Jupiter Vuorikoski

# MetroIX Internet Exchange, suunnittelu ja toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

28.4.2015

Metropolia

**Alkulause**

Tämä insinöörityö tehtiin Metropolian tietoverkkolaboratoriolle. Harvoin kukaan pääsee tekemään täysin uutta kokonaista infrastruktuuria aamenesta, joten tämä onkin ollut ainutlaatuinen tilaisuus päästä toteuttamaan itseään. Suurkiitos ohjaajalleni Marko Uusitalolle joka hoiti suurimman osan byrokratiasta IP-osoitteisiin liittyen ja toimi tukena työn eri vaiheissa. Kiitos myös Thomas Willbergille S1-Networks Oy:ssä yhteistyöstä ja hinnoittelusta transit-kuidun ja linkin kanssa. Kiitän lisäksi Toni Anttilaa ja Henrik Lepistöä jotka olivat mukana tekemässä MetroIX:n prototyyppiä syksyllä 2014. Kiitos Jussi Alhorinteelle työn kielitarkastuksesta.

Erityiskiitos perheelleni joka on tukenut ja rakastanut minua opintojeni aikana enemmän kuin todennäköisesti koskaan tulen tietämään.

Helsingissä 29.4.2015.

Jupiter Vuorikoski

| | |
|---|---|
| Tekijä(t)<br>Otsikko<br><br>Sivumäärä<br>Aika | Jupiter Vuorikoski<br>MetroIX Internet Exchange, suunnittelu ja toteutus<br><br>20 sivua + 1 liitettä<br>28.4.2015 |
| Tutkinto | Insinööri (AMK) |
| Koulutusohjelma | Tietotekniikka |
| Suuntautumisvaihtoehto | Tietoverkot |
| Ohjaaja(t) | Lehtori Marko Uusitalo |


IXP eli Internet Exchange Point on kolmannen osapuolen ylläpitämä verkkoliikenteen yhdyspiste, jonka kautta operaattorit ja muut toimijat pystyvät vaihtamaan liikennettä keskenään. Etuna IXP:ssä on se, että riittää kun toimija rakentaa yhden fyysisen yhteyden IXP:n, jonka kautta hän pystyy vaihtamaan liikennettä jokaisen tai valitsemiensa toimijoiden kanssa, jotka ovat liittyneenä samaan IXP:n.

Tämän insinöörityön tavoitteena oli rakentaa Metropolia Ammattikorkeakoulun verkkolaboratorion käyttöön oma IXP-mallinen yhdysliikennepisteratkaisu, johon uudenlaiset verkkolaboratorion testi- ja opetusympäristöt tulevaisuudessa liitettäisiin sekä kirjoittaa dokumentaatio ja liittymis- ja liikennepolitiikkadokumentit IXP:n käyttöön

Työ on hyvin käytännönläheinen, ja siihen sisältyi paljon testausta erilaisilla konfiguraatioilla ja lähestymistavoilla. Lopullinen ratkaisu päätyi olemaan hyvin samankaltainen kuin FICIX:n toteutus Suomessa.

IXP-infrastruktuuri saatiin loppujen lopuksi toimimaan halutulla tavalla, ja sen suorituskyky ja vikasietoisuus saatiin riittävälle tasolle, jotta sitä voidaan käyttää opetustarkoituksissa tulevissa laboratorio- ja testiympäristöissä.



| | |
|---|---|
| Avainsanat | IXP, BGP, RIPE, Reititys, Kytkinverkot |

| | |
|---|---|
| Author(s)<br>Title<br><br>Number of Pages<br>Date | Jupiter Vuorikoski<br>MetroIX Internet Exchange planning and implementation<br><br>20 pages + 1 appendice<br>28 April 2015 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information and Communications Technology |
| Specialisation option | Information networks |
| Instructor(s) | Senior Lecturer Marko Uusitalo |

An IXP, abbreviation for Internet Exchange Point, is a 3rd party maintained traffic exchange point, through which ISPs and other operators on the Internet can exchange traffic with each other. The advantage of IXPs over building dedicated links is that just by building or buying a link to an IXP you can exchange traffic with many or even all parties connected to IXP simultaneously.

The goal of this work was to build a private IXP for the Metropolia University of Applied Sciences networking faculty to facilitate the connection of future testing- and teaching-environments of the faculty. The goal was also to create documentation for the new net-work and routing infrastructure and create policy documents for connecting to the IXP and how traffic is routed in the infrastructure.

The work is very much oriented towards practical implementation and involved a lot of testing with different configurations and approaches to how the infrastructure could be deployed. The resulting configuration is coincidentally not much unlike what FICIX had implemented in their environment.

The IXP-infrastructure was eventually made to operate in a desired fashion, and its performance and redundancy is on a sufficient level for use in a new generation of laboratory- and teaching environments.

| | |
|---|---|
| Keywords | IXP, BGP, RIPE, Reititys, Kytkinverkot |

## Sisällys

## Lyhenteet

| | |
|---|---|
| ARP | Address Resolution Protocol. Protokolla jolla IP-osoite yhdistetään MAC-osoitteeseen. |
| ASIC | Application Specific Integrated Circuit. Tiettyyn käyttötarkoitukseen suunniteltu piiri. |
| AS | Autonomous System. Internetissä itsenäisesti toimiva verkko ja sen tunniste. |
| BGP | Border Gateway Protocol. Reititysprotokolla joka vastaa Internetin toiminnasta. |
| ECMP | Equal Cost Multi-Pathing. Samanarvoisten reittien reititys useampaa linkkiä pitkin. |
| GPRS | General Packet Radio Service. 2g- ja 3g-GSM-verkkojen pakettidatapalvelu. |
| GRX | GPRS Roaming Exchange. Protokolla jolla roaming puhe- ja laskutusdata 2g-verkoissa voidaan reitittää toisen operaattorin verkosta alkuperäisverkkoon |
| IP | Internet Protocol. Internet Protokolla joka mahdollistaa laitteille oman osoitteen Internetissä IP-pohjaiseen kommunikointiin. |
| IPv4 | Internet Protocol version 4. Internet-protokollan versio 4, jossa osoiteavaruus on 32-bittinen. |
| IPv6 | Internet Protocol version 6. Internet-protokollan versio 6, jossa osoiteavaruus on 128-bittinen. |
| ISP | Internet Service Provider. Internet-palveluntarjoaja. |

| | |
|---|---|
| IXP | Internet Exchange Point. Yhdysliikennepiste johon organisaatiot voivat liittyä. |
| LACP | Link Aggregation Control Protocol. Useamman linkin loogisesti yhdeksi linkiksi yhdistämiseen käytetty protokolla. |
| LAN | Local Area Network. Lähiverkko. |
| LIR | Local Internet Registry. Paikallinen Internet-osoitteiden hallintataho. |
| MPLS | Multiprotocol Label Switching. Tekniikka jolla paketit kytketään ison reititysinfrastruktuurin yli. |
| MAC-osoite | Media Access Control-osoite. Verkkoportin fyysinen osoite mediassa. |
| OSI | Open Systems Interconnect. Malli kerrostetulle verkkorakenteelle. |
| OSPF | Open Shortest Path First. Reititysprotokolla jota yleisesti käytetään organisaation sisäisen verkon reitityksessä. |
| VLAN | Virtual Local Area Network. Virtuaalinen lähiverkko joka sallii kytkimen ja kytkin-infrastruktuurin pilkkomisen useampaan loogiseen osaan. |
| VPLS | Virtual Private LAN Service. MPLS:n avulla toteutettu virtuaalinen Ethernet palvelu. |
| VRF | Virtual Routing and Forwarding. Looginen eristetty reititysavaruus. |
| PI | Provider Independent. Toimijariippumaton osoiteavaruus |
| RIPE | Réseaux IP Européens. Organisaatio joka vastaa IP-osoitteiden hallinnasta Euroopassa. |
| SPOF | Single Point Of Failure. Yksittäinen objekti järjestelmässä joka voi aiheuttaa koko järjestelmän vikaantumisen. |
| UPS | Uninterruptible Power Supply. Akkuvarmenteinen virtalähde. |

# 1 Johdanto

Internet-solmupisteet (IXP) ovat kriittisessä asemassa ympäri maailmaa Internetin toimivuuden kannalta. [1.] Liittyminen IXP:n on kustannustehokas tapa siirtää liikennettä Internet-palveluntarjoajien (ISP), sekä muiden toimijoiden kesken. Esimerkiksi Suomessa suurin IXP-toimija on FICIX, jonka kautta suuri osa Suomessa toimivista operaattoreista ja isoista toimijoista vaihtaa liikenteensä keskenään.

Metropolia Ammattikorkeakoulun tietoverkkolaboratorion käyttöön saatiin syksyllä 2014 nykyään harvinaisia operaattoririippumattomia IPv4 PI-osoitteita, jotka mahdollistavat laboratoriolle julkiseen internetiin päin näkyviä, täysin laboratorion hallinnassa olevien palveluiden kehittämisen. PI-osoitteet ovat julkisia Internet-protokollan osoitteita, joiden reitittyminen ja sisäinen käyttö ovat täysin toimijan omassa hallinnassa ja jotka voidaan siirtää reititettäväksi myöhemmin toisen tai useampien toimijoiden kautta, olematta sidottuja linkin toimittajaan. Tietoverkkolaboratorio on jo pitkään halunnut kehittää erityisesti operaattoritason verkkoratkaisuiden opetusta, ja MetroIX-projekti on osa tätä kehitystyötä.

