovat liitetty toisiinsa käyttäen useita rajapintoja, jotta vaihtoehtoinen polku on mahdollista löytää vikatilanteen sattuessa. Usea fyysinen silmukka johtaa kuitenkin raskaisiin laskutoimituksiin, kun välityspuuta lasketaan, mikä hidastaa verkon toipuvuutta huomattavasti.

VPLS-tekniikassa on mahdollista päästä erittäin nopeisiin toipumisaikoihin, mikäli sen perustana käytetyssä MPLS-verkossa on hyödynnetty RSVP-TE -tekniikkaa. RSVP-TE -tekniikan avulla voidaan luoda toissijaiset välitysleimat valmiiksi, jotta vikatilanteen sattuessa varayhteydelle siirtyminen olisi erittäin nopeaa. Koska polut voidaan määrittää valmiiksi, ei vikatilanteen sattuessa tarvitse suorittaa raskasta laskutoimitusta.

PB:n toimintavarmuus jää matalaksi huolimatta siitä, että Spanning Tree -protokolla pyrkii aina etsimään uuden polun vikatilanteen sattuessa. Toimintavarmuus on heikkoa, koska uuden polun määrittämiseen kuluva aika on liian pitkä palveluntarjoajan verkossa. VPLS-tekniikan toimintavarmuus on huomattavasti parempi, koska vikatilanteen sattuessa VPLS-tekniikan toipumisaika on huomattavasti PB-tekniikan toipumisaikaa nopeampi.

2.8.4 Tietoturvauhkat

Ethernet-alueverkkovälityksessä, kuten muissakin perinteisissä Ethernet-tekniikoissa, MAC-osoitteiden käsittely muodostaa mahdollisen tietoturvauhan. Tekniikan perusperiaatteena on se, että MAC-osoitteet opitaan välitystauluihin ja jollei vastaanottajan sijaintia tiedetä, tulvitetaan kehys kaikkialle. Tämä johtaa siihen, että käyttäjä voi tahallisesti tai tahattomasti luoda verkkoon erittäin suuren määrän liikennettä. Vastaavasti käyttäjä voi tahallisesti, tai tahattomasti, vaihtaa omaa MAC-osoitettaan jokaiseen lähetettyyn kehykseen, jolloin kytkinten välitystaulut täyttyvät erittäin nopeasti. Tällainen palvelunestohyökkäys voidaan estää poistamalla MAC-osoitteiden oppiminen ja määrittämällä mitkä MAC-osoitteet ovat missäkin rajapinnassa. Tällainen toiminnallisuus ei kuitenkaan ole realistinen PB-tekniikkaa käyttävän palveluntarjoajan verkossa.

Ethernet-alueverkkovälitys hyväksyttiin standardiksi vuonna 2005 [17]. Tämän

lisäksi Ethernet-tekniikalla on pitkä historia. Tekniikka on hyvin stabiili, eikä eri laitevalmistajien toteutusten välillä pitäisi olla merkittäviä eroja. PB-tekniikka tunnetaan hyvin, joten sen käyttäminen lisää verkon kompleksisuutta vain vähän.

VPLS-palveluinstanssiin osallistuvat reitittimet joutuvat oppimaan asiakaslaitteiden MAC-osoitteet. Tämä johtaa siihen, että myös VPLS-tekniikassa yksi mahdollinen hyökkäysvektori on MAC-osoitteiden tulvittaminen. VPLS-tekniikka tosin mahdollistaa sen, että opittavien MAC-osoitteiden lukumäärää voidaan rajoittaa VPLS-palveluinstanssikohtaisesti. Tällöin havaittu palvelunestohyökkäys voidaan rajata ainoastaan yhteen VPLS-palveluinstanssiin.

VPLS-tekniikassa tulvitetaan kehykset kaikille VPLS-palveluinstanssiin osallistuville reitittimille, jos vastaanottajan sijaintia ei tiedetä. Verkon kuormittamisen lisäksi tämä kuormittaa huomattavasti VPLS-palveluinstanssiin liikennettä välittävää reititintä, koska kyseinen reititin on vastuussa kehysten monistamisesta. Kuormitusta voidaan rajoittaa, mikäli verkkoon asetetaan kaistanleveysrajoituksia verkon lävitse kulkeville tunneleille. Vastaavasti reunalaitteen kuormitusta voidaan pienentää, mikäli verkossa on määritettynä tunneli joka suuntautuu pisteestä-monipisteeseen.

PB:n tietoturva on heikko. Mahdollinen hyökkääjä pystyy häiritsemään verkon toimintaa lähetettyjen kehysten MAC-osoitteita muokkaamalla. Verkon ylläpitäjällä ei ole hyviä työkaluja kyseisen hyökkäyksen estämiseen tai hillitsemiseen PB-tekniikassa. VPLS:n tietoturva on PB-tekniikan tietoturvaa parempaa, koska verkon ylläpitäjällä on paremmat mahdollisuudet rajata hyökkäyksen vaikutuksia. VPLS-palveluinstanssikohtainen MAC-osoitteiden oppimisen rajoittaminen ja verkkon tunneleiden kaistanleveyksien rajoittaminen mahdollistavat tilanteen hallitsemisen.

2.8.5 Liitettävyys

Ethernet-alueverkkovälityksen liikennettä voidaan tunneloida muiden tekniikoiden lävitse. Yksi esimerkki on siirtää PB:n liikennettä PBB:llä toteutetun verkon läpi [5]. PB-tekniikalla toteutetun verkon yhdistäminen toiseen PB-tekniikalla toteutettuun verkkoon on myös mahdollista. Tällöin verkkojen rajalla tulee hallita verkoissa käytössä olevat palveluntarjoajan VLAN-tunnisteet. SVLAN-tunnisteiden hallitseminen voi käydä erittäin kompleksiseksi, jos PB-tekniikalla toteutettu verkko liitetään useaan ulkopuoliseen verkkoon, jolloin rajapintoja verkkojen välillä on useita. Lisäksi ulkopuolisia verkkoja liitettäessä on otettava huomioon se, että MAC-osoitteiden lukumäärä saattaa kasvaa merkittävästi.

VPLS vaatii toimiakseen MPLS-tekniikalla toteutetun verkon. MPLS-verkot ovat levinneet laajalle ja ovat yleisessä käytössä. Usean palveluntarjoajan verkon lävitse kulkeva VPLS-palveluinstanssi on mahdollista toteuttaa. Tällöin kuitenkin suositellaan, että verkkojen välinen signalointi toteutetaan RFC 4761 -standardin mukaisella toteutuksella. Tämä suositus johtuu siitä, että kyseisessä standardissa on paremmat toiminnallisuudet tiedonvaihdon hallintaan verrattuna RFC 4762 -standardin mukaiseen toteutukseen. Toimialueiden sisällä voidaan käyttää kumman tahansa standardin mukaista toteutusta. [21]

2.9 PBB- ja H-VPLS -tekniikoiden vertailu

Tässä luvussa esitetään tekniikoiden PBB ja H-VPLS vertailu. Tekniikoita voidaan käyttää sekä välityspalvelun että siirtopalvelun toteuttamiseen, ja ne vertautuvat esitetyistä tekniikoista parhaiten keskenään. Luvussa esitetyt tiedot pohjautuvat mainittujen lähteiden lisäksi lukujen 2.3 ja 2.6 sisältöön sekä näiden lähteisiin.

2.9.1 Skaalautuvuus

Hajautetun hallinnan Ethernet-runkoverkkovälityksen skaalautuvuus on parantunut merkittävästi verrattuna Ethernet-alueverkkovälitykseen. Asiakkaiden palveluinstanssit erotetaan toisistaan käyttämällä ISID-tunnistetta SVLAN-tunnisteen sijasta. Tämä mahdollistaa sen, että asiakkaiden palveluinstansseja voi olla 2^{24} eli noin 16 miljoonaa yhdessä PBB-tekniikalla toteutetussa verkossa. Toinen PB:n skaalautuvuutta rajoittanut asia on MAC-osoitteiden oppiminen. PBB-tekniikassa asiakaslaitteiden MAC-osoitteiden oppiminen on rajoitettu PBB:lla toteutetun verkon reunakytkimille. Verkon sisällä käytetään PBB-verkon kytkinten MAC-osoitteita, jolloin verkon sisällä olevien kytkinten tulee oppia vain hyvin pieni määrä MAC-osoitteita. [3], [5], [6]

PB-tekniikassa on myös se ongelma, että asiakkaiden palveluinstanssit sekä verkon loogiset välitysalueet tunnistetaan samalla palveluntarjoajan VLAN-tunnisteella. PBB-tekniikassa asiakkaiden palveluinstanssit tunnistetaan ISID-tunnisteen avulla ja loogiset välitysalueet BVLAN-tunnisteen avulla. BVLAN-tunnisteen kooksi on määritetty sama, kuin SVLAN-tunnisteen kooksi eli yhdessä PBB-tekniikalla toteutussa verkossa BVLAN-tunnisteita voi olla käytössä noin 4000 kappaletta. Yhteen BVLAN-tunnisteeseen voidaan kuitenkin assosioida monta ISID-tunnistetta. BVLAN-tunnisteilla muodostettujen loogisten verkkojen välityspolut muodostetaan käyttämällä Spanning Tree -protokollaa. [3], [5], [6]

PBB-tekniikassa MAC-osoitteiden oppimisesta johtuva skaalautuvuusongelma on onnistettu rajoittamaan ainoastaan PBB-verkon reunakytkimille. Tämän ansiosta verkon reunalaitteet voidaan mitoittaa MAC-osoitteiden oppimisen perusteella ja verkon keskellä olevat kytkimet välityskyvyn perusteella. Verkon kokoa rajoittaa kuitenkin edelleen se, että tekniikassa käytetään Spanning Tree -protokollaa. Tämä protokolla rajoittaa verkon maksimisyvyyttä, eli sitä kuinka monen kytkimen lävitse liikennettä voidaan siirtää. Tämän lisäksi kehykset, joiden vastaanottajan sijaintia ei tiedetä, tulvitetaan koko asiakaspalveluinstanssin sisällä, jolloin verkkoon voi olla mahdollista aiheuttaa palvelunesto. [8]

Hierarkkisen Ethernet-leimakytkennän avulla voidaan pienentää vaadittujen instanssileimojen määrää huomattavasti Ethernet-leimakytkentään verrattuna. Instanssileimojen lukumäärä N voidaan laskea H-VPLS -tekniikassa kaavan 2 avulla. Kaavassa n on runkoverkon, eli täysikytkettyjen, laitteiden lukumäärä. Symboli m kuvastaa reunalaitteiden lukumäärä, kun ne on kytkettyinä ainoastaan yhteen runkolaitteeseen. Jos käytössä on esimerkiksi 5 runkolaitetta joista jokaisessa on 10 reunalaitetta, niin VPLS-tekniikassa instanssileimoja tulee neuvotella 2450 kappaletta ja H-VPLS -tekniikassa vain 70 kappaletta. [12]

$$N = n(n-1) + m. \tag{2}$$

PBB-tekniikan skaalautuvuuden voidaan arvioida olevan keskitasoa. Asiakkaiden palveluinstanssien tunnisteita on käytössä noin 16 miljoonaa kappaletta ja asiakkaiden MAC-osoitteiden oppiminen on rajoitettu PBB-verkon reunakytkimille. Välityspolut kuitenkin rakennetaan edelleen käyttäen Spanning Tree -protokollaa. H-VPLS -tekniikassa välitysleimojen määrää on saatu huomattavasti pienennettyä ja koko VPLS-palveluinstanssin laajuinen täysikytkentäisyys on poistettu.

2.9.2 Hallittavuus

Kuten luvussa 2.9.1 kerrottiin, Hajautetun hallinnan Ethernet-runkoverkkovälityksessä käytetään Spanning Tree -protokollaa välityspolkujen määrittämiseen. Tämä johtaa siihen, että verkon ylläpitäjällä on hyvin vähän mahdollisuuksia vaikuttaa välityspolkujen muodostumiseen. Palvelunlaadun määrittäminen ei ole muuttunut merkittävästi verrattuna Ethernet-alueverkkovälitykseen. Verrattuna PB-tekniikkaan palveluita on helpompi hallinnoida PBB-tekniikassa, koska palvelutunniste on eriytetty loogisen verkon tunnisteesta. Tämän lisäksi PBB-tekniikassa palveluntarjoajan ohjaustaso on eriytetty asiakkaan ohjaustasosta [8].

H-VPLS -tekniikan hallittavuus ei eroa merkittävästi VPLS-tekniikan hallittavuudesta. VPLS-palveluinstanssin asiakkaita lähellä olevien reunalaitteiden ei tarvitse olla tehokkaita, koska näiden tulee välittää kehykset ainoastaan H-VPLS -verkon rungossa toimiville reitittimille. Tästä syystä merkittävä osa verkon hallinnasta tapahtuu runkoreitittimiä konfiguroimalla, jolloin konfiguroitavien laitteiden lukumäärä on huomattavasti pienempi kuin VPLS-verkossa.

PBB-tekniikan hallittavuus jää matalaksi, koska verkon ylläpitäjällä on hyvin heikot mahdollisuudet vaikuttaa välityspolkujen muodostumiseen. Hallittavuus on kuitenkin parantunut PB-tekniikkaan verrattuna, koska asiakaslaitteiden MAC-osoitteet eivät näy verkon runkolaitteille, ja koska käyttöön on otettu palvelutunniste ISID sekä verkon loogisiin välitysalueisiin jakava BVLAN-tunniste. H-VPLS -tekniikan hallittavuus on hyvä eikä se eroa merkittävästi VPLS-tekniikan hallittavuudesta, koska molemmat tekniikat pohjautuvat MPLS-tekniikkaan.

2.9.3 Toimintavarmuus

Ethernet-runkoverkkovälitys hajautetulla hallinnalla on edelleen riippuvainen Spanning Tree -protokollan automaattisesta välityspolun uudelleenlaskemisesta. Kuten luvussa 2.8.3 kerrottiin, Rapid Spanning Tree -protokollan toipumisaika olisi kymmenissä millisekunneissa, jollei välitystaulujen muokkaaminen, MAC-osoitteiden uudelleenoppiminen ja rajapintojen muokkaaminen nostaisi toipumiseen kuluvaa aikaa.

PBB-tekniikalla toteutetun verkon vikasietoisuus on riippuvainen myös siitä, montako itsenäistä polkua voidaan pisteiden välille luoda. Vikatilanteiden havaitsemiseen voidaan käyttää 802.1ag eli Connectivity Fault Management -standardia, jos käytössä olevat laitteet tukevat kyseisen standardin käyttöä. Esimerkiksi Juniper Networksin laitteet, joilla voidaan toteuttaa PBB-tekniikkaan pohjautuva verkko, tukevat 802.1ag-standardia, jonka avulla voidaan valvoa verkkoa sekä eristää vikatilanteet. [6], [22], [23]

Asiakasta lähellä olevien reunalaitteiden luotettavuus on oleellinen Hierarkkisen Ethernet-leimakytkennän kokonaisluotettavuuden kannalta. Jos reunalaite on kytkettynä ainoastaan yhdellä linkillä VPLS-runkoverkon reitittimeen, menettää reunalaite kaiken yhteydellisyyden, mikäli tämä yhteys katkeaa. Tämä tilanne voidaan välttää kytkemällä reunalaite useaan runkoreitittimeen. Tällöin reunalaitteen vastuulla on määrittää, mikä linkki on ensisijainen, ja käyttää ainoastaan sitä. Kun käytössä oleva yhteys katkeaa, voidaan MAC-osoitteiden oppimista nopeuttaa käyttämällä aiemmin mainittua MAC List TLV -elementtiä. [10]

Kun reunalaitteen ja runkoreitittimien välillä on olemassa useampi kuin yksi linkki, on reunalaitteen vastuulla estää välityssilmukoiden muodostuminen. Tämä tapahtuu siten, että reunalaite hylkää kaikki toissijaisilta linkeiltä saapuvat kehykset. Vikatilanteen ilmaantuessa käytetty välitysleima vaihdetaan toissijaiseen, jo etukäteen signaloituun välitysleimaan. Näin on mahdollista päästä erittäin nopeisiin toipumisaikoihin. [12]

PBB:n toimintavarmuus jää matalalle tasolle, koska käytössä on Spanning Tree -protokolla. Spanning Tree -protokollan takia vikatilanteesta toipuminen on hidasta. H-VPLS:n toimintavarmuus on hyvä. Toiminnallisuus on käytännössä identtinen VPLS:n kanssa. Ainoana erona ovat asiakkaita lähellä olevat reunalaitteet, jotka voidaan liittää VPLS-runkoverkon reitittimiin useita linkkejä käyttämällä, jotta myös reunalaitteiden luotettavuus on riittävä.

2.9.4 Tietoturvauhkat

Hajautetun hallinnan Ethernet-runkoverkkovälityksessä MAC-osoitteiden oppimisesta johtuvat tietoturvariskit ovat pienentyneet huomattavasti verrattuna PB-tekniikkaan. Tämä on suoraa seurausta siitä, että PBB-tekniikassa ainoastaan verkon reunakytkimet oppivat asiakkaiden MAC-osoitteet. Asiakkaiden MAC-osoitteilla ei ole vaikutusta verkon keskellä toimiviin runkokytkimiin. Tämän ansiosta verkon reunalla toimivat kytkimet voidaan mitoittaa siten, että ne kykenevät oppimaan huomattavan määrän MAC-osoitteita. PBB-tekniikassa kehykset, joiden vastaanottajan sijaintia ei tiedetä, tulvitetaan kaikille asiakkaan palveluinstanssiin osallistuville kytkimille. Tästä syystä PBB on jossain määrin altis palvelunestohyökkäyksille.

H-VPLS -tekniikassa VPLS-runkoverkossa olevien reitittimien on opittava asiakaslaitteiden MAC-osoitteet niistä palveluinstansseista, joihin ne osallistuvat. Lisäksi liikenteen monistaminen on edelleen runkoverkon reitittimien tehtävä. H-VPLS -tekniikassa olevan runkoverkon osalta tietoturvauhkat eivät eroa VPLS:n tietoturvauhista. Asiakasta lähellä olevien laitteiden ei kuitenkaan tarvitse oppia yhtä suurta osaa asiakkaiden MAC-osoitteista, koska niiden tehtävä on välittää kehykset runkoverkon reitittimille. Reuna- ja runkoreitittimen välinen linkki saattaa olla altis palvelunestohyökkäykselle.

PBB:n tietoturva on keskitasoa. Asiakaslaitteiden MAC-osoitteiden oppimista on onnistuttu rajoittamaan huomattavasti ja ISID-tunnisteita käyttämällä asiakkaiden palveluinstanssit ovat selkeästi eroteltuna BVLAN-tunnisteista, joiden avulla verkko jaetaan useaksi loogiseksi välitysverkoksi. H-VPLS -tekniikassa tietoturvataso on hyvä. Reunalaitteiden ei tarvitse olla yhtä tehokkaita kuin runkoreitittimien, koska

näiden tulee oppia pienempi määrä asiakkaiden MAC-osoitteita.

2.9.5 Liitettävyys

PBB-tekniikalla toteutetun verkon liikenne voidaan tunneloida muiden verkkojen lävitse. Yksi esimerkki on siirtää PBB-verkon liikenne MPLS-tekniikalla toteutetun verkon lävitse [5]. PBB-tekniikalla toteutettujen verkkojen liittäminen toisiinsa on kuitenkin haastavaa. Jotta yhteydellisyys verkkojen välillä toimisi, tulee asiakkaiden palvelutunnisteiden ja välitystunnisteiden olla molemmissa verkoissa samat. Tämä edellyttää kommunikointia verkkojen ylläpitäjien välillä. Tällainen verkkojen yhteen liittäminen on virheherkkää. Toinen vaihtoehto kahden PBB-tekniikalla toteutetun verkon yhdistämiseksi on poistaa PBB:n kapselointi ja siirtää kehykset verkkojen välillä PB:n kapselointia käyttäen. Tällä tavoin molemmat verkot voivat käyttää omia ISID- ja BVLAN-tunnisteitaan.

H-VPLS:n liitettävyys ei eroa merkittävästi VPLS-tekniikan liitettävyydestä. Jos H-VPLS -tekniikalla toteutettu verkko liitetään toiseen VPLS-verkkoon, on edelleen suositeltavaa toteuttaa verkkojen välinen rajapinta RFC 4761 -standardin mukaisesti. Lisäksi, verkkojen välinen rajapinta sijaitsee todennäköisesti H-VPLS -verkon runkoreitittimessä, koska asiakkaita lähellä olevat reunareitittimet eivät yleensä ole tarpeeksi tehokkaita verkkojen yhdistämiseen.

2.10 PBB-TE- ja MPLS-TP -tekniikoiden vertailu

Tässä luvussa esitetään tekniikoiden PBB-TE ja MPLS-TP vertailu. Tekniikoiden pääasiallinen käyttötarkoitus on siirtopalvelun toteuttaminen ja ne vertautuvat esitetyistä ratkaisuista parhaiten keskenään. Luvussa esitetyt tiedot pohjautuvat mainittujen lähteiden lisäksi lukujen 2.4 ja 2.7 sisältöön sekä näiden lähteisiin.

2.10.1 Skaalautuvuus

Keskitetyn hallinnan Ethernet-runkoverkkovälityksessä runkoverkon MAC-kohdeosoite yhdessä BVLAN-tunnisteen kanssa edustaa tiettyä polkua PBB-TE -tekniikalla toteutetun verkon lävitse. Tämä mahdollistaa sen, että palveluntarjoajan verkkoon voidaan luoda useita erillisiä polkuja tietystä lähtöpisteestä tiettyyn päätepisteeseen. PBB-TE -tekniikassa, kuten PBB-tekniikassakin, voidaan siis käyttää yhtä BVLAN-tunnistetta useaan kertaan, koska se on merkityksellinen ainoastaan MAC-kohdeosoitteen kanssa. Asiakkaiden palveluinstanssit tunnistetaan edelleen ISID-tunnisteen avulla. Tekniikan toiminnallisuudesta seuraa se, että PBB-TE -tekniikan skaalautuvuus riippuu voimakkaasti siitä, mitä hallintajärjestelmää tai ohjaustason toteutusta tekniikan yhteydessä käytetään.

Keskitetyn hallinnan leimakytkennässä ei ole määritetty mitä ohjaustason tekniikkaa tulee käyttää. Tämän takia MPLS-TP -tekniikan skaalautuvuus riippuu siitä, mikä ohjaustason toteutus tai hallintajärjestelmä on valittu käyttöön. Lähtökohtaisesti tekniikan skaalautuvuus on kuitenkin hyvä.

2.10.2 Hallittavuus

PBB-TE:n hallittavuus on parantunut huomattavasti siksi, että Spanning Tree -protokollaa ei tekniikassa käytetä. Hallittavuutta rajoittavat kuitenkin ne rajoitukset, jotka käyttöön valitulla ohjaustasolla tai hallintajärjestelmällä ovat.

MPLS-TP -tekniikan hallittavuus riippuu voimakkaasti käyttöön valitusta hallintajärjestelmästä tai ohjaustasosta. MPLS-TP -tekniikkaan on kuitenkin lisätty useita OAM-tekniikan toiminnallisuuksia, joten yleisesti arvioiden MPLS-TP -tekniikan hallittavuus on hyvä.

2.10.3 Toimintavarmuus

PBB-TE:n toimintavarmuus on hyvä. Vikatilanteista toipuminen on nopeaa, koska käytössä ei ole enää Spanning Tree -protokollaa, vaan vaihtoehtoiset polut voidaan määrittää verkkoon ennen vikatilanteita. Lisäksi verkkoon voidaan luoda polku, joka kiertää ainoastaan vikaantuneen kohdan verkossa. Käytössä olevasta ohjaustasosta tai hallintajärjestelmästä riippuu se miten monta ja millaista toissijaista polkua voidaan verkkoon luoda ennalta. OAM-tekniikan viestit mahdollistavat vikatilanteiden nopean havaitsemisen ja paikallistamisen. Lisäksi OAM-viestit siirtyvät automaattisesti samoja polkuja asiakasliikenteen kanssa, koska ne käyttävät samoja runkoverkon MAC-kohdeosoitetta ja BVLAN-tunnistetta kuin asiakasliikenne.

MPLS-TP:n toipumismekanismit vastaavat lähes täysin MPLS:n toipumismekanismeja. Ne ovat siis erittäin hyviä. Näitä mekanismeja kyetään kuitenkin nopeuttamaan entisestään, kun käytössä ovat MPLS-TP -tekniikkaan lisätyt OAM-toiminnallisuudet. Näiden toiminnallisuuksien avulla vikatilanteet kyetään havaitsemaan ja paikallistamaan nopeasti.

2.10.4 Tietoturvauhkat

Keskitetyn hallinnan Ethernet-runkoverkkovälityksessä MAC-osoitteiden oppiminen ei ole käytössä. Tämän lisäksi myös kehysten tulvitus on pois käytöstä. Nämä kaksi asiaa johtavat siihen, että palvelunestohyökkäyksen tekeminen PBB-TE -verkkoa vastaan on huomattavasti haasteellisempaa kuin se on PB- tai PBB-tekniikalla toteutettua verkkoa vastaan. Välitystaso on myös eriytetty ohjaustasosta, jolloin ohjaustasossa tapahtuva toimintahäiriö ei pysäytä liikenteen välitystä. PBB-TE -tekniikan tietoturvaa suunniteltaessa on kuitenkin huomioitava myös käytetyn ohjaustason tai hallintajärjestelmän tietoturva, jottei verkkoa vastaan ole helppo hyökätä.

Keskitetyn hallinnan leimakytkennässä tietoturva on hyvin samanlainen kuin MPLS-tekniikassa. Koska MPLS-tekniikka on jo varsin kypsä, on sen tietoturva ehtinyt kehittymään hyvälle tasolle. Kuitenkin on huomioitava, että myös MPLS-TP -tekniikassa käyttöön valitun ohjaustason tai hallintajärjestelmän turvallisuus vaikuttaa koko verkkoon.

