KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Teemu Kunnari

MPLS TE -TUNNELOINTITEKNIIKAN TESTAUS SIMUNET-YMPÄRISTÖSSÄ

Opinnäytetyö 2013

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

KUNNARI, TEEMU

MPLS TE -tunnelointitekniikan testaus SimuNet-ympäristössä

Opinnäytetyö 41 sivua + 16 liitesivua
Työn ohjaaja Yliopettaja Martti Kettunen
Toimeksiantaja SIMUNET/KYMP Oy
Toukokuu 2013
Avainsanat MPLS, MPLS TE, RSVP, LSR

Tietoverkkojen nopea kasvu on tehnyt verkkojen huolellisesta suunnittelusta ja kaistanhallinnasta merkittävän osan verkkoinfrastruktuureja. Verkkoliikenteen saatavuuden ja laadun takaaminen vaatii verkon liikennekuormien tasapainottamista ruuhkautumisen estämiseksi kriittisissä verkkopalveluissa.

Kymenlaakson ammattikorkeakoulussa toimii tietoverkkojen kehitys- ja testausympäristö SimuNet. SimuNet simuloi modernia operaattoriverkkoa teknisiltä osiltaan pienemmässä mittakaavassa. Työn tarkoituksena on luoda SimuNet-runkoverkkoon toimiva tunnelointi käyttäen MPLS Traffic Engineering -tekniikkaa ja testata tunnelien välistä konvergoitumista päätunneli-varatunneli-mallin avulla.

Käytännön osuudessa SimuNet-verkkoon luotiin kahden reuna- ja runkolaitteen välille päätunneli-varatunneli-mallin mukainen MPLS Traffic Engineering -tunnelointi. Tietoliikennettä ohjattiin SimuNetin MPLS-verkon läpi päätunnelia pitkin. Varatunneli luotiin päätunnelin suojaksi käyttäen Fast Reroute -tekniikkaa mahdollisten linkkivaurioiden varalta. Fast Reroute -tekniikan mahdollistamaa nopeaa uudelleenreititystä tunnelien välillä hyödynnettiin konvergoitumisajan minimoimiseksi.

Tuloksena SimuNet-verkkoon saatiin konfiguroitua toimiva tunnelointi, jossa liikenne kulkee kuvitteellisten asiakaskoneiden välillä MPLS-verkon läpi. Liikenne ohjattiin staattisin reitein tunneleihin niiden mahdollistaman suoraviivaisen liikenteen kohdentamisen avulla. Liikenteen uudelleenreititys päätunnelilta varatunnelille saatiin toimimaan käyttämällä MPLS TE Fast Reroute -tekniikkaa. Tunnelointi todettiin toimivaksi vaikka konvergoitumisajan suhteen ei päästy ennalta odotettuihin tuloksiin.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

KUNNARI, TEEMU	Testing of MPLS TE Tunneling Technology within SimuNet Environment
Bachelor's Thesis	41 pages + 16 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	SIMUNET/KYMP OY
May 2013	
Keywords	MPLS, MPLS TE, RSVP, LSR

Rapid growth of networks has made careful planning and load balancing vital parts of network infrastructures. Ensuring the quality and availability of network traffic requires the balancing of traffic loads to prevent congestion in critical network services.

In the premises of Kymenlaakso Unversity of Applied Sciences, a development and testing environment called SimuNet is hosted. SimuNet is used to simulate a modern operator network in a smaller scale. The goal of this study was to create an MPLS Traffic Engineering tunneling model into SimuNet core network and to test the convergence time of traffic steering between the main tunnel and the back-up tunnel.

In the empirical section of the study, an MPLS Traffic Engineering tunneling model was implemented into SimuNet. Network traffic was routed through the SimuNet MPLS network inside the main tunnel. The back-up tunnel was created to protect the main tunnel by using Fast Reroute technology in case of possible link failures. The quick rerouting abilities of Fast Reroute technology was used to minimize the convergence time.

As a result, an operational tunneling model was implemented into SimuNet where data traffic was sent between fictitious client computers through the SimuNet MPLS network. Traffic was steered into the tunnels by using static routing. Static routing provided for direct traffic controlling. The rerouting of traffic between the main tunnel and the back-up tunnel was put into effect by using Fast Reroute technology. Tunneling was found to work as intended even though convergence time measurements did not reach the expected results. To optimize the convergence time, future projects of MPLS Traffic Engineering should focus on technologies such as Dual TE Metrics and RSVP Hello State Timer.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

LYHENNELUETTELO 6

1 JOHDANTO 8

2 MPLS-TEKNIIKKA 9

2.1 Yleistä 9
2.2 MPLS-verkon toimintaperiaate 9
2.3 MPLS-header 10
2.4 Label Distribution Protocol (LDP) 10
2.5 Label Switched Path (LSP) 11
2.6 Label Switch Router (LSR) 12

3 MPLS TRAFFIC ENGINEERING 13

3.1 Yleistä 13
3.2 MPLS TE -käyttökohteet 14
3.3 Mitä MPLS TE tarvitsee toimiakseen? 15
3.4 MPLS TE -informaation jakelu 18

3.4.1 Vaatimukset IGP:lle 18
3.4.2 OSPF ja Traffic Engineering 19
3.5 Linkkien TE-attribuutit 20
3.6 TE-tunnelin attribuutit 21
3.7 PCALC 22
3.8 RSVP 23
3.9 FRR-tekniikka 23
3.10 Liikenteen ohjaus MPLS TE -tunneliin 24

4 SIMUNET 26

5 KÄYTÄNNÖN KONFIGUROINTIKÄSKYT 28

5.1 Runkolaitteiden tunnelikonfigurointi 28
5.2 Fast Reroute -konfigurointi 29

6 TEKNINEN TOTEUTUS 30

6.1 Alkutilanne 30

6.2 Tunnelien muodostus 31

6.3 Tunnelien testaus 35

7 YHTEENVETO 37

LÄHTEET 39

LIITTEET

Liite 1. SimuNet-verkon fyysinen topologia

Liite 2. Tunnelointi SimuNet-ympäristössä

Liite 3. PE3-laitteen konfiguraatio

Liite 4. PE4-laitteen konfiguraatio

Liite 5. P1-laitteen konfiguraatio

Liite 6. P2-laitteen konfiguraatio

LYHENNELUETTELO

EAKR	*Euroopan aluekehitysrahasto*
ERO	Explicit Route Object: *RSVP -signaalin reitityskartta*
FEC	Forward Equivalency Class: *Yhtenäisesti kohdeltu pakettiryhmä MPLS-verkossa*
FRR	Fast Reroute: *MPLS TE:n lisätekniikka nopeaan liikenteen uudelleenreititykseen ja linkkien suojaukseen*
IPv4	Internet Protocol version 4: *Internet-protokollan versio 4.*
IP	Internet Protocol: *TCP/IP-mallin protokolla, joka kuljettaa pakettikytkentäisen verkon paketteja*
IGP	Interior Gateway Protocol: *Yleisnimitys autonomisen alueen sisällä toimivista reititysprotokollista*
IOS	Internetwork Operating System: *Cisco Systemsin verkko-laitteiden käyttöjärjestelmä*
LDP	Label Distribution Protocol: *Protokolla lipputietojen vaih-toon*
LIB	Label Information Base: *Laitteiden ylläpitämä tietokanta lippumerkinnöistä MPLS- verkossa*
LSA	Link-State Advertisement: *OSPF -laajennus*
LSP	Label Switched Path: *MPLS-verkon polku, jota pitkin paketit kulkevat*
LSR	Label Switch Router: *Runkolaite MPLS-verkossa*

MPLS	Multiprotocol Label Switching: *Lippumerkintöihin perustuva pakettien kytkentätekniikka*
MPLS TE	Multiprotocol Label Switching Traffic Engineering: *MPLS-tekniikalle spesifinen tunnelointitekniikka*
OSPF	Open Shortest Path First: *Autonomisen alueen sisäinen reititysprotokolla*
PBR	Policy-Based Routing: *Sääntöihin perustuva reititys*
PE-laite	Provider Edge: *Operaattoriverkon reunalaite*
P-laite	Provider: *Operaattoriverkon runkolaite*
QoS	Quality of Service: *Palvelun laatu*
RSVP	Resource Reservation Protocol: *MPLS TE:n käyttämä tunnelien signalointiprotokolla*
SPF	Shortest Path First: *Reititysprotokollan algoritmi*
TCP	Transmission Control Protocol: *tietoliikenneprotokolla yhteyksien luomiseksi tietokoneiden välille*
TLV	Type-Length Value: *Elementti, joka ylläpitää MPLS TE spesifistä informaatiota*
TTL	Time to Live: *Kertoo jäljellä olevien reititinhyppyjen määrän*
UDP	User Datagram Protocol: *yhteydetön protokolla, jota käyettään yleisesti reaaliaikaisissa sovelluksissa*

1 JOHDANTO

Tietoverkkojen nopea kasvu viime vuosien aikana on tehnyt verkkojen suunnittelusta ja kaistanhallinnasta entistä tarkempaa. Verkkojen kasvu ja laajeneminen asettaa kaistahallinnalle aiempaa suuremman roolin. Suunnitteluvaiheessa ei koskaan voida täysin ennustaa kuinka liikenne tulee jakautumaan verkossa. Tämän takia joudutaan etsimään hyötyä monimutkaisista tekniikoista, joilla liikennettä voidaan hallita ja tätä kautta parantaa saatavuutta sekä toimivuutta. Suurissa runkoverkoissa ongelmana on usein huonosti kontrolloitu verkkoliikenteen ohjaus eri linkkien välillä. Hetkelliset suuret piikit liikennemäärässä voivat aiheuttaa hallitsemattoman suuren tulvan yhdelle linkille, mutta samalla myös jättää toisaalla vapaita linkkejä hyödyntämättä. Tämän kaltaisia ongelmia varten on kehitetty MPLS-verkossa toimiva MPLS Traffic Engineering -tekniikka. (Osborne & Simha 2002, 26.)

Opinnäytetyön tarkoituksena on huolellisesti tutustua MPLS-verkkojen toimintaan, Traffic Engineering-tekniikkaan Cisco IOS -ympäristössä ja dokumentoida ohje TE-tunnelien muodostamista varten sekä siihen liittyvän teorian ymmärtämiseksi. Teoriaosuudessa käsitellään MPLS-tekniikkaa ja sen ominaisuuksia, TE-tekniikkaa ja esitellään SimuNET-ympäristö. Työssä esitetään myös varareitin konvergoitumisaikaa mittaava testi kahden TE-tunnelin välillä linkkivian sattuessa. Tekninen toteutus toteutetaan SimuNET-ympäristössä.

Teknisessä toteutuksessa käytetty SimuNET-ympäristö pyrkii mahdollisimman hyvin mallintamaan operaattoritason runkoverkkoa, joten TE-tunneloinnin testaukseen tarvittavat reuna (PE) sekä runkolaitteet (P) olivat käytettävissä valmiiksi toimivassa MPLS-verkossa.

Työssä käytettiin Cisco Systemin laitteita. Tästä johtuen konfiguraatiot ja termistöt ovat Cisco-laitteille ominaisia.

2 MPLS-TEKNIIKKA

MPLS-tekniikka on laajalti käytössä oleva reititystekniikka etenkin runkoverkkotasolla. MPLS-tekniikka on perinteistä IP-reititystä selkeämpi ja monipuolisempi tapa kuljettaa liikennettä verkossa. (RFC 3031.)

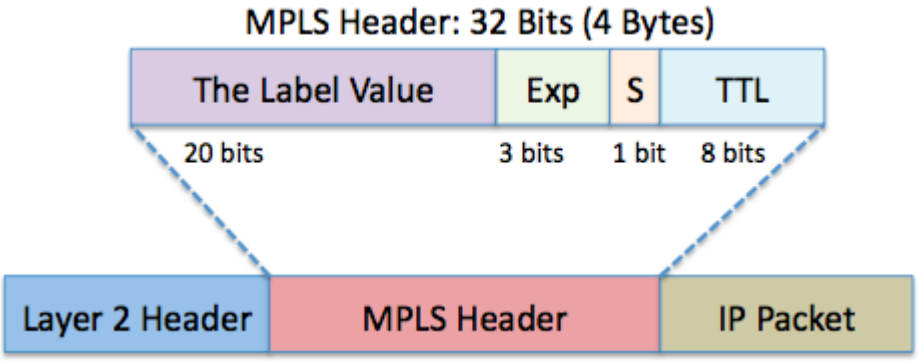
2.1 Yleistä

MPLS on normaalista IP-reitityksestä eroava tekniikka. MPLS käyttää lipuiksi kutsuttaja otsakemerkintöjä, joita avuksi käyttäen paketit kytketään ja kuljetetaan verkon läpi (RFC 4448.). Tämä mahdollistaa useiden eri protokollien kuljetuksen yhden infrastruktuurin ylitse. MPLS yhdistää Layer 2- ja Layer 3 -tekniikoiden parhaat ominaisuudet. MPLS-tekniikassa luodaan niin sanottuja LSP-polkuja verkon läpi reunalaitteiden välille. Tästä johtuen vain reunalaitteiden tarvitsee ymmärtää verkkoliikenne sen alkuperäisessä muodossa. Muut verkon laitteet toimivat vain välikäsinä reititysprosessissa. (Aziz & Azlam 2010, 24.)

2.2 MPLS-verkon toimintaperiaate

MPLS-kytkennässä IP-paketin otsikkotiedot analysoidaan liikennettä vastaanottavassa reunalaitteessa ja paketille annetaan lipuksi kutsuttu merkintä lukuarvon muodossa. Paketti ohjataan verkkoon lippuun sisällytettyjen merkintöjen perusteella ja kytkentäpäätökset paketin edetessä tehdään perustuen tähän lippumerkintään. MPLS-verkon reitittimet voivat tarvittaessa lisätä, poistaa tai vaihtaa lipun ennen edelleenvälitystä. MPLS-verkon laitteet koostuvat reunalaitteista (Edge LSR), jotka sijaitsevat MPLS-runkoverkon reunoilla, sekä runkolaitteista (LSR). Reunalaitteiden välille muodostetaan Label Switched Path (LSP) -polkuja, joita pitkin liikenne MPLS-verkossa kuljetetaan. Liikennettä vastaanottava reunalaite lisää lipun kuljetettavaan pakettiin, määrittää sen tiettyyn Forwarding Equivalence Class (FEC) -ryhmään ja lähettää sen kohti toista reunalaitetta LSP-polkua pitkin. FEC-ryhmä määrittää mihin LSP-polkuun liikenne ohjataan. Runkolaitteiden rooli on vain tutkia lippumerkintöjä paketeissa ja kytkeä liikennettä edelleenvälitettäväksi niiden mukaan. (Oinonen 2011, 11.)

2.3 MPLS-header



Kuva 1. MPLS -otsikko (The MPLS Forwarding Plane)

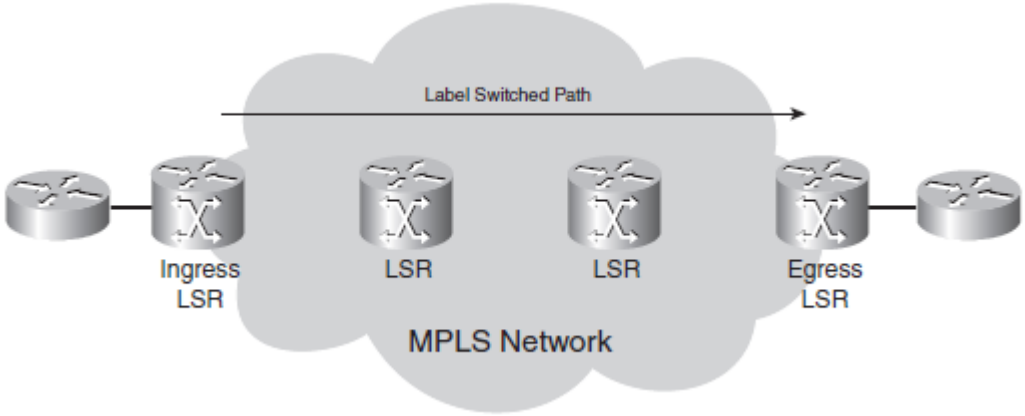
MPLS-header eli otsikko on 32-bittinen. Se koostuu neljästä eri kentästä. Ensin on otsikko-kenttä, joka on pituudeltaan 20-bittiä. (Aziz & Aslam 2010, 24.) Tämä kenttä pitää sisällään myös otsikon konkreettisen lippulukuarvon. Tämän jälkeen on 3 bitin pituinen EXP-kenttä, joka on ainoastaan palvelun laatu määrityksille (QoS) tarkoitettu. Seuraavaksi on 1-bitin pituinen kenttä, joka kertoo onko kyseessä lippupinon viimeinen lippu. Tämä on merkityksellinen vain paketilla, jolla on useampi kuin yksi lippumerkintä. Viimeisenä on 8-bitin pituinen Time to Live (TTL) -kenttä. TTL-kenttä estää paketin joutumisen ikuiseen silmukkaan. TTL-kentän arvo vähenee yhdellä jokaisella hypyllä ja saavuttaessaan arvon nolla paketti poistetaan (De Ghein 2007, 25-26.)

