Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Eetu Heikkilä

Kolmostason VPN-sovellus MPLS-verkossa

Insinöörityö 3.12.2009

Ohjaaja: yliopettaja Matti Puska
Ohjaava opettaja: yliopettaja Matti Puska

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä	Eetu Heikkilä
Otsikko	Kolmostason VPN-sovellus MPLS-verkossa
Sivumäärä	57 sivua
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja	yliopettaja Matti Puska
Ohjaava opettaja	yliopettaja Matti Puska

Tässä insinöörityössä käytiin läpi asioita joihin Multi Protocol Label Switching -tekniikka perustuu ja miten se toimii käytännön runkoverkoissa.

Teoriaosuudessa käytiin läpi MPLS-tekniikan sekä perustoimintoja ja ominaisuuksia että eroja IP-pohjaisen reitityksen ja MPLS-tekniikan välillä. Teoriaosuudessa tutustuttiin myös MPLS-tekniikan tarjoamiin sovelluksiin, esimerkiksi Virtual Private Network.

Käytännön osuudessa rakennettiin verkko, jonka avulla tutustuttiin VPN-yhteyden muodostamiseen MPLS-tekniikkaan pohjautuvassa runkoverkossa. VPN-yhteys selvitettiin esittämällä asiakasyhteyden muodostamiseen tarvittavia tietoja ja näiden käyttöä. Lisäksi esitettiin runkoverkon toteutukseen liittyvää konfiguraatiota.

Tutkimustuloksista mainittakoon, että yksistään jo VPN-toteutuksen mahdollisuus on hyvä syy MPLS-tekniikan lisäämiseen runkoverkoissa.

Hakusanat	MPLS, VPN, VPLS, VPWS, VPMS

Helsinki Metropolia University of Applied Sciences **Abstract**

Author	Eetu Heikkilä
Title	A Layer 3 VPN application in an MPLS network
Number of Pages	57
Date	3 December 2009
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor	Matti Puska, Principal Lecturer
Supervisor	Matti Puska, Principal Lecturer

The objective of this thesis was to present the basics of Multi Protocol Label Switching and how it works in a backbone.

The basics of the MPLS technology and differences between MPLS technology and IP routing are explained in the theoretical part. Application Virtual Private Network is also explained in this part.

In the research part of this thesis MPLS backbone and VPN connection are created.
The necessary information for VPN connection is also presented in this part. There are also some examples based on configurations and explanations of the configuration.

The research showed that one good reason for increasing MPLS in backbones, is the possibility to make VPN connections right to the backbone.

Keywords	MPLS, VPN, VPLS, VPWS, VPMS

Sisällys

Lyhenteet

AS	Autonomous System; reititysalue
BGP	Border Gateway Protocol; reititysprotokolla
CE	Customer Edge; asiakkaan reunalaite, joka kytkeytyy PE-laitteeseen
CEF	Cisco Express Forwarding;Ciscon lisensoima kolmostason kytkentätekniikka
CR-LDP	Constraint-based Routing LDP; LDP:n lisäosa
DOT1Q	Enkapsulointiprotokolla 802.1Q
EIGRP	Enhanced Interior Gateway Routing Protocol; reititysprotokolla
EoMPLS	Ethernet over MPLS; MPLS-lisäosa, joka mahdollistaa kakkostason Ethernet-tunneloinnin
EXP	Experimental; leiman osa, käytetään liikenteenluokittelussa
FEC	Forwarding Equivalence Class / Välitysekvivalenssiluokka; joukko IP-paketteja jotka kuljetetaan samoilla tiedoilla
FIB	Forwanding Information Base; reititystaulu / välitystietokanta
IETF	Internet Engineering Task Force; internet-protokollien standardoinnista vastaava organisaatio
IGRP	Interior Gateway Routing Protocol; reititysprotokolla
IOS	Internetwork Operating System; Ciscon käyttöjärjestelmä
IP	Internet Protocol; internetissä käytettävä pakettimuoto
IPsec	IP Security Architecture; joukko tietoliikenneprotokollia yhteyksien turvaamiseen
IPX	Internetwork Packet Exchange; Novell Netwaren verkkoprotokolla
IS-IS	Intermediate System to Intermediate System; reititysprotokolla
ISL	Inter-Switch Link; enkapsulointiprotokolla
LDP	Label Distribution Protocol; leimainformaation välitysprotokolla

LER	Label Edge Router/ Edge LSR; lisää / poistaa lippuinformaation paketeista
LFIB	Label Forwarding Information Base; MPLS reititys/leimataulu ja leiman välitystietokanta
LSP	Label Switched Path; polku LSR-laitteiden välillä
LSR	Label Switching Router; reititin joka tukee MPLS:ää
MPLS	Multiprotocol Label Switching; lippuinformaatiota käyttävä tiedonsiirtotapa
MP-BGP	BGP-Multiprotocol; BGP:n laajennettu reititysprotokolla, välittää VPN-osoitteet sekä verkkotiedot runkoverkon läpi
MTU	Maximum Transmission Unit; suurin mahdollinen pakettikoko, joka voidaan kuljettaa verkon läpi
NLRI	Network Layer Reachability Information; BGP:n käyttämä informaatio
OSI	Open Systems Interconnection; tiedonsiirtoprotokollien yhdistelmä
OSPF	Open Shortest Path First; reititysprotokolla
P	Provider; MPLS palveluntarjoajan runkolaite
PE	Provider Edge; MPLS palveluntarjoajan reunalaite
QoS	Quality of Service; liikenteenluokittelu
RD	Route Distinquisher; tunniste jolla muunnetaan IPv4-osoite VPNv4-osoitteeksi. Eroittelee reitit VPN-yhteyksissä
RFC	Request for Comments; IETF:n julkaisema dokumentti
RIP	Routing Information Protocol; reititysprotokolla
RID	Router ID; reitittimen tunnus MPLS-verkossa
RSVP	Resource ReServation Protocol; kaistanvarausprotokolla
RT	Route Target; väline reittien määritykseen VPN-yhteyksissä
S	Stack; leiman osa, ilmaisee leimapinon
SSL	Secure Sockets Layer; liikenteensalausprotokolla
TDP	Tag Distribution Protocol; välittää pakettien leimainformaation

TE	Traffic Engineering; sovellus liikenteen suunnitteluun ja ohjaukseen
TTL	Time To Live; hyppyjen maksimimäärä siirtotiellä
UDP	User Datagram Protocol; yhteyskäytäntö jolla sovellukset kommunikoivat
VC	Virtual Circuit; virtuaalipiiri
VLAN	Virtual LAN; virtuaalinen lähiverkko
VPN	Virtual Private Network; virtuaalinen yksityisverkko
VPLS	Virtual Private Lan Service; virtuaalinen yksityislähiverkkopalvelu
VTP	Vlan Trunking Protocol; virtuaalilähiverkkoprotokolla
VRF	Virtual Routing and Forwarding; teknologia joka mahdollistaa usean reititystaulun käytön samanaikaisesti
VPWS	Virtual Private Wire Service; kakkostasolla toimiva kaksipistepalvelu
VPMS	Virtual Private Multicast Service; kakkostasolla käytettävä ryhmälähetyspalvelu

1 Johdanto

Työn tarkoituksena on luoda Metropolia Ammattikorkeakoulun oppimisympäristöön soveltuva MPLS (Multi Protocol Label Switching) -runkoverkko, joka antaa opiskelijoille kuvan siitä, kuinka kytkeydytään operaattorin verkon eri kytkentäpisteisiin. Opiskelijoilla ei ole tietoa verkon rakenteesta, joten heidän on toimittava operaattorin antamia ohjeita noudattaen, ottamatta sen enempää kantaa runkoverkon laitteisiin tai toteutukseen. Käytännön harjoitusten avulla opiskelija voi runkoverkkoa hyväksikäyttäen tutustua MPLS VPN (Multi Protocol Label Switching Virtual Private Network) -sovellukseen.

Insinöörityön aiheeksi haettiin tietoliikenteeseen liittyvää tekniikkaa, joka tarjoaisi riittävästi haasteita ollen samalla mielenkiintoinen. Työskennellessäni tietoliikennetekniikan parissa törmään lyhenteisiin MPLS ja MPLS VPN lähes päivittäin. Toistuvat kohtaamiset noiden puolittain tuntemieni lyhenteiden kanssa osoittivat suunnan tämän insinöörityön aihetta miettiessäni. Kun luin lisää MPLS-tekniikan eduista sekä sen tarjoamista sovelluksista oli Metropolia Ammattikorkeakoulun ehdottaman aiheen valinta helppo.

2 Multiprotocol Label Switching

2.1 MPLS:n perusteet

Reititettävien protokollien tapauksessa olemme oppineet seuraavaa: IP-paketin (Internet Protocol) saapuessa reitittimelle se siirretään reitittimen prosessorin käsiteltäväksi. Paketin otsikkotiedoista luetaan kohdeosoite, jonka perusteella tehdään päätös liitynnästä, johon paketti ohjataan. Reitityspäätös muodostetaan olemassa olevaa FIB-reititystaulua (Forwarding Information Base) apuna käyttäen. Operaatio toistuu jokaisella verkon reitittimellä, kunnes paketti on päässyt kohdeosoitteeseen.
[1, s. 267–275.]

MPLS poikkeaa edellä mainitusta leimakytkennän takia, jossa jokaiselle paketille annetaan ennalta määritelty leima sen kohteen mukaan. Leimojen avulla paketti kuljetetaan verkon läpi nopeasti, ilman jokaisen reitittimen tekemää reitityspäätöstä.

Paketin saapuessa MPLS-verkkoon PE-reunareititin (Provider Edge) lukee otsikkotiedoista kohdeosoitteen, jonka mukaan suoritetaan LSP-leimapolun (Label Switched Path) sekä leiman valinta. Leima luetaan jokaisen solmupisteen sisääntulossa ja korvataan seuraavan hypyn leimalla ulosmenoliitännässä. Jokainen LSR-leimareititin (Label Switching Router) pitää yllä omaa LFIB-tunnistetaulua (Label Forwarding Information Base), jonka avulla se osaa leimata paketin oikein ennen eteenpäin lähetystä. Paketin poistuessa MPLS-verkosta verkon laidalla reunareititin poistaa paketista leimainformaation sekä välittää paketin eteenpäin joko seuraavalle IP-reitittimelle tai lopulliseen kohteeseen.

MPLS:n tarkoituksena on vähentää verkkokerrosreitityksen tarvetta korvaamalla se siirtoyhteyskerroksen kytkennällä. Toiminnalla saavutetaan huomattavaa eroa nopeudessa. MPLS tarjoaa seuraavia ominaisuuksia: skaalattavuus, yksinkertaisuus, reittienhallinta sekä parempi voimavarojen käyttö. [2, s. 2–4].

Traffic Engineering (TE) sekä kolmostason VPN-yhteydet (Virtual Private Network) ovat osa yhteydellisen MPLS:n tarjoamista lisäpalveluista.

2.2 Verkkolaitteet

Yleisen käsityksen mukaan MPLS-verkon muodostavat ainoastaan palveluntarjoajan käyttämät ja ylläpitämät aktiivilaitteet, jotka muodostuvat reitittimistä ja kytkimistä, joilla on kolmostason reititysominaisuudet. MPLS-tekniikan käyttöä ei kuitenkaan ole rajoitettu ainoastaan palveluntarjoajien yksinoikeudeksi, vaan se on yleisesti saatavilla sitä tarvitseville. Esimerkiksi Puolustusvoimilla on käytössään yksityisiä MPLS-verkkoja. [3.]

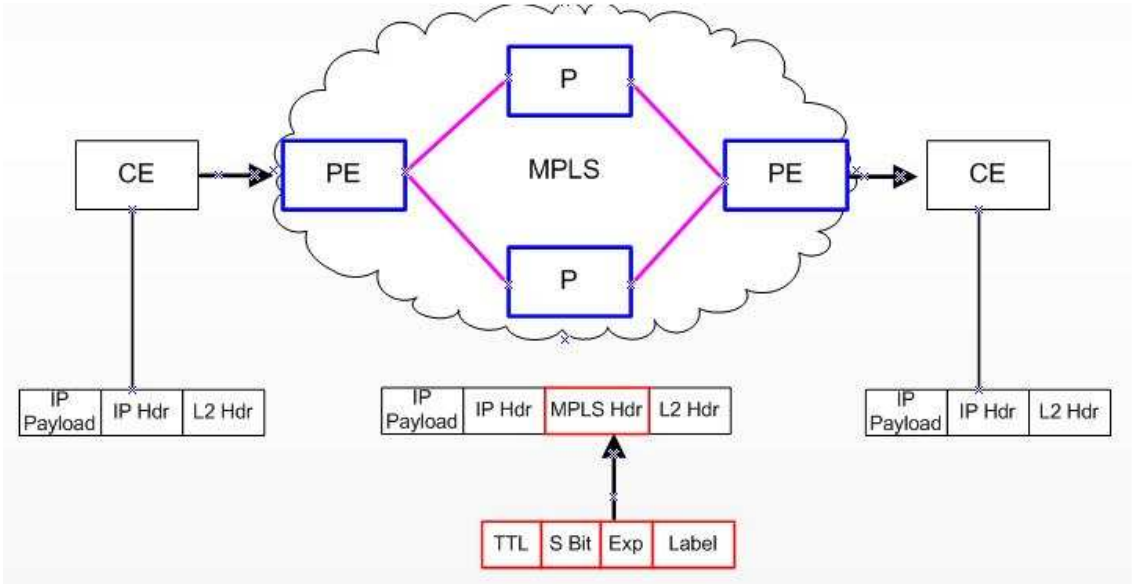
MPLS-verkon laitteet voidaan jakaa karkeasti kahteen pääryhmään niiden sijainnin mukaan.

P-runkolaitteiksi (Provider) luetaan rungon ydinreitittimet (core) sekä kaikki ne reitittimet, jotka eivät fyysisesti sijaitse runkoverkon reunalaitteina. P-reitittimen tehtävänä on kytkeä datapaketit leimainformaation perusteella, jolloin reitityksestä tulee joustavaa ja nopeaa. Tyypillisesti runkoreititin on yhteydessä yhteen tai useampaan reitittimeen, jotka voivat olla joko P tai PE tyyppisiä. (Kuva 1.)

