Miika Kesti

Internet-palveluntarjoajan verkon suunnittelu ja toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

26.11.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Miika Kesti Internet-palveluntarjoajan verkon suunnittelu ja toteutus 37 sivua 26.11.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaajat	Yliopettaja Janne Salonen Teknologiajohtaja Thomas Willberg

Työn tarkoituksena oli ottaa käyttöön Internet-palveluntarjoaja S1 Networksin verkkoympäristöön uudet runkoreitittimet. Samalla kehitettiin verkon arkkitehtuuria tulevaisuuden tarpeisiin helposti mukautuvaksi. Tavoitteena oli luoda toimiva vikasietoinen verkko, lisätä verkon kapasiteettia ja rakentaa verkko helposti muokattavaksi tulevia vastaavia päivitysprojekteja ajatellen.

Verkko suunniteltiin yrityksessä tiiminä. Verkon toteutuksessa päätettiin käyttää verkon rakenteen ja käyttötarkoituksien johdosta OSPF-, BGP- ja EAPS-protokollia. Tavoitteena oli saada aikaan verkko, missä minkä tahansa yksittäisen yhteyden, laitteen tai keskuksen vikaantuminen aiheuttaisi korkeintaan alueellisen katkoksen.

Suunnittelun jälkeen päävastuu verkon toteuttamisesta annettiin minulle. Verkko rakennettiin siten, että verkkolaitteita on seitsemällä eri verkkoalueella ja ne muodostavat rengastopologian. Verkossa on kaksi reunareititintä eri alueilla, jotka hoitavat BGP-reitityksen. Näiden reitittimien välissä olevilla kytkimillä on muodostettu Metro ethernet -runkoverkko.

Verkon päivitysprojekti onnistui odotetulla tavalla. Verkko suunniteltiin huolellisesti, joten varsinaista päivitys- ja konfiguraatiotyötä oli helppo lähteä toteuttamaan. Verkko todettiin testauksessa toimivaksi. Kaiken kaikkiaan verkon päivitysprojekti oli onnistunut, sillä asetetut tavoitteet saavutettiin.

Avainsanat	ISP, RIPE, Reititys, Kytkinverkot, BGP, EAPS

Author Title Number of Pages Date	Miika Kesti Designing and Implementing the Network of Internet Service Provider 37 pages 26 November 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Networks
Instructors	Janne Salonen, Principal Lecturer Thomas Willberg, CTO

The aim of the study was to implement a deployment of backbone routers for the network environment of the Internet Service Provider S1 Networks. The technical goal was to improve the architecture of the network and build it to be flexible considering future needs. The network needed to be redundant, to have more capacity and to be easily adaptable to possible future updates.

The network was planned in the company as teamwork. The team decided to use OSPF, BGP ja EAPS protocols due to the network's architecture and use. The network was planned in such a way that a failure of any single connection, device or POP (point of presence) would only cause a local interruption.

After the planning, the implementation of the project began. The network was built on seven different network sites and the devices form a ring topology. On different sites, there are two backbone routers which take care of the BGP routing. The switches connecting these routers and the routers themselves form the Metro Ethernet backbone network.

The deploying of the backbone routers succeeded as expected. The network was planned carefully in advance which made the actual updating and configuring quite easy. Thereafter the network was tested and it worked as wanted. After all, the project was a success since all the aims were accomplished.

Keywords	ISP, RIPE, Routing, Switching, BGP, EAPS

Sisällys

Lyhenteet

AS	Autonomous System. Internetin itsenäisen toimijan verkkokokonaisuus.
BGP	Border Gateway Protocol. Internetissä käytetty reititysprotokolla, joka vastaa reitityksestä eri AS:ien välillä.
EAPS	Ethernet Automatic Protection Switching. Extreme Networksin rengasprotokollassa käytetty protokolla.
EIGRP	Enhanced Interior Gateway Routing Protocol. Ciscon reititysprotokolla, jota käytetään organisaation sisäisessä reitityksessä.
HMV	Huomattava markkinavoima. Sellaisen vaikutusvallan omaava yritys, joka voi toimia sen turvin huomattavassa määrin riippumattomasti kilpailijoista.
IGRP	Interior Gateway Routing Protocol. Ciscon etäisyysvektoriprotokolla, jota käytetään organisaation sisäisessä reitityksessä.
IP	Internet Protocol. Internet-protokolla, joka mahdollistaa laitteille oman osoitteen Internetissä IP-pohjaiseen kommunikointiin.
IPv4	Internet Protocol version 4. Internet-protokollan versio 4, jossa käytetään 32-bittisiä osoitteita.
IPv6	Internet Protocol version 6. Internet-protokollan versio 6, jossa käytetään 128-bittisiä osoitteita.
IS-IS	Intermediate System-to-Intermediate System. Reititysprotokolla, jota käytetään erityisesti operaattorin sisäisessä reitityksessä.
ISP	Internet Service Provider. Internet-palveluntarjoaja.
LAN	Local Area Network. Lähiverkko.
LIR	Local Internet Registry. Paikallinen Internet-osoitteiden hallintataho.

MAC	Media Access Control. Verkkoportin fyysinen osoite.
OSI	Open Systems Interconnect. Kerrosmalli verkkorakenteelle.
OSPF	Open Shortest Path First. Linkkitilaprotokolla, jota käytetään organisaation sisäisessä reitityksessä.
PA	Provider Aggregatable. Palveluntarjoajan omistama osoiteavaruus.
PI	Provider Independent. Toimijariippumaton osoiteavaruus.
POP	Point of presence. Verkon yhdyspiste johon alueen kaapeloinnit päättyvät.
RIP	Routing Information Protocol. Etäisyysvektoriprotokolla, jota käytetään organisaation sisäisessä reitityksessä.
RIPE	Réseaux IP Européens. Organisaatio, joka vastaa IP-osoitteiden hallinnasta Euroopassa.
SFP	Small Form-Factor Pluggable. Kuituliitännöissä käytetty moduuli.
SFP+	Enhanced Small Form-Factor Pluggable. Kuituliitännöissä käytetty moduuli, joka tukee 10 Gbps:n tiedonsiirtonopeutta ja on yhteensopiva SFP-moduulien kanssa.
STP	Spanning Tree Protocol. Kytkinverkoissa käytetty protokolla.
TCP	Transmission Control Protocol, Tietoliikenneprotokolla, jolla luodaan yhteyksiä verkkolaitteiden välille.
XFP	10 Gigabit Small Form-Factor Pluggable. Kuituliitännöissä käytetty moduuli, joka tukee 10 Gbps:n tiedonsiirtonopeutta.

1 Johdanto

Työn tarkoituksena on ottaa käyttöön Internet-palveluntarjoajan verkkoympäristöön uudet runkoreitittimet. Samalla on tarkoitus kehittää verkon arkkitehtuuria tulevaisuuden tarpeisiin helposti mukautuvaksi. Työn toimeksiantaja on Internet-palveluntarjoaja S1 Networks, jonka päätuotteena ovat valokuidulla toteutetut Internet-liittymät.

Verkkokokonaisuutta suunnitellessa tärkeimpiä ominaisuuksia ovat suorituskyky ja vikasietoisuus. Verkosta halutaan tietenkin myös mahdollisimman kustannustehokas siten, että verkon suorituskyky on suunniteltu yrityksen tarpeiden mukaisesti. Verkkoa suunnitellessa täytyy ottaa huomioon jatkuvasti lisääntyvä kapasiteetin tarve ja tulevaisuudessa verkkoon tehtävät laajennukset – siten verkkoon pystytään liittämään myöhemmin helposti uusia alueita, ja verkon kapasiteettia pystytään nostamaan ilman suuria laitekustannuksia.

Verkon päivitysprojekti tehdään yrityksessä tiiminä, jossa käydään läpi eri toteutusvaihtoehdot ja päätetään toteutustavat. Itse konfiguraatiotyön tekemiseen saan päävastuun. Oletan projektin etenevän sujuvasti ja ongelmatilanteiden ratkeavan nopeasti, sillä projektiin on varattu hyvin resursseja työnantajan puolesta.

Tässä työssä esittelen sekä keskeistä Internet-palveluntarjoajiin ja tietoverkkoihin liittyvää teoriaa että itse päivitysprojektin toteutusta. Työn alkupuolella käyn läpi yleisesti Internet-palveluntarjoajan toimintatapoja ja -periaatteita. Kerron myös historiaa siitä, miten nykymuotoinen Internet on syntynyt, ja miten verkossa käytetyt laitteistot ja toimintaperiaatteet ovat muuttuneet ajan myötä. Teoriaosuudessa esittelen myös erilaisten protokollien toimintaa.

Työn pääpaino on kuitenkin verkon päivitysprojekti, ja etenkin siinä käytetyt laitteistot ja protokollat. Laitteiden hankintaa en käy työssä läpi, sillä kaikki käytetty laitteisto on jo valmiiksi yrityksen käytössä tai hankittu ennakkoon projektia varten. Projektia käsittelevissä luvuissa esittelen työn lähtökohtia ja tavoitteita, päivitysprojektissa käytettyjä laitteistoa ja protokollia sekä projektin toteutusta. Työn lopussa kerron työn testauksesta ja arvioin projektin onnistuneisuutta.

2 Internet-palveluntarjoaja

ISP eli Internet-palveluntarjoaja on yritys, joka tarjoaa asiakkailleen Internet-palveluita. Internet-palveluiden kategoria on suuri – siihen kuuluvat Internet-yhteyksien lisäksi esimerkiksi virtuaalipalvelin-, webhotelli-, verkkotunnus-, sähköposti- ja viestintäpalveluita. Jos yritys tarjoaa yhtä tai useampaa näistä palveluista, voi yritys nimittää itseään ISP:ksi. Internet-palveluntarjoajasta puhuttaessa tarkoitetaan kuitenkin yleensä yritystä, jonka päätuotteena ovat Internet-liittymät.

2.1 Internet-palveluntarjoajat Suomessa

Ensimmäiset Internet-palveluntarjoajat ovat pääosin vanhoja puhelinyhtiöitä, jotka alkoivat tarjota Internet-palveluita jo olemassa olevia puhelinkaapeleita pitkin. Suomessa on ollut parhaillaan satoja puhelinyhtiötä. Yksityisten puhelinyhtiöiden yhteistyö sai alkunsa, kun puhelinyhtiöt perustivat Puhelinlaitosten liiton vuonna 1921, joka nimettiin vuonna 1996 Finnet-liitoksi. Yhtiöiden määrä pieneni nopeasti 1900-luvun alkupuolella, kun yhtiöitä yhdistyi ja valtio otti huonosti kannattavia yhtiöitä hoitoonsa. [1.]

Suomessa oli aluksi kaksi merkittävää teleoperaattoriryhmää: yksityiset puhelinyhtiöt ja Suomen lennätinlaitos. Tähän tuli muutos, kun 1980-luvulla alalle sallittiin kilpailu – tällöin Helsingin Puhelinyhdistyksen ja Puhelinlaitosten liiton jäsenet perustivat valtakunnallisen dataverkkopalveluita tarjoavan yrityksen Datatie Oy. 1990-luvulla kännyköiden tullessa käyttöön puhelinyhtiöt perustivat Radiolinjan. Nämä kaksi valtakunnallista verkkoyritystä kilpailivat valtion Telecom Finlandiksi muuttunutta lennätinlaitosta vastaan. [2.]

Valtio yksityisti Telecom Finlandin ja sen nimeksi tuli Sonera. Myöhemmin Sonera yhdistyi Teliaan ja nimi vaihtui muotoon TeliaSonera Finland. Vuonna 2017 Telia otti käyttöön Telia-brändin myös Suomessa ja yhtiön nimeksi muutettiin Telia Finland Oyj. [2.]

Helsingin puhelinyhtiö vaihtoi nimensä Helsingin puhelimeksi, joka vuonna 2000 vaihtui edelleen Elisaksi. Helsingin puhelin osti muut osapuolet ulos Datatie Oy:sta ja Radiolinjasta 1990-luvun lopussa. Vuosituhannen vaihteessa Elisan muita yhtiöostoja olivat mm. Tampereen, Joensuun ja Keski-Suomen puhelimet. Samaan aikaan Sonera taas valtasi Turun puhelimen [2]. Elisan viimeaikaisimpia yhtiöostoja ovat vuonna 2013 ostettu PPO

Yhtiöt (ent. Pohjanmaan puhelin) ja vuonna 2016 ostettu Anvia (ent. Vaasan läänin puhelin) [3].

Soneran ja Elisan lisäksi kolmen suurimman Internet-palveluntarjoajan ryhmään kuuluu DNA. DNA:n historia alkaa vuosituhannen vaihteesta. Kun Elisa osti Radiolinjan, Finnet-liitto perusti kilpailevan matkapuhelinoperaattori DNA Finlandin. Vuonna 2007 Finnet-liitto kuitenkin hajosi, kun siitä erosivat Kuopion, Lohjan, Oulun, Lännen, Satakunnan ja Päijät-Hämeen Puhelimet. Nämä yhtiöt omistivat DNA Finlandista yli puolet, joten ne yhdistivät liiketoimintansa uudeksi valtakunnalliseksi operaattoriksi DNA Oy:ksi. DNA Oy laajensi yritysmarkkinoita huomattavasti ostamalla 2014 vuonna tanskalaisen yritysoperaattorin TDC:n Suomen liiketoiminnot. [2; 4.]

2.2 Internet-palveluntarjoajien toimintaperiaatteet

Internet-palveluntarjoaja (ISP) tarjoaa rajapinnan julkiseen Internetiin. Palveluntarjoajalla on useita toteutusvaihtoehtoja rajapinnan toteuttamiseen: asiakkaalle voi tarjota esimerkiksi yhden tai useamman julkisen IP-osoitteen siten, että verkon oletusyhdyskäytävä jää palveluntarjoajan reitittimelle. Erityisesti isot yritykset kuitenkin yleensä haluavat IP-verkon reititettynä kokonaan heidän reitittimilleen. Reitityksen toteuttamiseen on olemassa monia vaihtoehtoisia tapoja ja protokollia – valintoihin vaikuttavat muun muassa yhteyden fyysinen toteutus ja asiakkaan toiveet.