Molemmat tekniikat ovat siis voimakkaasti sidonnaisia käyttöön valitun hallintajärjestelmän tai ohjaustason tietoturvaan. Itse tekniikoissa ei ole tiedossa olevia merkittäviä haavoittuvuuksia.

2.10.5 Liitettävyys

PBB-TE -tekniikka pohjautuu Ethernetiin, ja tästä syystä tekniikan liikennettä voidaan siirtää millä tahansa alemman tason siirtotekniikalla, joka tukee Ethernetin liikenteen siirtoa. PBB-TE:n palveluihin voidaan liittää Ethernet-over-SDH -verkkoja tai PBB-TE -tekniikan liikennettä voidaan siirtää hyödyntämällä SDH- tai WDM-verkkoja. [3]

MPLS-TP:n liikennettä voidaan siirtää MPLS-tekniikalla toteutetussa verkossa, koska tekniikoiden siirtotasot ovat yhteensopivia. MPLS- ja MPLS-TP -tekniikoiden ohjaustasot eivät kuitenkaan ole yhteensopivia, joten eri tekniikoilla toteutettuja verkkoja ei voi »sekoittaa» keskenään.

2.11 Kirjallisuustutkimuksen perusteella tehdyn tekniikkavertailun yhteenveto

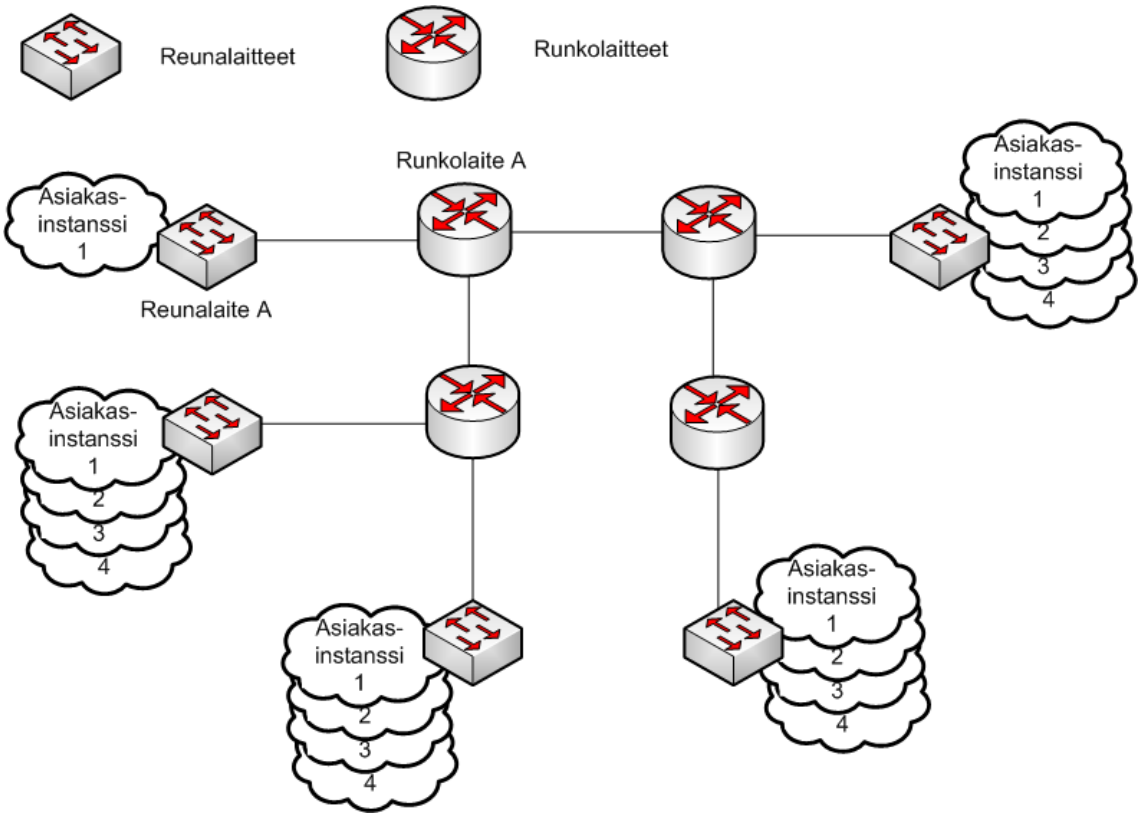
Taulukossa 1 esitetään yhteenveto kirjallisuustutkimuksen pohjalta tehdystä tekniikoiden vertailusta. Termillä »heikko» kuvataan kaikkein huonointa tasoa. Seuraavaa tasoa kuvataan termillä »matala». Termi »hyvä» on vertailun paras arvosana. Kenttä, jossa on kaksi arviointitermiä kauttamerkillä eroteltuna kuvastaa sitä, että ominaisuuden on arvioitu olevan näiden kahden arvosanan välillä.

Taulukko 1: Arviot eri tekniikoiden eri ominaisuuksista.

	Skaalautuvuus	Hallittavuus	Toiminta-varmuus	Tietoturva	Liitettävyys
PB	heikko	heikko	matala	heikko	matala
PBB	keskitaso	matala	matala	keskitaso	matala
PBB-TE	keskitaso/hyvä	keskitaso/hyvä	hyvä	hyvä	matala
VPLS	matala	hyvä	hyvä	keskitaso	matala/keskitaso
H-VPLS	keskitaso	hyvä	hyvä	hyvä	matala/keskitaso
MPLS-TP	keskitaso/hyvä	hyvä	hyvä	hyvä	keskitaso

Suurin painoarvo vertailussa annettiin skaalautuvuudelle. Kun tämä otetaan huomioon, parhaiten vertailussa menestyivät Ethernet-runkoverkkovälitys keskitetyllä hallinnalla (PBB-TE) ja Leimakytkentä keskitetyllä hallinnalla (MPLS-TP). Myös VPLS- ja H-VPLS -tekniikat menestyivät vertailussa yleisesti ottaen hyvin. Huonoiten menestyivät PB- ja PBB-tekniikat. Vertailussa havaittiin, että suuri syy näiden tekniikoiden heikkoon menestykseen on niiden riippuvuus Spanning Tree -protokollasta, joka ei sovellu hyvin palveluntarjoajien verkkoihin.

Taulukossa 2 esitetään paljonko reuna- ja runkolaitteiden välitystauluissa on kokonaisuudessaan palveluihin liittyviä asiakaslaitteiden MAC-osoitteita eri ratkaisuissa. Taulukon arvot on laskettu kuvan 10 mukaisesta esimerkkiverkosta, jossa on neljä asiaskasinstanssia. Jokaisessa instanssissa oletetaan olevan 5000 yksilöllistä MAC-osoitetta. Reunalaitteita on esimerkissä viisi kappaletta. Taulukon reunalaitteen A oletetaan palvelevan ainoastaan yhtä asiakasinstanssia.



Kuva 10: Esimerkkiverkko josta MAC-osoitteet lasketaan.

Taulukko 2: MAC-osoitetaulujen koot.

	Reunalaitteen A välitys-taulun asiakkaiden MAC-osoitteet	**Runkolaitteen A välitys-taulujen asiakkaiden MAC-osoitteet**
PB	5 000	20 000
PBB	5 000	0
PBB-TE	5 000	0
VPLS	5 000	0
H-VPLS	5 000	0
MPLS-TP	5 000	0

2.12 Tekniikkayhdistelmät

Tässä luvussa esitetään ratkaisuja, jotka toteutetaan käyttämällä aiemmin esiteltyjä tekniikoita samanaikaisesti. Käyttämällä kahta tekniikkaa samanaikaisesti, on mahdollista hyödyntää molempien tekniikoiden vahvuuksia siten, että toisen tekniikan heikkouksia paikataan toisen tekniikan vahvuuksilla. Usean tekniikan käyttäminen samanaikaisesti ei kuitenkaan ole täysin mutkatonta, koska tekniikoiden hallitsematon käyttäminen lisää verkon kompleksisuutta merkittävästi.

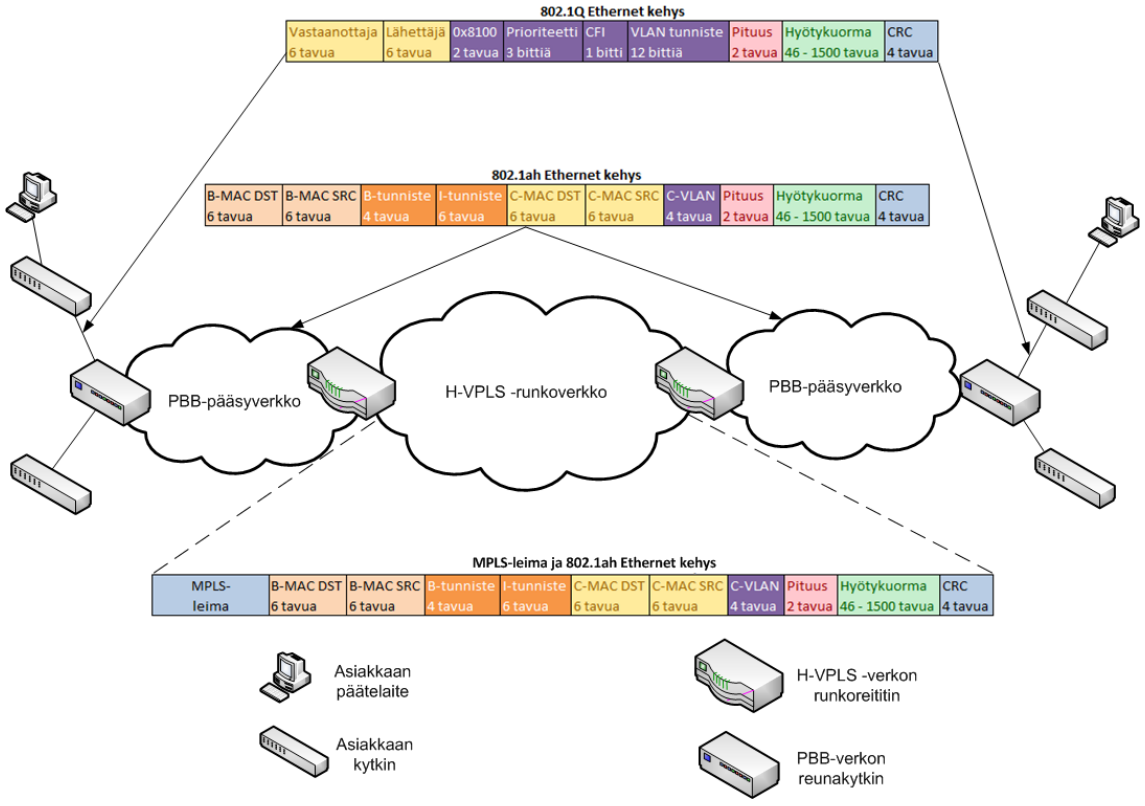
2.12.1 PBB ja H-VPLS

H-VPLS -tekniikan skaalautuvuutta voidaan parantaa entisestään, jos pääsyverkossa käytetään PBB-tekniikkaa. Asiakkaat voivat liittyä PBB-tekniikalla toteutettuun verkkoon käyttämällä PB- tai 802.1Q-tekniikkaa. Kytkimiin, jotka muodostavat PBB-tekniikalla toteutetun pääsyverkon, ei tarvitse tehdä muutoksia. Ne ainoastaan kapseloivat kehykset PBB-tekniikan kehysmuotoon, ja välittävät kehykset H-VPLS -tekniikalla toteutetun runkoverkon reunalle. Käytössä olevat palveluntarjoajan MAC-osoitteet ovat näiden kytkimien MAC-osoitteita. Kuvassa 11 esitetään kehyksen siirtoa PBB- ja H-VPLS -tekniikoilla toteutetun verkon lävitse. Kuvan esimerkissä asiakaskehykset ovat kapseloituna 802.1Q-tekniikan mukaisesti. PBB-tekniikalla toteutetun pääsyverkon reunakytkin kapseloi kehyksen PBB-tekniikan kehysmallin mukaisesti ja välittää kehyksen H-VPLS -tekniikalla toteutetun runkoverkon reunareitittimelle. Tämä reunareititin lisää kehykseen välitysleiman sekä instanssin palveluleiman, joiden perusteella kehys siirretään runkoverkossa. Verkon toisella laidalla kehyksen kapselointia puretaan aina, kun siirrytään tekniikkatasolta toiselle. [5]

PBB- ja H-VPLS -tekniikoiden yhteensopivuus riippuu pitkälti siitä, miten H-VPLS -verkon rakentavat reitittimet on toteutettu. Suurin osa nykyisin käytössä olevista MPLS-reitittimistä ei osaa käsitellä PBB-tekniikan kehysrakennetta. Yksinkertaisin tapa mahdollistaa PBB- ja H-VPLS -tekniikoiden käyttäminen yhdessä, on lisätä MPLS-reitittimiin mahdollisuus tunnistaa BVLAN-tunniste. Tällöin ainoa muutos on se, että H-VPLS hyödyntää BVLAN-tunnistetta SVLAN-tunnisteen tilalla, kun se erottelee asiakasrajapintoja. Tällöin MPLS-reitittimet eivät käsittele ISID-tunnisteita. [5]

Kehysten ei tarvitse aina kulkea H-VPLS -tekniikalla toteutetun verkon lävitse. Kehyksiä ei välitetä MPLS-reitittimelle, mikäli kehys voidaan välittää kohdeasiakkaalle siten, että molempia asiakkaita palvelevat kytkimet ovat kytkettyinä samaan PBB-tekniikalla toteutettuun pääsyverkkoon. [24]

Merkittävä haaste tekniikoiden käyttämisessä yhdessä on siinä, miten vikatilanteita hallitaan. Verkossa, joissa tekniikoita käytetään peräkkäin, on mahdollista, että yhden verkkotekniikan vikatilanne vaikuttaa toisen verkkotekniikan liikennevirtoihin. Esimerkiksi PB-tekniikalla toteutetussa pääsyverkossa tapahtunut vikatilanne voi johtaa siihen, että PBB-tekniikalla toteutetussa aggregointiverkossa asiakkaan liikenne vaihtuu yhdeltä BVLAN-tunnisteella erotellulta loogiselta välitysalueelta toiselle. Tällaisissa tapauksissa on tärkeää, että tiedot vikatilanteista ja niiden aiheuttamista muutoksista saadaan välitettyä koko verkkoon nopeasti. Toinen merkittävä



Kuva 11: Kehysten rakenteet verkossa, jossa pääsyverkko on toteuttu PBB-tekniikalla ja runkoverkko H-VPLS -tekniikalla. [5]

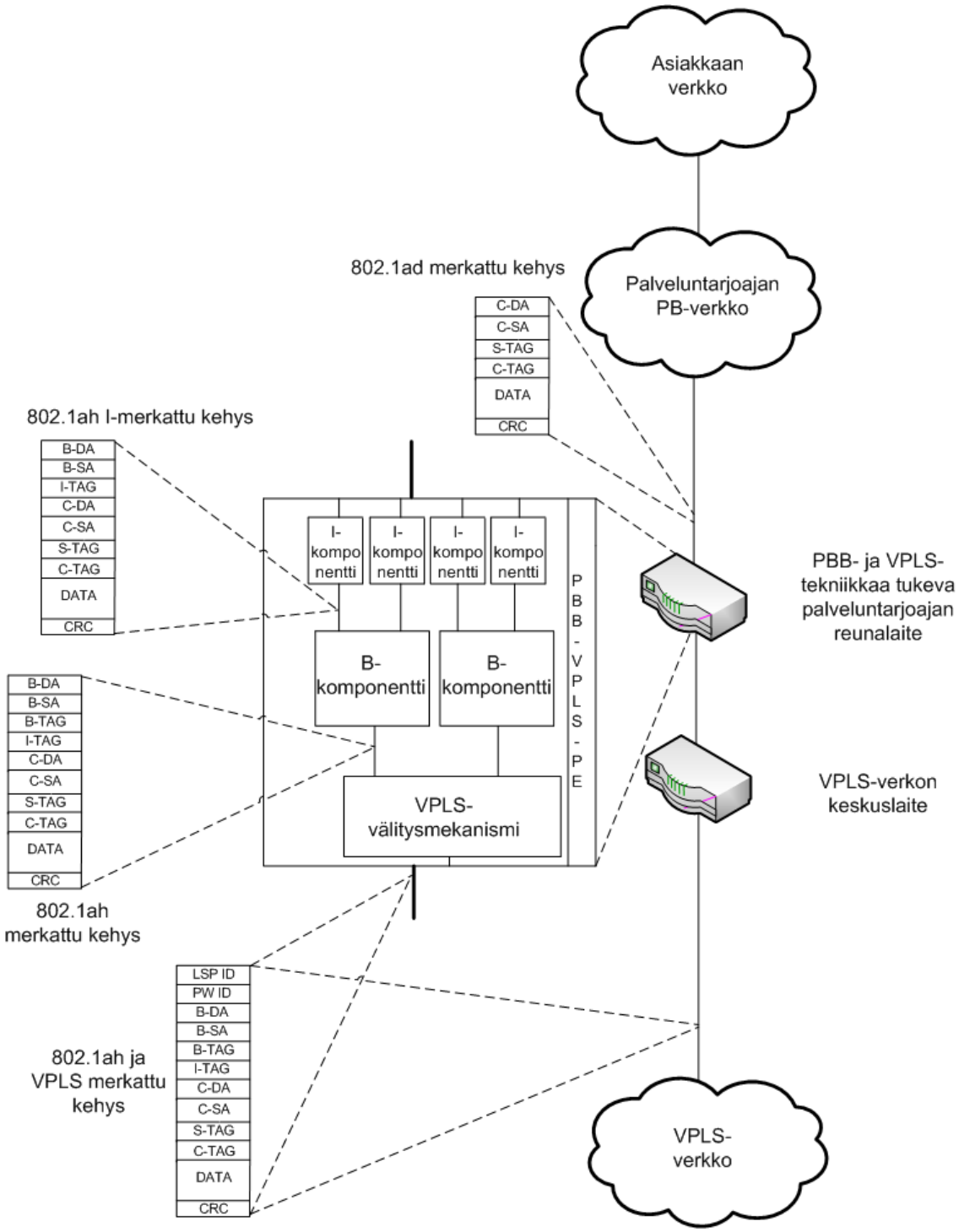
haaste on palvelunlaadun ylläpitäminen koko verkon lävitse. PB- ja PBB-tekniikassa käytetyt palvelunlaatutunnisteet on muunnettava H-VPLS -tekniikan käyttämäksi palvelunlaatutunnisteeksi ja päinvastoin. [24]

Mikäli verkkoon ei haluta lisätä erillistä PBB-tekniikalla toteuttua aggregointiverkkoa, sen toiminnallisuus voidaan sisällyttää myös H-VPLS -tekniikalla toteutetun verkon reunareitittimeen. Tällöin saavutetaan PBB-tekniikan edut MAC-osoitteiden oppimisen ja palveluinstanssien lukumäärien suhteen. Tällaista ratkaisumallia on ehdotettu RFC-standardiksi. Standardin vedos on nimeltään »Extensions to VPLS PE model for Provider Backbone Bridging» [26]. Tekniikassa reunareitittimen sisäinen rakenne on hyvin samanlainen PBB-tekniikan reunakytkimen sisäisen rakenteen kanssa, joka esitettiin kuvassa 5. Erona kytkimen sisäiseen rakenteeseen on se, että kun kehys on laitteen sisällä käsitelty B-komponentissa, kehys käsitellään vielä VPLS-välitysmekanismin mahdollistavassa komponentissa. B-komponentti voi siirtää kehyksiä reitittimen sisällä joko I-komponentille tai VPLS-välitysmekanismille. Tämä tarkoittaa sitä, että B-komponentti voi siirtää VPLS-välitysmekanismilta vastaanotetun kehyksen uudelleenkapseloinnin jälkeen takaisin VPLS-välitysmekanismille, jolloin uudelleenkapseloitu kehys siirretään taas H-VPLS -tekniikalla toteutetussa verkossa. Lisäksi B-komponentti voi välittää kehyksen suoraan toisen laitteen B-komponentille, jolloin kehys siirtyy samanlaisesti kuin PBB-tekniikalla toteutetussa verkossa. Tällaisen PBB- ja H-VPLS -tekniikan yhdistävän laitteen sisäistä

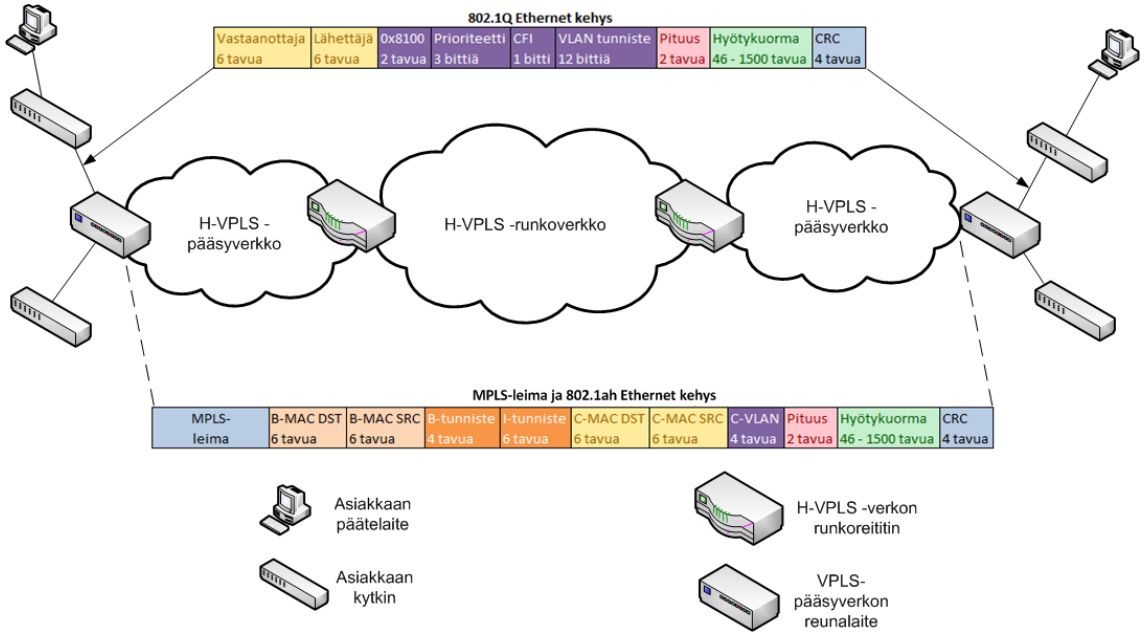
rakennetta esitetään kuvassa 12. [5], [24], [25], [26]

H-VPLS -tekniikalla toteutetussa verkossa looginen piste PBB-tekniikkaa tukevan MPLS-reitittimen sijoittamiseen on lähellä asiakkaita. Tällöin asiakaslaitteiden MAC-osoitteet näkyvät mahdollisimman pieneen osaan H-VPLS -tekniikalla toteutettua verkkoa. Samalla kaikki muut paitsi asiakasverkkojen reunoilla toimivat verkon reitittimet voivat olla perinteisiä MPLS-reitittimiä, jotka eivät pysty käsittelemään PBB:n mukaista kehysrakennetta. Tämä on mahdollista siksi, että asiakasverkkojen reunoilla olevat reitittimet lisäävät kehyksiin myös välitysleiman ja palvelun instanssileiman, joiden avulla kehys välitetään H-VPLS -verkossa. Verkon rakentaminen tällä tavalla johtaa kuitenkin siihen, että asiakasreunoilla olevien reitittimien on oltava tarpeeksi tehokkaita, jotta ne kykenevät kapseloimaan kehykset sekä PBB- että H-VPLS -tekniikoiden mukaisesti. Kuvassa 13 esitetään tällaisen toteutuksen kehysrakennetta ja kehysten välitystä. [5], [24], [25], [26]

PBB:n käyttäminen yhdessä H-VPLS:n kanssa tarjoaa useita etuja verrattuna siihen, että käytetään ainoastaan toista tekniikkaa. PBB:n ansiosta H-VPLS -verkon reitittimien tulee oppia huomattavasti vähemmän MAC-osoitteita, koska verkossa liikennöidään palveluntarjoajan MAC-osoitteiden perusteella. Jos H-VPLS -tekniikan reunareitittimet kykenevät käsittelemään ISID-tunnisteita, VPLS-palveluinstansseja voidaan luoda huomattavasti enemmän kuin käytettäessä SVLAN-tunnisteita. Lisäksi palveluntarjoaja voi liittää usean asiakkaan palveluinstanssin yhteen BVLAN-tunnisteeseen, jolloin H-VPLS -verkossa signaloitavien välitysleimojen ja instanssin palveluleimojen lukumäärä pienenee. [5], [24]



Kuva 12: MPLS-reititin, joka tukee myös PBB-tekniikkaa. [25]



Kuva 13: Kehysten rakenne ja välitys H-VPLS -verkossa, jossa reunalaite tukee myös PBB-tekniikkaa. [5]

2.12.2 PBB ja VPLS

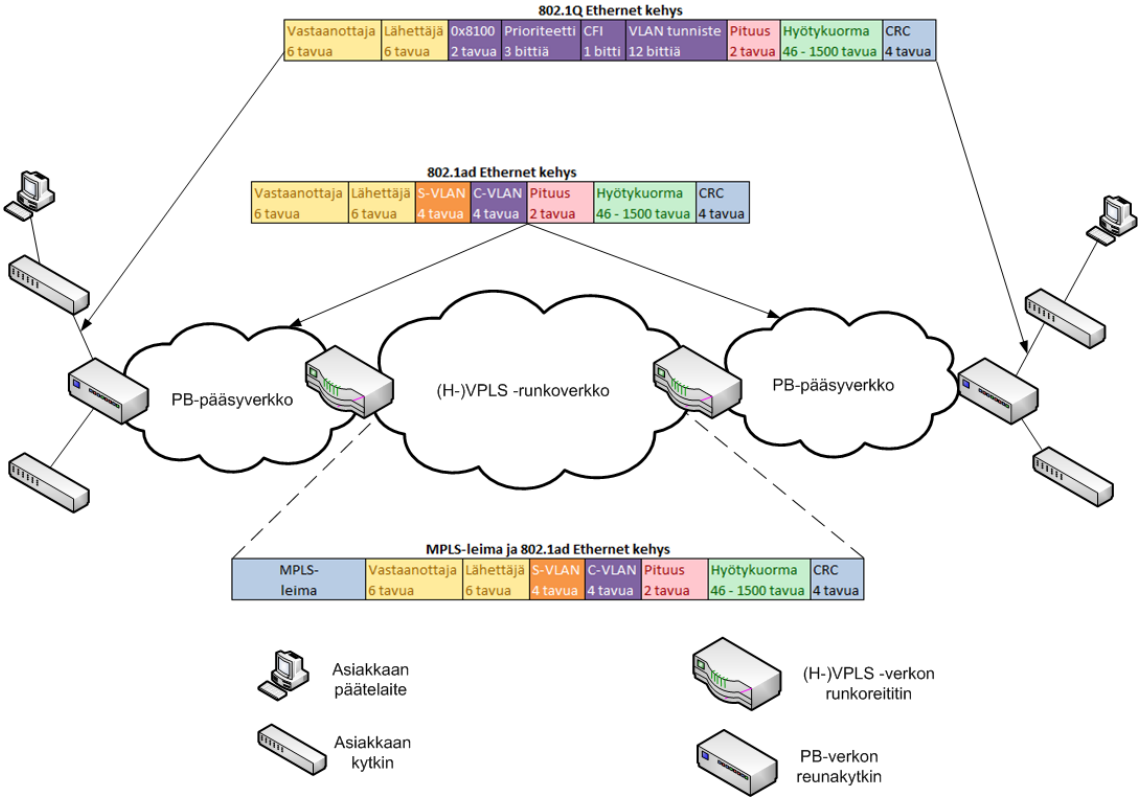
Jos Ethernet-runkoverkkovälitystä hajautetulla hallinnalla käytetään yhdessä Ethernet-leimakytkennän kanssa, tekniikkayhdistelmä ei eroa merkittävästi PBB- ja H-VPLS -tekniikoiden yhdistelmästä. Merkittävin ero on siinä, että PBB-VPLS -tekniikassa ei saavuteta yhtä suurta etua reitittimistä, jotka kykenevät toteuttamaan VPLS-tekniikan lisäksi PBB-tekniikan sisäisesti. Tämän lisäksi VPLS-tekniikka hyötyy PBB-tekniikasta H-VPLS -tekniikkaa enemmän. Tämä on seurausta siitä, että aggregoimalla eri asiakkaiden palveluinstansseja yhteen PBB-tekniikan avulla, VPLS-palveluinstansseja voidaan määrittää vähemmän käyttöön, kuin mitä tulisi käyttää ilman PBB-tekniikkaa. Tällöin signaloitavien palveluiden instanssileimojen lukumäärä pienenee.