PE-reunalaitteiksi kutsutaan niitä reitittimiä, jotka sijaitsevat MPLS-pilven reunalla. Nämä ovat yhteydessä asiakkaan verkkolaitteisiin ja ylläpitävät MPLS-reititystauluja. PE voi tarvittaessa kontrolloida liikenteen priorisointia, luokittelua sekä jonotusta. Paketin saapuessa MPLS-alueelle PE-reititin lukee otsikkotiedoista kohdeosoitteen, jonka mukaan se suorittaa leiman valinnan sekä asettamisen.

PE-reunareitittimen tehtävänä on välittää liikenne MPLS:n ja tavallisten IP-verkkojen välillä. Yksiselitteisesti palveluntarjoajan verkosta tulevat datapaketit välitetään asiakkaan verkkoon sekä asiakkaan verkosta tulevat paketit palveluntarjoajan verkkoon.

Asiakkaan hallinnoimia verkkolaitteita kutsutaan CE-laitteiksi (Customer Edge). Ne sijaitsevat asiakkaan verkon reunalla ja ovat suoraan yhteydessä palveluntarjoajan PE-reunalaitteisiin. Pääsääntöisesti asiakkaan reunalaitteet ovat IP-pohjaisia eivätkä ne näin ollen ole osana MPLS-verkkoa.



Kuva 1. MPLS-verkon laitteet sekä leima sijainteineen.

2.3 Leima

MPLS:n toiminta perustuu leimakytkentään, jossa ennalta määritetyn 32-bittisen leiman avulla paketteja reititetään joustavasti solmupisteeltä toiselle. Leima sijoitetaan paketissa siirto- ja verkkokerroksen otsikoiden väliin. (Kuva 1.)

Leima koostuu 32-bitistä, jotka jakautuvat neljään osaan. 20 ensimmäistä bittiä on leiman varsinainen arvo. Loput 12-bittiä jäävät muuhun tarkoitukseen, kuten liikenteen laadun luokitteluun, leimojen ja hyppyjen määrän hallintaan.[2, s. 66.]

Leima koostuu seuraavista osista:

- Label: Leiman arvo, 20 bittiä
- Exp (Experimental): 3 bittiä liikenteen luokitteluun (QoS, Quality of Service)
- S (Stack): 1 bitti useamman leiman pinoamiseen
- TTL (Time to Live): 8 bittiä, asettaa hyppyjen maksimimäärän paketille MPLS-verkossa, estäen silmukoiden syntymisen. Paketin poistuessa MPLS-verkosta synkronoidaan IP-TTL:n kanssa.

Leima muodostetaan FEC-taulukon (Forwarding Equivalence Class) mukaan paketille määriteltyjä vaatimuksia apuna käyttäen. Se on yksilöllinen tunniste FEC-luokasta, johon kyseinen paketti kuuluu. Leimalle voidaan antaa arvo väliltä 0–1048 576. Leiman arvot nollasta viiteentoista ovat kuitenkin varattuja. [4.]

Leima on yksikäsitteinen vain kahden LSR:n välisellä linkillä. Jokainen LSR pitää yllä omaa leimataulua, jonka avulla se valitsee oikean leiman paketille ennen eteenpäin lähetystä.

2.4 Leimapino

MPLS-verkossa on mahdollista kuljettaa useampaa leimaa yhden paketin mukana. Leimat pinotaan päällekkäin ja solmupisteissä vain pinon päällimmäinen tutkitaan, minkä perusteella tehdään reitityspäätös. [2, s. 67.]

Leimassa pinon arvoa edustaa arvo ”S”. Arvo ”1” kertoo leiman olevan kyseisen pinon viimeinen. Arvolla ”0” pinossa on useampi leima. Leimojen pinoamista käytetään hyväksi esimerkiksi MPLS VPN-yhteyksissä, joissa useita leimoja voidaan kuljettaa samanaikaisesti laitteiden välillä samaa LSP:tä käyttäen.

Pino toimii ”Last-In First Out” -periaatteella, jolloin viimeksi lisätty leima käytetään pinosta ensimmäisenä.

2.5 Välitysekvivalenssiluokka (FEC)

MPLS-verkossa paketille määritetään välitysekvivalenssiluokka (FEC), joka kertoo, mihin pakettien muodostamaan liikennevirtaan se kuuluu. FEC on joukko paketteja, jotka reititetään samalla tapaa verkon läpi. Pakettien ryhmittely voi perustua erimerkiksi kohdeverkon osoitteeseen, jolloin samaan osoitteeseen menossa olevat paketit reititetään MPLS-verkon läpi samoilla palveluilla samaa reittiä käyttäen. [5, s. 33.]

Paketit voidaan jakaa luokkiin seuraavin parametrein:

- Lähteen ja/tai kohteen IP-osoite
- Lähteen ja/tai kohteen porttinumero
- IP-protokollan ID (PID)
- IPv4-otsikon DS-kentän arvo
- IPv6-vuonimiön arvo.

FECiä voidaan käyttää avuksi liikenteen priorisoinnissa ja luokittelussa. Rajoittamalla matalampiarvoisen prioriteetin kaistanleveyttä saadaan turvattua korkeammalle prioriteetille enemmän kaistaa käyttöön. Esimerkkinä reaaliaikainen ääni ja video menevät priorisoinnissa tavallisen internetselailun ohi.

2.6 Leimanvälitystietokanta (LFIB)

MPLS-verkossa jokaisella reitittimellä on oma leimanvälitystietokanta (LFIB, Label Forwarding Information Base) (taulukko 1), joka sisältää tiedon sisään tulevista leimoista sekä vaihtoehtoisista reiteistä paketin edelleen lähetykseen. Paketin saapuessa sisääntuloliitäntään luetaan taulukosta eteenpäin lähtevälle paketille annettava leima, ulosmenoliitäntä sekä seuraavan hypyn osoite. LFIB-taulukoita voi olla yksi tai jokaiselle LSR:n liitännälle omansa.

Taulukko 1. LFIB-taulukko

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Outgoing interface	Next Hop
16	Untagged	172.16.1.0/24	Fa0/1	10.10.10.1
17	17	172.16.2.0/24	Se0/1	point2point
18	Pop tag	10.10.10.8/30	Se0/1	point2point
25	Untagged	10.10.10.101/32	Fa0/1	10.10.10.1
26	Untagged	192.168.1.0/24	Fa0/1	10.10.10.1
27	28	192.168.2.2/32	Se0/1	point2point

3 Leimaoperaatiot

Push

Paketin saapuessa MPLS-verkkoon lukee PE-reititin paketin otsikkotiedoista sen kohdeosoitteen sekä palveluvaatimukset, joiden mukaan suoritetaan LSP:n asettaminen sekä leiman valinta. Leiman asettaminen suoritetaan ”push”-operaatiolla. ”Push”-operaatiossa LSR:t myös siirtävät vanhoja leimoja pinossa alaspäin ja lisäävät uuden päälle, kun vastaanotetaan paketti varustettuna leimalla, jota tullaan käyttämään myöhemmin. Hypyssä seuraavalle reitittimelle alaspäin painettua leimaa ei vielä käytetä.

Swap

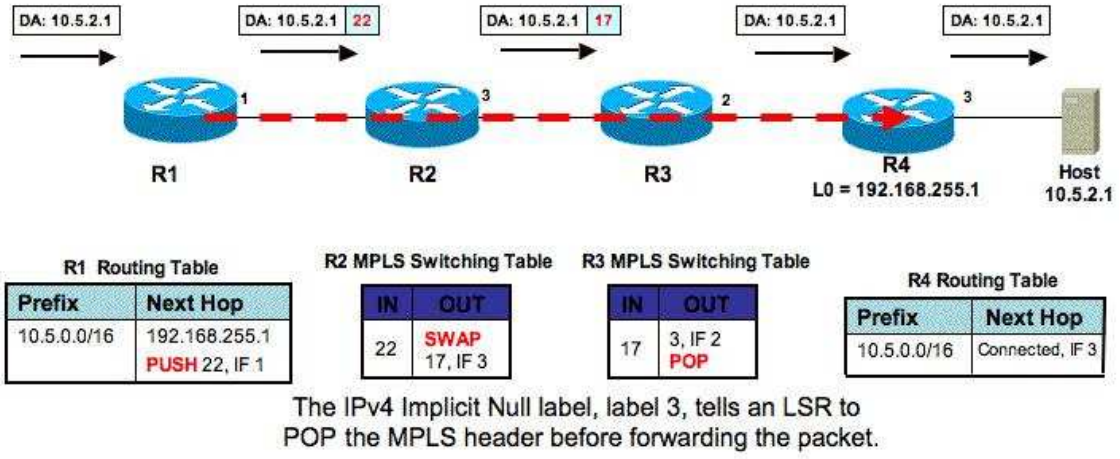
Paketin kulkiessa MPLS-verkossa luetaan sen leimainformaatio jokaisen solmupisteen sisääntulossa. Reititin katsoo leimataulustaan leimaa vastaavan ulosmenoportin ja ulosl̈ähetettävän leiman numeron. Näiden tietojen perusteella leima korvataan seuraavan hypyn leimalla ulosmenoliitännässä. Kyseistä tapahtumaa kutsutaan ”swap”-operaatioksi. [6.]

Pop

MPLS-verkossa LSR:t voivat myös avata eli poistaa ylimpiä leimatietoja paketilta. Tämä tapahtuu esimerkiksi, kun paketti poistuu MPLS-verkosta ja jatkoreititys tapahtuu IP-osoitteen perusteella. Kyseinen operaatio on nimeltään ”pop”, sitä voidaan käyttää myös usean leiman tapauksessa. ”Pop”-operaatiossa LSR voi poistaa vain yhden leiman kerrallaan.

Penultimate Hop Popping

Penultimate Hop Popping kehitettiin helpottamaan LSR:n toimintaa usean leiman tapauksissa. Operaatio antaa PE:lle mahdollisuuden pyytää naapuriaan suorittamaan ”pop”-operaation ennen kuin paketti saapuu pyytäjän sisääntuloliitäntään. Operaatiolla pyritään vähentämään PE:n kuormitusta. Pyyntö suoritetaan käyttämällä LPD:tä (Label Distribution Protocol) ja varattua leiman arvoa 3. Pyynnön saanut LSR poistaa leiman ja toimittaa paketin reunareitittimelle, jossa suoritetaan tarvittava jatkotoimenpide. Toimenpide voi olla viimeisen leiman poisto tai leimattoman IP-paketin tarkastus ja eteenpäin lähetys. (Kuva 2.)



Kuva 2. Leimaoperaatiot [7]

Leimaoperaatiot toimivat MPLS-verkossa seuraavasti:

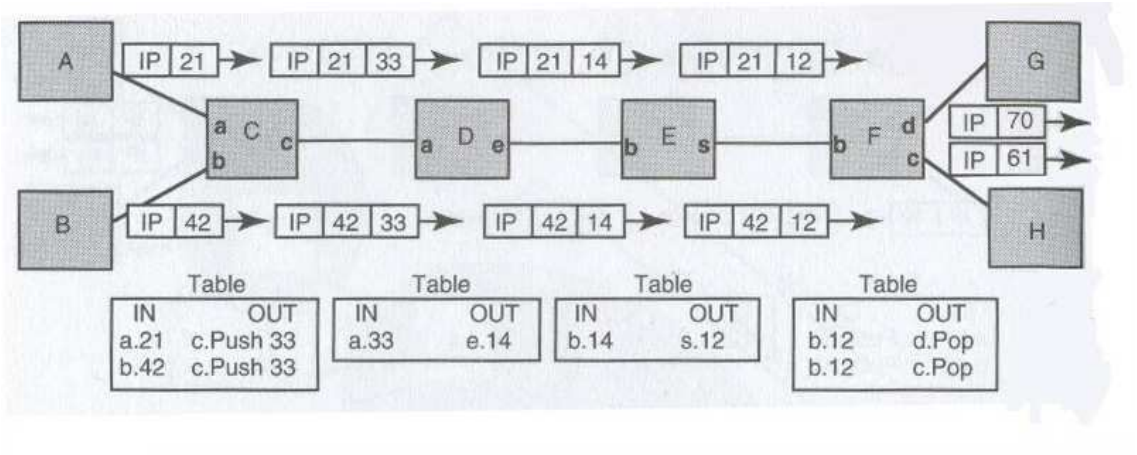
- Reititin R1 lisää paketille leiman 22 ”push”-operaatiolla.
- Reititin R2 vaihtaa leiman arvon 22 > 17 ”swap”-operaatiolla.
- R3 poistaa leiman R4:n pyynnöstä ”pop”-operaatiolla, pyyntö välitetään käyttämällä LDP:tä ja varattua leiman arvoa 3.
- R4 toimittaa IP-paketin kohteeseen.

Usean leiman käyttö

Kuten aikaisemmin on jo todettu, MPLS-verkossa on mahdollista kuljettaa useampaa leimaa yhden paketin mukana. Toiminta perustuu hierarkkisiin leimaoperaatioihin, jotka on suunniteltu vastaamaan suurien verkkojen tuomiin haasteisiin leimakytkennän yhteydessä. Hierarkkinen leimapino mahdollistaa P-reitittimen toimia reunareitittimien tapaan, jolloin leimoja vaihdetaan vain haluttujen laitteiden välillä runkoverkossa. Näin saadaan muodostettua verkon sisälle kuljetusalueita.

Hierarkkista leimapinoa hyödynnetään esimerkiksi MPLS VPN-yhteyksissä, joissa VPN-leimat ja normaalit MPLS-leimat saadaan pidettyä erillään käyttämällä kaksikerroksista leimapinoa. VPN-paketin saapuessa kuljetusalueen reunalaitteelle painetaan leima pinossa alaspäin ja päälle sijoitetaan MPLS-leima, jonka avulla paketti kuljetetaan alueen läpi. Kuljetusalueen reunalla MPLS-leima poistetaan ja VPN-leima nostetaan takaisin pinon päällimmäiseksi.

Leiman hierarkiatasolla ei ole merkitystä LSR:n toimintaan, LSR lukee pinosta ainoastaan päällimmäisen leiman ja toimii sen mukaisesti, puuttumatta pinon muihin leimoihin. Kuvissa 3 ja 4 esitellään eri toimintamalleja.