IP-osoitteita on olemassa kahta erilaista haltijatyyppiä: PI-osoitteita (Provider Independent) ja PA-osoitteita (Provider Aggregatable). PI-osoitteet ovat vanhojen yrityksien itse omistamia IP-osoitteita, jotka he ovat saaneet siihen aikaan, kun IP-osoitteiden omistuksia jaettiin suoraan yrityksille. PI-osoitteita kutsutaan toimijariippumattomiksi IP-osoitteiksi, sillä ne eivät ole riippuvaisia palveluntarjoajasta – ne voivat ottaa Internet-yhteyden miltä tahansa palveluntarjoajalta, joka suostuu reitittämään PI-osoitteita [5]. PI-osoitteita käyttävillä yrityksillä on yleensä usean palveluntarjoajan Internetyhteys. Tällöin osoitteet reititetään BGP-protokollalla yritykselle, ja yritys pystyy itse hallitsemaan, minkä palveluntarjoajan Internet-yhteyden kautta liikennettä reititetään.

PA-osoitteet ovat puolestaan operaattoreiden omistamia, joita he jakavat asiakkaidensa käyttöön. Tällöin IP-osoite on asiakkaan käytössä, mutta se palautuu operaattorille, jos asiakkuus päättyy. Operaattorit ovat aiemmin voineet hakea PA-osoitteita IP-osoitteita

hallinnoivalta organisaatiolta (lisää luvussa 7.1), mutta nykyään PA-osoitteita jaetaan vain uusille operaattoreille. Olemassa olevista PA-osoitteista voidaan käydä kauppaa operaattoreiden välillä.

Internet-rajapinnan lisäksi Internet-palveluntarjoajien palveluihin kuuluu muitakin palveluita – näistä tärkeimpiä ovat erilaiset yhdistämispalvelut. Niiden avulla yritys saa eri toimipisteiden verkot tai palvelinsalin palvelimet liitettyä yhdeksi sisäverkkokokonaisuudeksi. Lähes jokaisen Internet-palveluntarjoajan tuoteskaalaan kuuluvat myös nimipalvelinpalvelut, ja kasvavassa roolissa ovat myös Webhosting- ja pilvipalvelut. Jotkin yritykset ovat erikoistuneet pelkästään Webhosting- ja pilvipalveluihin.

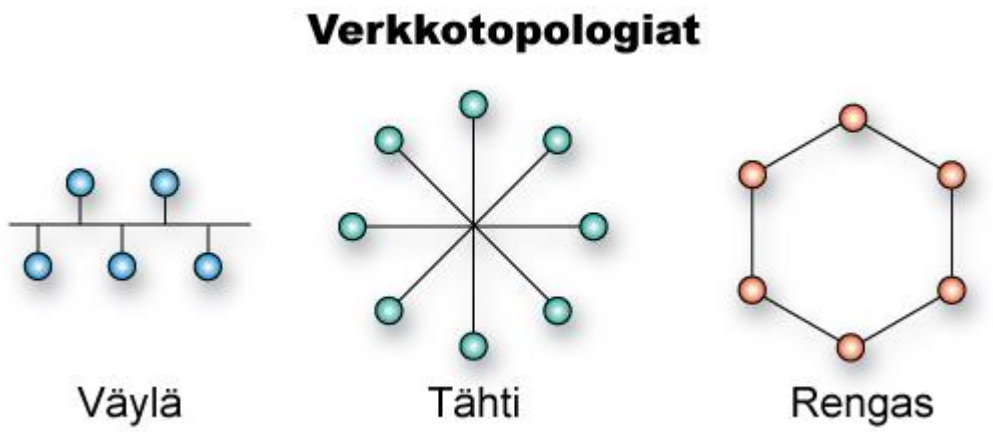
3 Tietoverkot

Internet on suuri pakettikytkentäinen tietoverkko. Se koostuu lukuisista pienistä tietoverkoista, joita kutsutaan Autonomisiksi järjestelmiksi (AS, Autonomic System). Järjestelmän nimitys AS tulee siitä, että jokaista autonomista järjestelmää hallitsee oma organisaatio. Tällaista autonomista järjestelmää ylläpitävä organisaatio voi olla operaattori, yritys, koulu tai jopa yksityishenkilö, jolla on oma AS-numero.

Pakettikytkentäinen verkko perustuu datan pilkkomiseen ennen lähettämistä – datan lähettäjä pilkkoo datan ennalta määrätyn kokoisiin paketteihin ja lähettää ne paketin osoitetietojen avulla vastaanottajalle. Vastaanottaja kokoaa paketeista lähetetyn datatiedoston. Pakettikytkentä soveltuu hyvin tietoverkoissa käytettäväksi, koska tiedonsiirto lähettäjän ja vastaanottajan välillä ei vie verkon siirtokapasiteettia. [6.]

3.1 Tietoverkon laitteisto

Tietoverkot koostuvat verkkolaitteista, niiden välisistä kaapeloinneista ja muista siirtoyhteyksistä. Tietoverkot sisältävät ison määrän erilaisia verkkolaitteita, kuten kytkimet, reitittimet, modeemit ja erilaiset päätelaitteet. Tietoverkkoja rakennettaessa on tärkeää suunnitella verkkotopologia eli verkon rakenne, jossa määritellään, mitkä verkkolaitteet ovat yhteydessä toisiinsa. Yksinkertaisimpia rakenteita ovat kuvassa 1 esitetyt väylä-, tähti- ja rengastopologiat. Tyypillisesti tietoverkoissa käytetyt topologiat ovat tähti- ja rengastopologian yhdistelmiä.



Kuva 1. Tyypilliset verkkotopologiat ovat väylä, tähti ja rengas. [7.]

Tietoverkon tärkein laite on reititin, joka huolehtii datan siirrosta eri tietoverkkojen välillä. Reitittimen tehtävä on pitää kirjaa reiteistä ulkoverkkoon ja organisaation sisäiseen verkkoon. Tätä kutsutaan reititystauluksi. Reititystaulun avulla reititin osaa reitittää liikenteen oikeaan paikkaan. Usein pienen organisaation reitittimillä on sisäverkon reittien lisäksi vain oletusreitti ulkoverkkoon, jolloin kaikki liikenne ohjataan yhdelle palveluntarjoajalle. Palveluntarjoajan reitittimillä on taas tiedossa koko Internetin reititystaulu, ja ne osaavat reitittää asiakkaan liikenteen haluttuun kohteeseen.

Kytkimet yhdistävät monia verkkolaitteita toisiinsa. Verkkokytkinten käyttö kasvoi 2000-luvun alussa, sillä silloin kytkimien hintaero aiemmin paljon käytettyihin keskittimiin ei ollut enää merkittävä [8]. Keskitin (Hub) eli moniporttitoistin vastaanottaa datan ja lähettää sen edelleen jokaiseen laitteen muuhun porttiin. Tästä johtuen keskitin ei ole kovin tietoturvallinen verkkolaite, ja se myös ruuhkautuu helposti. Kytkin on keskitintä älykkäämpi laite, sillä se opettelee porttien takana olevien laitteiden fyysiset osoitteet (MAC-osoitteet) ja osaa siten kytkeä saapuvan liikenteen oikeaan porttiin. Kytkimet ovat myös syrjäyttäneet pienimpiä reitittimiä, sillä markkinoille on tullut tehokkaita 3. tason kytkimiä, jotka osaavat myös reitittää IP-osoitteita. Normaalit kytkimet ovat 2. tason laitteita. Tasot perustuvat OSI-mallin kerroksiin. OSI-malli esitellään myöhemmin tässä luvussa. [9.]

3.2 Internetin kehitys

Internetin historia ulottuu vuoteen 1969, jolloin Yhdysvalloissa ARPANET aloitti toimintansa. ARPANET (Advanced Research Projects Agency Network) perustettiin sotilaallista tutkimusta varten ja ensimmäinen viesti ARPANETissä lähetettiin 29.10.1969. Nykypäivän reitittimiä vastaavat armeijan solmutietokoneet erotettiin vuonna 1984 ARPANETistä omaan verkkoon, josta syntyi MILNET (Military Network). ARPANETin suosio kasvoi runsaasti 1980-luvulla teknologian halpenemisen myötä. Armeijan verkon erottaminen ARPANETistä helpotti myös Yhdysvaltojen ulkopuolisten tietokoneiden liittymistä verkkoon. ARPANET saapui suomeen vuonna 1984, kun Suomeen perustettiin Funet (Finnish University and Research Network), joka rakensi tietoliikenneyhteyksiä suomalaisten yliopistojen käyttöön. [10.]

Varsinaisen Internetin aikakausi alkoi 1980- ja 1990-lukujen vaihteessa, kun ARPANET muuttui Internetiksi. Internetin kasvu 1990-luvulla oli räjähdysmäistä. Vuonna 1969 pystytetyn neljän tietokoneen verkko oli pian laajentunut satojen miljoonien tietokoneiden verkoksi. Vuosi 1994 oli merkittävä Internetin historiassa, sillä silloin markkinoille tulivat ensimmäiset www-selaimet ja Internetiä alettiin tarjoamaan myös kotitalouksille. [10.]

Lähiverkkoratkaisuisista vanhin ja yleisin on Ethernet. Ensimmäinen Ethernet-verkko kehitettiin Xeroxin Palo Alton tutkimuskeskuksessa vuonna 1973. Se nimettiin Alto ALOHAnetiksi. Ethernetissä käytettiin aluksi väylätopologiaa, jossa kaikki tietokoneet olivat kiinni samassa kaapelissa. Pian kuitenkin kehitettiin toistin (HUB), jolla pystyttiin toistamaan yhden väylän liikenne toiseen väylään. Ethernetin topologia muuttui 1990-luvulla tähtimäiseksi, jossa jokaisella verkkolaitteella oli oma verkkokaapeli keskittimelle. [11.]

3.3 Viitemallit

1980-luvulla tietoverkkojen kehitys oli nopeaa. Haasteita aiheutti kuitenkin eri toimijoiden verkkojen liittäminen yhteen, sillä kilpailu oli kovaa laitevalmistajien välillä, eivätkä eri valmistajien laitteet olleet yhteensopivia keskenään. Tämän vuoksi luotiin standardeja, joiden mukaan laitteiden ja ohjelmistojen kuului toimia. Standardien luomiseen on kehitetty erilaisia malleja, joissa kaikki standardit toimivat yhdessä. Yleisimmin käytetyt viitemallit ovat OSI-malli ja TCP/IP-malli.

Kansainvälinen standardisoimisjärjestö ISO (International Standardization Organization) kehitti OSI-mallin 1980-luvun alussa. OSI-malli jakaa tiedonsiirron seitsemään tasoon siten, että alemmat tasot luovat pohjan ylempien tasojen toiminnalle. OSI-mallin kerrokset ovat alhaalta ylöspäin lueteltuna fyysinen kerros, siirtoyhteys-, verkko-, kuljetus-, istunto-, esitystapa- ja sovelluskerros (kuva 2). Neljä alinta kerrosta muodostaa OSI-mallin alemman kokonaisuuden, kolme ylintä ylemmän kokonaisuuden. [12.]

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Kuva 2. OSI-mallin seitsemän tasoa tarkoituksineen ja esimerkkisovelluksineen. [13.]

Fyysiseen kerrokseen kuuluvat tiedonsiirrossa käytetyt mekaaniset, loogiset ja sähköiset asiat. Fyysisen tason tiedonsiirto voidaan jakaa kahteen ryhmään: sarjamuotoiseen ja rinnakkaismuotoiseen. Sarjamuotoisessa tiedonsiirrossa bitit lähetetään peräkkäin yksi kerrallaan. Tällöin etuna on se, että dataa voidaan siirtää yhtä johdinta pitkin. Rinnakkaismuotoisessa tiedonsiirrossa bitit lähetetään samaan aikaan kukin omaa johdinta pitkin. Rinnakkaismuotoinen tiedonsiirto on yleensä sarjamuotoista nopeampaa, mutta sitä voidaan käyttää vain lyhyillä etäisyyksillä, koska bitit voivat saapua eri johtimista eri aikaan vastaanottajalle. Näistä syistä johtuen rinnakkaista tiedonsiirtoa käytetään lähinnä laitteiden sisäisessä tiedonsiirrossa, ja sarjamuotoista tiedonsiirtoa eri laitteiden välillä. Sarjamuotoista tiedonsiirtoa käytetään kupari- ja valokaapelien lisäksi myös radioteillä. [14.]

OSI-mallin toinen kerros on siirtoyhteyskerros, jossa hoidetaan virheiden korjaus sekä yhteyksien luominen ja purkaminen. Siirtoyhteyskerros pitää lisäksi huolta lähetysnopeudesta, jotta tietoa ei lähetetä nopeammin kuin vastaanottaja pystyy sitä käsittelemään. Siirtoyhteyskerroksen yleisin verkkolaite on kytkin. Verkkokerros on OSI-mallin kolmas kerros. Se välittää ylempien kerroksien tietoliikennepaketteja. Verkkokerros on verkon rakenteesta riippumaton, ja se piilottaa alleen alempien kerroksien fyysisen verkkorakenteen. Verkkokerroksen tehtävä on valita käytettävä reitti tiedonlähetystä varten. Tälle tasolle kuuluvat monet reititysprotokollat, kuten OSPF ja EIGRP. Neljäs ja korkein alempien kerroksien taso on kuljetuskerros, jonka tehtävä on huolehtia laadukkaasta tiedonsiirrosta – se vastaa muun muassa tietoliikennepakettien perillepääsystä ja oikeasta järjestyksestä. [13.]

OSI-mallin kolme ylintä kerrosta ovat sovellusprotokollakerroksia. Alin näistä kerroksista eli viides OSI-mallin taso on istuntokerros. Tälle kerrokselle kuuluvat erilaiset yhteyden avaamiseen, sulkemiseen ja salaamiseen käytetyt protokollat. Esitystapakerros on mallin kuudes kerros, ja se huolehtii numeroiden, tekstin, kuvien, äänen muodosta tiedonsiirrossa. Ylin OSI-mallin seitsemästä tasosta on sovelluskerros. Sovelluskerroksella toimivat erilaiset verkkosovellukset, joita ovat esimerkiksi Telnet- ja SMTP-sovelluskerros siis tarjoaa erilaisia käyttöliittymiä tietoliikenneverkon käyttöön. [13.]