Tämän insinöörityön päämääränä oli rakentaa uusi tietohallinnosta riippumaton verkko-infrastruktuuri, jonka kautta tätä osoite-avaruutta voidaan hyödyntää uusissa laboratorio- sekä testiympäristöissä. Tavoitteena oli myös visioida, miten ympäristöjä ja infra-struktuuria voidaan tulevaisuudessa laajentaa.

# 2 Tausta

## 2.1 Mikä on IXP?

IXP, eli yhdysliikennepiste, on hyvin yksinkertaisesti paikka, johon organisaatiot rakentavat fyysisen liityntäyhteyden (nykyään yleisimmin valokuidulla), joka liitetään jollakin tuetulla liitintavalla IXP-organisaation ylläpitämään infrastruktuuriin. IXP toimii yleensä jossakin datakeskustilassa, joka on joko jaettu muiden toimijoiden kanssa, tai suurempien IXP:n tapauksessa dedikoitu IXP:n käyttöön. Suurimmat IXP-organisaatiot toimivat usealla eri mantereella ja useassa IXP tilassa. [2.] IXP-organisaation vastuulla

on ylläpitää liityntään tarvittava kytkin-infrastruktuuri, sähkömagneettisen säteilyn suojaus, sähkön-syöttö sekä konfiguraatiot.

Aikaisemmin IXP:t olivat käytössä lähinnä Internet-palveluntarjoajien välisen liikenteen maksuttomaan vaihtoon, mutta Internetin kehittyessä niiden rooli on muuttunut yksinomaan operaattorien välisen liikenteen välittämisestä yleiseksi organisaatioiden väliseksi solmukohdaksi, jonka jäsenten väliseen liikenteeseen ja sopimuksiin IXP-organisaatio ei itse ota kantaa.

## 2.2 IXP:n historia

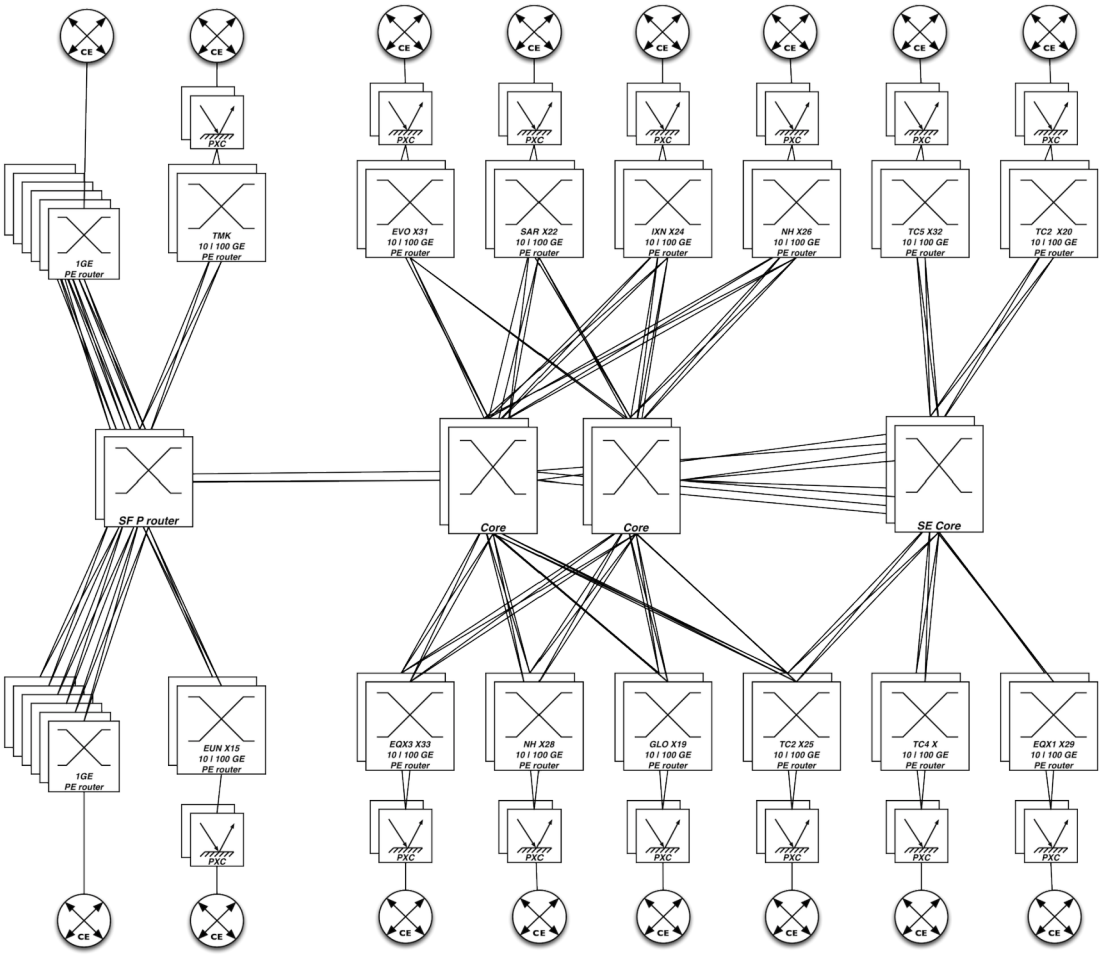
Ensimmäinen IXP:n kaltainen organisaatio oli CIX, eli Commercial Internet eXchange. Tämä perustettiin vuonna 1991, jotta operaattorit saisivat siirtää kuluvapaasti kaupallista liikennettä keskenään vanhojen puhelinten minuutti- ja määrälaskutus periaatteiden si-jaan. Tämä oli aikanaan ennenkuulumaton periaate datan ja liikenteensiirron kannalta, mutta oli nykyisen vapaan Internetin periaatteiden kulmakiviä. Ennen CIX:a USA:n hallitus oli tiukasti säännöstellyt minkälaista liikennettä silloisen Internetin ja infrastruktuurin kautta sai kulkea. CIX tarjosi kaupallisille operaattoreille kanavan siirtää liikennettä keskenään.

NAP eli Network Access Point oli konsepti, joka syntyi CIX:n jälkeen ja nopeasti kehittyi nykyiseksi IXP:n toimintamalliksi. NAP oli konseptiltaan hyvin samanlainen moderneihin IXP:n nähden mutta salli ainoastaan operaattoreiden liittyä itseensä.

## 2.3 Miten IXP toimii?

Yksinkertaisimmillaan IXP:n verkkotopologia on nykyään litteä ethernet-verkko yhdellä kytkimellä. Tämä tosin skaalautuu huonosti, ja on vaikea hallita suuremmassa mittakaavassa. Liittyvät tahot kytketään ns. peering fabriciin, joka on yllämainittu ethernet-verkko [3.], reititetyllä portilla, jonka jälkeen tämän portin yli on mahdollista yhdistää jokaiseen toiseen liittyneeseen tahoon. Suuremmat IXP:t käyttävät MPLS-teknologiaa virtuaalisen peerausfabricin määrittelyyn ja hallitakseen helpommin, kuinka liikenne IXP:n infrastruktuurissa kulkee. [4.] MPLS eli Multi-Protocol Label-switching on

teknologia, jossa IP-tason reititysinformaation avulla päätepisteet muodostavat kytkentäisiä reittejä eri protokollille suuren reititetyn infrastruktuurin lävitse.




Kuva 1. AMS-IX:n MPLS verkon konseptikuva

## 2.4 IXP-infrastruktuurin haasteet

IXP:n kannalta haasteellista on litteän ethernet-topologian (joko fyysisen, virtuaalisen tai MPLS:n kautta toteutetun) levittäminen suurelle määrälle liittyviä laitteita. Liittyvän tahon laite tai portti saattaa vikaantua ja lähettää suuren määrän broadcast-paketteja, laitteistossa saattaa olla ohjelmistovirhe, joka aiheuttaa kehysten lähettämisen vääristä porteista, tai vastaavia ongelmia. Tuhansien laitteiden liittyessä myös validit lähetykset kuten ARP-broadcastit ja esim. reitittimien multicast router solicitation -viestit voivat aiheuttaa huomattavan määrän liikennettä, joka äärimmäisissä tapauksissa voi haukata huomattavan määrän hitaampien porttien kaistasta.

## 2.5 Esimerkki-IXP: FICIX

Työtä varten haastateltiin FICIX:n hallituksen jäsentä Jorma Melliniä, jotta työn tekijälle valottuisi hieman, miten oikea toimiva IXP-infrastruktuuri on rakennettu ja millä periaatteilla kyseinen infrastruktuuri toimii. Haastattelu tehtiin sen jälkeen kun työn varsinainen työ-osuus oli jo saatettu päätökseen. Haastattelun yhteydessä ilmeni, että perusperiaatteiden osalta työn varsinaisen toteutus oli hyvin pitkälti samoilla jäljillä kuin miten FICIX:n ympäristössä asiat on toteutettu.

