

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikka / Tietoverkkotekniikka

Timi Posti & Anssi Taka

MPLS INTER-AUTONOMOUS SYSTEM

Opinnäytetyö 2014

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikka

POSTI, TIMI & TAKA, ANSSI

MPLS Inter-Autonomous System

Opinnäytetyö

39 sivua + 22 liitesivua

Työn ohjaaja

Yliopettaja Martti Kettunen

Toimeksiantaja

SIMUNET/KYMP OY

Toukokuu 2014

Avainsanat

MPLS, MPLS Inter-AS, MPLS VPN, Inter-AS Optio B

Suurten yritysten nopea laajentuminen maailmanlaajuisesti on johtanut MPLS- tekniikoiden kehitykseen. MPLS Inter-AS -tekniikkaa hyödynnetään, kun yritysten toimipisteet sijaitsevat eri palveluntarjoajien toiminta-alueilla. Palveluntarjoajien on nykyäänä pystyttävä toimimaan luotettavasti toisten palveluntarjoajien kanssa. Tämä on johtanut eri MPLS Inter-AS -optioiden kehittämiseen.

Opinnäytetyössä hyödynsimme SimuNet-verkkoa, joka on tietoverkkojen kehitys- ja testausympäristö Kymenlaakson ammattikorkeakoulussa. SimuNetin tärkeimpänä tarkoituksena on simuloida nykyaikaista operaattoriverkkoa pienemmässä mittakaavassa. Työn tarkoituksena oli suunnitella ja rakentaa SimuNetin kaltainen verkko Kymenlaakson ammattikorkeakoulun ICT-laboratorioon ja luoda verkkojen välille toimiva Inter-AS-yhteys.

Käytännön toteutuksessa luotiin MPLS Inter-AS -yhteys ICT-laboratorion ja SimuNetin välille käyttäen Inter-AS optio B:tä. Kuvitellun yrityksen tietoliikennettä ohjattiin näiden operaattoriverkkojen läpi. Tilannetta simuloitiin kytkemällä kaksi kuvitellun yrityksen toimipistettä eri palveluntarjoajien asiakkiksi. Tässä tapauksessa palveluntarjoajina toimivat SimuNet ja ICT-laboratorio.

Työn tuloksena saatiin rakennettua ja konfiguroitua toimiva SimuNetin kaltainen operaattoriverkko ICT-laboratorioon. MPLS Inter-AS -yhteys todettiin toimivaksi optio B:n osalta, mutta Inter-AS Hybrid -tekniikan suhteen ei päästy haluttuun lopputulokseen.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Information Technology

POSTI, TIMI & TAKA, ANSSI

Bachelor's Thesis

Supervisor

Commissioned by

May 2014

Keywords

MPLS Inter-Autonomous System

39 pages + 22 pages of appendices

Martti Kettunen, Principal Lecturer

SIMUNET/KYMP OY

MPLS, MPLS Inter-AS, MPLS VPN, Inter-AS Option B

The fast globalization of large companies has led to the development of MPLS-technologies. MPLS Inter-AS –technology is used when the company offices are located in different service provider's operating areas. Modern-day service providers have to be able to work reliably with other service providers, this has led to the development of different MPLS Inter-AS options.

In this study the SimuNet network was utilized, which is a development and testing environment for networks. It is located at Kymenlaakso University of Applied Sciences. The main purpose of the SimuNet is to simulate modern-day operator network in a smaller scale. The purpose of the study was to design and create a working Inter-AS connection between two different service providers.

In the empirical part MPLS Inter-AS connection was created between ICT-laboratory and SimuNet by using Inter-AS option B. The dataflow of a fictional company was forwarded through these operator networks. The situation was simulated by connecting two offices of the company to different service providers. In this case service providers were SimuNet and ICT-laboratory.

As the result, a working operator network was built and configured to ICT-laboratory similar to SimuNet. The MPLS Inter-AS connection was found to be functional for option B, but the Inter-AS Hybrid –technology did not reach the desired outcome.

SISÄLLYS

LYHENTEET	6
1 JOHDANTO	8
2 OSPF - OPEN SHORTEST PATH FIRST	9
2.1 Yleistä	9
2.2 Linkkitila-reititysprotokollat (Link-State Routing Protocols)	9
2.3 OSPF-alueet	10
3 BGP - BORDER GATEWAY PROTOCOL	11
3.1 BGP-toiminta	11
3.2 External and Interior BGP (eBGP & iBGP)	12
4 MPLS - MULTIPROTOCOL LABEL SWITCHING	12
4.1 Yleistä	12
4.2 MPLS:n toiminta	13
5 MPLS VPN	13
5.1 MPLS Layer 2 VPN (L2VPN)	14
5.2 MPLS Layer 3 VPN (L3VPN)	15
5.2.1 Yleistä	16
5.2.2 Komponentit	16
6 MPLS INTER-AS -OPTIOT	17
6.1 Inter-AS Back-to-Back VRFs (Optio A)	18
6.2 Inter-AS VPNv4 Exchange (Optio B)	18
6.3 Inter-AS VPNv4 Exchange Between Route Reflectors (Optio C)	19
7 SIMUNET	20
8 TEKNINEN TOTEUTUS	23
8.1 Yleistä	23
8.2 Testiympäristö	23
9 KÄYTÄNNÖN KONFIGUROINTIKÄSKYT	26

9.1	Asiakkaan reunalaitteet ICT-laboratoriossa	26
9.2	Operaattoriverkon laitteet ICT-laboratoriossa	27
9.3	SimuNetin laitteet	30
10	YHTEYDEN TESTAUS	32
11	YHTEENVETO	36
	LÄHTEET	38
	LIITTEET	
	Liite 1. SimuNet-verkon fyysinen topologia	
	Liite 2. ICT-laboratorio-verkon fyysinen topologia	
	Liite 3. SimuNetin PE3-laitteen konfiguraatio muutokset	
	Liite 4. SimuNetin PE4-laitteen konfiguraatio muutokset	
	Liite 5. SimuNetin PE7-laitteen konfiguraatio muutokset	
	Liite 6. SimuNetin PE8-laitteen konfiguraatio muutokset	
	Liite 7. ICT-laboratorion PE3-laitteen konfiguraatio	
	Liite 8. ICT-laboratorion PE4-laitteen konfiguraatio	
	Liite 9. ICT-laboratorion PE5-laitteen konfiguraatio	
	Liite 10. ICT-laboratorion PE6-laitteen konfiguraatio	
	Liite 11. ICT-laboratorion P1-laitteen konfiguraatio	
	Liite 12. ICT-laboratorion P2-laitteen konfiguraatio	
	Liite 13. ICT-laboratorion CE7-laitteen konfiguraatio	
	Liite 14. ICT-laboratorion CE8-laitteen konfiguraatio	

LYHENTEET

AS	Autonomous System eli <i>autonominen järjestelmä</i>
ASBR	Autonomous System Boundary Router eli <i>reititin, joka yhdistää autonomiset järjestelmät</i>
ATM	Asynchronous Transfer Mode eli <i>palveluntarjoajien runkoverkkotekniikka</i>
BGP	Border Gateway Protocol eli <i>autonomisten alueiden välinen reityspankollalla</i>
CE-laite	Customer Edge eli <i>asiakasverkon reunalaitte</i>
eBGP	External Border Gateway Protocol
FEC	Forwarding Equivalence Class eli <i>termi, jolla kuvataan samankaltaiset paketit MPLS-verkossa ja jotka voidaan ohjata eteenpäin</i>
iBGP	Internal Border Gateway Protocol
IOS	Internetwork Operating System eli <i>ohjelmisto, jota käytetään Cisco Systemin laitteissa</i>
IPv4	Internet Protocol version 4 eli <i>Internet-protokollan versio 4</i>
IPv6	Internet Protocol version 6 eli <i>Internet-protokollan versio 6</i>
LSA	Link-State Advertisement eli <i>linkkitilan mainostus</i>
LSDB	Link-State Database eli <i>linkkitilan tietokanta</i>
LSP	Link-State Packet eli <i>reitittimen generoima linkkitila paketti, joka sisältää informaatiota naapurireitittimistä</i>

MPLS	Multiprotocol Label Switching eli <i>leimamerkintöihin perustuva pakettien kytkentäteknikka</i>
MTU	Maximum Transmission Unit eli <i>suurin datayksikkö, jonka kerros voi välittää kerrallaan</i>
OSPF	Open Shortest Path First eli <i>autonomisen alueen sisäinen reititysprotokolla</i>
P-laite	Provider eli <i>operaattoriverkon runkolaite</i>
PE-laite	Provider Edge eli <i>operaattoriverkon reunalaite</i>
QoS	Quality of Service eli <i>palvelun laatu</i>
VLAN	Virtual Local Area Network eli <i>virtuaalinen lähiverkko</i>
VPN	Virtual Private Network eli <i>virtuaalinen erillisverkko</i>
VRF	Virtual Routing and Forwardin eli <i>virtuaalinen reititys ja jatkolähetys</i>

1 JOHDANTO

MPLS on vakiinnuttanut itsensä yhtenä keskeisimmistä teknologioista tietoverkko-maailmassa. Tietoverkkojen kehittyessä on selvää, että tulevaisuuden tietoverkkojen täytyy kuljettaa monia eri palvelutyyppejä, aina äänestä ja videosta luotettavaan suuri-en nopeuksien tiedonsiirtoon. Nämä verkot ovat erittäin tärkeitä yrityksille, joten niiden luotettavuuden täytyy olla huippuluokkaa, yhdistettynä pieneen verkkojentoipu-misaikaan vikojen sattuessa. Niiden täytyy myös tarjota erilaisia QoS-ratkaisuja. MPLS on teknologia, joka on valmis vastaamaan kaikkiin näihin haasteisiin. (Guichard, Le Faucheur & Vasseur 2005, xx.)

Kuluttajien vaatimus tehokkaammista tavoista kuljettaa ääntä, videota ja dataa, on tehnyt selväksi, kuinka tärkeä MPLS-tekniikka on nykypäivänä. Nämä vaatimukset asettavat useita haasteita teollisuudelle, joka ei enää yksinkertaisesti pysty rakenta-maan suurempia verkkoja vastaamaan tarpeitaan. Tarve saavuttaa kilpailullinen etu on vaatinut palveluntarjoajilta ideoita rakentaa uuden sukupolven järjestelmä, jossa yh-distyvät verkot, palvelut ja sovellukset. (Lobo & Lakshman 2006, xxv.)

Cisco tarjoaa kattavan strategian uuden sukupolven verkkojen rakentamiseen IOS MPLS:n avulla. Ciscon MPLS-tekniikka yhdistää älykkään ja skaalautuvan reitityk-sen, joka on lisäksi luotettava ja helposti hallittava. (Lobo & Lakshman 2006, xxv.)

Opinnäytetyön tarkoituksena on tutkia ja testata erilaisia MPLS Inter-AS -tekniikoita SimuNet- ja ICTLAB-ympäristöissä. Opinnäytetyössä keskitytään erityisesti malleihin B ja Inter-AS Hybrid AB. Työssä simuloidaan kahden eri operaattoriverkon välistä In-ter-AS-yhteyttä. Toteutuksessa käytetään ICT-laboratorioon mallinnettua operaattori-verkkoa ja SimuNetin jo käytössä olevaa operaattoriverkkoa.

Cisco Systemin laitteita käytettiin testiympäristön rakentamisessa. SimuNet-verkko on rakennettu myös näillä laitteilla. Tämän takia konfigurointikäskyt ja termit ovat Cisco-laitteille ominaisia.

2 OSPF - OPEN SHORTEST PATH FIRST

OSPF on yksi käytetyimmistä, jollei käytetyin sisäinen yhdyskäytäväprotokolla. Se perustuu pääosin RFC 2328 -dokumenttiin. OSPF on monimutkainen protokolla, joka koostuu monien muiden protokollien yhteistoiminnasta, tietokannan mainostamisesta ja pakettien tyypeistä. (Teare 2010, 185.)

2.1 Yleistä

OSPF:n toiminta perustuu siihen, että se ei jatkuvasti lähetä reititystauluja eteenpäin vaan ainoastaan silloin, kun ne muuttuvat. OSPF pystyy käsittelemään verkkomaskeja, jotka ovat eripituisia. OSPF:n avulla pystytään myös yhdistämään eri alueita yhdeksi loogiseksi alueeksi. Reitittimet ryhmitellään alueisiin, jonka jälkeen ne jakelevat ulospäin reititystiedon alueen sisälle ja pois alueesta. Reitittimet alueen sisällä jakavat tietonsa keskenään, eikä tämä häiritse reitittämiä, jotka eivät kuulu samaan alueeseen. Tämän takia OSPF-verkon ei välttämättä tarvitse olla tasainen, vaan sen avulla pystytään konfiguroimaan helposti hallittavissa olevia aliverkkoja. (OSPF 1998.)

2.2 Linkkitila-reititysprotokollat (Link-State Routing Protocols)

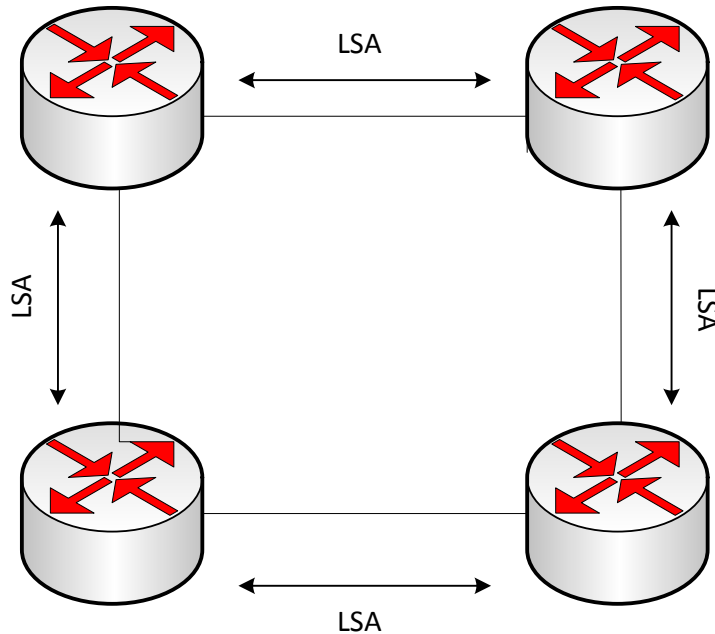
Linkkitilaprotokollan kehitys aloitettiin, kun huomattiin, että etäisyysvektori-protokollien suorituskyky ei riittänyt vastamaan nykypäivän vaatimuksia. (Teare 2010, 186.)

Linkkitila protokollilla on seuraavia ominaisuuksia:

- Ne reagoivat nopeasti verkon muutoksiin.
- Kun verkossa tapahtuu muutoksia, ne käynnistävät päivitysviestien lähetyksen.
- Ne lähettävät ajoitettuja päivityksiä pitkien aikajaksojen välillä, kuten joka 30. minuutti.

