Ari Piippo

Multi Protocol Label Switching -tekniikalla toteutettu laboratoriotyöympäristö

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
11.5.2011

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Ari Piippo Multi Protocol Label Switching -tekniikalla toteutettu laboratoriotyöympäristö 37 sivua 11.5.2011
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoliikenneverkot
Ohjaaja	yliopettaja Matti Puska

Tellabs on yhdysvaltalainen telekommunikaatiolaitteita valmistava yritys, jonka tuotekehitys-osasto toimii Suomessa. Tellabsin insinöörit tarvitsevat työssään verkkoympäristön, missä reitittimien ominaisuuksia ja asetuksia voidaan testata mahdollisimman realistisesti ja kätevästi. Työn tavoitteena on luoda ympäristö, missä reitittimien näitä ominaisuuksia ja asetuksia voidaan testata.

Työympäristö pohjautuu Multi Protocol Label Switching –verkkotekniikkaan. Työympäristössä on Ethernet-runkoverkko, joka on jaettu eri reititysprotokollien vaikuttaviin alueisiin. Runkoverkkoon on kytketty reunareitittimiä, joiden avulla voidaan luoda esimerkiksi toisen ja kolmannen tason Virtual Private Service –sovelluksia runkoverkon yli.

Teoriaosuudessa käytiin läpi MPLS-tekniikkaa sekä esiteltiin perinteiseen reititykseen kuuluvia osa-alueita. MPLS-tekniikasta käytiin läpi sen ominaisuuksia, esiteltiin siihen liittyviä protokollia, käytiin läpi MPLS-leimojen koostumus ja niiden käyttö. Reititystekniikkaan liittyen käytiin läpi reititysprotokollat sekä niiden toiminta.

Käytännön osuudessa esiteltiin rakennettava verkko. Esiteltiin käytettävät verkot ja niiden Internet Protocol -osoitteet. Luotiin reititysprotokollien alueet ja varmistettiin saavutettavuus verkon yli. Verkkoliitäntöjen turvaamiseen liittyvä tekniikkaa esiteltiin ja toteutettiin.

Toimivalla MPLS-tekniikalla toteutetulla verkolla reitittimillä on yhteys verkon muihin reitittimiin. Reitittimet ovat kykeneviä vaihtamaan leimoja keskenään. Leimojen jakaminen mahdollistaa virtuaalilinjojen sekä tunnelien luonnin.

Avainsanat	MPLS, VPN, OSPF, IS-IS, verkkoympäristö

Metropolia

Abstract

Author Title Number of Pages Date	Ari Piippo Multi Protocol Label Switching Laboratory environment 37 pages 11 May 2011
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networks
Instructor	Matti Puska, Principal Lecturer

Tellabs is a telecommunications equipment manufacturer from the United States. Tellabs has a research and development division in Finland. Engineers that work in Tellabs have a constant need for an environment where they can test product features and abilities conveniently.

The laboratory environment is based on the Multi Protocol Label Switching-technique. The testing environment has an Ethernet-backbone network, which has been divided into multiple areas where different routing protocols are interacting. The backbone network is interoperated with edge routers, which can be used when for example creating pseudo wires or layer three Virtual Private Networks over the backbone network.

The Theoretical section is about the fundamentals of the MPLS technique and it also contains an introduction to basic routing. The MPLS chapter comprises the features of the MPLS technique, related protocols, different MPLS labels and the usage of MPLS labels. In the routing chapter different routing protocols are covered with regard to basics and operation.

In the practical part the network to be implemented was presented concerning subnetworks and Internet Protocol addresses. Routing protocol areas were created and connectivity tested. Interface protecting techniques were introduced and implemented.

MPLS based network functionality was tested with successful creation of pseudo wires and tunnels.

Keywords	MPLS, VPN, OSPF, IS-IS, Laboratory environment

Sisällys

1 Johdanto

Työskentelen yrityksessä nimeltä Tellabs Oy. Yritys on yhdysvaltalaisomistuksessa oleva yritys, mikä on toiminut Suomessa vuodesta 1993 lähtien. Vuonna 1993 Tellabs osti espoolaisen 1976 perustetun Martis Oy:n. Siitä lähtien Tellabs on keskittynyt reitittimien kehitykseen. Yritys on siitä mielenkiintoinen, että se on itse suunnitellut, valmistanut ja kehittänyt omat tietoliikennereitittimensä alusta loppuun. Tänä päivänä yritys toimii varteenotettavassa asemassa yhtenä suurimmista reititintoimittajista. Asiakkaana Tellabsilla on monia kansainvälisesti tunnettuja ja johtavia teleoperaattoreita ympäri maailmaa. Työni suunnitellaan ja toteutetaan Tellabs Oy:lle Suomen yksikköön. [14.]

Opinnäytetyöni tarkoitus on suunnitella ja olla osana toteutuksessa, jossa rakennetaan kokonaan uusi laboratoriotestiympäristö. Laboratorio toimii testiympäristönä tietoliikennereitittimille ja korvaa vanhan ympäristön. Laboratorion tarkoitus on simuloida nykyaikaisen teleoperaattorin verkkoa. Tämä tarkoittaa liikennöintiä aina radiomastolta runkoverkkoon asti. Radiomaston ja runkoverkon välissä olevaa verkkoa kutsutaan backhaul-verkoksi. Tellabs on nimenomaan erikoistunut tarjoamaan tuotteita tämänkaltaisiin ratkaisuihin. Tavoitteena on onnistua luomaan ympäristö, joka on mahdollisimman ymmärrettävä topologialtaan ja vastaa modernia verkon suunnittelua. Yrityksen laatimassa aikataulussa pysyminen on myös tärkeää, ja sitä tullaan noudattamaan.

Laboratoriolle on olemassa kolme pääkäyttötarkoitusta, joiden mukaan se myös suunnitellaan. Tarkemmin sanottuna se jakaantuu kolmeen fyysisesti erilaiseen alueeseen, jotka eivät ole kytköksissä toisiinsa. Ensimmäinen ja suurin toteutus tulee olemaan asiakasverkkojen simulointi. Tämä verkko tulee olemaan käsittelyssä tässä työssä, rajaten muut ulos. Verkon tulee olla mahdollisimman realistinen suhteessa toteutuksiin, joita maailmalla käytetään verkkoratkaisuina. Verkon tulee olla myös tarpeeksi iso, jotta sitä voidaan tarvittaessa kuormittaa realistisesti. Samalla varmistetaan, että se on mukautuvampi. Verkko pohjautuu MPLS (Multiprotocol Label Switching) -tekniikkaan. Toinen alue testaa reitittimien käyttöjärjestelmäversioiden toimivuutta. Reitittimet ovat monimutkaisia laitteita. Niiden sulautetut järjestelmät

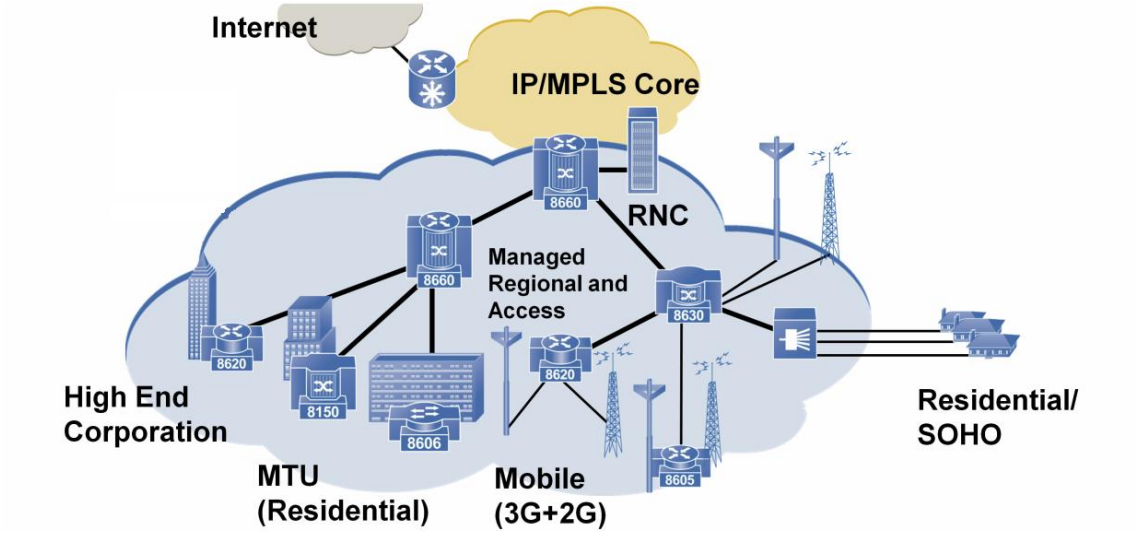
vaativat miljoonia rivejä ohjelmistokoodia, joten ohjelmakoodin laatu on tärkeässä asemassa. Ohjelmistokoodia varten tarvitaan ympäristö, missä voidaan simuloida mahdollisia ohjelmistovirheitä. Kolmas alue on niin sanottu harjoitusalue, missä voi itse rakentaa haluamansa käyttöympäristön alusta alkaen. Tässä ympäristössä on tarkoitus rakentaa pääasiallisesti tarkkoja kopioita asiakkaiden ympäristöistä.

Itse verkon fyysinen rakentaminen jätetään huomioitta tässä työssä, koska sitä ei katsota tarpeelliseksi itse tekniikkaan lähestyvältä näkökannalta. Paneudun projektin tekniseen toteutukseen. Työssä tullaan käsittelemään nykyaikaisia verkkoratkaisuja ja verkkotekniikoita. Työstä rajataan pois vanhempien vähemmän käytössä olevien tekniikoiden sekä protokollien esittely, sillä niiden läpikäymistä ei katsota tarpeelliseksi.

2 Nykyaikainen verkko

Tietoliikenneverkkojen kasvu on kiihtynyt vuosi vuodelta sitten internetin yleistymisen 1990-luvulla. Tekniikan kehittyessä verkot ovat kasvaneet. Verkkojen koot sekä nopeudet ovat moninkertaistuneet. Erityisesti nopeuden tarve on kasvanut räjähdysmäisesti ja se luo suurimmat haasteet nykyajan verkoissa. Matkapuhelimien yleistyminen ja nykyään niiden ominaisuuksien lisääntymisellä on suuri osuutensa tietoliikenneverkkojen kasvamiselle. Palveluiden lisääntyessä ja kehityksen edetessä on puhelimien tiedonsiirtokapasiteetin tarve kasvanut moninkertaisesti.

Palveluntarjoajat voivat tänä päivänä taata mobiililaitteille tiedonsiirtonopeuden, joka pärjää kiinteälle laajakaistayhteydelle. Laajakaistayhteyksien nopeudet ovat myös kasvaneet. Tämän hetken niin sanotut kolmannen sukupolven 3G-yhteydet takaavat teoriassa paikallaan oleville mobiililaitteille 2 Mbps:n nopeuden, kun taas liikkuvan päätelaitteen maksiminopeus on vain 384 kbps. Suurissa kaupungeissa voi siis olettaa tukiasemille tulevien yhteyksien vaativan paljon kaistanleveyttä voidakseen tarjota huippunopeaa palvelua mobiililaitteille. [15, s.10.]



Kuva 1. Moderni tietoliikenneverkko [4, s. 29].

Tellabsin reitittimet on kehitetty ensisijaisesti toimimaan ratkaisuina kuvan 1 kaltaisille moderneille tietoliikenne- ja puhelinverkkoratkaisuille. Yrityksen sivukonttoreista tuleva liikenne reititetään keskusreitittimelle ja sitä kautta välitetään palveluntarjoajan verkon yli kohteeseensa. Data liikkuu palveluntarjoajan verkossa VPN:ssä (Virtual Private Network). Tämä virtuaalinen verkko mahdollistaa, että data liikkuu turvallisesti piilotettuna ulkopuolisilta. Puhelu matkapuhelimella kulkeutuu tukiasemalle. Tukiasema välittää liikkuvan datan virtuaalilinjoja (Pseudowire) pitkin aina RNC:lle (Radio Network Controller) asti. Siitä matka jatkuu runkoverkkoa pitkin toiselle puolelle pilveä aina päämääräänsä asti.