PBB-tekniikka puolestaan hyötyy merkittävästi VPLS-tekniikan ominaisuuksista. PBB-tekniikalla luodut aggregointiverkot voidaan pitää pieninä, jolloin Spanning Tree -protokollan välityspuiden laskenta ei muodostu raskaaksi. Lisäksi liikenne on mahdollista siirtää VPLS-verkossa huomattavasti deterministisemmin, kuin olisi mahdollista vain PBB-tekniikalla toteutetussa verkossa. VPLS-verkossa tapahtuvat vikatilanteet voidaan kiertää huomattavasti PBB-tekniikassa tapahtuvia vikatilanteita nopeammin, jolloin verkon luotettavuus kasvaa verrattuna ainoastaan PBB-tekniikalla toteuttuun verkkoon.

2.12.3 PB ja VPLS

Tässä aliluvussa tarkoitetaan sekä VPLS- että H-VPLS -tekniikkaa, kun puhutaan VPLS-tekniikasta. Ethernet-alueverkkovälityksen yhdistäminen Ethernet-leimakyt-

kentään johtaa siihen, että PB-tekniikka hyötyy tekniikoiden yhdistämisestä huomattavasti enemmän kuin VPLS-tekniikka. Asiakasinstanssit yhdistetään VPLS-palveluinstansseihin SVLAN-tunnisteiden perusteella. Tämä johtaa siihen, että yhdellä VPLS-palveluinstanssilla voidaan palvella ainoastaan yhtä asiakasinstanssia. Lisäksi VPLS-tekniikan toteuttavat reitittimet joutuvat oppimaan kaikkien palvelemiensa asiakaslaitteiden MAC-osoitteet. Käytännössä PB- ja VPLS-tekniikoiden käyttäminen yhdessä on sama, kuin käytettäessä pelkkää VPLS-tekniikkaa. PB- ja VPLS-tekniikoiden avulla tehdyn kokonaistoteutuksen esimerkki esitetään kuvassa 14. [24]



Kuva 14: PB-tekniikalla toteutetut pääsyverkot yhdessä VPLS-tekniikalla toteutetun runkoverkon kanssa. [24]

Taulukossa 3 on listattu yhdistelmätekniikoiden käyttämisestä saavutettavia etuja. Taulukossa on yhdistettu PBB-VPLS sekä PBB-H-VPLS -toteutuksien edut, koska ratkaisut ovat lähes identtiset.

Taulukko 3: Yhdistelmätekniikoiden etuja.

PBB-(H)VPLS	**PB-VPLS**
VPLS-verkko ei näe asiakaslaitteiden MAC-osoitteita	PB-liikennettä kyetään siirtämään deterministisemmin
Signaloitavien palveluiden instanssileimojen määrä pienenee	
PBB-liikennettä kyetään siirtämään deterministisemmin	
PBB-verkot kyetään pitämään pieninä	

2.13 Katsaus optisiin siirtojärjestelmiin

Tässä luvussa luodaan katsaus optisiin siirtojärjestelmiin. Luku on jaettu alilukuihin siten, että luvussa 2.13.1 esitetään optisen tiedonsiirron perusteet. Luvussa 2.13.2 käsitellään nykyaikana yleisimmässä käytössä olevat optiset siirtojärjestelmät. Luvussa 2.13.3 esitetään optisia siirtojärjestelmiä, joita kehitetään nykyään. Luvussa 2.13.4 arvioidaan optisten siirtojärjestelmien tulevaisuutta.

2.13.1 Yleistä optisista siirtojärjestelmistä

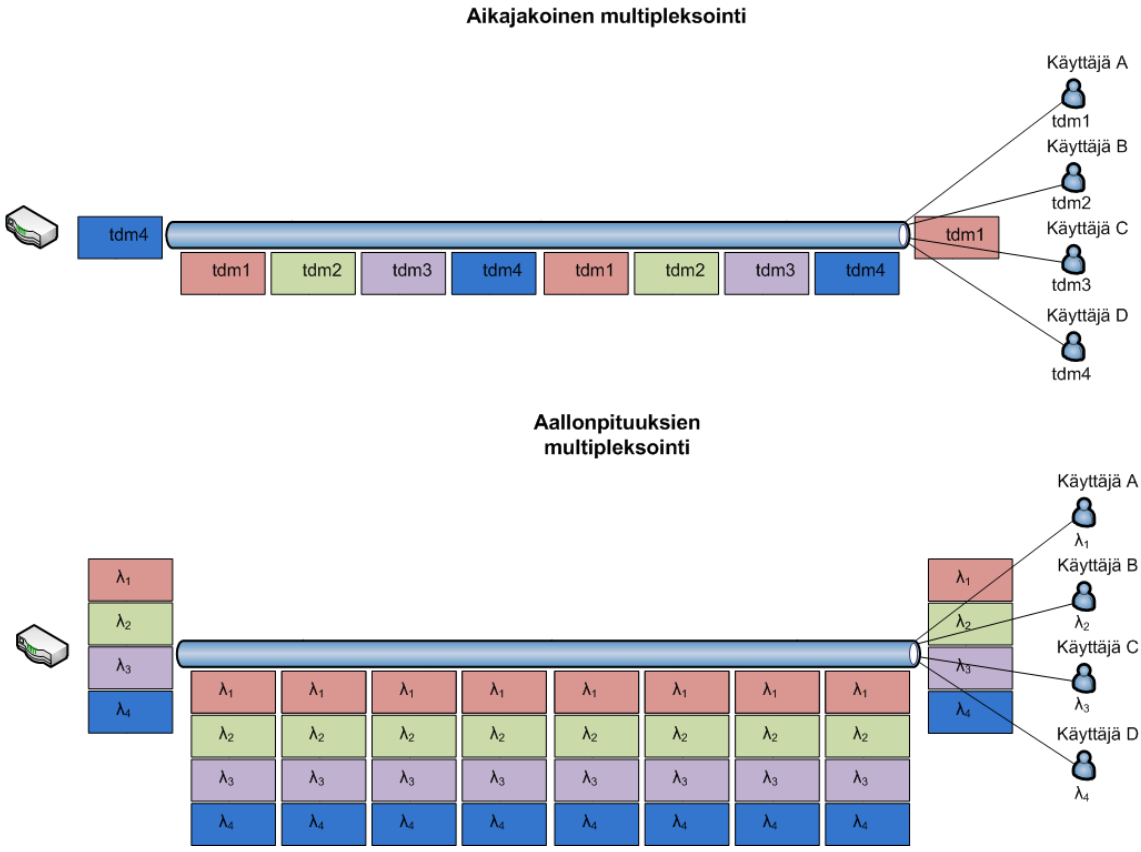
Optisilla siirtojärjestelmillä viitataan tekniikoihin, jotka mahdollistavat optisen tiedonsiirron. Optisissa verkoissa tiedonsiirto tapahtuu käyttämällä valosignaalia, joka siirretään valokuidussa. Valokuitu on erityisesti valmistettu siten, että kuidun ytimen ympärillä olevan vaipan taitekerroin on pienempi kuin ytimen taitekerroin. Tällöin suurin osa kuidussa siirretystä valosta ei pääse poistumaan kuidun ytimestä ennen valokuidun toista päätä. Valosignaalien yleisimmät aallonpituudet ovat joko noin 1550, 1300 tai 850 nanometriä. Kaikki aallonpituudet ovat ihmisen silmän näkemän valospektrin ulkopuolella, ja ne on valittu käyttöön siksi, että ne soveltuvat hyvin optiseen tiedonsiirtoon. [27]

Valokuidulla on tiettyjä etuja verrattuna perinteisiin siirtojärjestelmiin, joissa tieto siirretään käyttäen sähkösignaaleja mm. kuparikaapeleita pitkin. Optiset kuidut ovat täysin vapaita sähköisiltä häiriöiltä ja laadukkaat optiset kuidut eivät reagoi kosteuden tai lämpötilan muutoksiin. Optisten kuitujen siirtokapasiteetti on huomattavasti suurempi kuin esimerkiksi kuparikaapelin kapasiteetti. Kustannusten ollessa samat, valosignaalia voidaan siirtää huomattavasti pidemmälle optisessa kuidussa, kuin elektronista signaalia kuparikaapelissa. Lisäksi optista kuitua on käytännössä mahdotonta hyödyntää tai tarkkailla huomaamattomasti. [27]

Optisissa järjestelmissä käytettävillä valokuiduilla on kuitenkin myös heikkoutensa, joita ovat muun muassa: optiset kuidut on huomattavasti vaikeampi ja kalliimpi korjata kuin kuparikaapeli. Tietoliikennesignaali on muunnettava optoelektronisella muunnoksella elektronisesta muodosta optiseen, jotta se voidaan siirtää optisessa kuidussa. Tästä muunnoksesta seuraa viivettä Lisäksi optisten kuitujen asennus

vaatii erityistä suunnittelua, koska kuituja ei voi esimerkiksi taivuttaa yhtä jyrkästi kuin kuparikaapeleita. [27]

Koska optisten kuitujen kapasiteetti on niin suuri, on yleistä hyödyntää yhtä kuituparia useiden yhteyksien luomiseen. Tällöin kuituparin kapasiteetti on jaettava eri yhteyksien kesken. Yleisimmät menetelmät kapasiteetin jakamiseen ovat aikakytkentäinen multipleksointi (Time-Division Multiplexing, TDM) ja aallonpituuksien jakamiseen perustuva multipleksointi (Wavelength Division Multiplexing, WDM). Aikakytkentäisyyteen perustuvassa menetelmässä jokaisella yhteydellä on oma lyhyt aikaikkunansa, jonka aikana ne voivat käyttää kuitua liikenteen siirtämiseen. Aallonpituuksien multipleksointiin perustuvassa järjestelmässä käytetyn aallonpituuden ympärillä on määritetty kapeita aallonpituusikkunoita, jotka on allokoitu tiettyjen yhteyksien käyttöön. Molempia järjestelmiä voidaan laajentaa siten, että yhteydet voivat pyytää hallintajärjestelmältä resursseja käyttöön tarpeen mukaan. Kuvassa 15 on esitetty yksinkertaisten passiivisten TDM- ja WDM-toteutusten eroja.



Kuva 15: Aikaan ja aallonpituuksiin perustuvien multipleksointien erot.

Optiset siirtojärjestelmät ovat merkittävä osa nykyaikaisten verkkojen suunnittelua ja rakentamista. Näiden osuus tulee kasvamaan tulevaisuudessa, johtuen muun muassa valokaapelien teknisistä ja taloudellisista eduista kuparisiin parikaapeleihin verrattuna [28].

2.13.2 Optisten siirtojärjestelmien nykytilanne

Palveluntarjoajat ovat kyenneet parantamaan runkoverkon linkkien tehokkuutta. Tämä on ollut mahdollista hyödyntämällä nykyisin käytössä olevia passiivisia optisia tekniikoita. Lisäksi näiden optisten tekniikoiden käyttäminen on mahdollistanut myös sen, että pääsyverkkojen liityntänopeuksia on kyetty kasvattamaan. Nykytekniikkaa hyödyntämällä pääsyverkkojen kaistanleveyksiä ei kuitenkaan pystytä kasvattamaan niin paljoa, että ne riittäisivät uusien suurempia kaistanleveyksiä vaativien verkkosisältöjen hyödyntämiseen tehokkaasti. Tämä on seurausta muun muassa siitä, että kun pääsyverkkoja alun perin rakennettiin, tärkeintä oli kattaa suuret maantieteelliset alueet nopeasti pienillä kustannuksilla. Lisäksi loppukäyttäjien liikenneprofiilit olivat hyvin erilaiset, kun niitä verrataan loppukäyttäjien nykyaikaisiin liikenneprofiileihin. [29], [30]

Nykyisin käytössä olevat optiset järjestelmät pohjautuvat pääsääntöisesti joko Gigabit Passive Optical Network (GPON) tai Ethernet Passive Optical Network -tekniikkaan (EPON). Molemmat tekniikat ovat passiivisia ja ne hyödyntävät aikajaksoisuutta eri yhteyksien erotteluun. Passiivisuudella viitataan siihen, ettei laitteen tarvitse käsitellä siirrettävää liikennettä. Optinen signaali tai kuitupari ei välttämättä näy loppukäyttäjälle, vaan optinen signaali on voitu muuntaa elektroniseen muotoon ennen sen siirtoa loppukäyttäjälle. Passiivisten optisten verkkojen pääasiallinen tarkoitus on vähentää vaadittujen syöttökuitujen lukumäärää, kun palvellaan määritettyä määrää asiakasinstansseja. [29]

Ethernet Passive Optical Network (EPON) -tekniikka noudattaa IEEE-järjestön määrittelemää Ethernet-First-Mile (EFM) eli 802.3ah-standardia. EPON-tekniikka on otettu laajaan käyttöön Japanissa ja Koreassa. Gigabit Passive Optical Network (GPON) -tekniikka pohjautuu ITU-T -järjestön G.984-standardiin [31], ja se on laajemmin käytetty Yhdysvalloissa ja Euroopassa. Sekä EPON- että GPON-tekniikka käyttää aikajaksoista kanavointia eri liikennevirtojen erottamiseen. Tekniikat eroavat toisistaan hyötysuhteen, linjanopeuden, optisen yhteyden tehobudjetin ja tekniikan kokonaiskäyttökustannuksien suhteen. Lisäksi tekniikat eroavat sen suhteen, montako liikennevirtaa voidaan palvella yhdellä kuituparilla. [32]

EPON-tekniikka tukee natiivisti Ethernet-tekniikkaa liityntätekniikkana. Tästä syystä EPON-tekniikkaa käytettäessä yhden gigabitin Ethernet-rajapintojen kustannukset ovat pitkällä aikavälillä alhaisemmat verrattuna muihin tekniikoihin. Lisäksi EPON-tekniikka tukee 802.3ah-standardissa määritettyjä OAM-toiminnallisuuksia hyvin. Tämän ansiosta EPON-tekniikkaa voidaan hallita helposti homogeenisestä hallintajärjestelmästä. [32]

GPON-tekniikka puolestaan soveltuu EPON-tekniikkaa paremmin tilanteisiin, joissa on tuettava myös muita perinteisiä tekniikoita ja palveluita, kuin Ethernet-tekniikkaa. Tämä johtuu mm. GPON-tekniikan suuremmasta hyötysuhteesta. Lisäksi GPON-tekniikan avulla siirtoetäisyydet voivat olla suurempia kuin EPON-tekniikassa. GPON-tekniikka mahdollistaa ATM-, TDM- ja IP/Ethernet-tekniikoiden hyötykuormat, joten tekniikka mahdollistaa usean perinteisen tekniikan siirtämisen natiivisti. GPON-tekniikassa on myös EPON-tekniikkaa matalammat infrastruktuurin kustannukset, koska sen kaistanleveys on suurempi. [32]

Molemmat tekniikat hyödyntävät asiakkaalle suunnatussa liikenteessä aallonpituutta 1490±10nm ja asiakkaalta tulevalle liikenteelle aallonpituutta 1310±50nm. Lisäksi molempien tekniikoiden normaalit fyysiset maksimisiirtoetäisyydet ovat kaksikymmentä kilometriä. GPON-tekniikassa on kuitenkin mahdollista käyttää lisäprotokollaa, jonka avulla maksimisiirtoetäisyys voidaan kasvattaa kuuteenkymmeneen kilometriin. GPON-tekniikan suurin optinen tehobudjetti on 28,5dB, joka on 2,5dB enemmän kuin EPON-tekniikan suurin tehobudjetti. GPON-tekniikassa yhdellä kuituparilla voidaan palvella 64 liikennevirtaa, joka on kaksinkertainen verrattuna EPON-tekniikan tukemaan jakosuhteeseen. GPON-tekniikassa asiakkaalle siirretyn liikenteen kaistanleveys voi olla 1244Mb/s tai 2488Mb/s. Asiakkaalta vastaanotetun liikenteen kaistanleveys voi olla 155Mb/s, 622Mb/s, 1244Mb/s tai 2488Mb/s. EPON-tekniikassa kaistanleveys on molempiin suuntiin sama 1250Mb/s. GPON-tekniikan tehokkuuden keskiarvo on 93% ja EPON-tekniikan 55%. [32], [33]

EPON-tekniikka on kuitenkin GPON-tekniikkaa edullisempaa. Kun kustannukset normalisoidaan GPON-tekniikan kustannuksiin 20dB tehobudjetilla, EPON-tekniikan suhteellinen kustannus on vain 78% GPON-tekniikan kustannuksista. Tekniikoiden oleellisimmat yhtenäisyydet ja erot esitetään taulukossa 4. [32], [33]

Taulukko 4: EPON- ja GPON-tekniikoiden tärkeimmät ominaisuudet. [32], [33]

	EPON	**GPON**
Tekniikan käyttämä standardi	IEEE 802.3ah	ITU-T G.984
Suurin mahdollinen tehobudjetti	26dB	28,5dB
Pisin fyysinen siirtoetäisyys (looginen siirtoetäisyys)	20km (20km)	20km (60km)
Suurin mahdollinen jakosuhde	1:32	1:64
Tehon keskiarvo	n. 55%	n. 93%
Käytetyt aallonpituudet	1490±10nm / 1310±50nm	1490±10nm / 1310±50nm
Asiakkaalle siirretyn liikenteen kaistanleveys	1250Mb/s	1244Mb/s, 2488Mb/s
Asiakkaalta tulevan liikenteen kaistanleveys	1250Mb/s	155Mb/s, 622Mb/s, 1244Mb/s, 2488Mb/s
RF-ylätaajuudelle varattu aallonpituus	1555±5nm	1555±5nm
Normalisoitu kustannus	78	100

2.13.3 Katsaus optisten siirtojärjestelmien kehittymiseen

EPON- ja GPON-tekniikat ovat kasvattaneet loppukäyttäjien käytössä olevia kaistanleveyksiä huomattavasti. Tulevaisuudessa näiden tekniikoiden mahdollistamat kaistanleveydet eivät kuitenkaan riitä, koska tulevaisuuden palvelut, kuten Ultra High Definition Television tai IP-televisio, vaativat huomattavasti nykyistä suurempia kaistanleveyksiä. Palveluiden kehittymisen nopeuden perusteella voidaan arvioida, että käytössä olevat optiset tekniikat tulee uudistaa 1–5 vuoden sisällä. Tarkempi aikataulu riippuu verkon asiakasmäärästä, asiakkaiden liikenneprofiileista ja palveluiden kehittymisestä. [30], [34]

EPON-tekniikka on tarkoitus korvata 10G-EPON -tekniikalla. GPON-tekniikan korvaajaa on suunniteltu NG-PON -arkkitehtuurissa. Näiden kahden lisäksi on mahdollista siirtyä myös käyttämään WDM-PON -tekniikkaa, joka hyödyntää aallonpituuksiin pohjautuvaa multipleksointia. [34]

10G-EPON -tekniikan (IEEE P802.3av) suunnittelu alkoi IEEE-järjestössä syyskuussa 2006. Jo ennen tekniikan suunnittelun aloittamista, olemassa oli kuitenkin jo tekniikoita, joiden avulla EPON-tekniikan kaistanleveyksiä voitiin kasvattaa. Nämä »Turbo-EPON» -tekniikat olivat kuitenkin laitevalmistajakohtaisia, jonka takia ne eivät olleet levinneet laajalle. Käyttämällä 10G-EPON -tekniikkaa asiakasrajapintojen nopeus voidaan kasvattaa lähes kymmenkertaiseksi EPON-tekniikkaan verrattuna. Todellinen asiakasrajapintojen käytössä oleva kaistanleveys on noin 8,9Gb/s johtuen 10Gb/s kaistanleveydellä käytetystä virheenkorjauksesta. Lisäksi 10G-EPON -laitteiston ennustetaan seuraavan Ethernet-laitteiston hinnan ja kapasiteetin kehityskaarta, jolloin nykyiseen laitteistoon verrattuna kolminkertaisella kustannuksella saavutetaan kymmenkertainen kasvu kapasiteettiin. [34]

10G-EPON -tekniikka ei kuitenkaan ole täysin ongelmaton. Ongelmia, jotka on ratkaistava ennen kuin tekniikka voidaan ottaa käyttöön, ovat muun muassa tekniikan yhteensopivuus EPON-tekniikan kanssa. Toinen ratkaistava haaste on se, että 10G-EPON -tekniikassa kaistanleveydet ovat todella asymmetriset. Asiakasrajapintoihin siirretään liikennettä 10Gb/s mutta asiakasrajapinnasta vastaanotetaan liikennettä ainoastaan 1Gb/s. Lisäksi kaistanleveyden kasvattaminen lähes kymmenkertaiseksi aiheuttaa valon dispersoitumista ja vastaanottimien herkkyyden heikentymistä. [34]

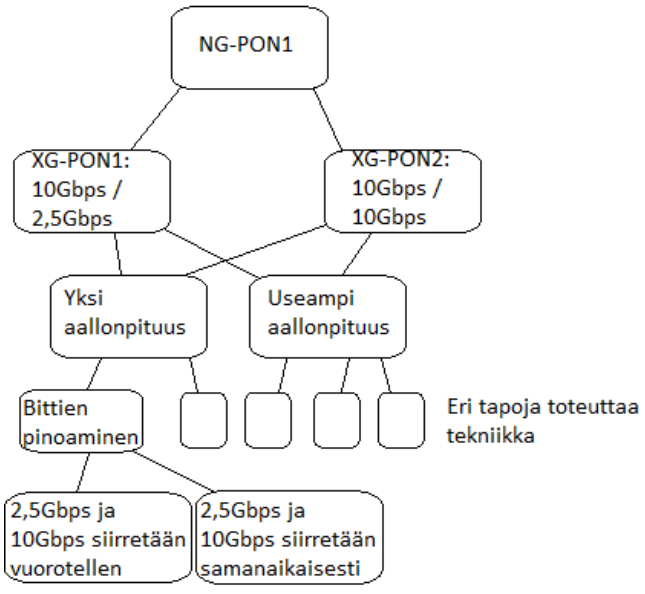
10G-EPON -tekniikan oleellisimmat yksityiskohdat ovat: asiakasrajapinnasta vastaanotettu liikenne käyttää aallonpituutta 1270±10nm. Asiakasrajapintaan siirretty liikenne käyttää aallonpituutta 1577,5±2,5nm. Käytetyt aallonpituudet mahdollistavat sen, että tekniikkaa voidaan käyttää rinnakkain EPON-tekniikan kanssa. Optiset laitteet voivat neuvotella verkkolaitteiden laserien käyttöajastuksen. EPON-tekniikassa on käytössä ainoastaan kiinteä 512 nanosekunnin ajastus. Virheenkorjaustekniikka on Forward Error Coding RS(255,223), joka korjaa virheitä tehokkaammin kuin EPON-tekniikassa käytetty tekniikka, mutta sen hukkakuorma on suurempi. [34]

ITU-T -järjestön standardoiman GPON-tekniikan seuraajaksi on suunniteltu NG-PON1 -tekniikka (G.987). NG-PON1 -tekniikkaa voidaan käyttää samanaikaisesti GPON-tekniikan kanssa, jolloin asiakasyhteyksiä voidaan siirtää NG-PON1 -tekniikkaan niin, ettei verkkoon tarvitse tehdä muutoksia tai muut asiakasyhteydet

katkea. NG-PON1 -tekniikan suunnittelussa on keskitytty pääasiallisten järjestelmän skaalautuvuuteen eli asiakasyhteysmäärien maksimointiin, palvelunlaatumääreiden parantamiseen sekä verkon turvaamiseen. Nämä ominaisuudet ovat rakennettu siten, että ne ovat suoria laajennuksia GPON-tekniikan vaatimuksille. [34]

NG-PON1 -tekniikka jaetaan kahteen aliryhmään: XG-PON1 ja XG-PON2. Nämä tekniikat eroavat toisistaan asiakasrajapinnasta vastaanotetun kaistanleveyden perusteella. XG-PON1 -tekniikassa asiakasrajapinnasta vastaanotetaan liikennettä 2,5Gbit/s ja XG-PON2 -tekniikassa kaistanleveydellä 10Gbit/s. Tekniikat voidaan jakaa edelleen ryhmiin sen perusteella, hyödyntävätkö ne yhtä vai useaa aallonpituutta. Järjestelmissä, jotka käyttävät useaa aallonpituutta, 10Gbit/s kaistanleveys saavutetaan yhdistämällä eri aallonpituuskanavien tiedonsiirto. Toteutus voi käyttää esimerkiksi 2,5Gbit/s kaistanleveyttä aallonpituuskanavalla, jolloin olemassa olevia GPON-järjestelmiä voidaan hyödyntää tehokkaammin kun palveluntarjoaja siirtyy NG-PON1 -tekniikkaan. [34]

Yhtä aallonpituutta käyttävät toteutuksetkin voidaan toteuttaa usealla eri tavalla. Yksi merkittävä tapa tällaisen järjestelmän toteuttamiseen on hyödyntää bittien pinoamista (bit stacking). Menetelmässä kaksi eri kaistanleveydellä toimivaa signaalia välitetään yhdellä aallonpituudella. Menetelmä kuitenkin rajoittaa optista tehobudjettia, jottei 10Gbit/s kaistanleveyttä hyödyntävä signaali peitä 2,5Gbit/s kaistanleveyden signaalia. Bittien pinoaminen voidaan toteuttaa kahdella tavalla. Ensimmäisessä tavassa molemmat tietovirrat siirretään samanaikaisesti. Tässä menetelmässä 2,5Gbit/s-signaalin modulaatioamplitudin on oltava 30% normaalia suurempi. Toinen tapa on siirtää tietovirrat eri aikaan. Tällöin haasteena on 2,5Gbit/s-signaalin amplitudin pienentäminen niin, ettei vastaanottimien synkronointi katkea eikä se häiritse toista signaalia. [34]



Kuva 16: Eri tapoja erotella NG-PON1 -tekniikan toteutustavat toisistaan.