OSI-mallin protokollapino ei kuitenkaan yleistynyt kuten jäljempänä esiteltävä TCP/IP-viitemallin protokollapino. OSI-mallia käytetään kuitenkin laajasti kerroksittaisten protokollien viitekehyksenä, ja myös TCP/IP-protokollapino voidaan esittää OSI-mallin kautta. OSI-mallin merkitys korostuu opetus- ja esityskäytössä, sillä sen kautta esitellään usein pakettipohjaisen tietoliikenneverkon toimintaa. TCP/IP-viitemalli kehitettiin vasta TCP/IP-protokollien kehittämisen jälkeen. Niinpä se soveltuukin paremmin TCP/IP-protokollien mallintamiseen. Nimensä TCP/IP-viitemalli on saanut kahdelta ensimmäiseltä ja tärkeimmältä standardin protokollalta, jotka ovat TCP- ja IP-protokollat. [15.]

Taulukko 1. OSI- ja TCP/IP-mallit voidaan rinnastaa taulukon mukaisesti. [15.]

<table>
<tr><th>OSI-malli</th><th>TCP/IP-malli</th></tr>
<tr><td>Sovelluskerros (Application Layer)</td><td rowspan="3">Sovelluskerros (Application Layer)</td></tr>
<tr><td>Esityskerros (Presentation Layer)</td></tr>
<tr><td>Istuntokerros (Session Layer)</td></tr>
<tr><td>Kuljetuskerros (Transport Layer)</td><td>Kuljetuskerros (Transport Layer)</td></tr>
<tr><td>Verkkokerros (Network Layer)</td><td>Verkkokerros (Internet Layer)</td></tr>
<tr><td>Siirtokerros (Data Link Layer)</td><td rowspan="2">Peruskerros (Network Access Layer)</td></tr>
<tr><td>Fyysinen kerros (Physical Layer)</td></tr>
</table>

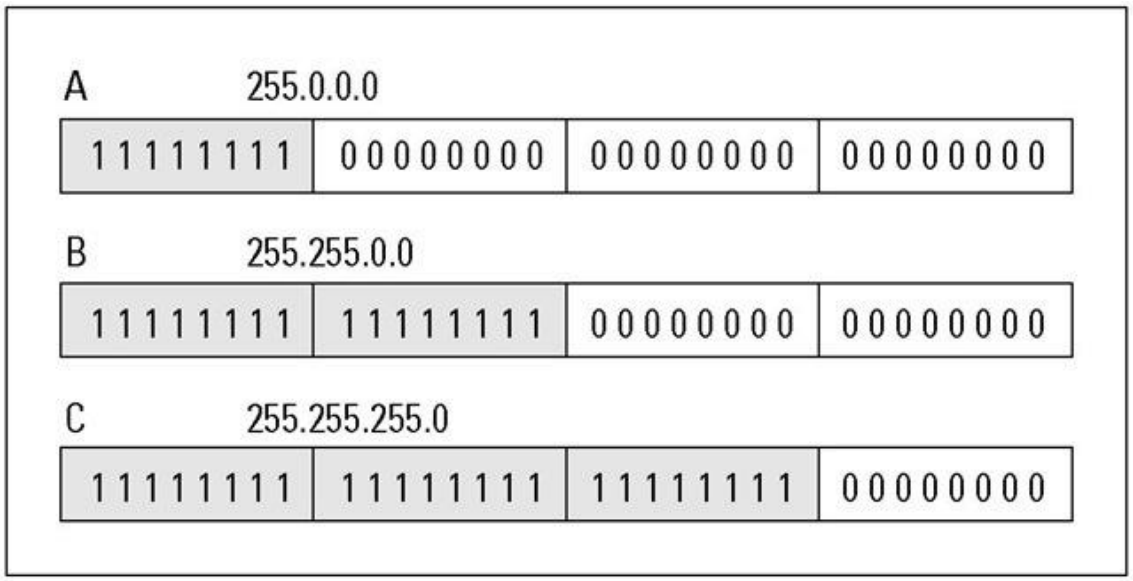
TCP/IP-malli koostuu neljästä kerroksesta, jotka ovat peruskerros, verkkokerros, kuljetuskerros ja sovelluskerros. TCP/IP-malli voidaan rinnastaa OSI-malliin seuraavasti: TCP/IP-mallin peruskerros pitää sisällään OSI-mallin fyysisen ja siirtoyhteyskerroksen, molemmissa malleissa on omat verkko- ja kuljetuskerroksensa, ja TCP/IP-mallin sovelluskerros sisältää OSI-mallin istunto-, esitystapa- ja sovelluskerroksen. TCP/IP-mallin protokolliin kuuluu paljon erilaisia protokollia, joista keskeisin on IP (Internet-protokolla). IP kuuluu verkkokerrokseen, ja se eristää peruskerroksen ylemmistä kerroksista. Minkä tahansa peruskerroksen protokollan päällä voidaan lähettää IP-paketteja. IP eristää myös ylemmän tason protokollat peruskerroksesta, sillä kaikki ylemmän tason palvelut, sovellukset ja protokollat käyttävät IP:aa. IP:n keskeisyydestä johtuen TCP/IP-mallista käytetään myös nimitystä tiimalasimalli. Se on ollut hyvin menestynyt malli laajaverkkojen suunnittelussa ja tärkeä pohja IPv6:n kehittämisessä. [15.]

3.4 IP-osoitteet

IP-osoite eli internetin protokollaosoite on numerosarja, jolla yksilöidään Internetiin yhdistettyjä verkkolaitteita. IP-osoitteiden avulla verkossa kulkevat paketit löytävät perille oikeaan osoitteeseen. Eniten käytetty IP-osoite on IPv4-osoite, joka on 32-bittinen luku, ja se esitetään neljänä 8-bittisenä merkkijonona. 8-bittisellä merkkijonolla voidaan esittää luvut väliltä 0-255, joten IP-osoitteet ovat väliltä 0.0.0.0 ja 255.255.255.255. Osoitteita on yhteensä täten 256^4 eli 4 294 967 296 kappaletta. Aikoinaan loppumattomaksi ajateltu IP-osoitteiden määrä loppui kesken Internetin räjähdysmäisen kasvun takia ja avuksi kehitettiin Osoitemuunnos (NAT – Network Address Translation). Osoitemuunnoksen avulla voitiin luoda sisäverkkoja, joissa verkon käyttäjille jaettiin yksityisosoitteita

ja heidän kaikkien liikenne reititettiin ainoastaan yhden julkisen osoitteen kautta Internetiin. Yksityiskäyttöön sallitut osoiteavaruudet ovat 10.0.0.0/8, 172.16.0.0/12 ja 192.168.0.0/24.

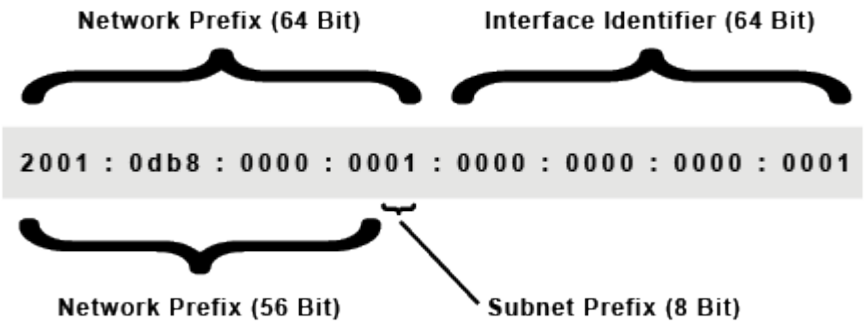
Osoiteavaruuksista puhuttaessa oleellinen asia on verkon peite. Koko IP-verkko voidaan ilmaista osoiteavaruudella 0.0.0.0/0, josta kahtia jaettuna saadaan 0.0.0.0/1 ja 128.0.0.0/1. Kun verkkoa 0.0.0.0/1 halutaan pilkkoa edelleen, se jaetaan neljään, jolloin saadaan verkot 0.0.0.0/2, 32.0.0.0/2, 64.0.0.0/2 ja 96.0.0.0/2. Seuraavaksi yksi /2-verkko voidaan jakaa kahdeksaan /3-verkkoon. Tällä käytännöllä jatkettaessa verkko 0.0.0.0/0 voidaan jakaa esimerkiksi 255 /8-verkkoon, 65 536 /16-verkkoon tai 16 777 216 /24-verkkoon jne. Pilkkomista voidaan jatkaa, kunnes jäljellä on yksi osoite. Tällöin verkkopeite on /32.



Kuva 3. Verkon koosta puhuessa voidaan verkkomaskin mukaan käyttää nimityksiä A-, B- tai C-luokka. [16.]

Verkkopeitteet voidaan imaista usealla eri tavalla. Tavallisin merkintätapa on yllä käytetty 1-bittien määrän merkintä, joka merkataan IP-osoitteen perään /-merkin jälkeen. Toinen paljon käytetty tapa on merkitä bittien määrä IP-osoitteen muodossa. Esimerkiksi /16 voidaan merkitä IP-osoitteen muotoon 255.255.0.0, kun taas peite /17 voidaan merkitä 255.255.128.0. Kuvan 3 mukaan verkon koosta puhuttaessa käytetään myös nimityksiä A-, B- ja C-luokka – A-luokalla tarkoitetaan /8-verkkoa, B-luokalla /16-verkkoa ja C-luokalla /24-verkkoa.

Kun IPv4-osoitteet loppuivat kesken, kehitettiin IPv6-osoitteet. IPv6-osoite on pituudeltaan 128 bittiä, joten osoitteita on yhteensä 2^{128} eli noin $3{,}4 * 10^{38}$. Tämä 39-numeroinen osoitteiden määrä takaa sen, etteivät osoitteet tule loppumaan kesken. IPv6-osoitteet esitetään kahdeksana 16 bitin kokoisena ryhmänä. Nämä 16 bitin ryhmät kirjoitetaan heksadesimaalimuodossa. IPv6-osoitteet ovat siis väliltä 0:0:0:0:0:0:0:0 ja ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. IPv6-osoitteita voidaan lyhentää jättämällä turhat nollat pois. Esimerkiksi osoite 2001:dead:beef:0000:0000:0bad:cafe:0001 voidaan lyhentää muotoon 2001:dead:beef::bad:cafe:1. Yllä mainittu ns. nollaosoite (0:0:0:0:0:0:0:0) voidaan myös kirjoittaa pelkästään kahdella kaksoispisteellä, ::. IPv6-osoitteissa käytetään IPv4-osoitteiden kaltaisesti verkkopeitteitä, joten koko IPv6-osoiteavaruus voidaan merkitä ::/0. Yleinen yritykselle käyttöön annettava verkko on kooltaan /48. Tällöin verkko sisältää 64000 /64-verkkoa, joka on pienin reititettävä verkko – siinäkin osoitteita on vielä 2^{64}. eli noin $1{,}8 * 10^{19}$. [17]



Kuva 4. IPv6-osoite voidaan jakaa kahtia verkko- ja linkkiosaan. [18.]

Kuvassa 4 esiitetty IPv6-osoite havainnollistaa, miten 64 ensimmäistä bittiä ovat osoitteen verkko-osa ja viimeiset 64 bittiä osoitteen liitäntäosa. Esimerkisi /56-verkkoon jää vielä 8 bittiä aliverkkoja verten, joten se voidaan jakaa vielä 2^8 eli 256:een /64-verkkoon. [17.]

4 Protokollat

Internetin toiminta perustuu moniin eri protokolliin, joiden avulla liikennettä reititetään sekä operaattorin sisällä että muille operaattoreille. Yleisesti reititysprotokollien tarkoitus on reitittää liikenne oikeaan paikkaan parasta tai sille määritettyä reittiä pitkin, ja reitin

vikaantuessa siirtää liikenne toimivalle reitille. Tässä osiossa käyn läpi työn kannalta tärkeitä ja keskeisiä protokollia.

Reititysprotokollia löytyy iso valikoima. Valtaosa niistä on avoimiin standardeihin perustuvia protokollia, mutta jotkin ovat pelkästään yhden laitevalmistajan laitteisiin sopivia. Esimerkiksi Cisco Networksin kehittämä EIGRP (IGP eli Interior Gateway Protocol) on suljettu kaupallinen protokolla. Reititysprotokollat jakaantuvat kahteen ryhmään: ulkoisiin reititysprotokolliin (EGP eli Extrerior Gateway Protocol) ja sisäisiin reititysprotokolliin (IGP eli Interior Gateway Protocol).

Standardiaseman saavuttanut BGP on käytännössä ainut käytössä oleva ulkoinen protokolla. Sen asema johtuu Internetin rakenteesta – Internet perustuu AS-järjestelmiin, jotka reitittävät liikennettä keskenään BGP:n avulla. Sisäisiä reititysprotokollia on olemassa huomattavasti enemmän, kuten OSPF, IS-IS, EIGRP ja RIP.

Sisäiset ja ulkoiset protokollat voidaan jakaa toimintatavan mukaan kahteen ryhmään: etäisyysvektoriprotokolliin (Distance vector) ja linkkitilaprotokolliin (Link State). Etäisyysvektoriprotokollat perustuvat reittien pituuksiin, kun taas linkkitilaprotokollat perustuvat linkkitietoihin ja niiden muodostamaan topologiakuvaan. Taulukko 2 kuvaa protokollien toimintatapoja.

Taulukko 2. Eri reititysprotokollat jaoteltuna ryhmiin toimintatavan ja tarkoituksen mukaan. [19]

<table>
<tr><th></th><th>Etäisyysvektoriprotokollat</th><th>Linkkitilaprotokollat</th></tr>
<tr><td>EGP</td><td>BGP</td><td></td></tr>
<tr><td rowspan="3">IGP</td><td>RIPv1, RIPv2</td><td>OSPF</td></tr>
<tr><td>IGRP</td><td>IS-IS</td></tr>
<tr><td colspan="2">EIGRP</td></tr>
</table>

Kuten taulukosta käy ilmi, BGP, RIP ja IGRP kuuluvat etäisyysvektoriprotokolliin, OSPF ja IS-IS puolestaan linkkitilaprotokolliin. EIGRP luetaan usein etäisyysvektoriprotokollien ryhmään, mutta se pitää muistissa naapurisuhteiden lisäksi myös linkkitilaprotokollien tyylisesti topologiakuvan. EIGRP:llä on siis myös linkkiprotokollan ominaisuuksia, minkä vuoksi sitä nimitetään hybridiprotokollaksi ja kehittyneeksi etäisyysvektoriprotokollaksi. [19.]