Linkkitilan reititysprotokollat luovat reitityspäivityksiä vain, jos verkossa tai verkon-topologiassa tapahtuu muutoksia. Kun linkki vaihtaa tilaansa, se laite joka huomaa muutoksen luo linkkitila mainoksen (LSA). LSA levittyy kaikkiin naapurilaitteisiin käyttäen erityistä multicast-osoitetta. Jokainen laite, joka saa LSA-viestin, lähettää sen

eteenpäin kaikille naapurilaitteille ja päivittää oman linkkitilietokannan. Alla (kuva 1) havainnollistetaan LSA:n toiminta. LSA-viestin lähettäminen varmistaa, että kaikki laitteet päivittävät linkkitilietokantansa ja tämän jälkeen päivittävät reititystaulut vastaamaan verkon uutta topologiaa. (Teare 2010, 186.)



Kuva 1. Linkkitilan mainostus

2.3 OSPF-alueet

Linkkitila-reititysprotokollassa kaikkien reitittimien täytyy pitää kopio OSPF:n topologi tietokannasta (LSDB). Mitä enemmän OSPF-reitittämiä on, sitä suurempi on LSDB. Pienissä verkoissa on hyödyllistä, että kaikki reitittimet tuntevat toisensa, mutta suurissa verkoissa ongelmana on se, että LSDB ei skaalaudu tarpeeksi. OSPF voidaan kuitenkin konfiguroida siten, että jokainen verkko saa oman alueensa (area), jotta skaalautuvuuden puute ei enää ole ongelma. OSPF-alueet vaativat hierarkkisen rakenteen tarkoittaen sitä, että kaikkien alueiden on oltava suoraan yhteydessä 0-alueeseen (area 0). (Teare 2010, 191.)

3 BGP - BORDER GATEWAY PROTOCOL

BGP on reititysprotokolla, sen tarkoitus on hoitaa reititys autonomisten alueiden välillä. BGP-protokolla käyttää reittien yhdistämistä pitääkseen reititystaulujen koon pienenä. BGP-protokolla tukee myös luokatonta reititystä.

BGP:n avulla autonomisten järjestelmien reunareitittimet voivat muodostavat yhteyden naapurijärjestelmiin. BGP on protokolla, joka pohjautuu polkuvektoreiden käyttöön. Järjestelmät etsivät BGP:n avulla lyhimmän reitin lähdeosoitteesta kohdeosoitteeseen eri autonomisten järjestelmien läpi. Reitittimet, joissa on käytössä BGP-protokolla, ylläpitävät muistissaan taulukkoa kaikista IP-verkoista ja autonomisten järjestelmien muodostamista reitistä.(Cisco, Border Gateway Protocol 2013.)

3.1 BGP-toiminta

BGP:n naapuruussuhteet, joita kutsutaan peereiksi (peers), muodostetaan siten, että reitittimien välille konfiguroidaan TCP-sessio portille 179. BGP lähettää 19-bitin keep-alive viestejä 30 sekunnin välein ylläpitääkseen yhteyden. Poiketen muista reititysprotokollista BGP käyttää TCP:tä sen kuljetusprotokollana. Kun BGP on käynnissä kahden peerin välillä, jotka kuuluvat samaan autonomiseen alueeseen, sitä kutsutaan sisäiseksi BGP:ksi (Interior Border Gateway Protocol). Kahden eri autonomisen alueen välillä olevaa reitintä kutsutaan ulkoiseksi BGP:ksi (Exterior Border Gateway Protocol) ja reitittimiä jotka ovat kahden eri autonomisen alueen välillä, kutsutaan raja- tai reunareitittimiksi. (Cisco, Border Gateway Protocol 2013.)

3.2 External and Interior BGP (eBGP & iBGP)

iBGP on reititysprotokolla, joka vaihtaa reititystietoja autonomisen alueen sisällä. Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System – to – Intermediate System (IS-IS) ja Enhanced Interior Gateway Routing Protocol (EIGRP) ovat esimerkkejä IGP:stä. (Teare 2010, 472.)

eBGP (tai EGP) on reititysprotokolla, joka vaihtaa reititystietoja kahden eri autonomisen alueen välillä. BGP on esimerkki EGP:stä. BGP on interdomain reititysprotokolla (IDRP), joka tunnetaan paremmin EGP:nä. (Teare 2010, 472.)

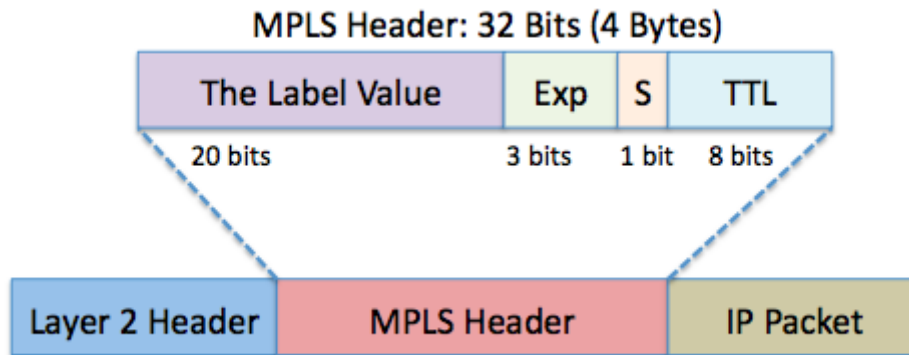
4 MPLS - MULTIPROTOCOL LABEL SWITCHING

MPLS on tekniikka, joka takaa korkean suorituskyvyn operaattoriverkoille. Tätä protokollaa käytetään tietoliikenteen kuljettamiseen operaattorien runkoverkoissa. MPLS pystyy kytkemään paketteja kohteisiinsa useista verkkoprotokollista. (Guichard, Le Faucheur & Vasseur 2005, xx.)

4.1 Yleistä

MPLS on tekniikka, joka tarjoaa Layer 2 -yhteyspainotteisen kuljetustavan Layer 3 -verkossa. Tämä näennäisesti suoraviivainen mekanismi on niin tehokas, että se on muuttanut tietoverkkoalaa perusteellisesti. (Guichard, Le Faucheur & Vasseur 2005, xx.)

MPLS toimii siten, että se lisää paketteihin MPLS-”otsikon”, joka sisältää yhden tai monta leimaa. Tätä tekniikkaa kutsutaan leimojen pinoamiseksi. Jokainen leimamerkintä sisältää neljä kenttää: 20-bittinen leiman arvo, 3-bittinen tietoliikenneluokka palvelunlaatua varten, 1-bittinen kasan loppulippu, joka kertoo, että kyseinen leima on viimeinen pinossa ja 8-bittinen elinikäkenttä (ks. Kuva 2). (RFC3031 2001.)



Kuva 2. MPLS-otsikon rakenne (INE Instructor, The MPLS Forwarding Plane 2010.)

4.2 MPLS:n toiminta

MPLS on yhteispainotteinen tekniikka, jonka toiminta perustuu siihen, että paketteihin, jotka tulevat MPLS-verkkoon, liitetään leimamerkinä. Leimalla tunnistetaan pakettien virta, joka tunnetaan myös nimellä FEC. Paketit, jotka kuuluvat samaan FEC-virtaan, saavat samantasoista kohtelua verkossa. FEC voidaan määrittellä monenlaisilla eri parametreilla, kuten lähteen tai kohteen IP-osoitteella tai porttinumerolla, IP protokollalla, IP arvojärjestyksellä tai Layer 2 piirin tunnisteella. Näin ollen FEC pystyy määrittelemään QoS:n tarpeet. Lisäksi FEC:iin pystytään määrittelemään oikeanlaiset jonotus- ja hylkäysmenettelyt. (Teare 2010, 126.)

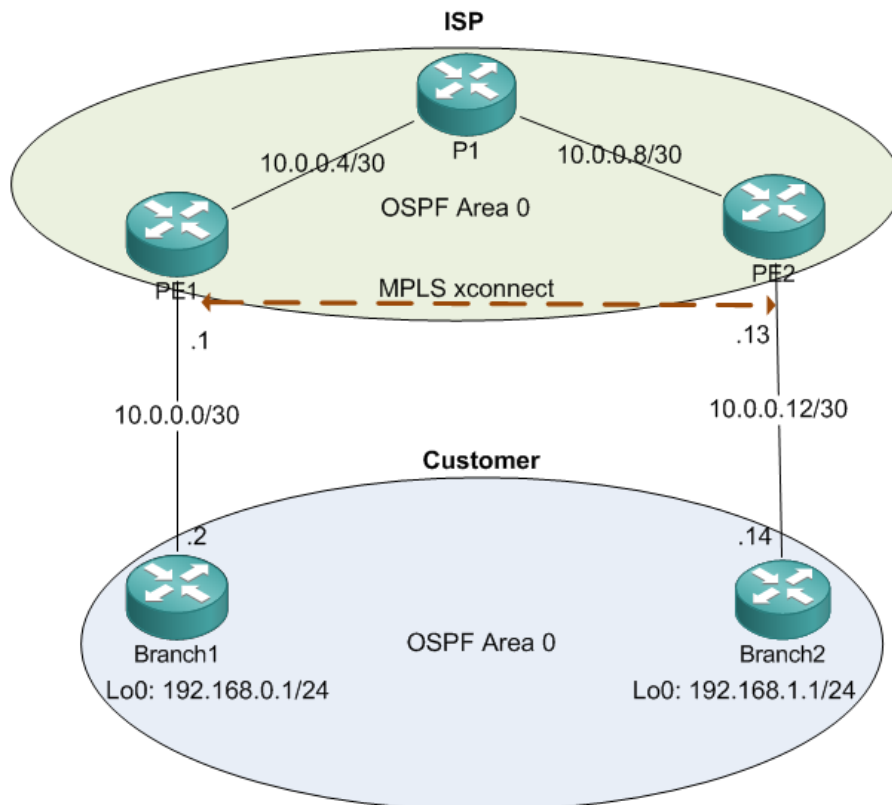
5 MPLS VPN

MPLS:ään pohjautuvat VPN-ratkaisut käyttävät yhdistelmää, johon kuuluu yhteydetömiä ja yhteydellisiä VPN-palveluita. Yhteydettömät VPN-palvelut toimivat asiakkaan ja palveluntarjoajan välillä. Yhteydelliset VPN-palvelut toimivat verkon rungossa vähentäen P-laitteiden raskautusta. Lisäksi monia muita tekniikoita käytetään, jotta asiakkaat voivat käyttää päällekkäisiä osoiteavaruuksia. (Pepelnjak, Guichard & Aparcar 2003, 14.)

5.1 MPLS Layer 2 VPN (L2VPN)

Layer 2 VPN emuloi paikallisen lähiverkon käyttäytymistä IP tai MPLS-IP verkon läpi, sallien Ethernet-laitteiden kommunikoida keskenään, kuten ne kommunikoisivat normaalissa lähiverkkoympäristössä. Kuvassa 3 on tyypillinen MPLS VPN L2 topologia.

Palveluntarjoajat etsivät ratkaisuja ATM infrastruktuurin korvaamiseen IP-infrastruktuurilla, koska niillä on tarve tarjota normaaleja IP-infrastruktuuri metodeja tarjotakseen käyttökelpoisen L2-rajapinnan asiakkailleen. Erityisen tärkeää on pystyä tarjoamaan normaaleja tapoja käyttää IP-infrastruktuuria tarjoamaan virtuaalisia piirejä asiakastoimipaikkaparien välillä. (Cisco Systems, Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router. 2012. 16.)



Kuva 3. MPLS VPN L2-verkon topologia (CCIP and CCIE R&S study blog. MPLS VPN. 2012)

L2VPN-järjestelmän rakentaminen vaatii koordinoitua palveluntarjoajan ja asiakkaan välillä. Palveluntarjoaja tarjoaa L2-tason yhteyden; asiakas rakentaa verkon käyttäen

datalinkki resursseja, jotka on saatu palveluntarjoajalta. L2VPN-palvelussa palveluntarjoaja ei vaadi informaatiota asiakkaan verkkotopologiasta, käytännöistä, reititysinformaatiosta, point-to-point linkeistä tai verkon point-to-point linkeistä toiselta palveluntarjoajalta. (Cisco Systems, Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router. 2012. 17.)

5.2 MPLS Layer 3 VPN (L3VPN)

MPLS Layer 3 VPN:t käyttävät vertaisverkkomallia, joka käyttää BGP-protokollaa välittämään VPN-informaatiota. Hyvin skaalautuva vertaisverkkomalli mahdollistaa yritysasiakkaiden ulkoistaa reititysinformaatio palveluntarjoajille. Tällä tavoin yritykset saavat merkittävät säästöt kuluissa ja vähentävät operatiivista monimutkaisuutta yrityksissä. Lisäksi palveluntarjoajat voivat tarjota lisäpalveluita, kuten Quality of Service (QoS) sekä Traffic Engineering, jotka mahdollistavat verkon konvertoitumisen sisältäen ääntä, videota ja dataa. (Cisco, Layer 3 VPNs 2013.)

Tyypillisessä MPLS VPN -verkkossa CE- ja PE-reitittimet vaihtavat reittejä keskenään käyttäen mitä tahansa sopivaa reititysprotokollaa. Nämä reitit lisätään VRF:ään, joka toimii PE-reitittimisissä. Näin taataan täydellinen eristys asiakkaiden välillä. (Pepelnjak, ym. 2003, 14.)

Kun asiakasreitit lisätään VRF:ään PE-reitittimet varaavat erillisen MPLS-leiman, jota tarvitaan VPN-tietojen jälleenlähetykseen jokaiseen asiakasreittiin. Asiakasreitit ja liitetty MPLS-leima kuljetetaan P-verkon läpi käyttäen multiprotocol BGP:tä. Asiakkaan IP-osoitteet vahvistetaan käyttämällä 64-bitin reitintunnistinta, ennen kuin ne lisätään palveluntarjoajan BGP-protokollaan, jotta taataan uniikki asiakasosoite. (Pepelnjak, ym. 2003, 14.)

Lisäksi käytetään BGP-protokollan lisäominaisuuksia kontrolloimaan reittien vaihtoa eri VRF-palveluiden kesken, jotta palveluntarjoajat voivat rakentaa VPN-topologiaa, jotka olisivat muuten lähes mahdottomia toteuttaa käyttäen muita VPN-tekniikoita. (Pepelnjak, ym. 2003, 14.)

5.2.1 Yleistä

Layer 3 MPLS VPN -palvelut ovat yhä keskeisemmässä roolissa nykypäivänä, koska tarve luoda yhteyksiä eri autonomisten alueiden välille on kasvanut. Suuret palveluntarjoajien asiakkaat ovat usein kansainvälisiä ja sijaitsevat maantieteellisesti erilaisissa paikoissa, joten VPN-yhteyksien luominen yhden palveluntarjoajan kautta ei aina ole mahdollista. Vaikka yhteys olisi mahdollista pelkästään yhden palveluntarjoajan avulla, voidaan verkon topologia joutua pilkkomaan eri autonomisiin alueisiin. Sen takia Layer 3 MPLS VPN -palveluiden on pystyttävä kulkemaan useamman kuin yhden autonomisen alueen läpi. (Guichard, ym. 2005, 19.)