NG-PON1 -tekniikka ei varsinaisesti ole vain yksi tekniikka, vaan se voidaan

toteuttaa usealla eri tavalla. Nämä toteutukset voidaan jakaa kategorioihin esimerkiksi sen perusteella paljonko liikennettä vastaanotetaan asiakasrajapinnasta. Tämän jaottelun jälkeen on vielä useita tapoja erottaa toteutukset toisistaan. NG-PON1 -tekniikkojen jaottelu on suhteellisen monimutkaista, joka voidaan havaita myös kuvasta 16, jossa esitetään eri tapoja eritellä NG-PON1 -tekniikan toteutukset toisistaan. Kuvassa ei esitetä kaikkia mahdollisia toteutuksia vaan annetaan ainoastaan yksinkertainen esimerkki.

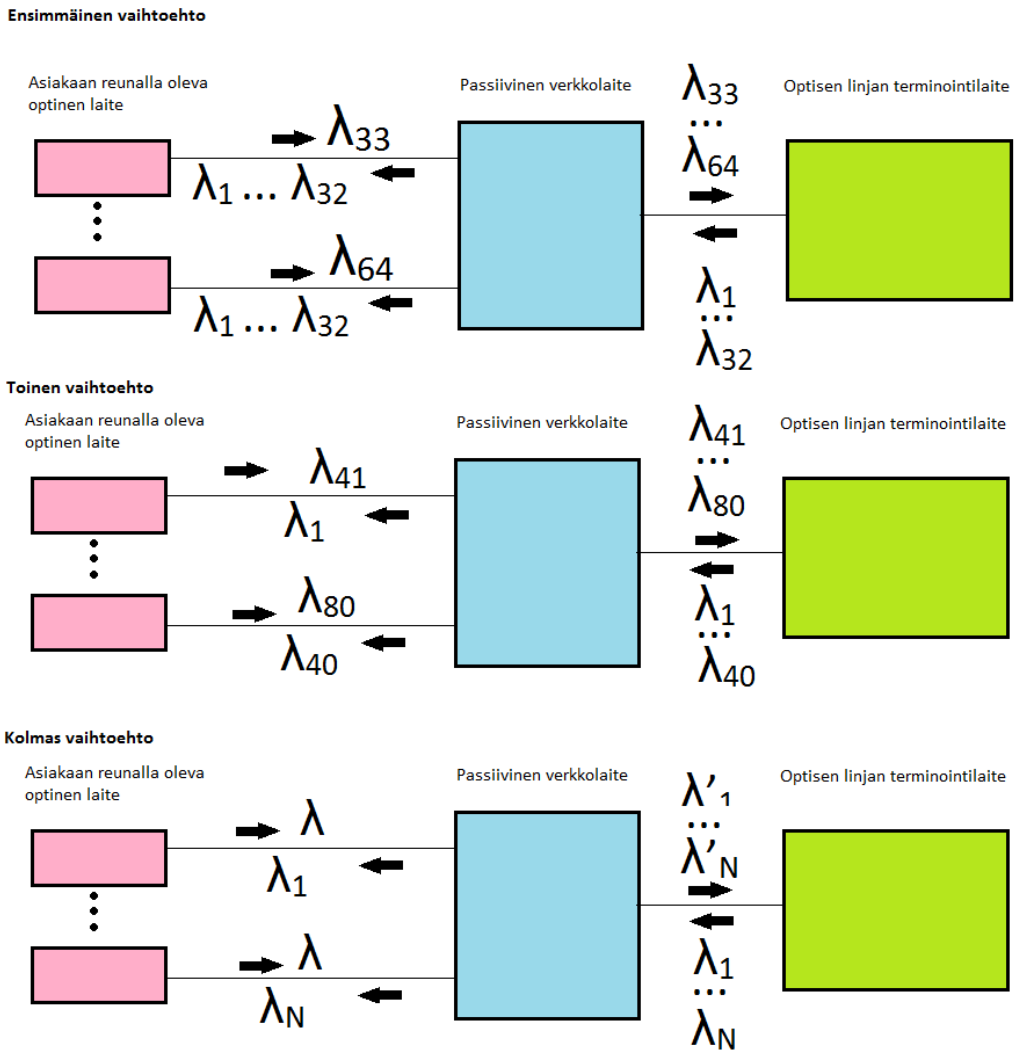
NG-PON1 -tekniikan toteutukset määritetään ITU-T standardissa G.987, ja se sisältää määritykset, lyhenteet ja akronyymit [35]. Standardin uusin versio on tullut voimaan lokakuussa 2010. Standardissa G.987.1 esitetään tekniikan yleiset vaatimukset, ja sen uusin versio on tullut voimaan tammikuussa 2010 [36]. Standardissa G.987.2 määritetään fyysinen kerros ja se on tullut voimaan lokakuussa 2010 [37]. Standardiin on tullut lisäys helmikuussa 2012 [37]. Siirtokerros määritetään standardissa G.987.3 ja se on tullut voimaan lokakuussa 2010 [38].

WDM-PON -tekniikassa asiakasyhteyksille määritetään omat kapeat aallonpituusalueet, joita ne käyttävät tiedonsiirtoon. Koska yhteydet ovat eroteltuina aallonpituuksien mukaan, verkon turvallisuus ja asiakasyhteyksien yksityisyys on parempi kuin aikajaksoihin perustuvassa jaottelussa. Tämän lisäksi erilliset aallonpituusalueet mahdollistavat sen, että jokaisella aallonpituusalueella voidaan käyttää eri kaistanleveyttä. Tämän lisäksi asiakasyhteyksien kaistanleveyksiä voidaan kasvattaa, koska aallonpituudet voidaan varata ainoastaan yhden asiakasyhteyden käyttöön. WDM-PON -tekniikassa optisen signaalin pisin siirtomatka voi olla sata kilometriä. Lisäksi WDM-PON -tekniikka voidaan yhdistää esimerkiksi EPON- tai GPON-tekniikan kanssa, jolloin asiakasyhteyksien lukumäärää voidaan kasvattaa merkittävästi. Ennen kuin tekniikoita voidaan käyttää yhdessä, GPON- tai EPON-tekniikka on muokattava, jotta se toimii myös muilla aallonpituuksilla kuin niillä mitä standardiin on määritelty. Lisäksi mahdollinen jakosuhde 1:1000 edellyttää myös virheenkorjauksen parantamista sekä optisen signaalin vahvistuksen hyödyntämistä. [33]

WDM-PON -tekniikan yksityiskohtia ei ole vielä täysin standardoitu, joten ehdotuksia tekniikan toteuttamiseen on useita. Useimmat ehdotukset ehdottavat tiheää tai erittäin tiheää aallonpituuksien jaottelua. Tällaiset tiheään jaetut aallonpituudet (Dense Wavelength-division Multiplexing, DWDM) mahdollistavat huomattavasti suuremmat kaistanleveydet kuin EPON- tai GPON-tekniikka, mutta DWDM-tekniikoiden kustannukset ovat merkittävät. DWDM-tekniikan sijasta aallonpituudet voidaan jakaa myös karkeasti Coarse Wavelength-division Multiplexing -tekniikan (CWDM) avulla, joka on edullisempi kuin DWDM. CWDM-tekniikalla voidaan saavuttaa kustannussäästöjen lisäksi DWDM-tekniikkaa paremmat optiset tehobudjetit, mutta jakosuhde ei ole yhtä hyvä kuin DWDM-tekniikassa. [32]

DWDM- ja CWDM-tekniikoiden välinen hintaero muodostuu lähes täysin tekniikoissa käytettävien lasereiden ominaisuuksista. DWDM-tekniikassa käytettävät laserit edellyttävät jäähdytystä, joka kasvattaa lähettimien kompleksisuutta. CWDM-tekniikan lähettimien valmistaminen on huomattavasti yksinkertaisempaa, jolloin se on myös kustannustehokkaampaa. Molemmat menetelmät mahdollistavat kuitenkin WDM-PON -tekniikan toteuttamisen siten, että se mahdollistaa TDM-tekniikoita paremmat jakosuhteet ja yhteenlasketun kaistanleveyden. [32]

WDM-PON -tekniikan toteutustavat voidaan jaotella myös sen mukaan, miten ne käyttävät aallonpituuskanavia. Ratkaisevaa on asiakaslaitteen ja palveluntarjoajan ensimmäisen optisen laitteen välinen liikennöinti. Ensimmäisessä menetelmässä jokaiselle asiakasreunan laitteelle siirretään kaikki asiakkaiden suuntaan menevät aallonpituudet ja asiakaslaitteen vastuulla on vastaanottaa ainoastaan sille allokoitu aallonpituus. Jokainen laite lähettää oman liikenteensä käyttäen omaa aallonpituuttaan. Toisessa menetelmässä jokaiselle asiakaslaitteelle siirretään ainoastaan sille tarkoitettu aallonpituus, ja se lähettää liikenteen omalla aallonpituudellaan. Kolmannessa menetelmässä jokaiselle laitteelle siirretään liikennettä sille tarkoitetulla aallonpituudella, mutta kaikki asiakaslaitteet käyttävät samaa aallonpituutta liikennöidessään palveluntarjoajalle. Kuvassa 17 on esitetty nämä kolme menetelmää. [32]



Kuva 17: Kolme pääasiallista tapaa WDM-PON -tekniikan toteuttamiseen. [32]

Ensimmäisessä toteutustavassa verkon tietoturva heikkenee, koska asiakaslaitteiden vastuulle jää ainoastaan oman aallonpituuden hyödyntäminen. Tämä ei kui-

tenkaan eroa merkittävästi aikajaksoihin perustuvan multipleksoinnin tietoturvasta. Toisessa toteutustavassa saavutetaan parempi tietoturva. Lisäksi syöttöhävikin määrää saadaan pienennettyä verrattuna ensimmäiseen toteutustapaan ja laitteet voidaan toteuttaa yksinkertaisemmin. Kolmas toteutustapa mahdollistaa edullisimmat asiakaspäätteet, mutta palveluntarjoajan ensimmäisen optisen verkkolaitteen on muunnettava asiakaslaitteilta saapuvat aallonpituudet. Huomioitavaa on myös se, että eri toteutustapojen välillä ei voida käyttää samanlaisia verkkolaitteita. [32]

2.13.4 Arvio optisten siirtojärjestelmien tulevaisuudesta

Verkkojen liikennemäärien ennustetaan kasvavan lähitulevaisuudessa entistä voimakkaammin. Liikennemäärien kasvu johtuu verkkoa kuormittavien ilmiöiden yleistymisestä. Tällaisia ilmiöitä ovat esimerkiksi pilvipalvelut, korkealaatuiset videot sekä tietokoneiden laskentatehon jakaminen verkon ylitse. Samalla viiveiden ja viivevaihteluiden tulee olla entistä pienempiä, koska videoneuvottelujärjestelmien ja IP-puhepalveluiden (Voice over IP, VOIP) käyttö on lisääntynyt. Samalla palveluntarjoajien liikevaihdon määrä siirrettyä bittiä kohden on pienentynyt. Asiakkaat maksavat kasvaneista kaistanleveyksistä entistä vähemmän, joten palveluntarjoajien on maksimoitava verkkojensa kustannustehokkuudet. [29], [30]

Nykyisin käytössä olevia tekniikoita käyttäen on erittäin haasteellista kasvattaa liittymien kaistanleveyksiä tai pienentää kustannuksia. Perinteisillä xDSL-tekniikoilla on vaikeaa tarjota suurta, symmetristä kaistanleveyttä. Aktiiviset Ethernet-tekniikkaan pohjautuvat ratkaisut eivät puolestaan kykene toimimaan yhtä kustannustehokkaasti kuin passiiviset ratkaisut. GPON-tekniikka kykenee periaatteessa tarjoamaan yhden gigabitin kaistanleveyttä asiakasinstansseille, mutta käytännössä siirtoetäisyyksien ja jakosuhteiden takia kaistanleveys jää sataan megabittiin. Tästä syystä palveluntarjoajien on jossain vaiheessa uudistettava verkkonsa. Uudistuksen yhteydessä WDM-PON -tekniikan käyttöönotto on erittäin houkuttelevaa. [29], [30]

TDM-tekniikkaan pohjautuvat ratkaisut eivät kykene tarjoamaan yhtä tehokasta skaalautuvuutta kuin WDM-PON-tekniikka. Jotta TDM-tekniikassa saavutettaisiin hyvä kustannustehokkuus, on jakosuhdetta kasvatettava. Tämä lyhentää signaalin maksimisiirtoetäisyyttä. TDM-tekniikan alkuinvestoinnit ovat pienemmät kuin WDM-PON -tekniikan vaatimat alkuinvestoinnit. On kuitenkin todennäköistä, että WDM-PON -tekniikkaa kyetään jatkokehittämään TDM-tekniikoita tehokkaammin. Merkittävä keino kustannustehokkuuden kasvattamiseen on hyödyntää passiivisia tekniikoita. Kaikki kolme esiteltyä tekniikkaa, 10G-EPON, NG-PON1 ja WDM-PON ovat passiivisia. [30]

WDM-PON -tekniikassa voidaan jokaiselle aallonpituudelle määrittää eri kaistanleveys riippumatta siitä käytetäänkö aallonpituutta meno- vai paluuliikenteelle. Mahdolliset kaistanleveydet ovat 1Gbit/s, 2,5Gbit/s, 4Gbit/s ja 10Gbit/s. TDM-tekniikassa näin yksityiskohtainen kaistanleveyden määrittäminen ei ole mahdollista. Tämän ansiosta palveluntarjoajat kykenevät tarjoamaan monipuolisempia palveluvaihtoehtoja asiakkaille WDM-PON -tekniikkaa käyttämällä. [32]

WDM-PON -tekniikan merkittävimmät heikkoudet ovat suuret käyttöönottokustannukset ja yhteisen standardin puute. Erinäisiä projekteja on käynnistetty,

jotta tekniikan kustannuksia saadaan laskettua. Yksi tällainen projekti on GigaWam, jonka tavoitteena on WDM-PON -tekniikan vaatimien komponenttien kustannusten pienentäminen. Projektin yhteydessä yritetään saada esimerkiksi säädettävien laserlähettimien hintatasoa pienemmäksi. Standardoinnin puute vaikuttaa myös komponenttien hintatasoon. Koska selkeää yhteistä standardia ei ole, ei WDM-PON -tekniikkaan soveltuvia optisia komponentteja kyetä valmistamaan suurissa tuotantoerissä. Lisäksi standardin puute johtaa siihen, että eri laitevalmistajien toteutukset eivät välttämättä ole yhteensopivia. [30]

Selvää on kuitenkin se, että jotta palveluntarjoaja kykenee menestymään kaupallisesti, on sen tarjottava sopivia kaistanleveyksiä asiakkaille ja hyödynnettävä käytössä olevaa infrastruktuuria tehokkaasti. Tehokkaaseen infrastruktuurin hyödyntämiseen kuuluu sekä hyvän jakosuhteen ylläpitäminen että mahdollisimman pitkät signaalin siirtovälit ilman ylimääräistä vahvistusta. Näiden tavoitteiden täyttäminen on helpompaa WDM-PON -tekniikalla kuin 10G-EPON tai NG-PON1 -tekniikalla. Huolimatta WDM-PON -tekniikan puutteista, on se silti hyvin potentiaalinen vaihtoehto optiseksi siirtojärjestelmäksi erityisesti silloin kun palveluntarjoajalla ei ennestään ole olemassa optista verkkoa. Jos palveluntarjoajalla on jo käytössään optinen siirtoverkko, EPON-tekniikan päivittäminen 10G-EPON -tekniikaksi tai GPON-tekniikan päivittäminen NG-PON1 -tekniikaksi voi olla hyvin perusteltua. [33]

On myös todennäköistä, että tulevaisuudessa hyödynnetään tekniikkaa, joka pohjautuu sekä WDM- että TDM-tekniikoihin. Tällainen tekniikka kykenee skaalautumaan selkeästi paremmin kuin mihin tekniikat kykenevät itsenäisesti.

3 PBB-VPLS -tekniikan testaaminen käytännössä

Tässä luvussa esitetään diplomityön kokeellisen osion eteneminen. Luvussa 3.1 esitetään käytössä ollut testilaitteisto sekä mihin mitäkin laitetta käytettiin. Luvussa 3.2 käsitellään testiverkon rakentaminen sekä testien eteneminen. Testattavaa tekniikkaa valittaessa vaihtoehdot olivat parhaiten kirjallisuustutkimuksessa pärjänneet tekniikat: PBB-TE, MPLS-TP sekä PBB-VPLS. Näistä tekniikoista testattavaksi valittiin PBB-VPLS, koska tekniikalla on hyvät mahdollisuudet parantaa olemassa olevien verkkojen suorituskykyä. Lisäksi tekniikkaa ei ole tutkittu yhtä laajalti kuin MPLS-TP ja PBB-TE -tekniikkaa. Käytössä ollut testilaitteisto soveltui parhaiten PBB-VPLS -tekniikan testaamiseen.

3.1 Käytetty testilaitteisto

Testiverkko rakennettiin Aalto-yliopiston Tietoliikenne- ja tietoverkkotekniikan laitoksen testikonesaliin. Käytössä oli laitteita usealta eri laitevalmistajalta, mutta kunkin laitevalmistajan laitteita käytettiin ainoastaan yhdessä roolissa. Juniper Networksin reitittimiä käytettiin ainoastaan VPLS:n toteuttamiseen ja Extreme Networksin kytkimillä toteutettiin PBB-aggregointiverkko. Taulukossa 5 on esitetty käytössä olleet laitteistot, niiden ohjelmistoversiot ja roolit testiverkossa.

Taulukko 5: Testiverkossa käytössä olleet laitteet, ohjelmistoversiot ja laitteiden roolit.

Laite	**Kpl**	**Ohjelmistoversio**	**Rooli**
Spirent Testcenter SPT-2000 -runko ja CPR-2001B -linjakortti	1	3.70.4406	Testiliikenteen generointi verkkoon ja sen vastaanottaminen
Juniper Networks MX80-48t	3	JunOS 10.3R2.11	VPLS-verkon toteuttaminen
Extreme Networks Black-Diamond 20804/20808	3	ExtremeXOS 12.5.2.6	PBB-aggregointiverkon toteuttaminen
Accedian Ethernid GE	7	AEN_4.9_16352	Liikenteen heijastaminen kaappausta varten sekä CVLAN-tunnisteen lisääminen ja poistaminen kehyksiin
Lenovo SL500 kannettava tietokone	1	Ubuntu 10.04 LTS (2.6.32-41), Wireshark 1.2.7	Ethernid-demarkaatiolaitteiden heijastaman liikenteen kaappaaminen

Spirent Testcenter -liikenneanalysaattoria käytettiin liikenteen luomiseen testiverkkoon. Testcenter-laitteisto myös vastaanotti luomansa liikenteen. Liikenneanaly-

saattoria käyttämällä tiedetään tarkkaan liikenteen kehysrakenne, joten testiverkosta otetuista liikennekaappauksista voidaan selvittää, ovatko verkkolaitteet muokanneet kehyksen tietoja, muuten kuin kapseloinnin osalta. Käytössä olleessa linjakortissa oli kahdeksan gigabitin Ethernet-rajapintaa RJ-45 -kupariliittimellä. Kaikkia asiakasinstansseja oli siis mahdollista emuloida samanaikaisesti ilman ongelmia. Lisäksi testilaitteiston avulla kyettiin mittaamaan testiverkon viive, viivevaihtelu ja kehyshukka. Vastaavasti testilaitteiston avulla kyettiin varmentumaan siitä, ettei testiliikenne välity vääriin rajapintoihin testien aikana. Lisäksi Spirent Testcenter -liikenneanalysaattorin avulla voidaan kaapata rajapintojen liikennettä. Kuvassa 18 on käytetty liikenneanalysaattori.

Kuva 18: Spirent Testcenter -liikenneanalysaattori yhdellä linjakortilla.

Juniper Networksin valmistamilla MX80-48t -reitittimillä luotiin verkkoon VPLS-palvelut ja ne muodostivat testiverkon rungon. Reitittimiin oli määritetty sisäverkon reititysprotokolla IS-IS. Reitittimet neuvottelivat MPLS-välitysleimat käyttämällä RSVP-protokollaa. VPLS-palveluinstanssileimat neuvoteltiin käyttämällä LDP-protokollaa. Näiden protokollien avulla testiverkkoon luotiin MPLS-verkko, jonka päällä toteutettiin VPLS-palvelut. Reitittimet olivat kytkettyinä toisiinsa suoraan tai Ethernid-demarkaatiolaitten lävitse. Kytkennät tehtiin käyttämällä gigabitin Ethernet RJ-45 -kuparirajapintoja. Testeissä hyödynnettiin vain pientä osaa MX80-sarjan reitittimien rajapinnoista ja liikenteen maksimiläpäisystä. Myöskään laitteissa olevaa neljää XFP-kuiturajapintaa ei hyödynnetty. Kuvassa 19 näkyy kaksi MX80-48t -reititintä.

Extreme Networksin valmistamia BlackDiamond 20804 ja BlackDiamond 20808 -reitittäviä kytkimiä käytettiin pääsy- ja aggregointiverkon luomiseen testiverkossa. Nämä kytkimet toteuttivat PBB-tekniikan, eli kytkimet oppivat asiakaslaitteiden MAC-osoitteet ja suorittivat kehysten PBB-tekniikan mukaisen kapseloinnin ja sen purkamisen asiakasinstanssien ja VPLS-palvelun välissä. Kytkinmallit 20804 ja 20808 kuuluvat samaan BlackDiamond-tuoteperheeseen, eikä niiden toiminnassa ole merkittäviä eroavaisuuksia. Mallin 20808 kytkin on hieman tehokkaampi kuin 20804-mallin kytkin ja siihen sijoitetaan linjakortit kyljittäin. Mallin 20804 kytkimeen linjakortit sijoitetaan vaakatasoon. PBB-tekniikan toteutus on molemmissa laitteissa identtinen. Kaikissa kytkimissä käytettiin G40X-linjakortteja, joissa on 40 yhden gigabitin SFP-rajapintaa. Spirent Testcenter -liikenneanalysaattorin asiakasinstanssien rajapinnat kytkettiin kytkimiin käyttämällä kupari-SFP -rajapintoja. Ethernid-demarkaatiolaitteisiin kytkimet kytkettiin käyttämällä 1310 nanometrin

Kuva 19: Kaksi MX80-48t -reititintä.

optisia SFP-rajapintoja ja kuituja. Kuvassa 20 esitetään Extreme Networksin Black-Diamond 20804 -kytkin.

Kuva 20: Extreme Networksin BlackDiamond 20804 -sarjan kytkin.

Accedian Ethernid GE -demarkaatiolaitteilla mahdollistettiin reitittimien ja kytkimien välissä siirretyn liikenteen kaappaaminen. Demarkaatiolaitteita sijoitettiin kytkimien ja reitittimien väliin sekä pelkkien reitittimien väliin. Demarkaatiolaitteen läpikulkeva liikenne heijastettiin kolmanteen rajapintaan, johon liitettiin kannettava tietokone, jonka avulla liikenne kaapattiin. Liikennekaappausten avulla voidaan selvittää millaisia kapselointeja tai kehysten muokkaamisia laitteet ovat tehneet.