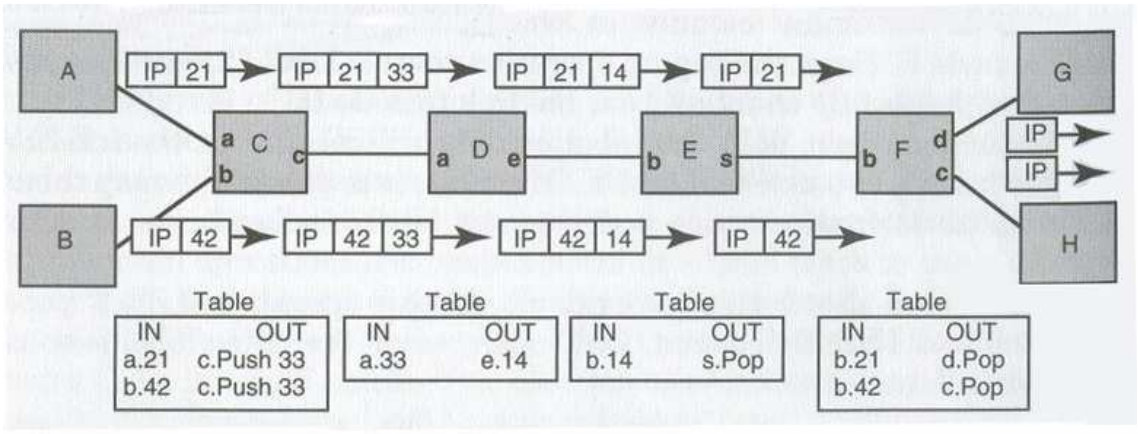


Kuva 3. Kaksikerroksisen leimapinon käyttö esimerkki 1. [2, s. 70.]

Kuvassa 3 solmut A, B, G ja H ovat reunalaitteita solmujen C, D, E ja F muodostamalle kuljetusalueelle. Jokainen solmuista tukee MPLS-leimakytkentää. Solmujen A, B, G ja H takana voi olla työasemia sekä palvelimia.

Leimojen välitys kaksikerroksisen leimapinon avulla sujuu seuraavasti:

- A lähettää paketin solmulle C, leiman arvolla 21.
- C lukee leimataulustaan suoritettavan tehtävän, painaa leimaa pinossa alaspäin ja sijoittaa pinon päälle leiman 33, jota käytetään välillä C – D.
- D lukee kaksikerroksisen leimataulun päällimmäisen leiman, suorittaa leiman vaihdon ja lähettää paketin reitittimelle E leimalla 14.
- E lukee kaksikerroksisen leimataulun päällimmäisen leiman, suorittaa leiman vaihdon ja lähettää paketin eteenpäin leimalla 12 vastaanottajana F.
- F vastaanottaa paketin, poistaa pinon päällimmäisen leiman ja toimittaa paketin eteenpäin leimalla 70.
- G vastaanottaa paketin leimalla 70 ja suorittaa tarvittavat jatkotoimenpiteet.



Kuva 4. Kaksikerroksisen leimapinon käyttö esimerkki 2. [2, s. 70.]

Kuvassa 4 G- ja H-solmut eivät tue MPLS-leimakytkentää. Ne voivat olla joko palvelimia tai reitittimiä. Edelliseen kuvaan verrattuna leiman poisto tapahtuu E- ja F-solmuissa.

Leimojen poisto kaksikerroksisessa leimapinossa tapahtuu seuraavasti:

- B lähettää paketin leiman arvolla 42 solmulle C.
- C lukee leimataulustaan suoritettavan tehtävän, painaa leimaa pinossa alaspäin ja sijoittaa pinon päälle leiman 33, uudeksi pinonarvoksi tulee 1.
- D lukee leimataulun päällimmäisen leiman, suorittaa leiman vaihdon ja lähettää paketin E:lle leimalla 14. Pinonarvo on 1.
- E vastaanottaa paketin, poistaa pinon päällimmäisen leiman ja toimittaa paketin eteenpäin alkuperäisellä leimalla 42, pinonarvon ollessa 0.
- F vastaanottaa paketin ja poistaa viimeisen leiman.
- G vastaanottaa IP-paketin.

Esimerkkitapauksissa paketit on kuljetettu onnistuneesti runkoverkon läpi käyttäen kaksikerroksista leimapinoa. Kuljetukseen tarvittiin vain yksi sisäinen leima, vaikka kuljetettiinkin kahta ulkoista leimaa samanaikaisesti.

4 Leimanjakoprotokollat

Leimojen jakamiseen MPLS-verkon sisällä ei ole määritelty yhtä ja ainoaa oikeaa tapaa. Standardointeja on useita, ja vanhoja reititysprotokollia on muokattu, jotta ne voivat tarjota palveluitaan myös leimojen välityksessä. [8, s. 5.]

Käytetyimmät protokollat leimojen jakamiseen ovat seuraavat:

- LDP: Label Distribution Protocol
- TDP: Tag Distribution Protocol (Ciscon lisensoima, vastaa LDP:tä)
- CR-LDP: Constraint-based Routing Label Distribution Protocol
- RSVP: Resource ReSerVation Protocol
- RSVP-TE: RSVP-Traffic Engineering
- MP-BGP: Multiprotocol Border Gateway Protocol.

Leimanjakoprotokollista käytetyin on LDP, koska se on IETF:n (Internet Engineering Task Force) standardoima ja yleisesti valmistajien tukema. LDP:n tarjotessa tukevan perustan leimakytkennälle käytetään sitä lähes kaikissa MPLS-verkoissa, joilta ei vaadita lisäominaisuuksia, esimerkiksi Traffic Engineering -palvelua.

Leimanjakoprotokolla LDP

Tässä insinöörityössä leimojen jakaminen kahden LSR:n välillä suoritetaan käyttämällä siihen kehitettyä leimanjakoprotokollaa LDP, joka samalla mahdollistaa reittien muodostuksen MPLS-verkon läpi. LDP:n avulla LSR välittää kehittämänsä leima- ja FEC-informaation naapurireitittimelle.

Kaksisuuntaisen viestien lähetyksen ansiosta LSR saa paluuviestinä tiedot naapurireitittimien tarjoamista mahdollisuuksista reitittää paketit verkon läpi annetuilla määrityksillä sekä niiden muodostamat leima- ja FEC-informaatiot. LDP voi välittää leimainformaatiota myös kahden sellaisen reitittimen välillä, jotka eivät ole fyysisesti

suoraan toisiinsa kytkettyinä. Tällöin välissä olevan reitittimen tehtäväksi jää leimatiedon välittäminen näiden välillä puuttumatta sen sisältöön.

LDP:llä on kaksi tapaa havainnoida LSR:t verkosta. Perinteistä havainnointitapaa käytetään, kun LSR-naapurit ovat yhteydessä toisiinsa suoralla linkillä. Tällöin LSR lähettää jaksottain *hello*-viestejä UDP (User Datagram Port) -portista 646, multicast-osoitteella 224.0.0.2 ”kaikki aliverkon reitittimet”, mukanaan lähettäjän LDP-tunniste. Vastaanottaja kuittaa saamansa viestin ja näin aloitetaan parin muodostus. Laajennetusta tavassa LSR:t eivät ole suoraan kytkettyinä toisiinsa, jolloin LSR jaksoittain lähettää kohdennettuja *hello*-viestejä LDP-tunnisteineen määritettyyn IP-osoitteeseen.

LDP:llä on neljä erityyppistä tehtäväkategoriaa, joiden mukaan se toimii: [9, s. 13.]

- Discovery hallinnoi ja vaihtaa kuulumisia LSR laitteiden välillä.
- Session muodostaa, hallitsee ja purkaa yhteyksiä LSR laitteiden välillä.
- Advertisement muodostaa, vaihtaa ja poistaa leimoja FEC-tauluista.
- Notification kertoo tilanne-, diagnostiikka- ja virhetiedoista.

LDP:n sekä FEC:n avulla LSR:t saavat muodostettua verkossa LSP-polkuja (Label Switched Path), joiden avulla paketit saadaan toimitettua paikasta A paikkaan B. Polut ovat yksisuuntaisia, joten paluupaketit kulkevat toista polkua pitkin. Toisinaan LSP:tä kutsutaan MPLS-tunneliksi sen ominaisuuksien takia, koska se ei näy verkkokerroksen puolella toimiessaan tasojen 2 ja 3 välissä.

Leimanjakoprotokolla CR-LDP

CR-LDP (Constraint-based Routing Label Distribution Protocol) on leimanjakoprotokolla LDP:n lisäosa, joka antaa verkon ylläpitäjälle mahdollisuuden muodostaa etukäteen suunniteltuja ja täsmällisesti reititettyjä LSP-polkuja. CR-LDP:tä käytetään viiveelle herkän dataliikenteen reitityksessä. [2, s. 87.]

Verkonvarausprotokolla RSVP

RSVP (Resource ReSerVation Protocol) on kuljetuskerrosprotokolla, joka on suunniteltu varaamaan riittävä kapasiteetti yhdelle yksisuuntaiselle datavuolle verkon läpi asiakkaan vaatimustason mukaisesti. Reitittimet käyttävät RSVP:tä välittämään palvelutasovaatimukset (QoS) solmupisteille ja varmistamaan vaaditun palvelun toimivuuden. RSVP on pelkästään kontrolliprotokolla, joka ei osallistu datan kuljetukseen. [2, s. 104–108; 10, s. 138–140.]

Liikenteenohjausprotokolla RSVP-TE

RSVP-TE (RSVP Traffic Engineering) on RSVP:n lisäosa. Se antaa mahdollisuuden muodostaa LSP-polkuja kapasiteettivarauksin sekä ilman varauksia. TE:n käyttö mahdollistaa polkujen joustavan uudelleenreitityksen, priorisoinnin sekä silmukoiden havainnoinnin. RSVP-TE määrittelee yksityiskohtaisesti jokaisen datasiirron määränpään sekä käytetyn kuljetuskerroksen protokollan.

RSVP-TE:tä käytetään leimanjakoprotokollana MPLS-TE:n yhteydessä, jolloin aikaansaadaan joustavuutta ja parempaa yleisilmettä. TE:n pääasiallinen tehtävä on asiakkaan QoS-vaatimuksiin vastaaminen mitoittamalla ja kontrolloimalla liikennettä. [11.]

MultiProtocol-Border Gateway Protocol

Alkujaan BGP (Border Gateway Protocol) kehitettiin reitittämään IPv4-liikennettä (Internet Protocol version 4) eri AS-alueiden (Autonomous Systems) välillä, joskin sitä voidaan käyttää myös saman AS:n sisällä. Myöhemmin protokollaa on laajennettu vastaamaan nykyaikaisia tarpeita. Laajennuksen avulla BGPv4 kykenee kuljettamaan useiden verkkokerrosprotokollien reititystietoja, esimerkkeinä mainittakoon IPv6 (Internet Protocol version 6), IPX (Internetwork Packet Exchange) sekä VPN-IPv4 (Virtual Private Network - Internet Protocol version 4). [12.] Tarvittaessa laajennettu BGPv4 voi hoitaa myös leimojen välityksen BGP-naapureiden välillä, jolloin ei tarvita erillistä leimanjakoprotokollaa. MultiProtocol-BGP on IETF:n (Internet Engineering Task Force) standardointi RFC2858 (Request For Comments) vuodelta 2000.

BGP reititysprotokollan käyttämät reitit eivät perustu mihinkään erityistekniikkaan vaan ne pohjautuvat pääasiassa operaattorin verkolle määrittelemiin sääntöihin, joiden avulla valitaan reititykseen käytettävät reitit.

5 VPN-sovellus MPLS-verkossa

5.1 VPN:n perusteita

VPN eli Virtual Private Network on tapa muodostaa suojattuja yhteyksiä julkisessa verkossa. VPN-tekniikalla voidaan muodostaa yhteys yrityksen eri toimipisteiden lähiverkkojen välille. Yhteys voidaan muodostaa myös yksittäisen etäkäyttäjän koneen ja yrityksen lähiverkon välille, jolloin käyttäjä pääsee yrityksen järjestelmiin etätyöpisteeltään. Nykyaikaisen tietoturvatason ylläpitämiseksi VPN-sovelluksen käyttö lisääntyy koko ajan. [13.]

VPN-yhteys voidaan toteuttaa usealla eri tavalla. Vanhemmissa suljetun verkon toteutuksissa toimipisteiden välille kytkettiin suora suljettu fyysinen kupari- tai valokuituyhteys. Toteutuksena tämä on vanhanaikainen ja kallis. Toimipisteet voivat

sijaita pitkienkin välimatkojen päässä toisistaan, ja nykyaikana tarvittaisiin useita linjoja kasvaneiden siirtonopeuksien vuoksi.

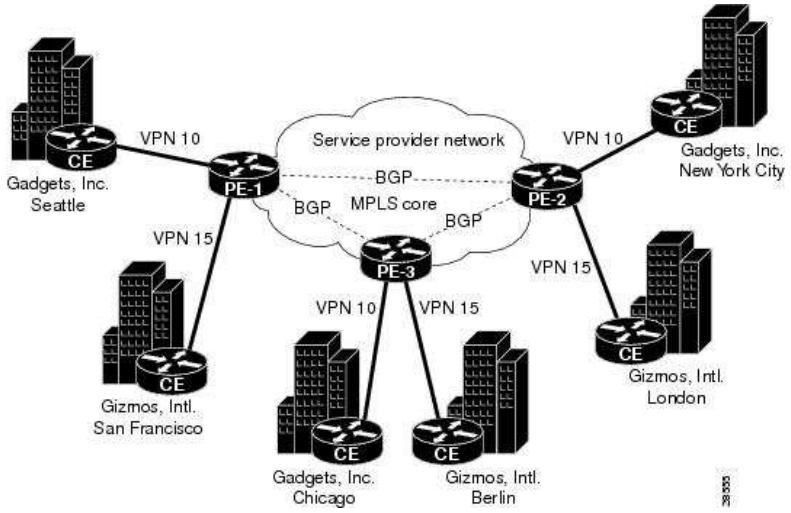
Nykyaikaisempi vaihtoehto on salatut yhteydet, jotka voidaan muodostaa liikennetunneleilla tai ohjelmistopohjaisesti. Tunneloinnissa operaattorin runkoverkon läpi muodostetaan toimipisteiden välille salattu IPsec-tunneli (Internet Protocol security architecture), joka mahdollistaa pakettien kuljetuksen suojattuna toimipisteiden välillä.