5.2.2 Komponentit

Layer 3 MPLS VPN -arkkitehtuuriin kuuluu monia erilaisia verkkokomponentteja. Jokaisella niistä oma tehtävänsä, jotta koko verkkoarkkitehtuuri toimisi oikein. Nämä komponentit suorittavat erilaisia toimintoja koko kehysrakenteen sisällä, ja niiden yhdistelmiä käytetään Layer 3 VPN -palvelun perustamisessa. (Guichard, ym. 2005, 5.)

Palveluntarjoajan verkko (Provider network) on MPLS/IP-verkon ydin ja sitä hallinnoi palveluntarjoaja. Kaksi palveluntarjoajan verkkoa havainnollistaa, miten erilaiset autonomiset voidaan yhdistää.

- Palveluntarjoajan reititin (Provider router) on sijoitettu palveluntarjoajan verkkoon siten, että sillä ei ole kytköksiä verkonreunapalveluihin.
- Palveluntarjoajan reunareititin (Providen edge router) on laite, joka tarjoaa VPN-palveluita loppukäyttäjälle
- Autonomisen alueen raja reititin (ASBR-router) on palveluntarjoajan autonomisen alueen reunareititin, joka tarjoaa liittynnän läheiseen autonomiseen alueeseen, mikä kuuluu joko samalle tai eri operaattorille.
- Asiakasverkko (Customer network) on verkko, joka on liitetty palveluntarjoajan MPLS VPN Layer 3 -palveluihin.

Asiakkaan reunareititin (Customer edge router) mahdollistaa yhdyskäytävän luomisen asiakasverkon ja palveluntarjoajanverkon välille. Sitä voi hallinnoida, joko loppukäyttäjä tai palveluntarjoaja. (Guichard ym. 2005, xx.)

6 MPLS INTER-AS -OPTIOT

Autonominen järjestelmä on verkko tai ryhmä verkkoja, jota hallinnoi yleinen järjestelmän ylläpitoryhmä ja se käyttää yksittäistä selvästi määriteltyä reititysprotokollaa. VPN-verkkojen suurentuessa niiden vaatimukset kasvavat. Joissakin tapauksissa VPN:t kuuluvat eri autonomisiin järjestelmiin, jotka sijaitsevat maantieteellisesti eri alueilla. Lisäksi joidenkin VPN:ien täytyy laajentua useiden palveluntarjoajien yli. Monimutkaisuudesta ja VPN:ien sijainneista huolimatta autonomisten järjestelmien välinen yhteys asiakkaisiin täytyy olla saumatonta. (Cisco Systems, MPLS VPN User Guide, 5.2 2009, 273.)

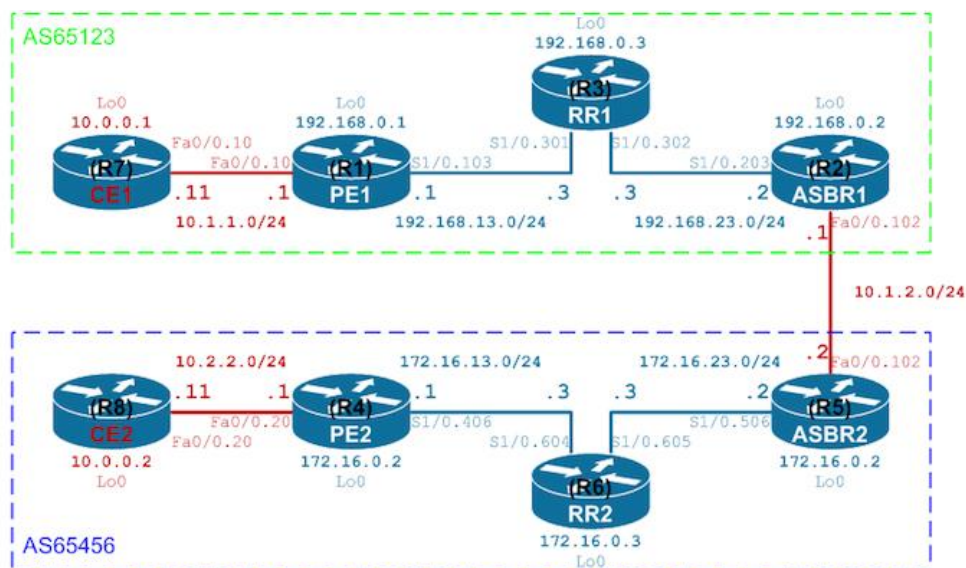
MPLS VPN:ien Inter-AS-ominaisuus tarjoaa saumattoman integraation autonomisten järjestelmien ja palveluntarjoajien välillä. Erilliset autonomiset järjestelmät eri palveluntarjoajien välillä voivat kommunikoida vaihtamalla IPv4-verkon kerrosinformaatiota VPN-IPv4-osoitteiden muodossa. Autonomisten järjestelmien reunareitittimet käyttävät eBGP:tä vaihtaessaan tätä informaatiota. Tämän jälkeen IGP jakelee verkon kerrosinformaation VPN-IPv4 prefiksille jokaisen VPN:n ja autonomisen järjestelmän läpi. (Cisco Systems, MPLS VPN User Guide, 5.2 2009, 273.)

MPLS VPN, joka tukee Inter-AS:ää, mahdollistaa palveluntarjoajan tarjota asiakkaille skaalautuvia Layer 3 VPN -palveluita, kuten verkon ylläpitoa, interaktiivista opetusta, sähköistä kaupankäyntiä ja puhelin palveluita. VPN palveluntarjoaja mahdollistaa turvallisen IP-pohjaisen verkon, joka jakaa resursseja yhdelle tai useammalle fyysiselle verkolle. (Cisco Systems, MPLS VPN User Guide, 5.2 2009, 273.)

Inter-AS-yhteys voidaan muodostaa monella eri tavalla, mutta yleisesti käytössä ovat optiot A, B ja C. Optiot A ja B ovat käytetyimmät kahden eri operaattoriverkon välillä. Kuitenkin B on nykypäivänä näistä kahdesta laajemmin käytössä. Optio C:tä käytetään yleisesti vain silloin, kun on kyse saman operaattoriverkon eri autonomisten alueiden välisistä yhteyksistä. (Guichard, ym. 2005, 19.)

6.1 Inter-AS Back-to-Back VRFs (Optio A)

Tätä mallia käytettäessä oletetaan, että PE-reitittimillä, jotka kuuluvat eri autonomisiin alueisiin, on suora yhteys toisiinsa. PE-reitittimet on yhdistetty usealla fyysisellä tai loogisella rajapinnalla, joista kukin on liitetty tiettyyn VPN-verkkoon. Täten jokainen PE-reititin kohtelee naapurin PE-reititintä CE-reitittimenä ja normaalia Layer 3 MPLS VPN -mekanismia käytetään reittien jakeluun jokaisessa autonomisessa järjestelmässä. Kuvassa 4 havainnollistetaan optio A. (Guichard, ym. 2005, 19.)



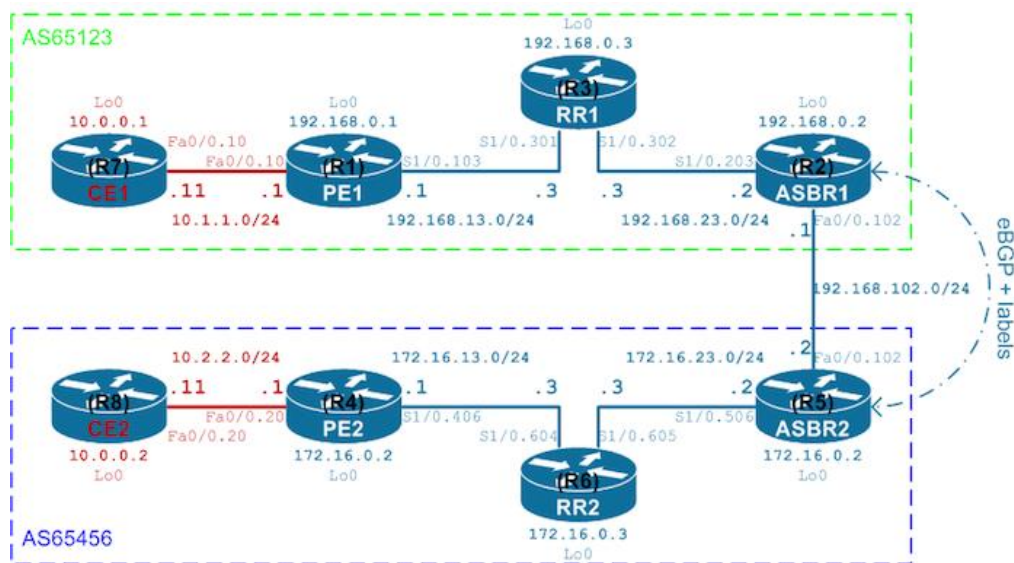
Kuva 4. MPLS Inter-AS Optio A (Marko Milivojevic 2010.)

Optio A:sta on tullut suosittu eri VPN-palveluntarjoajien välillä, koska jokainen autonominen järjestelmä on erotettu toisistaan. Tämä tarjoaa paremman kontrollin reittien vaihdossa ja paremman tietoturvallisuuden verkkojen välillä. Optio A tarjoaa monia hyödyllisiä toimintoja, mutta se on kolmesta optiosta huonoiten skaalautuva, minkä takia sen käyttö nykypäivänä on vähentynyt. (Guichard, ym. 2005, 20.)

6.2 Inter-AS VPNv4 Exchange (Optio B)

Tämä malli sallii ASBR-reitittimien käyttää ulkoista Multi Protocol BGP:tä mainostukseen VPNv4 reittejä autonomisten alueiden välillä. Vastaanottava ASBR-reititin lähettää VPNv4-tiedot paikalliseen autonomiseen järjestelmään. (Guichard, ym. 2005, 20.)

Ulkoinen MP-BGP tarjoaa mahdollisuuden mainostaa VPNv4-prefiksi/leima -tietoja palveluntarjoajan rajojen yli. Mainostava ASRB-reititin korvaa kahden kerroksen leimapiinin paikallisesti varatulla leimalla, ennen kuin se mainostaa VPNv4-reittiä. Tämä on välttämätöntä, koska kaikkien reittien next-hop attribuutti, jota mainostetaan palveluntarjoajien välillä, palautetaan ASBR-reitittimen peering osoitteeseen, jotta ASBR-reitittimestä tulee päätepiste jaettujen reittien LSP:lle. Säilyttääkseen leimavaihtoreitin sisään- ja ulosmeno reunareitittimien välillä, ASBR-reitittimen täytyy varata paikallinen leima, jota voidaan käyttää leimakasan tunnistamiseen paikallisessa VPN-verkossa. Kuvassa 5 havainnollistetaan optio B. (Guichard, ym. 2005, 20.)



Kuva 5. MPLS Inter-AS Optio B (Marko Milivojevic 2010.)

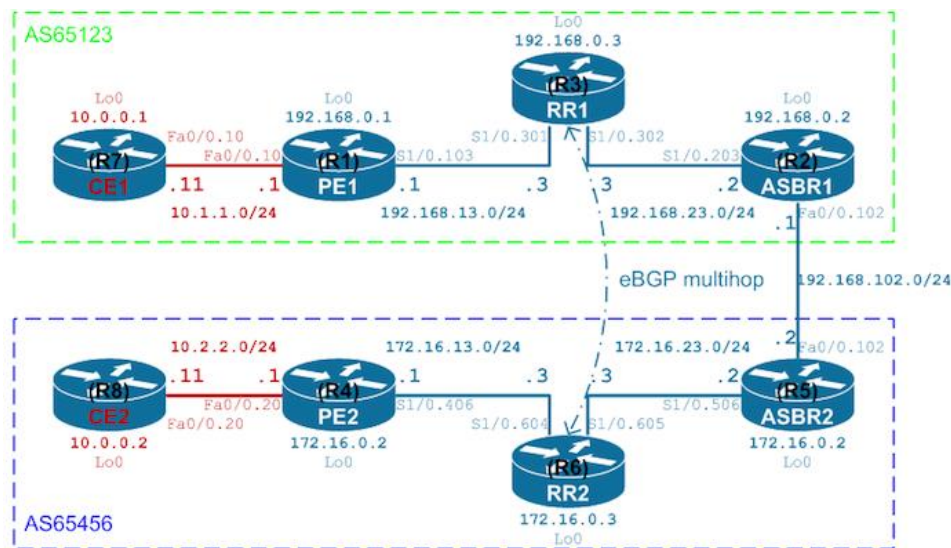
Optio B on suosittu, koska kuten optio A sillä voidaan luoda yhteys eri autonomisten alueiden välille ja myös se eristää molemmat autonomiset alueet, mutta optioon A verrattuna sillä on paremmat skaalautuvuusominaisuudet. Kuitenkin tällä optiolla on joitakin haavoittuvuuksia tietoturvassa ja ongelmia QoS:ssä. (Guichard, ym. 2005, 21.)

6.3 Inter-AS VPNv4 Exchange Between Route Reflectors (Optio C)

Optio C yhdistää VPNv4-reittien ulkoisen MP-BGP:n vaihdon route reflektorien välillä, jotka kuuluvat eri autonomisiin alueisiin ja näiden reittien next-hop attribuuttien vaihdot hoidetaan ASBR-reitittimien kautta. Eri autonomisten alueiden route reflektorit eivät ole suoraan kytketty toisiinsa, joten multihop toiminto täytyy olla käytössä, jotta ulkoinen MP-BGP sessio saadaan aikaiseksi. Next-hop attribuuttien vaihto on tarpeellinen, koska route reflektorit eivät palauta VPNv4-reittien next-hop attribuuttia,

kun niitä mainostetaan viereiseen autonomiseen alueeseen, sillä niiden ei haluta aiheuttavan huomiota toisen autonomisen alueen liikenteessä. (Guichard, ym. 2005, 21.)

PE-reitittimien VPNv4 next-hop-osoitteet vaihdetaan ASBR-reitittimien välillä. Osoitteiden vaihdos autonomisten alueiden välillä tapahtuu siten, että PE-reitittimet jakavat uudelleen 32 maskibitin osoitteita kahden autonomisten alueiden välillä tai käyttämällä BGP- ja leima-toimintoa, joka toimii siten, että BGP-4 protokollaan lisätään leimatieto, jota voidaan lähettää ASBR-reitittimien välillä. Kuvassa 6 havainnollistetaan optio C. (Guichard, ym. 2005, 21.)



Kuva 6. MPLS Inter-AS Optio C (Marko Milivojevic 2010.)