Lisäksi kaappausten avulla voidaan varmentua siitä miten liikenne leviää verkossa. Tämän lisäksi havaittiin, että Ethernid-demarkaatiolaitteita on käytettävä lisäämään ja poistamaan CVLAN-tunniste BlackDiamond-kytkimien ja MX80-reitittimien välissä. Tästä kerrotaan tarkemmin luvussa 3.2.4. Näiden tehtävien lisäksi Ethernid-demarkaatiolaitteiden avulla toteutettiin mediamuunnos, koska testikäytössä oli vain rajallinen määrä kupari-SFP -moduuleja. Yhteydet kytkimien ja reitittimien välillä luotiin siten, että BlackDiamond-kytkimet liitettiin demarkaatiolaitteeseen käyttämällä optista rajapintaa ja MX80-reitittimet kuparista rajapintaa. Kuvassa 21 esitetään monta Ethernid-demarkaatiolaitetta, jotka ovat sijoitettuna räkkihyllyyn.

Kuva 21: Useita Accedian Ethernid GE -demarkaatiolaitteita niille tarkoitetulla räkkihyllyllä.

Lenovo SL500 -kannettavaa tietokonetta käytettiin Ethernid-demarkaatiolaitteiden heijastaman testiliikenteen kaappaamiseen. Kaappaus toteutettiin käyttämällä Wireshark-ohjelmistoa. Kannattevan tietokoneen käyttöjärjestelmä oli Ubuntu 10.04 LTS ja kernelin versio 2.6.32-41. Wireshark-ohjelmiston versio oli 1.2.7. Kannettavassa tietokoneessa oli vain yksi RJ-45 -rajapinta, joten liikennettä jouduttiin kaappaamaan aina yhdestä verkon topologian pisteestä kerrallaan. Kunkin testitopologian testiliikenne ajettiin aina identtisesti eri mittauskertojen välillä, jotta liikennekaappaukset olisivat verrannollisia. Merkittävin ero liikennekaappausten välillä on aikaleimojen eroavaisuudet. Kaappauksista kyetään kuitenkin havaitsemaan, mihin testivaiheeseen kaapattu liikenne kuuluu.

3.2 Testaus

Testaus jakaantui kahteen pääasialliseen osioon. Luvut 3.2.3–3.2.6 käsittelevät testauksen ensimmäistä osiota, jonka pääasiallinen tehtävä oli varmentaa testiverkon

oikeellisuus samalla kun sitä rakennettiin. Samalla näiden testien avulla kyettiin varmentumaan siitä, että käytetyt testimetodit olivat tehtävään sopivia. Toinen osio esitetään luvuissa 3.2.7–3.2.9, jotka sisältävät tekniikan varsinaiseen testaamiseen käytetyt testitopologiat. Tästä syystä nämä kolme lukua esittelevät käytössä olleen testitopologian muita lukuja tarkemmin.

3.2.1 Yleistä testauksesta ja testauksen eteneminen

Kaikissa eri testivaiheissa verkon toimivuus varmennettiin Spirent Testcenter -liikenneanalysaattorilla siten, että sen varmennettiin vastaanottavan lähetetyt kehykset oikeista rajapinnoista ilman kehysvirheitä. Tämän lisäksi verkkolaitteiden omia työkaluja käytettiin MAC-osoitteiden oppimisen varmentamiseen. Näin kyettiin todentamaan myös se, ettei MAC-osoitteita näkynyt laitteilla, joilla tekniikoiden mukaan niiden ei pitäisi näkyä. Näiden tietojen oikeellisuus kyettiin varmentamaan verkosta kaapatun liikenteen avulla. Kahta täysin itsenäistä tiedonkeruumenetelmää käyttämällä kyettiin minimoimaan mahdollisten virheellisten tietojen vaikutus tutkimustuloksiin. Oleellisimmat tiedot testeistä ovat: mikäli käytetyssä testitopologiassa oli ainoastaan kaksi kappaletta kutakin verkkolaitetta, emuloituja asiakasmääriä muutettiin testien aikana. Mikäli käytetyssä testitopologiassa oli kolme kappaletta kutakin verkkolaitetta, emuloituja asiakasmääriä ei muutettu. Kun käytössä oli kolme asiakasintanssia, kontrolloitiin sitä, mihin asiakasrajapintoihin testiliikennettä lähetettiin. Testiliikennettä luotaessa tietyissä välikohdissa tyhjennettiin laitteiden välitystaulut. Verkkojen loogista erottelua testattiin yrittämällä siirtää ISID-, BVLAN- tai VPLS-palveluinstanssitunnisteiden välistä liikennettä. Testi oli kuitenkin vain pintapuolinen, koska täyden varmuuden saaminen erottelukyvystä edellyttää laajempaa testaamista kuin oli mahdollista toteuttaa diplomityön yhteydessä. Käytetty kaistanleveys oli vain 1Mbps. Testiliikenteen käyttämä kehyskoko oli 128 tavua. Kaikissa laitteissa oli otettu käyttöön normaalia suurempien kehysten (jumbo frames) välitys. Käytetyt asiakasmäärät olivat 25, 50 tai 75 asiakaslaitetta asiakasrajapintaa kohden. Testeissä, joissa asiakasmäärää ei muutettu, käytettiin 25 asiakaslaitetta asiakasrajapintaa kohden.

3.2.2 VPLS-tekniikan MAC-osoitteiden oppimisen varmentaminen

VPLS-tekniikassa jokainen VPLS-palveluinstanssiin osallistuva reititin joutuu oppimaan palveluinstanssiin kuuluvien asiakaslaitteiden MAC-osoitteet. Ennen testiverkon rakentamisen aloittamista haluttiin varmentua siitä, että Juniper Networksin MX80-reitittimet esittävät tämän toimintaperiaatteen oikein. Tämä kyettiin varmentamaan siten, että kun hyödynnetään pelkkää VPLS-tekniikkaa, reitittimien VPLS-osoitetaulussa esitetään kaikkien VPLS-palveluinstanssiin kuuluvien asiakaslaitteiden MAC-osoitteet.

Tämän varmistamiseksi luotiin VPLS-palveluinstanssi kahden MX80-reitittimen välille. Alla esitetään näiden reitittimien VPLS-osoitetaulut kun kumpaankin reitittimeen on ollut kytkettynä 25 asiakaslaitetta. Alla olevan tiedon perusteella voidaan todeta, että MX80-reitittimet ovat oppineet kaikki VPLS-palveluinstanssiin kuulu-

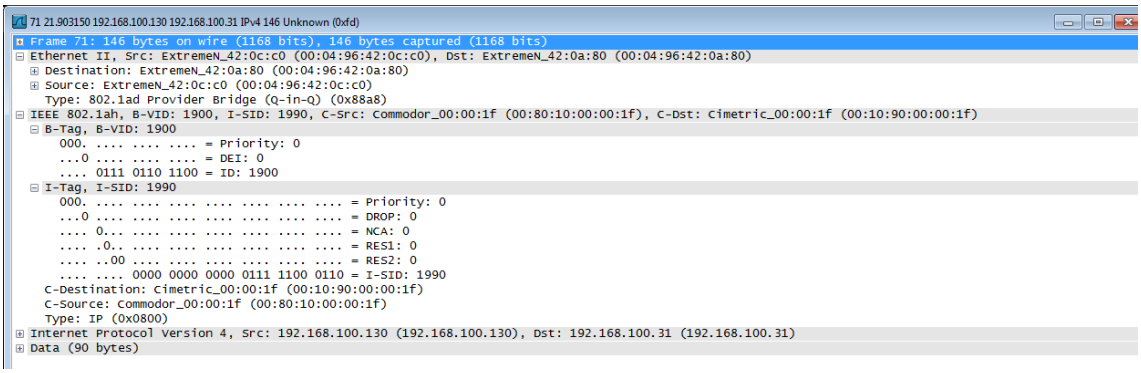
vien asiakaslaitteiden MAC-osoitteet. Tämä toiminallisuus varmennettiin myös, kun VPLS-palveluinstanssiin osallistui kolme reititintä.

```
MX80-1:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:10:90:00:00:01   D        ge-1/1/5.2
   00:10:90:00:00:02   D        ge-1/1/5.2
   ...
   00:10:90:00:00:19   D        ge-1/1/5.2
   22:22:11:11:99:01   D        lsi.1048832
   22:22:11:11:99:02   D        lsi.1048832
   ---
   22:22:11:11:99:19   D        lsi.1048832


MX80-3:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:10:90:00:00:01   D        lsi.1048832
   00:10:90:00:00:02   D        lsi.1048832
   ...
   00:10:90:00:00:19   D        lsi.1048832
   22:22:11:11:99:01   D        ge-1/1/5.2
   22:22:11:11:99:02   D        ge-1/1/5.2
   ...
   22:22:11:11:99:19   D        ge-1/1/5.2
```

3.2.3 Pelkkä PBB-tekniikka kahdella kytkimellä ja kahdella asiakasrajapinnalla

Testiverkon rakentaminen aloitettiin hyödyntämällä ainoastaan kahta PBB-tekniikkaa toteuttavaa kytkintä ja kahta asiakasrajapintaa. Verkon rakentaminen aloitettiin tällä tavalla, jotta voitiin varmentua siitä, että käytetyt BlackDiamond-kytkimet toteuttavat PBB-tekniikan oikein. Lisäksi käytössä oli ainoastaan yksi BVLAN-tunniste ja yksi ISID-tunniste. Sellaisenaan tällainen testiverkko ei ole vielä kiinnostava, mutta PBB-tekniikan toteutuksen varmentamisen lisäksi verkosta kyettiin kaappaamaan ainoastaan PBB-tekniikan mukaisesti kapseloitu kehys. Tällainen kehys näytetään

kuvassa 22, jonka visualisointi on saatu Wireshark-ohjelmistosta. Kuvasta nähdään, että käytetty ISID-tunniste oli 1990 ja käytetty BVLAN-tunniste oli 1900. Lisäksi liikennekaappauksesta havaittiin, että verkossa kehysten siirtämiseen käytettiin kytkimien rajapintojen MAC-osoitteita emuloitujen asiakaslaitteiden MAC-osoitteiden sijaan.



Kuva 22: Kahden BlackDiamond-kytkimen välistä kaapattu PBB-tekniikan kehys.

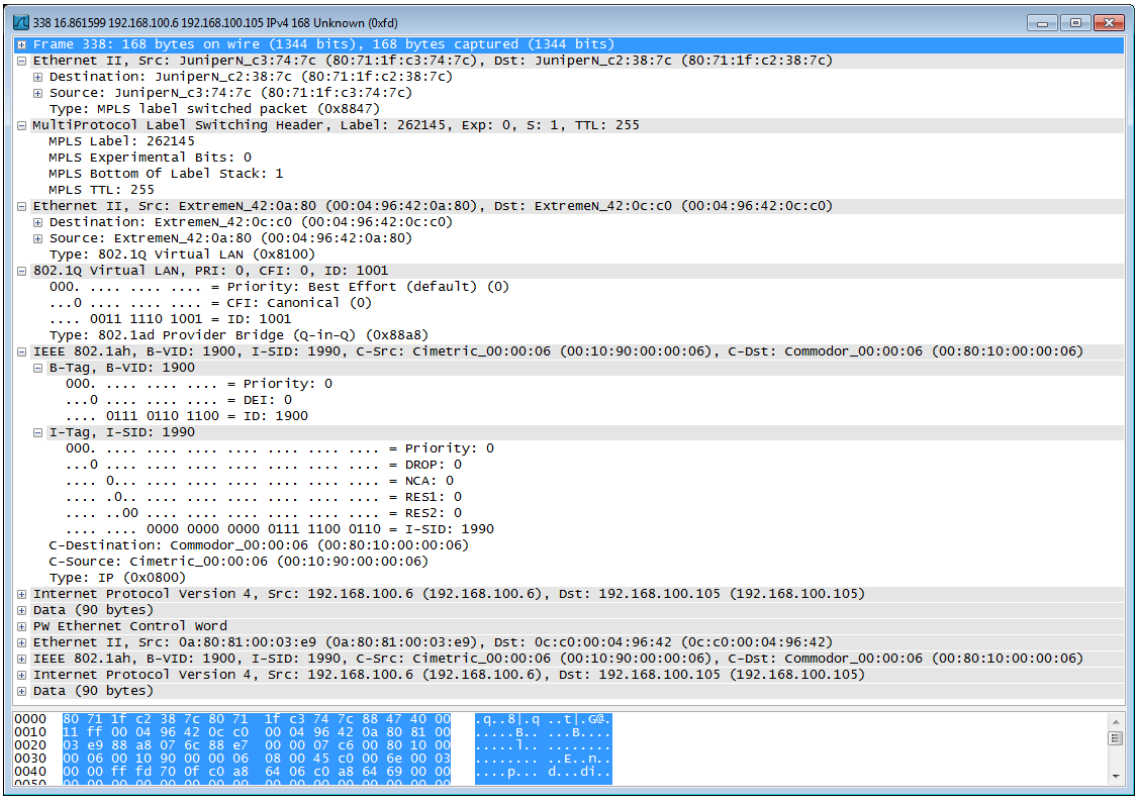
3.2.4 PBB-VPLS -tekniikka kahdella reitittimellä, kytkimellä ja asiakasrajapinnalla

Testiverkon rakentaminen jatkui VPLS-tekniikan lisäämisellä verkkoon. Käytössä oli edelleen vain yksi ISID-tunniste, yksi BVLAN-tunniste ja käyttöön otettiin vain yksi VPLS-palveluinstanssi. Tämän testivaiheen tärkein tavoite oli saada PBB- ja VPLS-tekniikan kokonaistoteutus varmennettua. Kummassakaan tuoteperheessä, MX80-reitittimissä tai BlackDiamond-kytkimissä, ei ole erityisiä PBB-VPLS -tekniikan toteutukseen liittyviä toimintoja. Kun BlackDiamond-kytkimien verkkorajapinnat liitettiin MX80-reitittimien VPLS-palveluinstanssin rajapintaan, havaittiin, ettei liikennettä kulje verkon lävitse. Tarkempi selvitys paljasti, että kytkimet lähettävät emuloitujen asiakaslaitteiden liikenteen oikeasta rajapinnasta, mutta reitittimet eivät havaitse yhtään liikennettä vastaanotetuksi VPLS-palveluinstanssin asiakasrajapinnassa.

Ongelman syyksi paljastui laitevalmistajien tavat käsitellä, PBB- ja VPLS-tekniikoiden yhteydessä, Ethertype-kehystyyppimerkintää. Dokumentaation mukaan BlackDiamond-kytkimet asettavat kehystyypiksi »0x88B5», vaikka kuvasta 22 voidaan nähdä, että arvoksi tulee »0x88a8» ilman CVLAN- tai SVLAN-tunnisteita [12]. MX80-reitittimet kuitenkin edellyttävät, että kehystyyppi on »0x8100», »0x88a8» (tunnisteen kera), »0x9100» tai »0x9901» [39].

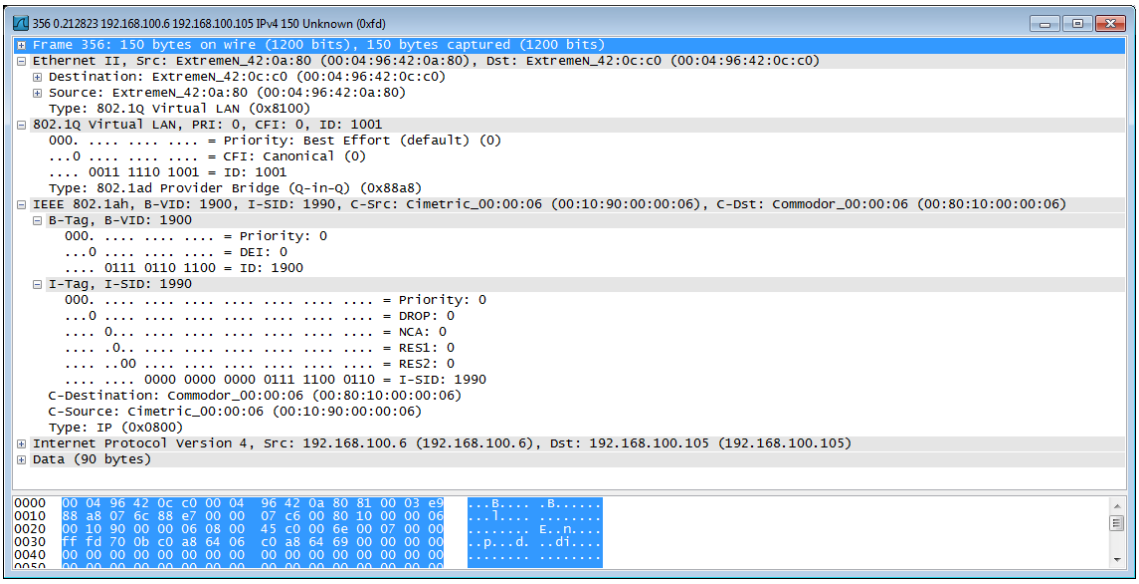
Tilanteen korjaamiseksi reitittimien ja kytkimien välissä oleviin Ethernid-demarkaatiolaitteisiin määritettiin liikenteen peilaamisen lisäksi CVLAN-tunnisteen käsittely. Kytkimiltä reitittimille suunnattuihin kehyksiin demarkaatiolaitteet lisäsivät CVLAN-tunnisteen arvolla 1001 ja reitittimiltä kytkimille suunnatuilta kehyksiltä ne poistivat CVLAN-tunnisteen. Näin liikenne saatiin siirtymään verkon yli ja PBB- ja VPLS-tekniikoiden kokonaistoteutus tehdyksi.

Kaapattaessa PBB-VPLS -tekniikalla kapseloitua liikennettä kahden MX80-reitittimen välistä havaittiin, että käytössä ollut Wireshark-ohjelmisto ei kykene esittämään kehysrakennetta oikein. Osa kehyksen tiedoista esitetään käyttäjäystävällisessä näkymässä kahteen kertaan, mutta kun kehysrakennetta tarkasteltiin heksanäkymän avulla, todettiin kehyksen olevan kunnossa. Tätä havaintoa tukee se, että reitittimien ja kytkimien välistä kaapatut, ainoastaan PBB-tekniikan mukaisesti kapseloidut, kehykset olivat täysin kunnossa. Myöskään liikenneanalysaattori ei havainnut ongelmia vastaanotetuissa kehyksissä. Kuvassa 23 esitetään kahden MX80-reittimen välistä kaapattu kehys, joka on kapseloitu PBB-VPLS -tekniikan mukaisesti. Kuvasta nähdään kuinka Wireshark virheellisesti esittää osan kehyksen tiedoista kahteen kertaan.



Kuva 23: Kahden MX80-reitittimen välistä kaapattu PBB-VPLS -tekniikan kehys.

Kuvassa 24 esitetään MX80-reitittimen ja BlackDiamond-kytkimen välistä kaapattu kehys. Kehyksessä ei ole enää VPLS-tekniikan kapselointia. MX80-reititin on poistanut sekä välitysleiman, että instanssin palveluleiman kehyksestä. Kehyksessä kuitenkin näkyy CVLAN-tunniste arvolla 1001. Tämä johtuu siitä, että Ethernid-demarkaatiolaite ei ole poistanut CVLAN-tunnistetta ennen liikenteen peilaamista kaappaukseen.



Kuva 24: MX80-reitittimen ja BlackDiamond-kytkimen välistä kaapattu kehys.

3.2.5 PBB-VPLS -tekniikka kahdella reitittimellä, kytkimellä ja kolmella asiakasrajapinnalla

Seuraava vaihe testiverkon rakentamisessa oli kolmannen asiakasrajapinnan lisääminen verkkoon. Testilaitteiden lukumäärää ei kuitenkaan kasvatettu ja käytössä oli edelleen yksi ISID-tunniste, yksi BVLAN-tunniste ja yksi VPLS-palveluinstanssi. Asiakasrajapinnat A ja C liitettiin ensimmäiseen 20804-kytkimeen ja asiakasrajapinta B toiseen 20804-kytkimeen. Laitteiden toiminassa ei havaittu ongelmia vaikka asiakasrajapintojen lukumäärää kasvatettiin. Lisäksi saatiin ensimmäiset varmistukset siitä, että PBB-tekniikkaa toteuttavat BlackDiamond-kytkimet käsittelevät asiakaslaitteiden MAC-osoitteet oikein. Jos ensimmäinen 20804-kytkin on oppinut asiakasrajapinnan A MAC-osoitteet, kyseisiin osoitteisiin tarkoitettu liikenne ei näy asiakasrajapinnassa B tai C.

3.2.6 PBB-VPLS -tekniikka kolmella reitittimellä, kytkimellä ja asiakasrajapinnalla

Testiverkon rakentamista jatkettiin laajentamalla se yhdellä reitittimellä ja kytkimellä. Tällöin asiakasrajapinta C siirrettiin ensimmäisestä 20804-kytkimestä lisättyyn 20808-kytkimeen. Tällä tavoin jokaisessa kytkimessä oli liitettynä yksi asiakasrajapinta. Käytössä oli edelleen yksi ISID-tunniste, yksi BVLAN-tunniste ja yksi VPLS-palveluinstanssi. Tätä järjestelyä testattiin kahdella eri verkkotopologialla. Ensimmäisessä topologiassa kaikki reitittimet olivat täysin kytkettyjä toisiinsa (full mesh). Toisessa topologiassa reititin MX80-1 oli kytkettynä reitittimiin MX80-2 ja MX80-3, mutta reitittimet MX80-2 ja MX80-3 eivät olleet liitettyinä toisiinsa fyysisesti. VPLS-tekniikan edellyttämä looginen täysikytkentäisyys saavutettiin toisessa topologiassa siten, että reitittimet neuvottelivat välitysleimat, joiden avulla MX80-2 ja MX80-3 kykenivät liikennöimään keskenään MX80-1 -reitittimen lävitse.

Reitittimet muodostivat nämä välitysleimat automaattisesti.

Kun testiliikennettä oli siirretty verkossa vähän aikaa, havaittiin, ettei käytössä ollut BlackDiamond 20808 -kytkin reagoinut verkon yli siirrettyyn hallintayhteyteen. Testiliikenteen välitykseen tällä ei ollut vaikutusta, koska laitteiden hallintataso on eriytetty välitystasolta. Laitteen komentoliittymä saatiin käyttöön sarjakaapelin välityksellä. Kytkimen uudelleenkäynnistys palautti myös verkon ylitse siirretyn hallintayhteyden käyttöön. Tällöin havaittiin, että laite ilmoittaa prosessorin virheestä (CPU error) komentoliittymässä. Tällöin päätettiin vaihtaa käytössä ollut 20808-kytkin varalla olleeseen 20808-kytkimeen, jotta mahdolliset suunnittelemattomat vikatilanteet eivät vaikuta testituloksiin.

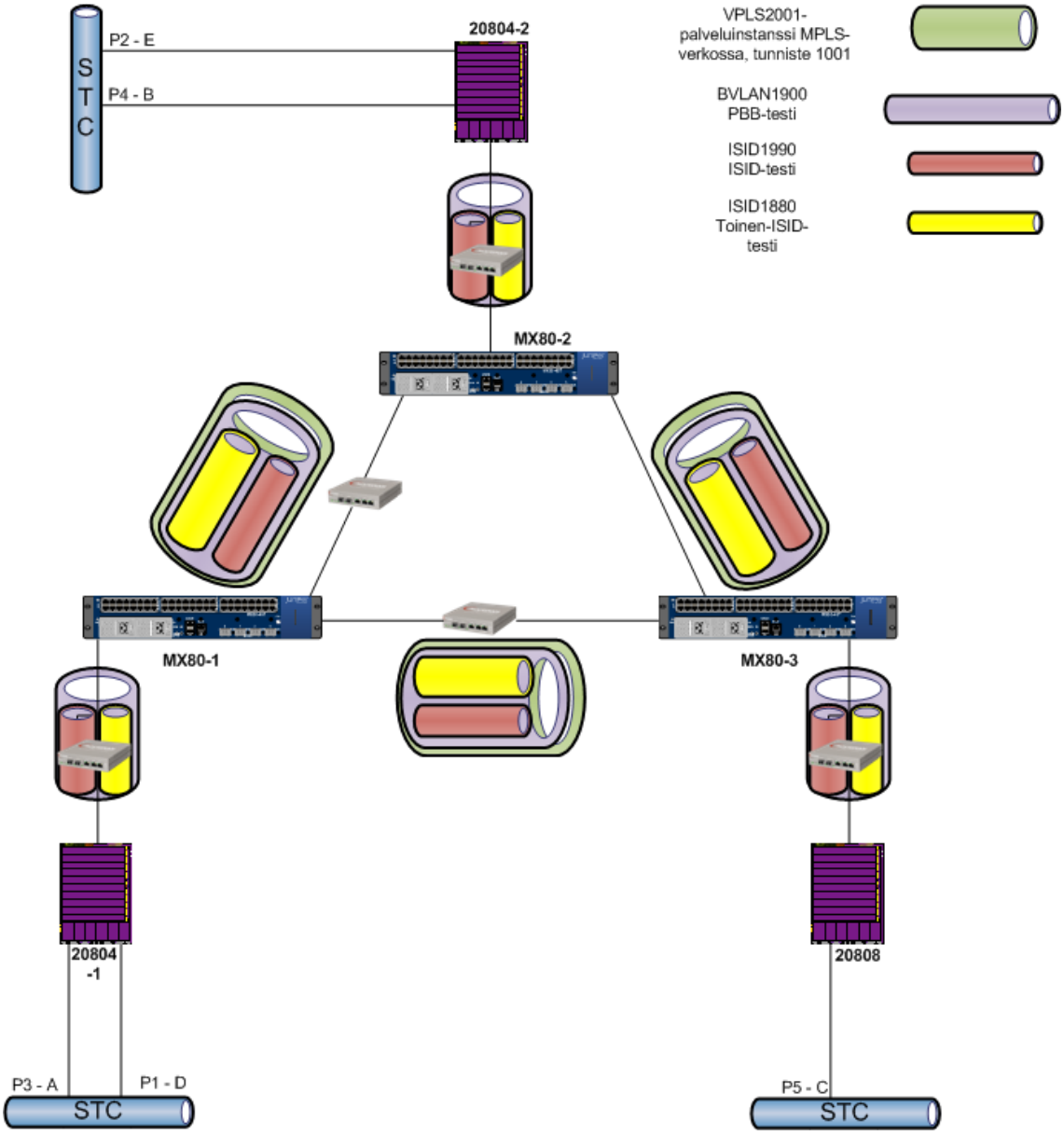
Tämän lisäksi havaittiin, että verkkoon lisätty Ethernid-demarkaatiolaitteen liikenteen peilaamista ei oltu määritelty oikein. Demarkaatiolaite peilasi ainoastaan toiseen suuntaan siirretyn liikenteen MX80-3 -reitittimen ja 20808-kytkimen välistä. Tämä määrittelyvirhe korjattiin, jotta kyseisten laitteiden välistä kaapatussa liikenteessä näkyy myös asiakasrajapintaan C suunnattu liikenne. Koska kaikki laitteet, joiden liikenteen kaappaamiseen määrittelyvirhe vaikutti, oli lisätty vasta tässä testivaiheessa, ei vain yksisuuntaista liikennekaappausta kertynyt merkittävästi.