3 Tekniikka

3.1 OSI-malli

Jotta ymmärtäisimme hiukan paremmin käsiteltäviä tekniikoita, on hyvä käydä lyhyesti läpi OSI (Open Systems Interconnection) -malli. Kuvan 2 OSI-malli kehitettiin, että sen puitteissa voitaisiin suunnitella tietoliikennejärjestelmät. Sen kautta on helpompi sisäistää ja erottaa selvästi tekniikoita ja protokollia toisistaan. Malli koostuu seitsemästä kerroksesta (Layer), jotka muodostavat tiedonvälityksen. Malli toimii siten, että ylempi kerros käyttää hyväkseen ainakin yhtä alemman kerroksen palvelua ja

tarjoaa vastaavasti palvelua kerrosta ylemmäksi. Mitä alempi kerros on, sitä alkeellisempi se on. Esimerkiksi seitsemäs eli ylin kerros käyttää hyväkseen kaikkia kuutta alempaa. Seuraavassa käydään läpi lyhyesti alimmat kerrokset 1–4.

Kuva 2. OSI-mallin havainnollistava kuva [2].

Fyysinen kerros

Alin kerros, johon kaikki loogiset, sähköiset ja mekaaniset komponentit liittyvät. Tällä kerroksella voidaan siirtää tietoa kahdella tavalla; sarja- tai rinnakkaismuotoisena. Sarjamuotoisena bittejä siirretään peräkkäin yksi kerrallaan. Rinnakkaismuotoisena siirretään yhden merkin kaikki bitit yhtaikaa omia johtimia pitkin. Hubit ja toistimet toimivat tällä tasolla. [1.]

Siirtoyhteyskerros

Siirtoyhteyskerros tarjoaa luotettavan siirtoyhteyden fyysisen kerroksen kautta. Tarkistussummien avulla siirtoyhteyskerros seuraa siirrettyjen bittien virheettömyyttä. Virheen sattuessa kerros pyytää lähettämään datalohkon uudelleen. Ethernet-verkkokortti ja sen ohjaimen toiminta edustavat siirtoyhteystason ja osin fyysisen kerroksen tehtäviä. Yhteyksiä luodaan niin sanottujen P-P (Point-to-Point) -laitteiden

välille. Esimerkiksi perinteinen puhelin on P-P -väline. Sillat (Bridge) ja kytkimet (Switch) toimivat tällä tasolla. [16, s.25.]

Verkkokerros

OSI-mallin kolmannen eli verkkokerroksen tehtävänä on tarjota riippumaton tiedonsiirto. Riippumaton tiedonsiirto tarkoittaa että tiedonsiirto voidaan toteuttaa fyysisesti monin eri tavoin. Verkko ei näin rajoitu tiettyyn muottiin tai malliin. Nykyään IP:tä (Internet Protocol) voidaan käyttää langallista ja langatonta puhelinlinjaa tai lähiverkkoa hyväksikäyttäen. Jokainen näistä on toteutuksena fyysisesti erilainen. Verkkokerros myös valitsee reitin, jota pitkin tiedon tulee kulkea. Näistä valinnoista huolehtivat reitittimet. IP toimii tällä tasolla OSI-mallissa.

Kuljetuskerros

Kuljetuskerros huolehtii yhteyksistä järjestelmien välillä (Point-to-Point). Kuljetuskerroksella voidaan myös huolehtia virheenkorjaamisesta. Kerros piilottaa alempana toimivat siirtojärjestelmät ylemmiltä. Tällöin se ei olisi niistä riippuvainen, vaan toimisi itsenäisesti. Kuljetuskerros hyväksikäyttää verkkokerroksen palvelua, mikä mahdollistaa pakettien kulkemisen verkoista toiseen läpinäkyvästi. Kerroksen protokollat huolehtivat myös siitä, että paketit saapuvat perille oikeassa järjestyksessä. Mahdollisten ongelmien ilmetessä huolehtii kuljetuskerros vaihtoehtoisen reitin valinnasta tietoliikenteen säilyttämiseksi. TCP (Transmission Control Protocol) ja UDP (User Datagram Protocol) ovat tunnetuimmat protokollat kuljetuskerrostasolla. [1.]

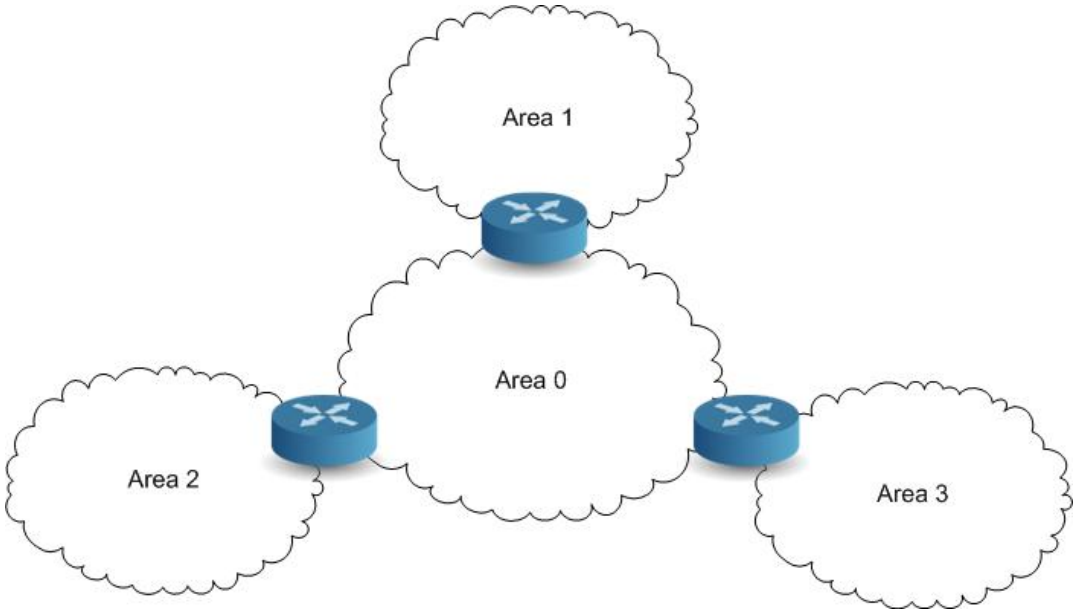
3.2 OSPF-protokolla

OSPF (Open Shortest Path First) on nykyaikana yleisimmin käytetty verkkoprotokolla. OSPF on linkkitila-algoritmiin perustuva reititysprotokolla. [17, s.5.] Sana ”Open” tulee siitä, että sen ominaisuudet ovat julkistettuja ja avoimia kaikille. Näin ollen sen käytöstä ei tarvitse maksaa lisenssimaksuja. Sen kehittäjät ovatkin toivoneet, että protokollan avoimuus auttaa sitä kasvamaan korvaavaksi protokollaksi ohitse patentoitujen yksityisten kehittäjien protokollien. Näin on myös tapahtunut. Toinen

nykyaikana suosittu protokolla on IS-IS (Intermediate System-to-Intermediate System). IS-IS on reititysprotokollana paljon skaalautuvampi, etenkin jos reitittimien määrä alueella on suuri. IS-IS:n vianhaku on yksinkertaisempaa kuin OSPF:n. OSPF on kuitenkin suositumpi protokolla, sillä sen asetukset on hiukan yksinkertaisempi määritellä. [5, s. 279.]

Tyypillinen OSPF -verkko voi koostua useista alueista (area) autonomisen järjestelmän (AS - Autonomous Systems) sisällä [17]. Jokainen OSPF-reititin mainostaa omia linkkitilojaan oman alueensa sisällä. Nämä linkkitilamainostukset sisältävät tietoa reitittimen verkkoliitännöistä sekä reititysmetriikoista. Hinta (cost) on arvo, jota reititin noudattaa valitessaan lyhintä reittiä kohteeseensa. Jokaisella verkkoliitännäisellä on oma arvonsa. Mitä pienempi hinta, sitä parempi reitti on reitittimen silmin. [6, s. 10.]

Reitittimillä, jotka kuuluvat samaan alueeseen, on identtinen linkkitilatietokanta. Ne eivät näe reitittimiä, mitkä ovat alueensa ulkopuolella. Tämä vähentää reititysliikennettä alueen sisällä. Poikkeuksena on niin sanotut aluerajareitittimet (ABR – Area Border Router), jotka ovat osana useampaa aluetta. Niillä on molemmille alueille oma linkkitilatietokanta ja ne huolehtivat kommunikoinnista alueelta toiselle. Jotta tämä kommunikointi olisi mahdollista, ABR mainostaa saavutettavuuttaan toisille alueille. Näitä mainostuksia kutsutaan LSA:ksi (Link-State Advertisement). ABR-reitittimellä on yksi sääntö. Sen pitää olla osana runkoverkkoa. Tämä on alue 0.0.0.0 tai alue 0. Kuvassa 3 alue 0 esittää runkoverkkoa. Runkoverkkoalue huolehtii mainostuksista muille alueille, siksi ABR-reitittimien täytyy olla osana sitä. Muuten tämä ei olisi mahdollista.



Kuva 3. OSPF ABR -reittimet [7].

OSPF-alueita on mahdollisuus määrittää myös eri lailla. Jos reitittimien määrä alueen sisällä kasvaa suureksi, kasvaa myös OSPF-mainostuksien määrä. On mahdollista vähentää näiden mainostusten tuottamaa muistin käyttöä määrittelemällä alue suppeaksi (Stub area). Ulkopuoliset mainostukset eivät näin ollen pääse suppeille alueille. Reititys ulkopuolisille alueille tapahtuu oletusreitin turvin. Toinen erikoinen määrittely on suppeahko-alue (NSSA - Not-So-Stubby Area). NSSA hyväksyy alueen sisäiset reititysmainokset, mutta ei hyväksy ulkoisia reittejä muilta alueilta [6, s.11]. En kuitenkaan käytä näitä edellä mainittuja ominaisuuksia toteutuksessa, sillä laitteiden määrä verkossa ei tule olemaan lähellekään niin runsas. Niiden olemassaolo on kuitenkin syytä mainita. Tämä ei kuitenkaan pois sulje alueiden lisäämistä jälkikäteen.

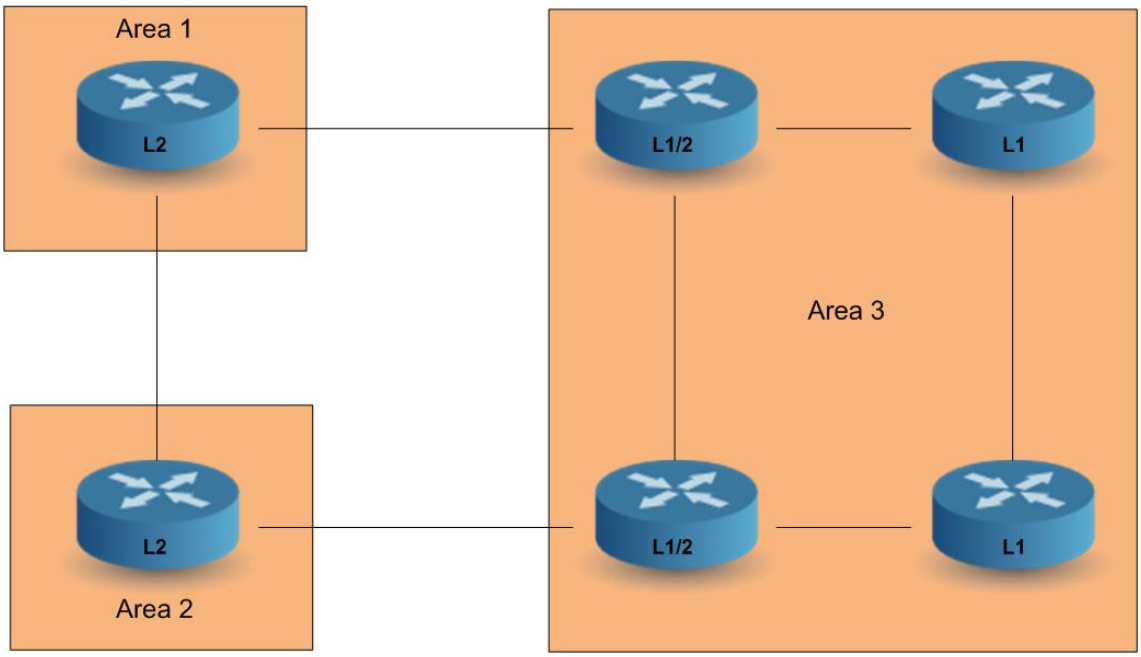
3.3 IS-IS-protokolla

IS-IS on linkkitilaprotokolla OSPF:n tavoin. IS-IS ja OSPF ovat molemmat reititysprotokollia, jotka toimivat AS:n sisällä. Näitä AS:n sisällä toimivia protokollia kutsutaan IGP (Interior Gateway Protocol) -protokolliksi [18]. IS-IS on alun perin määritelty ISO:ssa (International Organization for Standardization) tarjoamaan palveluja ISO:n kuljetusprotokollille ilman riippuvuutta TCP/IP -protokollasta [8.]. IS-IS on OSPF:n tavoin protokolla, jota yleisimmin käytetään sisäverkon tai autonomisen alueen sisällä hoitamaan mainostusta. Vaikka OSPF on yhä yleisimmin käytetty

protokolla, on IS-IS sitä tehokkaampi ja parempi. IS-IS on kykenevä hallitsemaan paljon suurempia aluekokonaisuuksia. Eri arvioihin perustuen on väitetty IS-IS pystyvän hallitsemaan yhden alueen sisällä tuhansia reitittimiä, kun taas OSPF:n tapauksessa määrä on rajoittunut 50—200 reitittimeen. [10.]