4.1 BGP

BGP eli Border Gateway Protocol on Internetissä käytetty reititysprotokolla. Sitä voidaan pitää Internetin tärkeimpänä reititysprotokollana, sillä BGP:tä käytetään reititykseen eri AS:ien eli autonomisten järjestelmien (Autonomic System) välillä. Autonomisella järjestelmällä tarkoitetaan yksittäisen hallinnon alla olevaa reititinkokonaisuutta, jonka osat ovat yhteydessä toisiinsa sisäisellä reititysprotokollalla. Eri autonomisten järjestelmien reunareitittimet muodostavat toisiinsa naapurisuhteita, joiden avulla liikennöinti tapahtuu esimerkiksi eri operaattoreiden välillä. [20.]

BGP toimii TCP-protokollan päällä ja käyttää porttia 179. BGP perustuu reitittimien muodostamiin naapurisuhteisiin (Peer). Naapurisuhteet määritetään reitittimille käsin, jonka jälkeen reitittimet lähettävät toisilleen Open-viestin muodostaakseen yhteyden. Yhteyden muodostumisen jälkeen reitittimet lähettävät Update-viestin, joka sisältää reititystaulun. Tämän jälkeen reititystaulua ei enää lähetetä, ja pelkästään tapahtuvista muutoksista kerrotaan Update-vieteillä. Jos muutoksia tapahtuu harvoin, reitittimet lähettävät Keepalive-viestejä pitääkseen naapuruutta yllä. Neljäs BGP:n käyttämä viestityyppi on Notification, jota käytetään BGP-naapurisuhteen katkaisemiseen virhetilanteessa. [20.]

BGP on etäisyysvektoriprotokolla, sillä järjestelmät etsivät BGP:n avulla lyhimpiä polkuja eri autonomisten järjestelmien läpi kohdeosoitteisiin. BGP:n reititystauluun hyväksytään se reitti, jossa on matkan varrella vähiten autonomisia järjestelmiä. BGP:n reititystaulu sisältää reitin kaikkiin muihin Internetin lähiverkkoihin [20]. IPv4-reittejä on olemassa tällä hetkellä noin 440 000 ja IPv6-reittejä noin 40 000. Nämä määrät voidaan tarkistaa esimerkiksi S1 Networksin BGP-reitittimiltä.

BGP-reitit jaetaan kahteen eri tyyppiin: sisäiseen ja ulkoiseen. Jos naapurireitittimet ovat saman AS-alueen sisällä, tätä kutsutaan sisäiseksi BGP:ksi (iBGP eli internal BGP). Jos naapurireitittimet ovat eri AS-alueiden sisällä, on kyseessä ulkoinen BGP (eBGP eli external BGP). Sisäistä BGP:tä käytetään BGP-reittien jakamiseen saman järjestelmän muille reitittimille. Sisäistä BGP:tä ei välttämättä tarvita, jos AS-alueella on vain yksi liitäntäpiste toiseen AS-alueeseen. Useimmiten AS-alueella on kuitenkin useita liitäntäpisteitä muihin AS-alueisiin, eli alueella on useampi niin sanottu reunareititin. Tällöin on tärkeää pitää reunareitittimet sisäisen BGP:n avulla tietoisina toisien reunareitittimien rei-

teistä. Kun alueen reitittimet tietävät kaikki mahdolliset reittivaihtoehdot kohdeosoitteisiin, reitittimet pystyvät tutkimaan eri AS-alueiden mainostamien reittivaihtoehtojen pituudet, ja lyhin reitti valitaan aktiiviseksi. [20.]

4.2 OSPF

OSPF eli Open Shortest Path First on Internet Engineering Task Forcen (IETF) kehittämä reititysprotokolla. OSPF:n tehtävä on välittää reititystietoja reitittimien välillä. OSPF-alueen kaikilla reitittimillä on tieto koko alueen topologiasta. OSPF voidaan jakaa pienempiin alueisiin, jotta reitittimien muistissa pidettävän topologiakuvan koko ei kasva liian suureksi. Alueiden pilkkomisella voidaan myös hallita verkon toimintaa paremmin. OSFP on ilmainen protokolla, joten kuka tahansa voi lisätä sen laitteeseensa. Tämän vuoksi lähes kaikki reitittimet tukevat OSFP-protokollaa. [21.]

OSPF:n ensimmäisen version standardi julkistettiin vuonna 1990. OSPFv1 oli kuitenkin lähinnä vain testiversio, jonka korvasi vuoden myöhemmin julkaistu toinen versio. OSPFv2 oli ensimmäinen yleiseen käyttöön tullut OSPF. Sen rinnalle luotiin toisen version pohjalta jatkokehitetty kolmas versio, joka toimii IPv6-osoitteilla. OSPF luotiin alun perin vastaamaan sitä edeltäneen RIP-protokollan puutteisiin. RIP-protokolla oli aiemmin käytetyin lähiverkkojen reititysprotokolla, mutta sen heikkouksia olivat etenkin skaalautuvuus isoihin verkkoihin, verkon iso kuormitus ja reittivalintojen nopeuden huomiotta jättäminen. [21.]

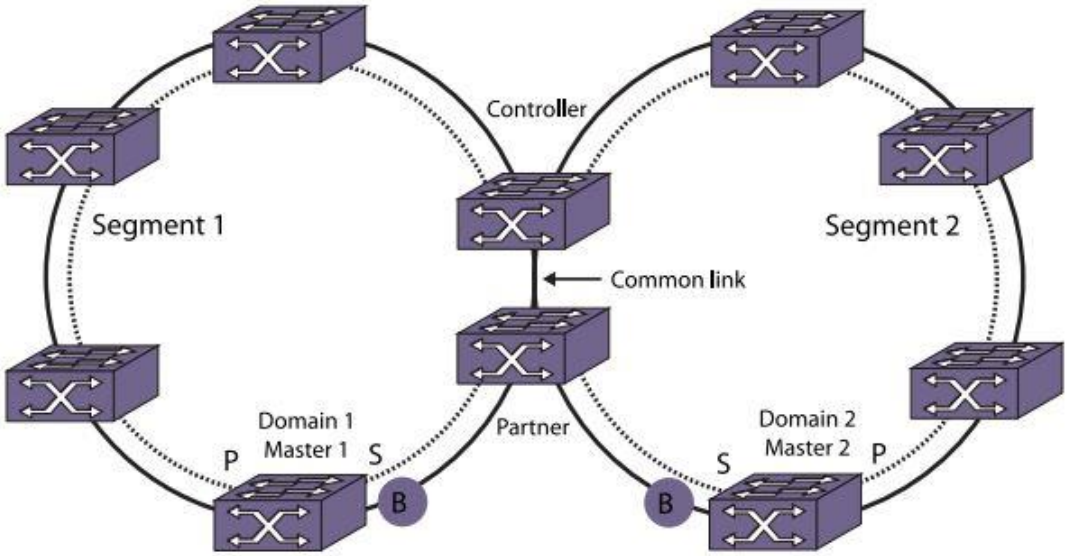
OSPF on linkkiprotokolla, ja se käyttää reititystaulun lisäksi linkkitietokantaa. Jokaisella OSPF-reitittimellä on linkkitietokanta oman alueen linkeistä ja reitittimistä. OSPF käyttää protokollapaketteja reittien väliseen kommunikointiin. Paketteja ovat naapureihin tutustumiseen käytettävä hello-paketti, linkkitietokannan jakamiseen käytettävä database descroption -paketti, reittitietojen pyytämiseen käytettävä link-state request -paketti, reittitietojen levittämiseen käytettävä link-state Update -paketti sekä paketin vastaanottoilmoituksena käytettävä link-state ack -paketti. [22.]

4.3 EAPS

EAPS on Extreme Networksin kehittämä rinkiprotokolla. Rinkiprotokollat ovat tulleet haastamaan Layer-2 yhteyksissä varmennukseen käytettyä Spanning Tree -protokollaa [23, s. 11-12]. Extreme Networksin kehittämän EAPS:n jälkeen monelta muulta valmistajalta tuli markkinoille vastaavia rinkiprotokollia – esimerkiksi Ciscon PRP (Resilient Packet Ring), Huawein RRPP (Rapid Ring Protection Protocol) ja Brocaden MRP (Metro Ring Protocol). Myöhemmin tietoliikenteen standardisoimisjärjestö ITU-T (ITU Telecommunication Standardization Sector) teki rinkiprotokollasta standardin G.8032 Ethernet ring protection switching (ERPS).

EAPS:in toiminta perustuu EAPS-domaineihin eli EAPS-alueisiin, joita voidaan konfiguroida useita yhteen rengastopologiaan. Jokaiselle domainille määritetään yksi rengastopologian kytkimistä master-tilaan eli kyseisen domainin hallisijaksi. Muut kytkimet määritetään transit-tilaan. Master-kytkimen tehtävä on pitää toinen runkolinkkinsä estettynä ja avata se vikatapauksen sattuessa. Liikenteen kääntämiseen menee EAPS-protokollalla 50 ms. Transit-tilassa olevien kytkinten tehtävä on lähettää master-kytkimelle ilmoitus, jos toinen runkolinkeistä katkeaa tai alkaa taas toimia. [23, s. 11-14.]

Jokaiselle EAPS-domainille konfiguroidaan myös niin sanottu liikenteen kulkusuunta. Useimmiten jokaiseen EAPS-rengastopologiaan tehdään kaksi EAPS-domainia siten, että liikennettä ajetaan eri suuntiin. Tällöin toisen EAPS-domainin estetty runkolinkki on käytössä toisella EAPS-domainilla. Siten normaalitilanteessa saadaan hyödynnettyä verkon koko kapasiteettia. [23, s. 11-14.]



Kuva 5. Rengastopologian mukaisia verkkoja voidaan liittää toisiinsa. Tämä on huomioitava EAPS-protokollaa konfiguroitaessa. [23, s. 16.]

Jotta verkko olisi mahdollisimman vikasietoinen, on hyvä toteuttaa kaksi rinnakkaista rengastopologian mukaista verkkoa, joilla on yksi yhteinen kytkinväli, kuten kuvassa 5. Tällöin EAPS:n tyylisen protokollan toteutuksessa on otettava huomioon jaetun kytkinvälin tuottamat vaarat. Kuvan 5 mukaisessa toteutuksessa samat VLAN-ID:t kulkevat molemmissa renkaissa. Ongelmatilanne syntyy, jos kuvaan merkitty Common link katkeaa. Tällöin kuvaan B-kirjaimilla merkityt estetyt portit avataan, ja koko verkko muodostaa loopin eli silmukan, joka aiheuttaa broadcast-myrskyn. Tällaisesta tilanteesta käytetään nimitystä super loop. EAPS-protokollassa tällainen tilanne estetään konfiguroimalla kyseiseen kytkinväliin shared-port-ominaisuus, jolla valvotaan kahden EAPS-rengastopologian jakamaa kytkinväliä. Shared-port-ominaisuudessa toinen kytkin on Controller- ja toinen Partner-moodissa. Common link -yhteyden vikaantuessa Controller-kytkin estää liikenteen kulkemasta toiseen toimivista EAPS-porteista. [23, s. 12-19.]

5 Verkon päivitysprojektin lähtökohdat

Työantajallani S1 Networksilla on kasvaneen asiakaskunnan ja suuremman verkkokapasiteetin tarpeen vuoksi tulossa suurehko verkkolaitteiden päivitysprojekti, jonka sain ottaa lopputyön kohteeksi. Päivitysprojektin suurin osuus on uusien runkoreitittimien käyttöönotto, jota tässä työssä käyn läpi. Myös kytkinverkkoon täytyy tehdä muutoksia,

joten tämän työn tarkoituksena on käydä läpi myös reitittimien ja kytkimien muodostamaa vikasietoista verkkokokonaisuutta.

5.1 Toimeksiantaja

Työn toimeksiantaja on S1 Networks, joka on Internet-palveluntarjoaja eli ISP. Yritys on uusi ja nopeasti kasvava toimija alalla – yritys on perustettu vasta vuonna 2011, ja yrityksellä on jo kattava verkko pääkaupunkiseudulla. Yrityksen tärkeimmät palvelut ovat valokuituinternetyhteydet, konesalipalvelut ja yhdistämispalvelut toimistojen ja konesalien välillä. Yrityksen toimintaperiaatteena on tarjota verkkoyhteyksien lisäksi kokonaisvaltaisia asiakkaiden tarpeisiin räätälöityjä verkkototeutuksia, joihin kuuluvat verkko-, tietoliikenne- ja IT-laitteet, varmistus-, konesali-, verkko- ja virtualisointiratkaisut, puhelinjärjestelmät, matkapuhelimet, ohjelmistot sekä etähallinta- ja tukipalvelut.

S1 Networks hyödyntää muiden operaattorien olemassa olevia kuituyhteyksiä, sillä yrityksen omistuksessa ei ole kovinkaan laajaa kuituinfrastruktuuria. Uusien kiinteistöjen kohdalla kartoitetaan aina oman kuidun rakennusmahdollisuudet ja selvitetään fyysisen kuidun vuokrausmahdollisuudet alueen HMV-operaattorilta. Tämän jälkeen tehdään päätös, miten kuituyhteydet toimitetaan kohdekiinteistöön. HMV-operaattori on operaattori, jolla on alueella huomattava markkinavoima ja sitoutuu vuokraamaan yhteyksiä viestintäviraton asettamilla hintarajoitteilla. Tästä johtuen S1 Networksin liiketoiminta painottuu vielä suurelta osalta yhteen HMV-alueeseen eli pääkaupunkiseutuun. Vaikka S1 Networks hyödyntää vuokrayhteyksiä, yritys on täysin itsenäinen Internet-palveluntarjoaja. Yrityksen yhteydet eivät perustu yhden ison operaattorin ulkoverkon yhteyteen, vaan S1 Networksilla on useita liityntäpisteitä usealle maailmanlaajuiselle runkoverkon tarjoajalle.