2.4 Label Distribution Protocol (LDP)

LDP on protokolla, jota MPLS verkko tarvitsee signalointiin laitteiden välillä. LDP tulee olla aktiivisena kaikissa laitteissa, jotka ovat lippukytkentäisten polkujen varrella. Sen avulla mainostetaan MPLS -pakettien lippumerkinnät runkoverkossa. LDP-protokollan pohjalta muodostuu myös lippumerkintöjen tietokanta Label Information Base (LIB), johon lippumerkinnät säilötään. (De Ghein 2007, 68.) Toisiinsa suoraan kytketyt laitteet MPLS -verkossa muodostavat LDP-istunnon. LDP-istunto on TCP yhteys, joka muodostuu kahden IP-osoitteen välille LSR-laitteissa. Istuntoa ylläpidetään LDP -paketeilla tai keep-alive viestein.

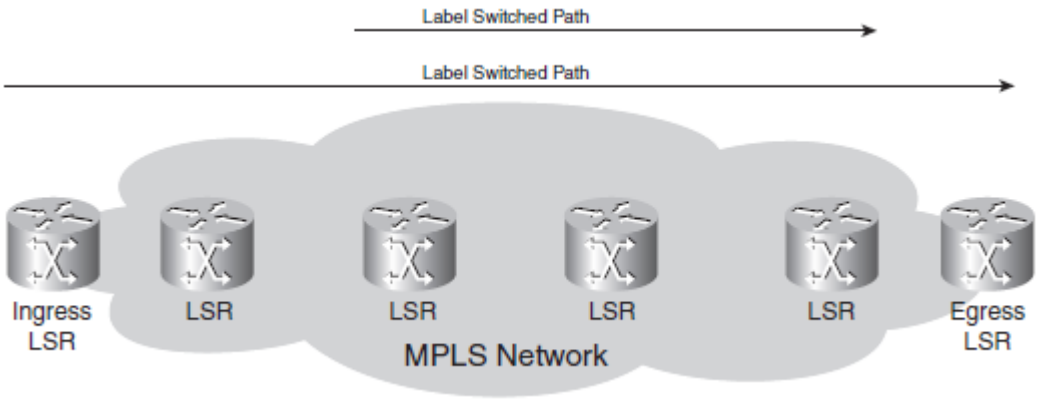
LDP tarvitsee toimiakseen erillisen reititysprotokollan (IGP). LDP-paketit kulkevat LSP-poluissa, jotka käyttävät IGP-taulun mukaisia lyhyimpiä reittejä ja tekevät tarvittavat muutokset reitityksessä IGP:tä analysoiden. (Osborne & Simha 2002, 67-75.)

2.5 Label Switched Path (LSP)



Kuva 2. MPLS -verkon läpi kulkeva LSP -polku (De Ghein 2007, 30.)

LSP on polku lippukytkentäisten laitteiden (LSR) välillä MPLS-verkossa. LSP on polku, jonka sille määrätyt paketit tai ryhmät (FEC) valitsevat. LSP-polun alkupäässä oleva laite on ingress LSR ja loppupään laite on egress LSR. Välissä sijaitsevat laitteet ovat runkolaitteita (intermediate LSR). LSP -polut ovat yksisuuntaisia. Jos halutaan polku verkon molemmista päistä reunalaitteiden välille, on luotava kaksi eri polkua, vaikka reitti olisi sama. LSP-polkuja voi muodostaa myös sisäkkäin (nested LSP), tällöin ingress LSR ei välttämättä ole ensimmäinen reititin, joka on enkapseloinut paketin. Jos LSP alkaa keskeltä MPLS-verkkoa, niin paketin lippupinoon lisätään toinen lippu. Pinon ensimmäinen lippu kuuluu sisemmälle LSP-polulle ja ulompi lippu ingress-ja egress-laitteiden välissä olevalle pääreitille. Tätä ideaa sovelletaan esimerkiksi MPLS Traffic Engineering -tunneleissa. (De Ghein 2007, 29-30.)



Kuva 3. Nested LSP; LSP -polku toisen polun sisällä (De Ghein 2007, 30.)

2.6 Label Switch Router (LSR)

LSR-laite on reititin, joka tukee MPLS-tekniikkaa. LSR-laite ymmärtää MPLS:ssä käytettyjä lippuja ja osaa lähettää ja vastaanottaa MPLS:lle ominaista lippukytkentäistä tietoliikennettä. MPLS-verkossa esiintyy kolmea erilaista LSR-laitetta, joilla jokaisella on omanlaiset tehtävät. Nämä ominaisuudet muodostavat kokonaisuuden kun paketti kuljetetaan MPLS-verkon läpi.

LSR -laitteet:

-Ingress LSR: vastaanottaa paketin, joka ei ole vielä lippukytketty ja lisää pakettiin lippupinon ennen paketin siirtoa LSP-polkuun.

-Egress LSR: vastaanottaa lippukytkentäisen paketin, poistaa lipun tai liput paketilta ja siirtää paketin eteenpäin ulos MPLS-verkosta.

-Intermediate LSR (runkolaite): runkolaitteen tehtävänä on vastaanottaa lippukytketty paketti, suorittaa operaatio ja välittää se edelleen oikeaan linkkiin

LSR-laitteet pystyvät suoriutumaan kolmesta eri operaatiosta. Nämä operaatiot ovat pop (poisto), push (lisäys) ja swap (vaihto). Jotta lippukytkentäinen reititys toimii, laitteiden tulee osata käsitellä paketteja oikein. Sisään tuleville paketeille lisätään lippupino (push) liikenteen saapuessa verkkoon sisääntuloreunalla (ingress). Matkan varrella lippupinoon voidaan lisätä myös enemmän kuin yksi lippu push-operaatiolla. LSR-laite osaa myös vaihtaa lippujen järjestystä pinossa swap-operaatiolla ennen jatko kytkentää ja liikenteen edelleenvälitystä. LSP-polun loppupisteessä (egress) käyte-

tään pop-operaatiota poistamaan paketista lippupino ennen kuin paketti kytketään ulos MPLS-verkosta. (De Ghein 2007, 29.)

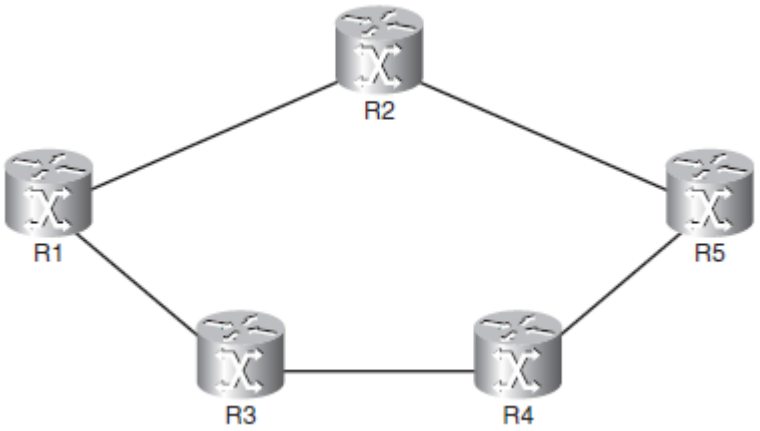
3 MPLS TRAFFIC ENGINEERING

MPLS Traffic Engineering -tekniikan (MPLS TE) perusidea on optimoida MPLS-verkon sisällä kulkeva tietoliikenne luomalla Traffic Engineering –tunneleita tuomaan tasapainoa linkkien liikennekuormiin. Traffic Engineering -tunnelit ovat LSP-polkuja, joilla on uniikkeja ominaisuuksia.

3.1 Yleistä

IP-reitityksen perusidea on saada mahdollisimman nopeasti tietoliikennettä kuljettava verkkokokonaisuus. IP-reitityksessä tukeudutaan cost-arvoihin, joita määritetään linkeille. Linkki, jolle on määritetty pienin cost-arvo, toimii ensisijaisena valintana paketeille. Näiden cost-arvojen pohjalta reititysprotokolla laskee ensisijaisesti käytettävän reitin. Esimerkkinä voisi mainita Open Shortest Path First -protokolla (OSPF), joka käyttää linkeissä metric-arvoja.

Jos kyseessä on suuri verkko, tämän tyylisestä reititysmenetelmästä aiheutuu myös linkeille erittäin suurta kuormaa. Reititysprotokolla laskee koko verkon liikenteelle saman reitin johtuen least-cost ideasta ja linkit tukkeutuvat. Normaali IP-reititysmalli ei myöskään osaa huomioida linkkien kaistakapasiteettia. Linkin optimaalinen kaistakapasiteetti voi erota huomattavasti kuormasta, joka sille aiheutuu liikenteen kulkiessa sen läpi. Tämä aiheuttaa myös pakettien katoamista, ja voi johtaa myös tilanteisiin, joissa liikennettä työnnetään linkkiin, joka jo pudottaa paketteja kapasiteetin puutteen takia. Suuri osa verkon linkeistä saattaa jäädä käyttämättä, mutta samalla osa voi myös olla ylikuormitettuja, jos asiaa tarkastellaan optimoinnin ja eheän verkkokokonaisuuden näkökulmasta. MPLS Traffic Engineering (MPLS TE), on tekniikka, jonka avulla tätä ongelmaa voidaan lievittää. MPLS TE:n avulla liikennettä voidaan ohjata tunneleiden avulla pois ylikuormitetuilta verkon osilta kokonaan tai osittain. (De Ghein 2007, 249.)



Kuva 4. MPLS TE -havainnollistus (De Ghein 2007, 250.)

Jos ajatellaan, että kuvassa 4 jokaisella linkillä on yhtä suuri cost-arvo, niin normaalin IP-reititysmallin mukaisesti lyhin reitti R1-R5 on R1-R2-R5. Kaikki liikenne ei oikeassa verkossa kuitenkaan ikinä kulje vain yhtä kyseistä reittiä. Liikennettä voi tulla verkkoon toisesta reitittimestä ja lähteä toisesta. Tästä syystä edes cost-arvoja säätämällä ei linkkikuormia saada optimoitua järkevästi. Verkon optimointi cost-arvoilla onnistuisi ainoastaan jos liikenne kulkisi aina esimerkiksi kuvan 4 mukaisesti laitteiden R1-R5 välillä. Jos katsotaan kuvaa 4 ja oletetaan, että liikennettä saapuu verkkoon R3:n kautta ja poistuu R2:n kautta, niin tämä luo tilanteen, jossa toista kautta on yhden hypyn pidempi etäisyys. Tilannetta on mahdoton hallita cost arvoja muuttamalla. Linkkien kaistakapasiteetti voi myös kasvaa laiteuudistusten myötä, joka sekoittaisi cost-arvoilla luodun optimoinnin. (De Ghein 2007, 250)

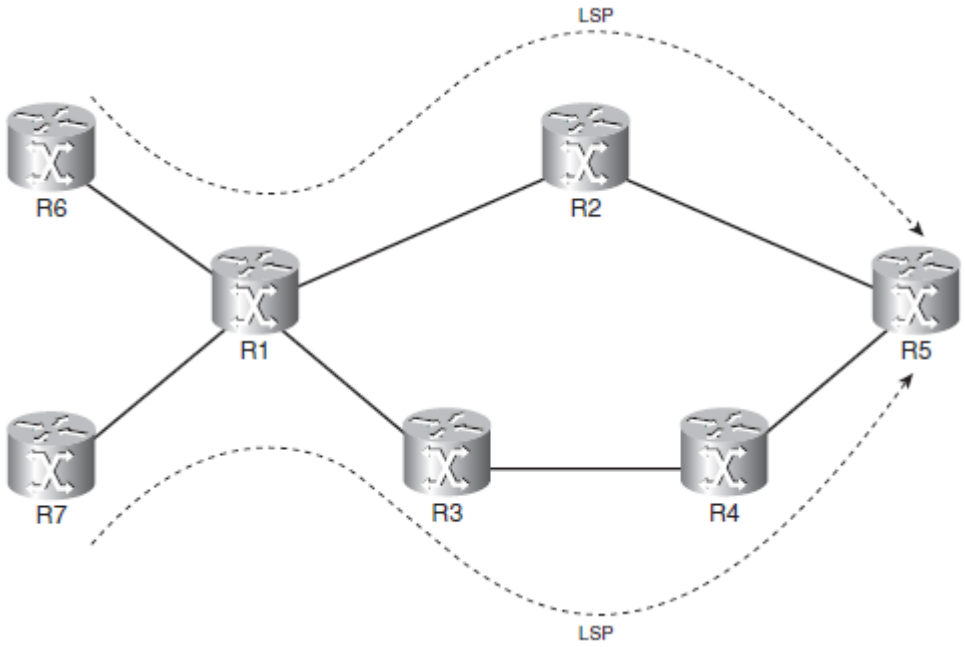
3.2 MPLS TE -käyttökohteet

MPLS TE -tekniikkaa käytetään tilanteissa, joissa verkkoliikenne MPLS -verkon sisällä on suurta ja liikennettä saapuu ja poistuu useilta eri laitteilta aiheuttaen hankalia tilanteita kontrolloida liikennettä ja pitää linkkikuormat tasapainossa.

MPLS TE:n pääperiaatteet:

- Liikennevirtojen hallittu ohjaus läpi verkkoinfrastruktuurin ja ylikuormittuneiden linkkien poisto
- Huomioi linkkien kaistakapasiteetit
- Huomioi linkkien attribuutit. Esimerkiksi viive ja kohina

- Mukautuu automaattisesti linkkien attribuuttien muutoksiin ja kaistakapasiteetin kasvuun tai pienenemiseen.
- TE:llä kontrolloitu liikenne käyttää lippukytkentäistä reititystä, haluttu reitti määritetään jo verkon sisääntuloreunalla. (De Ghein 2007, 251)



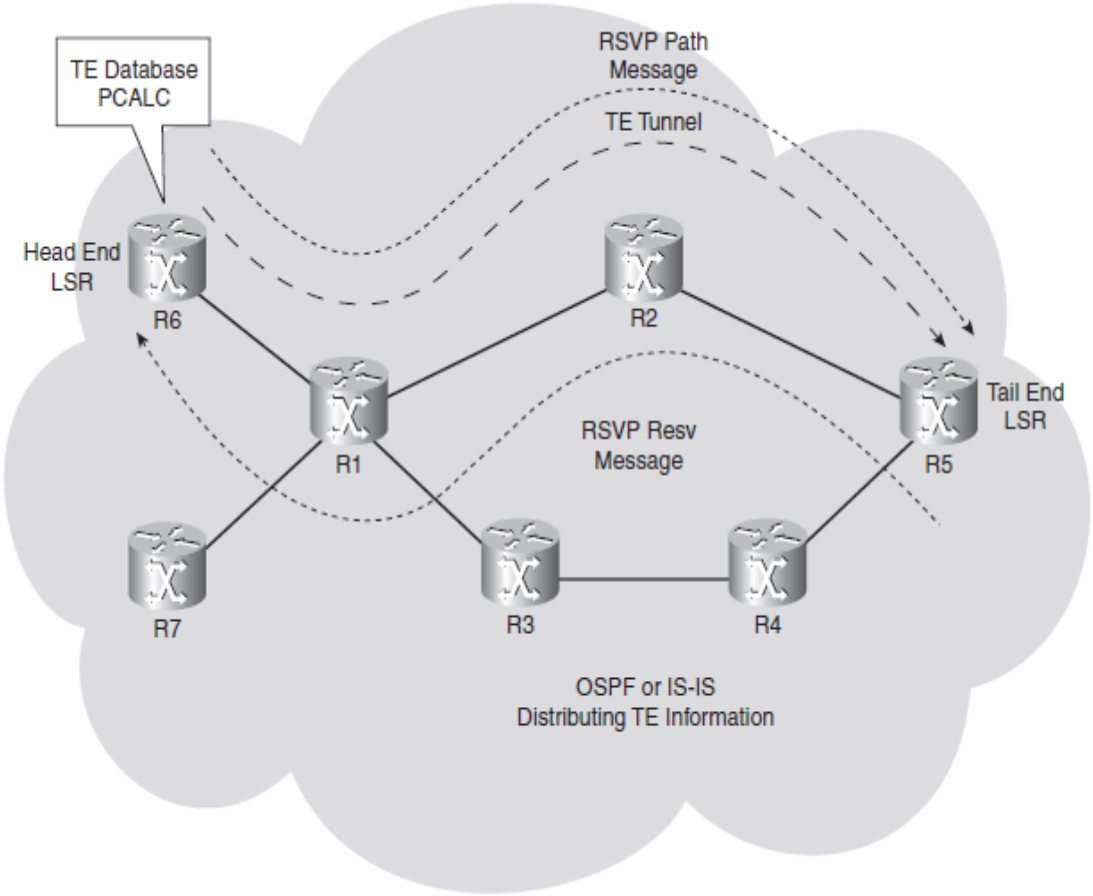
Kuva 5. Kaksi MPLS TE -tunnelia. (De Ghein 2007, 251.)