Ohjelmistopohjaisesti salattu yhteys voidaan muodostaa SSL VPN (Secure Sockets Layer Virtual Private Network) -yhteydellä. Asiakas ottaa etäkoneeltaan SSL-yhteyden yrityksen palomuurin ennaltamääriteltyyn porttiin X, muodostaen suojatun SSL-tunnelin laitteiden välille. Asiakkaan kone allokoi itselleen suljetun verkon osoitteen, luo virtuaaliverkon laitteiden välille ja näin ollen saa pääsyn yrityksen tietojärjestelmiin. SSL VPN eroaa IPsec-tunnelista siten, että se on toteutettu OSI (Open Systems Interconnection) -kerroksilla 4─7. IPsec-tunnelointi käyttää toimiakseen verkkokerrosta 3 ja täten vastaa itsenäisesti tiedonsiirron luotettavuudesta.

Palveluntarjoajan ylläpitämässä MPLS-verkossa VPN-yhteys voidaan muodostaa joko kakkos- tai kolmostason toteutuksella.

5.2 Kolmostason MPLS VPN

Kolmostason MPLS VPN poikkeaa vanhemmista VPN-yhteyksistä toteutus- ja toimintatapansa vuoksi. MPLS VPN-toteutuksessa tilaajan jokainen toimipiste liitetään suoraan operaattorin runkoverkon PE-reunareitittimeen omalla yhteydellään. Jokainen PE voi sisältää useita VPN-yhteyksiä. Näitä yhteyksiä käsitellään operaattorin puolelta omina yksityisverkkoinaan ja niitä voidaan tarvittaessa yhdistää. (Kuva 5.)



Kuva 5. VPN verkko [14]

Vaikka tiedonsiirrossa käytetäänkin yhteistä verkkoa, kulkevat paketit vain samaan VPN-yhteyteen määritettyjen toimipisteiden välillä eikä kukaan ulkopuolinen niitä pysty näkemään. Toimipiste voi kuulua yhteen tai useampaan VPN-yhteyteen ja voi olla yhteydessä vain saman VPN-alueen sisällä oleviin verkkoihin.

Toiminta perustuu VRF-reititystauluihin (Virtual Routing and Forwarding), joissa kerrotaan reititystiedot ainoastaan saman VPN:n sisällä oleviin verkkoalueisiin. VPN-yhteyden ulkopuolisilla alueilla ei ole mitään tietoa sisäpuolen verkosta tai liikenteestä, joten MPLS VPN on jopa turvallisempi kuin IPsec-tunnelointi, vaikkei käytettäisikään erillistä liikenteensalausprotokollaa.

VRF eli ”VPN Routing and Forwarding” on tekniikka, joka mahdollistaa usean yksittäisen reititystaulun käytön PE-reitittimessä. VRF-taulu sijoitetaan kyseisen asiakkaan sisääntuloliitynnälle, jolloin liitynnästä saapuvat paketit voidaan reitittää VRF-taulun mukaisesti runkoverkon läpi kohdeosoitteeseen. IP-reititystauluihin ei tule merkintää asiakkaan käyttämästä sisääntuloliitynnästä eikä sen takana sijaitsevista verkoista, jolloin ne näkyvät ainoastaan kyseisen yhteyden VRF-taulussa.

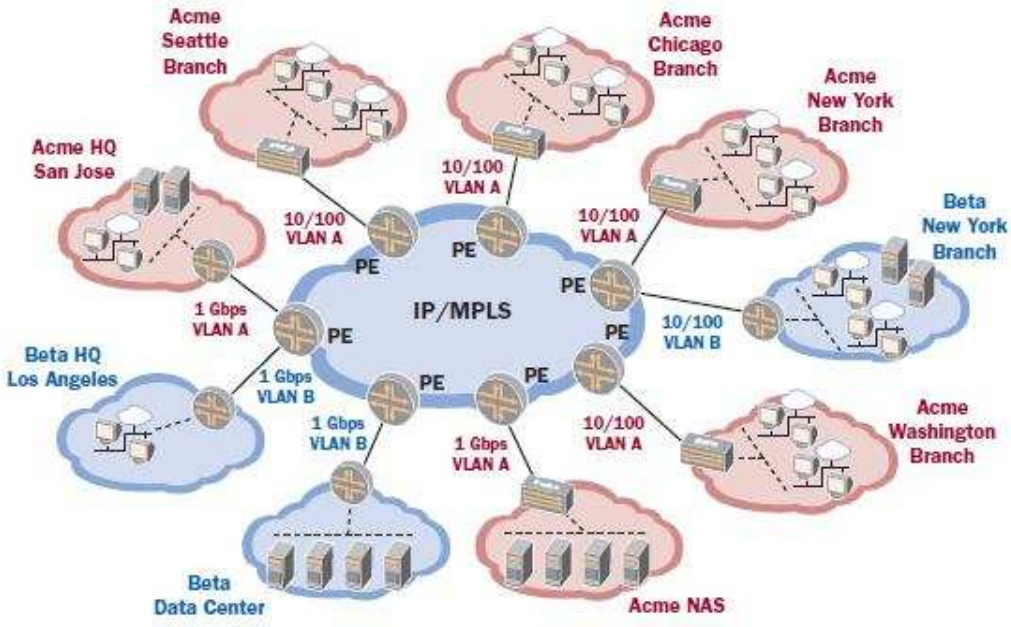
MPLS-verkossa PE-reitittimet määrittävät uniikin leiman jokaiselle VPN:lle. Määritys suoritetaan, vaikka seuraavan paketin reitti pysyisikin samana. VPN-leimojen ja normaaleiden MPLS-leimojen levitys saadaan pidettyä erillään käyttämällä kaksikerroksista leimapinoa.

VPN-reititysinformaatio PE-reitittimille välitetään MPLS-verkossa käyttämällä tarkoitukseen sopivaa MP-BGP-reititysprotokollaa. Reititettävän paketin saapuessa reunareitittimelle muunnetaan sen IPv4-prefiksi (etuliite) VPNv4-prefiksiksi (Virtual Private Network version 4), jonka jälkeen paketti kuljetaan runkoverkon läpi. Muunnoksessa IPv4-prefiksiin lisätään 64-bittinen *Route Distinquisher* eli RD. Alkuperäinen prefiksi sekä lisätty RD muodostavat yhdessä NLRI-arvon (Network Layer Reachability Information), joka viittaa kohteen verkko-osoitteeseen. Lisäys tarjoaa eri asiakkaille mahdollisuuden käyttää päällekkäisiä IPv4-osoitteita lähiverkoissaan, niiden kuitenkaan vaikuttamatta runkoverkon toimintaan.

MPLS-runkoverkossa jokainen PE-reititin tarvitsee uniikin RID-tunnisteen (router ID), jota käytetään pakettien vastaanottoon ja lähetykseen. Yleensä RID-tunnisteena käytetään reitittimen 32-bittistä loopback-osoitetta.

5.3 Kakkostason VPLS-virtuaalilähiverkkopalvelu

VPLS (Virtual Private LAN Service) on siirtoyhteyskerroksella toteutettava VPN-kuljetustekniikka, jonka käyttö lisääntyy jatkuvasti MPLS-runkoverkoissa. VPLS antaa operaattorille mahdollisuuden tarjota lähiverkkojen yhdistämispalveluita olemassa olevaa MPLS-verkkoa käyttäen. Konsepti on yksinkertainen, asiakkaalle tarjotaan tunneloinnin avulla mahdollisuus yhdistää maantieteellisesti erillään sijaitsevia Ethernet-verkkoja yhdeksi loogiseksi Ethernet- tai VLAN-alueeksi (Virtual Local Area Network) (kuva 6). [15.] Tekniikan etuja ovat niin ikään sekä kustannustehokkuus että kohonneet siirtonopeudet, koska toimipaikat voidaan yhdistää luotettavasti joko Fast Ethernet- tai Gigabit Ethernet -tekniikalla.

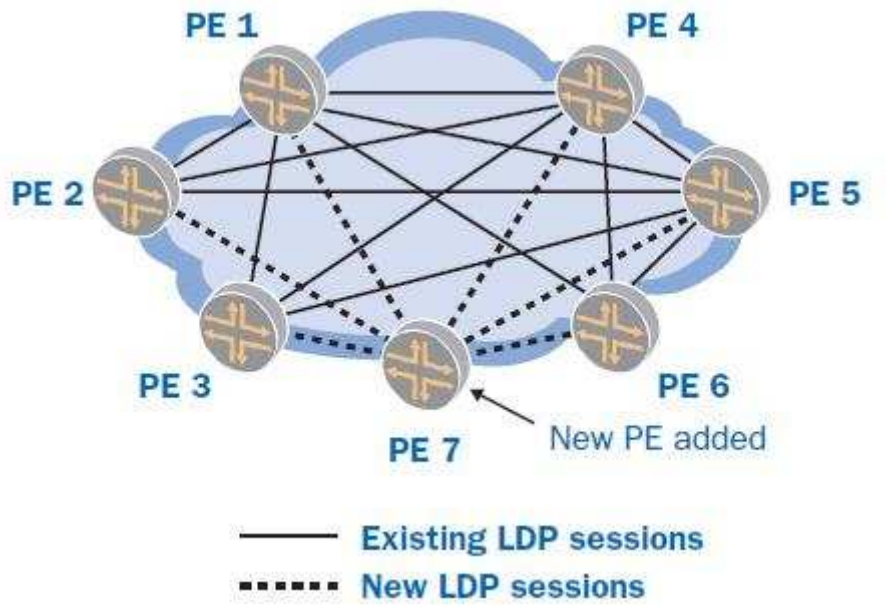


Kuva 6. VPLS toteutus [16]

VPLS eroaa kolmostason toteutuksesta toimintatavoiltaan. Parien muodostus voidaan suorittaa käyttämällä joko BGP- tai LDP-protokollaa.

Käytettäessä LDP:n laajennettua toimintatapaa parin muodostukseen *hello*-viestit lähetetään suoraan jo tiedossa olevalle LSR:lle. Parin muodostamisen jälkeen VPLS:ää tukevat PE-reunalaitteet muodostavat tunnelin, jonka avulla ne kuljettavat Ethernet-kehyksiä verkon läpi. VPLS MPLS käyttää kaksikerroksista leimapinoa, jonka ensimmäisellä kerroksella on reunalaitteen ulosmenoportin kertova VC-leima (Virtual Circuit). Uloimmalla kerroksella sijaitsee Ethernet-paketin leima, jonka avulla paketti kuljetetaan runkoverkon läpi. [17.]

Suurien verkkojen tapauksessa LDP:n käyttö aiheuttaa ylläpidolle ylimääräistä työtä, koska tunnelit useiden PE-laitteiden välille pitää muodostaa manuaalisesti (kuva 7). Lisääntynyt työmäärä taas osaltaan vaikuttaa tarjottavan palvelun hintaan sekä mahdollisten virheiden syntyyn.

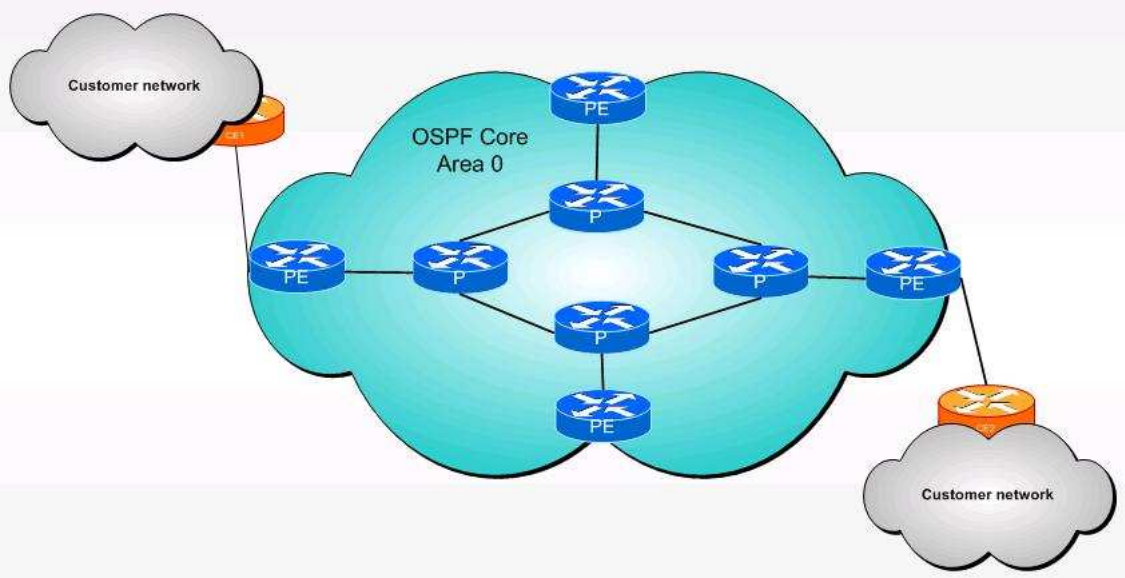


Kuva 7. Käytettäessä LDP:tä vaaditaan useita tunneleita täyden kattavuuden saamiseksi [16]

Muita kakkostason MPLS VPN -toteutuksia ovat Virtual Private Wire Service (VPWS), Virtual Private Multicast Service (VPMS) sekä IP-only L2VPN [18].

6 Laboratorioverkon toteutus

Seuraavien alalukujen tarkoituksena on tutustua verkon rakenteeseen (kuva 8). Aluksi käydään läpi verkon suunnittelun perusajatukset sekä tekninen toteutus. Myöhemmin selvitetään MPLS-leimakytkennän käyttöönotto IP-verkossa sekä leimakytkentää hyödyntävän kolmostason MPLS VPN -yhteyden toteutus.



Kuva 8. Runkoverkon rakenne

6.1 Suunnittelu

Insinöörityön tarkoituksena oli suunnitella ja toteuttaa Metropolia Ammattikorkeakoulun oppimisympäristöön soveltuva MPLS-runkoverkko, jonka avulla opiskelijat voivat tutustua MPLS VPN -yhteyksiin käytännössä. Metropolialla on Leppävaaran toimipisteessään käytettävissä neljä laboratoriotilaa, joissa kyseistä MPLS-verkkoa halutaan hyödyntää. Suunnittelun lähtökohtana pidetään mahdollisuutta rakentaa jokaiseen neljään laboratoriotilaan täysin identtiset liityntäpisteet MPLS-runkoverkkoon, jolloin samat käytännön ohjeistukset pätevät käytettävästä tilasta riippumatta. Toteutettaessa oppimisympäristöön soveltuvaa MPLS-runkoverkkoa täytyy

suunnittelussa huomioida niin runkoverkon toimivuus kuin mahdollisuudet verkon kehittämiseen ja laajentamiseen tulevaisuudessa.