5.2 Tarkoitukset ja päämäärät

Työn tarkoitus on parantaa palveluntarjoajaverkon suorituskykyä, vikasietoisuutta ja tietoturvallisuutta, jotta se kattaisi nykyiset ja tulevaisuuden tarpeet. Pääpiirteittäin tarkoituksena on saada aikaan verkko, jossa on kaksi reunareititintä eri alueilla, jotka hoitavat BGP-reitityksen. Näiden reitittimien välissä on kytkimillä muodostettu rengastopologian mukainen Metro ethernet -runkoverkko. Riittävän kapasiteetin lisäksi verkon tärkeimmät

vaatimukset ovat vikasietoisuus ja skaalautuvuus tuleviin laajennuksiin. Tavoitteena on saada aikaan verkko, missä minkä tahansa yksittäisen yhteyden, laitteen tai keskuksen vikaantuminen aiheuttaisi korkeintaan alueellisen katkoksen.

6 Laitteisto

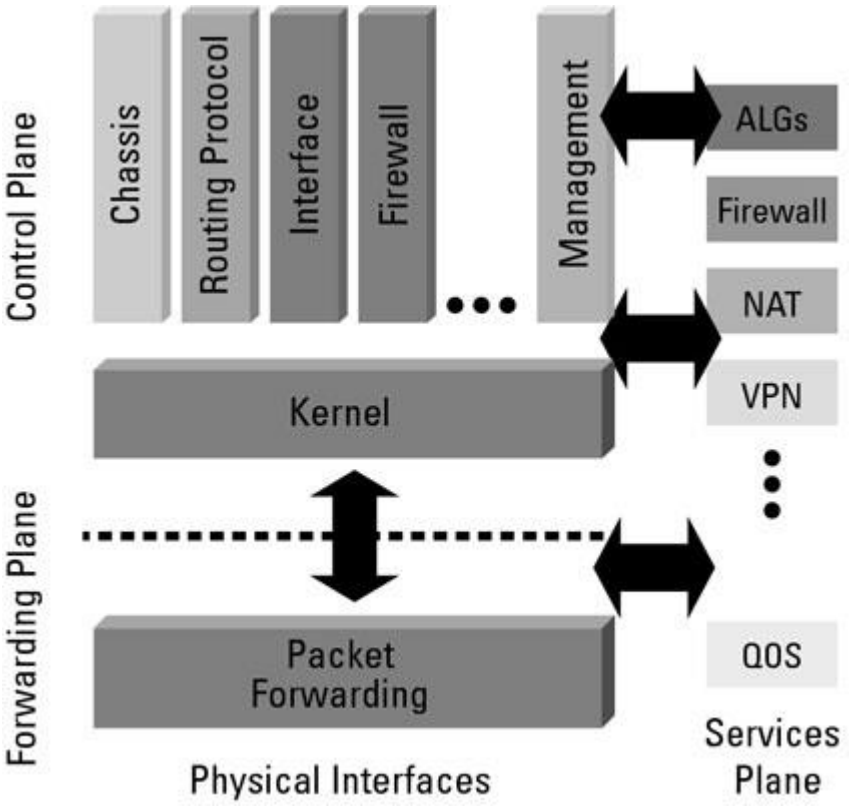
Työssä käytettävä laitteisto on suurimmaksi osaksi ennestään olemassa olevaa, ja uudet runkoreitittimet on hankittu jo ennen tämän työn aloittamista. Siksi tähän työhön ei kuulu minkäänlaista hankintaprosessia. Verkossa käytetään pääasiassa Extreme Networksin kytkimiä. Reitittiminä käytetään Internet-palveluntarjoajien suosimia Juniper Networksin MX-sarjan reitittimiä.

6.1 Juniper Networks

Juniper Networks on yhdysvaltalainen yksi johtavista tietoliikenne- ja verkkolaitteiden laitevalmistajista. Juniperin tuotevalikoimasta löytyy laitteita aina pientoimistokytkimistä ja -reitittimistä todella järeisiin runkoreitittimiin. Juniper on keskittynyt erityisesti runkoreitittimien valmistukseen ja heidän markkinaosuutensa runkoreititinmarkkinoilla on todella suuri.

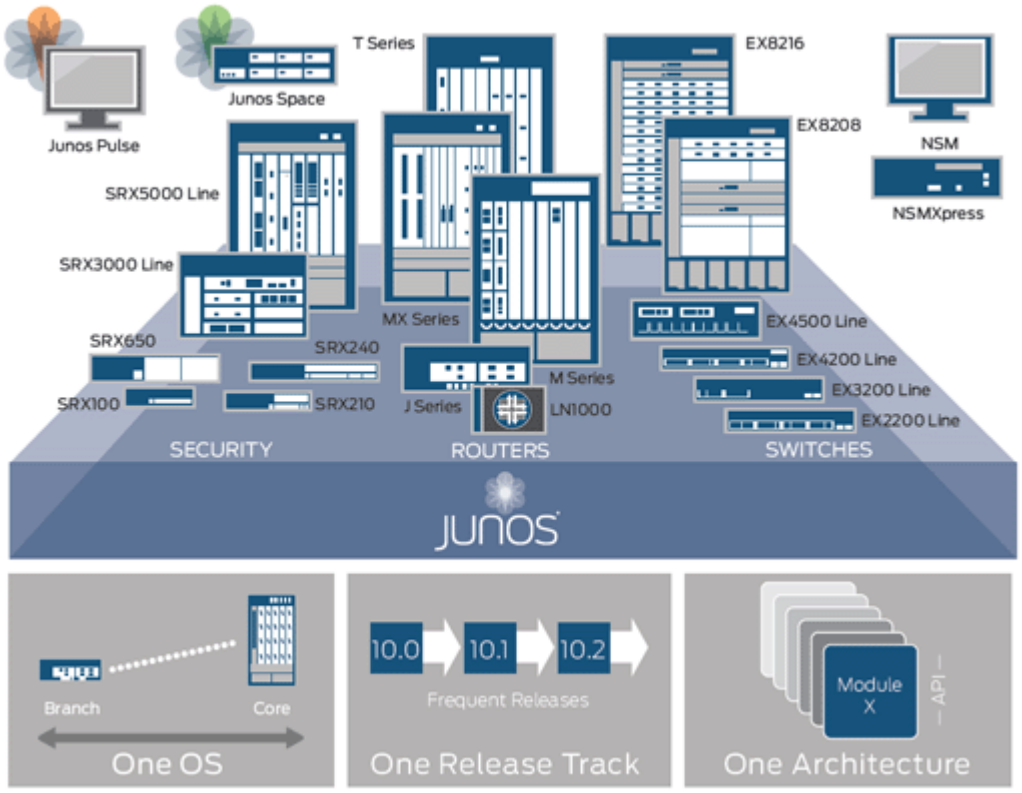
6.1.1 Junos

Juniperin käyttämä käyttöjärjestelmä tunnetaan nimellä Junos. Junos eli Juniper Networks Operation System -käyttöjärjestelmä on käytössä nykyään lähes kaikilla Juniperin valmistamilla laitteilla. Junos pohjautuu FreeBSD:een, ja ensimmäisen kerran Junos julkaistiin M40-reititttimen kanssa vuonna 1998. Junos on modulaarinen käyttöjärjestelmä. Modulaarisen arkkitehtuurin hyötynä on moduulien itsenäinen toiminta – yhden moduulin vikatoiminto ei voi kaataa toista moduulia, sillä jokainen moduuli pyörii omassa suojatussa muistissaan. Käyttöjärjestelmä voidaan jakaa kolmeen eri toimintatasoon, joita ovat hallinta, palvelu ja edelleenlähetys. Kuva 6 esittää Junosin arkkitehtuuria, jossa näkyvät nämä kolme toimintatasoa sekä kullakin tasolla suoritettavia esimerkkiprosesseja. [24, s. 9-18.]



Kuva 6. JUNOS koostuu kolmesta toimintatasosta, joilla suoritetaan kuhunkin tasoon kuuluvat prosessit. [24, s. 12.]

Junos on erittäin pidetty käyttöjärjestelmä erityisesti sen tehokkaan kielen ja hyvän konfiguraatioversion hallinnan takia. Juniper Networks käyttää monista muita valmistajista poiketen yhtä käyttöjärjestelmää kaikissa kytkimissään pientoimistotason tuotteista konesalitason tuotteisiin. Tämän säästää yrityksien koulutuskuluja ja helpottaa monen verkkoinsinöörin työtä. Kuva 7 esittää Juniper Networksin tuoteperhettä ja sitä, kuinka yksi käyttöjärjestelmä kattaa kaikki tuotteet.



Kuva 7. Koko Juniperin tuoteperhe muodostuu JUNOS-käyttöjärjestelmän ympärille. [25]

6.1.2 Työssä käytetty laitteisto

Tässä työssä on käytössä kaksi Juniperin MX104-reititintä. MX104 on modulaarinen, korkean vikasietoisuuden ja täydet ominaisuudet tarjoava MX-sarjan reititin. MX104-reitittimen rungosta löytyy neljä 10GbE SFP+ -paikkaa ja neljä MIC-moduulipaikkaa. Näiden liitäntöjen kautta reititin pystyy tarjoamaan yhteensä 80 Gbps kapasiteettia. Reitittimestä löytyy myös kaksi virtalähdettä ja kaksi reititysmoduulipaikkaa.

6.2 Extreme Networks

Extreme Networks on erityisesti verkkokytkimien valmistukseen keskittynyt yhdysvaltalainen laitevalmistaja. Extremen tuotevalikoimaan kuuluvat runkokytkimien lisäksi langattomat tukiasemat ja kevyet toimistokytkimet. Extreme on tunnettu hinta-laatusuhteeltaan hyvistä ja tehokkaista kytkimistä.

Tässä työssä käytetään Extremen Summit-sarjan X670-, X480-, X460- ja X440-kytkimiä. Nämä Summit-sarjan kytkimet ovat L3-kytkimiä, joista löytyy suurin osa reititysprotokollista jaettuna eri lisenssitasoihin. Verkon suorituskykyisimmät kytkimet ovat Summit X670-48X -kytkimet, joista löytyy 48 SFP+ -paikkaa. X480-, X460- ja X440-kytkimet ovat 26–52-porttisia, joista 2–6 on SFP+-portteja ja loput SFP- tai Ethernet-portteja. Useimmissa kytkimissä osa porteista on yhdistelmäportteja, joissa on sekä Ethernet- että SFP-liitännät. Extremen käyttöjärjestelmänä toimii ExtremeXOS, joka toimii vain CLI:n kautta. Monista muista käyttöjärjestelmistä poiketen Extremen käyttöjärjestelmässä on vain yksi taso, johon syötetään kaikki laitteen muutoksiin ja hallintaan liittyvät käskyt.

7 Suunnittelu ja toteutus

Verkon suunnittelussa on otettava huomioon verkon käyttötarkoitukset, kapasiteetin tarve, haluttu luotettavuustaso ja käytössä olevat resurssit. Verkon pystytykseen pätee sanonta ”hyvin suunniteltu on puoliksi tehty” – verkon toteutus on melko helppoa ja mekaanista työtä, jos suunnitelma on tehty huolella. Tässä luvussa kerron sekä työn suunnittelun kannalta oleellisia seikkoja että toteutuksen eri vaiheista. Tämä luku neljään alalukuun: Luvussa 7.1 käyn läpi IP-osoitteita ja AS-numeroita. Luvussa 7.2 kerron verkkotopologian suunnittelusta. Kahdessa viimeisessä alaluvussa kerron itse konfiguraatiotyöstä siten, että luvussa 7.3 kerron reititinverkon konfiguroinnista ja luvussa 7.4 kytkinverkon konfiguraatioista.

7.1 IP-osoitteet ja AS-numerot

IP-osoitteet ovat laitekohtaisia, joten niiden käyttöä täytyy hallita koko Internetin laajuisesti. IP-osoitteita maailmanlaajuisesti hallitseva organisaatio on IANA (Internet Assigned Numbers Authority). Osoitteiden hallinta on jaettu alueellisille RIR-organisaatioille (Regional Internet Registry). Euroopassa osoitteita ja AS-numeroita hallitsee RIPE NCC (RIPE Networks Coordination Center). Omistaakseen PA-osoitteita tai reitittääkseen asiakkaisen PI-osoitteita täytyy olla rekisteröitynyt LIR:ksi. LIR eli Local Internet Registry on organisaatio, jolle alueellinen RIR-organisaatio on myöntänyt osoiteavaruuden. LIR-organisaatio on puolestaan luvannut jakaa osoiteavaruudestaan osoitteita omille asiakkailleen. Suurin osa LIR-organisaatioista on Internet-palveluntarjoajia. [26.]

Tämän työn toimeksiantaja S1 Networks on rekisteröitynyt LIR-organisaatioksi. Yritys omistaa osoiteavaruuksia ja reitittää myös asiakkaittensa IP-osoitteita. Työssä käytetyt IP-osoitteet ovat työn toimeksiantajan S1 Networksin omistuksessa tai S1 Networksin asiakkaiden omistuksessa. Esimerkiksi S1 Networksin asiakkaalla Metropolia Ammattikorkeakoulun verkkolaboratoriolla on oma PI-avaruus IP-osoitteita ja transit-linkki S1 Networksin verkkoon. Näin ollen Metropolian verkkolaboratorion verkon liikenne reititetään S1 Networksin AS-numeron kautta Internetiin.