Kuvasta 5 voi helposti selventää MPLS TE:n perusideaa. Jos kyseenomaisessa verkossa olisi käytössä vain normaali IP-reititys, kaikki liikenne kulkisi aina R1:stä eteenpäin reittiä R1-R2-R5, koska siinä on vähiten hyppyjä. Kun käyttöön otetaan MPLS-reititys, niin kuvan 5 mukaisesti voidaan luoda kaksi erillistä tunnelia jo ennen laitetta R1. Koska menetelmä käyttää lippukytkentäistä reititystä määritetään tunnelit jo reunalaitteilla R6 ja R7. Tunnelien risteyskohdassa R1-laite osaa aiempien määritysten myötä kytkeä liikenteen oikeisiin tunneleihin, eikä ohjaa liikennettä ainoastaan yhtä polkua. (De Ghein 2007, 252.)

3.3 Mitä MPLS TE tarvitsee toimiakseen?

MPLS TE:tä voidaan käyttää verkoissa, joissa on LSR-laitteita. TE-tunnelien reunalaitteiden eli head-end ja tail-end laitteiden välillä pitää olla käytössä reititysprotokolla esimerkiksi OSPF. OSPF:n kaltainen reititysprotokolla vaaditaan linkkitietojen jakamiseen verkossa, jotta reunalaitteiden välillä sijaitsevat runkolaitteet oppivat verkko-

topologian. MPLS TE -tunneli on yksisuuntainen LSP. MPLS TE -tunneli vaatii signaloinnin verkossa toimiakseen. Signalointiin käytetään RSVP-signalointiprotokollaa



Kuva 6. MPLS -TE tunnelin osat. (De Ghein 2007, 253.)

Tekniset osat, joihin TE perustuu:

- Linkkikohtaiset rajoitteet: linkin maksimi kapasiteetti, tunnelikohtaiset reittimääritykset.
- TE-informaation jakaminen verkolle reititysprotokollan toimesta TE-laajennuksilla.
- Algoritmi, joka laskee parhaan reitin head-end ja tail-end laitteiden välille (PCALC).
- Signalointiprotokolla, jolla signaloidaan tunnelia verkossa: Resource Reservation Protocol (RSVP).
- Eri keinot, joilla tietoa välitetään tunneliin. (De Ghein 2007, 252-253)

MPLS TE pyrkii kontrolloimaan tietoliikennevirtoja verkon sisällä mukaillen verkon resursseja. Näitä resursseja ovat esimerkiksi linkkien kapasiteetit ja niille käsin määri-

tetyt attribuutit. (Osborne & Simha 2002, 108.) Attribuutit, joita linkeille määritetään jaetaan verkon sisällä käyttäen OSPF-reititysprotokollaa. OSPF-reitiysprotokollaan on luotu laajennuksia, jotta se ymmärtää MPLS TE:n uniikkeja määrityksiä. (De Ghein 2007, 254.)

TE-informaation tietokanta luodaan reititysprotokollan jakeleman linkki-informaation pohjalta. Tietokanta ylläpitää kaikkien MPLS TE -tunneleita käyttävien linkkien TE-määritykset. Tietokantaa hyväksikäyttäen lasketaan paras reitti verkon läpi reuna-laitteiden välillä. Reitin valintaan käytetään path calculation (PCALC) tai constrained SPF(CSPF) -algoritmeja. Molemmat ovat TE-laajennuksin modifioituja algoritmeja lyhyimmän reitin laskemiseksi reititystauluista kerätyn tiedon perusteella. Muunnelmat koskevat TE:lle ominaisten linkkimääritysten ymmärtämistä. MPLS TE:tä konfiguroitaessa varsinaiset tunnelikohtaiset määritykset tehdään aina head-end LSR-laitteessa. Määritykset koskevat kaistakapasiteettia ja tunneliattribuutteja. Linkeille määritetään omat kaistamääritykset ja attribuutit. Algoritmi valitsee lyhyimmän reitin vertailemalla tunnelin määrityksiä linkkien määrityksiin. Laskenta tehdään aina head-end LSR-laitteessa. (De Ghein 2007, 254.)

Jotta MPLS TE -tunneli pystyy operoimaan, myös verkon runkolaitteiden täytyy tietää mitä kytkentöjä sen tulee suorittaa paketeille, jotka se vastaanottaa ja välittää edelleen tunneleihin. Runkolaitteet eivät pysty oppimaan tarvittavia tietoja ilman signalointia tunnelin päästä päähän. MPLS TE käyttää RSVP-protokollaa signalointiin. TE-tunnelien käyttämä RSVP -protokolla on muunneltu versio alkuperäisestä RSVP- protokollasta. RSVP -protokolla signaloi tunnelia alkupäästä loppupäähän, sitä reittiä pitkin, jonka head-end laite on muodostanut pohjautuen PCALC-algoritmin laskentaan. RSVP-protokolla lähettää RSVP PATH -viestin head-end LSR-laitteesta tail-end laitteelle. Viestiin on sisällytetty request-komento MPLS-lipulle. Tail-end LSR lähettää vastauksena RSVP RESV -viestin, johon on sisällytetty MPLS-lippu, runkolaitteita varten. Jokaisen MPLS TE -tunnelin varrella olevan laitteen tulee signaloida yhteistä MPLS-lippua. RSVP-protokolla myös varmistaa, että TE-tunneli pystytään ottamaan käyttöön jokaisessa solmukohdassa. (De Ghein 2007, 255.)

RSVP-viestit reititetään verkon läpi käyttäen Explicit Route -objektia (ERO). (Explicit Route Objects). ERO kertoo RSVP-viestille mitä reittiä sen pitää kulkea saavuttaakseen tail-end LSR-laitteen. ERO saa reittitiedon PCALC-algoritmin avulla ja laskenta

suoritetaan aiemmin mainitun mukaisesti head-end LSR-laitteessa. RSVP-viesti varaa hetkellisesti kaistan jokaisessa linkissä ja pyytää lippua. Saavuttaessaan kohteen (tail-end), paluuviesti lähetetään takaisin toiselle reunalle. Paluuviestin mukana kulkeutuu lippu, joka kertoo mitkä paketit ohjataan tähän MPLS TE -tunneliin. RESV-viesti kertoo myös runkolaitteille, missä linkeissä niiden pitää varata resursseja TE-paketeille. (Osborne & Simha 2002, 168.)

3.4 MPLS TE -informaation jakelu

Reititysprotokollaa (OSPF TE laajennuksilla) käytetään jakamaan linkkikohtaiset määritykset kaikille verkon TE:tä käyttäville laitteille . Reititysprotokollan tulee ymmärtää TE-linkkien määritykset ja pystyä jakamaan tieto linkkien tilasta yhdessä laitteessa koko verkolle. (RFC 3906)

3.4.1 Vaatimukset IGP:lle

Kaikkien reitittimien, joita käytetään MPLS TE -tunneloinnissa tulee vastaanottaa verkkotopologiainformaatiot toisiltaan. Protokollalta (esim OSFP) vaaditaan ominaisuus, joka jakaa tiedon linkkien tilojen muutoksista verkolle. Tästä syystä esimerkiksi EIGRP-protokollaa ei voida käyttää, koska se perustuu tekniikkaan, joka valitsee aina parhaimman reitin, eikä huomioi vaihtoehtoisia reittejä. Reititysprotokollan täytyy myös tukea niitä resurssitietoja, joita TE käyttää linkeissä. (Minei & Lucek 2005, 44.)

TE:ssä käytetyt linkkiresurssit:

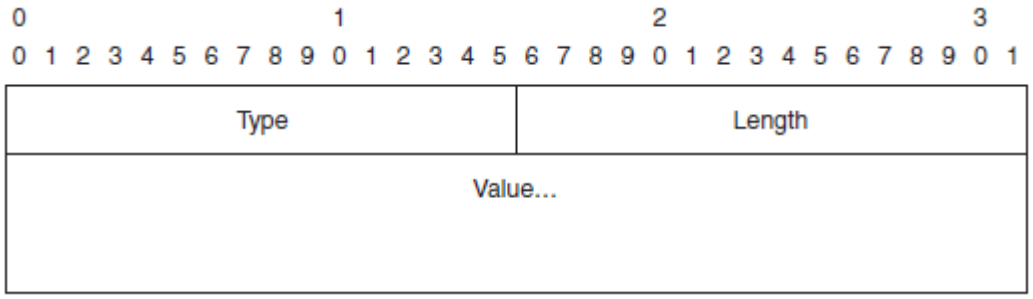
- TE metric -parametri
- Maksimikaista
- Kokonaiskaistanleveys, joka on käytettävissä TE:lle
- Varaamaton kaista (De Ghein 2007, 256)

TE metric -parametria voidaan käyttää muokkaamaan verkkotopologiaa. IP-topologian metric-parametria voidaan käyttää yhdessä TE:n metric-parametrin kanssa. (De Ghein 2007, 275.) Lähtökohtaisesti TE metric -parametri on yhtäläinen IGP metric -parametrin kanssa (OSPF cost) (Cisco Systems 2005b). IGP metric ja TE metric -parametreja voidaan tästä huolimatta käyttää yhtäaikaisesti ja molempia voidaan muunnella, jos topologiamuutokset sitä vaativat. Maksimi kaista on laitteen lin-

kin teoreettinen maksimi arvo tietoliikenteelle. TE:lle käytettävissä varattava kokonais kaista asetetaan jokaiselle linkille erikseen. Varaamaton kaista on linkin TE:lle varaaman kaistan ja vapaan käytettävissä olevan kaistan erotus. (De Ghein 2007, 256.)

3.4.2 OSPF ja Traffic Engineering

Jotta OSPF-protokolla pystyy toimimaan yhteistyössä MPLS TE -tunnelien kanssa siihen on luotu laajennuksia. RFC 2370:ssa on määritelty kolme mainostustekniikkaa: LSA-9, LSA-10 ja LSA-11 (Opaque LSAs; Opaque Link-state advertisements). Nämä laajennukset mahdollistavat ulkopuolisen informaation kuljetuksen OSPF:n kanssa. Näiden LSA-laajennusten myötä TE-informaatio voidaan sisällyttää OSPF-protokollaan, joka edelleen välittää tiedot koko verkolle (RFC 2370). MPLS TE käyttää Opaque LSA-10:tä, johon on sidottu yksi tai useampi Type Length Value -elementti (TLV). TLV-elementti sisältää MPLS TE -informaation.



Kuva 7. TLV-elementti (Type Length Value) (De Ghein 2007, 258.)

TE käyttää kahta eri tyyppistä TLV-elementtiä: Router Address TLV ja Link TLV. Router Address TLV -elementtiin on sidottu router ID, jota MPLS TE tarvitsee. Link TLV -elementtiin on sisällytetty alielementtejä (sub-TLV), jotka ylläpitävät linkkikohtaisia TE-tietoja. (RFC 3630)

OSPF Link TLV Sub-TLVs

Sub-TLV Number	Name	Length in Octets
1	Link type	1
2	Link ID	4
3	Local interface IP address	4
4	Remote interface IP address	4
5	Traffic engineering metric	4
6	Maximum bandwidth	4
7	Maximum reservable bandwidth	4
8	Unreserved bandwidth	32
9	Administrative group	4

Kuva 8. OSPF Link TLV SubTLVs (linkkikohtaiset alielementit TE-resursseille) (De Ghein 2007, 258.)

OSPF määritetään MPLS TE:n käyttöön konfiguroimalla suoraan OSPF-rajapintoihin. OSPF-rajapintoihin määritetään konfiguroitavan laitteen tunnisteosoite Router-id sekä sen käyttämän OSPF-alueen area tunnus.

3.5 Linkkien TE-attribuutit

MPLS verkossa Traffic Engineeringin asetettujen linkkien TE-attribuutit pitää jaella, jotta head-end LSR-laite pystyy arvioimaan mitkä linkeistä ovat käytettävissä kullekin TE-tunnelille.

Linkkien MPLS TE -attribuutit:

- Maksimi varattava kaista TE-tunneleille
- Attribuuttimääritykset
- TE metric -arvo (De Ghein 2007, 266)

Jokaiselle linkille määritetään TE-tunneleille varattava maksimi kaistaleveys suoraan linkkien porttirajapintoihin. Kaistavaraus tehdään kaikille TE-tunneleille samasta globaalista kaistamäärästä 1 – 4,294,967,295 kbps. (Osborne & Simha 2002, 374.) Tunneleiden toiminnan kannalta rajapintoihin tehtävät kaistaleveys määritykset ovat tärkeimmät ja vaikuttavat olennaisesti signalointiin reunalaitteiden välillä.

Linkeille voidaan konfiguroida attribuutti määrityksiä, joilla ilmenee linkin resurssivaatimukset suhteessa tunneliin. Lyhyesti esitettynä ne määrittävät, mitkä tunnelit voivat kulkea linkeistä, vertaamalla tunnelin ja linkin tietoja. Linkkien attribuuttimääritykset eivät ole tunnelien toimimisen kannalta välttämättömiä eikä niitä konfiguroitu työn toteutuksessa. (De Ghein 2007, 267.)

MPLS TE -tunneli voidaan määrittää käyttämään omaa TE metric -parametria. Ilman muutoksia TE-metric käyttää IGP:n cost arvoja linkeille. Head-end LSR-laitteessa voidaan tunneleille konfiguroida IGP cost arvojen sijaan TE metric arvot, mutta niitä voidaan myös käyttää samanaikaisesti paremman hallittavuuden saavuttamiseksi. (De Ghein 2007, 275.)

3.6 TE-tunnelin attribuutit

Linkkien lisäksi varsinaiset tunnelimääritykset tehdään erikseen jokaisen TE-tunnelin omaan rajapintaan (interface).

TE -tunneli määrityksiä ovat:

- Tunnelin päätepiste
- Haluttu kaista
- Setup- ja holding-prioriteetit
- Polkumääritykset
- Uudelleen optimointi (De Ghein 2007, 268)

TE-tunnelin päätepiste (tunnel destination) on tail-end laitteen Router ID (Osborne & Simha 2002, 107.). Jokaiselle luotavalle tunnelirajapinnalle määritetään kaistaleveys suoraan rajanpintoihin (Osborne & Simha 2002, 110.). TE-tunnelin kaistaleveyttä ei pidä sekoittaa linkkien TE-tunneleille varattuun kaistaleveyteen, jolla vaikutetaan signalointiin.

Toiset tunnelit ovat luonnollisesti tärkeämpiä verkon sisällä kuin toiset. Tästä syystä tunneleille voidaan määrittää kaksi eri prioriteetti määritystä (setup- ja holding- priority). (RFC 3209.)

Setup-prioriteetilla määritetään tunnelin prioriteetti yli muiden tunneleiden. Holding-prioriteetilla tunneli puolustaa itseään nähden muihin uusiin tunneleihin. Prioriteettitasoja on kahdeksan: 0 – 7. Nollatason prioriteetti on korkein. Tärkeille tunneleille on hyvä määrittää alhaiset setup-ja holding-prioriteetit, jotta ne voivat syrjäyttää muita tunneleita (alhainen setup-prioriteetti), eikä muut syrjäytä niitä (alhainen holding-prioriteetti). (Osborne & Simha 2002, 116)

Tunneli rajapinnoille (tunnel interface) voidaan määrittää 1 – 1000 väliltä polkumääritykset. Mitä pienempi arvo polkumääritykselle valitaan, sitä korkeammalla se on prioriteetissa, kun reunalaite laskee tunnelille reittiä. Korkeimman prioriteetin omaavaa tunnelia pyritään käyttämään ensisijaisesti. Seuraaviin polkumäärityksiin siirrytään, jos ensimmäinen vaihtoehto ei ole käytettävissä. Kaikkien vaihtoehtojen ollessa kelvottomia tunneli-rajapinta ei muutu aktiiviseksi. (De Ghein 2007, 269.)

MPLS Traffic Engineering tunneleita konfiguroitaessa pitää miettiä, miten tunneli halutaan asettaa MPLS-verkkoon (path setup option määritykset). Tunnelille voidaan määrittää käsin tietty reitti next-hop menetelmällä (explicit path) (Minei & Lucek 2005, 25.), tai reitti voidaan määrittää dynaamisesti pohjautuen täysin MPLS TE -tietokannan informaatioon. Dynaaminen polkumenetelmä huomioi automaattisesti verkkotopologian ja linkkien TE-määritykset. TE LSP -polun laskennan suorittaa PCALC-prosessi. (De Ghein 2007, 269.)