3.2.7 PBB-VPLS -tekniikan toteuttaminen viidellä asiakasrajapinnalla ja kahdella ISID-tunnisteella

Testiverkossa oli tähän asti käytössä yksi VPLS-palveluinstanssi (tunnistettu tunnisteella 1001), yksi BVLAN-tunniste (1900) ja yksi ISID-tunniste (1990). Testiverkon todettiin olevan valmis, joten siihen lisättiin kaksi asiakasrajapintaa jotka eroteltiin ISID-tunnisteella 1880. Nämä lisätyt asiakasrajapinnat sijaitsivat ensimmäisessä ja toisessa BlackDiamond 20804 -kytkimessä. Testiverkolla ja käytetyillä tunnisteilla kyettiin MAC-osoitteiden oppimisen ja leviämisen lisäksi varmentumaan siitä, miten PBB-aggregointiverkko käsittelee useamman kuin yhden ISID-tunnisteen käyttämisen yhdessä BVLAN-tunnisteella merkityssä loogisessa välitysverkossa. VPLS-palvelu ei käsitellyt PBB-tekniikalla kapseloituja kehyksiä millään tavalla testiverkossa. Tästä syystä se monisti ja välitti ISID-tunnisteella 1880 merkittyjä kehyksiä myös 20808-kytkimelle tietyissä tapauksissa. Kytkin ei kuitenkaan käsitellyt kyseisiä kehyksiä, koska ISID-tunnistetta 1880 ei ollut määritelty sille, vaan hylkäsi kehykset.

Kuvassa 25 esitetään käytössä ollut testitopologia. Huomioitavaa siinä on, että kuvaan on piirretty ISID-tunnisteella 1880 merkitty liikenne myös laitteiden MX80-3 ja 20808 välille. Tämä kuvastaa sitä, että VPLS-palvelu monisti kyseiset kehykset 20808-kytkimelle. Yhtään ISID-tunnisteella 1880 merkittyä kehystä ei siirtynyt 20808-kytkimeltä MX80-3 -reitittimelle. Kytkin ei myöskään oppinut asiakaslaitteiden MAC-osoitteita, kun ne oli merkitty ISID-tunnisteella 1880, vaan hylkäsi kyseiset kehykset heti vastaanottavassa rajapinnassa. Asiakasinstanssit A, B ja C merkittiin ISID-tunnisteella 1990 ja ne sijaitsivat Testcenter-liikenneanalysaattorin rajapinnoissa P3, P4 ja P5. Liikenneanalysaattorin rajapinnoissa P1 ja P2 sijaitsivat ISID-tunnisteella 1880 merkityt asiakasrajapinnat D ja E.

Jokaisessa testiliikenteen eri vaiheessa tarkistettiin laitteiden välitystaulut, jotta varmennuttiin MAC-osoitteiden leviämisestä ja siitä miten laitteet oppivat asiakas-



Kuva 25: Testiverkon topologia, kun käytössä oli yksi VPLS-palveluinstanssi, BVLAN-tunniste ja kaksi ISID-tunnistetta.

laitteiden MAC-osoitteet. Lisäksi testiliikenne oli aina hetken päällä, jotta verkon tilanne ehti tasoittua. Spirent Testcenter -liikenneanalysaattorin avulla tarkasteltiin myös kehysten kokemia viiveitä, viivevaihteluita sekä kehyshukkaa. Testiverkkoon luotiin liikennettä seuraavalla tavalla ja seuraavassa järjestyksessä:

1. Asiakasrajapinnasta A (P3) asiakasrajapintaan B (P4) suuntautuva liikenne päälle
2. Asiakasrajapinnasta B asiakasrajapintaan A suuntautuva liikenne päälle
3. Testiliikenne pois ja välitystaulujen tyhjennys

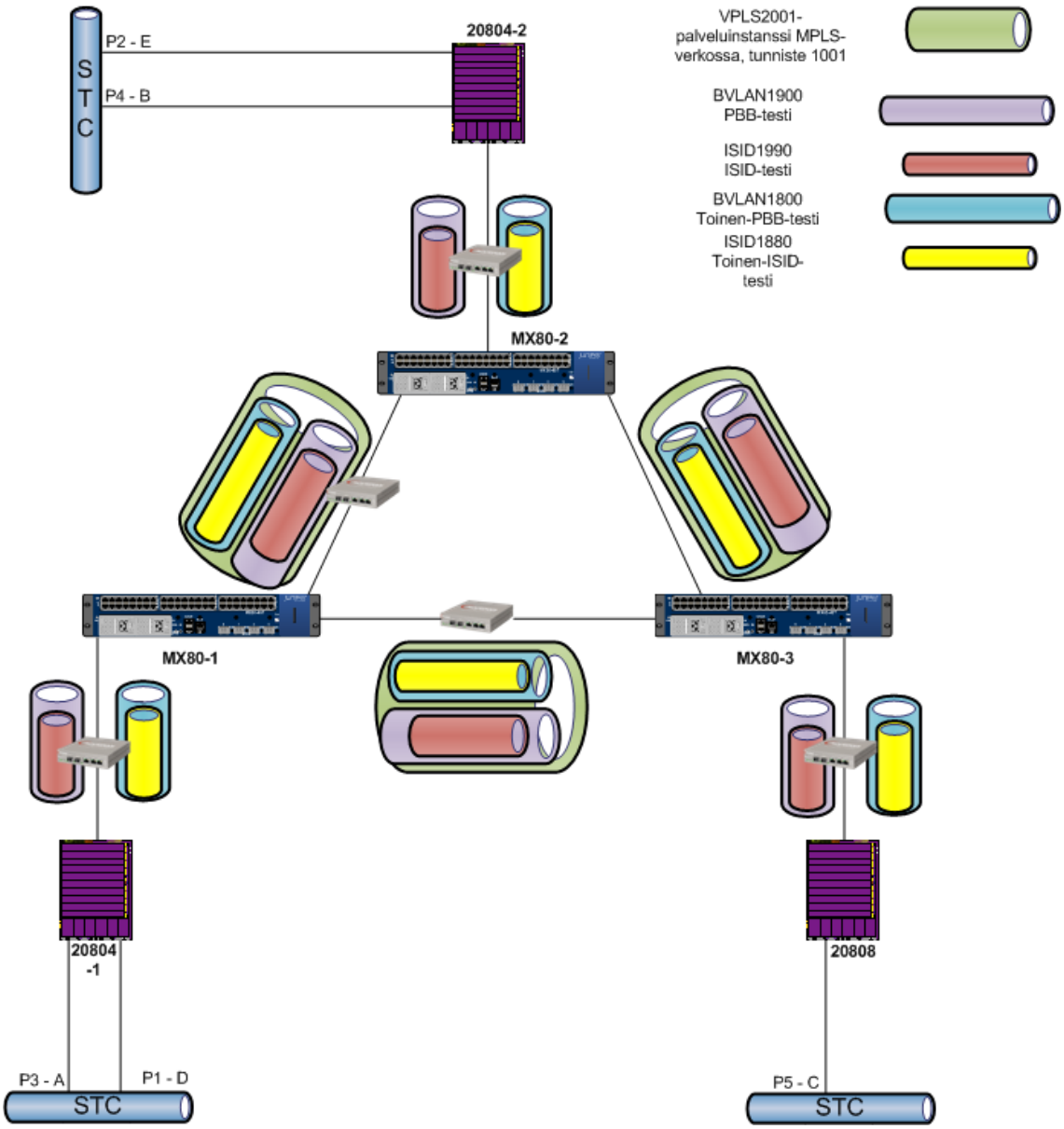
4. Asiakasrajapinnasta A asiakasrajapintaan C (P5) suuntautuva liikenne päälle
5. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
6. Testiliikenne pois ja välitystaulujen tyhjennys
7. Asiakasrajapinnasta D (P1) asiakasrajapintaan E (P2) suuntautuva liikenne päälle
8. Asiakasrajapinnasta E asiakasrajapintaan D suuntautuva liikenne päälle
9. Testiliikenne pois ja välitystaulujen tyhjennys
10. Eri ISID-tunnisteilla merkittyjen asiakaspalveluinstanssien välinen liikenne, jonka ei pidä siirtyä instanssien välillä, päälle
11. Testiliikenne pois
12. Kaikki liikenneparit, joiden tulisi toimia, päälle
13. Testin päättäminen.

3.2.8 PBB-VPLS -tekniikan toteuttaminen viidellä asiakasrajapinnalla ja kahdella BVLAN-tunnisteella

Kun PBB-VPLS -tekniikan käyttäytyminen tilanteessa, jossa kaksi ISID-tunnisteella eroteltua asiakaspalveluinstanssia siirretään käyttäen samaa BVLAN-tunnistetta, oli varmennettu, lisättiin verkkoon toinen BVLAN-tunniste. ISID-tunnisteella 1880 eroteltu asiakaspalveluinstanssi siirrettiin uuteen BVLAN-tunnisteella 1800 määritettyyn loogiseen välitysverkkoon. Tällä testitapauksella kyettiin varmentumaan PBB-VPLS -tekniikan käyttäytymisestä tilanteessa, jossa yhdessä VPLS-palveluinstanssissa siirretään useampaa kuin yhtä BVLAN-tunnisteella eroteltua loogista välitysverkkoa. VPLS-palveluinstanssi ei tässäkään tapauksessa käsitellyt PBB-tekniikan mukaisesti kapseloituja kehyksiä, joten se monisti BVLAN-tunnisteella 1800 merkityn liikenteen myös 20808-kytkimelle, kun MAC-kohdeosoitteeksi oli merkattu MAC-yleislähetysosoite tai jos reitittimet eivät tienneet runkoverkon MAC-kohdeosoitteen sijaintia. BlackDiamond 20808 -kytkin kuitenkin hylkäsi BVLAN-tunnisteella 1800 merkatut kehykset heti ne vastaanottaessaan, koska kyseistä BVLAN-tunnistetta ei ollut määritelty kyseiselle kytkimelle.

Kuvassa 26 esitetään käytetty testitopologia. Kuvassa on merkattu myös BVLAN-tunnisteella 1800 merkatut kehykset MX80-3 -reittimen ja 20808-kytkimen väliin. Tämä liikenne suuntautui ainoastaan reitittimeltä kytkimelle niissä tapauksissa, kun VPLS-palveluinstanssi monisti kyseisen liikenteen 20808-kytkimelle. Kyseistä liikennettä ei siirtynyt kertaakaan 20808-kytkimeltä MX80-3 -reitittimelle. Tätä liikennettä ei muodostunut verkkoon kuin niissä tapauksissa, kun asiakasrajapinta D tai E lähetti liikennettä verkkoon. Asiakasrajapinnat A (P3), B (P4) ja C (P5) kuuluivat BVLAN-tunnisteella 1900 merkattuun loogiseen välitysverkkoon sekä ISID-tunnisteella 1900 merkattuun asiakasinstanssiin. Asiakasrajapinnat D (P1) ja E (P2)

kuuluivat loogiseen välitysverkkoon, joka tunnistettiin BVLAN-tunnisteella 1800 ja näiden asiakasinstanssin ISID-tunniste oli 1880.



Kuva 26: Testiverkon topologia, kun käytössä oli yksi VPLS-palveluinstanssi, kaksi BVLAN-tunnistetta ja kaksi ISID-tunnistetta.

Testiliikennettä generoitaessa toimittiin luvussa 3.2.7 esitettyjen periaatteiden mukaan. Testiliikennettä luotiin niin pitkään, että verkko ehti stabiloitumaan ja jokaisessa välivaiheessa varmennuttiin MAC-osoitteiden leviämisestä ja oppimisesta laitteiden välitystaulujen perusteella. Lisäksi Spirent Testcenter -liikenneanalysaattoria hyödynnettiin viiveiden, viivevaihteluiden sekä kehyshukan havainnointiin. Testiliikenteen luonnissa havaittiin kuitenkin se, että siirtämällä ensin liikennettä asiakasrajapinnasta E asiakasrajapintaan D, voitiin havainnoida verkon käyttäytymistä

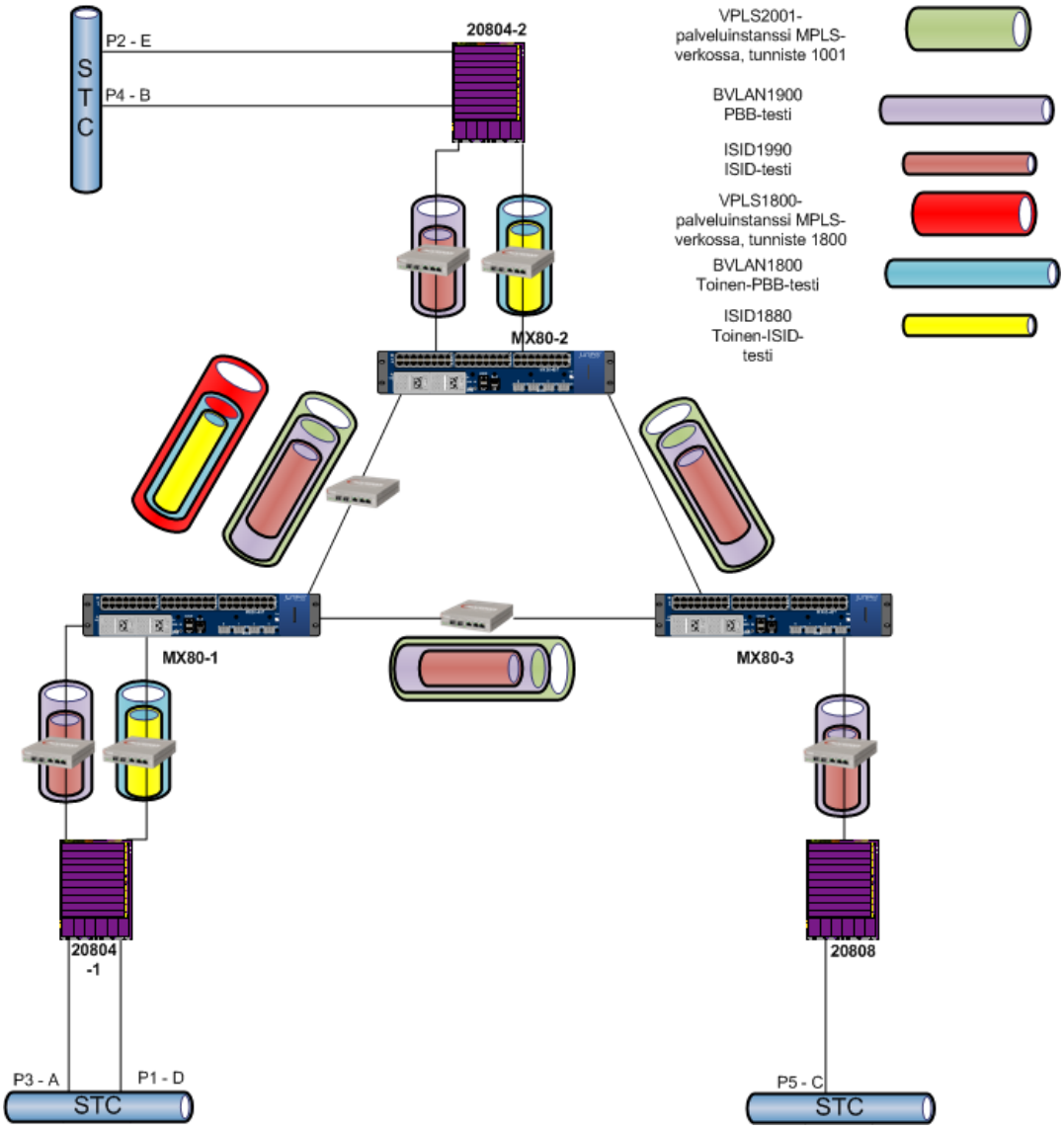
monipuolisemmin. Testiverkkoon luotiin testiliikennettä seuraavalla tavalla:

1. Asiakasrajapinnasta A asiakasrajapintaan B suuntautuva liikenne päälle
2. Asiakasrajapinnasta B asiakasrajapintaan A suuntautuva liikenne päälle
3. Testiliikenne pois ja välitystaulujen tyhjennys
4. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
5. Asiakasrajapinnasta A asiakasrajapintaan C suuntautuva liikenne päälle
6. Testiliikenne pois ja välitystaulujen tyhjennys
7. Asiakasrajapinnasta A asiakasrajapintaan B suuntautuva liikenne päälle
8. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
9. Testiliikenne pois
10. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
11. Testiliikenne pois ja välitystaulujen tyhjennys
12. Asiakasrajapinnasta E asiakasrajapintaan D suuntautuva liikenne päälle
13. Asiakasrajapinnasta D asiakasrajapintaan E suuntautuva liikenne päälle
14. Testiliikenne pois ja välitystaulujen tyhjennys
15. Eri BVLAN-tunnisteilla merkittyjen loogisten verkkojen välinen liikenne, jonka ei pidä siirtyä alueiden välillä, päälle
16. Testiliikenne pois
17. Kaikki liikenneparit, joiden tulisi toimia, päälle
18. Testin päättäminen.

Testin jälkeen päätettiin suorittaa lyhyt testi verkon toimivuudesta, kun kehyskokoja kasvatetaan. Tällöin havaittiin, ettei kaikki liikenne välittynyt verkon lävitse. Syyksi paljastui se, ettei yhteen Ethernid-demarkaatiolaitteeseen oltu määritelty käyttöön normaalia suurempien kehysten (jumbo frames) välittämistä. Normaaliin testiliikenteeseen tällä ei kuitenkaan ollut vaikutusta, koska kehyskoot eivät ylittäneet normaalien kehyskokojen rajoja. Kun yhden Ethernid-demarkaatiolaitteen konfiguraatio oli korjattu, ei kehyskoolla todettu olevan merkitystä käytetyllä siirtonopeudella ja asiakasmäärillä ja kehyskoko palautettiin 128 tavuun.

3.2.9 PBB-VPLS -tekniikan toteuttaminen viidellä asiakasrajapinnalla ja kahdella VPLS-palveluinstanssilla

Viimeinen PBB-VPLS -tekniikkaa hyödyntävää testi oli sellainen, jossa verkkoon lisättiin toinen VPLS-palveluinstanssi, joka tunnistettiin CVLAN-tunnisteella 1800. BVLAN-tunnisteella 1800 erotettu looginen välitysverkko siirrettiin tähän VPLS-palveluinstanssiin. Tällöin molemmissa VPLS-palveluinstansseissa oli yksi BVLAN-tunnisteella erotettu looginen välitysverkko, joista molemmissa oli yksi ISID-tunnisteella tunnistettu asiakaspalveluinstanssi. Tällä testiverkolla kyettiin arvioimaan MAC-osoitteiden leviämistä silloin, kun VPLS-palveluinstansseja on käytössä enemmän kuin yksi kappale.



Kuva 27: Testiverkon topologia, kun käytössä oli kaksi VPLS-palveluinstanssia, BVLAN-tunnistetta ja ISID-tunnistetta.

Kuvassa 27 on esitetty käytössä ollut testiverkko. Ethernid-demarkaatiolaitteita

lisättiin verkkoon kaksi kappaletta, jotta BlackDiamond-kytkimien ja MX80-reitittimien väliset CVLAN-tunnisteiden lisäykset ja poistot kyettiin toteuttamaan. Asiakasrajapinnat A (P3), B (P4) ja C (P5) olivat alkuperäisessä VPLS-palveluinstanssissa. Asiakasrajapinnat D (P1) ja E (P2) siirrettiin uuteen lisättyyn VPLS-palveluinstanssiin. Kuvaan ei ole enää piirretty BVLAN-tunnisteella 1800 merkatun liikenteen välitystä 20808-kytkimelle, koska kyseinen liikenne siirrettiin VPLS-palveluinstanssissa, jota ei ollut määriteltynä MX80-3 -reitittimellä.

Tässä testiverkossa käytettyjen MX80-1 ja 20804-1 -laitteiden konfiguraatiot esitellään liitteissä A ja B. Konfiguraatiot ovat käytännössä identtiset eri laitteiden välillä lukuun ottamatta esimerkiksi rajapintojen IP-osoitteiden määrityksiä. Lisäksi laitteiden asetusten määritykset ovat hyvin samanlaiset kuin luvuissa 3.2.7 ja 3.2.8 esitetyissä testiverkoissa oli käytössä.

Testeissä ei havaittu poikkeamia: VPLS-palveluinstanssien looginen erottelu ja MAC-osoitteiden leviämisen rajaaminen toimivat odotetulla tavalla. Yksityiskohtaisemmat tulokset on esitetty luvuissa 4.2.1 ja 4.2.2. Testiliikennettä luotiin testiverkkoon seuraavassa järjestyksessä:

1. Asiakasrajapinnasta A asiakasrajapintaan B suuntautuva liikenne päälle
2. Asiakasrajapinnasta B asiakasrajapintaan A suuntautuva liikenne päälle
3. Testiliikenne pois ja välitystaulujen tyhjennys
4. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
5. Asiakasrajapinnasta A asiakasrajapintaan C suuntautuva liikenne päälle
6. Testiliikenne pois ja välitystaulujen tyhjennys
7. Asiakasrajapinnasta A asiakasrajapintaan B suuntautuva liikenne päälle
8. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
9. Testiliikenne pois
10. Asiakasrajapinnasta C asiakasrajapintaan A suuntautuva liikenne päälle
11. Testiliikenne pois ja välitystaulujen tyhjennys
12. Asiakasrajapinnasta E asiakasrajapintaan D suuntautuva liikenne päälle
13. Asiakasrajapinnasta D asiakasrajapintaan E suuntautuva liikenne päälle
14. Testiliikenne pois ja välitystaulujen tyhjennys
15. Eri VPLS-palveluinstanssien välinen liikenne, jonka ei pidä siirtyä alueiden välillä, päälle
16. Testiliikenne pois ja välitystaulujen tyhjennys
17. Kaikki liikenneparit, joiden tulisi toimia, päälle
18. Testin päättäminen.

4 Tulokset ja johtopäätökset

Tuloksia esittäessä kiinnitetään erityistä huomiota luvuissa 3.2.7, 3.2.8 ja 3.2.9 esitettyjen testitapauksien tuloksiin. Kaikkien testitapauksien välillä yhteistä oli siinä, että kytkimet asettivat runkoverkon MAC-kohdeosoitteeksi yleislähetykseen tarkoitetun osoitteen tapauksissa, joissa ne eivät vielä olleet oppineet mihin PBB-kytkimeen kohdeasiakas oli kytkeytynyt. Tuloksissa keskitytään pääasiallisesti vastaamaan käytännön testauksen tutkimuskysymyksiin. Tutkimuskysymykset olivat:

1. Pystytäänkö PBB-VPLS -tekniikalla toteutettu verkko rakentamaan ilman erityisesti tämän tekniikan toteuttamiseen kehitettyjä laitteita?
2. Toimiiko tekniikan MAC-osoitteiden skaalautuvuuden parantaminen käytännössä tällaisessa verkossa?

4.1 Tutkimuskysymys 1

Ensimmäiseen tutkimuskysymykseen voidaan vastata tulosten perusteella myönteisesti. Verkkolaitteilla, joita ei ole erityisesti suunniteltu toteuttamaan PBB-VPLS -tekniikka, voidaan luoda PBB-VPLS -tekniikan mukainen tietoliikenneverkko. Tärkeää on kuitenkin huomioida, että eri laitteiden käyttäminen testiverkon mukaisesti ei ole täysin mutkatonta. Jotta tällä tavoin rakennettu verkko toimisi, on PBB-kytkimien ja VPLS-reitittimien rajapintojen väliin lisättävä Ethernid-demarkaatiolaite. Tämän demarkaatiolaitteen tehtävä on lisätä ja poistaa CVLAN-tunnisteita. Toinen tapa luoda PBB-VPLS -tekniikalla toteutettu verkko, on käyttää laitteita, jotka mahdollistavat tekniikan käyttämisen ilman ylimääräisiä demarkaatiolaitteita. Tällaisia laitteita on esimerkiksi Juniper Networksilla, kuten käy ilmi Eantc:n tekemästä tutkimuksesta [40]. Testeissä käytetyt MX80-sarjan reitittimet eivät kuitenkaan tukeneet tätä ominaisuutta.