Suunnittelussa on otettava huomioon seuraavat pääkohdat:

- verkon laitteet
- asiakasverkkojen liitäntä runkoverkkoon
- verkon topologia
- käytettävät osoitteet
- runkoverkon reititys
- asiakasverkkojen reititys
- runkoverkon toiminnan verifiointi.

6.1.1 Verkon laitteet

Koska Metropolia Ammattikorkeakoulu on Ciscon yhteistyökumppani käytettävä laitteisto on kaikilta osin kyseisen valmistajan tuotantoa. Runkoverkon muodostavat Ciscon 2811-sarjan reitittimet, joita käytetään niin P- kuin PE-laitteina. 2811-sarjan reitittimet sisältävät oletuksena kaksi 100 Mbit/s FastEthernet-liitäntää. Tarpeen vaatiessa porttimäärää voidaan kasvattaa lisäämällä verkkomoduuleja joita on saatavilla useilla eri liitäntätekniikoilla. Reitittimien IOS-käyttöjärjestelmän (Internetwork Operating System) versio valitaan tarvittavien ominaisuuksien mukaan, joita ovat MPLS, LDP, TE, QoS sekä MPLS-VPN.

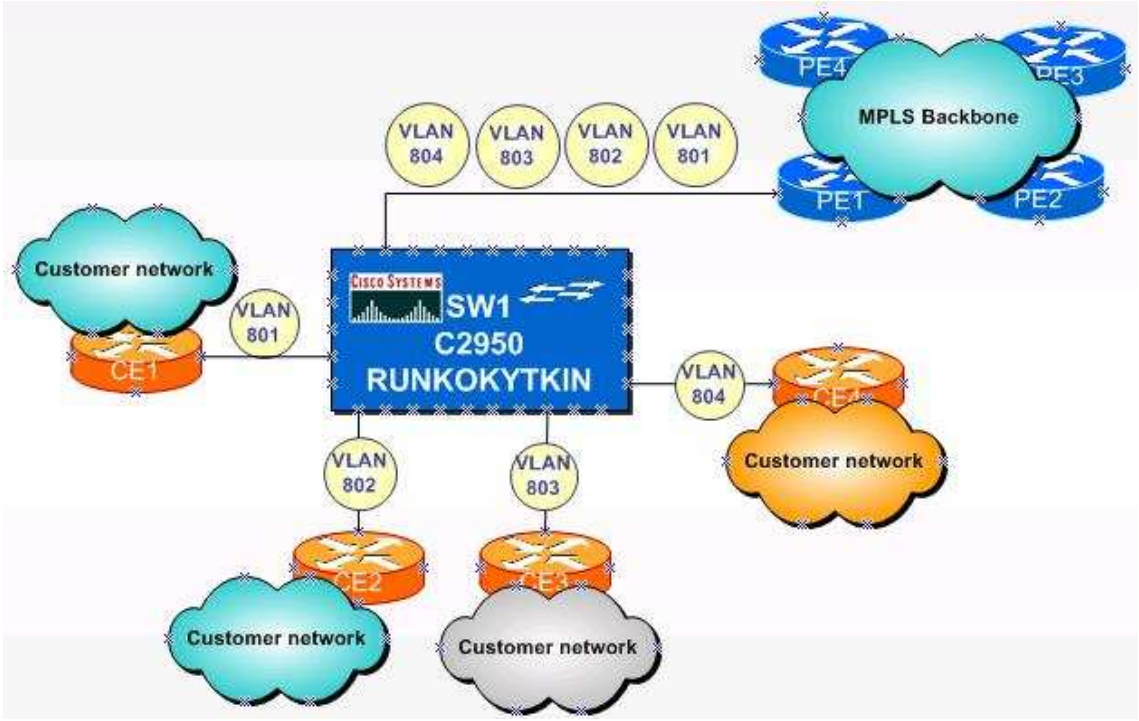
Asiakasyhteyksien CE-reitittiminä voidaan käyttää 1600-, 2600- tai 2800-sarjan reitittimiä. Asiakasyhteyksissä käytettävä reititinmalli riippuu käytettävän opetustilan tarjoamasta laitteistosta. Asetusten määrittelyyn käytettävän reitittimen malli ei juurikaan vaikuta.

Verkon topologiasta johtuen PE- ja CE-reitittimien välillä käytetään OSI-järjestelmän kakkostasolla toimivia verkkokytkimiä, jotka eivät sisällä kolmostason reititysominaisuuksia. Toteutuksen kohteena olevassa laboratorioverkossa

runkokytkiminä käytetään Ciscon Catalyst 29xx-sarjan verkkokytkimiä, joissa on 24 FastEthernet-porttia, sekä kaksi GigaEthernet porttia. Ainoa vaatimus käytettäville kytkimille on riittävä porttimäärä sekä VLAN-tuki, jota ei aivan halvimmista peruskytkimistä löydy.

6.1.2 Asiakasverkkojen liitäntä runkoverkkoon

Normaalisti asiakasyhteydet palveluntarjoajan runkoverkkoon toteutetaan joko kuparijohtimilla, käyttämällä radiolinkkiä tai optisilla kuiduilla. Ensisijaisesti toteutustapaan vaikuttaa asiakkaan tarvitsema verkkokapasiteetti ja toissijaisesti asiakkaan toimipisteen sijainti. Koska rakennettava runkoverkko toimii Metropolia Ammattikorkeakoulun kampusalueella voidaan asiakasyhteydet toteuttaa käyttämällä jo olemassa olevaa FastEthernet-kaapelointia. Asiakasyhteyden CE-reititin kytketään luokkatilassa sijaitsevaan runkokytkimeen, joka on yhdistetty CAT5-kaapeloinnin avulla runkoverkon PE-reunareitittimelle sekä muiden luokkien runkokytkimiin. Jokaiselle asiakasyhteydelle on määritetty runkokytkimessä oma kytkinportti (kuva 9).



Kuva 9. Asiakasverkkojen liitäntä runkoverkkoon

Runkokytkimen määritykset

Runkokytkinten sisällä asiakkaiden yhteydet saadaan pidettyä erillään käyttämällä VLAN-tunnisteita. VLAN tulee sanoista Virtual Local Area Network. VLANien käyttö mahdollistaa loogisen segmentoinnin kytkimissä. Segmentoinnin avulla varmistetaan se, että asiakkaan tiedot eivät missään vaiheessa pääse sekoittumaan jonkun toisen asiakkaan tietojen kanssa.

Käytettäessä useita identtisiä runkokytkimiä on niiden VLAN-asetuksien oltava yhdenmukaisia sekaannusten välttämiseksi. Yhdenmukaisuuden varmistamiseen on kehitetty VTP-protokolla (VLAN Trunking Protocol), joka hallinnoi VLANien lisäystä, poistoa ja nimeämistä. Toisiinsa kytketyt kytkimet muodostavat VTP-alueen eli domainin. VTP-alueella jokin kytkimistä toimii VTP-palvelimena (server), sen lisäksi alueella voi olla yksi tai useampi asiakaskytkin (client). VLANien lisäys ja poisto voidaan suorittaa ainoastaan VTP-palvelimella, jonka tehtävänä on huolehtia alueeseen kuuluvien kytkinten VLAN-tietokantojen yhdenmukaisuudesta. [19.]

Käytettäessä useita kytkimiä on hyvä mainita myös Spanning Tree -protokolla. Kyseinen protokolla on kehitetty kakkostason silmukoiden (loop) havainnointiin ja estämiseen verkoissa. Kytkimet keskustelevat keskenään huomatakseen verkkoon muodostuvat silmukat, ennen kuin ne aiheuttavat vahinkoa. Silmukan muodostus estetään sulkemalla tarpeettomia kytkinportteja. Protokollan käyttämän algoritmin ansiosta kytkimet pystyvät muodostamaan silmukattoman topologian verkosta.

Runkoreitittimen määritykset

Runkoreitittimellä asiakkaiden yhteydet toteutetaan niin sanottua inter-VLAN toteutusta käyttäen. [20.] Toteutuksessa runkoreitittimellä asiakkaalle määritetään aliportti liittyen siihen porttiin joka on runkoportti (trunk) käytettävän runkokytkimen ja PE-reitittimen välillä. Jos käytettävän runkoportti on esimerkiksi FastEthernet 0/1, asiakkaan aliportti voi olla muotoa FastEthernet 0/1.801. [21.]

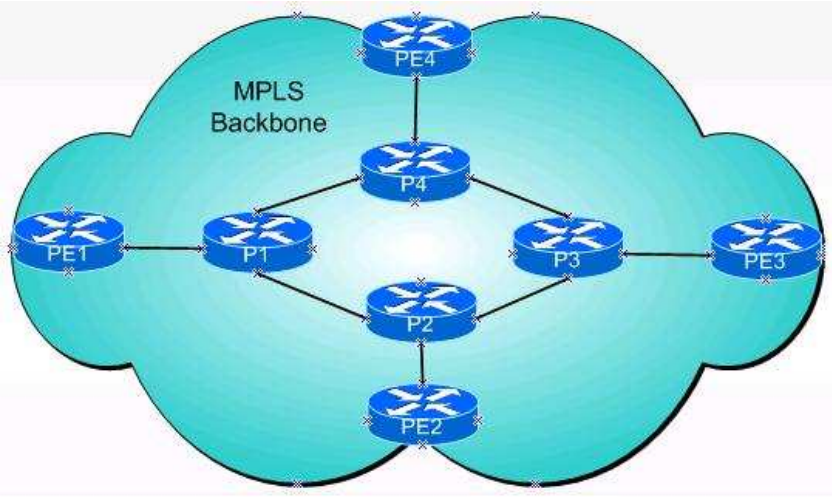
Runkoportin vaatima enkapsulointi kytkimen ja reitittimen välille voidaan suorittaa joko isl- (Inter-Switch Link) tai 802.1Q-protokollaa käyttäen. Protokollilla on sama toimintaperiaate, mutta ne käyttävät erilaista tiedostomuotoa. ISL toimii ainoastaan Ciscon verkkolaitteilla, kun 802.1Q puolestaan on usean laitteistovalmistajan tukema.

6.1.3 Verkkotopologia

Suunnittelun kannalta verkon topologia muodostuu kahdesta osasta. Runko-osan muodostavat verkon P- ja PE-laitteet, kun taas asiakasosa koostuu PE- ja CE-laitteista sekä niiden välisistä yhteyksistä. Verkkotopologian muoto on niin sanottu laajennettu tähti, jossa yksittäiset tähdet on liitetty hierarkkisesti toisiinsa.

Runkoverkko

Toteutettavan MPLS-runkoverkon muodostavat kahdeksan reititintä, jotka toimivat kuvan 10 mukaisesti joko P- tai PE-reitittiminä. Reitittimien rooli määräytyy niiden sijoituspaikan ja tehtävien mukaan. P-reitittimet on sijoitettu runkoverkon keskelle, jolloin niiden tehtävänä on kytkeä datapaketteja leimainformaation perusteella. PE-reitittimet vuorostaan sijaitsevat MPLS-pilven reunalla, josta ne ovat yhteydessä asiakasverkkojen suuntaan sekä ylläpitävät MPLS-reititystauluja.

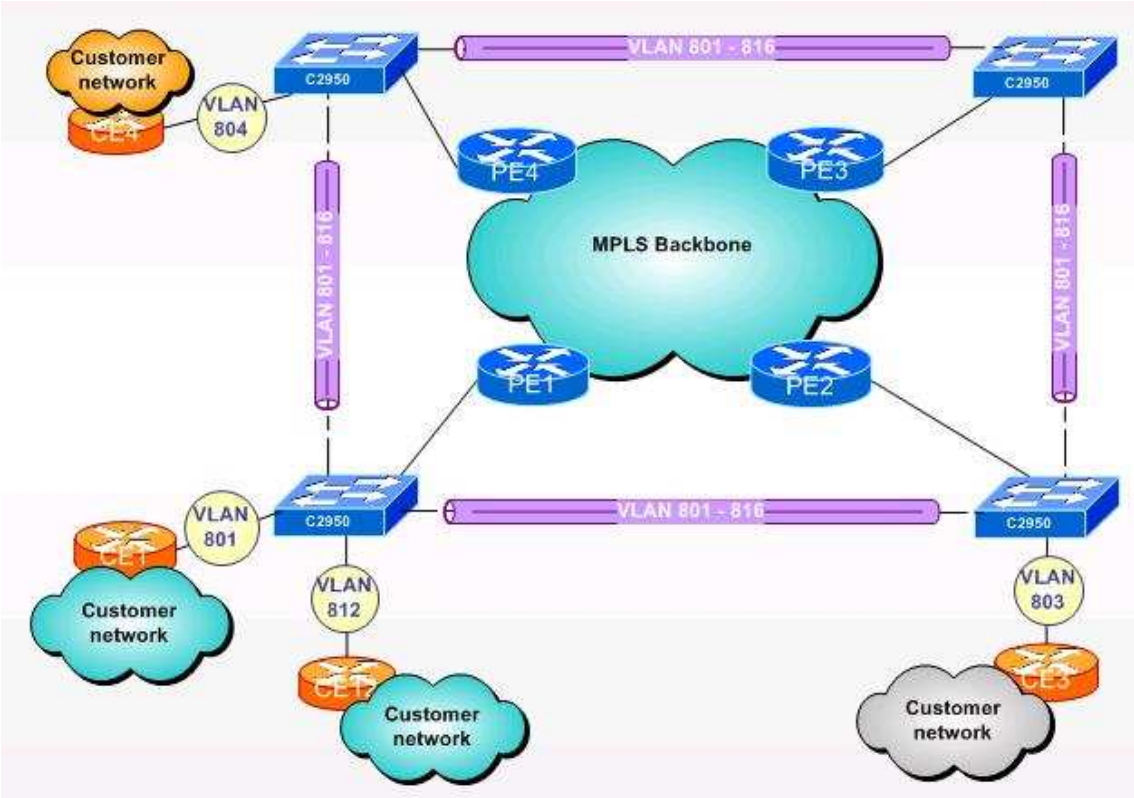


Kuva 10. MPLS-runkoverkko

Asiakasverkot

Asiakasverkkoihin toteutettavan verkon topologiassa kuuluvat asiakasyhteyksien CE-reitittimet, neljä kappaletta runkokytkimiä sekä niihin liitetyt PE-reunareitittimet.