Suurissa verkoissa, joissa on useita TE-tunneleita yhtäjaksoisesti ja linkkien ylitse kulkeva liikennekuorma on suurta, syntyy tilanteita jolloin TE-tunnelin polku ei enää ole paras mahdollinen. Tämän kaltaisia tilanteita voi syntyä esimerkiksi jos kaatunut linkki nousee ylös ja tälle linkille ajautuu liikennettä, jota sinne ei kuulu ylittäen kaistakapasiteetin salliman rajan. TE-tunnelit käyttävät uudelleenoptimointitekniikkaa reitittääkseen tunnelit paremmalle polulle. On olemassa kolmea eri tyyppistä uudelleenoptimointitapaa: jaksollinen uudelleenoptimointi, tilannekohtainen uudelleenoptimointi ja manuaalinen uudelleenoptimointi. (RFC 4736)

3.7 PCALC

MPLS TE käyttää PCALC-algoritmia (SPF -algoritmi). SPF -algoritmi on OSPF:n käyttämä laskenta-algoritmi optimaalisimmalle reitille MPLS -verkossa. PCALC pystyy laskemaan polun tunneleille sekä lyhyimmän reitin (hop-by-hop), että linkkien

TE-vaatimusten perusteella. PCALC:n laskema reitti ei ole reititystaulu, vaan polku. PCALC laskee jokaiselle tunnelille yhden polun. Tästä johtuen verkkoa suunniteltaessa on tarkasti konfiguroitava linkeille sellaiset TE-määritykset, että niiden kautta kulkevien tunnelien määritykset vastaavat niitä. (De Ghein 2007, 279.)

3.8 RSVP

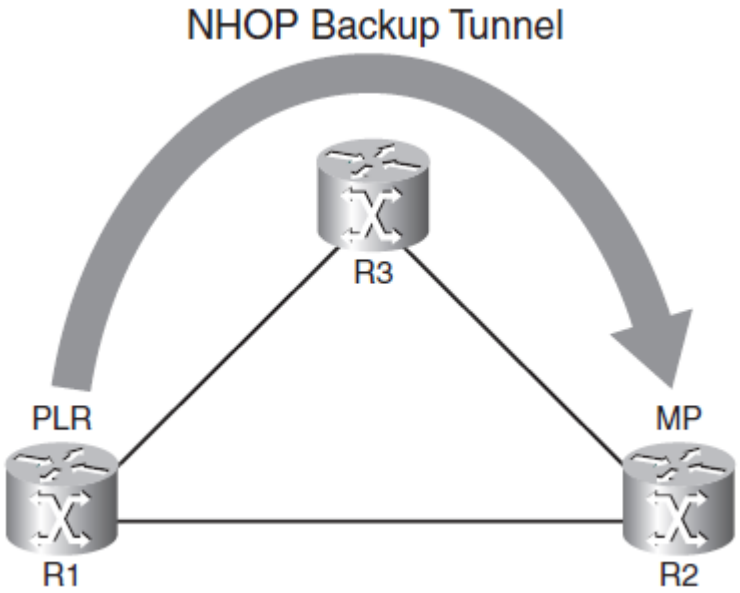
RSVP on MPLS TE:n käyttämä tunnelien signalointitekniikka. Signaloinnilla varmistetaan, että tunneli pysyy aktiivisena jatkuvasti. RSVP perustuu viestien keskusteluun, jotka kulkevat edestakaisin TE-tunnelissa head-end- ja tail-end LSR-laitteiden välillä. RSVP lähettää PATH-viestin tail-end laitteelle head-end laitteesta ja saa palautusviestin RESV. RSVP -viesteissä kulkee Explicit Route Object (ERO), runkolinkkien tiedot (IP RSVP - kaista) ja tunnelien omat spesifiset määritykset (prioriteetit). ERO on LSR -laitteiden fyysisten porttien IP-osoitteiden tietokanta. ERO:sta poistetaan aina yksi osoite jokaisen hypyn yhteydessä aina tail-end laitteelle asti. Tail-end palauttaa täsmälleen samaa reittiä RESV-viestin tunnelin alkupäähän. Jos paluuviesti vastaanotetaan ilman RSVP virheilmoituksia tunnelin signalointi onnistuu ja se muuttuu aktiiviseksi. (Minei & Lucek 2005, 49.)

3.9 FRR-tekniikka

Tietoverkoissa on niiden alkuajoilta lähtien aina ilmennyt eri tasoisia vikoja. Tästä johtuen on kehitetty monenlaisia tekniikoita ennaltaehkäisemään ja estämään viat. MPLS TE:n oma tekniikka suojata tunnelien liikenne on Fast Reroute (FRR) (Osborne & Simha 2002, 332.). Minkään tekniikan avulla ei pystytä täydellisesti estämään vikojen aiheuttamaa pakettihävikkiä, eikä verkon konvergoitumiseen kuluvaa aikaa saada kokonaan poistettua. FRR jakautuu kahteen alatekniikkaan, FRR-Link protection ja FRR-Node protection. FRR:n avulla kaatuneen MPLS TE tunnelin liikenne voidaan uudelleenohjata varalle luotuun MPLS TE -tunneliin kymmenissä millisekunneissa (<50ms). (Osborne & Simha 2002, 333.)

FRR-tekniikalla tietty MPLS TE -tunnelien käytössä oleva linkki suojataan luomalla varatunneli siitä laitteesta eteenpäin, jossa suojattava linkki sijaitsee. Se mahdollistaa

myös sen, että kaikki MPLS TE -tunnelit, jotka kulkevat kyseisen suojatun linkin kautta ovat suojattuna saman varatunnelin avulla.



Kuva 9. FRR varatunneli linkille R1-R2 (De Ghein 2007, 292.)

Kuvasta 9 nähdään FRR varatunnelin idea. Linkki R1-R2 on suojattu NHOP- varatunnelilla (Next-hop backup tunnel), joka kulkee reittiä R1-R3-R2. Koska MPLS TE -tunnelit ovat yksisuuntaisia täytyy varatunneli luoda myös reitille R2-R3-R1 paluuliikennettä varten. Varatunnelia signaloidaan RSVP -protokollalla täysin samaan tapaan kuin muitakin MPLS TE -tunneleita. FRR-varatunneli on aina next-hop täsmäreitti (explicit path). (De Ghein 2007, 292.) (Varatunnelin konfigurointi tarkemmin työn kappaleessa 5. Tekninen toteutus)

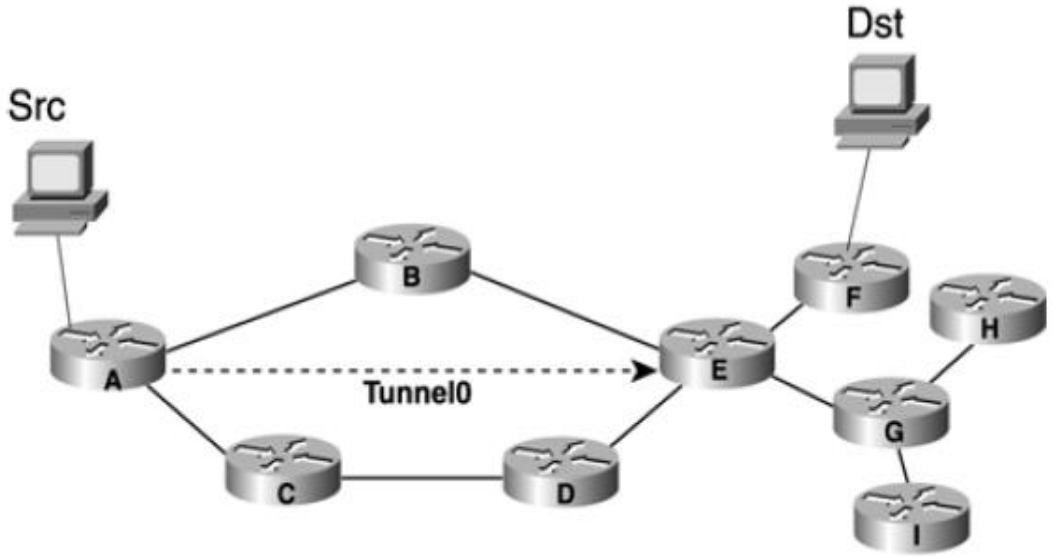
3.10 Liikenteen ohjaus MPLS TE -tunneliin

MPLS TE -tekniikan tärkein osa-alue on liikenteen ohjaus tunneleihin. MPLS TE -tekniikan yleisimmät keinot reitittää haluttua liikennettä tunneleihin ovat staattinen reititys, Policy-based-reititys (PBR) ja Autoroute announce.

Staattinen reititys on helpoin ja selkein keino. Staattinen reititys toimii MPLS TE -tekniikassa täysin samalla tavalla kuin missä tahansa muussa yhteydessä. Staattisen reitityksen määritykset tehdään globaalissa konfigurointitilassa komennolla **ip route**

10.1.0.0 255.255.0.0 tunnel 1. Tässä esimerkissä verkon 10.1.0.0 liikenne ohjataan tunneliin tunnel 1. (Osborne & Simha 2002, 238.)

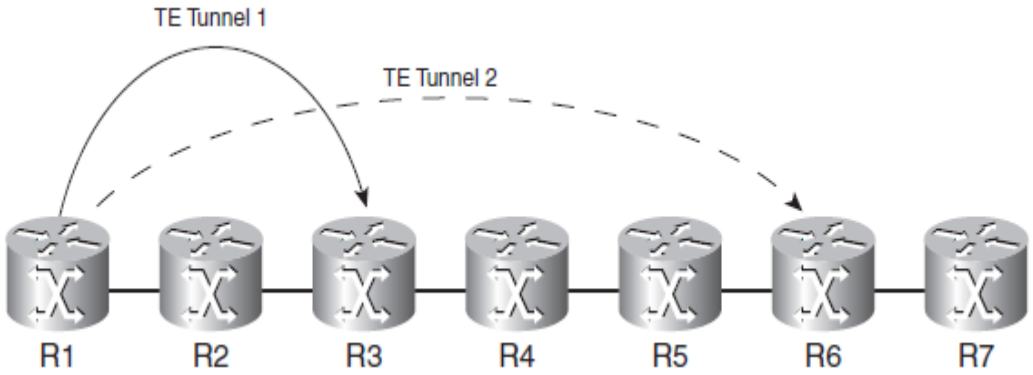
PBR-tekniikalla reititetään käyttämällä route-map-objekteja, jotka määritetään sisääntuloportteihin. Route-map-objekteihin voidaan rajata tietyn tyyppinen liikenne esimerkiksi VoIP-ääniliikenne erilleen muusta verkon tietoliikenteestä. PBR-tekniikka on erittäin hyödyllinen tilanteissa, joissa halutaan rajata ääniliikenne, joka saapuu reitittimelle ja kulkee MPLS-verkon läpi TE-tunnelia pitkin.



Kuva 10. Äänidata SRC→DsT, tunnelin 0 läpi PBR-tekniikalla (Osborne & Simha 2002, 239.)

Src-laitteelta saapuu verkkoon VoIP-paketteja, jotka halutaan ohjata tunneliin 0. Ensin luodaan pääsylista, joka määritetään sallimaan liikenne verkon VoIP-pakettien gateway-osoitteelle x.x.x.x. Pääsylistan luonnin jälkeen luodaan route-map-objekti johon määritetään luotu pääsylista, ja sille kuuluva tunnelirajapinta. Viimeisenä määritetään sisääntulevaan fyysiseen rajanpintaan laitteella A route-map-objekti aktiiviseksi. (Osborne & Simha 2002, 239.)

Autoroute announce-tekniikka mahdollistaa tunnelien lisäyksen perinteisen reititystaulun käyttöön. Autoroute announce muokkaa SPF -algoritmia niin, että LSR -laite lisää IP-prefixejä tunnelin head-end-laitteen reititystauluun. Tunnelin tail-end-laite ja sen jälkeiset fyysiset laitteet kuuluvat kullekin tunneleille next-hop-osoitteina.



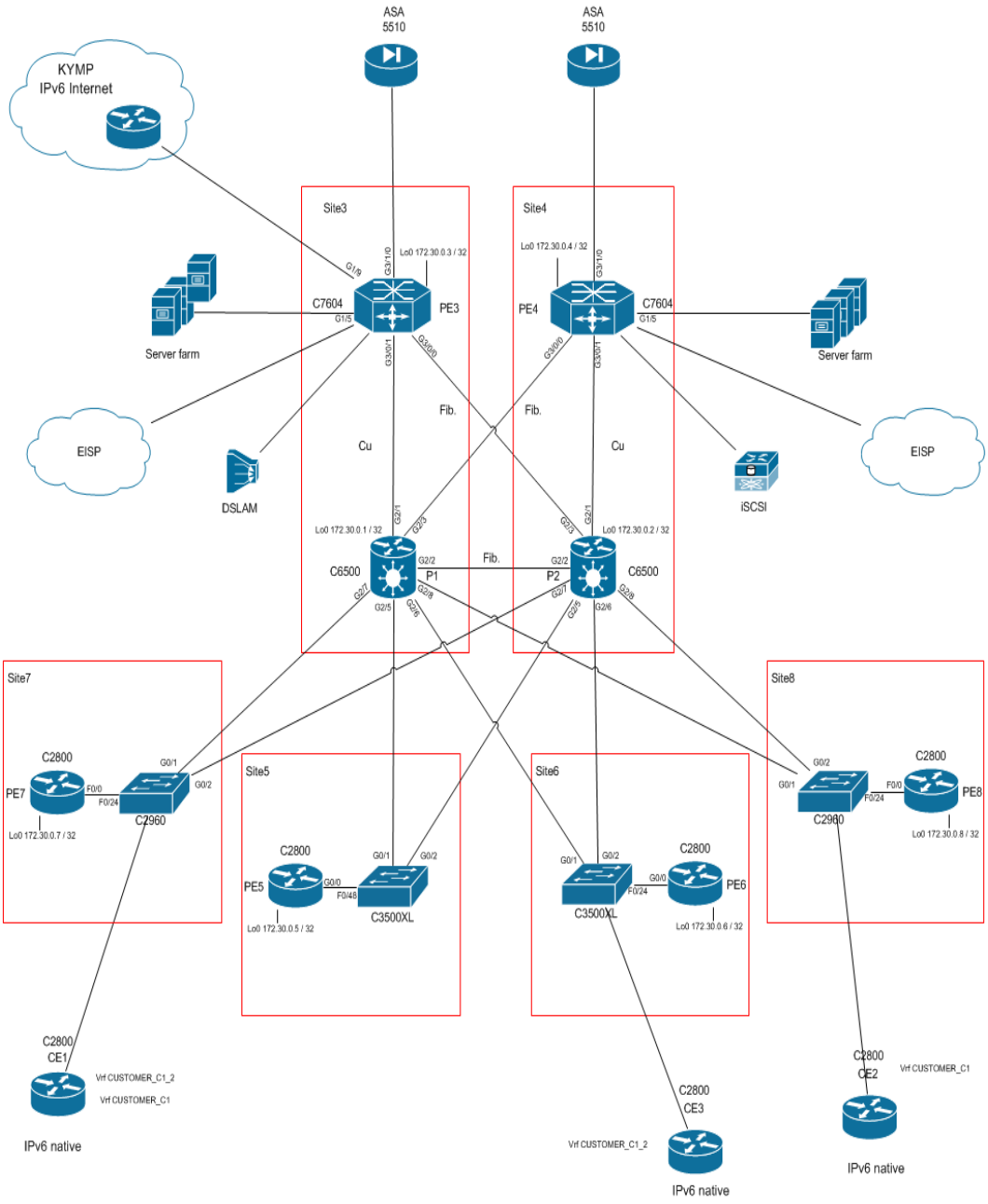
Kuva 11. Autoroute announce kahdella eri TE-tunnelilla. (De Ghein 2007, 306.)

IP-prefixit, jotka kuuluvat laitteille R3, R4 ja R5 käyttävät tunnelia 1 next-hop:na. Laitteiden R6 ja R7 IP-prefixit käyttävät tunnelia 2. Laitteen R1 reititystaulu ylläpitää tietoja molemmista tunneleista. (De Ghein 2007, 306.)

4 SIMUNET

Simunet on EAKR-rahoitettu vuonna 2009 aloitettu hanke. Hankkeen myötä Kymenlaakson ammattikorkeakoulun ICT-laboratorioon perustettiin SimuNet-verkko. Simunet on Kymenlaakson ammattikorkeakoulun ja Kaakkois-Suomen verkko-ja palveluoperaattoreiden yhteistyönä aikaansaatu kokonaisuus (Kettunen 2009, 1). SimuNet toimii testausalustana työn tekniselle toteutukselle.