On myös hyvin todennäköistä, että valmistajan itse toteuttama ratkaisu on yksinkertaisempi ottaa käyttöön kuin kahden eri laitevalmistajien laitteiden, jotka eivät suoranaisesti tue PBB-VPLS -tekniikkaa. Tämä johtuu muun muassa siitä, että valmistajien tekemissä toteutuksissa verkkoon ei lisätä »ylimääräisiä» laitteita, tekemään esimerkiksi CVLAN-tunnisteiden muokkausta. Tällainen ylimääräinen laite heikentää aina verkon luotettavuutta, koska se luo verkkoon uuden yksittäisen pisteen, joka voi vikaantua. Tämän lisäksi verkon ylläpitäjän on konfiguroitava käyttöön otettava ylimääräinen laite. Vikaantumisen lisäksi on siis mahdollista, että verkon ylläpitäjä joko tahallisesti tai tahattomasti määrittää demarkaatiolaitteeseen väärät asetukset, jolloin vikatilanteen selvittäminen on erittäin hankalaa.

Käyttämällä verkkolaitteita, jotka eivät suoraan tue PBB-VPLS -tekniikkaa, mutta tukevat PBB- ja VPLS-tekniikkaa erikseen, voidaan luoda PBB-VPLS -tekniikan mukainen verkko. Testiverkosta käy kuitenkin selväksi se, että tällainen toteutus vaatii ylimääräistä konfiguraatiota, joka on virheherkkää. PBB-VPLS -tekniikalla toteutetun verkon rakentaminen tutkimuskysymyksen 1 mukaisella tavalla ei ole käytännöllistä, vaikka se on mahdollista. Virhekonfiguraatioiden todennäköisyys

on merkittävä ja testeissä käytetty toteutus lisää verkkoon useita laitteita, jotka heikentävät verkon luotettavuutta.

4.2 Tutkimuskysymys 2

Toiseenkin tutkimuskysymykseen voidaan vastata tulosten perusteella myönteisesti. Testiverkossa PBB-tekniikan toteuttavien kytkimien pääasiallinen tarkoitus oli toimia aggregointiverkkona, jonka tehtävänä on oppia asiakkaiden MAC-osoitteet ja piilottaa nämä osoitteet runkoverkossa toimivilta, VPLS-palvelun toteuttavilta, reitittimiltä. Tämän suhteen BlackDiamond 20804 ja 20808 -kytkimet toimivat erittäin hyvin. Asiakaslaitteiden MAC-osoitteita ei valunut testien yhteydessä kertaakaan VPLS-palveluun. Toisin sanoen PBB-tekniikan käyttäminen poistaa asiakaslaitteiden MAC-osoitteiden oppimisen VPLS-verkosta. Reitittimien tulee oppia ainoastaan aggregointiverkossa toimivien kytkinten rajapintojen MAC-osoitteita, joita on huomattavasti vähemmän kuin asiakaslaitteita.

4.2.1 Testit yhdellä VPLS-palveluinstanssilla

Testattaessa tekniikkaa luvuissa 3.2.7 ja 3.2.8 yhdellä VPLS-palveluinstanssilla havaittiin, että MAC-osoitteiden oppiminen tapahtuu PBB-tekniikan laitteissa standardin mukaisesti ja ettei VPLS-palveluinstanssiin valu emuloitujen asiakaslaitteiden MAC-osoitteita. Kaikilla MX80-reitittimillä näkyi VPLS-palveluinstanssin välitystaulussa maksimissaan neljä MAC-osoitetta. Näistä osoitteista kolme oli VPLS-palveluinstanssin asiakasrajapintoihin liitettyjen kytkimien rajapintojen MAC-osoitteet. Neljäs välitystaulussa näkynyt MAC-osoite oli Extreme Networksin Extreme Encapsulation -protokollan käyttämä MAC-osoite (00:e0:2b:00:00:01). VPLS-palveluinstanssi monisti kehyksen kaikille muille kytkimille paitsi lähettäjälle, jos vastaanottajan MAC-osoitteeksi oli merkattu yleislähetysosoite tai reititin ei tiennyt missä kohdeosoite sijaitsee. VPLS-palveluinstanssi ei käsitellyt kehyksien BVLAN- tai ISID-tunnisteita millään tavalla vaan kehykset tunnistettiin VPLS-palveluinstanssiin demarkaatiolaitteiden lisäämien CVLAN-tunnisteiden perusteella.

Alla esitetään kaikkien kolmen MX80-reitittimen VPLS-palveluinstanssin välitystaulut, kun kaikki testiverkossa emuloidut asiakkaat liikennöivät keskenään eli asiakaslaitteiden MAC-osoitteita oli eniten käytössä. VPLS-palveluinstanssien välitystaulut olivat identtiset riippumatta siitä oliko käytössä yksi BVLAN-tunniste ja kaksi ISID-tunnistetta vai kaksi BVLAN-tunnistetta ja kaksi ISID-tunnistetta. Välitystauluista nähdään, että VPLS-palveluinstanssiin opittiin ainoastaan PBB-tekniikkaa toteuttavien kytkimien MAC-osoitteita, joten tekniikan avulla kyettiin piilottamaan asiakaslaitteiden MAC-osoitteet VPLS-palveluinstanssista.

```
MX80-1:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
```

```
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        lsi.1049862
   00:04:96:42:0a:80   D        ge-1/1/5.2
   00:04:96:42:0c:c0   D        lsi.1049863
   00:e0:2b:00:00:01   D        ge-1/1/5.2

MX80-2:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        lsi.1049860
   00:04:96:42:0a:80   D        lsi.1049862
   00:04:96:42:0c:c0   D        ge-1/1/5.2
   00:e0:2b:00:00:01   D        lsi.1049862

MX80-3:

MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        ge-1/1/5.2
   00:04:96:42:0a:80   D        lsi.1049091
   00:04:96:42:0c:c0   D        lsi.1049089
   00:e0:2b:00:00:01   D        lsi.1049091
```

BlackDiamond-kytkimet kuitenkin käsittelevät PBB-tekniikan mukaisesti kapseloidut kehykset täysin, joten kytkimien näkökulmasta ISID- ja BVLAN-tunnisteilla on merkitystä. Kun testiverkossa oli käytössä kaksi ISID-tunnistetta ja yksi BVLAN-tunniste, 20808-kytkin, jossa ei ollut määritettynä ISID-tunnistetta 1880, oppi toisten samaa BVLAN-tunnistetta käyttävien kytkimien MAC-osoitteet myös vastaanottamalla ISID-tunnisteella 1880 merkittyä liikennettä. Kyseisillä ISID-tunnisteilla merkatuista kehyksistä kytkin ei oppinut asiakaslaitteiden MAC-osoitteita. Kytkin kykeni oppimaan toisten kytkimien MAC-osoitteet, koska kyseisiä runkoverkon MAC-osoitteita käytetään kytkimille määritetyn BVLAN-tunnisteen kanssa.

Kun testiverkossa oli käytössä kaksi ISID- ja BVLAN-tunnistetta, 20808-kytkin ei oppinut BVLAN-tunnisteella 1800 merkityistä kehyksistä toisten kytkimien MAC-osoitteita. Tämä johtuu siitä, että kytkimellä ei ollut määritettynä kyseistä BVLAN-tunnistetta, jolloin kytkin hylkäsi kyseisellä tunnisteella merkatut kehykset heti,

kun se vastaanotti sellaisen. Tämäkin käyttäytyminen on PBB-tekniikan standardin mukaista.

Alla esitetään 20804-1 -kytkimen lyhennetyt välitystaulut kun käytössä on kaksi ISID-tunnistetta ja yksi BVLAN-tunniste sekä kaksi BVLAN- ja ISID-tunnistetta. Kytkimen 20808 välitystaulussa ei näkynyt toista ISID- tai BVLAN-tunnistetta kummassakaan testitapauksessa. Varmistus sille, että VPLS-palveluinstanssi monisti kyseiset kehykset 20808-kytkimelle saatiin MX80-3 -reitittimen ja 20808-kytkimen välisestä liikennekaappauksesta.

```
Yksi BVLAN-tunniste, kaksi ISID-tunnistetta:
Mac   Vlan       Age  Flags         Port / Virtual Port List
------------------------------------------------------------------
00:04:96:3f:02:40  pbb-testi(1900) 0027 d o 3:6
00:04:96:42:0c:c0  pbb-testi(1900) 0027 d o 3:6
00:10:90:00:00:01 svlan-pbb-testi(1999) 0000 dhm 3:5
00:10:90:00:00:02 svlan-pbb-testi(1999) 0000 dhm 3:5
...
00:10:90:00:00:19 svlan-pbb-testi(1999) 0000 dhm 3:5
00:88:00:00:00:01 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8
...
00:88:00:00:00:19 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8

Flags : d - Dynamic, s - Static, p - Permanent, n - NetLogin,
m - MAC,  i - IP, x - IPX, l - lockdown MAC,
L - lockdown-timeout MAC, M- Mirror, B - Egress Blackhole,
b - Ingress Blackhole,
v - MAC-Based VLAN, P - Private VLAN, T - VLAN translation,
D - drop packet, h - Hardware Aging,
o - IEEE 802.1ah Backbone MAC,
S - Software Controlled Deletion

Total: 52 Static: 0  Perm: 0  Dyn: 52  Dropped: 0  Locked: 0
Locked with Timeout: 0
FDB Aging time: 2560
Mac-binding
BVLAN             VID   B MAC                SVLAN
VID   CMAC                Flag  Age   Ports
==================================
pbb-testi         1900  00:04:96:42:0c:c0  svlan-pbb-testi
1999  00:80:10:00:00:01  d--   0     3:6
...
pbb-testi         1900  00:04:96:42:0c:c0  svlan-pbb-testi
1999  00:80:10:00:00:19  d--   0     3:6
pbb-testi         1900  00:04:96:3f:02:40  svlan-pbb-testi
1999  22:22:11:11:99:01  d--   0     3:6
...
pbb-testi         1900  00:04:96:3f:02:40  svlan-pbb-testi
1999  22:22:11:11:99:19  d--   0     3:6
```

```
pbb-testi         1900  00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888  00:66:00:00:00:01  d--   0     3:6
...
pbb-testi         1900  00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888  00:66:00:00:00:19  d--   0     3:6

Flags : d - Dynamic, s - Static, p - Permanent

Total: 75 Static: 0 Perm: 0 Dyn: 75


Kaksi BVLAN- ja ISID-tunnistetta:
Mac                      Vlan       Age  Flags         Port
------------------------------------------------------------
00:04:96:3f:02:40  pbb-testi(1900) 0045 d o 3:6
00:04:96:42:0c:c0  pbb-testi(1900) 0045 d o 3:6
00:04:96:42:0c:c0 toinen-pbb-testi(1800) 0045 d o 3:6
00:10:90:00:00:01 svlan-pbb-testi(1999) 0000 dhm 3:5
...
00:10:90:00:00:19 svlan-pbb-testi(1999) 0000 dhm 3:5
00:88:00:00:00:01 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8
...
00:88:00:00:00:19 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8

Total: 53 Static: 0  Perm: 0  Dyn: 53  Dropped: 0  Locked: 0
Mac-binding

BVLAN     VID  B MAC                SVLAN
 VID   CMAC        Flag  Age   Ports
=================================
pbb-testi 1900 00:04:96:42:0c:c0  svlan-pbb-testi
1999 00:80:10:00:00:01  d--   0 3:6
...
pbb-testi 1900 00:04:96:3f:02:40  svlan-pbb-testi
1999 22:22:11:11:99:01  d--   0 3:6
...
pbb-testi 1900 00:04:96:3f:02:40  svlan-pbb-testi
1999 22:22:11:11:99:19  d--   0 3:6
toinen-pbb-testi 1800 00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888 00:66:00:00:00:01  d--   0 3:6
...
toinen-pbb-testi 1800 00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888 00:66:00:00:00:19  d--   0 3:6

Total: 75 Static: 0 Perm: 0 Dyn: 75
```

Luvuissa 3.2.7 ja 3.2.8 esitettyjen testien perusteella voidaan siis todeta, että asiakaslaitteiden MAC-osoitteet eivät näy VPLS-palveluinstanssin välitystaulussa,

kun aggregointiverkko on toteutettu PBB-tekniikalla. Lisäksi voidaan todeta, että PBB-tekniikan toteuttavien kytkimien MAC-osoitteiden oppiminen on täysin riippuvainen siitä mitkä BVLAN- ja ISID-tunnisteet on määritetty kytkimen asetuksiin. Yhteenvetona voidaankin siis sanoa:

- VPLS-palveluinstanssin välitystauluun opitaan ainoastaan PBB-tekniikan toteuttavien kytkimien MAC-osoitteita
- PBB-tekniikan kytkimet oppivat toisten kytkimien MAC-osoitteet BVLAN-tunnisteiden perusteella
- PBB-tekniikan kytkimet oppivat asiakaslaitteiden MAC-osoitteet ISID-tunnisteiden perusteella.

4.2.2 Testi kahdella VPLS-palveluinstanssilla

VPLS-tekniikassa jokaiselle VPLS-palveluinstanssille luodaan oma välitystaulu. Testeissä havaittiin, että näihin välitystauluihin opittiin PBB-tekniikkaa toteuttavien kytkimien MAC-osoitteet. VPLS-palveluinstanssien rajapinnat erotettiin Ethernid-demarkaatiolaitteiden lisäämien CVLAN-tunnisteiden perusteella. Opitut MAC-osoitteet eivät vaikuttaneet toisen VPLS-palveluinstanssin toimintaan eikä näiden palveluinstanssien välistä liikennettä sallittu.

Ensimmäisessä VPLS-palveluinstanssissa esiintyi enintään neljä MAC-osoitetta: kolmen kytkimen MAC-osoitteet sekä EEP-protokollan osoite. Toisessa VPLS-palveluinstanssissa esiintyi maksimissaan kolme MAC-osoitetta: kahden kytkimen MAC-osoitteet sekä EEP-protokollan osoite. Lisäksi testissä BVLAN-tunnisteilla erotellut loogiset verkot olivat eriytettyinä eri VPLS-palveluinstansseihin, eli VPLS-palveluverkko ei monistanut ensimmäisellä BVLAN-tunnisteella merkattuja kehyksiä toista BVLAN-tunnistetta käyttäviin rajapintoihin.

Alla esitetään kaikkien MX80-sarjan reitittimien VPLS-palveluinstanssien välitystaulut, kun maksimimäärä emuloituja asiakaslaitteita liikennöi keskenään. Välitystauluista nähdään, että PBB-tekniikalla toteutettu aggregointiverkko piilotti asiakaslaitteiden MAC-osoitteet VPLS-palveluinstansseilta.

```
MX80-1:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan1800
 Bridging domain : __vpls-vlan1800__, VLAN : 1800
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:42:0a:80   D        ge-1/1/6.2
   00:04:96:42:0c:c0   D        lsi.1049865
   00:e0:2b:00:00:01   D        lsi.1049865

MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)
```

```
Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        lsi.1049867
   00:04:96:42:0a:80   D        ge-1/1/5.2
   00:04:96:42:0c:c0   D        lsi.1049866
   00:e0:2b:00:00:01   D        lsi.1049867

MX80-2:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan1800
 Bridging domain : __vpls-vlan1800__, VLAN : 1800
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:42:0a:80   D        lsi.1049865
   00:04:96:42:0c:c0   D        ge-1/1/6.2

MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        lsi.1049860
   00:04:96:42:0a:80   D        lsi.1049864
   00:04:96:42:0c:c0   D        ge-1/1/5.2
   00:e0:2b:00:00:01   D        lsi.1049860

MX80-3:
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls-vlan2001
 Bridging domain : __vpls-vlan2001__, VLAN : 1001
   MAC                 MAC      Logical
   address             flags    interface
   00:04:96:3f:02:40   D        ge-1/1/5.2
   00:04:96:42:0a:80   D        lsi.1049092
   00:04:96:42:0c:c0   D        lsi.1049089
   00:e0:2b:00:00:01   D        ge-1/1/5.2
```

PBB-tekniikan toteuttavien kytkimien toiminnassa ei havaittu muutoksia luvuissa 3.2.7, 3.2.8 ja 3.2.9 esiteltyjen testien välillä. Merkittävin ero viime luvussa esitettyihin

tuloksiin on se, ettei VPLS-palveluverkko monistanut kehyksiä BVLAN-tunnisteilla merkattujen loogisten verkkojen välillä, jolloin kytkimille ei siirretty kehyksiä, joita niiden olisi pitänyt hylätä. Alla esitetään kytkimen 20804-1 välitystaulut lyhennetyssä muodossa, kun kaikki emuloidut asiakaslaitteet liikennöivät keskenään. Kytkimen 20808 välitystauluissa ei näkynyt yhtään toisella BVLAN-tunnisteella merkittyä osoitetta, koska kyseisellä kytkimellä ei ollut määriteltynä kyseistä tunnistetta eikä VPLS-palveluverkko monistanut sellaisia kehyksiä 20808-kytkimelle.

```
Mac      Vlan       Age  Flags         Port / Virtual Port List
-----------------------------------------------------------
00:04:96:3f:02:40  pbb-testi(1900) 0040 d o 3:6
00:04:96:42:0c:c0  pbb-testi(1900) 0040 d o 3:6
00:04:96:42:0c:c0 toinen-pbb-testi(1800) 0040 d o 3:7
00:10:90:00:00:01 svlan-pbb-testi(1999) 0000 dhm 3:5
...
00:10:90:00:00:19 svlan-pbb-testi(1999) 0000 dhm 3:5
00:88:00:00:00:01 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8
...
00:88:00:00:00:19 toinen-svlan-pbb-testi(1888) 0000 dhm 3:8

Total: 53 Static: 0  Perm: 0  Dyn: 53  Dropped: 0  Locked: 0
Mac-binding
BVLAN             VID  B MAC                SVLAN
VID  CMAC               Flag  Age   Ports
=======================================
pbb-testi         1900  00:04:96:42:0c:c0  svlan-pbb-testi
1999  00:80:10:00:00:01  d--   0     3:6
...
pbb-testi         1900  00:04:96:42:0c:c0  svlan-pbb-testi
1999  00:80:10:00:00:19  d--   0     3:6
pbb-testi         1900  00:04:96:3f:02:40  svlan-pbb-testi
1999  22:22:11:11:99:01  d--   0     3:6
...
pbb-testi         1900  00:04:96:3f:02:40  svlan-pbb-testi
1999  22:22:11:11:99:19  d--   0     3:6
toinen-pbb-testi  1800  00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888  00:66:00:00:00:01  d--   0     3:7
...
toinen-pbb-testi  1800  00:04:96:42:0c:c0  toinen-svlan-pbb-testi
1888  00:66:00:00:00:19  d--   0     3:7

Total: 75 Static: 0 Perm: 0 Dyn: 75
```

Tuloksista nähdään, että PBB-VPLS -tekniikalla kyetään hyödyntämään sekä PBB- että VPLS-tekniikan vahvuuksia. Asiakaslaitteiden MAC-osoitteet kyetään piilottamaan VPLS-palveluinstansseilta ja riippuvuutta Spanning Tree -protokollaan kyetään vähentämään. Yhteenveto esitetään taulukossa 6.

Taulukko 6: Yhteenveto havainnoista.

VPLS-palveluinstanssin välitystauluun opitaan ainoastaan PBB-tekniikan toteuttavien kytkimien MAC-osoitteita.
Kytkimien MAC-osoitteet opitaan ainoastaan niihin VPLS-palveluinstansseihin, joihin ne kuuluvat.
VPLS-palveluinstanssiin kuuluvat yhteydet tunnistetaan Ethernid-demarkaatiolaitteen lisäämän CVLAN-tunnisteen perusteella.
PBB-tekniikan kytkimet oppivat toisten kytkimien MAC-osoitteet BVLAN-tunnisteiden perusteella.
PBB-tekniikan kytkimet oppivat asiakaslaitteiden MAC-osoitteet ISID-tunnisteiden perusteella.

PBB-VPLS -tekniikalla toteutetun verkon rakentaminen on kuitenkin erittäin haastavaa, mikäli käytössä on laitteita, jotka eivät tue PBB-VPLS -tekniikkaa ilman ylimääräisiä verkkolaitteita. Tällainen verkko, jota käytettiin esimerkiksi testauksessa, sisältää monta konfiguroitavaa verkkoelementtiä, jolloin verkon hallittavuus heikkenee. Lisäksi mahdollisten tahallisesti tai tahattomasti tehtyjen virhekonfiguraatioiden selvittäminen muodostuu hankalaksi.

4.3 Muut huomiot

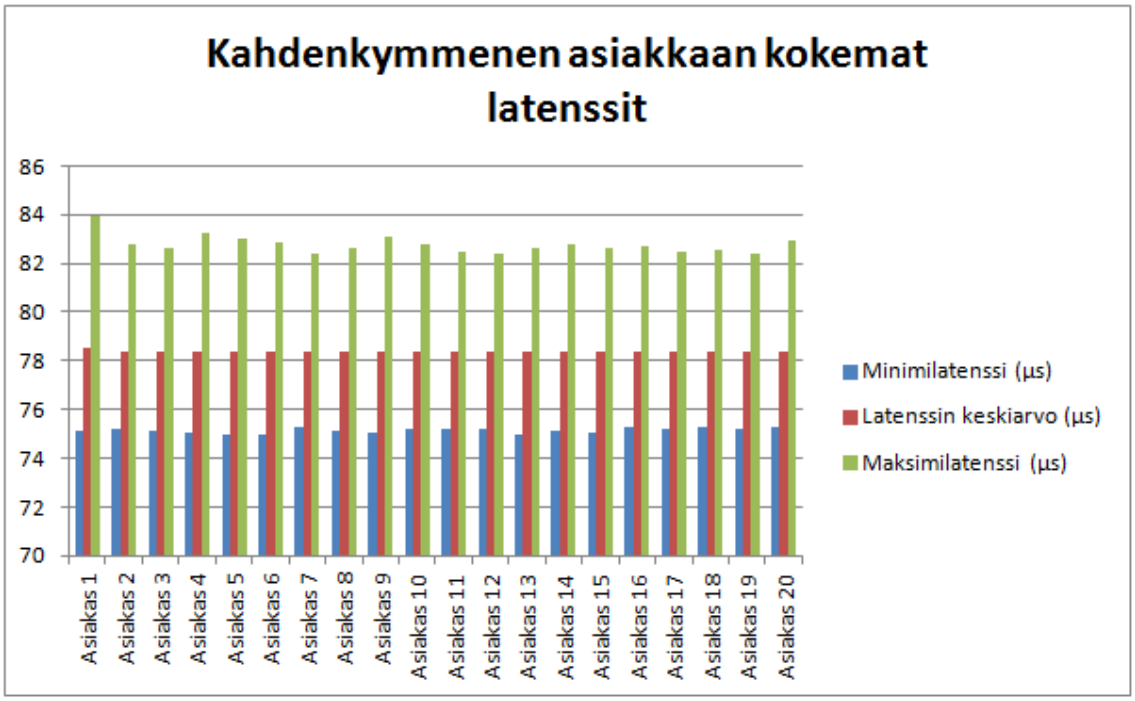
Asiakasliikenteen looginen erottelu, joka voidaan toteuttaa PBB-tekniikan ISID-tunnisteella tai BVLAN-tunnisteella tai VPLS-tekniikan VPLS-palveluinstansseilla, ei ollut tutkimuksen pääaiheena. Tästä huolimatta tutkimuksen tulosten perusteella tästä voidaan esittää tiettyjä havaintoja. VPLS-tekniikalla toteutetussa verkossa aggregointiverkon MAC-osoitteiden oppiminen tapahtuu erikseen jokaisessa VPLS-palveluinstanssissa. PBB-tekniikassa asiakaslaitteiden oppiminen tapahtuu ISID-tunnisteiden perusteella ja kytkimien MAC-osoitteiden oppiminen BVLAN-tunnisteiden perusteella. Periaatteessa PBB-VPLS -tekniikalla toteutetulla verkolla on hyvät mahdollisuudet rakentaa erilaisia loogisesti eroteltuja verkkoja usealla eri tasolla. Mikäli koko palveluverkko on yhden toimijan hallittavissa, eri liikennevirrat voidaan erottaa loogisesti ensin ISID-tunnisteen avulla, sitten BVLAN-tunnisteella ja lopuksi VPLS-palveluinstanssien perusteella. Tässä tutkimuksessa ei kuitenkaan voitu varmentaa näiden loogisten erotteluiden varmuutta täysin, koska toiminnallisuuden varmentaminen edellyttää huomattavasti raskaampaa kuormitusta pitkällä aikavälillä. Testien yhteydessä ei kuitenkaan havaittu yhtään tapausta, jossa MAC-osoitteita tai liikennettä olisi vuotanut loogisesti eroteltujen alueiden välillä.

Testauksessa ei ollut käytössä hallintajärjestelmiä BlackDiamond-kytkimien tai MX80-reitittimien konfiguroimiseen. Tämä ei aiheuttanut ongelmia testiverkossa koska testiverkko oli kooltaan pieni. Testauksen yhteydessä havaittiin kuitenkin se, että asiakasinstanssien lukumäärän kasvaessa muodostuu erityisesti PBB-tekniikkaan määritettävien ISID- ja BVLAN-tunnisteiden konfigurointi erittäin työlääksi. Siksi

on suositeltavaa, että suuremmissa verkoissa käytettäisiin hallintajärjestelmää, jotta mahdollisilta virhekonfiguraatioilta kyettäisiin välttymään.

Aina kun kehyksen MAC-kohdeosoitteena on yleislähetysosoite, VPLS-tekniikka monistaa kehyksen kaikille VPLS-palveluinstanssiin osallistuville reitittimille. PBB-tekniikka puolestaan merkkaa kehyksen vastaanottajaksi yleislähetysosoitteen aina, kun se ei tiedä vastaanottajan tarkkaa sijaintia. Tästä syystä on mahdollista, että PBB-VPLS -tekniikalla toteutetussa verkossa voi siirtyä huomattavat määrät liikennettä, joten verkkoa suunniteltaessa on huomioitava se, ettei VPLS-palveluverkko pääse ylikuormittumaan mahdollisen kehysten monistamisen takia.