FICIX toimii kolmessa eri IXP-tilassa: Helsingin Pasilassa, Espoon Otaniemessä ja Oulussa. Näitä tiloja ei ole liitetty topologioiltaan toistaiseksi toisiinsa, vaan jokainen piste on itsenäinen. [5.] Tämänhetkinen toteutus toimii neljän IXP:n jäsenien käytössä olevan VLAN:n pohjalta. VLAN:lla eli Virtual Local Area Network -teknologialla voidaan loogisesti erotella kytkinportteja kuulumaan useaan ethernet-segmenttiin. Yksi VLAN on tarkoitettu IPv4- ja IPv6-liikenteelle, toinen pelkästään IPv6-liikenteelle (Tämä kuitenkin on poistumassa ja on paikallaan lähinnä historiallisista syistä, ja kaikki IP-pohjainen liikenne on tarkoitus kulkea tulevaisuudessa yhden ethernet-segmentin kautta), kolmas on tar-koitettu multicast-reititykselle ja neljäs operaattorien GRX-protokollan liikenteelle. GRX-protokollaa käytetään reitittämään GPRS-puhelut ja data tele-operaattoreiden välillä roaming-asiakkaita varten.

Mellin kertoi haastattelussa, että FICIX:n tavoitteena on liittää Pasilan ja Otaniemen pisteet toisiinsa, jotta kummassa tahansa pisteessä olevat jäsenet voisivat vaihtaa liikennettä keskenään helpommin. Tämän liitoksen tekeminen pelkästään Layer2-tekniikoilla olisi erittäin vaikeaa ja liikenteen hallinta lähestulkoon mahdotonta suuremmassa skaalassa ja suuremmilla porttinopeuksilla. Layer2 viittaa tässä OSI-mallin, joka on malli kerrostetulle verkkorakenteelle protokollien standardin toimivuuden ja modulaarisuuden takaamiseksi toiseen kerrokseen, johon esim ethernet-teknologia on määritelty kuuluvaksi. FICIX onkin siirtymässä MPLS-tekniikkaan toteutuksessaan muutaman vuoden sisällä. Tämänhetkinen porttien vikasietoisuus on toteutettu erinäisillä porttitason tietoturvatekniikoilla, joihin kuuluu mm. se, että liittyvän laitteen MAC-osoite on sidottu staattisesti porttiin ja tuntematon unicast-, tuntematon multicast- sekä broadcast-liikenne on rajoitettu hyvin pieneen pakettimäärään. MPLS-arkkitehtuurissa tätä on hieman helpompi hallita, mutta samat periaatteet tulevat pätemään.

### 2.6 MetroIX-konsepti ja valmistelut

Metropolian organisaatiomuutoksen jälkeen pilvi- ja verkkopalveluiden osaamisalueen opetushenkilökunta totesi, että laboratorio tarvitsee uudenlaisia opetusympäristöjä tulevaisuuden verkkotekniikan opetusta varten. Tietohallinto pystyy toimittamaan perustavanlaatuiset IT-palvelut sekä käyttötuen, mutta tämä ei tule jatkossa riittämään laboratorion tarpeisiin vaste-ajan eikä teknisten toteutusten osalta. Tämän vuoksi laboratorion käyttöön alettiin suunnittelemaan omaa tietohallinnosta irrallaan olevaa infrastruktuuria uusien opetusympäristöjen käyttöön.

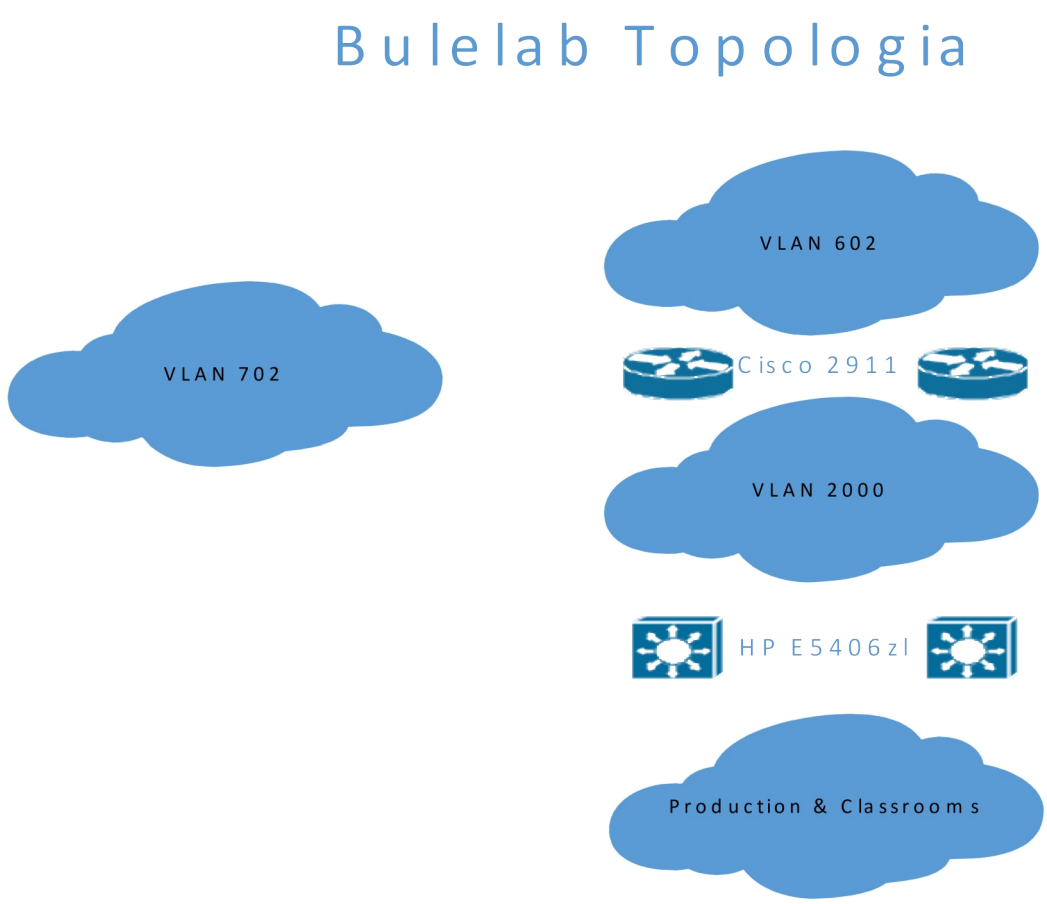
Lehtori Marko Uusitalo on joskus 90-luvulla rekisteröinyt Helsingin teknillisen oppilaitoksen käyttöön IPv4 PI -osoiteblokin, joka mahdollistaa laboratoriolle oman palveluntarjoajariippumattoman Internet-reitityksen. Tämä osoiteblokki on tarkoitus ottaa uudelleen käyttöön.

Tietohallinto tarjoaa Bulevardin ja Leppävaaran kampusten välille 2 kpl 1Gb:n linkkejä Metropolian oman kuituinfrastruktuurin yli. Näitä linkkejä on käytetty aikaisemmin MPLS-teknologian testaukseen, mutta ne olivat olleet käyttämättöminä joitain vuosia. Keväällä 2014, kun MetroIX-konseptia ensimmäisen kerran pohdittiin, ilmeni, että linkkien kuiduissa oli suuri määrä vaimennusta. Kyseisten linkkien päät tutkittiin kuitumikroskoopilla ja huomattiin, että häntäkuitujen liittimien päät olivat yksinkertaisesti erittäin likaiset. Kuitujen päät puhdistettiin isopropyylialkoholilla, jonka jälkeen linkit toimivat moitteetta.

## 3 Prototyyppi

### 3.1 Laboratorion reititys

Syksyllä 2014 tulevasta MetroIX-infrastruktuurista tehtiin prototyyppi. Tällä hetkellä Bulevardin laboratorion verkko reitittyy Ciscon kahden 2911-reitittimen kautta, joiden suorituskyky on noin 230-250 Mbps luokkaa. [6.] Tietohallinto tarjoaisi ainakin gigabitin luokkaa olevan linkin, joten näiden laitteiden suorituskyky on tällä hetkellä pullonkaulana.