IS-IS käyttää kahden alueen reitityshierarkiaa parantaakseen suurten verkkojen skaalautuvuutta. Käytännössä nämä alueet jakaantuvat alueen sisäisiin (ensimmäinen taso) ja alueiden välisiin tasoihin (toinen taso). Reititin voi olla myös molemmilla tasoilla samaan aikaan (ns. tason yksi ja kaksi reititin). Toiminta perustuu siihen, että saman alueen sisälle kuuluvat reitittimet jakavat täyden reititystiedon keskenään ja ovat tietoisia alueensa topologiasta. Hyöty reititystiedon jakamisesta on, että reitittimet osaavat tehdä optimaalisen valinnan reitityksestään alueensa sisällä, kun ne ymmärtävät täyden topologian.

Reitittimet jaetaan eri alueisiin. Ensimmäisen tason mainostukset eivät voi kulkea alueelta toiselle. Toisella tasolla toimiva reititin huolehtii alueiden välisistä mainostuksista. Jokainen ensimmäisellä tasolla oleva reititin voi halutessaan kommunikoida toisella alueella olevan reitittimen kanssa. Tällöin täytyy reitittimen kommunikoida oman alueensa toisen tason reitittimen kanssa, kuten kuvassa 4. Jokaisella alueella on yhteys runkoverkkoon, joka kulkee aina vähintäänkin yhden toisen tason reitittimen kautta. Toisen tason reitittimet muodostavat näin myös oman vaikutusalueensa. [10.]



Kuva 4. IS-IS -tasotopologia [7].

IS-IS vaatii jokaiselta reitittimeltä NSAP-osoitteen (Network Service Access Point), joka koostuu aluetunnuksesta ja systeemitunnuksesta sekä NSAP valitsimesta (NSEL), joka on yhden tavun kokoinen. NSAP -osoitteen maksimipituus on 20 tavua. Reitin puolestaan tunnistetaan verkko-osoitteesta NET (Network Entity Title), joka sisältää aluetunnuksen ja systeemitunnuksesta NSEL:n ollessa asetettuna nollaksi. Ensimmäinen tavu verkko-osoitteesta on ns. AFI (Authority and Format Identifier), joka osoittaa käytetyn osoitealueen.

IP loopback osoite 123.23.123.3
AFI = 49
Alue 1 = 0001
NSEL = 00
=> 49.0001.1230.2312.3003.00

Esimerkkikoodi 1. IS-IS– osoitteen koostumus.

3.4 Multiprotocol Label Switching

MPLS-tekniikka tulee toimimaan pohjana laboratorion IP-perustaiselle verkkoratkaisulle. Nykyaikaiset verkkoratkaisut pohjautuvat MPLS- ja Ethernet-tekniikkaan. Lyhyesti kerrottuna MPLS:n parhaita puolia ovat nopea ja yksinkertainen paketin

välittämiskaava, liikenteenhallintamahdollisuudet eli TE (Traffic Engineering) ja ehkäpä tärkeimpänä palvelunlaadun takaaminen eli QoS (Quality of Service). Useiden eri verkkotekniikoiden tuominen yhteen on myös yksi suuri hienous MPLS-tekniikassa.

MPLS on nykyaikainen menetelmä, jolla voidaan kuljettaa paketteja nopeasti runkoverkon reitittimien kautta. Kuljetukseen MPLS käyttää leimoja. Tämä nopeuttaa huomattavasti toimintaa. Runkoverkon reitittimet pitävät yllä reititystaulujaan. Aina kun runkoverkkoon liitetään uusi reititin, päivittyvät reitittimien taulut. Vain siten reitittimet tulevat tietoisiksi toisistaan sekä uusista reitittimistä. Asiakkaan uuden tai uusien reitittimien liittäminen vaatii reititintaulujen päivityksen. Tämä reititystietojen päivitys tietenkin kuormittaa verkkoa turhaan. MPLS mahdollistaa, että runkoverkon reitittimet eivät saa näitä päivityksiä. Idea on, että MPLS runkoverkon ei tarvitse olla tietoinen sen ulkopuolelle olevien reitittimien reitityksistä. Runkoverkko huolehtii omasta topologiastaan. Runkoverkkoa kuvataankin yleensä pilvenä. Pilven sisällä olevien laitteiden määrä ja tekniikka on asiakkaan näkökulmasta tuntematon. Näin asiakkaan oma verkko voi muuttua, lisääntyä tai kutistua runkoverkon siitä välittämättä.

Ennen MPLS:ää reitittimiltä vaadittiin ominaisuutta reitittää paketteja useilta eri protokollilta. Tästä johtuen lähes jokainen paketti saattoi olla koostumukseltaan erilainen, mikä tarkoittaa vaihtelevaa kenttien sijoitusta pakettien otsakkeissa (eng. Header). Erilaisten pakettien käsittely taas hidastaa pakettien välittämistä eteenpäin. MPLS-tekniikka perustuu nimensä mukaisesti useamman protokollan tukemiseen samanaikaisesti. MPLS:n etuna on, että eri tekniikoihin pohjautuvia verkkoja voidaan yhdistää kätevämmin kuin ennen. MPLS tukee seuraavia tekniikoita: Frame Relay, ATM (Asynchronous Transfer Mode), TDM (Time-Division Multiplexing), sarjalinkkejä, POS (Packet Over SDH/SONET) ja Ethernet VLAN (Virtual Local Area Network). Tämän ansiosta operaattorit voivat huoletta yhdistää eri tekniikoilla toteutettuja verkkoja ongelmitta. Nykyaikana Ethernet on yleisin käytettävistä tekniikoista. Samaisesta syystä tulee se olemaan pääosassa yrityksen verkossa.

Ohjauskomponentin (Control component) tehtävä on vaihtaa reititysinformaatiota muiden verkkoelementtien eli reitittimien kanssa. Jokainen reititin kerää itselleen tästä informaatiosta tietoa, jonka se tallentaa omaan tietokantaansa. Kun tieto on kerätty tietokantaan, luo reititin tästä tiedosta reititystaulun. Reititystaulun tarkoitus on

kartoittaa verkko reitittimen silmistä katsottuna. Reititystaulun avulla reititin pystyy päättelemään parhaan mahdollisen reitin mihin tahansa saatavilla olevaan kohteeseen. Kun paketti saapuu reitittimelle, sillä on otsake, joka sisältää sen lähteen, kohteen ja muuta informaatiota. Reitittimen tehtävänä on päättää, mihin porttiin tai portteihin se välittää saapuneen paketin. Välityskomponentti (Forwarding component) tutkii paketin kohteen osoitteen. Se vertaa osoitetta välitystietokannan (Forwarding database) tietoihin ja tekee sen mukaan päätöksen paketin ohjaamisesta.

MPLS on rakennettu siten, että siinä selvästi erotettu hallinta- ja välitysominaisuudet verrattuna aikaisempiin ratkaisuihin. Näin molemmista saadaan yksilölliset edut käyttöön kätevimmin. Nämä kaksi MPLS:n ominaisuutta pohjautuvat IP:n protokolliin, joihin kuuluu muun muuassa IP, RSVP (Resource Reservation Protocol), BGP (Border Gateway Protocol) ja OSPF (Open Shortest Path First).

MPLS -verkko toteutetaan LSR (Label Switched Router) -reitittimillä, jotka toimivat verkon runkona. MPLS LSR:n tehtävänä on huolehtia informaation vaihdosta muiden LSR:ien kanssa ja päivittää nämä tiedot reititystauluihin. Reititys perustuu leimoihin (label), mitä käytetään OSI-mallin toisella kerroksella. Se kuinka reitittimet vaihtavat näitä leimoja tapahtuu LDP:n (Label Distribution Protocol) avulla. LDP on ehkä tärkein protokolla liittyen MPLS:ään. LDP määrittelee prosessin ja viestit jolla yksi LSR viestittää toista LSR:ää siihen sidotuista leimoista. Näin leimat pysyvät uniikkeina ja eivät voi mennä sekaisin keskenään. LDP:stä lisää myöhemmin. Jokaisen naapurireitittimen välille luodaan oma LDP-istunto mikä mahdollistaa leimojen vaihdon. Yksinkertaisesti sanottuna edellä mainittu prosessi mahdollistaa, että LSR:t luovat LSP:t (Layer Switched Path). [3, s. 147–149.]

Leimanjakoprotokolla (LDP)

LDP on istuntoon pohjautuva protokolla, joka käyttää TCP:tä leimojen jakamiseen. LDP on yleisin leimanjakoprotokollista, sillä se on IETF:n (Internet Engineering Task Force) standardoima. Kättelymekanismi, joka pohjautuu UDP:een, luo automaattisesti istunnot fyysisesti kahden LSR:n välille. Kun istunto on luotu, jakaa LDP leimat, joko pyytämättömästi tai pyydettäessä. [11, s. 18.]

Prosessi toimii siten, että LDP lähettää hello-viestejä käyttäen UDP-porttia 646 kaikille naapureille ryhmälähetysosoitteeseen 224.0.0.2. Reitittimen tunniste-osoite on Router-ID, joka on liitettynä tähän viestiin. Näin reititin aloittaa naapuruussuhteiden luonnin. Vastaanottaja kuittaa tämän viestin. TCP-protokolla (portti 646) aloittaa naapuruussuhteen luonnin. Vastaus lähetetään yksittäislähetyksenä, eli vastaanottaja on tietty reititin (hello-viestin lähettäjä). Naapuruuden syntyessä aloitetaan leimojen mainostus. [12, s. 83.]

Resurssienvarausprotokolla (RSVP-TE)

RSVP-TE on kuljetusprotokolla, jolla varataan leimoja sekä kaistanleveyttä verkkoreitillä. MPLS-arkkitehtuuri ei määrittele vain yhtä protokollaa leimojen jakamiseen. RSVP on yksi leimojen jakamisen mahdollistava protokolla [13.1]. RSVP-TE (Traffic Engineering) on lisäosa normaaliin RSVP-protokollaan. TE yhdistää mukaan ”IntServ” (Integrated Services) QoS:n, tarkemmin sanottuna liikennetyypit, joille varataan palvelua. RSVP-TE LDP:stä poiketen pyytää aina leimoja.

RSVP -protokollaa käytetään varaamaan tietynlaisia palveluita verkolta. Nämä palvelut voivat olla esimerkiksi datavoita (data stream). RSVP:tä käytetään myös välittämään QoS-pyyntöjä kaikilta reitittimiltä polun varrelta (LSP). Näin se pystyy varaamaan tarvittavat resurssit palveluilleen. RSVP ei itsessään ole reititysprotokolla, ja se toimii IP:n yläpuolella. [22.]

RSVP-TE käyttää tunneleita LSP:n yli. Tunneli on virtuaalinen linkki, mikä tarkoittaa sitä, että vaikka kahden reitittimen välissä olisi useampia reitittimiä, eivät nämä näy. Tunneli näkyy käyttäjälle aivan kuin reitittimet olisivat fyysisesti vierekkäin liitetty.

Välitysekvivalenssiluokka (FEC)

Reitittimen päätehtävä on reitittää liikennettä kohti sen lopullista kohdetta. Lopullisen kohteen reititin pystyy päättelemään sen reititystaulusta. Reititystaulu taas muodostuu datasta, jonka reitittimen ohjaustaso (control plane) sille ohjelmoi. FEC (Forwarding Equivalence Class) on ryhmä IP-paketteja, jotka välitetään samalla tavalla. Toisin

sanoen kaikki IP–paketit, jotka kulkevat samaa reittiä läpi MPLS-verkon ja saavat saman kohtelun jokaisella reitittimellä, kuuluvat saman FEC:iin. [19, s. 3.]