7.2 Verkkotopologia

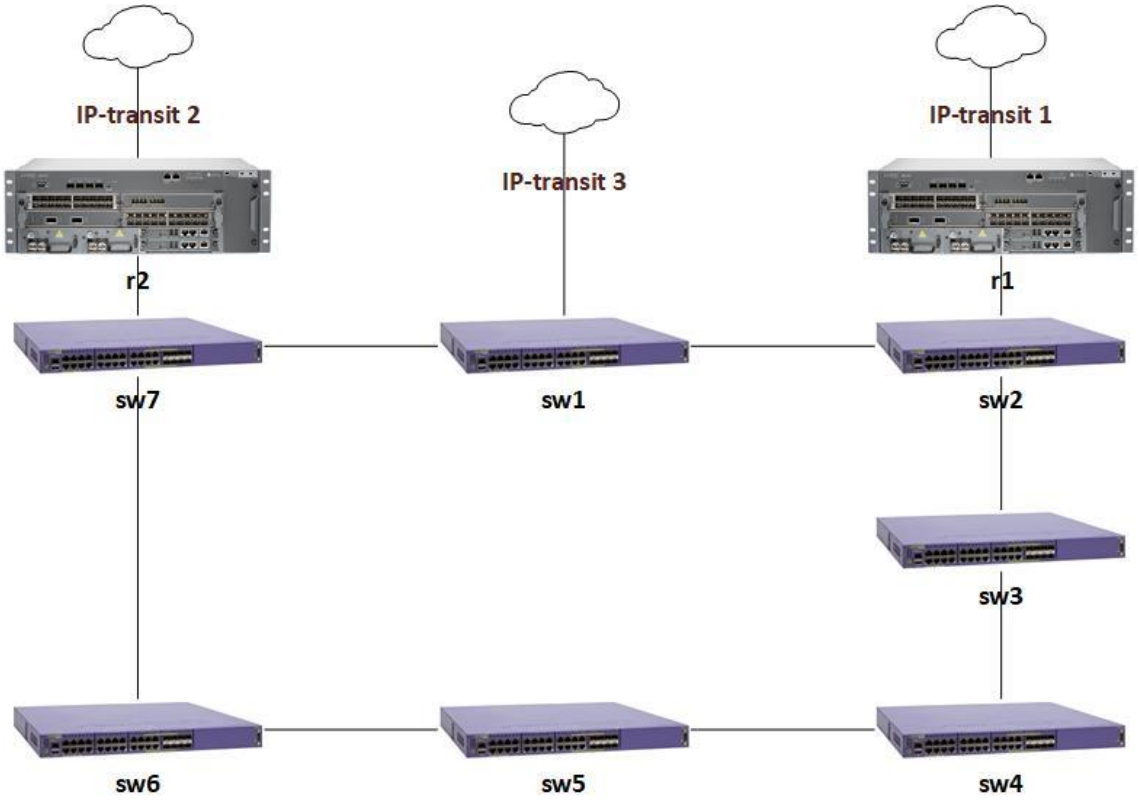
Verkkotopologiaa suunnitellessa tärkeintä on huomioida verkon vikasietoisuus ja käydä läpi, miten verkko reagoi missäkin vikatilanteessa. Huomioon on kuitenkin otettava myös topologian kustannukset. Vikasietoisuuden näkökulmasta verkko kannattaisi rakentaa Mesh-topologialla, jossa kaikilla laitteilla on linkki toisiinsa. Tämä ei kuitenkaan ole lainkaan kustannustehokas ratkaisu.

Verkkolaitteiden päivitysprojektissamme suunnittelun lähtökohta on se, että verkko kestää minkä tahansa yksittäisen verkkolaitteen, linkin tai verkkoalueen vikaantumisen. Yhden verkkolaitteen tai kokonaisen verkkoalueen vikaantumisesta voi kuitenkin aiheutua alueellinen katkos, sillä viimeistä linkkiä asiakkaan suuntaan ei kahdenneta muissa kuin korkean palvelutason liittymissä (SLA).

Asetettujen lähtökohtien pohjalta rengastopologia sopii hyvin työn kohteena olevaan verkkokokonaisuuteen. Rengastopologiassa jokaisella verkkolaitteella on kaksi naapuria eli kaksi suuntaa, johon liikennettä voidaan lähettää. Jos toinen naapuri tai yhteys naapurille vikaantuu, voidaan liikennettä lähettää toimivan naapurin suuntaan. Rengastopologia vaatii tietenkin protokollan hallitsemaan liikenteen kulkua. Rengastopologia sinänsä on silmukka (loop), josta aiheutuu broadcast-myrsky. Tästä johtuen jokin renkaan linkeistä täytyy olla aina estettynä. Suunnitellun rengastopologiaan perustuvan verkon laitteina käytetään ainoastaan Extreme Networksin laitteita, ja Extreme Networksin kehittämä EAPS-protokolla sopii hyvin verkon varmistukseen.

Päivitysprojektissa on käytettävissä kaksi kappaletta Juniper MX104 -reititintä, jotka halutaan tietenkin käyttöön eri verkkoalueille. MX104-reitittimien päätehtävä on huolehtia liikenteen BGP-reitityksestä IP-transitien ja asiakkaiden suuntaan. MX104-reitittimissä

olemassa olevilla lisensseillä on käytössä kaksi 10 Gbps:n porttia. Tämä asettaa jonkin verran rajoitteita verkkoarkkitehtuuriin reitittimien osalta. Molemmista reitittimistä toinen portti varattiin IP-transitin suuntaan ja toinen operaattorin runkoverkon suuntaan. MX104-reitittimien väliin olisi hyvä saada oma linkki sisäistä BGP-liikennettä varten, mutta sitä ei kuitenkaan voida rakentaa vielä tässä projektissa. Sisäinen BGP-liikenne ajetaan tästä johtuen varmistetun kytkinverkon läpi. Lisäportit laitetaan hankintalistalle seuraavaa päivitysprojektia varten.



Kuva 8. Yksinkertaistetussa topologiakuvassa on kolme IP-transitia, kaksi MX104-reititintä ja seitsemän kytkintä rengastopologian muodossa.

Verkko rakennetaan siten, että verkkolaitteita on seitsemällä eri verkkoalueella ja ne muodostavat rengastopologian. Kahdella alueella on Juniperin MX104-reititin ja IP-transit-yhteydet. Lisäksi yhdellä verkkoalueella on IP-transit-linkki, jonka naapurireititintä voidaan vahtaa tarvittaessa. Täten rakennetaan kuvan 8 esittämän verkkotopologian kaltainen verkko.

7.3 Reitittimien konfiguraatiot

Reitittimille tärkeimmät käyttöönotettavat protokollat ovat BGP- ja OSPF-protokollat. Tässä luvussa esittelen, miten kyseiset protokollat konfiguroidaan ja miksi tiettyihin ratkaisuihin päädytään. Vertailen myös vaihtoehtoisia konfiguraation toteutustapoja. Käytän tietoturvasyistä tulevissa konfiguraatioesimerkeissä sisäverkko-osoitteita oikeiden julkisten IP-soitteiden sijaan.

7.3.1 IP-transit-konfiguraatiot

IP-transit on palvelu, joka tarjoaa rajapinnan globaaliin Internettiin. IP-transitien konfiguraatiossa on tärkeää mainostaa verkot kokonaisia blokkeina ja estää pilkottujen, sisäisessä käytössä olevien, verkkojen vuotaminen IP-transitin suuntaan. Kun verkot pilkotaan eri käyttötarkoituksia varten pienempiin verkkoihin, reitittimen reititystaulusta ei löydy esimerkiksi kokonaisia /22-verkkoja. Jotta voidaan mainostaa kokonaisia verkkoja, niiden pitää löytyä reitittimen reititystaulusta. Tämä tehdään yleensä reitittämällä verkko reitittimeen itseensä. Junoksesta löytyy kuitenkin oma komento verkon ”summaamista” varten:

```
set routing-options aggregate route 10.10.10.0/23
```

Tällä voidaan summata esimerkiksi verkot 10.10.10.0./24, 10.10.11.0./25 ja 10.10.11.128./25 yhdeksi verkoksi, jotta verkot tulisivat mainostetuiksi oikein muiden autonomisten järjestelmien läpi. Jotta saadaan estettyä muiden kuin haluttujen verkkojen mainostumien transitin suuntaan, on tehtävä prefix-list eli lista verkoista, jota mainostetaan transitille. Jokaiselle IP-transitille on parasta tehdä oma lista, jotta voidaan tarvittaessa estää jonkin verkon mainostus tietylle transitille.

```
set policy-options prefix-list transit1-prefix 10.10.10.0/23
set policy-options prefix-list transit1-prefix 10.20.10.0/22
set policy-options prefix-list transit1-prefix 10.100.20.0/22
```

Yllä esitetyillä komennoilla saadaan aikaiseksi transit1-prefix-niminen prefix-list, joka sisältää verkot 10.10.10.0/23, 10.20.10.0/22 ja 10.100.20.0/22. Seuraavaksi voidaan tehdä itse sääntö, jolla määrätään, mitkä prefix-listit ovat sallittuja transitin suuntaan.

```
set policy-options policy-statement transit1-export term 1 from
prefix-list transit1-prefix
set policy-options policy-statement transit1-export term 1 then
accept
set policy-options policy-statement transit1-export term 2 then
reject
```

Näillä komennoilla tehdään sääntö transit1-export, jonka ensimmäisessä säännössä sallitaan prefix-listan transit1-prefix verkot, ja toisessa termissä estetään muut verkot. Kun säännöt on tehty BGP-konfiguraatiota varten, voidaan konfiguroida BGP-naapurisuhde transitille. Junoksessa voidaan tehdä BGP-ryhmiä, joiden avulla voidaan hallita helposti verkkojen mainostusta. BGP-konfiguraatiota varten reitittimelle asetetaan AS-numero eli autonomisen järjestelmän numero. S1 Networksin AS-numero on 199508. Listaus kaikista AS-numeroista löytyy esimerkiksi sivulta http://bgp.potaroo.net/cidr/autnums.html.

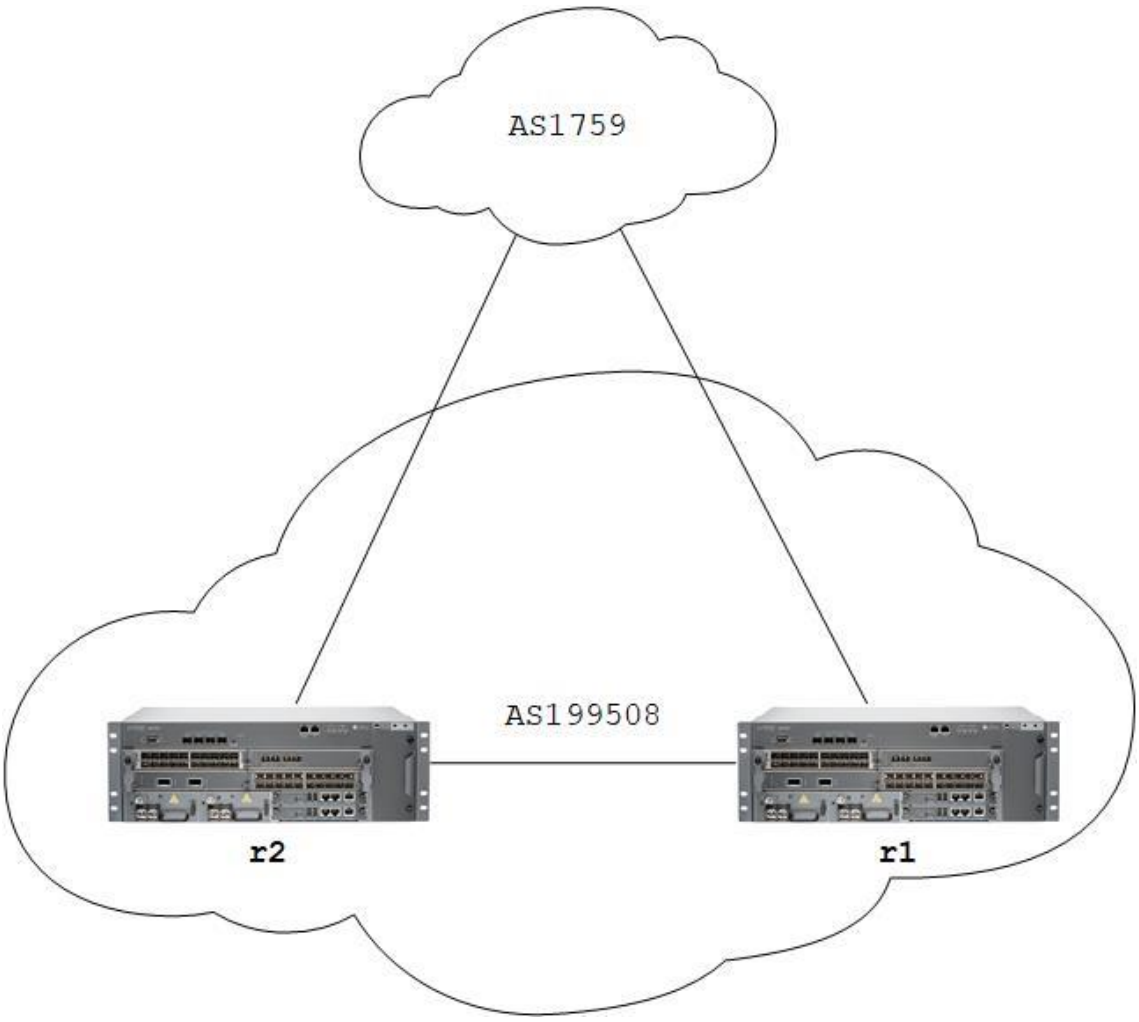
```
set routing-options autonomous-system 199508
set protocols bgp group transit1-peers type external
set protocols bgp group transit1-peers description ”IPtransit 1"
set protocols bgp group transit1-peers export transit1-export
set protocols bgp group transit1-peers local-address 172.32.12.2
set protocols bgp group transit1-peers peer-as 1759
set protocols bgp group transit1-peers neighbor 172.32.12.1 re-
move-private
set xe-2/0/1 unit 0 family inet address 172.32.12.1/30
```

Yllä olevissa esimerkeissä AS-numeron asettamisen jälkeen tehdään BGP-ryhmä transit1-peers, johon konfiguroidaan tärkeimmät asetukset. Koska kyseessä on IP-transit, BGP:n tyyppi on ulkoinen eli external. BGP-ryhmällä on hyvä olla myös kuvaus, joka voidaan asettaa description-kenttään. Seuraavalla komennolla asetetaan aiemmin tehty sääntö export-komennolla, jolloin vain säännössä määrätyt verkot tulevat mainostetuiksi IP-transitille.