Simunet on testausverkko, joka simuloi operaattoriverkkoa mahdollisimman tarkasti. Ympäristö tarjoaa opiskelijoille hyvän työvälineen tutustua lähemmin operaattoritasoiseen verkkoratkaisuun. SimuNet-verkkoa käytetään paljon opiskelijoiden opinnäytetöissä sekä suuremmissa projekteissa. SimuNet-verkko elää jatkuvasti opiskelijoiden tekemien projektien avulla. Paikallinen verkko-operaattori hyödyntää SimuNet-verkkoa tilanteissa, joissa pitää tehdä suurempia muutoksia palveluissa käytettyihin verkkoihin. SimuNet minimoi kriittisten virheiden määrää ja palvelee operaattoria turvallisena testialustana. (Oinonen 2011, 21)



Kuva 12. SimuNet-verkon fyysinen topologia (Tuntematon 2012). Liitteenä kuva alkuperäisessä koossa.

Työni kannalta olennaisia, fyysistä topologiaa tarkasteltaessa, ovat laitetilat Site3 ja Site4. Työni runkoverkko muodostuu kahdesta PE -laitteesta (PE3 & PE4) ja kahdesta P-laitteesta (P1 & P2). Verkon IGP -protokollana toimii OSPF.

Työssä käytetyt laitteet ovat Cisco Systemsin. PE3 ja PE4-reunalaitteet ovat Cisco 7600 -sarjan reitittimiä. P1 ja P2-laitteet ovat Cisco Catalyst 6000 -sarjan runkokytkimiä.

Kuva 13. SimuNet-verkon fyysinen topologia (Tuntematon 2012). Liitteenä kuva alkuperäisessä koossa.

5 KÄYTÄNNÖN KONFIGUROINTIKÄSKYT

SimuNet-ympäristön MPLS-runkoverkko käyttää Cisco Systemin laitteita, joten huolellinen perehtyminen Cisco IOS spesifisiin Traffic Engineering käskyihin oli tarpeellista. Tässä kappaleessa esittelen tarkasti teknisessä toteutuksessa sovellettuja Cisco-käskyjä.

5.1 Runkolaitteiden tunnelikonfigurointi

Laitteisiin, joiden kautta TE-tunnelit kulkevat täytyy määrittää globaalisti TE-ominaisuus käyttöön. Globaali TE-määritys asetetaan globaalissa konfigurointitilassa komennolla **mpls traffic-eng tunnels**. Globaalin määritettelyn jälkeen laite asettaa itsensä aktiiviseksi TE-ominaisuuksille. Tämä käsky voidaan asettaa viimeisenä, jos halutaan rauhassa totetuttaa konfigurointi ja nostaa tunnelirajapinnat ylös myöhemmin. (De Ghein 2007, 259)

Seuraavana asiana on tärkeää selvittää tarkasti kaikki portit, joiden kautta tunnelit kulkevat ja määrittää niihin linkkikohtaiset TE-määritykset. Tärkein näistä on TE-liikenteelle varatun kaistan määritys linkeissä. TE-tunnelien kaistanvaraus määritetään komennolla **ip rsvp bandwidth** *interface-kbps*. Määritykset tehdään suoraan laitteiden porttirajapintoihin. Porttirajapintoihin määritetään myös komento **mpls traffic-eng tunnel** RSVP-signaloinnin aktivoimiseksi. (De Ghein 2007, 256)

Jotta MPLS TE -informaatio saadaan jaettua MPLS-verkossa tulee reititysprotokollaan tehdä myös TE-määritykset. Cisco IOS:ssa OSPF-määritykset tehdään suoraan OSFP asetuksiin. Tärkeimmät komennot ovat **mpls traffic-eng router-id**, jolla määritetään konfiguroitavan laitteen tunniste-osoite ja **mpls traffic-eng area []**, jolla TE sidotaan verkossa käytettyyn autonomiseen alueeseen. Komennoilla **show ip ospf** ja **show ip ospf database** voidaan tarkistaa, että MPLS TE on aktivoitu OSPF-alueelle. (Osborne & Simha 2002, 130)

TE-tunnelit luodaan suoraan globaalissa konfigurointitilassa komennolla **interface tunnel** *1-1000.* Tunnelien rajapintoihin määritetään jokaiselle tunnelille ominaiset

määritykset. Tunnelin signalointi IP-osoite määritetään komennolla **ip unnumbered Looback<**loopback-rajapinnan arvo> (Osborne & Simha 2002, 155). Tunneli täytyy myös aktivoida TE-tunneliksi komennolla **tunnel mode mpls traffic-eng** (Osborne & Simha 2002, 155). TE-tunnelin kohdeosoitteeksi määriteään aina verkon toisella reunalla sijaitsevan reunalaitteen Loopback-rajapinnan osoite. Tunnelin kohdeosoite määritetään komennolla **tunnel destination** <ip –osoite> (Osborne & Simha 2002, 155). Tunnelikohtainen setup- ja holding-prioriteetti määritetään rajapintaan komennolla **tunnel mpls traffic –eng priority** *setup-priority [hold-priority]* (Osborne & Simha 2002, 116). TE-tunnelirajapintoihin määritetään lisäksi vielä tunnelin kaistaleveys, polun tyyppi ja tarvittaessa Fast Reroute -ominaisuus. Kaistaleveys asetetaan käskyllä **tunnel mpls traffic-eng bandwidth** *kpbs* (Osborne & Simha 2002, 255). Polkumääritykset tehdään täsmäreitille kommenolla **tunnel mpls traffic-eng path-option <**prioriteettilukuarvo> **explicit name <**täsmäpolun nimi> ja dynaamiselle tunnelille komennolla **tunnel mpls traffic-eng path-option** <prioriteettilukuarvo> **dynamic.** Täsmäreitille pitää luoda myös erikseen määritetty polku, jossa fyysisten linkkien osoitteet määritetään. Tämä tehdään globaalissa config-tilassa komennolla **ip explicit-path name <**täsmäpolun nimi> **enable**, jonka jälkeen voidaan lisätä osoitteita **next-address**-komennolla tai välttää osoitteita **exclude-address**-komennolla. (De Ghein 2007, 273.)

5.2 Fast Reroute -konfigurointi

Työssä käytetittiin Fast Reroute -tekniikkaa konvergoitumisajan minimoimista varten. Fast Reroute -määritykset tehdään reunalaitteella (head-end) siihen porttirajapintaan, josta päätunneli lähtee sekä suojattavan tunnelin tunnelirajapintaan. Tunnelin rajapintaan, jota suojataan määritetään komento **tunnel mpls traffic-eng fast-reroute**. Sen portin rajapintaan, josta suojattava tunneli lähtee muualle verkkoon määritetään komento **mpls traffic-eng backup-path** *Tunnel<1-1000>*. Tämä kertoo suojattavalle tunnelille mihin kohdentaa liikenteen kun se havaitsee vian nykyisessä reitissä. (De Ghein 2007, 295)

6 TEKNINEN TOTEUTUS

Ensisijaisena tavoitteena oli oppia ymmärtämään MPLS- ja MPLS TE -tekniikoita teoriatasolla Cisco IOS -ympäristössä ja muodostaa yksinkertainen MPLS TE -tunnelointi. SimuNet-runkoverkkoon luotiin kaksi MPLS TE -tunnelia PE3-ja PE4-laitteiden välille. Toinen tunneleista toimii päätunnelina ja toinen varatunnelina. Työssä käytettiin myös kahta Linux-pohjaista virtuaalikonetta (asiakaskoneet) MPLS-verkon molemmilla reunoilla. Tunneliin kuljetettava liikenne saapuu verkkoon toisesta virtuaalikoneesta, jota kuljetetaan toiselle virtuaalikoneelle MPLS TE -tunnelia pitkin.

6.1 Alkutilanne

Ennen tunnelien konfiguroimista luotiin kaksi kuviteltua asiakaskonetta runkoverkon ulkopuolelle MPLS-verkon molemmille reunoille. Asiakaskoneina käytettiin ICT-laboratorion kahta eri työpistettä, joihin luotiin virtuaalikoneet. Virtuaalikoneisiin asennettiin Linux Mint -käyttöjärjestelmät. Koneet määritettiin molemmat omiin aliverkkoihinsa ja kytkettiin kiinni SimuNet-verkon laitteisiin PE3 ja PE4. Koneet pystyttiin liittämään helposti ICT-laboratorion etähallintaporttien kautta.

PE3-laitteeseen kytketty asiakaskone määritettiin käyttämään aliverkkoa 192.168.123.1/24 ja PE4-laitteeseen kytketty verkkoa 192.168.124.1/24. Määritykset tehtiin PE-laitteille GigabitEthernet 3/1/3-portteihin. PE-laittesiin tehtiin seuraavat konfiguraatiot:

PE3(conf)#interface GigabitEthernet3/1/3
PE3(conf-if)#ip address 192.168.123.1 255.255.255.0

PE4(conf)#interface GigabitEthernet3/1/3
PE4(conf-if)#ip address 192.168.124.1 255.255.255.0

Virtuaalikoneiden verkkoasetuket määritettiin taulukon 1 mukaisesti.

Taulukko 1. Virtuaalikoneiden IP-osoitteet.

Virtuaalikone	Asiakaskone 1	Asiakaskone 2

IP-osoite (IPv4)	192.168.123.10	192.168.124.10
Aliverkon peite (IPv4)	255.255.255.0	255.255.255.0
Oletusyhdyskäytävä (IPv4)	192.168.123.1	192.168.124.1

6.2 Tunnelien muodostus

Aluksi PE3, PE4, P1 ja P2 laitteisiin määritettiin globaalisti aktiiviseksi MPLS TE. Muita globaaleja määrityksiä ei tarvinnut tehdä sillä SimuNet-verkko itsessään on täysin valmis IP/MPLS-verkko. Jokaiseen laitteeseen konfiguroitiin seuraava komento:

PE3(conf)#mpls traffic-eng tunnels.

Globaalin MPLS TE -ominaisuuden asetuksen jälkeen luotiin tunnelirajapinnat tunnel 158 ja tunnel 159. Tunneli 158 konfiguroitiin kulkemaan polkua PE3-P1-PE4 ja tunneli 159 reittiä PE3-P2-PE4. Tunnelirajapinnat luotiin molempiin laitteisiin samalla tavalla mutta eri suuntiin. Tunnelit luotiin molempiin suuntiin, koska MPLS TE -tunnelit ovat yksisuuntaisia. Tunnelimääritykset tehtiin laitteisiin PE3 ja PE4, koska ne toimivat tunnelien head-end ja tail-end –laitteina. Seuraavat komennot määritettiin (esitettynä vain PE3-laitteen konfiguraatio. Tarkat konfiguraatiot löytyvät liitteinä):

PE3(conf)#interface tunnel 158
PE3(conf)#interface tunnel 159

Molempiin tunnelirajapintoihin määritettiin tunnelin IP-osoitteeksi (IP Unnumbered) laitteen Loopback0 osoite (MPLS TE Router-ID). Tunneli tulee myös määrittää MPLS TE -tunneliksi ja määrittää sille kohdeosoite. Kohdeosoite on tail-end-laitteen Loopback-osoite (Cisco Systems 2005a). Seuraavat MPLS TE -tunnelille spesifiset määritykset asetettiin rajapintoihin: prioriteetti, tunnelin kaistaleveys ja täsmäreitin polkumääritys. Seuraavat komennot määritettiin PE3-laitteeseen:

PE3(conf)#interface tunnel 158

PE3(conf-if)#ip unnumbered Loopback0
PE3(conf-if)#tunnel mode mpls traffic-eng
PE3(conf-if)#tunnel destination 172.30.0.4
PE3(conf-if)#tunnel mpls traffic-eng priority 1 1
PE3(conf-if)#tunnel mpls traffic-eng bandwidth 3500
PE3(conf-if)#tunnel mpls traffic-eng path-option 1 explicit name mainpath

PE3(conf)#interface tunnel 159
PE3(conf-if)#ip unnumbered Loopback0
PE3(conf-if)#tunnel mode mpls traffic-eng
PE3(conf-if)#tunnel destination 172.30.0.4
PE3(conf-if)#tunnel mpls traffic-eng priority 2 2
PE3(conf-if)#tunnel mpls traffic-eng bandwidth 3500
PE3(conf-if)#tunnel mpls traffic-eng path-option 1 explicit name secpath

Tunneli 158:lle asetettiin setup-ja holding-prioriteeteiksi arvot yksi (1), koska kyseinen tunneli on pääreitti eikä toinen tunneli saa syrjäyttää sitä verkon toimiessa normaalisti. Täsmäreitin määritykset luodaan erikseen globaalissa config tilassa jokaiselle polulle erikseen. PE3-laitteeseen tehtiin täsmäreittikonfiguraatio seuraavasti:

PE3(conf)#ip explicit path name mainpath enable
PE3(cfg-ip-expl-path)#next-address 192.168.13.3
PE3(cfg-ip-expl-path)#next-address 192.168.13.1
PE3(cfg-ip-expl-path)#next-address 192.168.14.1
PE3(cfg-ip-expl-path)#next-address 192.168.14.4
PE3(cfg-ip-expl-path)#next-address 172.30.0.4

PE3(conf)#ip explicit path name secpath enable
PE3(cfg-ip-expl-path)#next-address 192.168.23.3
PE3(cfg-ip-expl-path)#next-address 192.168.24.2
PE3(cfg-ip-expl-path)#next-address 192.168.23.2
PE3(cfg-ip-expl-path)#next-address 192.168.24.4
PE3(cfg-ip-expl-path)#next-address 172.30.0.4

Varsinaisten tunnelien määrittämisen jälkeen, jokaiseen porttiin, jonka kautta TE-tunnelit kulkevat määritetään asetukset signalointia varten. Niihin portteihin, jotka ovat tunnelin 158 varrella määritettiin suurempi **ip rsvp bandwidth** arvo, jotta kyseistä tunnelia signaloidaan ensisijaisesti. Jokainen portti määritettiin myös käyttämään MPLS TE:tä. Seuraavat komennot määritettiin laitteeseen PE3:

PE3(conf)#interface GigabitEthernet3/0/1
PE3(conf-if)#mpls traffic-eng tunnels
PE3(conf-if)#ip rsvp bandwidth 4000

PE3(conf)#interface GigabitEthernet3/0/0
PE(conf-if)#mpls traffic-eng tunnels
PE3(conf-if)#ip rsvp bandwidth 3900

Jotta IGP-protokolla OSPF pystyy jakamaan MPLS TE -informaatiota verkossa PE-laitteisiin, tehtiin muutoksia OSPF-konfiguraatioon. Reititin määritetään IGP-protokollan käyttöön Loopback-osoitteen avulla. Reititysprotokollan käyttämä autonomisen alueen määritys tulee myös konfiguroida TE:n käyttöön. Seuraavat komennot määritettiin:

PE3(conf)#router ospf 1
PE3(conf-router)#mpls traffic-eng router-id Loopback0
PE3(conf-router)#mpls traffic-eng area 0

P1 ja P2 laitteisiin tehtiin myös konfiguraatiot sen mukaan, miten tunnelit kulkevat niiden kautta. Konfiguraatiot ovat identtisiä PE3-laitteen porttikonfiguraatioiden kanssa. Tunnelien määritysten jälkeen tarkistettiin, että tunnelit ovat toimivassa tilassa. Tunnelin toimintoja ja tilaa voi tarkastella komennolla **show mpls traffic-eng tunnels tunnel**<tunnelirajapinnan numero>.

```
Name: PE3_t158                          (Tunnel158) Destination: 172.30.0.4
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit mainpath (Basis for Setup, path weight 20)

  Config Parameters:
    Bandwidth: 3500     kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: disabled LockDown: disabled Loadshare: 3500 [571428] bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
```

Kuva 14. Tunnelin 158 status.

```
Name: PE3_t159                          (Tunnel159) Destination: 172.30.0.4
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit secpath (Basis for Setup, path weight 11)

  Config Parameters:
    Bandwidth: 3500     kbps (Global)  Priority: 2  2   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: disabled LockDown: disabled Loadshare: 3500 [571428] bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
```

Kuva 15. Tunnelin 159 status.