Kuva 2. Tämänhetkinen reitityskuvio Bulevardin verkkolaboratoriossa

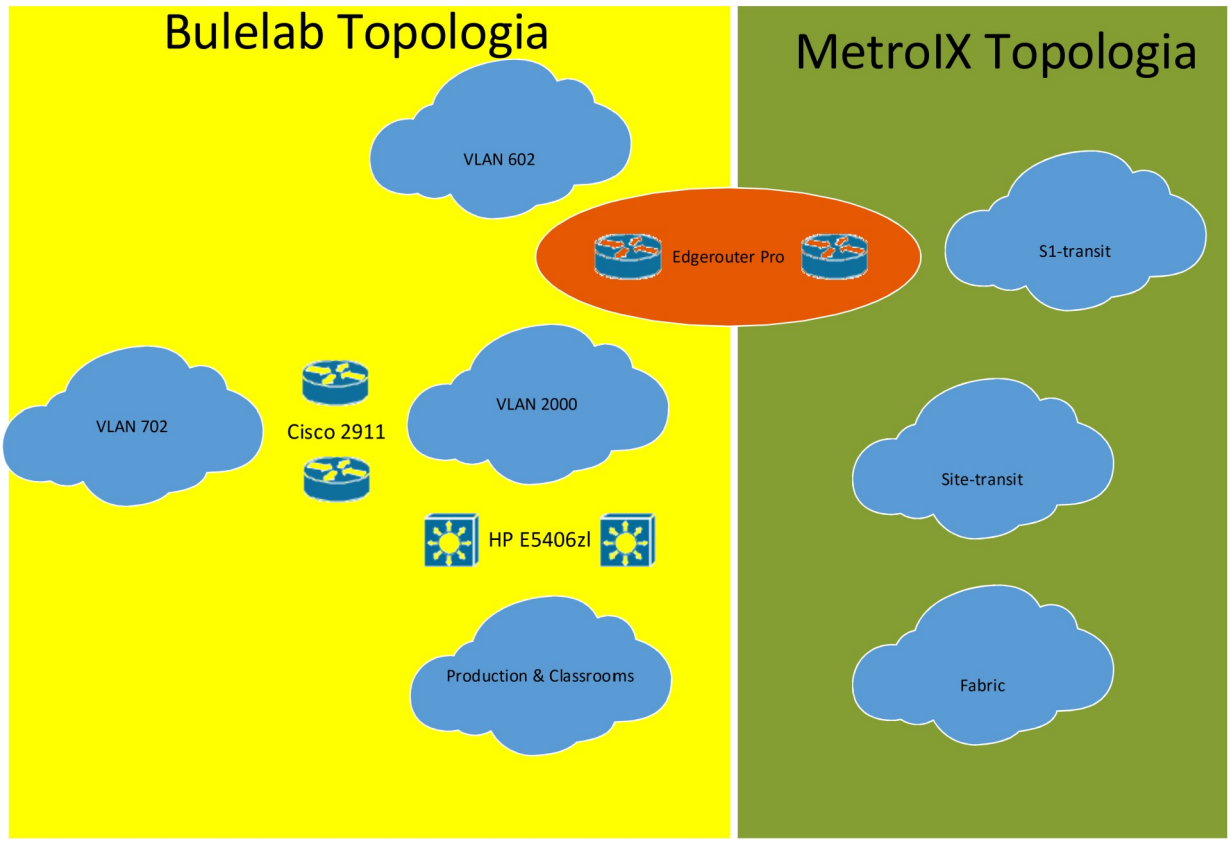
Kuvassa 2 on esitetty, miten reititys toimii laboratorion ympäristössä tällä hetkellä. Cisco 2911-laitteet ovat runkolinkin VLAN2000 ja tietohallinnon tarjoaman VLAN602:n välissä laboratorion reunareitittiminä. Lisäksi ne reitittävät VLAN702:n, jossa suurin osa laboratoriotöistä tehdään. VLAN:ssa 702 on tarkka suodatus sen suhteen, miten sen takaa pystyy reitittymään liikennettä. Suunnitelma oli korvata vlanien 2000 ja 602 välinen reititys EdgeRouter Pro -laitteilla niin, että ne hoitaisivat myös MetroIX:n reitityksen.

## 3.2 Prototyypin toteutus

Ensimmäinen ajatus oli toteuttaa eristys ns. policy-based -reitityksellä. Tässä ideana oli reitittää kaikki liikenne, joka tulee osoiteavaruudesta 10.95.0.0/16, joka on tietohallinnon toimesta annettu Bulevardin tietoverkkolaboratoriolle, reitittyväksi Internetiin päin vlanin 602 läpi, ja MetroIX:n osoiteavaruuden reitittyväksi S1-

Networksin transit-linkin läpi. Tämä todettiin kuitenkin kestämättömäksi, koska EdgeRouter -laitteiden ohjelmisto sallii vain staattisen reitityksen tällä tavalla.

Seuraava idea oli eriyttää verkkolaboratorion ja MetroIX:n reititys omiksi VRF-instansseikseen. VRF, eli Virtual Routing and Forwarding, on tekniikka, joka mahdollistaa reitittimessä useamman erillisen reititystaulun pitämisen samanaikaisesti. [7.]

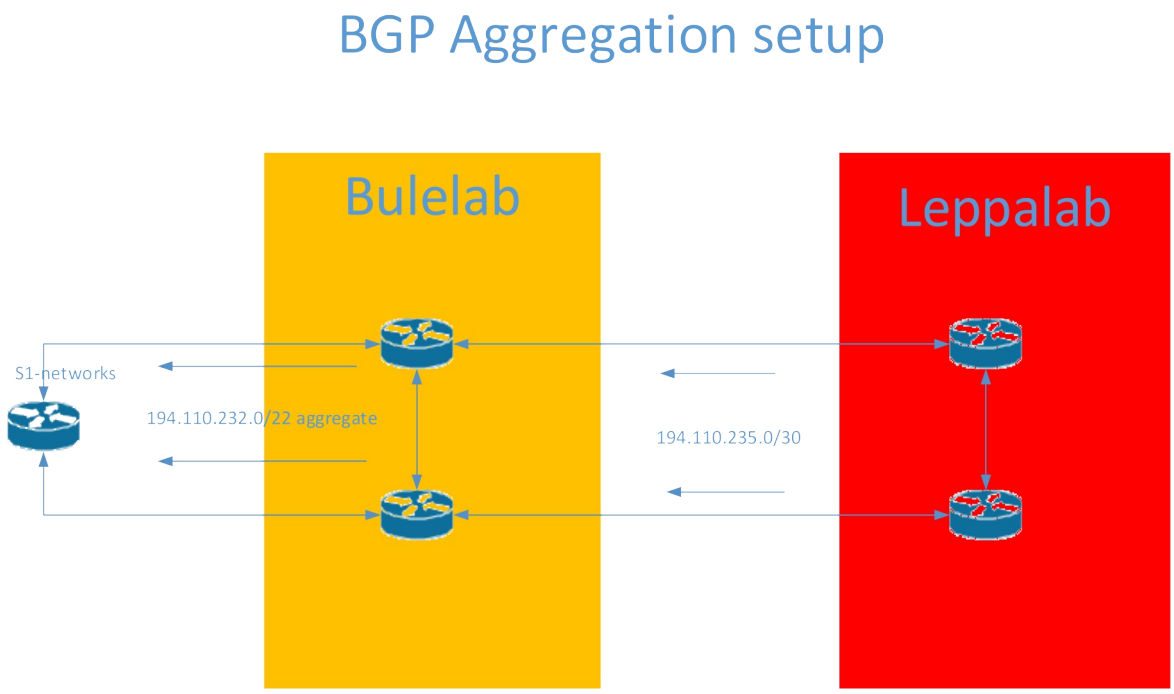



Kuva 3. Idea VRF-toteutuksesta Bulelab- ja MetroIX-infrastruktuurien reitittämiseksi.

Kuvassa 3 on esitetty, kuinka vanhat 2911-reitittimet jäisivät reitittämään laboratoriotöiden verkkoa ja EdgeRouter -laitteet reitittäisivät Internetiin päin liikkuvan liikenteen laboratorion puolella sekä MetroIX:n liikenteen. Tämän kanssa ongelmaksi muodostui myös EdgeRouter -laitteiden vrf- ja useampien reititystaulujen tuen puute. Myöhemmin ilmeni lisäksi, että tietohallinto halusi MetroIX:n laitteiden olevan fyysisesti eristetty laboratorion muusta laitteistosta.

### 3.3 Prototyypissä testatut BGP-menetelmät

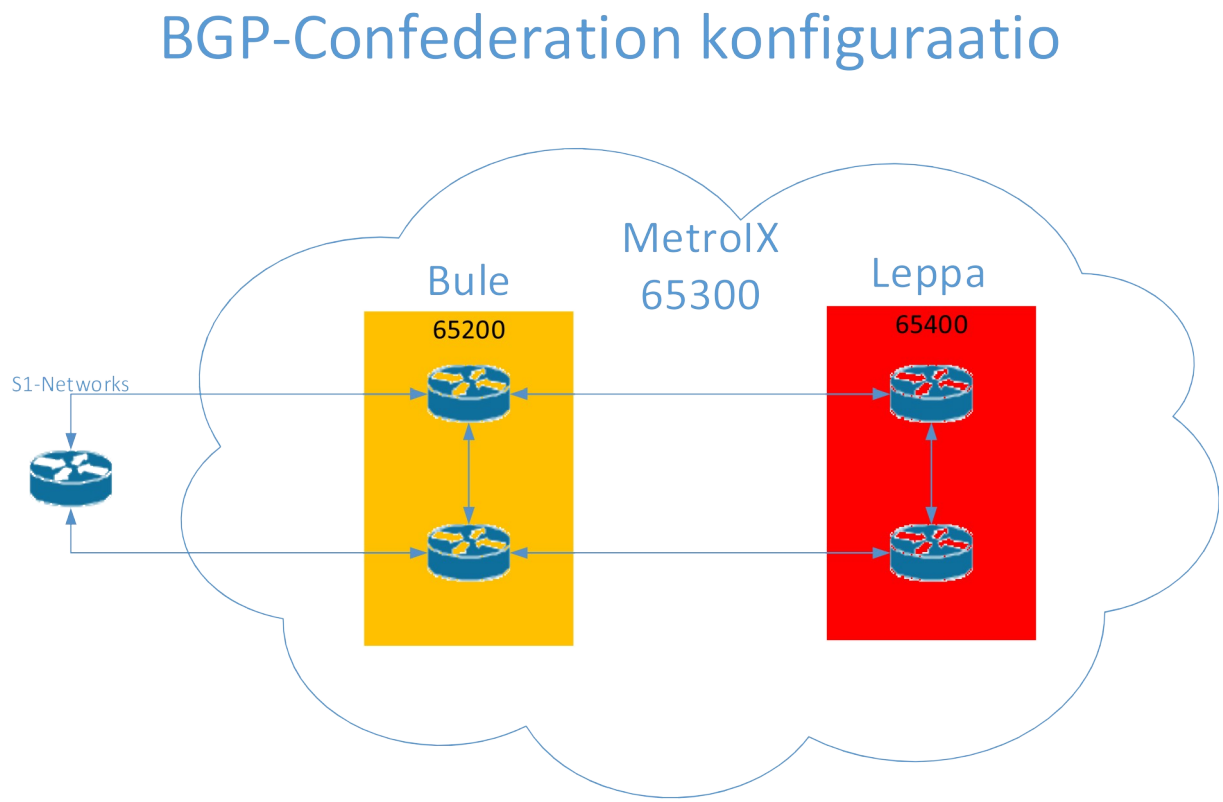
Ensimmäinen versio BGP-reitityskuviosta toteutettiin ns. BGP-aggregation-menetelmällä, jossa kun aggregoiva reititin saa mainostuksen tauluunsa johonkin siihen konfiguroiduista aggregate-address prefixeistä, se alkaa mainostamaan summattua reittiä. BGP eli Border Gateway Protocol on reititysprotokolla, jota käytetään Internetissä ope-raattoreiden ja muiden toimijoiden välillä.