Alkuperäisen suunnitelman mukaan Leppävaaran toimipisteeseen halutaan neljä identtistä liityntäpistettä MPLS-runkoverkkoon. Suunnitelma on mahdollista toteuttaa käyttämällä inter-VLAN toteutustapaa asiakasverkkojen liittämiseksi runkoverkkoon. Suunnitelman mukaisesti runkokytkimet vaihtavat keskenään VLAN-tietoja VTP-protokollaa käyttäen, jonka vuoksi niiden välille vaaditaan kakkostason verkkoyhteys. Kakkostason yhteys saadaan muodostamalla kytkinten välille fyysinen runkoyhteys (trunk). Runkoverkon liityntäpisteiden ollessa identtisiä voidaan asiakasyhteyden reititin liittää mihin tahansa runkokytkimeen, kunhan käytetään sille osoitettua kytkinporttia. Asiakasverkkojen suuren määrän vuoksi ei niitä kaikkia ole esitetty kuvan 11 topologiassa.



Kuva 11. Asiakasverkkojen topologia

6.1.4 Käytettävät osoitteet

Projektia varten Metropolia Ammattikorkeakoulun tietohallinnolta allokoitiin yksityinen A-luokan osoiteavaruus 10.255.0.0/16. Varauksen ansiosta kyseisen verkkoavaruuden osoitteita ei tulla käyttämään muissa projekteissa. Laboratorioverkolle varattu 16-bittinen osoiteavaruus mahdollistaa maksimissaan 256 kappaletta 24-bittisiä aliverkkoja sekä 65536 IP-osoitetta. Käyttämällä vaihtuvamittaisia verkkomaskeja voidaan osoiteavaruudesta muodostaa maksimissaan 16384 pienempää aliverkkoa.

Verkkoavaruus jaettiin aliverkkoihin seuraavasti:

- 10.255.0.0/24 – 10.255.127.0/24 Leppävaaran asiakasverkkojen osoitteet
- 10.255.128.0/24 – 10.255.253.0/24 Bulevardin toimipisteen asiakasverkot
- 10.255.254.0/24 Bulevardin toimipisteen runkoverkon osoitteet
- 10.255.255.0/24 Leppävaaran toimipisteen runkoverkon osoitteet.

Verkkoavaruuden jakamisessa otettiin huomioon käytännön asiat, kuten käytettävissä olevien osoitteiden suuri määrä sekä mahdollinen verkon laajennus Bulevardin toimipisteen alueelle. Koska tämä insinöörityö keskittyy ainoastaan Leppävaaran toimipisteen alueelle, jätetään Bulevardia koskevat varaukset käsittelemättä sen tarkemmin.

Leppävaaran rungon verkkoavaruus jaettiin osiin seuraavasti:

- 10.255.255.0/26 Runkoreitittimien väliset yhteydet sekä loopback-osoitteet
- 10.255.255.64/26 Runko- ja reunareitittimien väliset osoitteet
- 10.255.255.128/25 Reuna- ja asiakasreitittimien väliset yhteydet.

6.1.5 Runkoverkon reititys

Runkoverkon reititykseen on käytettävissä useita dynaamisia reititysprotokollia. Käytettävän reititystekniikan valinnassa verkon ylläpitäjällä sekä suunnittelijalla täytyy olla ymmärrystä valittavan protokollan toiminnasta, suunnittelusta, testauksesta sekä käyttöönotosta, jotta saataisiin valittua juuri se oikea ja tarpeeseen sopivin reititysprotokolla.

Reititysprotokollia on tarjolla useita [22, s. 69]:

- RIPv1 (Routing Information Protocol, version 1)
- RIPv2 (Routing Information Protocol, version 2)
- OSPF (Open Shortest Path First)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- IGRP (Interior Gateway Routing Protocol)
- IS-IS (Intermediate System to Intermediate System)
- BGP (Border Gateway Protocol).

Tässä insinöörityössä runkoverkon reititykseen käytettiin OSPF (Open Shortest Path First) -linkkitilaprotokollaa, joka kehitettiin vastaamaan suurien verkkojen vaatimuksiin korvaten samalla vanhempaa ja laajalti käytössä olevaa RIP-reititysprotokollaa. OSPF verkot toimivat Autonomous System (AS) -alueella, joka on joukko verkkoja, joilla on yhteinen päämäärä reitityksen suhteen. OSPF:ää käyttävät verkot jaetaan alueisiin (area), jolloin liikennettä kyseisillä alueilla voidaan kontrolloida hallitusti ja näin vähentää reitittimien kuormitusta. Alueen muodostavat reitittimet, jotka käyttävät yhtenäistä verkkotopologiaa sekä samoja reititysalgoritmeja. [22, s. 87.]

OSPF:n etuja esimerkiksi IS-IS-protokollaan verrattuna ovat reititystietojen vaihto, IS-IS:n jatkuvan reititystaulujen siirron sijaan OSPF lähettää tiedot vain muuttuneista reiteistä. OSPF osaa myös käsitellä eripituisia verkkomaskeja sekä yhdistää useita alueita yhdeksi loogiseksi alueeksi. OSPF ei ole määrittele rajoituksia verkon koon suhteen, joten se sopii hyvin runkoverkon reititysprotokollaksi. [23.]

OSPF-verkossa jokaisella alueen reitittimellä on yhteneväinen topologia kuvaus verkosta, jonka perusteella voidaan suorittaa reittien valinnat. Reititin laskee verkkopuun, jossa se itse sijaitsee ylimpänä, ja muut reitittimet sekä verkot sen alahaaroina. Reitit lasketaan ja valitaan niin sanotun linjataksan mukaan, siten että nopeammalla linjalla on pienempi taksa. Näin pyritään lähettämään paketteja nopeampaa linjaa pitkin jättäen hitaampi linja johonkin muuhun käyttöön. Vaikka reititin lähettääkin paketin vain seuraavalle reitittimelle, laskee se kuitenkin koko reitin taksan, jonka mukaan suoritetaan seuraavan hypyn valinta. Mikäli kohteeseen on kaksi samanarvoista reittiä, käytetään niitä kumpaakin kuormituksen tasaamiseksi.

6.1.6 Asiakasverkkojen reititys

Rungon ja tilaajan reitittimen väliseen reititykseen on käytettävissä useita dynaamisia reititystekniikoita, kuten RIP, RIP v2, OSPF ja EIGRP sekä staattiset- ja oletusreitit.

Staattinen reititys tarkoittaa sitä, että käytettävät reitit määritetään reitittimille manuaalisesti. Oletusreittien tapauksessa määritetään vain seuraavan hypyn osoite, jonka takaa oletetaan tuntemattomien verkkojen löytyvän. Dynaamisessa reitityksessä reittitietojen vaihtamiseen käytetään reititysprotokollaa, esimerkiksi RIP v2.

Tässä työssä tilaajan verkkojen reititykseen käytetään staattisia sekä oletusreittejä. Ne ovat optimaalinen toteutustapa tilanteessa, jossa asiakkaalla on käytössään vain yksi toimipiste, pieni määrä aliverkkoja tai molemmat vaihtoehdot täyttävä infra. Lisäetuna staattiset reitit myös estävät asiakasta tai operaattoria jakamasta tahallaan tai vahingossa väärää reititysinformaatiota, joka muiden reititysprotokollien tapauksessa olisi huomattavasti helpompaa.

Verkon kasvaessa tai muuttuessa reitit täytyy päivittää manuaalisesti, koska staattinen reititys ei tue dynaamista uudelleenreititystä. [9, s. 111.]

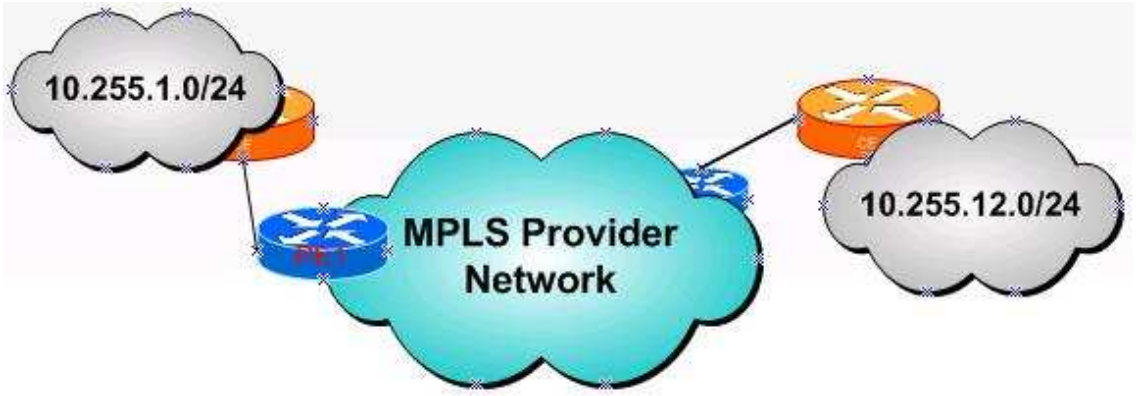
6.1.7 Runkoverkon toiminnan verifiointi

Seuraavaksi tarkastellaan runkoverkon asetuksia, reititykseen liittyviä tietoja sekä suoritetaan muutamia perustestejä. Testien tarkoituksena on varmistaa runkoverkon toimivuus ja todentaa liikenteen kulku verkon läpi. Seuraavasta osittaisesta tulosteesta nähdään verkkoliitäntöjen sekä reitityksen määrittelyjä PE1-reitittimeltä. Tulosteesta selviää käytettävän aliporttia, 802.1Q (dot1Q) -enkapsulointia, OSPF-reititysprotokollaa sekä staattisia reittejä suunnitelman mukaisesti.

PE1#show running-config

```
!
interface Loopback0
 ip address 10.255.255.53 255.255.255.255
!!
interface FastEthernet0/1.801
 encapsulation dot1Q 801
 ip address 10.255.255.129 255.255.255.252
!
router ospf 65500
 log-adjacency-changes
 redistribute static
 redistribute static subnets
 network 10.255.255.0 0.0.0.127 area 0
!
ip route 10.255.1.0 255.255.255.0 10.255.255.130
ip route 10.255.2.0 255.255.255.0 10.255.255.134
```

Verkon toimivuus voidaan verifioida ping- ja tracert-testeillä. Ping-testillä pystytään tarkistamaan, onko yhteys kunnossa. Tracert-testillä puolestaan voidaan tarkistaa, mitä reittiä paketti kulkee määränpäähänsä. Runkoverkon toiminnan verifioimiseksi testit suoritetaan asiakasverkkojen 10.255.1.0 ja 10.255.12.0 välillä. Kyseiset verkot soveltuvat hyvin testiin, koska ne sijaitsevat fyysisesti runkoverkon eri puolilla ja näin ollen testi kattaa koko runkoverkon (kuva 12).



Kuva 12. Testiverkko

Ensiksi suoritetaan ping-testi IP-osoitteeseen 10.255.12.2, kyseinen osoite on toiseen asiakasverkkoon kytketyn tietokoneen verkko-osoite. Testi suoritetaan asiakasverkkoon 10.255.1.0/24 yhdistetyltä tietokoneelta. Tulos kertoo yhteyden olevan kunnossa ja liikenteen kulkevan verkkojen välillä.

C:\ >ping 10.255.12.2

Pinging 10.255.12.2 with 32 bytes of data:
Reply from 10.255.12.2: bytes=32 time=2ms TTL=250
Reply from 10.255.12.2: bytes=32 time=2ms TTL=250
Reply from 10.255.12.2: bytes=32 time=2ms TTL=250
Reply from 10.255.12.2: bytes=32 time=2ms TTL=250

Ping statistics for 10.255.12.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms

Komennolla *tracert 10.255.12.2* nähdään paketin käyttämä reitti sekä keskimääräinen viive verkon toisella puolella sijaitsevaan tietokoneeseen. Tuloksen perusteella voidaan todeta liikenteen kulkevan kohteeseen odotetusti ilman suurempia ongelmia.

C:\ >tracert 10.255.12.2

Tracing route to 10.255.12.2 over a maximum of 30 hops

1 1 ms <1 ms <1 ms 10.255.1.1
2 1 ms 1 ms <1 ms 10.255.255.129
3 1 ms <1 ms <1 ms 10.255.255.65
4 2 ms 1 ms 1 ms 10.255.255.2
5 2 ms 1 ms 1 ms 10.255.255.74
6 2 ms 1 ms 1 ms 10.255.12.2
Trace complete.

6.2 MPLS:n käyttöönotto

Koska runkoverkko toimii odotetusti, on aika siirtyä eteenpäin ja ottaa käyttöön MPLS leimakytkentä. Luvussa 6.2 käydään lyhyesti läpi tärkeimmät käskyt leimakytkennän käynnistyksessä sekä suoritetaan muutamia perustestejä toiminnan verifioimiseksi. Täydellisiä ohjeita leimakytkennän käyttöönottamiseksi runkoverkoissa ei tässä insinöörityössä tulla esittämään. Ohjeet MPLS-tekniikan käyttöönottoon löytyvät lähteenä 9 käytetystä kirjasta ”MPLS Configuration on Cisco IOS Software”.

6.2.1 Keskeiset käskyt käyttöönotossa

Seuraavissa erimerkeissä käsitellään lyhyesti tärkeimmät käskyt MPLS:n käyttöönottoon. [9, s. 35–41.]

Tukijalkana MPLS:n toiminnalle on *Cisco Express Forwarding* -toiminne. CEF on reitittimen sisäinen kytkentätekniikka, jonka avulla voidaan määrittää, kuinka paketti reititetään seuraavalle solmupisteelle. CEFiä käytetään muutenkin kuin MPLS-tekniikan kanssa. CEFin käynnistys suoritetaan yleisessä määrittelytilassa *ip cef* -komennolla, uudemmissa IOS versioissa CEF on käytössä oletusarvoisesti. Erikoistapauksissa CEF voi olla pois toiminnasta myös porttikohtaisesti, jolloin se saadaan palautettua takaisin käyttöön *ip route-cache cef* -komennolla.

Komennolla *mpls label protocol [ldp | tdp]* valitaan leimanjakoprotokollaksi LDP. Leimanjakoprotokollan valinta on tarpeellinen ainoastaan vanhempien Ciscon IOS-käyttöjärjestelmien kanssa sekä siirryttäessä TDP:stä LDP:n käyttöön tai toisinpäin. Uudemmissa käyttöjärjestelmissä LDP on oletusarvoisesti valittuna.