Optio C on normaalisti käytössä vain silloin, kun eri autonomiset alueet kuuluvat samalle operaattorille. Esimerkiksi, jos operaattorilla on toimipisteitä maailmanlaajuisesti. Toisaalta myös optio B soveltuu yhtä hyvin tähän tarkoitukseen ja sitä käytetäänkin verkoissa, joissa halutaan saavuttaa autonomisuus kahden eri maantieteellisen alueen välillä. (Guichard, ym. 2005, 22.)

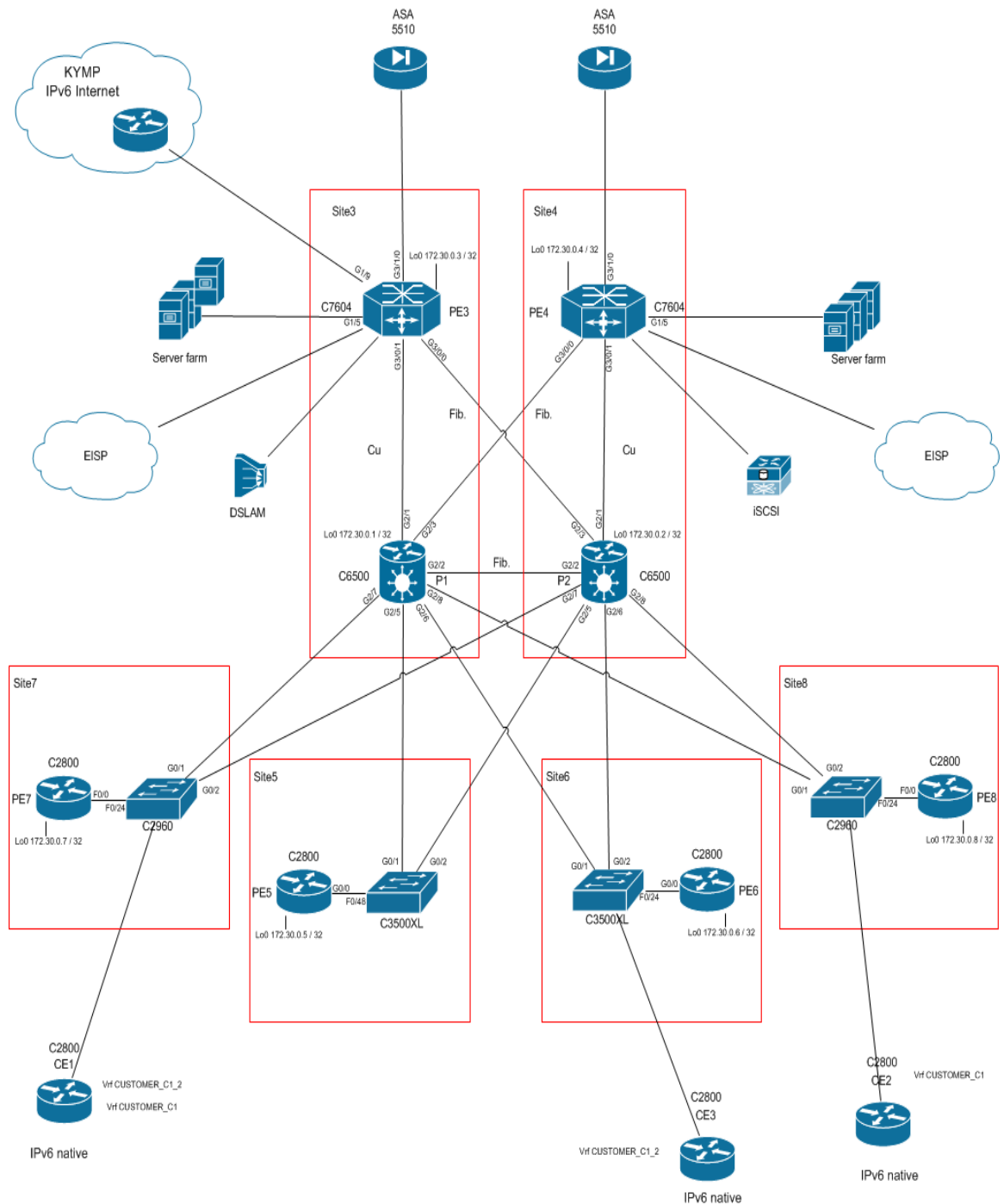
7 SIMUNET

SimuNet on Kymenlaakson ammattikorkeakoulussa sijaitseva operaattoriverkkoa simuloiva testaus-, tutkimus ja kehityslaboratorio. SimuNet hanke on rahoitettu Euroopan aluekehitysrahaston avustuksella ja se toimii yhteistyössä monien paikallisten yritysten kanssa, tärkeimpänä näistä KYMP Oy. SimuNet-verkkoa voidaan käyttää sellaisten haastavien tilanteiden mallintamiseen, joita on oikeilla verkko-operaattoreilla

uusien ratkaisujen toteuttamisessa. (KyAMK Information Technology, SimuNet-hanke 2014.)

SimuNet-verkkoa voidaan myös etähallita ja se hyödyntää virtualisointitekniikkaa tietoverkkopalvelujen testaus-, tutkimus- ja kehitysympäristössä. SimuNet-verkkoympäristössä opiskelijat voivat harjoitella esimerkiksi. verkon migraatiota vaihe vaiheelta etukäteen ennen muutoksen käyttöönottoa oikeassa tuotantoverkossa.

Esimerkkejä tällaisista migraatiosta ovat nykyisestä IP-versio neljästä (IPv4) siirtyminen uuteen versio kuuteen (IPv6) tai runkoverkon reititysyhteyskäytännön vaihtaminen kokonaan uuteen. Alla (kuva 7) SimuNet-verkon topologia. (KyAMK Information Technology, SimuNet-hanke 2014.)



Kuva 7. SimuNet-verkon topologia (Tuntematon 2014.)

Opinnäytetyön kannalta olennaisia laitteita ovat PE3, PE4, PE7 ja PE8. Reitittimet PE3 ja PE4 toimivat operaattoriverkon reunalaitteina ja reitittimet PE7 ja PE8 toimivat asiakasverkon reunalaitteina. Yhteys ICTLAB:n simuloituun operaattoriverkkoon muodostetaan PE3 ja PE4 -laitteiden avulla. Asiakasverkon reitittimisessä PE7 ja PE8 on toiminnassa VRF (yritys1).

8 TEKNINEN TOTEUTUS

MPLS VPN -arkkitehtuuri tarjoaa palveluntarjoajille mallin, joka yhdistää parhaimmat ominaisuudet kerros- ja vertaisverkko-malleista. Inter-Autonomous System MPLS VPN -ominaisuus sallii VPN:n ylittää useamman kuin yhden palveluntarjoajan runkoverkon. Se mahdollistaa VPN-sijaintien yhdistämisen useiden palveluntarjoajien yli käyttäen erillisiä AS-numeroita ja luo niin sanotun liiton palveluntarjoajien runkoverkkojen välille.

8.1 Yleistä

Normaalissa MPLS VPN -skenaariossa CE-reitittimet on kytketty PE-reitittimiin, jotka kuuluvat samaan AS-alueeseen. PE-reitittimet vaihtavat VPN-reittejä käyttäen multiprotocol iBGP:tä.

Inter-AS MPLS VPN -skenaariossa CE-reitittimet on kytketty PE-reitittimiin siten, että ne kuuluvat eri AS-alueisiin. PE-reitittimet vaihtavat VPN-reittejä AS-reunareitittimen kanssa, joka kuuluu samaan AS-alueeseen käyttäen iBGP:tä. AS-reunareitittimet, jotka kuuluvat eri AS-alueisiin vaihtavat VPN-reittejä käyttäen eBGP:tä.

Reitittimen täytyy jakaa VPN-leimat, jotta MPLS VPN toimii oikein. Tämä reititin on merkitty reitin next-hop ominaisuuden avulla. BGP:ssä prefixin next-hop -ominaisuus muuttuu, kun reititin mainostaa sitä naapurilleen käyttäen eBGP:tä. Inter-AS MPLS VPN -toiminnossa VPN-reitin next-hop -osoitteet vaihtuvat AS-reunareitittimen toimesta. Näin tapahtuu, kun VPNv4-osoitetta mainostetaan naapurin reunareitittimeen, joka kuuluu eri AS-alueeseen. Tässä työssä keskityttiin testamaan MPLS Inter-AS optio B:tä.

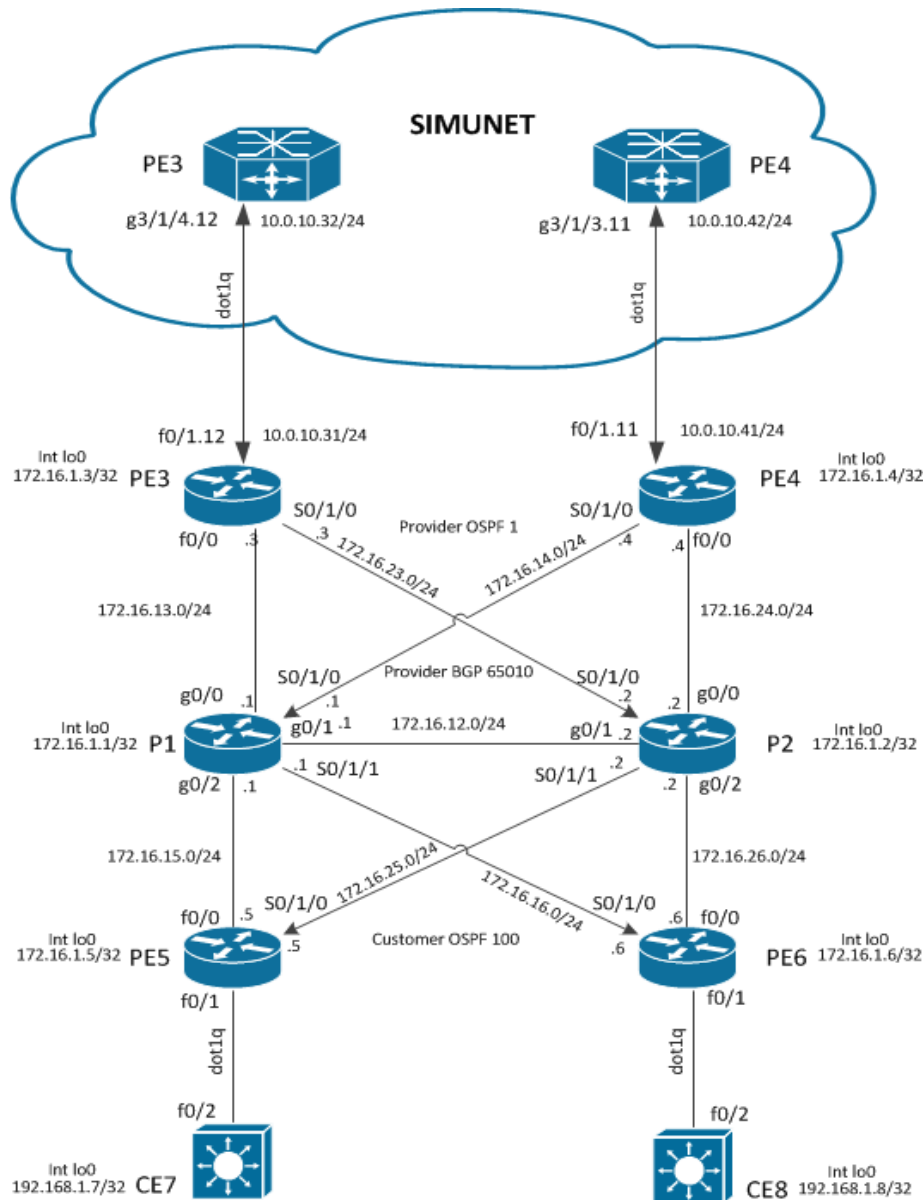
8.2 Testiympäristö

Tavoitteena oli rakentaa ICT-laboratorion laitteilla toimiva operaattoritason verkko ja tämän jälkeen testata kahden eri kuvitellun operaattorin välistä Inter-AS -yhteyttä, jota mahdollisesti tullaan hyödyntämään Kymenlaakson ja Metropolian ammattikorkeakoulujen välillä.

Työssä toisena operaattorina toimi ICT-laboratorioon mallinnettu operaattoritason verkko ja toisena SimuNetin valmis operaattoriverkko. Operaattorien asiakkaana toimii kuviteltu yritys (yritys1), jolla on kaksi toimipistettä ja niistä molemmat ovat eri operaattorien asiakkaita.

Aikaisempaa kokemusta operaattoritason verkkotekniikoista ei ollut, joten työ aloitettiin tekemällä erinäisiä operaattoriverkkoihin liittyviä harjoituksia. Harjoitusten pohjalta rakennettiin operaattoritason vastaava verkko ICT-laboratorioon.

Kytkenässä käytettiin neljää Cisco 2800 -sarjan reititintä (PE3, PE4, PE5 ja PE6), kahta Cisco 2900 -sarjan reititintä (P1 ja P2) ja kahta Cisco 3560 -sarjan kytkintä (CE7 ja CE8). Alla (kuva 8) ICT-laboratorion operaattoriverkon topologia. Konfiguraation valmistuttua aloitettiin operaattorien välisen yhteyden rakentaminen.



Kuva 8. ICT-laboratorion operaattoriverkon topologia

ICT-laboratorion operaattoriverkossa on käytössä kaksi eri OSPF-prosessia, asiakkaalle on varattu prosessinumero 100 ja operaattorille prosessinumero 1. Operaattori käyttää verkkoa 172.16.0.0/24 ja asiakkaalle on varattu verkko 192.168.0.0/24. ICT-laboratorion verkko käyttää AS-numeroa 65010 ja SimuNet-verkko AS-numeroa 65001.

Verkon BGP-protokolla on konfiguroitu vertaisryhmä nimeltä SISAVERKKO, jotta konfigurointi olisi yksinkertaisempaa. Asiakasverkon reunareitittimiin (PE5 ja PE6) on konfiguroitu VRF (yritys1), jonka avulla asiakasverkot jaetaan BGP-protokolla.

Reitittimet PE3, PE4, PE5 ja PE6 on konfiguroitu naapureiksi osoiteperheissä IPv4 ja VPNv4.

PE3 ja PE4 ovat autonomisen järjestelmän reunareitittimiä. Tämä tarkoittaa sitä, että ne ovat suoraan kytkettyjä toiseen autonomiseen järjestelmään, joka on tässä tapauksessa SimuNet. Autonomisten järjestelmien välillä käytetään trunk-linkkiä, joka toimii verkossa 10.0.10.0/24. Fyysisten porttien säästämiseksi käytetään aliliityntäportteja.