Testiverkoissa mitattiin myös emuloitujen asiakkaiden kokemat latenssit. Kun asiakaskehys siirrettiin kolmen Ethernid-demarkaatiolaitteen, kahden PBB-tekniikan kytkimen ja kahden VPLS-palveluinstanssiin osallistuvan reitittimen lävitse, kehyksen kesimääräinen latenssi oli hieman yli 78 mikrosekuntia. Tässä ajassa valosignaali etenee valokuidussa noin 15,5km. Kahdenkymmenen sattumanvaraisesti valitun emuloidun asiakkaan kokemat minimi-, keskiarvo- ja maksimilatenssit esitetään kuvassa 28. Vaikka latenssit eivät ole suuria, havaittiin että kapseloinnin ja sen purkamisella on selkeä vaikutus latensseihin. Tämä ei kuitenkaan ollut työn kannalta oleellista, joten sitä ei käsitellä tämän työn yhteydessä tarkemmin.



Kuva 28: Kahdenkymmenen sattumanvaraisesti valitun emuloidun asiakkaan kokemat latenssit PBB-VPLS -tekniikkalla toteutussa verkossa.

5 Tulosten arviointi ja mahdollinen jatkotutkimus

Testimenetelmiä valittaessa kiinnitettiin huomiota siihen, että mahdolliset mittaus- tai konfiguraatiovirheet kyetään tunnistamaan mahdollisimman todennäköisesti, jotta ne eivät aiheuta virheitä tuloksiin. Tästä syystä, kun tuloksia mitattiin, ei luotettu pelkästään laitevalmistajien komentoliittymien ilmoittamiin tietoihin vaan lisäksi tiedot varmennettiin verkosta otetuilla liikennekaappauksilla. Testimenetelmiä käytettiin myös välittömästi, kun testiverkkoa alettiin rakentaa. Näin toimimalla oli mahdollista havaita asioita, jotka mahdollistivat laadukkaampien tulosten saamisen. Yksi esimerkki tällaisesta havainnosta oli se, että muuttamalla testiliikenteen generoimisjärjestystä alkuperäisestä, voidaan testituloksista nähdä paremmin MAC-osoitteiden leviäminen. Tällä tavoin toimimalla testejä saatiin myös toistettua useita kertoja, jotta mahdolliset poikkeamat olisivat tulleet esille. Näistä syistä johtuen, testituloksia voidaan pitää luotettavina ja oikeina.

Tuloksia voidaan pitää laadukkaina, koska niiden avulla kyettiin vastaamaan ennen testejä määritettyihin tutkimuskysymyksiin. Lisäksi tulosten perusteella havaittiin, ettei eri laitevalmistajien laitteiden yhdistäminen tavalla, jota käytettiin testiverkossa, ole soveltuva tuotantoverkkoon. Tämä johtuu siitä, että testiverkossa käytetty toteutus on erittäin hankala ylläpitää verkon laajentuessa. PBB-VPLS -tekniikkaa voidaan kuitenkin hyödyntää myös tuotantoverkoissa, kunhan verkko toteutetaan siten, että se on ylläpidettävissä.

Tämän tutkimuksen käytännön testien yhteydessä ei selvitetty esimerkiksi PBB-VPLS -verkon maksimikapasiteettia. Myöskään PBB-VPLS -verkon vikasietoisuutta tai liitettävyyttä muihin verkkoihin ei tutkittu. Esimerkiksi näistä asioista on mahdollista tehdä jatkotutkimusta. Toinen mahdollinen jatkotutkimusaihe on eri tasojen loogisten erottelukykyjen varmentaminen. Tämä varmentaminen vaatii huomattavasti pidempiaikaista tutkimusta kuin mitä oli mahdollista tämän tutkimuksen yhteydessä suorittaa. Koska diplomityön yhteydessä testattiin ainoastaan MAC-osoitteiden skaalautuvuuden periaate, on aiheesta mahdollista tehdä useita jatkotutkimuksia.

6 Yhteenveto

Tämän tutkimuksen ensimmäisenä tehtävänä toteutettiin kirjallisuustutkimus, joka kattaa PB, PBB, PBB-TE, VPLS, H-VPLS ja MPLS-TP -tekniikat. Näiden tekniikoiden toimintaperiaatteet esitettiin, jonka jälkeen suoritettiin kirjallisuustutkimuksen perusteella tekniikoiden vertailu, jossa huomioitiin seuraavat asiat:

- Skaalautuvuus: verkko, liitännät, palvelut ja asiakkaat
- Hallittavuus: palvelu, laatu ja verkko
- Toimintavarmuus: vikasietoisuus ja toipuvuus
- Tietoturvauhkat: palveluestot ja kuuntelu, protokollat ja tilakoneet
- Liitettävyys: kyky liittyä ulkoisiin verkkoihin ja palveluihin tai kyky hyödyntää ulkoisia verkkoja osana palvelua

Vertailun tuloksena havaittiin, että PBB-TE, MPLS-TP sekä PBB-VPLS -tekniikat ovat parhaita vaihtoehtoja käytettäväksi verkkotekniikaksi.

Toinen työhön liittyvä tehtävä oli luoda kirjallisuustutkimuksen perusteella katsaus optisiin siirtojärjestelmiin. Tämän selvityksen perusteella voidaan sanoa, että tulevaisuudessa käytettävät optiset siirtojärjestelmät hyödyntävät todennäköisesti aallonpituuteen pohjautuvaa multipleksointia eli WDM-tekniikkaa. Tekniikka skaalautuu paremmin kuin aikajaksoihin perustuva multipleksointi eli TDM-tekniikka. On myös mahdollista, että tulevaisuuden optiset siirtojärjestelmät hyödyntävät molempia tekniikoita samanaikaisesti.

Käytännön testeissä selvitettiin vastaukset kahteen tutkimuskysymykseen:

1. Pystytäänkö PBB-VPLS -tekniikalla toteutettu verkko rakentamaan, ilman erityisesti tämän tekniikan toteuttamiseen kehitettyjä laitteita?
2. Toimiiko tekniikan MAC-osoitteiden skaalautuvuuden parantaminen käytännössä tällaisessa verkossa?

Testien perusteella molempiin tutkimuskysymyksiin voidaan vastata myönteisesti. Testiverkko jouduttiin kuitenkin rakentamaan siten, että vastaavaa ratkaisua ei suositella käytettäväksi tuotantoverkkoihin. Suositeltu tapa toteuttaa PBB-VPLS -tekniikalla toteutettu verkko on käyttää verkkolaitteita, jotka eivät vaadi ulkopuolisia lisälaitteita. PBB-VPLS -tekniikassa ei kuitenkaan havaittu sellaisia puutteita, ettei tekniikkaa voisi käyttää tuotantoverkoissa. Tekniikkaa valittaessa on tärkeää huomioida sen vahvuudet ja heikkoudet sekä verrata onko kyseinen tekniikka paras vaihtoehto, kun otetaan huomioon verkon käyttötarkoitukset ja muut ominaisuudet.

Ennustaminen on vaikeaa. Tulevaisuuden ennustaminen on vielä vaikeampaa, joten työssä on esitetty ainoastaan arvioita siitä, mitkä verkkotekniikat ja optiset siirtojärjestelmät ovat todennäköisesti merkittävässä asemassa tulevaisuudessa. Tulosten perusteella voidaan lisäksi arvioida, että erinäiset tekniikkayhdistelmät voivat olla merkittävä ratkaisumalli, suunniteltaessa verkkojen päivityksiä. Tekniikkayhdistelmiä ovat esimerkiksi työssä esitetty PBB-VPLS tai WDM- ja TDM-tekniikoiden

käyttämien yhdessä optisessa siirtojärjestelmässä. Tällaisia tekniikkayhdistelmiä käyttämällä voi olla mahdollista hyödyntää olemassa olevia verkkoja huomattavasti nykyistä tehokkaammin. Näin voidaan välttyä suurilta investoinneilta, koska verkkoinfrastruktuuria ei tarvitse uudistaa täysin.

Viitteet

[1] Allan, D., Bragg, N., McGuire, A. ja Reid, A. Ethernet as carrier transport infrastructure. *IEEE Communications Magazine,* 2006, vol. 44, nro 2, s. 95–101.

[2] Pallos, R., Farkas, J., Moldovan, I. ja Lukovszki, C. Performance of rapid spanning tree protocol in access and metro networks. *Second International Conference on Access Networks & Workshops,* 2007, s. 1–8.

[3] TPACK. PBB-TE, PBT Carrier Grade Ethernet Transport whitepaper. Toinen versio. Verkkodokumentti. Päivitetty kesäkuu 2007. Viitattu 20.6.2011. Saatavissa: http://www.tpack.com/resources/tpack-white-papers/pbb-te-pbt.html.

[4] Kasim, Abdul. Delivering carrier Ethernet: extending Ethernet beyond the LAN. New York, McGraw-Hill, 2007.

[5] Salam, S., Sajassi, A. Provider Backbone Bridging and MPLS: Complementary Technologies for Next-Generation Carrier Ethernet Transport *IEEE Communications Magazine,* 2008, vol. 46, nro 3, s. 77–83.

[6] Juniper Networks. Technical documentation, Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX series Routers Verkkodokumentti. Päivitetty 28.10.2009. Viitattu 29.8.2011. Saatavissa: http://www.juniper.net/techpubs/en_US/junos10.0/topics/example/pbb-eline-elan-mx-series-configuring.html.

[7] Metro Ethernet Forum. What is Carrier Ethernet? Verkkodokumentti. Viitattu 20.6.2011. Saatavissa: http://metroethernetforum.org/page_loader.php?p_id=140.

[8] Fujitsu Network Communications. Understanding PBB-TE for Carrier Ethernet whitepaper. Verkkodokumentti. 2008. Viitattu 21.6.2011. Saatavissa: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/UnderstandingPBBTE.pdf.

[9] Kompella, K., Rekhter, Y. 2007 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. RFC 4761.

[10] Lasserre, M., Kompella, V. 2007 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. RFC 4762.

[11] Juniper Networks. LDP-BGP VPLS Interworking whitepaper. Verkkodokumentti. Päivitetty 2009. Viitattu 22.6.2011. Saatavissa: http://kb.juniper.net/library/CUSTOMERSERVICE/GLOBAL_JTAC/technotes/2000282-en.pdf.

[12] Extreme Networks. ExtremeXOS Concept Guide, Software version 12.5.2. Verkkodokumentti. Päivitetty Helmikuu, 2011. Viitattu 22.6.2011. Saatavissa: http://www.extremenetworks.com/libraries/services/EXOSConcepts12_5_2.pdf.

[13] Extreme Networks. Ridgeline Concepts and Solutions Guide, Software Version 3.0. Verkkodokumentti. Julkaistu Helmikuu, 2011. Viitattu 22.6.2011. Saatavissa: http://www.extremenetworks.com/libraries/services/Ridgeline_Concepts_and_Solutions_Guide_V1.pdf.

[14] Juniper Networks. MPLS TRANSPORT PROFILE (MPLS-TP), A Set of Enhancements to the Rich MPLS Toolkit. Verkkodokumentti. Julkaistu 2011. Viitattu 23.6.2011. Saatavissa: http://www.juniper.net/us/en/local/pdf/whitepapers/2000406-en.pdf.

[15] Luoma, M. S-38.3191 Verkkopalvelujen tuotanto, luento 4: MPLS. Kurssin Verkkopalvelujen tuotanto luentokalvot. Aalto-yliopisto, Tietoliikenne- ja tietoverkkotekniikan laitos, Espoo. 15.9.2011.

[16] Wang, P., Chan, C. ja Lin, P. MAC Address Translation for Enabling Scalable Virtual Private LAN Services. *21st International Conference on Advanced Information Networking and Applications Workshops,* 2007, vol. 1, s. 870–875.

[17] Parsons, G. Ethernet Bridging Architecture [Standards Topics] *IEEE Communications Magazine,* 2007, vol. 45, nro 12, s. 112–119.

[18] Santos, D. et al. Traffic Engineering of Multiple Spanning Tree Routing Networks: the Load Balancing Case. *Next Generation Internet Networks,* 2009, s. 1–8.

[19] Chiruvolu, G., Ge, A., Elie-Dit-Cosaque, D., Ali, M. ja Rouyer, J. Issues and approaches on extending Ethernet beyond LANs. *IEEE Communications Magazine,* 2004, vol. 42, nro 3, s. 80-86.

[20] Cisco. Cisco ME 3400E Ethernet Access Switch Software Configuration Guide, Rel. 12.2(58)SE. Verkkodokumentti. Päivitetty 11.1.2008. Viitattu 23.6.2011. Saatavissa: http://www.cisco.com/en/US/docs/switches/metro/me3400e/software/release/12.2_58_se/configuration/guide/swqos.html#wp1701620.

[21] Juniper Networks. Cross-Domain VPLS Deployment Strategies, Scaling and Extending VPLS with LDP-BGP VPLS Interworking. Verkkodokumentti Julkaistu 2010. Viitattu 24.6.2011. Saatavissa: http://www.juniper.net/us/en/local/pdf/whitepapers/2000279-en.pdf.

[22] Juniper Networks. Example: Configuring Connectivity Fault Management for a PBB Network on MX Series Routers. Verkkodokumentti Julkaistu 28.10.2009. Viitattu 24.6.2011. Saatavissa: http://www.juniper.net/techpubs/en_US/junos10.0/topics/example/pbb-cfm-mx-series-configuring.html.

[23] Juniper Networks. Understanding Fault Isolation and Detection in a PBB using Connectivity Fault Management for MX Series Routers. Verkkodokumentti Julkaistu 19.10.2009. Viitattu 24.6.2011. Saatavissa: http://www.juniper.net/techpubs/en_US/junos10.0/topics/concept/pbb-cfm-understanding.html.

[24] Luyuan, F., Zhang, R., Taylor, M. The evolution of carrier ethernet services-requirements and deployment case studies [next-generation carrier ethernet]. *IEEE Communications Magazine,* 2008, vol. 46, nro 3, s. 69–76.

[25] Hoffmans, J. et al. 2007. VPLS Extensions for Provider Backbone Bridging. Internet-Draft draft-balus-l2vpn-vpls-802.1ah-03.txt, Internet Engineering Task Force. Work in progress.

[26] Hoffmans, J. et al. 2011. Extensions to VPLS PE model for Provider Backbone Bridging. Internet-Draft draft-ietf-l2vpn-pbb-vpls-pe-model-04.txt, Internet Engineering Task Force. Work in progress.

[27] Kuusivaara, J. S-38.116 Teletietotekniikka: Optiikan käyttö tiedonsiirtotekniikassa. Verkkodokumentti. 2007. Viitattu 26.1.2012. Saatavissa: http://www.netlab.tkk.fi/opetus/s38116/1997/esitelmat/41712j/.

[28] Viestintävirasto, Valokaapelityöryhmä. Optiset liityntäverkot. Verkkodokumentti. Päivitetty 26.2.2009. Viitattu 26.1.2012. Saatavissa: http://www.ficora.fi/attachments/suomiry/5f1Eutml7/TRaportti012006v2.pdf.

[29] Theodoras, J., Rettenberger, S. Introducing WDM into Next-Generation Access Networks. Verkkodokumentti. Päivitetty elokuu 2009. Viitattu 27.1.2012. Saatavissa: http://www.advaoptical.com/~/media/Resources/White%20Papers/WP_WDM_PON.ashx.

[30] Transmode. WDM-PON: A key component in next generation access. Verkkodokumentti. Päivitetty 21.9.2011. Viitattu 27.1.2012. Saatavissa: http://www.transmode.se/doc_download/534-wdm-pon-a-key-component-in-next-gen-access.

[31] ITU-T. 2009. G.984.1 : Gigabit-capable passive optical networks (GPON): General characteristics. International Telecommunication Union.

[32] Grobe, K., Elbers, J.-P. PON in adolescence: from TDMA to WDM-PON. *IEEE Communications Magazine,* 2008, vol. 46, nro 1, s. 26–34.

[33] Grobe, K., Elbers, J.-P. WDM-PON - A Platform for consolidated Metro Access and Backhaul. *2008 ITG Symposium on Photonic Networks,* 2008, s. 1–5.

[34] Hajduczenia, M., da Silva, H.J.A. Next generation PON systems - Current status. *11th International Conference on Transparent Optical Networks,* 2009, s. 1–8.

[35] ITU-T. 2011. G.987, 10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations, and acronyms. International Telecommunication Union.

[36] ITU-T. 2010. G.987.1, 10-Gigabit-capable passive optical networks (XG-PON): General requirements. International Telecommunication Union.

[37] ITU-T. 2012. G.987.2, 10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification. International Telecommunication Union.

[38] ITU-T. 2011. G.987.3, 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification. International Telecommunication Union.

[39] Juniper Networks. Encapsulation (Physical Interface). Verkkodokumentti. Päivitetty 3.1.2012. Viitattu 12.6.2012. Saatavissa: https://www.juniper.net/techpubs/en_US/junos/topics/reference/configuration-statement/encapsulation-edit-interfaces-physical.html.

[40] Eantc. Juniper Networks MX Series 3D with Junos Trio Chipset Performance, Scalability and Power Efficiency Validation. Verkkodokumentti. Päivitetty 16.10.2009. Viitattu 3.8.2012. Saatavissa: http://www.eantc.de/fileadmin/eantc/downloads/test_reports/2009-2011/EANTC-Juniper-MX-Marketing_Report-1.2.pdf.

A MX80-1 -reitittimen konfiguraatio

Tässä liitteessä esitetään luvussa 3.2.9 kuvatussa testiympäristössä käytetty konfiguraatio MX80-1 -reitittimestä. Konfiguraatiosta esitetään ne kohdat, jotka ovat merkityksellisiä testin kannalta. Käytössä olleilla rajapinnoilla otettiin käyttöön normaalia suurempien kehysten (jumbo frames) siirto, jotta kapseloinneista johtuvat normaalia suuremmat kehykset pystyttiin siirtämään verkon lävitse. MX80-3 -reitittimellä ei ole määritettynä asiakasrajapintaa »ge-1/1/6», koska reititin ei palvele kyseistä VPLS-palveluinstanssia. Käytetty AS-numero valittiin yksityiseen käyttöön tarkoitetulta numeroalueelta. Laitteiden annettiin itse rakentaa välitysleimat verkkotopologian perusteella, joka saatiin hyödyntämällä ISIS-protokollaa. BGP-reititysprotokollaa käytettiin mm. VPLS-palveluiden signalointiin. LDP-protokollaa tarvittiin, koska käytössä ollut VPLS-toteutus käytti sitä palveluiden signalointiin. Käytössä olleet VPLS-palveluinstanssit määritettiin »routing-instances» -osioon konfiguraatiota. Palveluinstanssiin »VPLS-VLAN1800» määritetään ainoastaan yksi naapuri, koska kyseinen palveluinstanssi on käytössä ainoastaan MX80-1 ja MX80-2 -reitittimillä.

```
version 10.3R2.11;
interfaces {
    ge-1/1/2 {
        mtu 9192;
        unit 0 {
            family inet {
                address 10.0.1.25/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-1/1/4 {
        mtu 9192;
        unit 0 {
            family inet {
                address 10.0.1.17/30;
            }
            family iso;
            family mpls;
        }
    }
    ge-1/1/5 {
        vlan-tagging;
        mtu 9192;
        encapsulation flexible-ethernet-services;
        unit 2 {
            description LDP-VPLS;
            encapsulation vlan-vpls;
```

```
            vlan-id 1001;
        }
    }
    ge-1/1/6 {
        vlan-tagging;
        mtu 9192;
        encapsulation flexible-ethernet-services;
        unit 2 {
            description LDP-VPLS;
            encapsulation vlan-vpls;
            vlan-id 1800;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 127.0.0.1/32;
                address 10.0.0.1/32;
            }
            family iso {
                address 49.0001.0100.0000.0001.00;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.1;
    autonomous-system 65000;
}
protocols {
    rsvp {
        interface ge-1/1/4.0;
        interface ge-1/1/2.0;
    }
    mpls {
        label-switched-path to_mx2 {
            to 10.0.0.2;
            ldp-tunneling;
            install 10.0.0.2/32 active;
        }
        label-switched-path to_mx3 {
            to 10.0.0.3;
            ldp-tunneling;
            install 10.0.0.3/32 active;
        }
```

```
        interface all;
        interface ge-1/1/4.0;
        interface ge-1/1/2.0;
    }
    bgp {
        group 65000 {
            type internal;
            local-address 10.0.0.1;
            family l2vpn {
                signaling;
            }
            peer-as 65000;
            neighbor 10.0.0.2;
            neighbor 10.0.0.3;
        }
    }
    isis {
        interface ge-1/1/2.0 {
            level 1 disable;
            level 2 {
                metric 1;
                hello-interval 5;
                hold-time 60;
            }
        }
        interface ge-1/1/4.0 {
            level 1 disable;
            level 2 {
                metric 1;
                hello-interval 5;
                hold-time 60;
            }
        }
        interface lo0.0 {
            passive;
        }
    }
    ldp {
        interface lo0.0;
    }
}
routing-instances {
    vpls-vlan1800 {
        description LDP-VPLS;
        instance-type vpls;
```

```
        vlan-id 1800;
        interface ge-1/1/6.2;
        route-distinguisher 10.0.0.1:1800;
        vrf-target target:1800:1;
        protocols {
            vpls {
                no-tunnel-services;
                vpls-id 1800;
                neighbor 10.0.0.2;
            }
        }
    }
    vpls-vlan2001 {
        description LDP-VPLS;
        instance-type vpls;
        vlan-id 1001;
        interface ge-1/1/5.2;
        route-distinguisher 10.0.0.1:2001;
        vrf-target target:1001:1;
        protocols {
            vpls {
                no-tunnel-services;
                vpls-id 2001;
                neighbor 10.0.0.2;
                neighbor 10.0.0.3;
            }
        }
    }
}
```

B BlackDiamond 20804-1 -kytkimen laitekonfiguraatio

Tässä liitteessä esitetään luvussa 3.2.9 kuvatussa testiympäristössä käytettyä konfiguraatio Blackdiamond 20804-1 -kytkimeltä. Muiden kytkinten konfiguraatioita ei esitetä, koska ne ovat käytännössä identtiset esitettyyn konfiguraatioon verrattuna. Konfiguraatiosta esitetään testin kannalta merkitsevät asiat. Konfiguraation alussa luodaan tarvittavat ISID-, BVLAN- ja asiakastunnisteet sekä liitetään näiden tunnisteiden käyttö tiettyihin rajapintoihin. Rajapinnoille määritetään myös normaalia suurempien (jumbo frames) kehysten siirto, jotta kapseloinnin takia kasvaneet kehykset voidaan siirtää verkossa oikein. Kytkimelle 20808 määritetään ainoastaan yksi BVLAN- ja ISID-tunniste, koska kyseinen kytkin palvelee ainoastaan yhtä palveluinstanssia. MAC-osoitteiden vanhentumisaika on 2560 sekuntia. Käytössä olleet kytkimet ja ohjelmistot hyväksyvät tämän arvon lisäksi ainoastaan arvon nolla, joka tarkoittaa, että MAC-osoitteet eivät vanhene ikinä. ExtremeXOS-käyttöjärjestelmä poistaa automaattisesti erinäisiä »snooping» ja »proxy-query» toiminnallisuuksia. Tämän lisäksi, mikään Spanning Tree -protokolla ei ollut käytössä.

```
#
# Module devmgr configuration.
#
configure slot 3 module GM-40XB
configure sys-recovery-level slot 3 reset

#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 3:1-40
configure vr VR-Default add ports 3:1-40
configure vlan default delete ports 3:5-8
create bvlan "pbb-testi"
configure bvlan pbb-testi tag 1900
create svlan "svlan-pbb-testi"
configure svlan svlan-pbb-testi tag 1999
create bvlan "toinen-pbb-testi"
configure bvlan toinen-pbb-testi tag 1800
create svlan "toinen-svlan-pbb-testi"
configure svlan toinen-svlan-pbb-testi tag 1888
enable jumbo-frame ports 3:5
enable jumbo-frame ports 3:6
enable jumbo-frame ports 3:7
enable jumbo-frame ports 3:8
configure vlan Default add ports 3:1-4, 3:9-40 untagged
configure bvlan pbb-testi add ports 3:6 tagged
```

```
configure svlan svlan-pbb-testi add ports 3:5 untagged
configure bvlan toinen-pbb-testi add ports 3:7 tagged
configure svlan toinen-svlan-pbb-testi add ports 3:8 untagged
configure vlan Mgmt ipaddress 10.129.99.101 255.255.255.0
create isid "isid-testi" 1990
create isid "toinen-isid-testi" 1880
configure isid "isid-testi" add svlan "svlan-pbb-testi"
configure isid "toinen-isid-testi" add svlan "toinen-svlan-pbb-testi"
configure bvlan "pbb-testi" add isid "isid-testi"
configure bvlan "toinen-pbb-testi" add isid "toinen-isid-testi"

#
# Module fdb configuration.
#
configure fdb agingtime 2560

#
# Module mcmgr configuration.
#
disable igmp snooping vlan "pbb-testi"
disable igmp snooping vlan "svlan-pbb-testi"
disable igmp snooping vlan "toinen-pbb-testi"
disable igmp snooping vlan "toinen-svlan-pbb-testi"
disable MLD snooping vlan "pbb-testi"
disable MLD snooping vlan "svlan-pbb-testi"
disable MLD snooping vlan "toinen-pbb-testi"
disable MLD snooping vlan "toinen-svlan-pbb-testi"
disable igmp proxy-query vlan "pbb-testi"
disable igmp proxy-query vlan "svlan-pbb-testi"
disable igmp proxy-query vlan "toinen-pbb-testi"
disable igmp proxy-query vlan "toinen-svlan-pbb-testi"

#
# Module stp configuration.
#
configure mstp region 000496420a80
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
```