Tärkeimpiä komentoja BGP:n toiminnan kannalta on asettaa naapurin AS-numero ja IP-osoite. Tässä esimerkissä naapurina olisi TeliaSonera Finland. Naapurin IP-osoitteen perään asetettu komento ”remote-private” estää palveluntarjoajan verkossa käytettyjen sisäiseen, yksityiseen käyttöön tarkoitettujen AS-numeroiden eli as-numeroiden 64512–

65534 ja 4200000000–4294967294 mainostamisen IP-transitin suuntaan. Tässä esimerkissä IP-transit tarjoajan ja kyseisen reitittimen välillä on linkkiverkko 172.32.12.0/30. Tästä verkosta osoite 172.32.12.2 on konfiguroitu esimerkin mukaisesti kyseiselle reitittimelle, ja osoite 172.32.12.1 on IP-transit tarjoajan reitittimellä. Näiden komentojen lisäksi BGP-yhteyksissä käytetään usein salauksena esimerkiksi MD5-autentikaatiota.

BGP-yhteyksiä voidaan painottaa eli säädellä sen mukaan, mitä kautta liikenteen halutaan oletuksena kulkevan. Jos IP-transitin suuntaan on tehty kaksi BGP-linkkiä, voidaan lähtevää liikennettä painottaa local-preferencellä ja saapuvaa liikennettä Metrikillä. Local-preferencen arvo on 32-bittinen luku, joten se on väliltä 0–4 294 967 295 ja sen oletusarvo on 100. Mitä suuremmaksi arvo asetetaan, sitä korkeampi painotus reitillä on. MED-arvo on samaan tapaan 32-bittinen luku, mutta sen painotus eroaa local-preferencesta – reitti on sitä matalammin painotettu, mitä korkeampi luku on. Esimerkiksi kuvan 9 mukaisessa toteutuksessa voidaan asettaa arvot.



Kuva 9. Toteutetussa verkossa on kaksi yhteyttä samalle IP-transit-tarjoajalle.

```
R1:
set protocols bgp group transit1-peers local-preference 150
set protocols bgp group transit1-peers neighbor 172.32.12.1 met-
ric-out 10

R2:
set protocols bgp group transit2-peers local-preference 50
set protocols bgp group transit2-peers neighbor 172.32.12.5 met-
ric-out 20
```

Kaikki liikenne kulkee R1:n BGP-linkkiä pitkin transit-tarjoajalle, koska R1 tarjoaa pienempää metric-arvoa transit-tarjoajan suuntaan ja isompaa local-preference-arvoa reitittimien sisäiseen reititystauluun. Tämä on yksinkertaistettu esimerkki BGP-painotuksesta. Usein eri verkot halutaan reitittää eri BGP-linkkejä pitkin, jolloin painotukset tehdään policy-sääntöjen avulla. Esimerkiksi seuraavilla komennoilla voidaan tehdä policy-säännöt, jotka asettavat metric-arvon 10:een, jos kyseessä verkko 10.20.10.0/22. Muussa tapauksessa metric-arvo on 30. Tällöin kuvan 9 mukaisessa tapauksessa vain verkolla 10.20.10.0/22 on paras reitti R1 BGP-linkin kautta.

```
R1:
set policy-options policy-statement med-10 from route-filter
10.20.10.0/22 exact
set policy-options policy-statement med-10 then metric 10
set policy-options policy-statement med-10 then accept
set policy-options policy-statement med-30 from route-filter
0.0.0.0/0 longer
set policy-options policy-statement med-30 then metric 30
set policy-options policy-statement med-30 then accept

set protocols bgp group external neighbor 172.32.12.1 export
med-10
set protocols bgp group external neighbor 172.32.12.1 export
med-30
```

7.3.2 BGP-asiakaskonfiguraatiot

Monet isot yritykset omistavat oman AS-numeron ja oman IP-avaruuden. Tällöin yritys haluaa internetyhteyden toimitettavan BGP-protokollalla. BGP-protokollalla toimitetussa yhteydessä on etuna Internet-yhteyden helppo varmistaminen eri ISP-tarjoajien yhteyksien välillä. Vaihtoehtoja BGP-yhteydelle on yleensä kaksi: joko yritys ottaa vastaan koko Internetin reititystaulun tai pelkästään oletusretin ulkoverkkoon.

Monilla yrityksillä ei ole tarvetta ottaa vastaan koko Internetin reititystaulua. Reitittimet, joihin Internetin reititystaulu mahtuu, ovat jo hintatasoltaan melko arvokkaita. Käytännössä reititystaulun sijasta asiakkaalle mainostetaan koko IP-avaruutta yhtenä reittinä, niin sanottuna nollareittinä. Kun asiakkaalle mainostetaan vain nollareittiä, asiakas ei pysty jakamaan liikennettä mahdollisien useiden operaattoreiden kesken. Tällöin liikenteen painotukset on tehty siten, että kaikki liikenne siirtyy toiselle palveluntarjoajalle, jos käytössä oleva yhteys katkeaa.

Asiakkaille tehtävät BGP-konfiguraatiot vastaavat pitkälle edellä tehtyä IP-transitille tehtyä BGP-naapurisuhdetta. On huolehdittava, että asiakkaalle tulevat mainostetuiksi oikeat reitit, esimerkiksi koko Internetin reititystaulu. Tärkeää on myös huolehtia, ettei asiakkaalle hyväksytä muita verkkoja kuin asiakkaalle varatut IP-osoitteet tai asiakkaan omat PI-osoitteet.

```
set policy-options prefix-list customer1-prefix 10.136.36.0/22
set policy-options policy-statement customer1-import term 1 from
prefix-list customer1-prefix
set policy-options policy-statement customer1-import term 1 then
accept
set policy-options policy-statement customer1-import term 2 then
reject
set protocols bgp group customer1-peers import customer1-import
```

Edellä olevassa esimerkissä luodaan lista customer1-prefix, joka sisältää asiakkaan osoiteavaruuden. Tämän jälkeen tehdään sääntö customer1-import, jossa sallitaan vain customer1-prefix-listalla olevat verkot ja muut verkot estetään. Lopuksi tämä sääntö lisätään import-komennolla asiakkaan BGP-ryhmään. Jos Internet halutaan mainostaa asiakkaalle vain yhtenä reittinä, tämä voidaan toteuttaa seuraavanlaisilla komennoilla.

```
set policy-options policy-statement advertise-default term 1
from route-filter 0.0.0.0/0 exact
set policy-options policy-statement advertise-default term 1
then accept
set routing-options static route 0.0.0.0/0 discard
set protocols bgp group customer1-peers export advertise-default
```

Esimerkissä luodaan sääntö advertise-default, jossa tehdään reittifiltteri, joka sallii vain 0.0.0.0/0-reitin. Tätä varten reititystaulusta täytyy löytyä kyseinen reitti. Tämä onnistuu erimerkiksi yläpuolella tehtyyn tapaan tekemällä staattinen reitti, jossa verkko reititetään niin sanotusti roskiin. Tämä sääntö pitää lisätä vielä export-komennolla asiakkaan BGP-ryhmään.

7.3.3 Internal BGP -konfiguraatiot

Sisäisen eli Internal BGP:n tarkoituksena on mainostaa muille saman AS-alueen reitittimille reitit ulkoverkkoon tai sisäisiin verkkoihin. Sisäisessä BGP:ssä aikaisempiin BGP-konfiguraatioihin eroten asetetaan tyypiksi Internal. Seuraavassa esimerkissä luodaan BGP-ryhmä internal-peers sisäiseen BGP-reititykseen.

```
set interfaces lo0 unit 2 family inet address 192.163.6.4/32
set routing-options router-id 10.1.10.2
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 10.1.10.2
set protocols bgp group internal-peers neighbor 10.1.10.3
set protocols bgp group internal-peers neighbor 10.1.10.4
```

Sisäistä BGP:tä varten reitittimelle kannattaa asettaa loopback-osoite, joka voidaan asettaa myös reitittimen tunnukseksi. Naapurisuhteita luodessa kannattaa BGP:lle antaa suoraan naapurin loopback-osoite. Loopback-osoitteiden reitityksestä muille alueen reitittimistä huolehditaan OSFP-protokollalla, jonka konfiguroinnista kerron seuraavassa luvussa. Kaikki reitittimien ulkoiset BGP-reitit mainostuvat sisäiseen BGP:hen. Ulkoisten reittien mainostusta ei usein haluta rajoittaa, joten mainostuksessa on huolehdittava vain sisäisten reittien mainostamisesta. Reitittimen omat reitit näkyvät reititystaulussa direct-reitteinä. Näiden reittien mainostus onnistuu luomalla seuraavalainen sääntö.

```
set policy-options policy-statement send-direct term 2 from pro-
tocol direct
set policy-options policy-statement send-direct term 2 then ac-
cept
set protocols bgp group internal-peers export send-direct
```

Esimerkissä tehdään sääntö send-direct ja hyväksytään siihen kaikki direct-reitit. Tämä sääntö lisätään aiemmin luotuun BGP-ryhmään internal-peers. Jos reitittimellä on staattisia reittejä, voidaan tehdä samanlainen sääntö korvaamalla vain sana direct sanalla static.

7.3.4 OSPF-konfiguraatiot

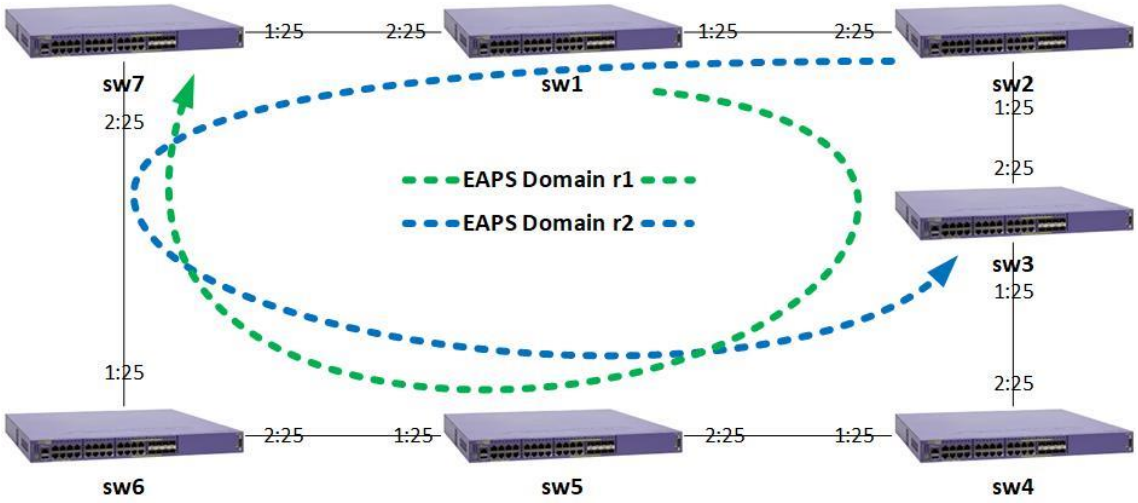
Sisäiseen reititykseen valitaan linkkitietokantaprotokolla OSPF- ja IS-IS -protokollien väliltä. Protokollien vertailussa OSPF-protokolla osoittautuu soveltuvan paremmin tähän verkkoon laajempien ominaisuuksiensa vuoksi. IS-IS-protokollan suurin etu on sen skaalautuvuus isoihin verkkoihin, mutta tätä ominaisuutta ei kuitenkaan pystytä hyödyntämään kyseisessä verkossa. OSPF-protokolla on kohtalaisen yksinkertainen konfiguroitava. Aluksi tarvitaan tietenkin linkkiverkko reitittimien välille.

```
set interfaces ge-0/1/1 unit 5 family inet address 10.2.10.1/30
set protocols ospf area 0 interface lo0.0 passive
set protocols ospf area 0 interface xe-2/0/0.10
```

IP-osoite asetetaan liitäntään, joka on kytketty toiseen reitittimeen. Kun reitittimien välillä on linkki, voidaan konfiguroida OSPF-alue. Runkoalueella käytetään aina nolla-aluetta. Alueen alle lisätään kaikki tarvittavat liitännät – tässä tapauksessa linkkiverkon liitännän lisäksi OSPF:n läpi halutaan mainostaa loopback-osoitetta. Edellä tehty sisäinen BGP-konfiguraatio hyödyntää OSPF:n kautta saatua tietoa naapurin loopback-osoitteesta. Loopback-osoitteen eli lo0.0-liitännän perään lisätään passive-komento, jottei kyseiseen liitäntään tarvitse lähettää OSPF-kyselyjä.

7.4 Kytkinkonfiguraatiot

Kytkinkonfiguraatioiden osalta merkittävin protokolla työn kannalta on EAPS, joten käyn seuraavaksi läpi, miten EAPS-rinki pystytetään. Tässä esimerkissä tehdään rinki, jossa on kaksi EAPS-domainia, jotka kiertävät rengastopologiassa eri suuntiin. Kytkimet sijaitsevat eri verkon yhdyspisteillä eli POP:ssa (point of presence). Jokainen rengastopologian kytkin on kahden tai useamman kytkimen pino eli stack. Koska kyseessä on kytkinpino, kannattaa runkoyhteydet kytkeä eri kytkimiin, jotta yhden laitteen vikaantuminen ei aiheuta koko keskuksen pimenemistä. Suunnitteluvaiheessa käytännössä tarvitsee vain päättää, mitkä kytkinvälit ovat estettynä kussakin domainissa. Kuva 10 esittää esimerkin kytkinrinkiä, josta näkyy, miten liikenteen on päätetty kulkevan r1- ja r2-domainessa.



Kuva 10. Rengastopologiassa on 7 kytkintä ja kaksi EAPS-domainia.