Reitittimet PE3 ja PE4 ICT-laboratoriossa ja reitittimet PE3 ja PE4 SimuNetissä ovat iBGP-naapureita. Ulkoisilla verkoilla ei ole pääsyä autonomisten alueiden reunareitittimien next-hop-attribuuttiin, joten käytetään komentoa ”*next-hop-self*”, joka mahdollistaa liikenteen lähettämisen BGP-reitittimeen, jolla on sen jälkeen tarvittavat tiedot liikenteen uudelleenohjaamiseen sisäverkosta. Autonomisten järjestelmien reunareitittimien välille on sallittava VPN-IPv4-liikenne, joten on käytettävä komentoa ”*no bgp default route-target filter*”.

MTU-arvo 1600 on laajalti käytössä Inter-AS-verkoissa, jotta varmistetaan myös suurien pakettien kulku koko verkon läpi. Reitittimet P1 ja P2 ovat operaattorin runkoreitittimiä eikä niissä ole merkittäviä konfiguraatioita, pois lukien IP-osoitteet, OSPF-protokolla ja loopback-osoitteet.

9 KÄYTÄNNÖN KONFIGUROINTIKÄSKYT

SimuNet-verkkoympäristö ja ICT-laboratorioon mallinnettu operaattoriverkko käyttävät Cisco Systemin laitteita, joten perehtyminen niiden konfigurointikäskyihin oli tarpeellista. Tässä kappaleessa käydään läpi tärkeimpiä laitekonfiguraatioita ja niiden toteuttamista käytännössä. ICT-laboratorion laitteet eivät ole samantasoisia kuin SimuNetissä, jonka takia täytyi ensin selvittää onko Inter-AS-yhteyden testaus mahdollista.

9.1 Asiakaan reunalaitteet ICT-laboratoriossa

Kytкимиin CE7 ja CE8 konfiguroitiin Loopback-osoitteet ja muutettiin FastEthernet-portit (F0/2) trunk-linjoiksi, joilla saatiin luotua yhteys operaattorin reunareitittimeen (PE5 ja PE6). Luotiin Vlan10 ja Vlan11, jotka simuloivat yrityksen lähiverkkoja ja

käynnistettiin OSPF-reititys prosessinumerolla 100. Nämä toteutettiin seuraavilla komennoilla (CE7):

```
CE7(conf)#interface Loopback0
CE7(conf-if)#ip address 192.168.1.7 255.255.255.255

CE7(conf)#interface FastEthernet0/2
CE7(conf-if)#switchport trunk encapsulation dot1q
CE7(conf-if)#switchport mode trunk

CE7(conf)#interface Vlan10
CE7(conf-if)#ip address 192.168.10.7 255.255.255.0

CE7(conf)#router ospf 100
CE7(conf-router)#network 192.168.0.0 0.0.255.255 area 0
```

9.2 Operaattoriverkon laitteet ICT-laboratoriossa

Asiakasverkon reunalaitteina toimivat reitittimet PE5 ja PE6. Nämä reitittimet ovat yhteydessä asiakasverkon kytkimiin CE7 ja CE8 aliliityntäporteilla (F0/1.10 ja F0/1.11). Aliliityntäporttia on konfiguroitu seuraavasti reitittimessä PE5:

```
PE5(conf)#interface FastEthernet0/1.10
PE5(conf-subif)#encapsulation dot1Q 10
PE5(conf-subif)#ip address 192.168.10.5 255.255.255.0
```

Asiakkaan eristäminen operaattorin sisäverkosta saavutetaan käyttämällä virtuaalisia reititystauluja tai instansseja PE-reitittimissä, jotka tunnetaan paremmin nimellä VRF. VRF:n toiminta muistuttaa globaalia reititystaulua, mutta se sisältää vain reitit, jotka kuuluvat tiettyyn VPN:ään. (Lobo & Lakshman 2006, 85.)

VRF konfiguroitiin seuraavilla komennoilla (PE5):

```
PE5(conf)#ip vrf yritys1
PE5(conf-vrf)#rd 100:1
PE5(conf-vrf)#route-target export 100:1
```

```
PE5(conf-vrf)#route-target import 100:1
```

```
PE5(conf)#interface FastEthernet0/1.10
```

```
PE5(conf-subif)#ip vrf forwarding yritys1
```

Operaattoriverkon reunareitittimiin PE5 ja PE6 on konfiguroitu kaksi eri OSPF-prosessia: 100 ja 1. Prosessi 100 on varattu asiakasverkoille ja prosessi 1 on varattu operaattorin sisäverkolle. Prosessi 100 välittää BGP:n avulla VRF-tiedot operaattorin sisäverkon yli ASBR-reitittimille. Prosessi 1 on toiminnassa ainoastaan operaattorin sisäverkossa. OSPF on konfiguroitu seuraavilla komennoilla (PE5):

```
PE5(conf)#router ospf 100 vrf yritys1
```

```
PE5(conf-router)#redistribute bgp 65010 metric 10 subnets
```

```
PE5(conf-router)#network 192.168.0.0 0.0.255.255 area 0
```

```
PE5(conf)#router ospf 1
```

```
PE5(conf-router)#network 172.16.0.0 0.0.255.255 area 0
```

Näihin reitittimiin konfiguroitiin myös BGP-protokolla AS-numerolla 65010, jotta reititys voidaan hoitaa kahden eri autonomisen järjestelmän (ICTLAB - SimuNet) välillä. ICTLAB-verkossa käytettiin vertaisryhmää nimeltä "SISAVERKKO" konfiguraation yksinkertaistamiseksi. iBGP, IPv4 ja VPNv4 -naapureiksi määriteltiin kaikki operaattoriverkon PE-laitteet. Kuvitellun yrityksen (yritys1) reititystaulu erotellaan globaalista reititystaulusta virtuaaliseen reititystauluun. Nämä konfiguraatiot on toteutettu seuraavilla komennoilla (PE5):

```
PE5(conf)#router bgp 65010
```

```
PE5(conf-router)#no bgp default ipv4-unicast
```

```
PE5(conf-router)#neighbor SISAVERKKO peer-group
```

```
PE5(conf-router)#neighbor SISAVERKKO remote-as 65010
```

```
PE5(conf-router)#neighbor SISAVERKKO update-source Loopback0
```

```
PE5(conf-router)#neighbor 172.16.1.3 peer-group SISAVERKKO
```

```
PE5(conf-router)#neighbor 172.16.1.4 peer-group SISAVERKKO
```

```
PE5(conf-router)#neighbor 172.16.1.6 peer-group SISAVERKKO
```

Seuraavilla komennoilla saadaan BGP välittämään IPv4-reitit naapureiden välillä:

```

PE5(conf-router)#address-family ipv4
PE5(conf-router-af)#neighbor 172.16.1.3 activate
PE5(conf-router-af)#neighbor 172.16.1.4 activate
PE5(conf-router-af)#neighbor 172.16.1.6 activate
PE5(conf-router-af)#exit-address-family

```

Seuraavilla komennoilla saadaan BGP välittämään VPNv4-reitit naapureiden välillä:

```

PE5(conf-router)#address-family vpnv4
PE5(conf-router-af)#neighbor SISAVERKKO send-community both
PE5(conf-router-af)#neighbor 172.16.1.3 active
PE5(conf-router-af)#neighbor 172.16.1.4 active
PE5(conf-router-af)#neighbor 172.16.1.6 active
PE5(conf-router-af)#exit-address-family

```

Yritysverkon OSPF-reittien jakelu BGP:lle:

```

PE5(conf-router)#address-family ipv4 vrf yritys1
PE5(conf-router-af)#redistribute ospf 100 vrf yritys1

```

Reitittimet P1 ja P2 toimivat operaattoriverkon runkoreitittiminä ja niihin on konfiguroitu ainoastaan operaattorin OSPF-prosessi (ospf 1) ja fyysiset rajapinnat. Tämän koluokan operaattoriverkossa näillä reitittimillä ei ole suurta merkitystä, mutta suuremmissa verkoissa niillä voidaan varmistaa, että verkko skaalautuu tarvittaessa suuremmaksi.

PE3 ja PE4 ovat operaattoriverkon autonomisen järjestelmän reunareitittimiä (ASBR), joiden tarkoitus on toimia linkkeinä eri autonomisten alueiden välillä. Ne vaihtavat autonomisen alueensa topologiatiedot toisen autonomisen järjestelmän reunareitittimien kanssa, jotka ovat tässä tapauksessa SimuNetin PE3 ja PE4. Reitittimiin on konfiguroitu aliliityntäportit (f0/1.12 ja f0/1.11), jotka ovat suoraan kytketty toisen operaattorin (SimuNet) aliliityntäportteihin (g3/1/4.12 ja g3/1/3.11) ja ne on määritelty trunklinkeiksi. Näissä reitittimissä ei tarvita yritysverkkojen OSPF-prosessia. Aliliityntäportit on konfiguroitu seuraavasti (PE3 ICTLAB):

```

PE3(conf)#interface FastEthernet0/1.12
PE3(conf-if)#mtu 1600

```

```
PE3(conf-if)#encapsulation dot1Q 12
PE3(conf-if)#ip address 10.0.10.31 255.255.255.0
```

MPLS-pakettien vastaanotto BGP-protokollan kautta:

```
PE3(conf-if)#mpls bgp forwarding
```

Konfiguraatio näissä laitteissa ei BGP:n osalta poikkea, lukuun ottamatta seuraavia komentoja (PE3 ICTLAB):

```
PE3(conf)#router bgp 65010
PE3(conf-router)#no bgp default route-targetfilter
PE3(conf-router)#neighbor 10.0.10.32 remote-as 65001
PE3(conf-router)#address-family vpnv4
PE3(conf-router-af)#neighbor 10.0.10.32 active
PE3(conf-router-af)#neighbor 10.0.10.32 send-community extended
```

9.3 SimuNetin laitteet

SimuNetin laitteisiin tehtiin tarvittavat konfiguraatiomuutokset, jotta MPLS Inter-AS -yhteys voitiin toteuttaa. Reitittimet PE3 ja PE4 toimivat autonomisen järjestelmän reunareitittiminä. SimuNetin reunalla toimivat reitittimet PE7 ja PE8 konfiguroitiin asiakasverkon (yritys1) reunareitittimiksi. PE3 ja PE4 -reitittimiin luotiin aliliityntäportit (g3/1/4.12 ja g3/1/3.11), jotka muutettiin trunk-linkeiksi ja kytkettiin suoraan toiseen operaattoriin (ICTLAB). Seuraavassa PE3-reitittimen aliliityntäportin konfiguraatio:

```
PE3(conf)#interface GigabitEthernet3/1/4.12
PE3(conf-if)#encapsulation dot1Q 12
PE3(conf-if)#ip address 10.0.10.32 255.255.255.0
PE3(conf-if)#mpls bgp forwarding
```

SimuNet on valmis operaattoritason testiympäristö, johon on valmiiksi konfiguroitu BGP-protokolla AS-numerolla 65001. SimuNetin BGP-protokollaan tehtiin seuraavat muutokset (PE3):

```
PE3(conf)#router bgp 65001
```

```

PE3(conf-router)#no bgp default route-target filter
PE3(conf-router)#neighbor 10.0.10.31 remote-as 65010
PE3(conf-router)#address-family vpnv4
PE3(conf-router-af)#neighbor RRSISAVERKKO send-community both
PE3(conf-router-af)#neighbor RRSISAVERKKO next-hop-self
PE3(conf-router-af)#neighbor 10.0.10.31 active
PE3(conf-router-af)#neighbor 10.0.10.31 send-community extended
PE3(conf-router-af)#172.30.0.4 activate
PE3(conf-router-af)#172.30.0.7 activate
PE3(conf-router-af)#172.30.0.8 activate

```

Laitteet PE7 ja PE8 ovat konfiguroidut, kuten laitteet PE5 ja PE6 ICT-laboratoriossa, pois lukien IP-osoitteita ja aliliityntäportteja. Alla esimerkkinä konfiguraatio muutok-
sista laitteessa PE7.

VRF konfiguroitiin seuraavilla komennoilla:

```

PE7(conf)#ip vrf yritys1
PE7(conf-vrf)#rd 100:1
PE7(conf-vrf)#route-target export 100:1
PE7(conf-vrf)#route-target import 100:1

PE7(conf)#interface FastEthernet0/0.12
PE7(conf-if)#mtu 1600
PE7(conf-if)#encapsulation dot1Q 12
PE7(conf-if)#ip vrf forwarding yritys1
PE7(conf-if)#ip address 192.168.20.11 255.255.255.0

```

OSPF-Prosessi 100 välittää BGP:n avulla VRF-tiedot operaattorin (SimuNet) sisäver-
kon yli ASBR-reitittimille (PE3 ja PE4). OSPF on konfiguroitu seuraavilla kome-
noilla:

```

PE7(conf)#router ospf 100 vrf yritys1
PE7(conf-router)#router-id 10.0.0.7
PE7(conf-router)#redistribute bgp 65001 metric 10 subnets

```

```
PE7(conf-router)#network 192.168.0.0 0.0.255.255 area 0
```

Seuraavilla komennoilla saadaan BGP välittämään VPNv4-reitit naapureiden välillä:

```
PE7(conf)#router bgp 65001
PE7(conf-router)#address-family vpnv4
PE7(conf-router-af)#neighbor RRSISAVERKKO send-community both
PE7(conf-router-af)#172.30.0.3 activate
PE7(conf-router-af)#172.30.0.4 activate
PE7(conf-router-af)#172.30.0.8 activate
```

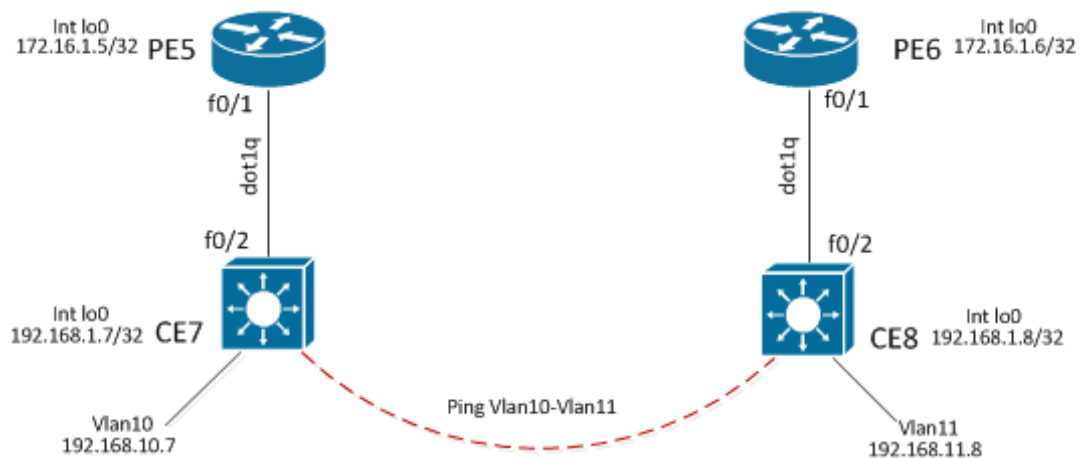
VRF:n erottelu globaalista reititustaulusta:

```
PE7(conf-router)#address-family ipv4 vrf yritys1
PE7(conf-router-af)#redistribute ospf 100 vrf yritys1
```

10 YHTEYDEN TESTAUS

Testauksessa selvitettiin saadaanko kuvitellun yrityksen (yritys1) toimipisteiden välille luotua yhteys, jotka ovat kahden eri operaattorin (SimNet ja ICTLAB) asiakkaita. Ensinnä testattiin saman operaattorin (ICTLAB) alla olevan toimipisteen yhteys pingtestin avulla ks. kuva 9. Tämä tapahtui suorittamalla **ping**-komento laitteessa CE7:

```
PE7#ping 192.168.11.8
```



Kuva 9. CE7 ja CE8 välinen ping-testi

Ping-testin jälkeen tarkistettiin asiakasverkon reunalaitteiden (CE7 ja CE8) reititystaulut, suorittamalla komento: *show ip route*. Kuvassa 10 esimerkkinä CE7:n reititystaulu.

```

CE7#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.30.0/24 [110/111] via 192.168.10.5, 01:25:17, Vlan10
C    192.168.10.0/24 is directly connected, Vlan10
O E2 192.168.11.0/24 [110/101] via 192.168.10.5, 01:25:17, Vlan10
O IA 192.168.20.0/24 [110/111] via 192.168.10.5, 01:25:17, Vlan10
     192.168.1.0/32 is subnetted, 2 subnets
O IA   192.168.1.8 [110/111] via 192.168.10.5, 01:25:17, Vlan10
C     192.168.1.7 is directly connected, Loopback0
CE7#_

```

Kuva 10. Laitteen CE7 reititystaulu

Reititystaulusta (kuva 10) voidaan todeta, että asiakasverkon reunareitittimet eivät ole oppineet reittejä operaattoriverkon (172.16.0.0/24) kautta. Tämä on tärkeää, koska operaattoriverkon reitit eivät saa vuotaa asiakkaalle.