Tulosteista voi nähdä, että molemmat tunnelit ovat toimivassa tilassa. Tämän jälkeen PE3 ja PE4 laitteille määritettiin **ip route** -komennolla staattinen reitti molempiin tunneleihin aliverkkojen 192.168.123.0 ja 192.168.124.10 liikenteelle. PE3-ja PE4-laitteille asetettiin seuraavat komennot:

PE3(conf)#ip route 192.168.124.0 255.255.255.0 Tunnel158
PE3(conf)#ip route 192.168.124.0 255.255.255.0 Tunnel159

PE4(conf)#ip route 192.168.123.0 255.255.255.0 Tunnel158
PE4(conf)#ip route 192.168.123.0 255.255.255.0 Tunnel159

Staattisten reittien avulla liikenteen ohjaus MPLS TE -tunneleihin on helppoa ja suoraviivaista. Työn kannalta selkein ratkaisu oli käyttää **ip route** -komentoa tätä toimenpidettä varten.

6.3 Tunnelien testaus

Testauksessa haluttiin selvittää, vaihtuuko liikenne tunnelista 158 tunneliin 159, jos tärkeämmän tunnelin varrella oleva reitti katkeaa. Uudelleenreititykseen kuluva aika haluttiin myös selvittää. Konvergoitumisaika mittaus suoritettiin linuxin ping -komennon laajennuksilla –i (interval time) ja –f (flood). Tunnelin liikenteen siirtyminen testattiin asettamalla PE3-laitteen GigabitEthernet3/0/1 shutdown-tilaan, joka myös sulkee tunnelin 158. PE3 -laitteeseen kytketyltä asiakaskoneelta varmistettiin uudelleenreitityksen onnistuminen traceroute-komennolla.

```
toppi2 Desktop # tracepath 192.168.124.10
 1:  toppi2.local                                          1.635ms pmtu 1500
 1:  192.168.123.1                                         1.463ms
 1:  192.168.123.1                                         1.603ms
 2:  192.168.23.2                                          2.190ms asymm  5
 3:  192.168.24.4                                          2.245ms
 4:  192.168.124.10                                        1.427ms reached
     Resume: pmtu 1500 hops 4 back 61
toppi2 Desktop #
```

Kuva 16. Traceroute PE3:n kytkekyltä asiaskaskoneelta osoitteeseen 192.168.124.10 (PE4:n kytketty asiakaskone)

Tulosteesta nähtiin, että liikenne on vaihtunut tunneliin 159 vian ilmetessä pääreitille. Seuraavaksi haluttiin testata kuinka pitkä aika menee liikenteen uudelleenreititykseen. PE3:n kytketyltä asiakaskoneelta testattiin ping –f –i komennolla osoitetta 192.168.124.10 osoitetta yhden sekunnin intervalli-ajalla.

```
toppi2 Desktop # ping -f -i 1 192.168.124.10
PING 192.168.124.10 (192.168.124.10) 56(84) bytes of data.
...........^C
--- 192.168.124.10 ping statistics ---
39 packets transmitted, 28 received, 28% packet loss, time 38481ms
rtt min/avg/max/mdev = 1.207/1.668/2.159/0.257 ms, ipg/ewma 1012.677/1.682 ms
```

Kuva 17. Konvergoitumisajan Ping-testi

Kuvasta 16 nähdään, että konvergoitumiseen kulunut aika on liian pitkä, liki 10 sekuntia. Konvergoitumisajan parantamiseksi otettiin käyttöön MPLS TE Fast Reroute -tekniikka. Fast Reroutea käytetään suojaamaan pääreittiä määrittämällä varareitti, joka toimii backup-tunnelina. Fast Reroute -tekniikalla konvergoitumisaika voi pienentyä jopa 50 ms:n tasolle. PE3 laitteisiin määritettiin seuraavat komennot:

PE3(conf)#interface tunnel 158
PE3(conf-inf)#tunnel mpls traffic-eng fast-reroute

PE3(conf)#interface GigabitEthernet3/0/1
PE3(conf-inf)#mpls traffic-eng backup-path Tunnel159

Kun Fast Reroute oli määritetty suojaamaan tunnelia 158 varatunnelin 159 avulla, tarkastettiin tekniikan toimivuus komennolla **show mpls traffic-eng fast-reroute database detail** PE3-laitteesta. Tuloste kertoo, että backup-tunneli on luotu ja käyttää tunnelia 159 varareittinä.

```
PE3#sh mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Protected interfaces    : 1
  Protected LSPs/Sub-LSPs : 1
  Backup tunnels          : 1
  Active interfaces       : 0

P2P LSPs:

 Tun ID: 158, LSP ID: 441, Source: 172.30.0.3
 Destination: 172.30.0.4
  State         : Ready
  InLabel       : Tunnel Head
  OutLabel      : Gi3/0/1:41
  FRR OutLabel  : Tu159:implicit-null
```

Kuva 18. Fast Reroute:n toiminnallisuus

Tämän jälkeen suoritettiin vielä Ping-testi PE3:n kytketyltä asiakaskoneelta Fast Reroute -tekniikan toimivuuden testaamiseksi.

```
toppi2 Desktop # ping -f -i 0.1 192.168.124.10
PING 192.168.124.10 (192.168.124.10) 56(84) bytes of data.
...........^C
--- 192.168.124.10 ping statistics ---
155 packets transmitted, 144 received, 7% packet loss, time 15843ms
rtt min/avg/max/mdev = 0.881/1.522/3.349/0.384 ms, ipg/ewma 102.879/1.625 ms
```

Kuva 19. Konvergoitumisajan Ping-testi Fast Rerouten ollessa käytössä.

Kyseinen testaus suoritettiin PE3:n kytketyltä koneelta Ping –f –i –komenolla osoitteeseen 192.168.124.10 0,1 sekunnin intervalli-ajalla. Kuvasta 18 voidaan huomata, että konvergoitumisaika on parantunut huomattavasti edellisestä. Tämän hetkinen aika on 0,1 sekunnin intervallilla n. 1000ms.

7 YHTEENVETO

Tämän opinnäytetyön tärkeimpänä päämääränä oli oppia ymmärtämään MPLS Traffic Engineering -tekniikka teoriatasolla ja toteuttaa MPLS TE -tunnelointiharjoitus SimuNet-verkossa. Työn alkuvaiheessa MPLS TE -tekniikkaan tutustuttiin rakentamalla MPLS-verkko ja TE-tunnelointi ICT-laboratorion laitteilla. ICT-laboratorion harjoitteluvaiheen jälkeen tunnelikonfiguraatiot implementoitiin SimuNet-tuotantoverkkoon. Tunnelikonfiguraation pohjustukseksi teoria piti sisäistää hyvin. Täysin toivottuun lopputulokseen ei päästy konvergoitumisajan suhteen, mutta työssä esitetään täysin toimiva päätunneli-varatunneli, joka jättää mahdollisuuksia jatkokehitykselle.

Opinnäytetyö perehdytti MPLS Traffic Engineering -tekniikkaan ja opetti ymmärtämään sen toimintaa ja siitä saatavaa hyötyä MPLS-runkoverkoissa. Tekniikan todellista hyötyä ei pääsee esittämään kunnolla pienissä verkoissa ilman riittävän suuria tietoliikennekuormia linkeille. Tekniikan optimaalinen toiminta vaatii huolellisen suunnittelun suurissa verkoissa, joissa voidaan saavuttaa merkittävää hyötyä kaistankuormien tasapainoituksesta. Työssä päädyttiin testaamaan tunnelikonfiguraatiota SimuNet:n MPLS-verkon läpi ja konvergoitumisaikaa, joka kuluu pakettien uudelleenreititykseen päätunnelista varatunneliin.

Tunneloinnin toteutus sujui perusteellisen teorian opiskelun avulla hyvin. Ainoa merkittävä ongelma ilmeni varatunnelien signaloinnissa, jota ei aluksi saatu kunnolla toimimaan. Asia kuitenkin ratkesi muuttamalla head-end-reitittimestä varatunnelin käyttämän GigabitEthernet3/0/0-portin ip rsvp bandwidth -arvoa. Toinen huomioitava asia oli konvergoitumisaika tunnelien välillä. Tässä opinnäytetyössä ei ehditty perehtymään niihin seikkoihin, joilla konvergoitumisaika olisi saatu minimoitua viidenkymmenen millisekunnin tasolle.

Työn totetuksen tuloksena oli SimuNet-verkkoon konfiguroitu tunneliratkaisu IP/MPLS-pilven lävitse. Tunneleihin ohjattiin liikenne runkoverkon ulkopuolelta ja kuljetettiin se päätunnelia pitkin verkon toisella reunalle ja sieltä ulos. Päätunneli suojattiin varatunnelilla käyttäen MPLS TE:lle ominaista Fast Reroute -reititystekniikkaa siltä varalta, että päätunnelin reitti katkeaa jostain syystä.

Jatkokehityksenä konvergoitumisajan optimointiin tulisi perehtyä. Näitä asioita ovat esimerkiksi Dual TE Metrics (De Ghein 2007, 275) ja RSVP Hello State timer (RFC

3209). Uskon, että konvergoitumisen optimointi tarjoaa uuden projektin tai mahdollisesti jopa aiheen opinnäytetyöhön.

LÄHTEET

Alvarez S. 2012. Deploying MPLS Traffic Engineering. Lontoo 2012. Cisco Systems. Cisco Live 2012 tapahtuman kalvosarja.

Cisco Systems. 2005a. MPLS Basic Traffic Engineering Using OSPF. Manuaali. Saatavissa: http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fd0.shtml[viitattu 15.3.2013]

Cisco Systems. 2005b. OSPF Design guide, OSPF Cost. Manuaali. Saatavissa: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml#t6 [viitattu 19.3.2013]

Configuring Basic MPLS TE tunnels. 2009. Blogi. Saatavissa: http://www.networking-forum.com/blog/?p=145. [viitattu 15.3.2013]

De Ghein L. 2007. MPLS Fundamentals. Indianapolis: Cisco Press.

Juniper Networks. Explicit Route Objects. Verkkojulkaisu. Saatavissa: http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-interfaces-and-routing/explicit-route-objects.html[viitattu 19.3.2013]

Kettunen M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana, Tutkimusjulkaisu 2010, Kymenlaakson ammattikorkeakoulun julkaisuja, Sarja B. Saatavissa: http://papaya.tlt.kyamk.fi/~amake/SimuNet/SimuNet%20artikkeliv6a.pdf [viitattu 15.3.2013]

Minei I, Lucek J. 2005. MPLS-Enabled Applications. West Sussex: John Wiley & Sons, Ltd.

Oinonen R. 2011. MPLS L2VPN ja operaattoriverkon kahdennetut palvelut. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Osborne E, Simha A.2002. Traffic Engineering with MPLS. Indianapolis: Cisco Press.

Rakotoranto H. 2011. Introduction to MPLS. Las Vegas 2011. Cisco Systems. Cisco Live 2011 tapahtuman kalvosarja.

RFC 2370, The OSPF Opaque LSA Option. IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc2370.txt [viitattu 19.3.2013]

RFC 3031, Multiprotocol Label Switching Architecture. IETF. Saatavissa: http://www.ietf.org/rfc/rfc3031.txt [viitattu 19.3.2013].

RFC 3032, MPLS Label Stack Encoding. IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc3032.txt [viitattu 19.3.2013].

RFC 3209. RSVP-TE: Extensions to RSVP for LSP Tunnels. IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc3209.txt [viitattu 19.3.2013].

RFC 3630. Traffic Engineering (TE) Extensions to OSPF Version 2. IETF. Saatavissa: http://tools.ietf.org/rfc/rfc3630.txt [viitattu 19.3.2013].

RFC 3906, Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels. IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc3906.txt [viitattu 19.3.2013].

RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks. IETF. Saatavissa: http://tools.ietf.org/html/rfc4448 [viitattu 19.3.2013].

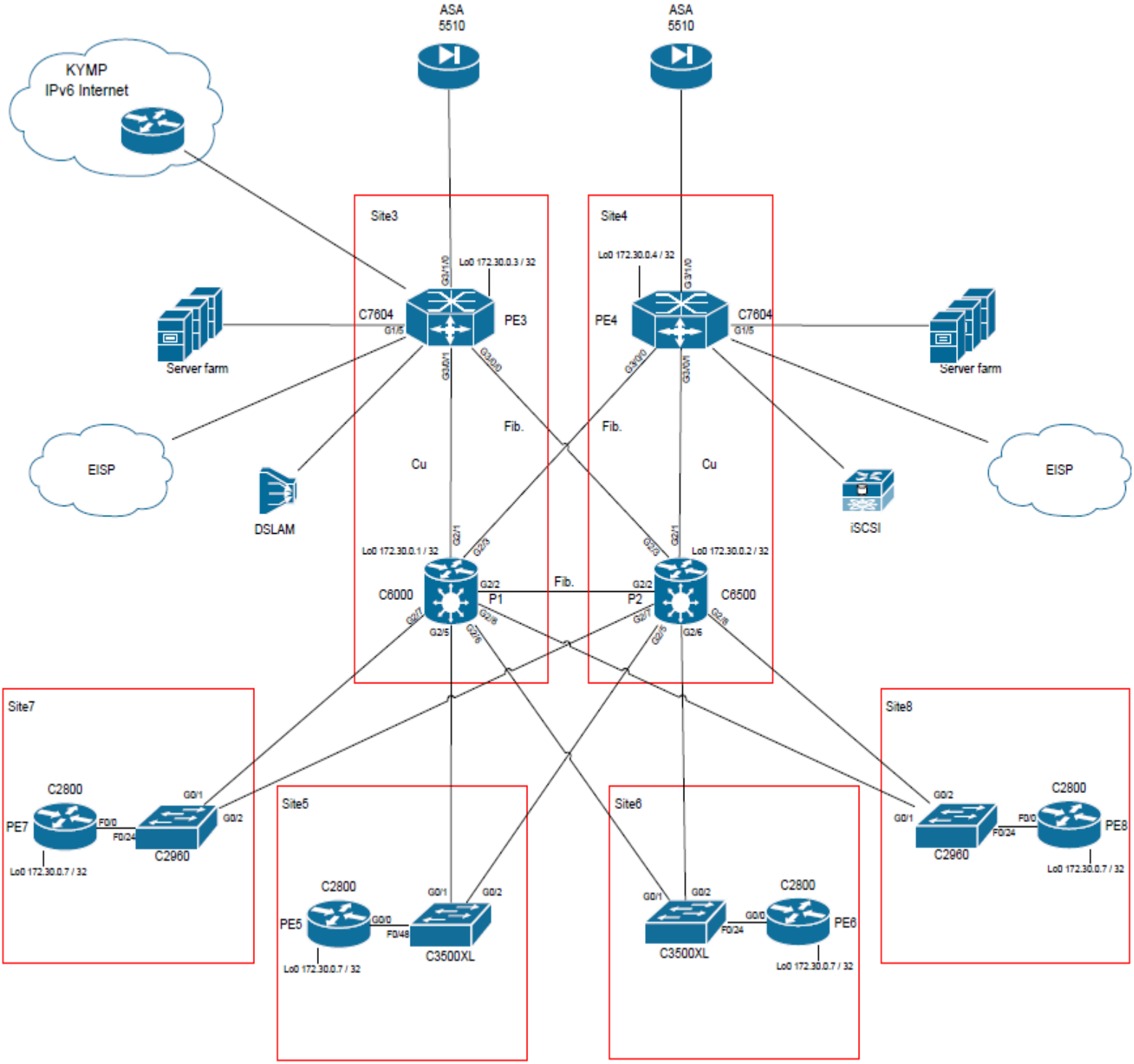
RFC 4736, Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP). IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc4736.txt [viitattu 20.3.2013]

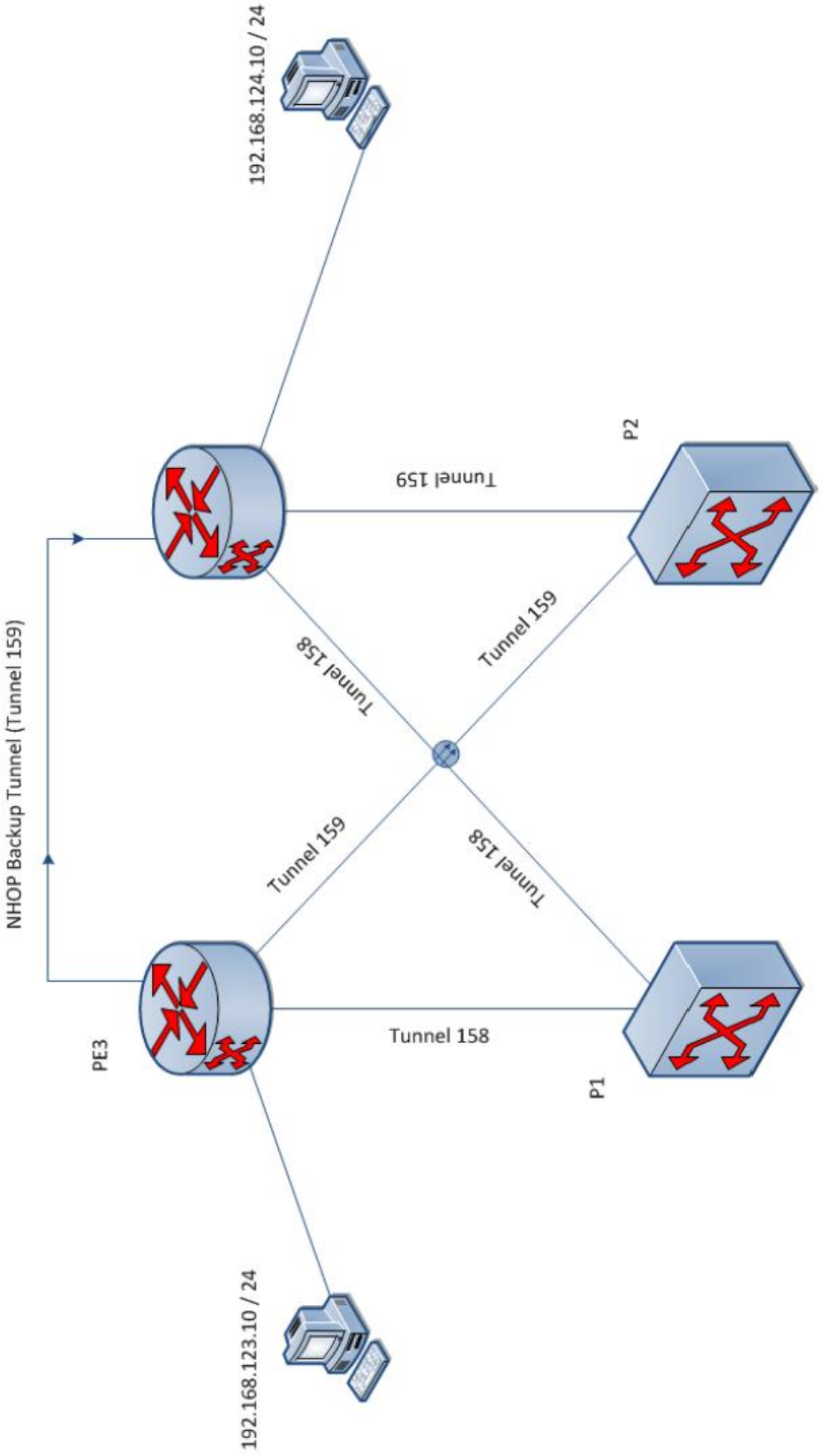
RFC 5786, Advertising a Router's Local Addresses in OSPF Traffic Engineering (TE) Extensions.IETF. Saatavissa: http://www.rfc-editor.org/rfc/rfc5786.txt[viitattu 19.3.2013].