Kuva 4. Periaate prototyypin aggregate-address-mainostuksesta.

Tämän ongelmaksi muodostui se, että mainostaessaan summatun verkkoalueen Internetiin päin, jää reittiin informaatioksi aggregator-osoite, Tämän pystyy kuka tahansa nappaamaan esim. eri toimijoiden ”Looking glass”-palveluista, ja saamaan selville linkin osoitteen. Lisäksi tämä saattaa aiheuttaa pahimmassa tapauksessa virhekonfiguraatiotilanteessa reitityssilmukoita MetroIX:n sisällä.

Toinen testattu konfiguraatio oli BGP-konfederaatio, jossa yhden BGP Autonomous System -numeron sisällä voi olla useampia ulkoisia BGP-naapuruussuhteita niin, että ne eivät näy ulospäin.




Kuva 5. BGP-confederaation toimintaperiaate

Vaikka tämä olisi muuten pätevä toteutustapa, sitä pidettiin tässä vaiheessa liian kankeana vaihtoehtona sekä turhana kompleksisuutena ilman julkista Autonomous System -numeroa. Tämä jätettiin kuitenkin optioksi tulevaisuutta varten, jos ja kun laboratorio hankkii oman julkisen Autonomous System -numeronsa.

# 4 Toteutus

## 4.1 IP-osoitteet

Työ MetroIX:n parissa aloitettiin syksyllä 2014. Ensimmäinen vaihe oli saada aiemmin mainittu IP-osoiteavaruus käyttöön ja laboratoriolle transit-linkki Internet-yhteyttä varten. Helsingin teknillinen oppilaitos, jolle PI-blokki oli rekisteröity, on fuusioitu useampaan otteeseen ja nimi vaihtunut pariinkin otteeseen ennen loppujen lopuksi päätymistään osaksi Metropolia Ammattikorkeakoulua. Lisäksi osoitteet olivat joskus kauan sitten rekisteröity EUNet:n kautta toimiviksi, joka oli mennyt konkurssiin ja myyty Qwest:lle vuonna 1998. Tämä aiheutti valtavan byrokratiakierteen, jossa jouduimme

todistamaan RIPE NCC:lle, että Metropolia on Helsingin teknillisen oppilaitoksen jatkaja ja ettei osoite-avaruus kuulu Elisalle, joka osti aikanaan EUNet:n Suomen toiminnot. Ennen pitkää useamman byrokratiakierroksen jälkeen osoitteet saatiin siirrettyä verkkolaboratorion nimiin. [8.]

PI-osoitteiden tapauksessa RIPE NCC vaatii, jotta osoitteet voivat reitittyä Internetissä oikein ja tiedetään, kenen järjestelmästä reitit mainostuvat, että organisaatio joko rekisteröityy LIR:ksi tai tekee sopimuksen jonkin olemassa olevan LIR:n kanssa. Tässä vaiheessa päätettiin, että verkkolaboratorio ei rekisteröidy LIR:ksi vaan tekee sopimuksen kolmannen osapuolen kanssa. S1-networks suostui toimimaan tässä roolissa transit-operaattorina.

LIR eli Local Internet Registry on taho, joka allokoi suurimman osan omasta osoiteblokistaan asiakkaille tai loppukäyttäjien käyttöön. LIR:llä on oma AS-numero (Autonomous System), joilla organisaatioiden reititysinformaatio mainostuu Internetissä ja on yksilöllisesti tunnistettavissa.

PI-osoitteiden etu on siinä, että organisaatio, jonka hallussa PI-osoiteavaruus on, pystyy täysin valitsemaan, miten osoitteita käytetään ja valitsemaan palveluntarjoajat, joiden kautta kyseiset osoitteet mainostuvat Internetiin päin. PA-osoitteet eli provider-assigned -osoitteet puolestaan on annettu palveluntarjoajalta organisaatiolle. Tietoverkkolaboratorion tapauksessa PI-osoitteet ovat ns. legacy-statuksella rekisteröity, jolloin niiden ei tarvitse olla suoraan merkattu kuuluvaksi millekään yhdelle LIR:lle.

## 4.2 Laitteisto

DNA Oy uusi keväällä 2014 joitain verkkolaitteitaan osana projektia, jossa he yhtenäisti-vät laitekantaansa, ja päättivät lahjoittaa Extreme Networksin laitteensa tietoverkkolabo-ratoriolle. Näistä laitteista Summit X460 -kytkimiä päätettiin käyttää kytkin-infrastruktuuria varten. Pyysimme S1-Networksilta, että he vuotaisivat koko Internetin IPv4 BGP -reititystaulun laboratoriolle päin, jotta tulevaisuudessa pystyttäisiin harjoittelemaan esim. traffic-engineering -skenaarioita. Koko Internetin BGP-taulu on kooltaan kirjoitushetkellä noin 520 000 reittiä. Näin suuren taulun nopea reititys vaatii reitittävältä laitteelta huomattavan määrän muistia, sekä hyvän ASIC:n, johon reiteistä

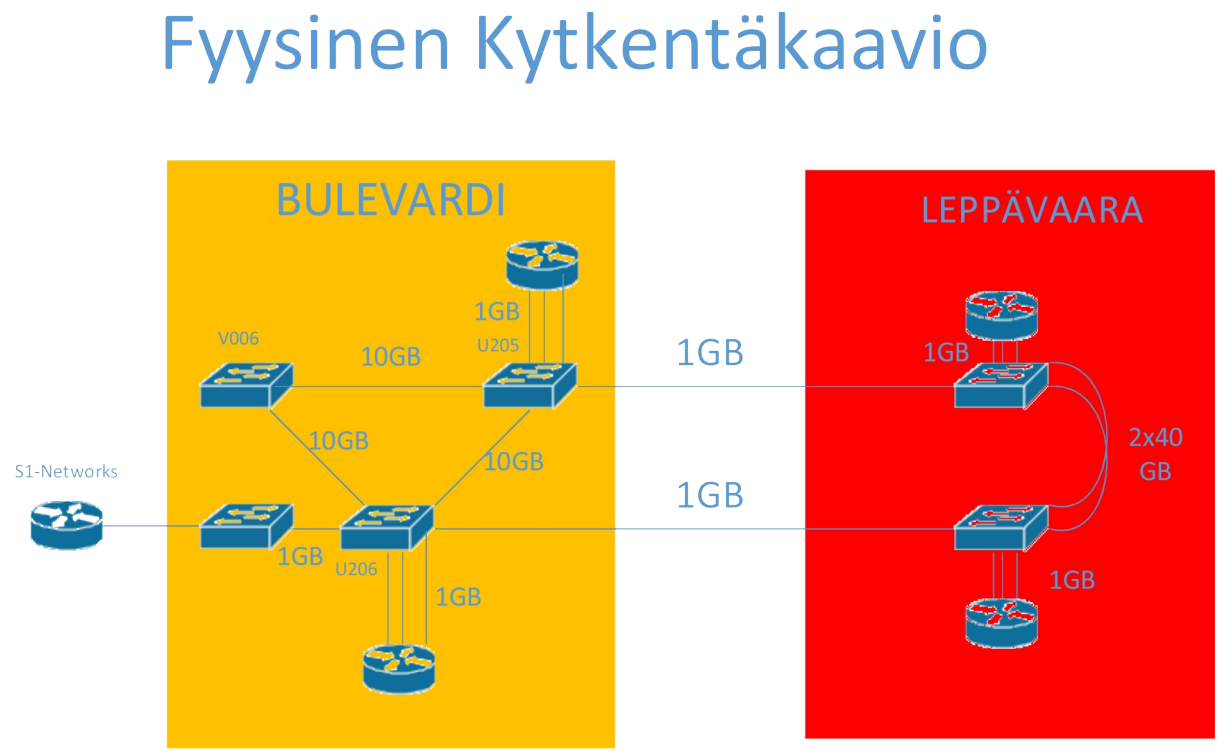
rakennetun kytkentäinformaation pystyy asentamaan nopeaa pakettien portista toiseen siirtämistä varten. ASIC eli application specific integrated circuit on piiri, joka on suunniteltu tiettyä tehtävää varten. Yleensä tämän suorituskyvyn laitteet maksavat helposti yli 20 000 euroa, mutta emme halunneet ainakaan alkuun laittaa projektiin tällaista summaa. Ubiquiti networksin Edgerouter -tuotesarjasta löytyi useiden pienien operaattoreiden käyttämä Edgerouter Pro -laite, joka kykenee tarvittavaan reititysnopeuteen, sekä omaa tyydyttävät ominaisuudet infrastruktuurin tämänhetkiseen tarpeeseen sekä tuleville muutamalle vuodelle. [9.] Hintaa laitteilla oli noin ~400 euroa per laite ja näitä tilattiin kuusi kappaletta.