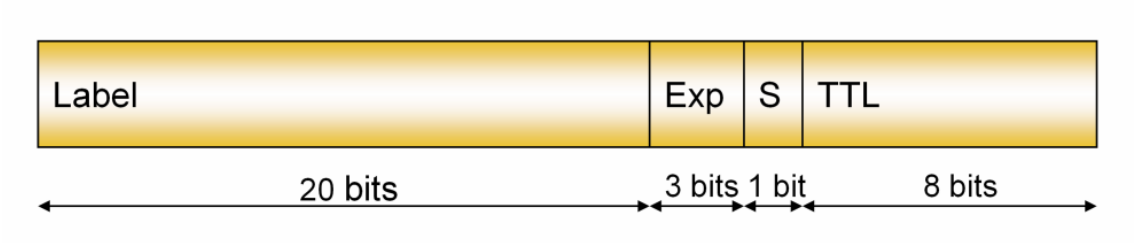
Aina kun dataa välitetään reitittimeltä toiselle, tapahtuu niin sanottu hyppy. Hypyn vastaanottavaa reititintä kutsutaan next-hop -reitittimeksi. Reitittimille muodostuu käytännössä useita FEC:jä, ja niille luodaan oma taulu. FEC -taulusta voidaan nähdä, mihin kaikkialle liikennettä välitetään, sillä se sisältää kohde IP -osoitteen. [3, s. 149.]

Leima

MPLS:llä on oma leima mikä tulee toisen kerroksen sekä kolmannen kerroksen väliin. Toisen kerroksen otsake merkitsee käytettävän verkkoprotokollan, esimerkiksi Frame Relay. Kolmas kerros puolestaan on vastuussa pakettien kuljettamisesta päätelaitteiden välillä [4, s.15]. MPLS-leiman pituus on 32 bittiä, ja se koostuu neljästä osasta, kuten kuvasta 5 nähdään.

Leima koostuu seuraavista osista:

- Leima (label) on pituudeltaan 20 bittiä. Se sisältää todellisen arvon. Leimasta nähdään nopealla vilkaisulla seuraava hyppy sekä muut mahdollisesti suoritettavat operaatiot (käydään läpi tarkemmin kappaleessa 3.4.6).
- Exp (Experimental) on pituudeltaan kolme bittiä, jotka on varattu kokeilukäyttöön. Tällä hetkellä aluetta käytetään merkkaamaan erilaisia QoS (Quality of Service) -arvoja.
- S (Bottom of Stack) on pituudeltaan yksi bitti, jolla ilmaistaan onko leima viimeinen. Arvon ollessa yksi (”1”) tiedetään leiman olevan pakan viimeinen.
- TTL (Time to Live) on pituudeltaan kahdeksan bittiä, mikä merkitsee hyppyjen maksimimäärän MPLS-verkossa. Jokainen hyppy vähentää TTL:n arvoa yhdellä. TTL:n saavuttaessa arvon nolla (”0”) leima poistetaan, eikä pakettia enää välitetä. [20.]



Kuva 5. MPLS-leiman koostumus [4, s. 13].

Leimapino

Verkossa kulkevat paketit voivat kuljettaa useampaa leimaa mukanaan. Leimat pinotaan päällekkäin. Käytännössä tämä tarkoittaa, että leimat laitetaan järjestykseen LIFO- (Last In First Out) periaatteella. Näin pinon päällimmäinen leima tutkitaan verkon solmupisteissä. Pinon päällimmäinen leima on siis ainoa, jonka MPLS LFIB (Label Forwarding Information Base) käsittelee muiden leimojen ollessa pinossa sen alapuolella. Jokainen pakan leima koostuu neljästä oktetista ja sisältää 32 bittiä dataa, kuten kuvasta 5 voidaan nähdä. [3, s. 150.]

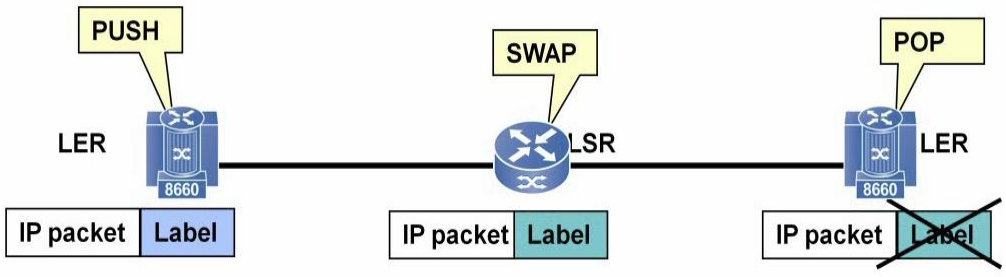
Leimojen vaihto

MPLS-välitystaso (forwarding plane) on vastuussa liikenteen välittämisestä MPLS-verkossa. Tähän se käyttää 20-bittistä leimaa kuten kuvassa 5. Tämä leima on aina lyhyt, kooltaan samankokoinen ja rakenteeton. Leimalla on merkitystä vain kahden LSR:n välillä, muutoin se on merkityksetön. Tästä johtuen samaa leimaa voidaan käyttää uudelleen. Jotta MPLS LSR voisi vaihtaa leimoja, täytyy sen tunnistaa tulevan paketin leima. Tulevan leiman täytyy täsmätä LSR:n tulo-otsakkeeseen, joka on määritelty LFIB:ssä. Kun leima on tunnistettu, LSR:n välitystaso tekee päätöksen paketin uudelleenohjaamisesta tai välityksestä. MPLS-verkon reunoilla LSR yhdistää IP-paketit FEC:ksi hallintatason toimesta. Kun FEC näille paketeille on luotu, voi välitystaso luovuttaa sen FEC:lle antaen sille MPLS-leiman.

Koska useammat paketit eri lähteistä käyttävät samaa FEC:iä, saavat ne myös saman MPLS-leiman. Niillä on siis yhteinen next-hop–reititin, jonka kautta ne kulkevat. Nyt paketeilla on leima, joka on liitetty niihin. Pakettien saapuessa next-hop -reitittimelle

tutkii se niihin liitetyn leiman. Se vertaa tulevaa leimaa LFIB:n tietoihin ja löytää sille lähtevän leiman. Nyt reititin poistaa olemassa olevan saapuvan leiman ja laittaa tilalle uuden lähtevän leiman. Tämä uusi lähtevä leima kertoo jälleen seuraavan next-hop -reitittimen ja lähettää paketit kohti sitä. Tätä periaatetta seuraten paketit löytävät lopulta perille. Paketin päästyä perille reititin poistaa paketeilta MPLS-leiman, ja paketti jatkaa matkaa normaali reitityksen mukaan.

Seuraavaksi käydään läpi itse leimojen merkkaus- ja vaihtamisprosessia tarkemmin. Niitä on kolme ”push”, ”pop” ja ”swap”. Push eli ”työntöä” käytetään aina, kun paketille halutaan antaa MPLS-leima. Tämä tapahtuu aina, kun paketti halutaan liittää MPLS-verkkoon. Paketti saapuu verkon reunalle ja reitin huomaa, että sen tiedot täsmäävät tietyn FEC:n kanssa. Paketti saa MPLS-leiman, ja se ”työnnetään” pakettiin. Aina kun leima työnnetään pakettiin, siirtyvät kaikki muut mahdolliset leimat yhden järjestysnumeron alaspäin pakassa. Lähettävän reitittimen silmin paketilla on nyt lähtevä leima push-operaatiolla. Push-operaatiota käytettäessä on LFIB:ssä vain lähtevä leima. Saapuessaan next-hop -reitittimelle käy reititin läpi tulevat leimat. Kun täsmäävä leima löytyy, ja tässä esimerkissä paketin on tarkoitus jatkaa matkaansa, suoritetaan vaihto-operaatio ”swap”. Reitittimen tehtävä on siis vaihtaa sille uusi leima, kuten kuvassa 6. Swap-operaatio tarkoittaa sitä, että reitittimellä on LFIB:ssä tuleva ja lähtevä leima erikseen. Saapuva leima vaihdetaan lähtevään. Pinon koko ei muutu missään vaiheessa, vaikka leimoja vaihdetaan, vaan se pysyy aina samana. Paketti lähetetään matkaan. Paketin saapuessaan päämääräänsä reititin tarkistaa saapuvan leiman ja huomaa, että sille on pop-operaatio. LFIB:ssä on siis vain saapuva leima. Tämä tarkoittaa, että paketti on saapunut perille, ja pop-operaatio poistaa MPLS-leiman kokonaan. Paketti jatkaa matkaansa normaalin reitityksen mukaan. [19.]



Kuva 6. Leimojen merkkaus- ja vaihtoprosessi [4, s. 19].

3.5 Virtuaalinen yksityisverkko

VPN (Virtual Private Network) eli virtuaalinen yksityisverkko on nykyisin yleisesti käytettävä verkkoratkaisu etenkin yrityskäytössä. VPN:llä voidaan yhdistää yrityksien eri toimipaikoissa sijaitsevia verkkoja. Käytännössä tämä tarkoittaa, että käytetään jonkin toisen (tässä tapauksessa operaattorin) tarjoamaa verkkoa, jossa ylitse VPN-yhteys toteutetaan. Tätä toisen yrityksen verkkoa kuvataan yleisesti pilvenä. Sen sisältö on tuntematon ulkopuolisille. Sillä ei ole väliä. Riittää se, että tiedetään sen toimittavan haluttu data pilven yli turvallisesti. VPN:stä puhuttaessa käytetään reitittimistä termejä PE (Provider Edge) ja CE (Customer Edge). PE-reitittimellä tarkoitetaan operaattorin runkoverkkoon liittävää reititintä. CE puolestaan on asiakkaan reititin, joka liitetään operaattorin PE-reitittimeen. PE-reitittimien muodostaman runkoverkon kautta asiakas saavuttaa yhteyden CE-reitittimiensä välille. [11.]

Kolmostason VPN

Kolmostason VPN:ssä palveluntarjoaja käyttää IP-runkoverkkoa tarjotakseen IP VPN -yhteyksiä asiakkailleen. Asiakkaiden CE-reitittimet mainostavat reitityksiään palveluntarjoajan PE-reitittimille. PE-reitittimellä on asiakkaille oma VRF (VPN Routing and Forwarding) -reititystaulu. VRF on tekniikka, joka mahdollistaa usean erillisen reititystaulun käytön PE-reitittimissä. VRF voidaan ajatella virtuaalisena reitittimenä fyysisen reitittimen sisällä. BGP -protokolla välittää nämä reititykset palveluntarjoajan PE-reitittimien läpi. [11.]

Kakkostason VPN

Kakkostasolla on kahta VPN-tyyppiä: VPWS (Virtual Private Wire Service) ja VPLS (Virtual Private LAN Service). VPWS on P-to-P -palvelu, VPLS:n ollessa palvelu mikä simuloi LAN:ia yli WAN:in (Wide Area Network). Molemmissa tapauksissa CE-reititin liitetään PE-reitittimeen joko loogisella tai virtuaalisella liitännällä VC (Virtual Circuit). Tämä liitäntä voi olla esimerkiksi Ethernet-portti, VLAN tai ATM VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier). Virtuaalilinjoja käytetään kuljettamaan liikennettä läpi PE-reitittimien. [21.]

3.6 Virtuaalilinja

Virtuaalilinja (Pseudowire) on mekanismi, jolla voidaan siirtää palveluja (tässä tapauksessa Ethernet, ATM, FR, TDM tai HDLC- (High-Level Data Link Control) liikennettä) pakettikytkentäverkon (PSN - Packet Switched Network) läpi. Virtuaalilinjat toimivat siirtokerroksella (tasolla kaksi OSI-mallissa), ja voivat kuljettaa läpi käytännössä melkein mitä tahansa liikennettä. Virtuaalilinjoja voidaan luoda kahden reitittimen välille tai läpi kokonaisen verkon.

MPLS-verkossa virtuaalilinjaa varten tarvitaan kaksi leimaa, jotta voidaan välittää virtuaalilinjoja. Oletetaan, että asiakkaalla on kaksi eri toimistoa eri kaupungeissa. Kummassakin toimistossa on asiakkaan oma CE-reititin, joka huolehtii heidän liikenteestään. Kumpikin asiakaslaite on kytkettynä operaattorin laitteisiin niin sanottuun reunareitittimeen. Reunareitittimen tarkoitus on kuljettaa liikennettä läpi operaattorin oman runkoverkon, aina kohteeseensa asti. Pakettiin lisätään ensimmäinen leima, joka on sisäinen leima, virtuaalilinjan leima. Tämä leima nimeää ja ohjaa liikenteen oikeaan määränpäähänsä, joka on verkkoliitäntä. Tämä tapahtuu reunareitittimen asiakaslaitteeseen päin olevalla liitännällä. Pakettiin lisätään toinen leima, ulkoinen leima, jota kutsutaan PSN-leimaksi. PSN-leima tulee sisäisen leiman eteen merkkaamaan seuraavaa PE-reititintä. Näin paketti kulkee läpi operaattorin runkoverkon. Perillä toisella reunareitittimellä ulkoinen leima poistetaan, jolloin reunareititin ohjaa paketin sisäisen leiman perusteella kohti oikeaa asiakaslaitteen liitäntää. Asiakaslaitteessa sisäinen leima poistetaan ja itse paketti voidaan välittää asiakkaan omassa verkossa kohteeseensa. Koko prosessi kulki läpi operaattorin MPLS-verkon nopeasti ja vaivattomasti. [21.]