Leimanjakoprotokolla LDP käyttää pakettien vastaanottoon ja lähetykseen reitittimen RID-tunnistetta. Oletusarvoisesti tunnisteena käytetään korkeimman IP-osoitteen omaavaa loopback-porttia. Loopback-portin käyttö on suotavaa portin ollessa ulkoisista tekijöistä riippumaton ja aina käytettävissä. Erikoistapauksissa tunnisteeksi valitaan reitittimen korkein IP-osoite, jos paikallista loopback-porttia ei syystä tai toisesta ole

määritelty. Manuaalisesti RID-tunniste voidaan määrittää komennolla *mpls ldp router-id [interface-type number]*. Leimakytkentä määritetään siihen osallistuville verkkoliitännöille komennolla *mpls ip*.

Koska runkoverkossa käytetään MPLS-leimapinoa, on pakettien *Maximum Transmission Unit* eli MTU huomioitava konfiguraatiossa. MTU on suurin mahdollinen pakettikoko, joka voidaan toimittaa verkon läpi. Perinteisessä reitittävässä verkossa maksimipakettikoon ylittävä paketti pudotetaan automaattisesti. MPLS-verkossa pakettia ei kuitenkaan pudoteta, vaan se fragmentoidaan ja kuljetetaan pakettikoon sallimissa osissa. Oletusarvoisesti maksimipakettikoko on 1500 tavua. Käytettäessä kolmikerroksista leimapinoa pakettikooksi muodostuu 1512 tavua (1500+4+4+4). Komennolla *mpls mtu override 1512* muutetaan pakettikoko vastaamaan haluttua.

6.2.2 Pakettikytkennän verifiointi

Runkoverkon MPLS määrittelyt on suoritettu, ja on aika tarkastella asetuksia sekä niiden vaikutusta järjestelmään eri kohteisiin. Seuraavassa nähdään osittaiset käyttömääritykset P1-reitittimeltä, MPLS toimintaan liittyvät rivit on merkitty keltaisella.

P1#show running-config

```
ip cef
!
mpls label protocol ldp
!
interface FastEthernet0/0
 description P1-PE1
 ip address 10.255.255.65 255.255.255.252
mpls mtu 1512
 mpls ip
!
router ospf 65500
 log-adjacency-changes
 network 10.255.255.0 0.0.0.127 area 0
!
mpls ldp router-id Loopback0
```

Pakettikytkennän toimintaa voi tarkastella seuraavilla komennoilla:

- *show ip cef* näyttää reitittimen kytkentätiedot.
- *show mpls interfaces* kertoo pakettikytkentään osallistuvat verkkoliitännät.
- *show mpls ldp discovery* tulostaa listan leimanjakoprotokolla LDP:n naapuruus-suhteista.
- *show mpls ldp neighbor* näyttää lisätietoja LDP:n naapureista.

Pakettikytkentään osallistuvan reitittimen leimataulu tulostuu komennolla *show mpls forwarding-table.* Osittaisesta taulusta käy ilmi reitittimen käyttämät leimat, verkon tunnukset, verkko-osoitteille määritetyt ulosmenoliitännät sekä seuraavien hyppyjen osoitteet.

P1#show mpls forwarding-table

Local Label	*Outgoing Label or VC*	*Prefix or Tunnel Id*	*Bytes Label Switched*	*Outgoing interface*	*Next Hop*
16	*16*	*10.255.1.0/24*	*10688*	*Fa0/0*	*10.255.255.66*
27	*27*	*10.255.12.0/24*	*8858*	*Se0/0/0*	*point2point*
32	*No Label*	*10.255.255.50/32*	*0*	*Se0/0/0*	*point2point*
33	*No Label*	*10.255.255.53/32*	*0*	*Fa0/0*	*10.255.255.66*
37	*Pop Label*	*10.255.255.72/30*	*0*	*Se0/0/0*	*point2point*

Lopuksi verifioidaan leimakytkennän toiminta traceroute-komennolla. Toiminnolla tutkitaan reitti PE1-reitittimeltä IP-osoitteeseen 10.255.12.2, joka on testiin osallistuvan asiakasyhteyden tietokoneen verkko-osoite. Tulosteesta voidaan verifioida käytettävän leimakytkentää pakettien välitykseen. Ensimmäiselle hypylle on käytetty leimaa arvolla 27, joka vastaa edellä esitetyn taulukon mukaisesti reittiä verkkoon *10.255.12.0/24.*

PE1#traceroute 10.255.12.2

1 10.255.255.65 [MPLS: Label 27 Exp 0] 4 msec 0 msec 0 msec
2 10.255.255.2 [MPLS: Label 27 Exp 0] 4 msec 0 msec 4 msec
3 10.255.255.74 [MPLS: Label 27 Exp 0] 4 msec 0 msec 4 msec
*4 10.255.255.174 4 msec 0 msec **

6.3 Kolmostason VPN-yhteyden käyttöönotto

Luvussa 6.3. käydään läpi tärkeimmät määritykset kolmostason VPN-yhteyden käyttöönotossa sekä VPN-yhteyden verifiointi.

6.3.1 VPN-määritykset

Komennolla *ip vrf [vrf-name]* määritetään yhteydelle VRF-nimi, joka on asiakaskohtainen ja määrittää VPN-yhteyden asiakasverkosta PE-reitittimelle. Yksittäinen reititin voi sisältää useita VRF-tauluja. VRF-taulu sisältää tiedot reititysprotokollista, IP-reititystaulusta, CEF-taulusta sekä käytettävistä porteista ja säännöistä. [9, s. 96–99.]

VRF-nimen lisäksi määritellään asiakaskohtainen 64-bittinen Route Distinquisher -numero, jonka avulla muodostetaan reititystauluja. RD:n käytön tarkoituksena on erottaa asiakkaiden verkko-osoitteet muiden asiakkaiden vastaavista tekemällä IPv4-prefikseistä uniikkeja VPNv4-prefiksejä.

RD voi koostua seuraavista vaihtoehdoista [9, s. 97]:

- 16-bittinen AS-numero: 32-bittinen numero (esim. 65500:100)
- 32-bittinen IP-osoite: 16-bittinen numero (esim. 10.10.10.101:1).

RD:n lisäys suoritetaan komennolla *rd [route-distinquisher]*. Tässä työssä RD-numerona käytetään alueen AS-numeroa 65500 sekä numeroa 100, joka edustaa määritettävän asiakasyhteyden tunnusta.

RD:n lisäksi lisätään Route Target eli RT. Komennolla *route-target [import | export | both] [RD-numero]* määritetään reititin vaihtamaan VRF-tietoja ainoastaan tunnettua RD-tunnusta käyttävien reitittimien kanssa.

Viimeiseksi assosioidaan VRF halutulle sisääntuloliitännälle komennolla *ip vrf forwarding [vrf-name]*. Huomioitavaa on, että VRF:n lisäys tai poisto liitännältä poistaa määritellyn IP-osoitteen, joka on asetettava takaisin manuaalisesti.

6.3.2 PE – PE-reititys

MPLS-VPN verkossa PE-laitteiden väliseen kommunikointiin käytetään MP-BGP-protokollaa, joka välittää VPN-reititysinformaation laitteiden välillä. Komennolla *router bgp [autonomous-system]* käynnistetään prosessi, jossa *autonomous-system* -numero kertoo AS-alueen tunnuksen. [21, s. 99–103.] Turvallisuussyistä käytetään yksityistä AS-numeroa 65500, jonka IANA (The Internet Assigned Numbers Authority) on varannut yksityiskäyttöön, eikä se näin ollen tule koskaan käytettäväksi julkisessa internetissä. [24.]

Komennolla *neighbor [ip-address | peer-group-name] remote-as [as-number]* määritetään PE-reititin, jonka kanssa halutaan vaihtaa VPN-reititysinformaatioita. Yleisesti BGP:n viestien lähetykseen ja vastaanottoon käytetään paikallista loopback-porttia, joka määritetään komennolla *neighbor [ip-address | peer-group-name] update-source [interface-type interface number]*.

Seuraavaksi aktivoidaan address-family -toiminne, jonka alaisuudessa toimivat VPNv4-naapurukset kuljettavat VPNv4-paketteja runkoverkon läpi. Aktivointi tapahtuu komennoilla *address-family vpnv4* ja *neighbor [ip-address] activate.*

Viimeiseksi määritetään VRF-IPv4 address-family -toiminne. Se muuntaa IPv4-verkot VPNv4-tiedoiksi, jotka kuljetetaan MP-BGP:n avulla runkoverkon läpi. *Redistribute connected* -käskyllä mainostetaan suoraan kytkeytyneitä verkkoja.

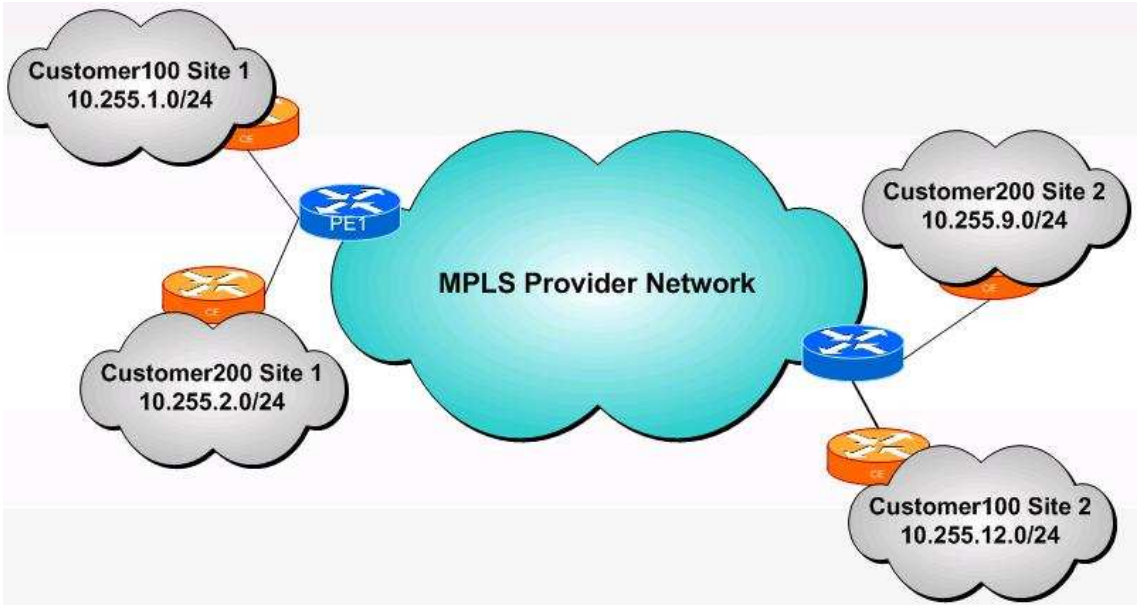
6.3.3 PE – CE-reititys

Lopuksi määritellään asiakasyhteyden reititys PE- ja CE-laitteiden välille. Reititys voidaan suorittaa joko staattisesti tai reititysprotokollaa käyttäen. Runkoverkon testivaiheessa käytössä oli staattinen reititys, joten pitäydytään sen käytössä edelleenkin. Staattinen VPN-reititys määritetään komennolla *ip route vrf [vrf-name] [destination prefix] [destination prefix mask] [next-hop]*.

Reititys CE:n suuntaan on kunnossa, joten seuraavaksi määritellään asetukset runkoverkon suuntaan. Asiakasverkkojen staattiset reitit saatetaan BGP:n tietoon *redistribute static* -komennolla.

6.4 VPN-yhteyden testaus

Seuraavilla sivuilla on nähtävissä muutamia käskyjä, joiden avulla tarkastellaan reititys- ja lipputauluja sekä niihin liittyvää informaatiota. Kaikki tulosteet ovat PE1-reitittimeltä, ja ne sisältävät tietoja saman asiakkaan VPN-yhteydestä. Kuvassa 13 on nähtävillä VPN-yhteydet, joiden avulla testaukset suoritetaan.



Kuva 13. VPN-yhteydet runkoverkossa.

Käskyllä *show ip cef vrf Customer100* nähdään *Customer100* -nimisen asiakkaan VPN-yhteyteen liittyvä CEF-taulu. Taulusta on nähtävissä kyseiseen VPN-yhteyteen liittyvät verkot, sekä niiden kytkentätiedot. Esimerkiksi verkko *10.255.1.0/24* löytyy osoitteen *10.255.255.130* takaa, johon päästään käyttämällä ulosmenoliitäntänä *FastEthernet0/1.801*-porttia.

PE1# show ip cef vrf Customer100

Prefix	*Next Hop*	*Interface*
0.0.0.0/0	*no route*	
0.0.0.0/8	*drop*	
0.0.0.0/32	*receive*	
10.255.1.0/24	*10.255.255.130*	*FastEthernet0/1.801*
10.255.12.0/24	*10.255.255.65*	*FastEthernet0/0*
10.255.255.128/30	*attached*	*FastEthernet0/1.801*
10.255.255.128/32	*receive*	*FastEthernet0/1.801*
10.255.255.129/32	*receive*	*FastEthernet0/1.801*
10.255.255.130/32	*attached*	*FastEthernet0/1.801*
10.255.255.131/32	*receive*	*FastEthernet0/1.801*
10.255.255.172/30	*10.255.255.65*	*FastEthernet0/0*
127.0.0.0/8	*drop*	
224.0.0.0/4	*drop*	
224.0.0.0/24	*receive*	
240.0.0.0/4	*drop*	
255.255.255.255/32	*receive*	

Komennolla *show ip bgp vpnv4 rd 65500:100* tulostetaan BGP:n käyttämä vpnv4-reititystaulu RD-tunnukselle 65500:100. Taulukosta on luettavissa kyseiseen VPN-yhteyteen kuuluvat verkot reititystietoineen. Voidaan myös havaita BGP-protokollan oppineen VPN-reitit saman AS-alueen sisältä IGP:tä käyttäen.