## 4.3 Arkkitehtuuri

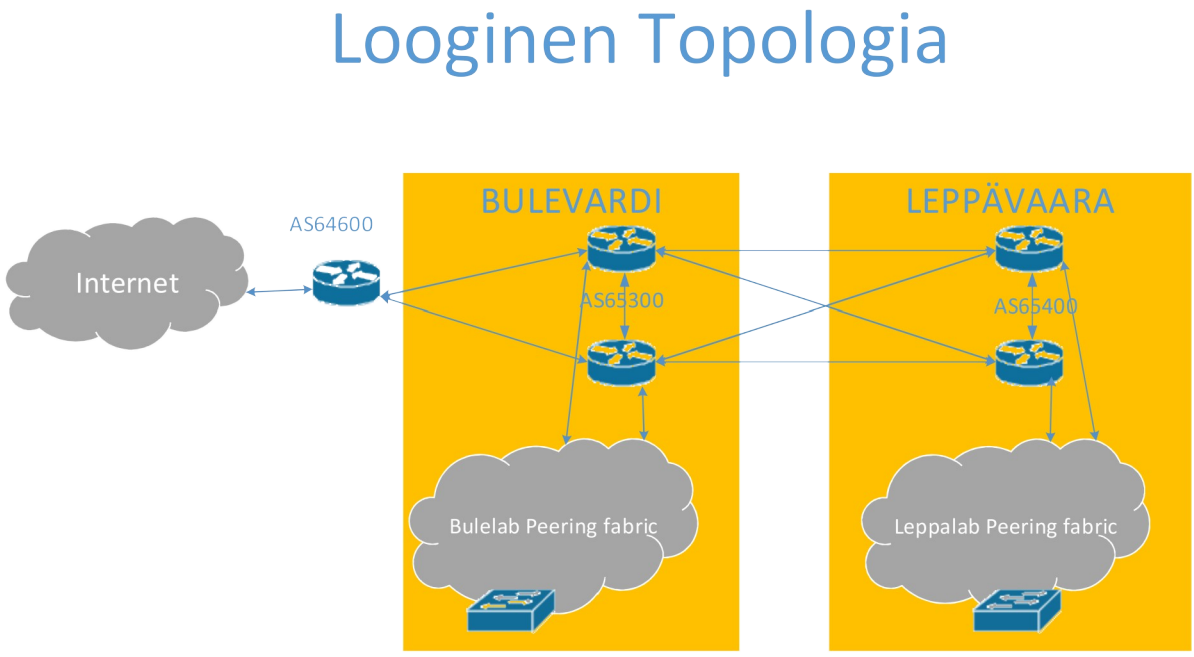
Alussa kun infrastruktuuria suunniteltiin, ajateltiin, että Bulevardin ja Leppävaaran kampuksilla olisi erilliset reitityslinkit S1-networksiin. Kyseinen ratkaisu todettiin liian epävar-maksi, vikaherkäksi ja vaikeasti hallittavaksi. Päätettiinkin, että reititys uplinkkiin hoide-taan Bulevardin päässä, johon toistaiseksi ainoa uplink-kuitu tulee. Kytkin-infrastruktuurin osalta liittyjän käytössä oleva peeraus-fabric kummallakin kampuksella ei ole ethernetin tasolla yhteydessä toisiinsa, vaan mikäli liittyjien tarvitsee siirtää liikennettä toisen kampuksen fabricciin, tai mikäli he tarvitsevat uplink-yhteyden IXP:stä Internetiin, heidän tulee tehdä se MetroIX:n reititysinfrastruktuurin kautta. Tämä tekee vianhallinnan reitityksen ja kytkennän osalta MetroIX:n infrastruktuurin sekä liittyvien järjestelmien välillä yksinkertaisemmaksi.

Vaikka molemmissa päissä kytkin-infrastruktuurin suorituskyky yltäisikin 10 gigabitin nopeuksiin tai enempäänkin, ei tietohallinnon Bulevardin ja Leppävaaran väliseen linkkiin saada kuitukanavointilaitteen rajoitteiden takia kuin 1Gb/s:n linkkejä. Uusilla linjakorteilla tämä selviäisi, mutta tämä olisi hyvin kallista.

Fyysisen asennuksen osalta Bulevardin verkkolaboratoriossa kytkimet on sijoitettu kolmeen eri tilaan ja reitittimet kahteen eri tilaan.




Kuva 6. MetroIX:n fyysiset kytkennät eri tilojen laitteiden välillä.




Kuva 7. MetroIX:n looginen IP-tason topologia

### 4.4 Reitityspolitiikka MetroIX -reititysinfrastruktuurissa

S1-networksin kanssa sovittiin toistaiseksi käytettäväksi Bulevardin päässä AS-numeroa 65300 ja S1-networksin päässä AS-numeroa 64600. Bulevardin päästä mainostetaan S1-networksin suuntaan ainoastaan kaksi verkkoaluetta: 194.110.224.0/21 ja 194.110.232.0/22. Tähän mainostukseen on lisäksi lisätty AS-path-filtteri, joka sallii ainoastaan nolla-path prefixin mainostuksen, jottei verkon sisäinen topologia vuoda S1-networksille vahingossakaan. Toistaiseksi S1-networksin päässä on vain yksi reititin, johon BGP-sessio on konfiguroitu Bulevardin reitittimistä. Bulevardin sekä S1-networksin reitittimissä tähän on konfiguroitu eBGP ECMP, jotta Bulevardin reitittimistä saataisiin maksimaalinen teho irti ja jotta yhden laitteen hajoaminen tai mykistyminen vaikuttaisi mahdollisimman vähän infrastruktuurin toimivuuteen. ECMP eli Equal Cost Multipathing on tekniikka, jossa reitittimessä on reititystaulussa kaksi reittiä samaan kohdeverkkoon, ja reititin jakaa kuorman näiden kahden reitin next-hop -reitittimen välille. eBGP, eli external BGP, on AS-järjestelmien välinen BGP-naapuruussuhde. [10.] Liitteessä 1 tämä mainostuspolitiikka on määritelty kohdassa route-map S1-EXPORT.

Tässä vaiheessa nähtiin helpoimmaksi ratkaisuksi jakaa 194.110.224.0/21 kahtia niin, että Bulevardin verkkolaboratorio käyttää jälkimmäistä puolikasta aluksi ja Leppävaaran laboratorio ensimmäistä puolikasta. Myös private-AS-numerot jaettiin niin, että Bulevardin pään laitteet käyttävät numeroita 65301–65399 ja Leppävaaran päässä numeroita 65401–65499.

AS-numerot olivat aluksi 16-bittisiä, mutta Internetin kasvaessa BGP-protokollaan tehtiin lisäys AS-numeroavaruuden kasvattamiseksi 32-bittiseksi. 16-bittisistä AS-numeroista numerot 64512-65534 ja 32-bittisistä numerot 4200000000-4294967294 on varattu organisaatioiden sisäiseen käyttöön samaan tapaan kuin Request For Comments -dokumentti numero 1918 määrittelee tietyt IP-osoiteavaruudet organisaatioiden sisäiseen käyttöön.

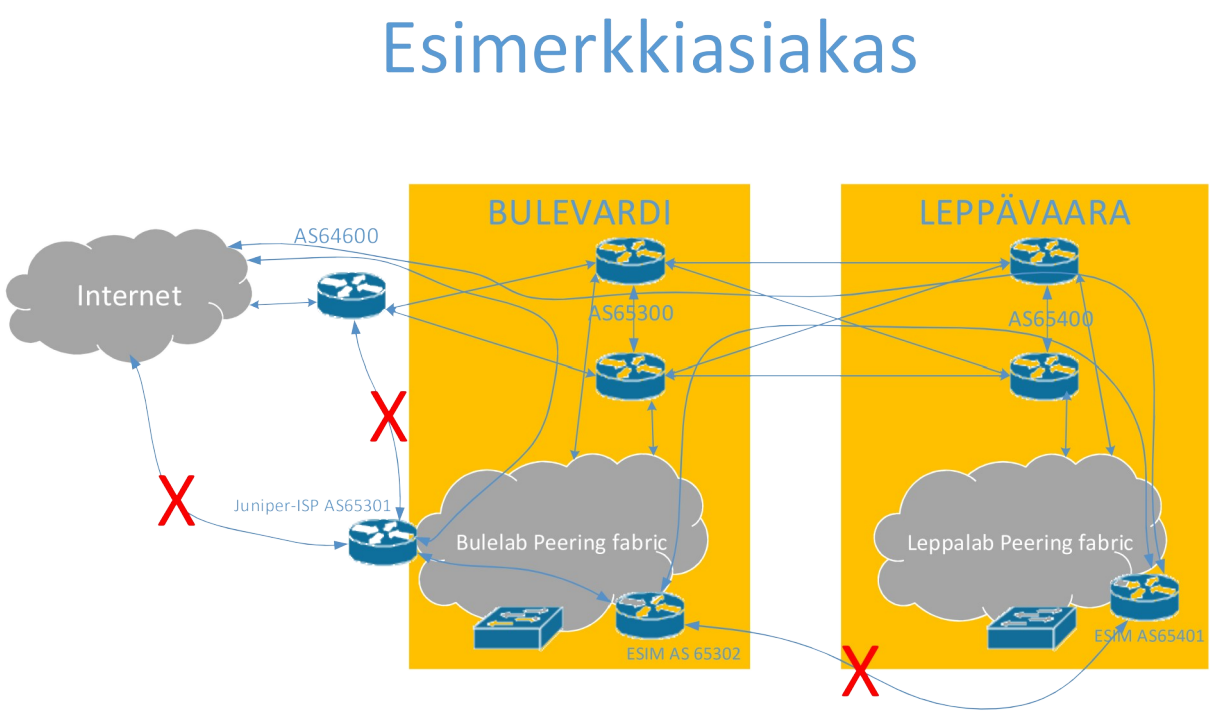
Jokaiselle liittyvälle järjestelmälle allokoidaan linkkiyhteys, sekä tarpeen mukaan reitit-tyviä privaatti-osoitteita sekä perustellusti tarpeen mukaan osoitteita MetroIX:n julkisesta osoiteavaruudesta. Tästä esimerkkinä reitityspolitiikan osalta on liitteessä 1 policy prefix-list Juniper-ISP-PA.