4 Toteutus

Rakennetun verkon tulisi tukea työntekijöitä työssään ongelmien ratkaisemisessa. Tarkoitus on rakentaa verkko, johon on helppo nopeasti pystyttää työntekijöiden haluamia palveluita. Näillä palveluilla voidaan simuloida mahdollisia ongelmia, joita

asiakkaat kohtaavat. Tämä vaatii, että verkko on tietyssä perustilassa, jotta näitä palveluita voidaan kätevästi pystyttää.

Nyt käydään läpi itse verkon rakentaminen reitittimillä. Reitittimet on koottu reititinkaappeihin ja yhdistetty toisiinsa verkkotopologian mukaisesti. Reitittimet, joihin asetukset laitetaan, kuuluvat kaikki Tellabsin 8600 -tuoteperheeseen. Käytettävät reitittimet ovat malleiltaan seuraavat: 8660, 8630, 8620, 8607 ja 8605.

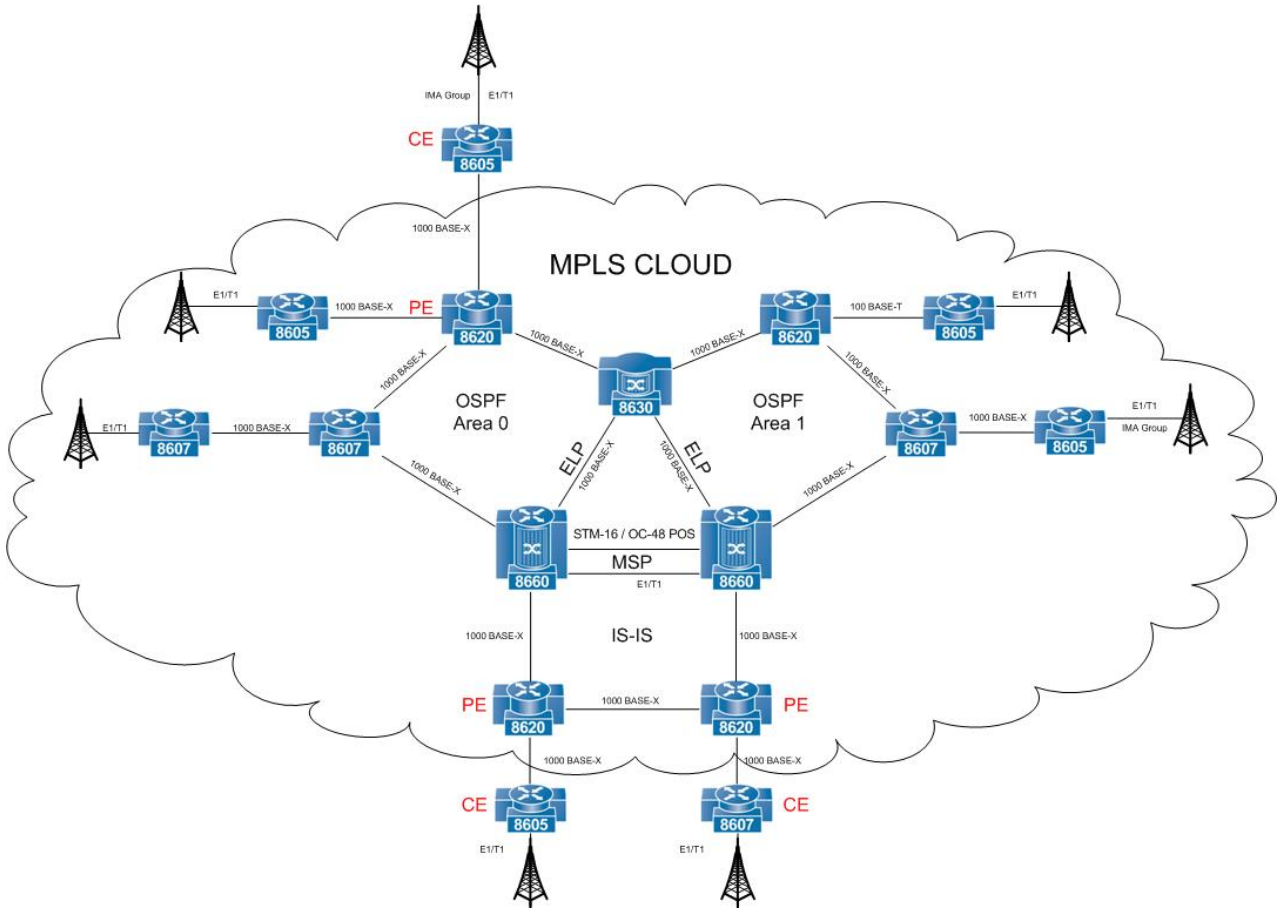
8660 on Tellabsin 8600 -tuoteperheen lippulaiva. Se pystytään varustamaan yhteensä 14 linjakortilla, joista kaksi on ohjauskortteja, jotka huolehtivat kaikista reitittimen toiminnoista. Käytännössä 12 jäljelle jäävää korttipaikkaa voidaan varustaa erilaisilla moduuleilla. Yhteen korttipaikkaan mahtuu kaksi moduulia. Moduuleja on erilaisia erilaisiin verkkoratkaisuihin [4, s. 7]. 8600:n käyttötarkoitus on olla keskitettynä suurelle määrälle liikennettä ja välittää tämä liikenne eteenpäin, oli se sitten 2G- (Second Generation) tai 3G (Third Generation) -liikennettä. Hallitut Ethernet- sekä IP VPN -palvelut ovat myös reitittimen suunniteltuja päätehtäviä. Laboratorioverkossa tämän tyypin reitittimet toimivat eri protokollien välisillä alueilla (esimerkiksi OSPF-alue 0 ja 1), kuten kuvassa 3. [4, s. 4.]

8630 on 8660:n pikkuveli. Se on ominaisuuksiltaan täysin identtinen reititin 8660:n kanssa. Ainoa ero on linjakorttien määrä. 8630 sisältää isonveljensä tavoin kaksi ohjauskorttia, mutta linjakortteja siinä on neljä. Tätä reititintyyppiä käytetään verkoissa yleensä keskittämällä liikennettä tehokkaammin kohti 8660:ta. Myös jos tarve on pienempi, voi se korvata täysin isoveljensä 8660:n.

8620 on jo pienemmän kokoluokan reititin, ja se voidaan varustaa kahdella moduulikortilla. Näin siitä on helppo tehdä tarkoitukseen soveltuva kustannustehokkaasti. 8607 ja 8605 ovat pienimpiä Tellabsin valmistavia MPLS/IP-kykeneviä reitittimiä. Niitä käytetään yleensä välittämään liikennettä tukiasemilta (Node B) kohti runkoverkkoa.

Verkon sisältö käydään läpi seuraavaksi. Jotta verkko olisi mahdollisimman monipuolinen, jaetaan se eri protokollien verkkoalueisiin (esim. OSPF-alue yksi ja kaksi), jotka on toteutettu eri verkkotekniikoilla, pääasiassa kuitenkin Ethernetillä, sillä

se on nyt ja tulevaisuudessakin dominoiva tekniikka. Alueita erottaa luonnollisesti reititin. Molemmat verkot ovat muodoltaan rengasverkkoja. Verkkotopologia voidaan nähdä kuvasta 7.



Kuva 7. Laboratorion topologia [7].

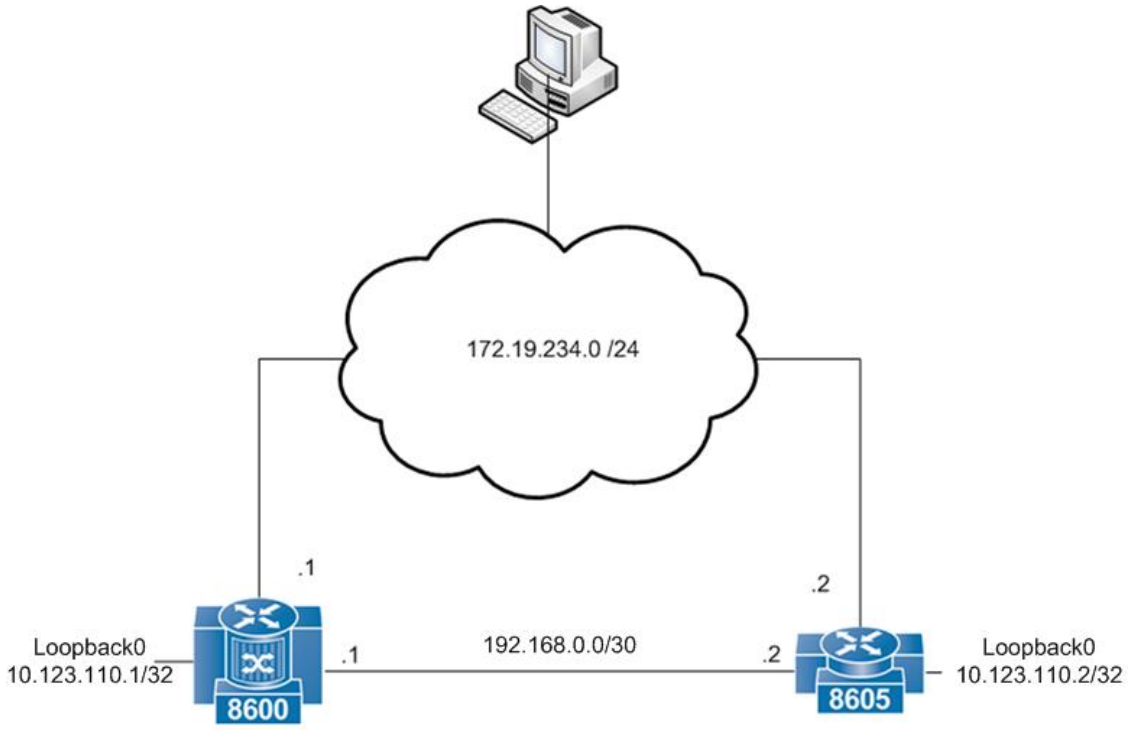
Tellabsin tuotteet mahdollistavat verkkoliitännän turvaamisen. Tämä on Tellabsin oma patentti. ELP (Ethernet Link Protection) huolehtii Ethernet-verkkoliitäntöjen turvaamisesta ja MSP1+1 (Multiplex Section Trail Protection) käytännössä muiden tekniikoiden turvaamisen. Esimerkkinä voidaan ajatella fyysisen kaapelin katkeamista, tai jotain muuta tilannetta mikä saa linkin menemään alas. Tällöin varmistava verkkoliitäntä aktivoituu ja ottaa ohjat käsiinsä, turvaten näin, että liikenne ei katkea. Todellisuudessa liikenteeseen tulee alle 50 millisekunnin katkos. Tarkoitus ei ole käyttää verkkoliitännän turvaamista jokaisessa verkkoliitännässä, vain tietyissä. Näin saadaan realistinen ympäristö turvaamisominaisuuden testaamiseen. Verkkoliitäntöjen turvaaminen on käytännössä helpointa Tellabsin tuotteilla joissa on linjakortteja. [23.]

Pääasiassa kaikki reitittimet ovat MPLS -pilven sisällä. Pilven ulkopuolelle on myös jätetty reitittimiä, verkon monipuolisuuden takia. Yleisesti kuitenkin asiakasverkoissa kaikki kuuluvat pilven sisälle. CE-reitittimen jättäminen pilven ulkopuolelle mahdollistaa kätevästi kolmannen tason VPN-yhteyden simuloinnin MPLS-pilven läpi. Kuvan 7 mastoilta on mahdollista luoda virtuaalilinjoja tai tunneleita verkossa yli toisille mastoille. Tämä toteuttaa toisen tason VPN:n toteuttamisen.

MPLS-leimojen jakaminen on mahdollistettu jokaisessa verkkoliitännässä MPLS-pilven sisällä ottamalla käyttöön myös RSVP-TE -protokolla. Näin tunnelien luominen RSVP-TE:tä käyttäen on mahdollista.