The MPLS Forwarding Plane. 2010. Verkkojulkaisu. Saatavissa: http://blog.ine.com/2010/02/21/the-mpls-forwarding-plane/. [viitattu 15.3.2013]

Tuntematon. 2012. SimuNetin fyysinen kytkentä. Kaavio. Saatavissa: Kymenlaakson Ammattikorkeakoulun ICT-Laboratorion sisäverkko.

Yassar A, Aslam M N. 2010. Traffic Engineering with Multi-Protocol Label Switching. Saarbrücken: LAP Lambert Academic Publishing AG & Co KG.


ASA
5510
ASA
5510
KYMP
IPv6 Internet
Site3
Site4
Lo0 172.30.0.3 / 32
Lo0 172.30.0.4 / 32
C7604
PE3
PE4
C7604
G1/5
G1/5
Server farm
Server farm
EISP
EISP
DSLAM
iSCSI
Fib.
Cu
Fib.
Cu
Lo0 172.30.0.1 / 32
Lo0 172.30.0.2 / 32
C6000
P1
P2
C6500
Fib.
Site7
Site8
Site5
Site6
C2800
PE7
C2960
C2800
PE8
C2960
C2800
PE5
C3500XL
C3500XL
C2800
PE6
Lo0 172.30.0.7 / 32
Lo0 172.30.0.7 / 32
Lo0 172.30.0.7 / 32
Lo0 172.30.0.7 / 32