## 4.5 Palomuurauslogiikka MetroIX:ssä

Bulevardin pään reitittimiin on tehty Internetistä päin tulevalle liikenteelle muutama tilatiedoton palomuurisääntö, joilla suojataan kaikkein haavoittuvimmat asiakaspäätteiden palvelut ja yleisimmin mm. palvelunestohyökkäyksissä hyväksikäytetyt palvelut. Liitteessä 1 on tarkemmin Access-list BLOCK-TRANSIT-ETH0-IN määritelty estetyt palvelut. Lisäksi reitittimeen itseensä kohdistuva liikenne on muurattu jokaisen portin osalta erikseen sallimaan liikenne vain tietyistä osoitteista ja tarpeen mukaan.

BLOCK-TRANSIT-ETH0-IN -listassa olevat palvelut ovat Windowsin ja Linuxin etäkutsu-palvelut, Windowsin NetBios-, sekä tiedostonjakopalvelut, nimi ja aikapalvelut sekä Universal Plug and Play -palvelut. Näitä kaikkia hyväksikäytetään laajasti hyökkäyksissä yksittäistä järjestelmää kohtaan sekä amplifikaatiohyökkäyksissä.

Viime aikoina uutisiinkin asti ovat nousseet ongelmat, joita palvelunestohyökkäykset ovat aiheuttaneet. Suurin osa palvelunestoliikenteeseen käytetystä liikenteestä on koostunut hyödyntämällä palveluita, jotka ovat luonteeltaan sellaisia, että ne eivät vaadi asiakkaalta kuin yhden paketin. Tätä voidaan hyväksikäyttää lähettämällä liikennettä väärennetyllä IP-osoitteella. Tämä voidaan estää tekemällä ns. ingress filtering -skeema verkon reunalle. [11.] Näistä säännöistä esimerkkeinä on liitteessä 1 firewall name BLOCK-OUT. Lisäksi kaikelle liikenteelle, joka tulee sisään MetroIX:n reititysinfrastruktuuriin, peerausfabricista on tehty oma filtteröinti, jottei myöskään asiakkaiden verkoista pysty tulemaan väärennettyä liikennettä MetroIX:n reititykseen. Tästä esimerkkinä liitteessä 1 ovat ALLOW-FROM-FABRIC-IN ja ALLOW-FROM-FABRIC-OUT muurauslistat. Tämä fabricin ingress-filtteröinti on tehty modulaariseksi niin, että address-group ON-FABRIC:n voi lisätä asiakkaille määritellyt osoitteet. Tämän voi myöhemmin laajentaa niin, että jokaiselle asiakkaalle on oma osoitelistansa, ja sääntöihin lisätään myös lähde MAC-osoite jokaiselle osoitelistalle.




Kuva 8. BGP-naapuruussuhteiden muodostamislogiikka, sekä miten liikenne pystyy kulkemaan eri järjestelmien välillä. Asiakkaalta voi siirtää liikennettä ainoastaan saman tilan toiselle asiakkaalle tai MetroIX:n reitittimille. Ainoastaan IXP:n reitittimien kautta liikenne voidaan siirtää muualle.

## 4.6 Kytkin-infrastruktuuri

Bulevardin laboratorion päässä suurin pulma oli, miten saada kytkin-infrastruktuuri kyllin vikasietoiseksi ja samalla säilyttää suorituskyky tarpeellisella tasolla. Ratkaisuna tähän kolmesta kytkimestä, jotka ovat eri tiloissa, tehtiin virtual-chassis -toiminnolla yksi looginen kytkin. Tämä toteutettiin X460-kytkimien 2x10Gb:n lisämoduuleilla tilojen välissä kulkevien kuitujen kautta.

Loogisesti kytkinpino on pilkottu kummallakin kampuksella IXP:n sisäisen liikenteen vlaniin, kampusten välisen reitityksen vlaniin sekä IXP:n liittymiseen tarkoitettuun fabric-vlaniin. Fabric-VLAN:ssa on sallittu IPv4- ja IPv6-liikenteen siirto ja tuntematonta unicast-, multicast- sekä broadcast-liikennettä on rajoitettu per-portti. Kampusten väliset kaksi linkkiä on konfiguroitu LACP-linkiksi, jossa käytetään L4 informaatioon perustuvaa hash-algoritmia. Tämä mahdollistaa yksinkertaisen topologian ethernetin osalta ja jakaa kuorman linkin porttien kesken per-yhteys pohjalta. [12.] Toistaiseksi

portteihin ei ole konfiguroitu staattisesti sallittuja MAC-osoitteita, kuten FICIX tekee omassa infrastruktuurissaan, mutta tätä saatetaan harkita myöhemmin.

### 4.7 Dokumentointi

Osa projektia oli tehdä uudenlainen keskitetty dokumentointijärjestelmä, johon pääsisi molemmilta kampuksilta käsiksi. Tämä päätettiin toteuttaa Racktables-ohjelmistolla, joka toimii Apache:n http-palvelimella Linuxin päällä. Racktables mahdollistaa räkkien kaapelointien ja laiteasennusten visualisoinnin sekä verkkojen ja IP-osoitteiden yksityiskohtaisen dokumentoinnin. Racktablesin tueksi asennettiin dokuwiki, johon pystytään dokumentoimaan yksityiskohtaisesti myös mm. tässä dokumentissa esitetyt konseptit.

## 5 Testaukset, suorituskyky ja lopputuloksen arviointi

### 5.1 Vikasietoisuuden testaus

Reitityksen vikasietoisuutta testattiin katkaisemalla virta jommastakummasta reitittimistä ja ajamalla samalla asiakaspään laitteella ping-ohjelmaa. Testauksissa ilmeni, että konvergenssi vikatilanteessa oli muutamien sekuntien luokkaa. Toisen laitteen pimentyessä toinen reitittimistä jatkoi toimintaansa normaalisti ilman, että enempää kuin muutama paketti jäi reitittämättä. Kun Edgerouter-laite palautettiin infrastruktuuriin, koko BGP-taulun asentaminen ASIC:n kesti keskimäärin neljä minuuttia ja koko infrastruktuurin stabilisoituminen noin seitsemän minuuttia.

Kytkimien vikasietoisuutta testattiin samalla periaatteella ottamalla yhdestä pinon jäsenestä virta pois ja katsomalla, miten tämä vaikuttaa liikenteeseen. Testeissä ei havaittu merkittävää viivettä vikaantumisen ja liikenteen uudelleenohjautumisen välillä. Koska pino on toteutettu kuitulinkkien yli dedikoitujen pinoamiskaapelien sijaan, testattiin myös optiikan vikaantumista irrottamalla kuitu yhdestä linkistä. Myöskään tässä testissä ei huomattu merkittävää viivettä vikaantumisen ja normalisoitumisen välillä.

## 5.2 Suorituskykymittaukset

Extreme Networksin X460-kytkimet pystyivät helposti kytkemään useamman portin yli linjanopeudella peering-fabricissa sekä kampusten välisessä LACP-linkissä. Suurin pullonkaula todettiin Edgerouter-laitteissa, joiden 64 tavun pakettien reitityskyky oli noin 300-450 Mbps. Valitettavasti ECMP-konfiguraatiolla suorituskykyä ei päästy testaamaan tarpeeksi järeiden asiakaspään reitityslaitteiden puutteen takia. ECMP:n kuitenkin arvioidaan nostavan reitityksen suorituskyvyn noin 600-700 Mbps:n kieppeille 64 tavun paketeilla. Suuremmilla paketeilla, 250 tavun paketeista lähtien, suorituskyvyn havaittiin ole-van lähes linjanopeuksista. Tämän arvioitiin skaalautuvan ECMP:llä lähelle 1700 Mbps:n nopeutta.

## 5.3 Lopputuloksen analysointi ja SPOF-analyysi

Valmis infrastruktuuri on kyllin vikasietoinen laboratorioiden sisäisen ja on-site-järjestelmien käyttöön. Yksittäisen verkkolaitteen vikaantuminen ei vaikuta millään tavalla Bulevardin ja Leppävaaran välisen liikenteen toimivuuteen. Suorituskyky kampuksen sisällä peering-fabricissa riittää helposti ainakin 10Gb:iin asti, ja riippuen missä tilassa laite on liitettynä, ja hieman ylikin. Extreme Networksin dokumenttien mukaan ExtremeXOS Virtual-Chassis-konfiguraatiossa liikenne kulkee stacking-porttien kautta aina lyhintä reittiä pitkin, joten kahden huoneen välillä liikenne on rajoitettu 10gbps nopeuteen. [13.] Kampusten välillä liikennettä ei Edgerouter Pro -laitteiden odotetun käyttöiän aikana odoteta sellaista määrää, että tämä koituisi pullonkaulaksi.