Operaattoriverkon ASBR-reitittimien reititystaulut tarkistettiin, koska ne eivät saa sisältää asiakasverkon (192.168.0.0/24) kautta opittuja reittejä. Testi suoritettiin samalla komennolla, kuin asiakasverkon laitteissa: *show ip route*. Kuvasta 11. voidaan todeta, että asiakasverkon reitit eivät ole vuotaneet ASBR-reitittimiin.

```

PE3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 15 subnets, 2 masks
O   172.16.33.0/24 [110/67] via 172.16.13.1, 01:14:09, FastEthernet0/0
O   172.16.24.0/24 [110/3] via 172.16.13.1, 01:15:06, FastEthernet0/0
O   172.16.26.0/24 [110/3] via 172.16.13.1, 01:14:19, FastEthernet0/0
C   172.16.23.0/24 is directly connected, Serial0/1/0
O   172.16.16.0/24 [110/65] via 172.16.13.1, 01:15:16, FastEthernet0/0
O   172.16.12.0/24 [110/2] via 172.16.13.1, 01:15:16, FastEthernet0/0
C   172.16.13.0/24 is directly connected, FastEthernet0/0
O   172.16.14.0/24 [110/65] via 172.16.13.1, 01:15:37, FastEthernet0/0
O   172.16.15.0/24 [110/2] via 172.16.13.1, 01:14:48, FastEthernet0/0
O   172.16.1.5/32 [110/3] via 172.16.13.1, 01:14:38, FastEthernet0/0
O   172.16.1.4/32 [110/4] via 172.16.13.1, 01:15:07, FastEthernet0/0
O   172.16.1.6/32 [110/4] via 172.16.13.1, 01:14:10, FastEthernet0/0
O   172.16.1.1/32 [110/2] via 172.16.13.1, 01:15:38, FastEthernet0/0
C   172.16.1.3/32 is directly connected, Loopback0
O   172.16.1.2/32 [110/3] via 172.16.13.1, 01:15:08, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   10.0.10.0/24 is directly connected, FastEthernet0/1.12
C   10.0.10.32/32 is directly connected, FastEthernet0/1.12
PE3#_

```

Kuva 11. Laitteen PE3 reititystaulu

Kun reititystaulut oli tarkastettu, aloitettiin MPLS Inter-AS -yhteyden testaus eri operaattorien ASBR-reitittimien välillä. Yhteys todettiin toimivaksi tarkastelemalla reititimestä PE3 (ICTLAB) MPLS-lähetystaulun tietoja. Tiedot saatiin suorittamalla komento: *show mpls forwarding-table next-hop 10.0.10.32* laitteessa PE3 (ICTLAB). Kuvasta 12. selviää minne ICT-laboratorion asiakasverkosta lähetetyt paketit ohjataan SimuNet-verkossa.

```

PE3#show mpls forwarding-table next-hop 10.0.10.32
Local  Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label  Label or UC  or Tunnel Id    Switched     interface
16     Pop Label    10.0.10.32/32   0            Fa0/1.12   10.0.10.32
24     78           100:1:192.168.30.0/24 \
                                     0            Fa0/1.12   10.0.10.32
25     72           100:1:192.168.20.0/24 \
                                     11292       Fa0/1.12   10.0.10.32
PE3#_

```

Kuva 12. Laitteen PE3 MPLS-lähetystaulu

Suorittamalla komento: *show ip bgp vpnv4* laitteessa PE3 (ICTLAB) saatiin esille VPNv4-tiedot BGP-tietokannasta. Kuvasta 13. selviää, että BGP on oppinut kaikki tarvittavat VPNv4-reitit ja näin ollen osaa ohjata paketit oikeisiin osoitteisiin.

```

PE3#show ip bgp vpnv4 all
BGP table version is 7, local router ID is 172.16.1.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1
*>i192.168.1.7/32    172.16.1.5         2      100     0 ?
*>i192.168.1.8/32    172.16.1.6         2      100     0 ?
*>i192.168.10.0     172.16.1.5         0      100     0 ?
*>i192.168.11.0     172.16.1.6         0      100     0 ?
* i192.168.20.0     172.16.1.4         0      100     0 65001 ?
*>                  10.0.10.32         0      100     0 65001 ?
* i192.168.30.0     172.16.1.4         0      100     0 65001 ?
*>                  10.0.10.32         0      100     0 65001 ?
PE3#_

```

Kuva 13. Laitteen PE3 VPNv4-tiedot BGP-tietokannassa

Paketit, jotka lähetetään yrityksen toimipisteestä toiseen (ICTLAB – SIMUNET), kulkevat MPLS-paketteina operaattoriverkkojen läpi. Tämä saatiin selville suorittamalla VRF-reitinjäljitys ICT-laboratorion asiakasverkon reitittimestä PE5 SimuNetin asiakasverkon reitittimeen PE7. Reitinjäljitys tehtiin komennolla: *traceroute vrf yritys1 192.168.20.11*. Kuvassa 14. näkyy pakettien kulku MPLS-pilven läpi operaattoriverkoissa.

```

PE5#traceroute vrf yritys1 192.168.20.11
Type escape sequence to abort.
Tracing the route to 192.168.20.11

 1 172.16.15.1 [MPLS: Labels 18/25 Exp 0] 0 msec 0 msec 0 msec
 2 172.16.13.3 [MPLS: Label 25 Exp 0] 0 msec 0 msec 4 msec
 3 10.0.10.32 [MPLS: Label 72 Exp 0] 0 msec 4 msec 0 msec
 4 192.168.13.1 [MPLS: Labels 24/55 Exp 0] 4 msec 0 msec 4 msec
 5 192.168.20.11 0 msec 0 msec *
PE5#

```

Kuva 14. VRF-reitinjäljitys PE5 - PE7

Lopuksi kytkettiin kuvitellun yrityksen (yritys1) päätekonne asiakkaan reunakytkimeen CE7. Päätekonne liitettiin kytkimessä olevaan virtuaaliseen lähiverkkoon (vlan10) ja koneelle annettiin IP-osoite verkosta 192.168.10.0/24. Seuraavaksi koneelta suoritettiin reitinjäljitys kuvitellun yrityksen toiseen toimipisteeseen, joka on SimuNet-operaattorin asiakas. Yrityksen toista toimipistettä kuvastaa laitteeseen PE7 konfiguroitu aliliityntäportti, jonka osoite on 192.168.20.11. Reitinjäljitys suoritettiin komen-

tokehotteessa komennolla: *tracert 192.168.20.11*. Kuvasta 15. voidaan todeta yhteyden toimivuus, sillä yhteys on saavutettu yrityksen toiseen toimipisteeseen.

```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert 192.168.20.11

Tracing route to 192.168.20.11 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    192.168.10.5
  2  <1 ms    1 ms     1 ms     172.16.15.1
  3  1 ms     2 ms     1 ms     172.16.13.3
  4  1 ms     1 ms     1 ms     10.0.10.32
  5  1 ms     1 ms     1 ms     192.168.13.1
  6  *        15 ms    *        192.168.13.1
  7  2 ms     2 ms     1 ms     192.168.20.11

Trace complete.

```

Kuva 15. Reitinjäljitys yrityksen päätekoneelta

11 YHTEENVETO

Opinnäytetyön tavoitteena oli ymmärtää MPLS Inter-AS -tekniikoita teoriatasolla ja toteuttaa toimiva MPLS Inter-AS -yhteys kahden eri operaattorin välillä. Työ aloitettiin tutustumalla MPLS-tekniikkaan teoriatasolla ja tekemällä MPLS-konfiguraatioharjoituksia ICT-laboratoriossa. Harjoitusten jälkeen alettiin suunnitella operaattoriverkon tasoista kytkentää ICT-laboratorioon. Suunnitelman pohjalta rakennettiin SimuNetin kaltainen verkko ICT-laboration laitteilla. Tavoitteena oli myös testata MPLS Inter-AS Hybrid -tekniikkaa, mutta se osoittautui käytössä olevilla laitteilla mahdottomaksi.

Työssä toteutettiin toimiva MPLS Inter-AS -yhteys käyttämällä optio B:tä. Varaa jatkokehitykselle kuitenkin jättää perehtyminen IPv6-, QoS- ja tietoturvaratkaisuihin. Molemmat operaattoriverkot ovat ns. kahdennettuja, joten niiden vikasietoisuus on hyvä. Tässä työssä ei kuitenkaan keskitytty tutkimaan verkkojen vikasietoisuutta, joka kuitenkin on tärkeää oikeissa operaattoriverkoissa. MPLS Inter-AS -yhteyttä käyttävät operaattorit, joilla on maanlaajuisesti suuria yritysasiakkaita, siksi näin pienessä testiympäristössä on vaikea todeta sen hyötyjä ja tehokkuutta.

Operaattoritason verkon rakentaminen onnistui harjoitusten ja teoriaopiskelun avulla hyvin. Työn alkuvaiheessa ongelmaksi muodostui BGP-protokollan VPNv4-osoiteperheen toiminnan ymmärtäminen ja yhteyden muodostaminen toiseen operaat-

toriin. Kytkennän testaamisen kannalta ongelmaksi muodostui se, että ICT-laboratorion laitteet ovat päivittäisessä käytössä eri opiskelijaryhmillä, joten kytkentä jouduttiin rakentamaan ja purkamaan useita kertoja uudelleen. Testauksen loppuvaiheessa ulkopuolinen opiskelija muutti SimuNetin konfiguraatiota siten, että verkkoon otettiin käyttöön Route Reflectorit ja tämän jälkeen MPLS Inter-AS -yhteys ei toiminut enää halutulla tavalla. Ongelma ratkaistiin muuttamalla konfiguraatiota SimuNet-verkon osalta.

Opinnäytetyön tuloksena syntyi toimiva MPLS Inter-AS -yhteys kahden eri operaattorin välille, jota voidaan tulevaisuudessa hyödyntää esimerkiksi SimuNetin ja toisen operaattorin välisessä yhteydessä. Työssä saavutettiin myös asiakasverkkojen eristäminen operaattoriverkoista halutulla tavalla.

MPLS Inter-AS -tekniikoiden tutkiminen ja testaaminen jättävät mahdollisuuksia uusien projekteihin tai jopa opinnäytetyöhön. Mikäli SimuNetin ja ICT-laboratorion laitteita uudistetaan tai päivitetään, on hyvät mahdollisuudet toteuttaa toimiva MPLS Inter-AS Hybrid -tasoinen yhteys tämän opinnäytetyön pohjalta.

LÄHTEET

CCIP and CCIE R&S study blog. 2012. MPLS VPN. Saatavissa:

<http://ccieblog.co.uk/mpls/mpls-vpn> [viitattu 26.03.2014]

Cisco. 2013. Border Gateway Protocol. Saatavissa:

http://docwiki.cisco.com/wiki/Border_Gateway_Protocol [viitattu 19.11.2013]

Cisco. 2013. Layer 3 VPNs (L3VPN). Saatavissa:

http://www.cisco.com/en/US/products/ps6604/products_ios_protocol_group_home.html [viitattu 19.11.2013]

Cisco Sytems. 2012. Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router. Saatavissa:

http://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-2/lxvpn/configuration/guide/vc42book.pdf [viitattu 26.03.2014]

Cisco Sytems. 2009. MPLS VPN User Guide, 5.2. Saatavissa:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ip_solution_center/5-2/mpls_vpn/user/guide/mpls52book.pdf [viitattu 26.03.2014]

Guichard, J., Le Faucheur, F. & Vasseur, J-P. 2005. Definitive MPLS Network Designs. Indianapolis: Cisco Press.

INE Instructor. 2010. The MPLS Forwarding Plane. Saatavissa:

<http://blog.ine.com/2010/02/21/the-mpls-forwarding-plane/> [viitattu 25.03.2014]

KyAMK Information Technology. 2014. SimuNet-hanke. Saatavissa:

<http://www.ictlab.kyamk.fi/index.php/simunet-hanke> [viitattu: 13.3.2014]

Lobo, L. & Lakshman, U. 2006. MPLS Configuration on Cisco IOS Software. Indianapolis: Cisco Press.