4.1 IP-osoitteet

IP-osoitteita, eli verkko-osoitteita en ole käyneet työssä sen enempää läpi. On kuitenkin tärkeää tietää osoitteet jotka verkkoliitännöille on jaettu. IP-osoitteita jaetaan kolmelle eri alueelle. Enempää ei tarvita. Alueet ovat hallinta-alue, loopback-alue sekä itse verkkoliitännälle jaettavat osoitteet. Kuvasta 8 voidaan nähdä, kuinka nämä alueet muodostuvat. Pilveä kuvaa tässä tapauksessa hallintaverkko.



Kuva 8. Verkko-osoitteita [7].

Hallinta-alueelle olen antanut yrityksen omasta sisäverkosta johtuen verkko-osoitteen 172.19.234.xx/24. Jokainen reititin siis saa yhden verkko-osoitteen tuolta alueelta, jotta niitä voidaan hallita. Tähän sinänsä en voi vaikuttaa, sillä yrityksen omaa lähiverkkoa hallinnoi IT-osasto.

Loopback-alue on alue, joka asetetaan jokaiselle reitittimelle erikseen. Tämä verkko-osoite voidaan käsittää virtuaalisena verkkoliitäntänä reitittimellä. Muut verkkoliitännät pääsevät siihen käsiksi reititysprotokollien avulla. Vaikka se on siis fyysisten käyttöliittymien saavutettavissa, on se kuitenkin täysin virtuaalinen. Osoitealueeksi on valittu 10.123.110.xx/32. Taulukosta 1 nähdään reitittimien loopback-osoitteet. Aliverkko voisi olla myös 24-bittinen, jolloin se kuvaisi saavutettavaa verkkoa.

Taulukko 1. Reitittimien nimet sekä virtuaaliverkkoliitännät. [7]

NODE (Hostname)	Loopback
HOT8660-1	10.123.110.1
HOT8660-2	10.123.110.2
HOT8630-1	10.123.110.3
HOT8620-1	10.123.110.4
HOT8620-2	10.123.110.5
HOT8620-3	10.123.110.6
HOT8620-4	10.123.110.7
HOT8605-1	10.123.110.8
HOT8605-2	10.123.110.9
HOT8605-3	10.123.110.10
HOT8605-4	10.123.110.11
HOT8605-5	10.123.110.12
HOT8607-1	10.123.110.13
HOT8607-2	10.123.110.14
HOT8607-3	10.123.110.15
HOT8607-4	10.123.110.16

Verkkoliitännöille jaetaan 30-bittisiä osoitteita verkosta 192.168.0.0 alkaen. Tämä on yleinen käytäntö runkoverkoissa. Taulukosta 2 voidaan nähdä verkkoliitäntöjen osoitteet. 30-bittinen aliverkonpeite tarkoittaa, että yhtä verkkoa kohti voi olla kaksi verkkoliitäntää. Näin säästetään IP-osoitteita turhalta käytöltä, se myös helpottaa suunnittelua.

Taulukko 2. Verkkoliitännäisten IP-osoitteet [7].

End-point 1	End-point 2	IP (End 1)	IP (End 2)	Network
8660-1	8660-2	192.168.0.1 / 30	192.168.0.2 / 30	192.168.0.0 / 30
8660-1	8630-1	192.168.0.5 / 30	192.168.0.6 / 30	192.168.0.4 / 30
8660-2	8630-1	192.168.0.9 / 30	192.168.0.10 / 30	192.168.0.8 / 30
8660-1	8607-2	192.168.0.13 / 30	192.168.0.14 / 30	192.168.0.12 / 30
8660-2	8607-3	192.168.0.17 / 30	192.168.0.18 / 30	192.168.0.16 / 30
8607-2	8620-1	192.168.0.21 / 30	192.168.0.22 / 30	192.168.0.20 / 30
8607-3	8620-2	192.168.0.25 / 30	192.168.0.26 / 30	192.168.0.24 / 30
8620-1	8630-1	192.168.0.29 / 30	192.168.0.30 / 30	192.168.0.28 / 30
8620-2	8630-1	192.168.0.33 / 30	192.168.0.34 / 30	192.168.0.32 / 30
8660-1	8620-3	192.168.0.37 / 30	192.168.0.38 / 30	192.168.0.36 / 30
8660-2	8620-4	192.168.0.41 / 30	192.168.0.42 / 30	192.168.0.40 / 30
8620-3	8620-4	192.168.0.45 / 30	192.168.0.46 / 30	192.168.0.44 / 30
8620-1	8605-4	192.168.0.49 / 30	192.168.0.50 / 30	192.168.0.48 / 30
8620-1	8605-1	192.168.0.53 / 30	192.168.0.54 / 30	192.168.0.52 / 30
8620-2	8605-2	192.168.0.57 / 30	192.168.0.58 / 30	192.168.0.56 / 30
8607-2	8607-1	192.168.0.61 / 30	192.168.0.62 / 30	192.168.0.60 / 30
8607-3	8605-3	192.168.0.65 / 30	192.168.0.66 / 30	192.168.0.64 / 30
8620-3	8605-5	192.168.0.69 / 30	192.168.0.70 / 30	192.168.0.68 / 30
8620-4	8607-4	192.168.0.73 / 30	192.168.0.74 / 30	192.168.0.72 / 30

4.2 Hallinta

Reitittimien käyttöliittymänä toimii CLI (Command Line Interface), joka toiminnaltaan muistuttaa Ciscon vastaavaa. Tällä käyttöliittymällä reitittimiin asetetaan kaikki asetukset. Reitittimen asetuksista esittelen rivit, jotka näkyvät laitteen käynnissä olevassa konfiguraatiossa. Konfiguraatio saadaan näkyviin antamalle laitteelle näyttökomentoja. Esimerkiksi ”show running-config” antaisi näytölle listauksen kaikesta reitittimen sisällä olevista asetuksista. Näkymää voi myös rajata, jos tiedetään etsittävä kohde, kuten esimerkkikoodissa 2.

```
HOT8660-1#show running-config | block hostname
hostname HOT8660-1
```

Esimerkkikoodi 2. Haun rajaus.

Ainoa tapa saada yhteys konfiguroimattomaan reitittimeen on yhdistää PC sarjaporttiin. Reitittimien hallintakortti eli CDC (Control and DC Power Card) sisältää sarjaportin ja Ethernet-verkkoportin. Kortti myös syöttää virtaa reitittimille. Konsoli-portin kautta laitteisiin asetetaan hallinnointi-IP, jonka jälkeen laite liitetään kytkimeen. Kytkin liittää laitteen yrityksen sisäiseen verkkoon. Näin laitteet ovat hallittavissa yrityksen sisäverkossa. Näin laitteet ovat saavutettavissa ilman, että tarvitsee välttämättä olla fyysisesti laboratoriossa. Hallintaverkko on täysin erillinen verkko kuin se verkko, jota itse laitteet simuloivat. Reitittimiin pääsee myös käsiksi esimerkiksi etäyhteydellä. Tämä tietenkin tarvitsee erillisen VPN-yhteyden yrityksen sisäverkkoon.

Hallintaverkko on 24-bittinen, ja sen verkkotunnus on 172.19.234.0. Hallinta IP asetetaan esimerkkikoodi 3:n mukaisesti. Samalla asetetaan staattinen reititys kommunikointipalvelimelle.

```
HOT8660-1#show running-config | block mfe14
interface mfe14/0
   no shutdown
   ip address 172.19.234.1/24
   qos mapping enable

HOT8660-1#show running-config | block "ip route"
ip route 172.19.0.0/16 172.19.234.254

HOT8660-1#ping 172.19.234.254
PING 172.19.234.254 (172.19.234.254): 40 data bytes
68 bytes from 172.19.234.254: icmp_seq=1 ttl=128 time=1 ms
```

Esimerkkikoodi 3. Hallintaverkon luominen.

Tästä eteenpäin reitittimeen saa yhteyden sen Ethernet-hallintaporttiin, joka tässä tapauksessa on MFE14/0 (Management Fast Ethernet).

4.3 Reitittimen perusasetukset

Nyt kun reititin on hallittavissa, on aika aloittaa sen perusasetuksien asentaminen. Reitittimelle täytyy tehdä inventaario, jos reititin on täysin uusi tai sen komponentit ovat vaihtuneet. Inventaario lisää kaikki komponentit reitittimen käyttöjärjestelmään. En käy sen enempää läpi inventaariota, kuin että se täytyy tehdä ennen käyttöä. Ilman fyysisten komponenttien muutosta sitä ei tarvitse enää tehdä.

Seuraavaksi määritellään reitittimelle nimi. Reitittimen nimestä tulee selvitä, minkä tyypin reitittimessä käyttäjä on, sekä sen järjestysnumero. Tämä ei ole pakollinen toimenpide, mutta helpottaa ja auttaa ymmärtämään paremmin mitä reititintä ollaan käyttämässä. Tästä voi olla apua virheiden välttämiseksi. Reititinnimi asetetaan esimerkkikoodi 4:n tavoin.

```
router#configure terminal
router(config)#hostname HOT8660-1
HOT8660-1(config)#
```

Esimerkkikoodi 4. Reititinnimen asettaminen.

4.4 Loopback ja router-id

Seuraavaksi määritellään reitittimelle niin sanottu loopback-verkkoliitäntä sekä router-id. Loopback toimii ikään kuin virtuaalisena verkkoliitäntänä ja verkkona. Router-id on taas reitittimen tunniste, johon kaikki protokollat ja palvelut liitetään. Router-id on uniikki tunniste, eikä toista samanlaista samassa verkossa saa olla. Siksi on yleistä, että router-id määritellään samaksi kuin loopback-verkkoliitännän IP-verkko-osoite. Näin se otetaan tarkasti huomioon, kun suunnitellaan verkon topologiaa. Asetetaan ensiksi loopback-verkkoliitäntä ja sen jälkeen router-id. Koska loopback on virtuaalinen verkkoliitäntä, voidaan se konfiguroida 32-bittiseksi, kuten esimerkkikoodi 5:ssä.

```
HOT8660-1#show running-config | block lo0
interface lo0
interface lo0
   description loopback 0
   no shutdown
   ip address 10.123.110.1/32
```

```
HOT8660-1#show running-config | block router-id
router-id 10.123.110.1
  bgp router-id 10.123.110.1
  ospf router-id 10.123.110.1
```

Esimerkkikoodi 5. Loopback-osoitteen asettaminen.

Router-id on nyt asetettu staattisesti, eikä se noudata automaattista valintakaavaa mikä normaalisti muodostuisi järjestyksessä:

1. LDP router-id
2. yleinen router-id
3. korkein loopback IP-osoite
4. korkein verkkoliitännän IP-osoite.

4.5 OSPF-reititys

Seuraavaksi asennetaan reitittimelle OSPF-prosessi. Reitittimellä voi olla useita prosesseja samalle reititysprotokollalle, mutta yleisemmin käytetään vain yhtä, jonka alle voidaan luoda muutkin OSPF-alueet. Prosessia luotaessa on laitettava itsensä reitittimen asemaan ja ajateltava kaikkia verkkoliitäntöjä, jotka kuuluvat OSPF prosessille, kuten esimerkkikoodissa 6. Tarkoitus on mainostaa jokaista OSPF-verkkoliitäntää, jotta muut reitittimet pystyvät oppimaan reitin kuhunkin verkkoon ja tallentamaan sen reititystietokantaansa.

Alueita laboratoriossa on kaksi: Alue 0, mikä vastaa runkoverkkoa ja alue 1. LSA-mainostuksien määrästä johtuen alueita voidaan luoda useampia, etenkin jos reitittimien määrä alueella on suuri. Näin vähennetään LSA-mainostuksia. Laboratorion näkökulmasta on mielenkiintoista saada ympäristö, jossa voidaan reitittää useampien alueiden kesken. Etenkin niin sanottu ”Inter-Area TE” (Inter-Area Tunnel Engineering) ja sen testaus on mahdollista.

```
HOT8630-1#show running-config | block ospf
router ospf 1
   ospf router-id 10.123.110.3
   network 10.123.110.3/32 area 0.0.0.0
   network 172.19.234.0/24 area 0.0.0.0
   network 192.168.0.4/30 area 0.0.0.0
   network 192.168.0.8/30 area 0.0.0.1
   network 192.168.0.28/30 area 0.0.0.0
   network 192.168.0.32/30 area 0.0.0.1
```

Esimerkkikoodi 6. OSPF-prosessin luonti.