SPOF, eli Single Point of Failure-analyysissa täytyy ottaa huomioon, mikä yksittäinen sisäinen tai ulkoinen asia pystyy potentiaalisesti kaatamaan koko järjestelmän. Kaikissa moderneissa järjestelmissä pyritään aina eliminoimaan kaikki SPOF:t, mutta tämä ei kaiken toiminnallisuuden osalta välttämättä ole aina mahdollista.

Suurimmat ongelmat ja potentiaaliset riskit liittyvät virtual-chassis-konfiguraatioon ja tästä aiheutuvaan jaettuun control-plane-tasoon. Mikäli jokin aiheuttaa kytkinten prosessoreille tarpeeksi kuormaa niin, että tämä vaikuttaa toimintoihin, virtual-chassis-konfiguraatiossa tämä vaikuttaa kaikkien kolmen kytkimen toimintaan. Toistaiseksi toinen suuri SPOF on S1-networksin toimittama yksittäinen kuitu ja heidän

toimittamansa kytkin, johon kuitu terminoidaan, joiden kautta transit-linkki kulkee. Tämä tosin vaikuttaa ainoastaan Internet-liikenteeseen, eikä näiden hajoaminen vaikuta MetroIX:n sisäisen liikenteen toimivuuteen. Lisäksi luokan U206 serveritilassa virransyöttöä näille laitteille ei ole varmistettu UPS:lla.

# 6 Jatkokehitys

## 6.1 MPLS ja Flow-based -arkkitehtuurit

Hankalan taloustilanteen vuoksi tässä vaiheessa MetroIX:n verkkoinfrastruktuuria varten ei pystytty hankkimaan järeämpiä laitteita. Mikäli uudet laboratorio- ja opetusympäristöt osoittautuvat menestyksiksi, täytyy infrastruktuuria varten hankkia myöhemmin järeämmät kytkimet. Nämä mahdollistaisivat L2-teknologioiden käytön minimoimisen ja MPLS-teknologian käytön, jolla pystyttäisiin helpommin ilman jaettuja control-plane-tasoja toteuttamaan MetroIX:n IXP-fabric.

Toinen lähestymistapa olisi implementoida OpenFlow-pohjainen verkkoinfrastruktuuri, jossa flow-pohjaisella reitityksellä ja kytkennällä pystyisi kontrolloimaan IXP-fabriccia.

Nämä toteutustavat eivät sulje toisiaan pois moderneilla alustoilla, ja todennäköisesti nämä tullaankin näkemään rinnakkain MetroIX:n seuraavassa iteraatiossa.

## 6.2 Reitityksen vikasietoisuus

Ilmeinen seuraava kehityskohde olisi hankkia esimerkiksi Leppävaaraan toiselta transit-operaattorilta kuitulinkki, jotta Internet-yhteys saataisiin vikasietoiseksi ja toimittajariippumattomaksi. Leppävaaran päässä reitityspolitiikka ja muut tarvittavat konfiguraatiot ovat jo valmiina, joten tämän toteuttaminen ei olisi kovinkaan hankalaa. S1-Networks on uusimassa toukokuussa 2015 omia reitittimiään, jonka jälkeen Bulevardin linkkiin toden-näköisesti konfiguroidaan S1:n päähän toinen reititin.

### 6.3 Virransyötön varmistaminen U206 laitteille

U206-tilassa olevien S1-Networksin kytkimen ja U206:n MetroIX-kytkinpinon kytkimen virransyötön varmistaminen UPS:lla olisi myös erittäin suotava parannuskohde. Tähän onkin kirjoitushetkellä jo saatu UPS laite, joka odottaa vaihtoakkuja.

### 6.4 Verkonvalvonta ja SLA

Tässä vaiheessa MetroIX:n infrastruktuurissa ei ole yhtään palvelinjärjestelmää MetroIX:n omaan käyttöön. Myöhemmin infrastruktuuriin tulee lisätä verkonvalvonnan komponentteja monitoroimaan laitteiden toimintaa, jotta vikaantumisiin voidaan puuttua nopeasti ja palvelukatkokset estää. Samalla järjestelmään voisi lisätä linkkien laadun monitoroinnin, jotta mahdollisesti vikaantuvat optiikat tai likaiset kuidut huomattaisiin nopeammin.

### 6.5 IPv6

S1-Networksilta on pyydetty myös tietoverkkolaboratorion omaan käyttöön IPv6 PI-osoiteblokki, joka myönnettiin loppukeväästä 2015. Tämän konfigurointi kuitenkin jouduttiin lykkäämään, kunnes S1-networks saa omassa päässään toukokuussa reitittimensä vaihdettua. IPv6-osoitteiden konfigurointi mahdollistaa infrastruktuurin käytön myös tulevaisuudessa ja eliminoi yksityisosoitteiden käytön verkoissa.

### 6.6 Julkinen AS-numero ja LIR-rekisteröinti

Myöhemmin mikäli tietoverkkolaboratorio päättää liittyä RIPE NCC:n jäseneksi ja hankkia oman AS-numeron, todennäköisesti kivuttomin tie uudelleenkonfigurointiin olisi tehdä MetroIX:n reitittimistä BGP-konfederaatio. Tämän avulla MetroIX:n sisäinen liikenne säilyisi logiikaltaan samana, mutta ulospäin näkyisi vain julkinen AS-numero ja fabricciin liittyvien asiakkaiden privaatti-AS-numero voitaisiin filtteröidä pois kuten normaalisti julkista AS-numeroa käyttäessä.

# 7 Yhteenveto

Kaiken kaikkiaan työ opetti tekijälle valtavan määrän BGP:n toiminnasta, sekä siitä, miten isot toimijat reitittävät liikenteensä Internetin mittakaavassa. Valmis infrastruktuuri vastaa suunniteltua topologiaa ja arkkitehtuuria niin suorituskyvyltään kuin vikasietoisuudeltaankin.

Seikka mikä teki suuren vaikutuksen työn tekijään sekä muihin Metropolian verkkolaboratorion jäseniin, oli Edgerouter Pro laitteiden suorituskyky sekä kyky reitittää täyden BGP-taulun kanssa. Noin 400 euron laitteen suorituskykyä epäiltiin useaan otteeseen monelta eri taholta ja tämän suoriutuessa mallikkaasti tehtävästään oli hämmästelyn määrä suuri jokaiselta näistä epäilijöistä.

Alun perin myös laboratorion tietohallinnon puoleinen liikenne suunniteltiin siirrettäväksi Edgerouter Pro -laitteiden reititettäväksi, mutta kyseisen alustan rajoitukset estivät tämän. Lisäksi tietohallinto vaati, että uusi rakennettava infrastruktuuri on laitetasolla erillään muusta laboratorion verkosta, joten tästä ideasta luovuttiin kokonaisuudessaan.

Työ oli hyvin käytännönläheinen ja tässä dokumentissa ei pyritty käymään yksityiskohtaisesti läpi jokaista konfiguraation palasta. Työn tekijä jatkaa nyt perustuksiltaan valmiin verkkoinfrastruktuurin jatkokehitystä.

## Lähteet


1 Promoting the use of Internet Exchange Points. 2012, Verkkodokumentti. <https://www.internetsociety.org/sites/default/files/Promoting%20the%20use%20of%20IXPs.pdf> Luettu 24.3.2015.

2 About AMS-IX. Verkkodokumentti. <https://ams-ix.net/about/about-ams-ix> Luettu 24.3.2015.

3 Switched fabric. Verkkodokumentti. <http://en.wikipedia.org/wiki/Switched_fabric> Luettu 24.3.2015.

4 AMS-IX MPLS/VPLS infrastructure. Verkkodokumentti. <https://ams-ix.net/technical/ams-ix-infrastructure/the-ams-ix-mplsvpls-infrastructure> Luettu 24.3.2015.

5 FICIX Tekniikka. Verkkodokumentti. Ficix RY. <http://www.ficix.fi/tekniikka.php> Luettu 24.3.2015.

6 Portable Product sheets – Routing Performance. 2009. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf> Luettu 24.3.2015.

7 Configuring VRF. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/vrf.html> Luettu 24.3.2015.

8 IPv4 Transfers – General overview. 2013. Verkkodokumentti. RIPE NCC. <https://www.ripe.net/lir-services/resource-management/ipv4-transfers> Päivitetty 7.4.2015. Luettu 24.3.2015.

9 Ubiquiti EdgeMax EdgeRouter Product datasheet. 2014. Verkkodokumentti. Ubiquiti Networks. <https://www.ubnt.com/downloads/datasheets/edgemax/EdgeRouter_DS.pdf> Luettu 24.3.2015.

10 BGP Case Studies. 2008. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html> Luettu 24.3.2015.

11 BCP38 Ingress filtering. Verkkodokumentti. <http://www.bcp38.info/index.php/Main_Page> Luettu 24.3.2015.

12 Link Aggregation – Order of frames. Verkkodokumentti. <http://en.wikipedia.org/wiki/Link_aggregation#Order_of_frames> Luettu 24.3.2015.

**13** SummitStack, Extreme Networks Virtual Chassis Stacking Technology. 2012. Verkkodokumentti. Extreme Networks. <http://www.usedcomp.de/pdf/Extreme-Networks-SummitStack-Virtual-Chassis-Stacking-Technology-Technical-Brief.pdf> Luettu 24.3.2015.