Milivojevic, M. 2010. Introduction to Interprovider MPLS L3 VPNs. Saatavissa: <http://blog.ipexpert.com/2010/06/30/introduction-to-interprovider-mpls-l3-vpns/> [viitattu 04.03.2014]

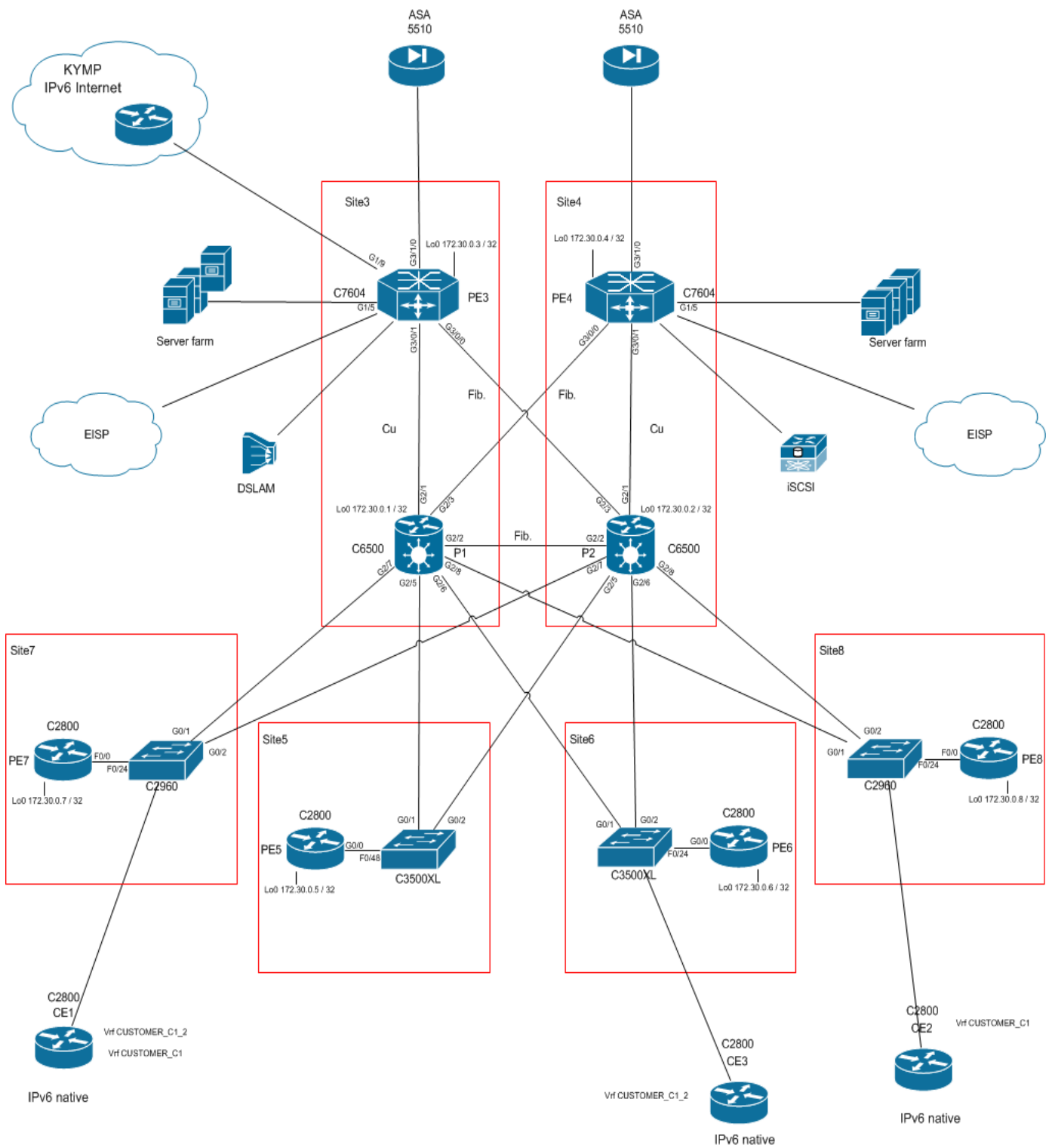
Moy, J. 1998. OSPF Version 2: RFC2328. Saatavissa: <http://www.ietf.org/rfc/rfc2328.txt> [viitattu: 19.11.2013]

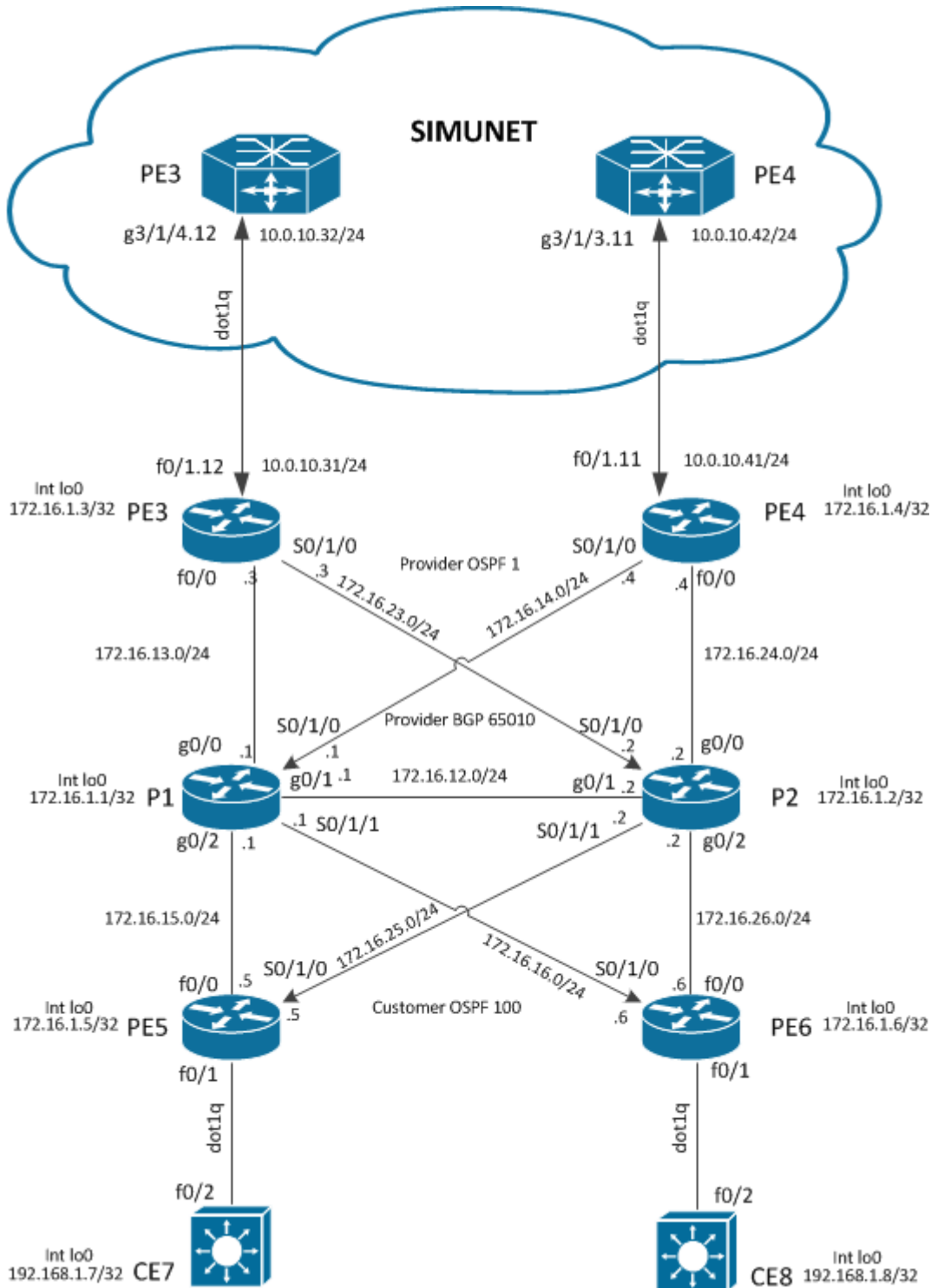
Pepelnjak, I. Guichard, J. & Apcar, J. 2003. MPLS and VPN Architectures Volume II. Indianapolis: Cisco Press.

Rosen, E. Viswanathan, A. Callon, R. 2001. Multiprotocol Label Switching Architecture: RFC3031. Saatavissa: <http://www.ietf.org/rfc/rfc3031.txt> [viitattu 19.11.2013]

Teare, D. 2010. Implementing Cisco IP Routing (ROUTE). Indianapolis: Cisco Press.

Tuntematon. 2012. SimuNetin fyysinen kytkentä. Kaavio. Saatavissa: Kymenlaakson ammattikorkeakoulun ICT-laboratorion sisäverkko.





SimuNetin PE3-laitteen konfiguraatio muutokset

Liite 3

```

interface GigabitEthernet3/1/4
description Posti_MPLS (SimuNet - ICTLAB)
mtu 1600
no ip address
speed 100
no negotiation auto
!
interface GigabitEthernet3/1/4.12
encapsulation dot1Q 12
ip address 10.0.10.32 255.255.255.0
mpls bgp forwarding
!
router bgp 65001
bgp log-neighbor-changes
no bgp default ipv4-unicast
no bgp default route-target filter
neighbor RRSISAVERRKKO peer-group
neighbor RRSISAVERRKKO remote-as 65001
neighbor RRSISAVERRKKO update-source Loop-
back0
neighbor RRSISAVERRKKO version 4
neighbor 10.0.10.31 remote-as 65010
neighbor 2A00:1DD0:400:102::1 remote-as
65000
neighbor 172.30.0.4 peer-group RRSISAVERRKKO
neighbor 172.30.0.5 peer-group RRSISAVERRKKO
neighbor 172.30.0.6 peer-group RRSISAVERRKKO
neighbor 172.30.0.7 peer-group RRSISAVERRKKO
neighbor 172.30.0.8 peer-group RRSISAVERRKKO
!
address-family ipv4
network 172.30.0.0 mask 255.254.0.0
neighbor RRSISAVERRKKO route-reflector-client
neighbor 172.30.0.4 activate
neighbor 172.30.0.5 activate
neighbor 172.30.0.6 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.8 activate
exit-address-family
!
address-family vpnv4
neighbor RRSISAVERRKKO send-community both

```

```

neighbor RRSISAVERRKKO route-reflector-client
neighbor RRSISAVERRKKO next-hop-self
neighbor 10.0.10.31 activate
neighbor 10.0.10.31 send-community extended
neighbor 172.30.0.4 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.8 activate
exit-address-family

```

```
interface GigabitEthernet3/1/3
description Taka_MPLS (Simunet - ICTLAB)
mtu 1600
no ip address
speed 100
no negotiation auto
!
interface GigabitEthernet3/1/3.11
encapsulation dot1Q 11
ip address 10.0.10.42 255.255.255.0
mpls bgp forwarding
!
router bgp 65001
bgp log-neighbor-changes
no bgp default ipv4-unicast
no bgp default route-target filter
neighbor RRSISAVERRKKO peer-group
neighbor RRSISAVERRKKO remote-as 65001
neighbor RRSISAVERRKKO update-source Loopback0
neighbor RRSISAVERRKKO version 4
neighbor 10.0.10.41 remote-as 65010
neighbor 172.30.0.3 peer-group RRSISAVERRKKO
neighbor 172.30.0.5 peer-group RRSISAVERRKKO
neighbor 172.30.0.6 peer-group RRSISAVERRKKO
neighbor 172.30.0.7 peer-group RRSISAVERRKKO
neighbor 172.30.0.8 peer-group RRSISAVERRKKO
!
address-family ipv4
network 172.30.0.0 mask 255.254.0.0
neighbor RRSISAVERRKKO route-reflector-client
neighbor 172.30.0.3 activate
neighbor 172.30.0.5 activate
neighbor 172.30.0.6 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.8 activate
exit-address-family
!
address-family vpv4
neighbor RRSISAVERRKKO send-community both
neighbor RRSISAVERRKKO route-reflector-client
neighbor RRSISAVERRKKO next-hop-self
neighbor 10.0.10.41 activate
neighbor 10.0.10.41 send-community extended
neighbor 172.30.0.3 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.8 activate
exit-address-family
```

```

ip vrf yritys1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface FastEthernet0/0.12
mtu 1600
encapsulation dot1Q 12
ip vrf forwarding yritys1
ip address 192.168.20.11 255.255.255.0
!
router ospf 100 vrf yritys1
router-id 10.0.0.7
log-adjacency-changes
redistribute bgp 65001 metric 10 subnets
network 192.168.0.0 0.0.255.255 area 0
!
router bgp 65001
bgp log-neighbor-changes
neighbor RRSISAVERRKKO peer-group
neighbor RRSISAVERRKKO remote-as 65001
neighbor RRSISAVERRKKO update-source Loopback0
neighbor RRSISAVERRKKO version 4
neighbor 2A00:1DD0:100:F110::2 remote-as 65006
neighbor 172.30.0.3 peer-group RRSISAVERRKKO
neighbor 172.30.0.4 peer-group RRSISAVERRKKO
neighbor 172.30.0.8 remote-as 65001
neighbor 172.30.0.8 update-source Loopback0
!
address-family ipv4
no neighbor 2A00:1DD0:100:F110::2 activate
neighbor 172.30.0.3 activate
neighbor 172.30.0.4 activate
neighbor 172.30.0.8 activate
no auto-summary
no synchronization
network 172.30.0.0 mask 255.254.0.0
exit-address-family
!
address-family vpv6
neighbor RRSISAVERRKKO send-community extended
neighbor 172.30.0.3 activate
neighbor 172.30.0.4 activate
neighbor 172.30.0.8 activate
neighbor 172.30.0.8 send-community both
exit-address-family

```

```

!
address-family vpv4
neighbor RRSISAVERRKKO send-community both
neighbor 172.30.0.3 activate
neighbor 172.30.0.4 activate
neighbor 172.30.0.8 activate
exit-address-family
!
address-family ipv4 vrf yritys1
redistribute ospf 100 vrf yritys1
no synchronization
exit-address-family

```

```

ip vrf yritys1
rd 100:1
route-target export 100:1
route-target import 100:1
!
!
router ospf 100 vrf yritys1
router-id 10.0.0.8
log-adjacency-changes
redistribute bgp 65001 metric 10 subnets
network 192.168.0.0 0.0.255.255 area 0
!
router bgp 65001
bgp log-neighbor-changes
neighbor RRSISAVERRKKO peer-group
neighbor RRSISAVERRKKO remote-as 65001
neighbor RRSISAVERRKKO update-source Loop-
back0
neighbor RRSISAVERRKKO version 4
neighbor 2A00:1DD0:100:F210::2 remote-as
65006
neighbor 172.30.0.3 peer-group RRSISAVERRKKO
neighbor 172.30.0.4 peer-group RRSISAVERRKKO
neighbor 172.30.0.7 remote-as 65001
neighbor 172.30.0.7 update-source Loopback0
!
address-family ipv4
no neighbor 2A00:1DD0:100:F210::2 activate
neighbor 172.30.0.3 activate
neighbor 172.30.0.4 activate
neighbor 172.30.0.7 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpv6
neighbor RRSISAVERRKKO send-community ex-
tended
neighbor 172.30.0.4 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.7 send-community both
exit-address-family
!
address-family vpv4
neighbor RRSISAVERRKKO send-community both
neighbor 172.30.0.3 activate
neighbor 172.30.0.4 activate
neighbor 172.30.0.7 activate
neighbor 172.30.0.7 send-community extended

```

```

interface FastEthernet0/0.11
mtu 1600
encapsulation dot1Q 11
ip vrf forwarding yritys1
ip address 192.168.30.22 255.255.255.0
exit-address-family
!
address-family ipv4 vrf yritys1
redistribute ospf 100 vrf yritys1
no synchronization
exit-address-family