Aloittaessa EAPS-protokollan konfigurointia pitää jonkin kytkinväleistä olla katkaistuna. Tämän jälkeen voidaan turvallisesti poistaa mahdolliset vanhat varmistukseen käytetyt protokollat. Sw1 toimii r1-domainin master-kytkimenä, ja sw2 taas toimii r2-domainin master-kytkimenä. R1-domainiin halutaan estää kytkimien sw7 ja sw1 väli – tällöin kytkimen sw1 toissijaiseksi portiksi asetetaan portti 1:25. R2-domainin estetty väli on kytkinten sw2 ja sw3 välinen yhteys. Tällainen asetelma saadaan tehtyä konfiguraatiolla.

sw1 – sw7:

```
create vlan r1_ctrl tag 51
configure vlan r1_ctrl add ports 1:25,2:25 tagged
create vlan r2_ctrl tag 52
configure vlan r2_ctrl add ports 1:25,2:25 tagged
```

Jokainen EAPS-domain tarvitsee control-VLANin, joka ohjaa EAPS:n toimintaa ja välittää EAPS-viestit laitteiden välillä. EAPS:n konfigurointi on hyvä aloittaa luomalla kaikkiin kytkimiin control-VLANit ja lisätä ne runkoportteihin. Tässä tapauksessa luodaan VLANit r1_ctrl ja r1_ctrl, ja lisätään se portteihin 1:25 ja 2:25 tagged-tilassa eli standardin 802.1Q mukaisesti.

sw1:

```
create eaps r1
configure eaps r1 mode master
configure eaps r1 primary port 1:25
configure eaps r1 secondary port 2:25
configure eaps r1 add control vlan r1_ctrl
create eaps r2
configure eaps r2 mode transit
configure eaps r2 primary port 2:25
configure eaps r2 secondary port 1:25
configure eaps r2 add control vlan r2_ctrl
```

Itse EAPS:n konfigurointi aloitetaan luomalla domain ja nimeämällä se. Kun r1-domain on luotu, asetetaan domain joko master- tai transit-tilaan. Sw1-kytkin asetetaan r1-domainille master-tilaan. Seuraavaksi päätetään liikenteen kiertosuunta – sw1:ltä halutaan r1-domainin liikennettä ajaa oletuksena sw2:lle päin, joten 1:25-portti asetetaan ensisijaiseksi ja 2:25 toissijaiseksi. Koska on kyseessä domainin master-kytkin, liikenne on estettynä porttiin 2:25. Lopuksi asetetaan domainille aiemmin luotu control-VLAN. Toinen domain konfiguroidaan samaan tyyliin, mutta Sw1-kytkin asetetaan transit-tilaan, kiertosuunta vaihdetaan ja ensi- ja toissijaiset portit asetetaan toisin päin.

sw2:

```
create eaps r1
configure eaps r1 mode transit
configure eaps r1 primary port 1:25
configure eaps r1 secondary port 2:25
configure eaps r1 add control vlan r1_ctrl
create eaps r2
configure eaps r2 mode master
configure eaps r2 primary port 2:25
configure eaps r2 secondary port 1:25
configure eaps r2 add control vlan r2_ctrl
```

Sw2-kytkin konfiguroidaan samaan tyyliin kuin sw1-kytkin, mutta r2-domainin liikenne halutaan estää sw2:n ja sw3:n välistä. Tällöin kytkimen domain-tilaksi asetetaan master. Sw1-kytkin on jo r1-domainin master-kytkin, joten sen tilaksi asetetaan transit.

sw3 - sw7

```
create eaps r1
configure eaps r1 mode transit
configure eaps r1 primary port 1:25
configure eaps r1 secondary port 2:25
configure eaps r1 add control vlan r1_ctrl
create eaps r2
configure eaps r2 mode transit
configure eaps r2 primary port 2:25
configure eaps r2 secondary port 1:25
configure eaps r2 add control vlan r2_ctrl
```

Lopuille ringin kytkimille voidaan konfiguroida samanlaiset komennot, koska esimerkin kaikissa kytkinpinoissa on samat runkoportit. Kun EAPS:n konfiguraatiot on tehty kaikkiin rengastopologian laitteisiin, voidaan aloittaa rengastopologiassa kulkevien VLANien lisääminen. VLANeita lisättäessä pitää päättää, kumpaan domainiin VLAN halutaan lisätä. Tähän vaikuttavat enimmäkseen VLANin käyttökohteet – ideaalitilassa liikenne kulkee lyhyintä reittiä kohteeseen eikä kuormita verkkoa turhaan. VLANeita kannattaa kuitenkin lisätä tasaisesti molempiin rinkeihin, jotta verkon kuormitus saadaan

tasaiseksi. VLANien lisääminen onnistuu seuraavanlaisella komennolla, jossa VLAN testi_vlan lisätään EAPS-domainin r1 suojeluun.

```
configure eaps r1 add protected vlan testi_vlan
```

VLANeja lisättäessä EAPS:n suojeluun on varmistettava, että ne on lisätty myös jokaiseen EAPS-runkoporttiin. Uusia VLANeja luotaessa kannattaa VLAN lisätä ensin EAPS:n suojeluun ja vasta sen jälkeen portteihin, ettei aiheuta vahingossa silmukkaa eli loopia verkkoon. Kun EAPS on konfiguroitu ja VLANit lisätty, voidaan EAPS ottaa käyttöön enable-komennoilla.

```
enable eaps
enable eaps r1
enable eaps r2
```

Kun EAPS on käytössä, mutta yksi rengastopologian linkeistä on vielä sammutettuna, EAPS on master-kytkimillä Fail-tilassa, joka voidaan todeta sho eaps -komennolla. Kun on varmistettu, että EAPS on käynnissä jokaisella laitteella, voidaan avata rengastopologian sammutettu portti. Tämän jälkeen sho eaps -komennolla nähdään alla olevan kaltaiset tiedot. Rengastopologian ollessa ehjä, master-kytkin on Complete-tilassa ja transit-kytkimet ovat Links-Up-tilassa. Jos jonkun transit-kytkimen linkki putoaa, sen tilaksi muuttuu Links-Down. Tästä lähetetään viesti master-kytkimelle, joka avaa liikenteen kulkemaan toista kautta.

```
sw1 # sho eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: Off
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP and MLD Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 2
# EAPS domain configuration :
-------------------------------------------------------------------------------
Domain         State           Mo  En  Pri    Sec    Control-Vlan VID   Count Prio
-------------------------------------------------------------------------------
r1             Complete        M   Y   1:25   2:25   r1_ctrl      (51  ) 11    N
r2             Links-Up        T   Y   2:25   1:25   r2_ctrl      (52  ) 15    N
-------------------------------------------------------------------------------
```

8 Yhteenveto

Tässä luvussa arvioin verkon päivitysprojektin onnistuneisuutta. Esittelen työvaiheiden sujuvuutta ja pohdin, mitä olisi kenties kannattanut tehdä toisin. Kerron myös lyhyesti verkon testauksesta ja siitä, millaisen pohjan tehty päivitys luo tuleville verkon päivitysprojekteille. Lopuksi arvioin työn sopivuutta opinnäytetyön aiheena.

Verkon päivitysprojekti onnistui odotetulla tavalla. Verkko suunniteltiin huolellisesti, joten varsinaista päivitys- ja konfiguraatiotyötä oli helppo lähteä toteuttamaan. Kytkinten ja reitittimien konfigurointi sujui pääasiassa hyvin – ainoastaan kytkinverkon muutosten toteuttaminen hallitusti huoltokatkojen aikana aiheutti hieman haasteita. Testauksessa verkko todettiin toimivaksi ja vikasietoiseksi. EAPS-protokollan todettiin toimivan erittäin tehokkaasti – linkin katkosta oli hankala todentaa, sillä katkosten kesto oli vain millisekuntien luokkaa. BGP-protokollan vikatilannetestauksissa todettiin liikenteen kääntyvän oikein toimiville BGP-yhteyksille noin 30 sekunnissa.

Kaiken kaikkiaan verkon päivitysprojekti oli onnistunut. Saavutimme ennalta asetetut tavoitteet, joita olivat toimivan vikasietoisen verkon luominen ja kapasiteetin lisääminen. Käyttämiemme Summit X670 -kytkinten ansiosta voimme toteuttaa myös kiinteistöyhteyksiä 10 Gbps linkeillä ja tarjota asiakkaille yli 1 Gbps yhteyksiä. Tehty päivitys luo myös hyvän pohjan mahdollisille tuleville päivitysprojekteille – kyseisissä X670-kytkimissä on 40 Gb:n runkolinkit, joiden avulla runkoverkkoa on mahdollisuus päivittää myöhemmin. Jos olisin ryhtymässä päivitysprojektiin uudelleen, voisin harkita uudelleen valintaa EAPS- ja ERPS-protokollien välillä. Tulevaisuudessa vaihtaminen avoimeen ERPS-protokollaan voisi olla järkevää, sillä EAPS-protokollan shared-port-ominaisuus vaatii kytkimille Core-lisenssit.

Opinnäytetyön aiheena verkon päivitysprojekti oli sopivan haastava ja monipuolinen. Projektissa pystyin soveltamaan opinnoissa hankkimiani taitoja ja syventämään tietämystäni projektissa käyttämistäni tekniikoista.

Lähteet

1 Historian havinaa. Verkkoaineisto. Finnet-liitto ry. <https://www.finnet.fi/tarina/>. Luettu 21.7.2017.

2 Puhelinyhtiöiden historia. 2008. Verkkoaineisto. Osakekerho Oy. <http://www.puhelinosake.com/historia.html>. Luettu 21.7.2017.

3 Tietoa Elisasta - Historia. 2017. Verkkoaineisto. Elisa Oyj. <http://corporate.elisa.fi/tietoa-elisasta/historia/>. Luettu 21.7.2017.

4 Matkaviestinoperaattorista tietoliikennekonserniksi. Verkkoaineisto. DNA. <https://corporate.dna.fi/dna-lyhyesti#historia>. Luettu 21.7.2017.

5 What are Provider Aggregatable (PA) addresses and Provider Independent (PI) addresses? Verkkoaineisto. RIPE NCC. < https://www.ripe.net/participate/member-support/copy_of_faqs/isp-related-questions/pa-pi>. Luettu 23.7.2017.

6 Laskutus tietoverkoissa. 2000. Verkkoaineisto. Teknillinen korkeakoulu. < https://www.netlab.tkk.fi/opetus/s38118/s00/tyot/51/2.htm >. Luettu 29.7.2017.

7 MiaK. Vaatimaton panokseni Wikipedian kuvagalleriaan. Verkkoaineisto. < https://fi.wikipedia.org/wiki/K%C3%A4ytt%C3%A4j%C3%A4:MiaK~fiwiki/Kuvat >. Luettu 29.7.2017.

8 Matthew Glidden. 2001. How to become a network guru. Verkkoaineisto. ATPM, Inc. < http://www.atpm.com/7.10/networking-1.shtml >. Luettu 29.7.2017.

9 Thayumanavan Sridhar. Layer 2 and Layer 3 Switch Evolution. Verkkoaineisto. < https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-19/switch-evolution.html>. Luettu 29.7.2017.

10 Internetin lyhyt historia. 2000. Verkkoaineisto. MTV Oy. < https://www.mtv.fi/lifestyle/digi/artikkeli/internetin-lyhyt-historia/1790878#gs.woi2Bt0>. Luettu 29.7.2017.

11 Charles E. Spurgeon. Ethernet: The Definitive Guide. Verkkoaineisto. < https://www.safaribooksonline.com/library/view/ethernet-the-definitive/1565926609/ch01.html>. Luettu 30.7.2017.

12 Margaret Rouse. OSI reference model. Verkkoaineisto. TechTarget. <http://searchnetworking.techtarget.com/definition/OSI>. Luettu 7.8.2017.

13 Are you a starter in Networking: OSI model. 2017. Verkkoaineisto. TTL BITS. < http://www.ttlbits.com/2017/02/are-you-starter-in-networking-osi-model.html>. Luettu 7.8.2017.

14 Sarjamuotoinen siirto. Verkkoaineisto. < http://ladu.htk.tlu.ee/erika/lasse/communication/sarjamuotoinen_siirto.html >. Luettu 12.8.2017.

15 Lou Frenzel. 2013. What's The Difference Between The OSI Seven-Layer Network Model And TCP/IP? Verkkoaineisto. <http://www.electronic-design.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip>. Luettu 12.8.2017.

16 Try Subnetting and NAT (TCP/IP) Part 1. Verkkoaineisto. what-when-how. <http://what-when-how.com/tcpip/need-more-addresses-try-subnetting-and-nat-tcpip-part-1/>. Luettu 22.8.2017.

17 FAQ: IPv6. 2016. Verkkoaineisto. RIPE NCC. <https://www.ripe.net/manage-ips-and-asns/resource-management/faq/faq-ipv6>. Luettu 22.8.2017.

18 IPv6-Adressen. Verkkoaineisto. Elektronik-Kompendium. <https://www.elektronik-kompendium.de/sites/net/1902111.htm>. Luettu 22.8.2017.

19 Aqeel Haider. 2010. IGP and EGP / Link state and distance vector. Verkkoaineisto. < http://basicitnetworking.blogspot.fi/2010/03/igp-and-egp-link-state-and-distance.html>. Luettu 11.9.2017.

20 Ivan Pepelnjak. BGP tutorial: The routing protocol that makes the Internet work. Verkkoaineisto. TechTarget. <http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work>. Luettu 11.9.2017.

21 Margaret Rouse. OSPF (Open Shortest Path First). Verkkoaineisto. TechTarget. < http://searchenterprisewan.techtarget.com/definition/OSPF>. Luettu 15.9.2017.

22 OSPF Design Guide. 2005. Verkkoaineisto. Cisco. <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>. Luettu 15.9.2017.

23 Layer 2 Protocols. 2014. Verkkoaineisto. Extreme Networks, Inc. < http://extrcdn.extremenetworks.com/wp-content/uploads/2014/04/Layer_2_Protocols.pdf>.

24 Goralski, Walter; Gadecki, Cathy; Bushong, Michael. 2011. Junos OS for dummies, 2nd Edition. Indianapolis, Indiana: Wiley Publishing, Inc.

25 Juniper Junos OS Support Services. Verkkoaineisto. Progent Corporation. < http://www.progent.com/juniper-junos-consultants.htm>. Luettu 12.10.2017.

26 What is a Local Internet Registry (LIR)? 2016. Verkkoaineisto. RIPE NCC. < https://www.ripe.net/manage-ips-and-asns/resource-management/faq/independent-resources/phase-three/what-is-a-local-internet-registry-lir>. Luettu 11.11.2017.