Reitittimen "router-id" sidotaan OSPF-prosessiin. Kaikki verkkoliitännät mainostetaan konfiguraatiossa. Vaikka kyseessä on verkko, jota mainostetaan, reititin mainostaa kuitenkin verkkoliitäntää. Asetuksissa käytetään villikorttia OSPF-alueiden mainostukseen. Kuvan 9 reititystaulusta nähdään OSPF-mainostuksia. [5.]

```
HOT8660-1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
    O - OSPF, IA - OSPF inter area, D - OSPF discard
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
    * - candidate default

C     10.123.110.1/32 is directly connected, lo0
O     10.123.110.2/32 [110/89] via 192.168.0.2, so9/0/0, 02w3d05h
O     10.123.110.3/32 [110/79] via 192.168.0.6, ge8/0/0, 01w4d17h
O     10.123.110.14/32 [110/111] via 192.168.0.14, ge8/0/1, 19:39:36
S     172.19.0.0/16 [1/0] via 172.19.234.254, mfe14/0
C     172.19.234.0/24 is directly connected, mfe14/0
C     192.168.0.0/30 is directly connected, so9/0/0
C     192.168.0.4/30 is directly connected, ge8/0/0
C     192.168.0.12/30 is directly connected, ge8/0/1
HOT8660-1#
```

Kuva 9. Reititystaulu, kun osa OSPF-mainostuksista on luotu.

4.6 Verkkoliitännät

Luon nyt yhden kiinteän linkin kahden verkkoliitännän välille. Verkkoliitännät ovat samassa aliverkossa. Verkkoliitännät ovat tyypiltään optisia Ethernet-liittymiä. Ethernet

on nykyaikana eniten kasvava ja nopein verkkotekniikka. Ethernetin kapasiteettiä kehitetään koko ajan nopeammaksi ja nopeammaksi. Laboratoriossa se tulee olemaan myös pääroolissa. Käyttöliittymien konfigurointi on mielenkiintoista ja tärkeää, sillä samalla otan käyttöön MPLS-ominaisuudet, sekä asetamme IP-osoitteen. Linkin IP-osoite on 192.168.0.2, mikä tarkoittaa, että 30-bittisessä verkossa toisen verkkoliitännän osoite on 192.168.0.1.

```
HOT8630-1#show run | blo ge8/0/0
interface ge8/0/0
   label-switching
   bandwidth 1G
   no shutdown
   ip address 192.168.0.2/30
   mpls label protocol ldp
   mpls label protocol rsvp
```

Esimerkkikoodi 7. Ethernet-verkkoliitännän asetukset.

Verkkoliitäntänä tässä esimerkissä on Gb (GigaBit) Ethernet -liittymä, joka sijaitsee korttipaikassa 8, moduulissa 0 ja on järjestyksessä ensimmäinen verkkoliitäntä (numerot alkavat nollasta). Tämä voidaan nähdä esimerkkikoodista 7. Komento ” mpls label protocol” ottaa käyttöön ohjaustason, joka antaa määrätylle protokollalle luvan mainostaa leimoja. Tässä tapauksessa molemmat LDP- ja RSVP-protokolla voivat mainostaa niitä. Komento ” label-switching” aktivoi datatason. Verkkoliitännän nopeutta voidaan myös rajoittaa. Siitä huolehtii komento ”bandwidth”, oletusarvoisesti se on verkkoliitännän maksimiarvon mukainen. Tämä eroaa Ciscon käytännöstä hieman. Tällä menetelmällä asetan osoitteet ja asetukset verkon kaikkiin verkkoliitäntiin.

STM-16 -verkkoliitännän asetukset eivät juuri eroa Ethernetistä, joten sitä ei käydä läpi sen enempää.

4.7 Verkkoliitännän turvaaminen

Jokaisen Tellabsin linjamoduulin verkkoliitännän pystyy turvaamaan mahdollisilta vikatilanteilta. Vikatilanteiksi luetellaan esimerkiksi kaapelin katkeaminen, linjakortin tai

moduulin vioittuminen. Vikatilanteessa varmistava kortti aktivoituu muuttaen entisen aktiivisena toimineen kortin passiiviseksi. Näin voidaan esimerkiksi vaihtaa moduuli liikenteen katkeamatta. Myös kaikenlaiset ohjelmistopäivitykset tai muut huoltotoimenpiteet voidaan tehdä katkaisematta liikennettä.

Suojattavat moduulit toimivat pareittain. Niitä varten pitää luoda ryhmä, johon verkkoliitännät lisätään. Ryhmän luonti ikään kuin sulauttaa molemmat kortit yhdeksi. Aktiivisena toimivaa korttia kutsutaan työskenteleväksi (working) kortiksi. Passiivista korttia kutsutaan suojaavaksi (protecting). Työskentelevää korttia käytetään ryhmän dominoivana korttina, ja sen asetuksia ja tunnistetietoja käytetään yleisesti. Esimerkkinä on MAC-osoite (Media Access Control), joka on jokaisen verkkokortin Ethernet-verkossa yksilöivä osoite. Toista samanlaista ei verkossa siis ole [9, s. 60]. Suojaavan ryhmän luonti piilottaa varmistavan moduulin verkkoliitännän tunnistetiedot. Se että käyttöliittymien MAC-osoite eroaa toisistaan, ei itsessään tuota ongelmia. Ongelmia syntyisi siinä vaiheessa, kun suojauksen aktiivisuutta vaihdetaan puolelta toiselle. IP-osoite pysyy identtisenä, mutta MAC-osoite vaihtuisi. Tämä vaatisi ARP (Address Resolution Protocol) -päivityksen, jotta uusi MAC-osoite voitaisiin kiinnittää samaan IP-osoitteeseen. Tämä aiheuttaisi pidemmän katkoksen liikenteeseen.

Seuraavaksi asetetaan kahdelle verkkoliitännälle Tellabsin ELP-suojaus. Sääntö ELP:tä ja muita suojauksia luotaessa on, että työskentelevän kortin tulee olla korkeammassa korttipaikassa kuin suojelevan. Moduulien pitää myös olla identtisiä ja niiden pitää sijaita samalla moduulipaikalla (linjakortin paikassa 1 tai 0).

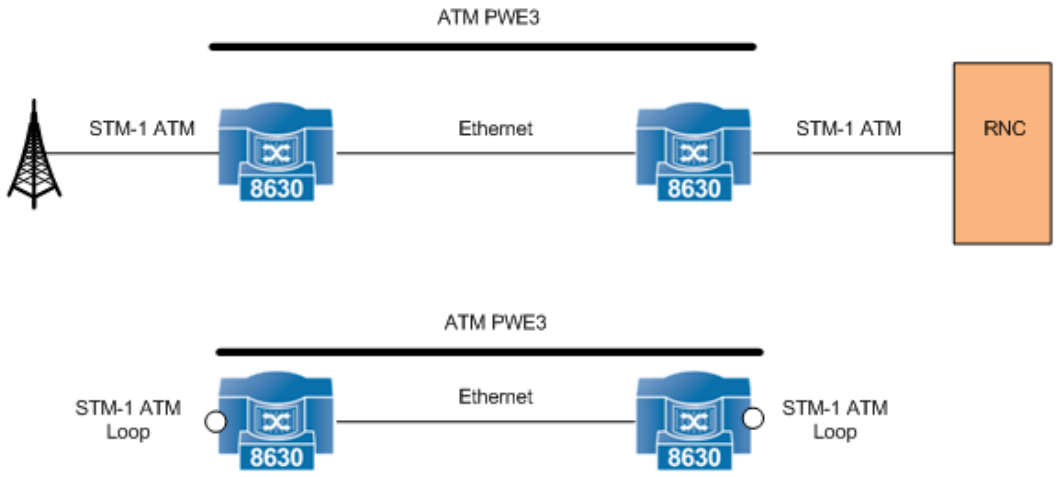
```
HOT8660-1#show run | blo protec
protection elp Hotline_ELP_101
   primary ge 8/0/0 backup ge 7/0/0
   passive-if-mode up rx-both
   l2-learning-tx-frames
```

Esimerkkikoodi 8. ELP-suojasryhmän luonti.

Ryhmälle ei anneta IP-osoitetta, vaan se määritellään työskentelevälle verkkoliitännälle (tässä tapauksessa primary ge8/0/0). [23.]

4.8 Virtuaalilinjan luominen

Verkkoliitännät IP-osoitteineen on jaettu. Nyt on mahdollista luoda virtuaalilinjoja läpi MPLS-verkon. Laboratoriossa on Ethernet -tekniikkaan pohjautuva runkoverkko valmiina. Virtuaalilinjoja voidaan luoda eri verkkotekniikoilla läpi tämän runkoverkon. Itse verkkoliitäntä, johon virtuaalilinja luodaan, voi olla jotain vallan muuta. Verkkoliittymän ei laboratoriossa tarvitse olla edes kytköksissä oikeaan päätelaitteeseen. Voin tehdä fyysisen silmukan verkkoliitäntään, jolloin sille tuleva signaali lähtee takaisin kohteeseensa, kuten kuvassa 10. Näin virtuaalilinja saadaan fyysisesti aktiiviseksi.



Kuva 10. Virtuaalilinjan silmukka [7].

Esimerkkikoodissa 9 luodaan ATM-virtuaalilinja verkon läpi (Kuva 7. vasemmalta oikealle, ylemmät Node B:t). Verkkoliitännäisenä käytän PDH:ta (Plesiochronous Digital Hierarchy) molempien päätepisteiden välillä. Signalointi toteutetaan LDP -protokollalla.

```
HOT8605-1(config)#router ldp
HOT8605-1(cfg-ldp)#targeted-peer 10.123.110.9

HOT8605-1(config)#pwe circuit ATM_PWE3 1 mpls ldp 10.123.110.9 vc-qos ef

HOT8605-1(config)#interface pdh1/15
HOT8605-1(config)#pdh framed
HOT8605-1(config)#interface pdh1/15:0
HOT8605-1(cfg-if[pdh1/15:0])#pdh timeslots 1 - 15 17 – 31
HOT8605-1(cfg-if[pdh1/15:0])#port-protocol atm
```

```
HOT8605-1(config)#interface pdh1/15:0#atm#50
HOT8605-1(cfg-if[pdh1/15:0#atm#50])#atm usage switched
HOT8605-1(cfg-if[pdh1/15:0#atm#50])#atm traffic-params servcat cbr confdef cbr.1 pcr 4528
4528 cdvt 1000 1000
HOT8605-1(cfg-if[pdh1/15:0#atm#50])#pwe3 circuit ATM_PWE3
HOT8605-1(cfg-if[pdh1/15:0#atm#50])#no shutdown
```

Esimerkkikoodi 9. ATM-virtuaalilinjan luonti käyttäen PDH-verkkoliitäntää.

Toiselle puolelle tehdään vastaava konfigurointi. Ensiksi LDP-protokollalle annetaan kohdereititttimen router-id (loopback, johon palvelut on sidottu). Luodaan itse virtuaalilinja. Virtuaalilinjan nimen jälkeen tuleva numero merkitsee virtuaalipiirin ID-tunnusta (tämän täytyy olla identtinen toisella puolella). Varataan verkkoliitäntä ja aikavälit (eng. timeslot). Kiinnitetään virtuaalilinja tiettyyn verkkoliitäntään. Kuvassa 11 nähdään virtuaalilinjan tilan.

```
HOT8605-1#show ldp pwe3
Transport     Client            VC      Trans     Local     Remote    Destination   Local
VC ID         Binding           State   Type      VC Label  VC Label  Address       Name
1             pdh1/15:0#atm#50  UP      atm-n1-p  86404     86406     10.123.110.9  ATM_PWE3

HOT8605-1#
```

Kuva 11. Virtuaalilinjan tila komentorivillä.

4.9 IMA-ryhmän luominen

IMA (Inverse Multiplexing ATM) ryhmällä voidaan liittää yhteen useita käyttöliittymiä isommaksi kokonaisuudeksi ja liittää siihen vaikkapa virtuaalilinja, joka on kykenevä näin kuljettamaan enemmän liikennettä. Esimerkkikoodissa 10 nähdään, kuinka IMA-ryhmä on luotu käyttäen chSTM-1 verkkoliittimiä.

```
HOT8660-1#show run | blo ima
interface ima8/10
   atm ima member so8/1/2:1:1:1:0
   atm ima member so8/1/2:1:1:2:0
   atm ima member so8/1/2:1:1:3:0
   atm ima member so8/1/2:1:2:1:0
   atm ima member so8/1/2:1:2:2:0
   atm ima member so8/1/2:1:2:3:0

HOT8660-1#show run | blo so8/1/2:1:1:1
interface so8/1/2:1:1:1
```

```
   pdh framed
   pdh signal-degraded threshold 123
   pdh signal-degraded seconds 2
interface so8/1/2:1:1:1:0
   pdh timeslots 1 - 15 17 - 31
   port-protocol atm
   atm ima member so8/1/2:1:1:1:0
interface so8/1/2:1:1:1
   no sdh report tu12 ais
   sdh report vc12 ssf
   sdh signal-degraded vc12 threshold 123
   sdh signal-degraded vc12 seconds 2
```

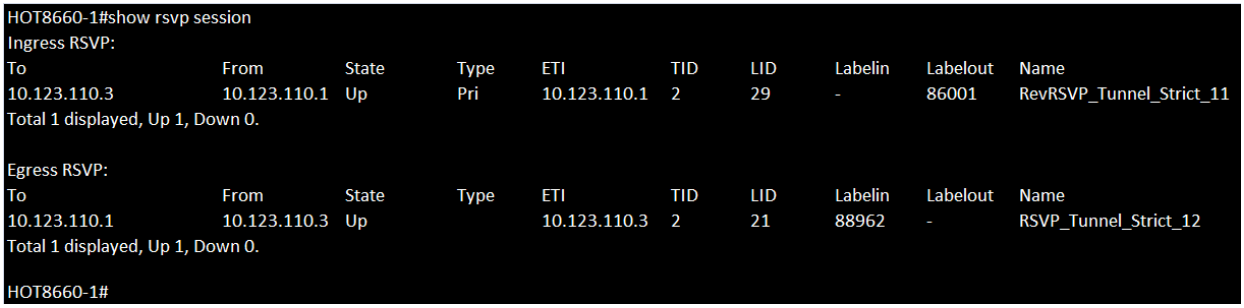
Esimerkkikoodi 10. IMA-ryhmän asetukset.