```

Current configuration : 2307 bytes

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
memory-size iomem 10
!
dot11 syslog
ip source-route
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
archive
log config
hidekeys
!
interface Loopback0
ip address 172.16.1.3 255.255.255.255
!
interface FastEthernet0/0
mtu 1600
ip address 172.16.13.3 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
mtu 1600
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.12

```

```

mtu 1600
encapsulation dot1Q 12
ip address 10.0.10.31 255.255.255.0
mpls bgp forwarding
!
interface Serial0/1/0
mtu 1600
ip address 172.16.23.3 255.255.255.0
mpls ip
no fair-queue
clock rate 72000
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
interface ATM0/3/0
no ip address
shutdown
no atm ilmi-keepalive
!
router ospf 1
log-adjacency-changes
network 172.16.0.0 0.0.255.255 area 0
!
router bgp 65010
no bgp default ipv4-unicast
no bgp default route-target filter
bgp log-neighbor-changes
neighbor SISAVERKKO peer-group
neighbor SISAVERKKO remote-as 65010
neighbor SISAVERKKO update-source Loopback0
neighbor 10.0.10.32 remote-as 65001
neighbor 172.16.1.4 peer-group SISAVERKKO
neighbor 172.16.1.5 peer-group SISAVERKKO
neighbor 172.16.1.6 peer-group SISAVERKKO
!
address-family ipv4
neighbor 172.16.1.4 activate
neighbor 172.16.1.5 activate
neighbor 172.16.1.6 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor SISAVERKKO send-community both
neighbor SISAVERKKO next-hop-self

```

ICT-laboratorion PE3-laitteen konfiguraatio

Liite 7 (2/2)

```
neighbor 10.0.10.32 activate
neighbor 10.0.10.32 send-community extended
neighbor 172.16.1.4 activate
neighbor 172.16.1.5 activate
neighbor 172.16.1.6 activate
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
end
```

Current configuration : 2194 bytes

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
dot11 syslog
ip source-route
!
ip cef
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
archive
log config
hidekeys
!
interface Loopback0
ip address 172.16.1.4 255.255.255.255
!
interface FastEthernet0/0
mtu 1600
ip address 172.16.24.4 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
mtu 1600
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.11
mtu 1600
encapsulation dot1Q 11

```

```

ip address 10.0.10.41 255.255.255.0
mpls bgp forwarding
!
interface Serial0/1/0
mtu 1600
ip address 172.16.14.4 255.255.255.0
mpls ip
no fair-queue
clock rate 72000
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
router ospf 1
log-adjacency-changes
network 172.16.0.0 0.0.255.255 area 0
!
router bgp 65010
no bgp default ipv4-unicast
no bgp default route-target filter
bgp log-neighbor-changes
neighbor SISAVERKKO peer-group
neighbor SISAVERKKO remote-as 65010
neighbor SISAVERKKO update-source Loopback0
neighbor 10.0.10.42 remote-as 65001
neighbor 172.16.1.3 peer-group SISAVERKKO
neighbor 172.16.1.5 peer-group SISAVERKKO
neighbor 172.16.1.6 peer-group SISAVERKKO
!
address-family ipv4
neighbor 172.16.1.3 activate
neighbor 172.16.1.5 activate
neighbor 172.16.1.6 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor SISAVERKKO send-community both
neighbor SISAVERKKO next-hop-self
neighbor 10.0.10.42 activate
neighbor 10.0.10.42 send-community extended
neighbor 172.16.1.3 activate
neighbor 172.16.1.5 activate
neighbor 172.16.1.6 activate
exit-address-family
!

```


ICT-laboratorion PE4-laitteen konfiguraatio

Liite 8 (2/2)

```
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
en
```

Current configuration : 2517 bytes

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
dot11 syslog
ip source-route
!
ip vrf yritys1
rd 100:1
route-target export 100:1
route-target import 100:1
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
vtp mode transparent
archive
log config
hidekeys
!
interface Loopback0
ip address 172.16.1.5 255.255.255.255
!
interface FastEthernet0/0
mtu 1600
ip address 172.16.15.5 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto

```

```

mpls ip
!
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip vrf forwarding yritys1
ip address 192.168.10.5 255.255.255.0
!
interface Serial0/1/0
mtu 1600
ip address 172.16.25.5 255.255.255.0
mpls ip
no fair-queue
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
interface Serial0/2/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/2/1
no ip address
shutdown
clock rate 2000000
!
interface ATM0/3/0
no ip address
shutdown
no atm ilmi-keepalive
!
router ospf 100 vrf yritys1
log-adjacency-changes
redistribute bgp 65010 metric 10 subnets
network 192.168.0.0 0.0.255.255 area 0
!
router ospf 1
log-adjacency-changes
network 172.16.0.0 0.0.255.255 area 0
!
router bgp 65010
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor SISAVERRKKO peer-group
neighbor SISAVERRKKO remote-as 65010
neighbor SISAVERRKKO update-source Loopback0
neighbor 172.16.1.3 peer-group SISAVERRKKO

```

```
neighbor 172.16.1.4 peer-group SISAVERKKO
neighbor 172.16.1.6 peer-group SISAVERKKO
!
address-family ipv4
neighbor 172.16.1.3 activate
neighbor 172.16.1.4 activate
neighbor 172.16.1.6 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor SISAVERKKO send-community both
neighbor 172.16.1.3 activate
neighbor 172.16.1.4 activate
neighbor 172.16.1.6 activate
exit-address-family
!
address-family ipv4 vrf yritys1
redistribute ospf 100 vrf yritys1
no synchronization
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
end
```

Current configuration : 2261 bytes

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE6
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
dot11 syslog
ip source-route
!
ip vrf yritys1
rd 100:1
route-target export 100:1
route-target import 100:1
!
ip cef
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
archive
log config
hidekeys
!
interface Loopback0
ip address 172.16.1.6 255.255.255.255
!
interface FastEthernet0/0
mtu 1600
ip address 172.16.26.6 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto

```

```

!
interface FastEthernet0/1.11
encapsulation dot1Q 11
ip vrf forwarding yritys1
ip address 192.168.11.6 255.255.255.0
!
interface Serial0/1/0
mtu 1600
ip address 172.16.33.6 255.255.255.0
mpls ip
no fair-queue
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
router ospf 100 vrf yritys1
log-adjacency-changes
redistribute bgp 65010 metric 10 subnets
network 192.168.0.0 0.0.255.255 area 0
!
router ospf 1
log-adjacency-changes
network 172.16.0.0 0.0.255.255 area 0
!
router bgp 65010
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor SISAVERKKO peer-group
neighbor SISAVERKKO remote-as 65010
neighbor SISAVERKKO update-source Loopback0
neighbor 172.16.1.3 peer-group SISAVERKKO
neighbor 172.16.1.4 peer-group SISAVERKKO
neighbor 172.16.1.5 peer-group SISAVERKKO
!
address-family ipv4
neighbor 172.16.1.3 activate
neighbor 172.16.1.4 activate
neighbor 172.16.1.5 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor SISAVERKKO send-community both
neighbor 172.16.1.3 activate
neighbor 172.16.1.4 activate
neighbor 172.16.1.5 activate

```

ICT-laboratorion PE6-laitteen konfiguraatio

Liite 10 (2/2)

```
exit-address-family
!
address-family ipv4 vrf yritys1
 redistribute ospf 100 vrf yritys1
 no synchronization
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

ICT-laboratorion P1-laitteen konfiguraatio

Liite 11 (1/2)

```

Current configuration : 1960 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
memory-size iomem 10
!
no ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2911/K9 sn FCZ160570LZ
license accept end user agreement
license boot module c2900 technology-package
securityk9
license boot module c2900 technology-package
datak9
!
!
vtp mode transparent
!
redundancy
!
interface Loopback0
ip address 172.16.1.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
mtu 1600
ip address 172.16.13.1 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface GigabitEthernet0/1
mtu 1600
ip address 172.16.12.1 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface GigabitEthernet0/2
mtu 1600
ip address 172.16.15.1 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface Serial0/1/0
mtu 1600
ip address 172.16.14.1 255.255.255.0
mpls ip
!
interface Serial0/1/1
mtu 1600
ip address 172.16.16.1 255.255.255.0
mpls ip
clock rate 72000
!
router ospf 1
network 172.16.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop
udptn v120 ssh

```

ICT-laboratorion P1-laitteen konfiguraatio

Liite 11 (2/2)

```
stopbits 1
line vty 0 4
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

ICT-laboratorion P2-laitteen konfiguraatio

Liite 12 (1/2)

```

Current configuration : 1941 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
memory-size iomem 10
!
no ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2911/K9 sn FCZ160570M1
license accept end user agreement
license boot module c2900 technology-package
securityk9
license boot module c2900 technology-package
uck9 disable
license boot module c2900 technology-package
datak9
!
redundancy
!
interface Loopback0
ip address 172.16.1.2 255.255.255.255
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
mtu 1600
ip address 172.16.24.2 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface GigabitEthernet0/1
mtu 1600
ip address 172.16.12.2 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface GigabitEthernet0/2
mtu 1600
ip address 172.16.26.2 255.255.255.0
duplex auto
speed auto
mpls ip
!
interface Serial0/1/0
mtu 1600
ip address 172.16.23.2 255.255.255.0
mpls ip
!
interface Serial0/1/1
mtu 1600
ip address 172.16.25.2 255.255.255.0
mpls ip
clock rate 72000
!
!
router ospf 1
network 172.16.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop
udptn v120 ssh
stopbits 1
line vty 0 4

```


ICT-laboratorion P2-laitteen konfiguraatio

Liite 12 (2/2)

```
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

```

Current configuration : 3306 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE7
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
ip routing
no ip domain-lookup
!
crypto pki trustpoint TP-self-signed-1160729728
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-
1160729728
revocation-check none
rsakeypair TP-self-signed-1160729728
!
crypto pki certificate chain TP-self-signed-
1160729728
certificate self-signed 01
 3082023C 308201A5 A0030201 02020101
300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D
53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31313630 37323937
3238301E 170D3933 30333031 30303134
 33375A17 0D323030 31303130 30303030
305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43
65727469 66696361 74652D31 31363037
 32393732 3830819F 300D0609 2A864886
F70D0101 01050003 818D0030 81890281
 81009DEF 56478451 36F1DBBE 56B6926A
BBA6CF81 E489CE75 7D730A06 CC59506C
 5FA0FA0F 8002E088 1C289AEF B1888834
DECB528C 8C75843D E5E511D8 5848A0C4
 F80FF8B8 623DE363 077B4CFA 8F07D3CD
1E1EA7DA 5A18A9F3 357596CE 948104E4
 A76A6DAF 975FB0D0 96346945 7585C76F
7913A8CB EAB7791E 69E87BDB 5DBA4FF2
 74F30203 010001A3 64306230 0F060355
1D130101 FF040530 030101FF 300F0603
 551D1104 08300682 04434537 2E301F06
03551D23 04183016 8014159B 035F202C
 37D00965 0CF22336 240ABAE7 8037301D
0603551D 0E041604 14159B03 5F202C37
 D009650C F2233624 0ABAE780 37300D06
092A8648 86F70D01 01040500 03818100
 165F334A CCF3ED73 8FDD1A0E D94BB43B
2BB05462 FDFFDA9F 0905F74A DF266A3C
 CB66222C 5D963D9D BD99F360 58B98447
244B8BAF A1CC0B4D 78F5AAE2 5E11022B
 9A3691AC 9E48C732 B35EB407 DA84F058
243E2F34 72EDA7F7 4242FE61 F061BB74
 6322F57A DE1987DB 77EC3895 521A5FE3
10D31984 036A896C CEB1BDD2 7770FA2B
quit
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 11
name testi
!
interface Loopback0
ip address 192.168.1.7 255.255.255.255
!
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
!
interface Vlan10
ip address 192.168.10.7 255.255.255.0
!
router ospf 100
log-adjacency-changes
network 192.168.0.0 0.0.255.255 area 0
!
ip classless
ip http server
ip http secure-server
!
ip sla enable reaction-alerts

```

ICT-laboratorion CE7-laitteen konfiguraatio

Liite 13 (2/2)

```
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous  
line vty 0 4  
  login  
line vty 5 15  
  login  
!  
end
```

```

Current configuration : 3345 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE8
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
vtp mode transparent
ip routing
no ip domain-lookup
!
crypto pki trustpoint TP-self-signed-131847936
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-
131847936
  revocation-check none
  rsakeypair TP-self-signed-131847936
!
crypto pki certificate chain TP-self-signed-
131847936
  certificate self-signed 01
    3082023A 308201A3 A0030201 02020101
300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D
53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31333138 34373933
36301E17 0D393330 33303130 30313631
  305A170D 32303031 30313030 30303030
5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365
72746966 69636174 652D3133 31383437
  39333630 819F300D 06092A86 4886F70D
01010105 0003818D 00308189 02818100
  B68150E8 A917F454 351EEB5F 6BC1A407
C1445423 EB3B6872 322C7A06 5D255655
  B1774E0E 99176034 101ABB9A 2D3EBB51
0066C3E2 C653FE26 36743F37 CCB9ECA4
  30CD09E6 B2C1F53B A6071734 8EE53861
2E13AFF0 1BF4D1CA B8277C2B 62CCA2A1
  A4EFEA83 3B4A10D2 7A9019D3 8BCB5B72
863884C6 9B954569 A6A0E86B 3825F4E7
02030100 01A36430 62300F06 03551D13
0101FF04 05300301 01FF300F 0603551D
  11040830 06820443 45382E30 1F060355
1D230418 30168014 65630311 1B463CA5
  09255921 53670210 794174B3 301D0603
551D0E04 16041465 6303111B 463CA509
  25592153 67021079 4174B330 0D06092A
864886F7 0D010104 05000381 81003571
  57C195F2 99132ECA 9F15D2AE 2F04A127
55FC65BD 06BE6AEE 54C7853A 954892F9
  B3BF101D E1CD8851 DF511B9E 6AF4FD03
A9BE7CCF 28CD36A1 58037D7E A9D6BAAE
  8E5F49DF C8CE4AC4 8B1CFD76 AA71EF31
AD32A30A CAE34CFC F38A9C05 897969FE
  83283779 95F6E51E D3D51AC2 FB2A10D0
197795F7 594B854D B72E1651 A845
quit
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 11
  name testi
!
interface Loopback0
  ip address 192.168.1.8 255.255.255.255
!
!
interface FastEthernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Vlan1
  no ip address
!
interface Vlan11
  ip address 192.168.11.8 255.255.255.0
!
router ospf 100
  log-adjacency-changes
  network 192.168.0.0 0.0.255.255 area 0
!
ip classless
ip http server
ip http secure-server
!
line con 0

```

ICT-laboratorion CE8-laitteen konfiguraatio

Liite 14 (2/2)

```
exec-timeout 0 0
logging synchronous
line vty 0 4
login
line vty 5 15
login
!
end
```