PE1#show ip bgp vpnv4 rd 65500:100

BGP table version is 9, local router ID is 10.255.255.53
*Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,*
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
Route Distinguisher:	*65500:100 (default for vrf Customer100)*				
*> 10.255.1.0/24	*10.255.255.130*	*0*		*32768*	*?*
*>i10.255.12.0/24	*10.255.255.55*	*0*	*100*	*0*	*?*
*> 10.255.255.128/30	*0.0.0.0*	*0*		*32768*	*?*
*>i10.255.255.172/30	*10.255.255.55*	*0*	*100*	*0*	*?*

Asiakkaan VPN-yhteyteen liittyvä reititystaulu tulostetaan käskyllä *show ip route vrf [vrf-name]*. Tulosteen perusteella reittien muodostukseen on käytetty staattista reititystä sekä BGP reititysprotokollaa.

PE1#show ip route vrf Customer100

Routing Table: Customer100

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.255.255.128/30 is directly connected, FastEthernet0/1.801
B 10.255.255.172/30 [200/0] via 10.255.255.55, 00:12:48
S 10.255.1.0/24 [1/0] via 10.255.255.130
B 10.255.12.0/24 [200/0] via 10.255.255.55, 00:12:48

Seuraavassa tulosteessa nähdään kyseisen VPN-yhteyden leimataulu lisätietoineen. Taulusta löytyy tieto käytetyistä leimoista, näihin sidotuista verkko-osoitteista sekä PE-reitittimen toimista lippujen suhteen. Leimanarvolla 41 saapuva paketti tutkitaan PE:n

toimesta, leimainformaatio poistetaan ”pop”-operaatiolla, jonka jälkeen paketti reititetään lähiverkkoon IP-osoitteen perusteella.

PE1#show mpls forwarding-table vrf Customer100 detail

Local Outgoing Prefix Bytes Label Outgoing Next Hop
Label Label or VC or Tunnel Id Switched interface
*27 No Label 10.255.255.128/30[V] *
0 aggregate/Customer100
MAC/Encaps=0/0, MRU=0, Label Stack{}
VPN route: Customer100
No output feature configured
41 No Label 10.255.1.0/24[V] 312 Fa0/1.801 10.255.255.130
MAC/Encaps=18/18, MRU=1504, Label Stack{}
0017590A994B0025456DDC99810003210800
VPN route: Customer100
No output feature configured

Kun asiakkaan VPN-yhteys on valmis, täytyy sen toiminta vielä verifioida. Toiminnan tarkistus voidaan suorittaa ping- ja traceroute-komennoilla asiakasyhteyden CE-reitittimeltä tai suoraan asiakkaan tietokoneelta. Ping kertoo, onko yhteys kunnossa ja traceroute kertoo käytettävän reitin asiakasverkkojen välillä. Vikatilanteissa tracerouten avulla voidaan selvittää, mihin runkoverkon solmupisteeseen paketin kulku pysähtyy, joten se on oiva työkalu verkon ylläpidossa.

Seuraavissa kolmessa testissä tutkitaan pakettien kulkua runkoverkon läpi *Customer100*-nimistä VPN-yhteyttä käyttäen (kuva 13). Testauksessa on käytetty samoja asiakasverkkoja kuin aiemmissakin testeissä. Reitittimet CE1 ja CE12 kuuluvat Customer100-nimiseen asiakasyhteyteen, kun CE2- ja CE9-reitittimet muodostavat Customer200-asiakkuuden.

CE1#ping 10.255.12.1 source 10.255.1.1

Sending 5, 100-byte ICMP Echos to 10.255.12.1, timeout is 2 seconds:
Packet sent with a source address of 10.255.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

CE1#traceroute 10.255.12.1

Tracing the route to 10.255.12.1
1 10.255.255.129 0 msec 0 msec 0 msec
2 10.255.255.65 [MPLS: Labels 35/41 Exp 0] 4 msec 4 msec 0 msec
3 10.255.255.2 [MPLS: Labels 35/41 Exp 0] 4 msec 0 msec 4 msec
4 10.255.255.173 [MPLS: Label 41 Exp 0] 4 msec 0 msec 4 msec
*5 10.255.255.174 4 msec 0 msec **

Tulos on erinomainen, liikenteen kulkiessa ”Customer100” asiakasverkkojen välillä. Traceroute tulosteesta nähdään käytettävän kaksikerroksista leimapinoa.

Seuraavan testin tarkoituksena on tarkastella liikenteen kulkua kahden erillisen VPN-yhteyden välillä. Suoritetaan ping-testi CE1-reitittimeltä toiseen VPN-yhteyteen kuuluvalle CE9-reitittimelle, jonka takaa löytyy asiakasverkko 10.255.9.0/24.

CE1#ping 10.255.9.1 source 10.255.1.1

Sending 5, 100-byte ICMP Echos to 10.255.9.1, timeout is 2 seconds:
U..U.
Success rate is 0 percent (0/5)

Ping-testin perusteella voidaan todeta, ettei kahden erillisen VPN-yhteyden välillä ole yhteyttä. Lopullinen varmistus saadaan suorittamalla ping-testi PE1-reitittimeltä asiakasverkon CE1-reitittimelle.

PE1#ping 10.255.1.1

Sending 5, 100-byte ICMP Echos to 10.255.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

PE1#ping vrf Customer100 10.255.1.1

Sending 5, 100-byte ICMP Echos to 10.255.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Tuloksen perusteella voidaan luotettavasti todeta VPN-yhteyden toimivan suunnitellusti. Reititystiedot *Customer100*-asiakkaan verkkoihin näkyvät vain kyseisen VPN-yhteyden VRF-taulussa eikä ulkopuolisilla ole kyseiseen verkkoon yhteyttä.

7 Dokumentointi

Tämän insinöörityön yksi merkittävä osa-alue oli riittävä dokumentointi suunnittelu- ja toteutusvaiheessa. Suunnitteluvaiheessa paperille kirjatut dokumentit koostuvat useista verkkotopologian piirroksista, sanallisista suunnitelmista, osoiteallokointikuvista sekä lyhyistä laitemäärittelyistä.

Laboratorioverkon toteutusvaiheessa dokumentit päivittyivät melkoisesti. Topologiakuvat saivat uusia muotoja ja osoiteavaruuksia muokattiin sekä lisättiin tarpeen mukaan. Toteutusvaiheen loppupuolella laboratorioverkon dokumentit ovat saaneet lopullisen muotonsa ja ne voidaan toimittaa Metropolia Ammattikorkeakoululle verkon kehitystä ja ylläpitoa varten.

Laboratorioverkon dokumentit koostuvat seuraavista osista:

- Verkon topologiakuvat
- Osoiteallokointikuvat
- Verkkolaitteiden määritykset
- Ohjeet asiakasreitittimien liittämisestä runkoverkkoon.
- Lista määritetyistä VPN-yhteyksistä.

8 Yhteenveto

Tämän insinöörityön tarkoituksena on käsitellä MPLS-tekniikkaa ja siinä toteutettavaa VPN-sovellusta. MPLS-tekniikassa tiedon välitys perustuu MPLS-tunnisteisiin eli leimoihin. Leimojen avulla suoritettavan leimakytkennän ansiosta MPLS-tekniikka tarjoaa joustavan ja nopean pakettien kuljetustavan runkoverkon läpi. MPLS on yhteensopiva kaikkien reititysprotokollien kanssa, joten sen lisääminen jo olemassa olevaan runkoverkkoon ei ole mahdottomuus.

MPLS mahdollistaa uusien palveluiden käyttämisen runkoverkoissa, esimerkkeinä mainittakoon VPN-yhteydet sekä Traffic Engineering -liikenteenohjaus. Koska MPLS-tekniikka sallii eksplisiittisen reitityksen käytön, pystytään liikenne jakamaan eri puolille verkkoa jo runkoverkon reunalla vähentäen samalla solmupisteiden kuormitusta.

Suurin muutos aikaisempiin VPN-toteutuksiin on pakettikytkentäisen VPN-yhteyden lisääminen suoraan palveluntarjoajan runkoverkkoon. Tämä mahdollistaa sen, että ei tarvitse muodostaa erillisiä VPN-tunneleita eikä myöskään käyttää erillistä liikenteensuojausprotokollaa. Vaikka VPN-yhteydet lisätään suoraan runkoverkkoon, on turvallisuus huomioitu toteutuksessa. Turvallisuus perustuu reittierottimiin, joiden avulla paketit kulkevat vain samaan VPN-yhteyteen määritettyjen toimipisteiden välillä, eivätkä ulkopuoliset pysty niitä näkemään.

MPLS-tekniikan käyttö runkoverkoissa tulee lisääntymään tulevaisuudessa, koska verkossa siirrettävät sovellukset kehittyvät koko ajan ja vaativat entistä enemmän myös verkon resursseilta. Omalta osaltaan syyn MPLS:n lisääntymiseen tulevat esittämään myös datan välittämisen nopeus sekä liikenteen priorisoinnin tarjoamat mahdollisuudet. Ei myöskään sovi unohtaa koko ajan lisääntyvää VPN-yhteyksien määrää.

Tälle insinöörityölle asetetut tavoitteet täyttyivät erinomaisesti, tutuksi tulivat niin MPLS-tekniikka kuin MPLS VPN-sovellus. Tämä insinöörityö antaa vahvan perustan

MPLS-tekniikan tuntemukselleni ja uskon vakaasti pystyväni hyödyntämään saatua taitotietoa tulevissa työtehtävissä.

Toteutettavan laboratorioverkon lopputulos on vähintäänkin kohtuullinen, MPLS pakettikytkentä sekä siihen liitetyt MPLS VPN-yhteydet toimivat suunnitellusti. Verkon laajennus ja kehitysmahdollisuudet tarjoavat tilaisuuden uusille projekteille, esimerkiksi Bulevardin toimipisteen liittäminen MPLS-runkoverkkoon sekä Traffic Engineering -sovelluksen käyttöönotto ja testaus. Varteen otettavana projektina voisi pitää myös pienimuotoisen palvelinympäristön liittämistä leimakytkentäiseen runkoverkkoon. Ei myöskään sovi unohtaa opiskelijoiden saamaa hyötyä, kun he opiskelevat MPLS-tekniikkaa sekä MPLS VPN-sovelluksia laboratorioverkkoa käyttäen.

Lähteet

1 Anttila, Aki. TCP/IP tekniikka. Juva, WSOY, 2000.

2 Black, Uyless D. MPLS and label switching networks. New Jersey, Prentice Hall, 2001.

3 Siirtoverkko 2008. (WWW-dokumentti.) Puolustusvoimien Tietotekniikkalaitos. http://tietokannat.mil.fi/kumppanuusohjelma/data/files/132.pdf. Luettu 21.8.2009.

4 MPLS Label Stack Encoding RFC3032. (WWW-dokumentti.) Internet Engineering Task Force. 2001. http://www.ietf.org/rfc/rfc3032.txt. Luettu 24.8.2009.

5 Alwayn, Vivek. Advanced MPLS design and Implementation. Indianapolis, Cisco Press, 2002.

6 MPLS Overview. (WWW-dokumentti.) Juniper Networks, Inc. http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-interfaces-and-routing/mpls-ov.html. Luettu 25.8.2009.

7 Understanding MPLS explicit and Implicit Null Labels (WWW-dokumentti.) Jeff Doyle and Associates, Inc. http://www.doyleassociates.net/Blog/Labels/Figure2.gif. Luettu 21.8.2009.

8 LDP Specification RFC3036. (WWW-dokumentti.) Internet Engineering Task Force. http://tools.ietf.org/html/rfc3036 2001. Luettu 21.8.2009.

9 Lobo, Lancy. MPLS Configuration on Cisco IOS Software. Indianapolis, Cisco Press, 2006.

10 Osborne, Eric. Traffic Engineering with MPLS. Indianapolis, Cisco Press, 2003.

11 RSVP-TE: Extensions to RSVP for LSP Tunnels RFC3209. (WWW-dokumentti.) Internet Engineering Task Force. 2001. http://www.ietf.org/rfc/rfc3209.txt. Luettu 21.8.2008.

12 Multiprotocol extensions for BGP-4 RFC2858. (WWW-dokumentti.) Internet Engineering Task Force. 2000. http://www.ietf.org/rfc/rfc2858.txt. Luettu 15.9.2009.

13 VPN. (WWW-dokumentti.) Viestintävirasto. 2007. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html. Luettu 14.8.2009.

14 Introduction to Cisco MPLS VPN Technology. (WWW-dokumentti.) Cisco Systems. http://www.cisco.com/en/US/i/000001-100000/25001-30000/28501-29000/28555.jpg. Luettu 14.8.2009.

15 Cisco 7600 Series Ethernet over MPLS. (WWW-dokumentti.) Cisco Systems. http://www.cisco.com/en/US/products/hw/routers/ps368/prod_technical_reference09186a00800ae418.html. Luettu 14.8.2009.

16 Virtual Private LAN Service (VPLS). (WWW-dokumentti.) Juniper Networks, Inc. 2007. http://www.juniper.net/solutions/literature/white_papers/200045.pdf. Luettu 26.8.2009.

17 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling RFC4762. (WWW-dokumentti.) Internet Engineering Task Force. 2007. http://tools.ietf.org/html/rfc4762. Luettu 25.9.2009.

18 Layer 2 Virtual Private Networks (l2vpn). (WWW-dokumentti.) Internet Engineering Task Force. 2009. http://www.ietf.org/dyn/wg/charter/l2vpn-charter.html. Luettu 7.10.2009.

19 Cisco VTP: VLAN Trunking Protocol. (WWW-dokumentti.) Javvin Technologies, Inc. http://www.javvin.com/protocolVTP.html. Luettu 15.9.2009.

20 Configuring InterVLAN Routing. (WWW-dokumentti.) Cisco Systems. http://www.cisco.com/en/US/docs/switches/lan/catalyst5000/hybrid/routing.html. Luettu 14.9.2009.

21 InterVLAN Routing. (WWW-dokumentti.) Hewlett-Packard. 2005. ftp://ftp.hp.com/pub/networking/software/ProCurve-SR-InterVLAN-Config-Guide.pdf. Luettu 15.9.2009.

22 Salvagno, Michael. Cisco Network Design Handbook. Foster City, M&T Books, 2000.

23 OSPF. (WWW-dokumentti.). Tietotekniikan ja Mediatekniikan laitos. 1997. http://www.tml.tkk.fi/Studies/Tik-110.300/1997/Essays/ospf.html. Luettu 10.9.2009.

24 Guidelines for creation, selection, and registration of an Autonomous System (AS) RFC1930. (WWW-dokumentti.) Internet Engineering Task Force. 1996. http://www.ietf.org/rfc/rfc1930.txt. Luettu 14.9.2009.