4.10 RSVP-tunnelin luonti

RSVP-tunneli on tunneli, jolla voidaan optimoida ja varata tietty määrä kaistaa tarvittaessa. RSVP-tunnelit ovat yhdensuuntaisia, joten täytyy luoda toinen tunneli takaisin päin, jotta kaksipuoleinen liikenne on mahdollista. Esimerkkikoodissa 11 luon RT- (Real Time) tunnelin, jolle on varattu 100 kilobittiä sekunnissa. RSVP-tunneleita voi olla kahdentyyppisiä: määrättyjä (strict) ja määräämättömiä (loose). Määrätyssä tunnelissa pakotetaan reititin valitsemaan reittinsä käyttäen määrättyjen reitittimien router-id:tä seuraavina hyppyinä. Määräämätön RSVP puolestaan huolehtii kaikesta itse. Toisin sanottuna protokolla käyttää omaa algoritmiaan hyväksi ja valitsee sen perusteella parhaimman reitin kohteeseensa. Esimerkkikoodissa 11 käytän määrättyä tunnelia.

```
rsvp-path Path_10
   10.123.110.3 strict
!
rsvp-trunk RevRSVP_Tunnel_Strict_11
   primary path Path_10
   primary label-record
   primary bandwidth 100k
   primary class-type ct2
   primary elsp-preconfigured
   from 10.123.110.1
   map-route 10.123.110.3/32 qos ef ip
   to 10.123.110.3
```

Esimerkkikoodi 11. RSVP-tunnelin luonti



```
HOT8660-1#show rsvp session
Ingress RSVP:
To              From          State  Type  ETI           TID  LID  Labelin  Labelout  Name
10.123.110.3    10.123.110.1  Up     Pri   10.123.110.1  2    29   -        86001     RevRSVP_Tunnel_Strict_11
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To              From          State  Type  ETI           TID  LID  Labelin  Labelout  Name
10.123.110.1    10.123.110.3  Up           10.123.110.3  2    21   88962    -         RSVP_Tunnel_Strict_12
Total 1 displayed, Up 1, Down 0.

HOT8660-1#
```

Kuva 12. RSVP-tunnelin tila komentorivillä.

Leimoja jaetaan vain toiseen suuntaan (kuva 12), joka puoltaa sitä, että tunnelit ovat yhdensuuntaisia. Paluuliikenteelle tuleva tunneli on nimetty Rev-tunnisteella (Reverse).

4.11 Testaus

Laboratorioympäristö voidaan todeta toimivaksi kokonaisuudeksi, kun kaikki käytettävät protokollat ja palvelut ovat ylhäällä. Reitittimillä on yhteys toisiinsa ja protokollat ovat kykeneviä luomaan sessioita toistensa kanssa. Tässä tilassa reitittimillä on mahdollisuus alkaa luoda haluttaja palveluita ja ympäristöjä tukemaan insinöörien työskentelyä.

Seuraavat tulosteet on kaikki otettu HOT8660-1 -reitittimeltä (kuvassa 7 keskellä vasemmalla). Osa reititystaulusta voidaan nähdä kuvasta 9. OSPF naapuruussuhteet näkyvät esimerkkikoodi 12:sta.

```
HOT8660-1#show ip ospf neighbor

OSPF process 1:
Neighbor ID     Pri  State      Dead Time   Address         Interface
10.123.110.14   1    Full/DR    0:00:38     192.168.0.14    ge8/0/0
10.123.110.2    1    Full/DR    0:00:38     192.168.0.2     so9/0/0
10.123.110.3    1    Full/DR    0:00:37     192.168.0.6     ge8/0/5
```

Esimerkkikoodi 12. OSPF-naapuruussuhteet.

LDP-naapurit nähdään esimerkkikoodissa 13. Loopback-osoitteen LDP-tunniste täsmää. Verkkoliitäntöjen LDP-tunniste tulee naapurin router-id:n mukaan.

HOT8660-1#show mpls ldp neighbor

IP Address	Intf Name	Holdtime	LDP-Identifier
10.123.110.14	lo0	36/45	10.123.110.14:0
10.123.110.2	lo0	36/45	10.123.110.2:0
10.123.110.3	lo0	40/45	10.123.110.3:0
192.168.0.14	ge8/0/0	15/15	10.123.110.14:0
192.168.0.6	ge8/0/5	13/15	10.123.110.3:0
192.168.0.2	so9/0/0	12/15	10.123.110.2:0

Esimerkkikoodi 13. LDP-naapuruussuhteet

Kun onnistuneet naapuruussuhteet protokollien välillä ovat aktiiviset, on verkon kaikilla laitteilla yhteys toisiinsa. Laitteiden pystyessä kommunikoimaan toistensa kanssa on muiden MPLS-palveluiden, kuten virtuaalilinjojen (luku 4.9) ja RSVP-tunneleiden (luku 4.11), luonti mahdollista.

5 Yhteenveto

Tämän insinöörityön tarkoituksena oli suunnitella ja toteuttaa MPLS-tekniikkaan pohjautuva verkko, jossa verkon ominaisuuksia voitaisiin soveltaa insinöörien töissä. Toimiessaan ympäristö tarjoaa valmiudet simuloida tai luoda tilanteita, joita Tellabsin asiakkaat ovat kohdanneet, ja tutkia näitä.

Runkoverkko toteutettiin Ethernet-tekniikkaan pohjautuen. Runkoverkko jaettiin useampaan eri alueeseen ja käytin kahta eri reititysprotokollaa alueilla. Käytetyt reititysprotokollat ovat OSPF ja IS-IS. Käyttäen useampia reititysprotokollia sekä alueita saadaan aikaan monipuolisempi reititystopologia, mikä välttämättä ei ole optimaalisin vaihtoehto. Monipuolisemmalla reititystopologialla on tarkoitus tutkia esimerkiksi virtuaalilinjojen käyttäytymistä alueiden välillä.

MPLS-tekniikka perustuu tiedon välittämiseen leimojen avulla. MPLS tarjoaa joustavan ja nopean kuljetustavan läpi runkoverkon. Yksi MPLS:n parhaita puolia on palvelunlaadun takaaminen (QoS), mukaan lukien TE (Traffic Engineering). Liikennettä

voidaan priorisoida antamalla korkeamman luokan liikenteelle (esimerkiksi puhe) etuoikeus ennen muuta liikennettä. Toinen MPLS:n parhaista ominaisuuksista on toisen ja kolmostason VPN:n käyttö. MPLS mahdollistaa pakettikytkentäisen VPN-yhteyden lisäämisen suoraan palveluntarjoajan runkoverkkoon.

Verkkoliitäntöjen turvaamisen tuonti työympäristöön on tärkeä osa toteutusta. Runkoverkkoon luotiin ELP- (Ethernet Link Protection) sekä MSP1+1- (Multiplex Section Trail Protection) verkkoliitäntäpareja, jotka voidaan nähdä kuvassa 7 (s. 19). Verkkoliitäntöjen turvaamisen testaaminen liikenteen kanssa on tärkeä ominaisuus laboratoriolle.

Kokonaisuudessaan projektissa onnistuttiin hyvin. Työympäristön monipuolisuus on lyhentänyt aikaa, jota yleensä kuluu erilaisten tilanteiden simuloimiseen. Koska verkko on myös suhteellisen laaja ja siinä on useampia alueita, on se mahdollistanut useamman käyttäjän samanaikaisen käytön.

Lähteet

1 Ala-Mutka Kirsti, Rintala Matti, Savikko Vespe, Palviainen Jarmo. Tietotekniikan peruskurssi. (Verkkodokumentti.) Tampere University of Technology. <http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html>. Päivitetty 4.2.2002. Luettu 18.4.2010.

2 OSI-malli. (WWW-kuva.) Wikipedia. <http://upload.wikimedia.org/wikipedia/fi/4/4c/OSI-malli.jpg>. Katsottu 19.4.2010.

3 Farrel, Adrian. Network Management – Know It All. Morgan Kaufmann Publishers, 2009.

4 Tellabs Training Centre – Managed Edge System. Tellabs 8600 Overview v1.2. Luettu 8.5.2010.

5 Comer Douglas E. Internetworking With TCP/IP Volume I: Principles, Protocols, and Architecture. Prentice-Hall, Inc. ISBN 0-13-216987-8.

6 Tellabs 8600 Managed Edge System – Routing Protocols Configuration Guide. 76.8600-50121A. 28.01.2010. Luettu 28.12.2010.

7 Piippo Ari, MS Visio 2007 piirretyt kuvat.

8 ISO10589. (Verkkodokumentti.) <http://www.networksorcery.com/enp/protocol/is-is.htm>. Luettu 28.2.2011.

9 Arnett, Matthew. Inside TCP/IP. New Riders Publishing, 1994.

10 OSI IS-IS Intra-domain Routing Protocol RFC 1142. (Verkkodokumentti). Network Working Group. 1990. http://tools.ietf.org/html/rfc1142. Luettu 6.4.2011.

11 BGP/MPSL IP Virtual Private Networks RFC 4364. (Verkkodokumentti). Network Working Group. 2006. http://tools.ietf.org/rfc/rfc4364.txt. Luettu 19.4.2011

12 LDP Specification RFC 5036. (Verkkodokumentti). http://tools.ietf.org/html//rfc5036. Luettu 8.4.2011.

13 RSVP-TE: Extensions to RSVP for LSP Tunnels RFC 3209. (Verkkodokumentti). D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivadan, G. Swallow. 2001. http://www.ietf.org/rfc/rfc3209.txt. Luettu 9.4.2011.

14 Tellabs Oy Suomessa. (Verkkodokumentti.) Tellabs Oy. http://www.tellabs.com/fi/. Luettu 13.4.2011.

15 TCP over Second (2.5G) and Third (3G) Generation Wireless Networks RFC 3481. (Verkkodokumentti.) Network Working Group. 2003. http://www.rfc-archive.org/getrfc.php?rfc=3481. Luettu 13.4.2011.

16 Sundell Lasse. Tietokonekommunikaatio. Hakapaino Oy. Helsinki. 2000

17 OSPF Version 2 RFC 2328 (Verkkodokumentti). Network Working Group. 1998. http://tools.ietf.org/html/rfc2328. Luettu 14.4.2011.

18 Choosing a common IGP for the IP Internet RFC 1371 (Verkkodokumentti). Networking Working Group. 1992. http://www.faqs.org/rfcs/rfc1371.html. Luettu 14.4.2011.

19 Multiprotocol Label Switching Architecture RFC 3031 (Verkkodokumentti). Network Working Group. 2001. http://www.ietf.org/rfc/rfc3031.txt. Luettu 15.4.2011.

20 MPLS Label Stack Encoding RFC 3032. (Verkkodokumentti). Network Working Group. 2001. http://tools.ietf.org/html/rfc3032. Luettu 15.4.2011.

21 Encapsulation Methods for Transport of Ethernet over MPLS networks RFC 4448. (Verkkodokumentti). Network Working Group. 2006. http://tools.ietf.org/html/rfc4448. Luettu 19.4.2011.

22 Resource ReServation Protocol (RSVP) RFC 2205. (Verkkodokumentti). Network Working Group. 1997. http://tools.ietf.org/html/rfc2205. Luettu 19.4.2011.

23 Tellabs 8600 Ethernet Link Protection Configuration Guide. 50127_02.pdf. 23.10.2009. Luettu 21.4.2011