192.168.124.10 / 24
P2
Tunnel 159
Tunnel 158
Tunnel 159
NHOP Backup Tunnel (Tunnel 159)
Tunnel 159
Tunnel 158
PE3
Tunnel 158
P1
192.168.123.10 / 24

```
Current configuration : 13654 bytes
!
! Last configuration change at 10:13:48 UTC Fri Feb 8 2013
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
!
vrf definition CUSTOMER_C1
!
!
no aaa new-model
!
!
!
ip source-route
!
ip vrf teemukim
!
ip flow-cache timeout active 5
ip name-server 2A00:1DD0:100:C1::100
ip name-server 172.16.91.92
ip multicast-routing
ip dhcp excluded-address 172.20.99.1 172.20.99.100
ip dhcp excluded-address 172.20.99.254
!
ip dhcp pool HALLINTA
 network 172.20.99.0 255.255.255.0
 default-router 172.20.99.1
!
ip dhcp pool VLAN2001
 network 10.10.11.0 255.255.255.0
 default-router 10.10.11.1
!
ip dhcp pool VLAN2000
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
!
!
ipv6 unicast-routing
ipv6 dhcp pool vlan2000
 prefix-delegation pool VLAN2000ipv6
 dns-server 2A00:1DD0:0:1::32
 dns-server 2A00:1DD0:0:1::132
 domain-name kymp.net
!
!
!
vtp mode transparent
mpls traffic-eng tunnels
mpls label protocol ldp
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
username HALLINTA secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
username simunet secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 7
!
vlan 10
 name Area1FWout
!
vlan 20
 name Area2FWout
!
vlan 69
 name DSLAMHALLINTA
!
vlan 80
 name INTERNET
!
vlan 81
 name INTERNET_C1
!
vlan 90
 name WLC&APs
!
vlan 91
 name WLC_C1
!
vlan 99
 name Hallinta
!
vlan 100
 name Servers1
!
vlan 101
 name Palomuurin_ohitus
!
vlan 110
 name teemukim
!
vlan 120
 name Nagios
!
vlan 130
 name mpls_te
!
vlan 200
 name Servers2
!
vlan 225
 name ServiceInstance
!
vlan 300
 name Failover
!
vlan 400
 name iSCSI&ClusterVLAN
!
vlan 2000
 name g4
!
```

```
!
l2 vfi FW_OUT_10 manual
 vpn id 10
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi FW_OUT_20 manual
 vpn id 20
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi INTERNET_C1 manual
 vpn id 81
 neighbor 172.30.0.4 encapsulation mpls
!
l2 vfi NAGIOS manual
 vpn id 120
 neighbor 172.30.0.4 encapsulation mpls
 neighbor 172.30.0.7 encapsulation mpls no-split-horizon
!
l2 vfi WLCAPS manual
 vpn id 100090
 neighbor 172.30.0.7 encapsulation mpls
 neighbor 172.30.0.4 encapsulation mpls no-split-horizon
!
l2 vfi WLC_C1 manual
 vpn id 100091
 neighbor 172.30.0.4 encapsulation mpls
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.3 255.255.255.255
!
interface Loopback5
 no ip address
 ip pim sparse-mode
 ip igmp version 3
!
interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::3/128
 ipv6 address 2A00:1DD0:401::3/128
!
interface Tunnel158
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 172.30.0.4
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 3500
 tunnel mpls traffic-eng path-option 1 explicit name mainpath
 tunnel mpls traffic-eng fast-reroute
!
interface Tunnel159
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 172.30.0.4
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 3500
 tunnel mpls traffic-eng path-option 1 explicit name secpath
!
interface GigabitEthernet1/1
 description simunet-srv
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/2
 description simunet-srv
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/3
 no ip address
!
interface GigabitEthernet1/4
 ip address 150.100.1.1 255.255.255.252
!
interface GigabitEthernet1/5
 description simunet-srv
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,91,99-101,110,120,150,200
 switchport mode trunk
!
interface GigabitEthernet1/6
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 99
 switchport mode trunk
!
interface GigabitEthernet1/7
 ip address 172.16.50.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/8
 description Firewall failover
 no ip address
 xconnect 172.30.0.4 300 encapsulation mpls
!
interface GigabitEthernet1/9
 description KYMP-SIMUNET IPV6 CONNECTION
 no ip address
 ip flow ingress
 speed 100
 duplex full
 ipv6 address 2A00:1DD0:400:102::2/64
!
interface GigabitEthernet3/0/0
 description P2-PE3 fiber
 dampening
 mtu 1600
 ip address 192.168.23.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 ip ospf cost 1
 carrier-delay msec 0
 negotiation auto
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 3900
!
interface GigabitEthernet3/0/1
 description P1-PE3 copper
 dampening
 mtu 1600
 ip address 192.168.13.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 carrier-delay msec 0
 speed 1000
 no negotiation auto
 mpls ip
 no mpls ldp igp sync
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel159
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 4000
!
```

```
interface GigabitEthernet3/0/2
 description ServiceInstance
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 210 ethernet
  encapsulation dot1q 210-220
  xconnect 172.30.0.4 210 encapsulation mpls
 !
!
interface GigabitEthernet3/0/3
 no ip address
 speed 1000
 negotiation auto
!
interface GigabitEthernet3/0/4
 description WLC EVC
 no ip address
 speed 100
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 90
  rewrite ingress tag pop 1 symmetric
  bridge-domain 90
 !
 service instance 2 ethernet
  encapsulation dot1q 91
  rewrite ingress tag pop 1 symmetric
  bridge-domain 91
 !
!
interface GigabitEthernet3/1/0
 description Firewall EVC
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
 service instance 2 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
 service instance 5 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 6 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
 !
!
interface GigabitEthernet3/1/1
 no ip address
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3/1/2
 no ip address
 shutdown
 speed 100
 no negotiation auto
 xconnect 172.30.0.4 6969 encapsulation mpls
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 7
 !
!
interface GigabitEthernet3/1/3
 ip address 192.168.123.1 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3/1/4
 description JOONAMATTIprojekti
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 30 ethernet
  encapsulation dot1q 30
  xconnect 172.30.0.4 30 encapsulation mpls
 !
 service instance 40 ethernet
  encapsulation dot1q 40
  xconnect 172.30.0.4 40 encapsulation mpls
 !
!
interface GigabitEthernet3/1/4.69
 encapsulation dot1Q 69
 ip address 172.16.69.69 255.255.255.0
!
interface GigabitEthernet3/1/4.2000
 encapsulation dot1Q 2000
 ip address 172.17.0.1 255.255.255.0
 ipv6 address 2A00:1DD0:100:4100::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp server vlan2000
!
interface GigabitEthernet3/1/4.2001
 encapsulation dot1Q 2001
 ip address 10.10.11.1 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Firewall context 1 outside
 mtu 1600
 ip address 172.30.1.3 255.255.255.248
 no ip redirects
 standby version 2
 standby 10 ip 172.30.1.5
 standby 10 priority 150
 standby 10 preempt
 standby 110 ipv6 FE80::1
 standby 110 priority 150
 standby 110 preempt
 ipv6 address FE80:A1::3 link-local
 ipv6 address 2A00:1DD0:100:A1::3/64
 xconnect vfi FW_OUT_10
!
interface Vlan20
 description Firewall context 2 outside
 mtu 1600
 ip address 172.31.1.3 255.255.255.248
 no ip redirects
 standby version 2
 standby 20 ip 172.31.1.5
 standby 20 preempt
 standby 120 ipv6 FE80::2
 standby 120 preempt
```

```
 ipv6 address FE80:A2::3 link-local
 ipv6 address 2A00:1DD0:100:A2::3/64
 xconnect vfi FW_OUT_20
!
interface Vlan43
 no ip address
 shutdown
!
interface Vlan80
 mtu 1600
 no ip address
!
interface Vlan81
 mtu 1600
 ip address 172.30.81.1 255.255.255.0
 xconnect vfi INTERNET_C1
!
interface Vlan90
 mtu 1600
 ip address 172.16.10.5 255.255.255.0
 ip helper-address 172.16.91.91
 standby version 2
 standby 90 ip 172.16.10.3
 standby 90 preempt
 standby 90 name WLC1
 xconnect vfi WLCAPS
!
interface Vlan91
 mtu 1600
 ip dhcp relay information trusted
 ip address 172.16.91.5 255.255.255.0
 ip helper-address 172.16.91.91
 standby version 2
 standby 91 ip 172.16.91.3
 standby 91 preempt
 standby 91 name WLC
 xconnect vfi WLC_C1
!
interface Vlan99
 ip address 172.20.99.1 255.255.255.0
!
interface Vlan100
 description Firewall context 1 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.4 100 encapsulation mpls
!
interface Vlan101
 description Palomuurin_ohitus
 ip address 172.30.101.3 255.255.255.0
 standby version 2
 standby 1 ip 172.30.101.254
 standby 1 preempt
 standby 101 ipv6 FE80:C1::1
 standby 101 priority 150
 standby 101 preempt
 ipv6 address FE80:101::3 link-local
 ipv6 address 2A00:1DD0:100:C1::3/64
 xconnect 172.30.0.4 101 encapsulation mpls
!
interface Vlan111
 ip vrf forwarding teemukim
 ip address 10.111.0.251 255.255.255.0
 shutdown
!
interface Vlan120
 mtu 1600
 ip address 172.16.120.3 255.255.255.0
 standby 1 ip 172.16.120.1
 standby 1 priority 150
 standby 1 preempt
 xconnect vfi NAGIOS
!
interface Vlan130
 description mpls_te
 ip address 172.16.130.3 255.255.255.0
 shutdown
!
interface Vlan200
 description Firewall context 2 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.4 200 encapsulation mpls
!
interface Vlan400
 description ISCSI/Cluster-VLAN
 mtu 1600
 no ip address
 no ip redirects
 xconnect 172.30.0.4 400 encapsulation mpls
!
interface Vlan1100
 mtu 1600
 no ip address
!
router ospf 1
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet3/0/0
 no passive-interface GigabitEthernet3/0/1
 network 172.16.50.0 0.0.0.3 area 0
 network 172.20.99.0 0.0.0.255 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 172.30.101.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
 neighbor 2A00:1DD0:400:102::1 remote-as 65000
 neighbor 172.30.0.4 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO
 !
 address-family ipv4
  network 172.30.0.0 mask 255.254.0.0
  neighbor 172.30.0.4 activate
  neighbor 172.30.0.6 activate
 exit-address-family
 !
 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100::/48
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  network 2A00:1DD0:401::/48
  neighbor SISAVERKKO send-label
  neighbor 2A00:1DD0:400:102::1 activate
  neighbor 2A00:1DD0:400:102::1 prefix-list SIMUNET6 out
  neighbor 172.30.0.4 activate
 exit-address-family
!
!
ip flow-export source GigabitEthernet1/9
ip flow-export version 9
ip flow-export destination 172.21.99.101 2055
```

```
no ip http server
no ip http secure-server
ip pim ssm default
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1
ip route 192.168.0.0 255.255.255.0 172.17.0.104
ip route 192.168.1.0 255.255.255.0 172.17.0.104
ip route 192.168.124.0 255.255.255.0 Tunnel158
ip route 192.168.124.0 255.255.255.0 Tunnel159
!
ip explicit-path name mainpath enable
 next-address 192.168.13.3
 next-address 192.168.13.1
 next-address 192.168.14.1
 next-address 192.168.14.4
 next-address 172.30.0.4
!
ip explicit-path name secpath enable
 next-address 192.168.23.3
 next-address 192.168.24.2
 next-address 192.168.23.2
 next-address 192.168.24.4
 next-address 172.30.0.4
!
logging esm config
access-list 1 permit 172.31.1.2
access-list 100 permit ip host 172.31.1.2 host 172.31.1.3
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100:4101::/64 2A00:1DD0:100:4100::104
ipv6 route 2A00:1DD0:100:4101::/64 GigabitEthernet3/1/4.2000
2A00:1DD0:100:4100::104
ipv6 route 2A00:1DD0:100:4102::/64 GigabitEthernet3/1/4.2000
2A00:1DD0:100:4100:21E:ABFF:FE50:5050
ipv6 route 2A00:1DD0:100::/48 Null0
ipv6 route 2A00:1DD0:401::/48 Null0
ipv6 local pool VLAN2000ipv6 2A00:1DD0:100:4000::/56 64
ipv6 local pool VLAN2000ipv7 2A00:1DD0:100:4200::/56 64
!
!
ipv6 prefix-list SIMUNET6 seq 5 permit 2A00:1DD0:100::/48
ipv6 prefix-list SIMUNET6 seq 10 permit 2A00:1DD0:401::/48
mpls ldp router-id Loopback0 force
snmp-server community public RO
snmp-server host 172.16.120.10 version 2c public
!
!
ipv6 access-list testilista
 permit udp any any eq domain
 permit udp any eq domain any
!
control-plane
!
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 session-timeout 60
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 session-timeout 60
 logging synchronous
 login local
 transport input ssh
!
!
!
end

PE3#
```

```
Current configuration : 12312 bytes
!
! Last configuration change at 10:04:55 UTC Fri Feb 8 2013
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
mls ipv6 vrf
!
vrf definition CUSTOMER_C1
 rd 6:6
 !
 address-family ipv6
  route-target export 6:6
  route-target import 6:6
 exit-address-family
!
!
no aaa new-model
!
!
!
ip source-route
!
ip vrf INTERNET
 rd 65001:80
 route-target export 65001:80
 route-target import 65001:80
!
ip vrf teemukim
!
no ip domain lookup
ip domain name ictlab.kyamk.fi
ip multicast-routing
ip dhcp excluded-address 172.21.99.1 172.21.99.100
ip dhcp excluded-address 172.21.99.254
!
ip dhcp pool HALLINTA
 network 172.21.99.0 255.255.255.0
 default-router 172.21.99.1
!
!
ipv6 unicast-routing
!
!
vtp mode transparent
mpls traffic-eng tunnels
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
username simunet secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 7
!
vlan 10
 name Area1FWout
!
vlan 20
 name Area2FWout
!
vlan 81
 name INTERNET_C1
!
vlan 90
 name WLC&APs
!
vlan 91
 name WLC_C1
!
vlan 99
 name HALLINTA
!
vlan 100
 name Servers1
!
vlan 101
 name Palomuurin_ohitus
!
vlan 110
 name teemukim
!
vlan 120
 name Nagios
!
vlan 130
 name mpls_te
!
vlan 200
 name Servers2
!
vlan 225
 name ServiceInstance
!
vlan 300
```

```
 name Failover
!
vlan 400
 name iSCSI&ClusterVLAN
!
!
l2 vfi FW_OUT_10 manual
 vpn id 10
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi FW_OUT_20 manual
 vpn id 20
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi INTERNET_C1 manual
 vpn id 81
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi NAGIOS manual
 vpn id 120
 neighbor 172.30.0.7 encapsulation mpls no-split-horizon
 neighbor 172.30.0.3 encapsulation mpls
!
l2 vfi WLCAPS manual
 vpn id 100090
 neighbor 172.30.0.3 encapsulation mpls
 neighbor 172.30.0.7 encapsulation mpls no-split-horizon
!
l2 vfi WLC_C1 manual
 vpn id 100091
 neighbor 172.30.0.3 encapsulation mpls
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.4 255.255.255.255
!
interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::4/128
!
interface Tunnel158
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 172.30.0.3
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 3500
 tunnel mpls traffic-eng path-option 1 explicit name mainpath
 tunnel mpls traffic-eng fast-reroute
!
interface Tunnel159
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 172.30.0.3
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 3500
 tunnel mpls traffic-eng path-option 1 explicit name secpath
!
interface GigabitEthernet1/1
 description simunet-srv
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/2
 description simunet-srv
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/3
 description iSCSI
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/4
 description iSCSI
 switchport
 switchport access vlan 400
 switchport mode access
!
interface GigabitEthernet1/5
 description simunet-srv
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,91,99-101,110,120,150,200
 switchport mode trunk
 no keepalive
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 description IPTV-palvelin
 ip address 172.16.50.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/8
 description Firewall failover
 no ip address
 xconnect 172.30.0.3 300 encapsulation mpls
!
interface GigabitEthernet1/9
 ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet3/0/0
 description P1-PE4 fiber
 dampening
 mtu 1600
 ip address 192.168.14.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 negotiation auto
 mpls ip
 no mpls ldp igp sync
 mpls traffic-eng tunnels
```

```
 mpls traffic-eng backup-path Tunnel159
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 4000
!
interface GigabitEthernet3/0/1
 description P2-PE4 copper
 dampening
 mtu 1600
 ip address 192.168.24.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 speed 1000
 no negotiation auto
 mpls ip
 no mpls ldp igp sync
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 3900
!
interface GigabitEthernet3/0/2
 description ASA5510 Kalaverkkoon
 no ip address
 speed 1000
 no negotiation auto
 ipv6 address 2A00:1DD0:100:F001::1/64
 ipv6 enable
!
interface GigabitEthernet3/0/3
 description ServiceInstance
 mtu 1600
 no ip address
 no negotiation auto
 service instance 210 ethernet
  encapsulation dot1q 210-220
  xconnect 172.30.0.3 210 encapsulation mpls
 !
!
interface GigabitEthernet3/0/4
 description WLC EVC
 no ip address
 speed 100
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 90
  rewrite ingress tag pop 1 symmetric
  bridge-domain 90
 !
 service instance 2 ethernet
  encapsulation dot1q 91
  rewrite ingress tag pop 1 symmetric
  bridge-domain 91
 !
!
interface GigabitEthernet3/1/0
 description Firewall EVC
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
 service instance 2 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
 service instance 5 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance 6 ethernet
  encapsulation dot1q 200
  rewrite ingress tag pop 1 symmetric
  bridge-domain 200
 !
!
interface GigabitEthernet3/1/1
 no ip address
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3/1/2
 no ip address
 shutdown
 speed 100
 no negotiation auto
 xconnect 172.30.0.3 6969 encapsulation mpls
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 7
 !
!
interface GigabitEthernet3/1/3
 ip address 192.168.124.1 255.255.255.0
 speed 1000
 no negotiation auto
!
interface GigabitEthernet3/1/4
 description JOONAMATTIprojekti
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 30 ethernet
  encapsulation dot1q 30
  xconnect 172.30.0.3 30 encapsulation mpls
 !
 service instance 40 ethernet
  encapsulation dot1q 40
  xconnect 172.30.0.3 40 encapsulation mpls
 !
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Firewall context 1 outside
 mtu 1600
```

```
 ip address 172.30.1.4 255.255.255.248
 no ip redirects
 standby version 2
 standby 10 ip 172.30.1.5
 standby 10 preempt
 standby 110 ipv6 FE80::1
 standby 110 preempt
 ipv6 address FE80:A1::4 link-local
 ipv6 address 2A00:1DD0:100:A1::4/64
 xconnect vfi FW_OUT_10
!
interface Vlan20
 description Firewall context 2 outside
 mtu 1600
 ip address 172.31.1.4 255.255.255.248
 no ip redirects
 standby version 2
 standby 20 ip 172.31.1.5
 standby 20 priority 150
 standby 20 preempt
 standby 120 ipv6 FE80::2
 standby 120 priority 150
 standby 120 preempt
 ipv6 address FE80:A2::4 link-local
 ipv6 address 2A00:1DD0:100:A2::4/64
 xconnect vfi FW_OUT_20
!
interface Vlan81
 mtu 1600
 ip address 172.30.81.2 255.255.255.0
 xconnect vfi INTERNET_C1
!
interface Vlan90
 mtu 1600
 ip address 172.16.10.4 255.255.255.0
 ip helper-address 172.16.91.91
 standby version 2
 standby 90 ip 172.16.10.3
 standby 90 priority 150
 standby 90 preempt
 standby 90 name WLC1
 xconnect vfi WLCAPS
!
interface Vlan91
 mtu 1600
 ip dhcp relay information trusted
 ip address 172.16.91.4 255.255.255.0
 ip helper-address 172.16.91.91
 standby version 2
 standby 91 ip 172.16.91.3
 standby 91 priority 150
 standby 91 preempt
 standby 91 name WLC
 xconnect vfi WLC_C1
!
interface Vlan99
 ip address 172.21.99.1 255.255.255.0
!
interface Vlan100
 description Firewall context 1 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.3 100 encapsulation mpls
!
interface Vlan101
 description Palomuurin_ohitus
 ip address 172.30.101.4 255.255.255.0
 standby version 2
 standby 1 ip 172.30.101.254
 standby 1 priority 150
 standby 1 preempt
 standby 101 ipv6 FE80:C1::1
 standby 101 preempt
 ipv6 address FE80:101::4 link-local
 ipv6 address 2A00:1DD0:100:C1::4/64
 xconnect 172.30.0.3 101 encapsulation mpls
!
interface Vlan120
 mtu 1600
 ip address 172.16.120.4 255.255.255.0
 standby 1 ip 172.16.120.1
 standby 1 preempt
 xconnect vfi NAGIOS
!
interface Vlan130
 ip address 172.16.130.4 255.255.255.0
 shutdown
!
interface Vlan200
 description Firewall context 2 inside
 mtu 1600
 no ip address
 xconnect 172.30.0.3 200 encapsulation mpls
!
interface Vlan400
 description iSCSI&ClusterVLAN
 mtu 1600
 no ip address
 no ip redirects
 xconnect 172.30.0.3 400 encapsulation mpls
!
router ospf 1
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet3/0/0
 no passive-interface GigabitEthernet3/0/1
 no passive-interface GigabitEthernet3/0/4
 network 172.16.50.0 0.0.0.3 area 0
 network 172.21.99.0 0.0.0.255 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 172.30.101.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 bfd all-interfaces
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
```

```
 neighbor 10.0.0.2 remote-as 65100
 neighbor 10.0.0.2 version 4
 neighbor 172.30.0.3 peer-group SISAVERKKO
 neighbor 172.30.0.5 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO
 neighbor 172.30.0.7 remote-as 65001
 neighbor 172.30.0.7 update-source Loopback0
 neighbor 172.30.0.8 remote-as 65001
 neighbor 172.30.0.8 update-source Loopback0
 !
 address-family ipv4
  network 172.30.0.0 mask 255.254.0.0
  neighbor 10.0.0.2 activate
  neighbor 172.30.0.3 activate
  neighbor 172.30.0.5 activate
  neighbor 172.30.0.6 activate
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.8 activate
 exit-address-family
 !
 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  network 2A00:1DD0:100:100::/56
  neighbor SISAVERKKO send-label
  neighbor 172.30.0.3 activate
 exit-address-family
 !
 address-family vpnv6
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.7 send-community extended
  neighbor 172.30.0.8 activate
  neighbor 172.30.0.8 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf CUSTOMER_C1
  redistribute connected
  redistribute static
 exit-address-family
!
!
no ip http server
no ip http secure-server
ip pim ssm default
ip route profile
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1
ip route 192.168.123.0 255.255.255.0 Tunnel158
ip route 192.168.123.0 255.255.255.0 Tunnel159
!
ip explicit-path name mainpath enable
 next-address 192.168.14.4
 next-address 192.168.14.1
 next-address 192.168.13.1
 next-address 192.168.13.3
 next-address 172.30.0.3
!
ip explicit-path name secpath enable
 next-address 192.168.24.4
 next-address 192.168.23.2
 next-address 192.168.24.2
 next-address 192.168.23.3
 next-address 172.30.0.3
!
logging esm config
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100:100::/56 GigabitEthernet3/0/2
2A00:1DD0:100:F001::2
ipv6 route vrf CUSTOMER_C1 2A00:1DD0:100:10C3::/64
2A00:1DD0:100:F310::2
ipv6 router ospf 6
!
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 session-timeout 60
 login local
 transport input ssh
line vty 5 15
 session-timeout 60
 login local
 transport input ssh
!
!
!
end

PE4#
```

```
Current configuration : 3852 bytes
!
! Last configuration change at 08:46:14 EEST Thu Jan 31 2013
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service counters max age 10
!
hostname P1
!
boot-start-marker
boot system sup-bootdisk:s3223-advipservicesk9-mz.122-33.SRE3.bin
boot-end-marker
!
!
no aaa new-model
!
!
!
clock timezone EEST 2
ip source-route
!
!
ip multicast-routing
mls ip multicast replication-mode ingress
no ip domain lookup
ip domain name ictlab.kyamk.fi
!
!
ipv6 mfib hardware-switching replication-mode ingress
!
!
mpls traffic-eng tunnels
mpls label protocol ldp
mls flow ip interface-full
no mls flow ipv6
no mls acl tcam share-global
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
!
spanning-tree mode pvst
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
username simunet secret 5 $1$NOYV$bvuNASs70XPVMoD7cxprn.
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.1 255.255.255.255
!
interface GigabitEthernet2/1
 description P1-PE3 copper
 dampening
 mtu 1600
 ip address 192.168.13.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 4000
!
interface GigabitEthernet2/2
 description P1-P2 fiber
 dampening
 mtu 1600
 ip address 192.168.12.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet2/3
 description P1-PE4 fiber
 dampening
 mtu 1600
 ip address 192.168.14.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 4000
!
interface GigabitEthernet2/4
 no ip address
!
interface GigabitEthernet2/5
 description P1-PE5
 dampening
 mtu 1600
 ip address 192.168.15.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
!
interface GigabitEthernet2/6
 description P1-PE6
 dampening
 mtu 1600
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
```

```
!
interface GigabitEthernet2/7
 description P1-PE7
 mtu 1600
 ip address 192.168.17.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet2/8
 description P1-PE8
 dampening
 mtu 1600
 ip address 192.168.18.1 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet5/3
 no ip address
 shutdown
!
interface GigabitEthernet5/4
 no ip address
 shutdown
!
interface GigabitEthernet5/5
 no ip address
 shutdown
!
interface GigabitEthernet5/6
 no ip address
 shutdown
!
interface GigabitEthernet5/7
 no ip address
 shutdown
!
interface GigabitEthernet5/8
 no ip address
 shutdown
!
interface GigabitEthernet5/9
 ip address 172.30.9.1 255.255.255.0
 speed 100
 duplex full
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 172.30.0.0 0.0.0.255 area 0
 network 172.30.9.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
!
no ip http server
no ip http secure-server
ip pim ssm default
ip route 172.30.90.0 255.255.255.0 GigabitEthernet5/9
!
ip sla 1
 icmp-echo 172.30.0.7
!
!
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 login local
 transport input ssh
!
!
monitor session 1 source interface Gi2/1
monitor session 1 destination interface Gi2/4
ntp clock-period 17179833
ntp server 172.30.90.2
!
end

P1#
```

```
Current configuration : 3586 bytes
!
! Last configuration change at 06:56:59 UTC Thu Feb 7 2013
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service counters max age 10
!
hostname P2
!
boot-start-marker
boot system sup-bootdisk:s3223-advipservicesk9-mz.122-33.SRE3.bin
boot-end-marker
!
!
no aaa new-model
!
!
!
ip source-route
!
!
ip multicast-routing
mls ip multicast replication-mode ingress
ip domain name ictlab.kyamk.fi
!
!
ipv6 mfib hardware-switching replication-mode ingress
!
!
vtp mode transparent
mpls traffic-eng tunnels
mpls label protocol ldp
mls flow ip interface-full
no mls flow ipv6
no mls acl tcam share-global
mls cef error action reset
multilink bundle-name authenticated
!
!
!
!
!
spanning-tree mode pvst
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
username simunet secret 5 $1$NOYV$bvuNASs70XPVMoD7cxprn.
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 172.30.0.2 255.255.255.255
!
interface GigabitEthernet2/1
 description P2-PE4 copper
 dampening
 mtu 1600
 ip address 192.168.24.2 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 3900
!
interface GigabitEthernet2/2
 description P1-P2 fiber
 dampening
 mtu 1600
 ip address 192.168.12.2 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet2/3
 description P2-PE3 fiber
 dampening
 mtu 1600
 ip address 192.168.23.2 255.255.255.0
 ip pim sparse-mode
 ip ospf cost 1
 carrier-delay msec 0
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 3900
!
interface GigabitEthernet2/4
 no ip address
!
interface GigabitEthernet2/5
 description P2-PE5
 dampening
 mtu 1600
 ip address 192.168.25.2 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
!
interface GigabitEthernet2/6
 description P2-PE6
 dampening
 mtu 1600
 ip address 192.168.26.2 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
```

```
!
interface GigabitEthernet2/7
 description P2-PE7
 dampening
 mtu 1600
 ip address 192.168.27.2 255.255.255.0
 ip pim sparse-mode
 ip ospf cost 1
 carrier-delay msec 0
 mpls ip
 bfd interval 100 min_rx 100 multiplier 3
!
interface GigabitEthernet2/8
 description P2-PE8
 dampening
 mtu 1600
 ip address 192.168.28.2 255.255.255.0
 ip pim sparse-mode
 carrier-delay msec 0
 mpls ip
!
interface GigabitEthernet6/1
 no ip address
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet6/3
 no ip address
 shutdown
!
interface GigabitEthernet6/4
 no ip address
 shutdown
!
interface GigabitEthernet6/5
 no ip address
 shutdown
!
interface GigabitEthernet6/6
 no ip address
 shutdown
!
interface GigabitEthernet6/7
 no ip address
 shutdown
!
interface GigabitEthernet6/8
 no ip address
 shutdown
!
interface GigabitEthernet6/9
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 172.30.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 bfd all-interfaces
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
!
no ip http server
no ip http secure-server
ip pim ssm default
!
!
!
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 login local
 transport input ssh
!
!
end

P2#
```