Heikki Salminen

Asiakasverkon suunnittelu konesaliympäristöön

Metropolia Ammattikorkeakoulu
Insinööri
Tietotekniikan koulutusohjelma (AMK)
Insinöörityö
7.5.2012

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Heikki Salminen Asiakasverkon suunnittelu konesaliympäristöön 25 sivua + 5 liitettä 7.5.2012
Tutkinto	Insinööri
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoliikennetekniikka
Ohjaajat	Chief Technical Officer Jerry Jalava lehtori Erik Pätynen

Tässä työssä asennettiin kolmannen osapuolen Nemein Oy:lle suunnittelema konesaliverkko, jonka pohjalta luotiin uudet verkkosuunnitelmat, joita mukaillen voidaan kasvattaa verkkoa tarpeen mukaan. Työssä on pyritty vaiheistamaan suunnitelmat siten, etteivät yksittäiset vaiheet ole taloudellisesti suhteettomia hyötyyn nähden, ja että jokainen päivitysvaihe on toteuttaa kannattavasti.

Työn alussa on esitelty erilaisia tietoverkkojen tekniikoita, joiden avulla verkosta saadaan mahdollisimman paljon hyötyä. Tämän jälkeen on tehtiin analyysi jo asennetusta verkosta, jonka lisäksi haluttiin korostaa verkon mahdollisuuksia parantaa asiakkaan järjestelmälle tärkeitä ominaisuuksia, kuten korkeaa palvelun saatavuutta, ja häiriötilanteiden automaattista ehkäisyä.

Työn tuloksena on saatu kolmivaiheinen suunnitelma, josta ensimmäinen vaihe sisältää sekä ehdotuksia laitevalinnoiksi, että ehdotettuja laitekokonaisuuksia mukailevat verkkokuvat. Toisen ja kolmannen vaiheen suunnitelmat ovat ainoastaan periaatteellisia, mutta niistä käy ilmi tavoitteet ja joitain mahdollisia toteutustapoja ominaisuuksien käyttöönottamiseksi. Nemein Oy voi verkon päivittäessään käyttää suunnitelmia joko sellaisenaan, tai viitteellisinä malleina, joiden perusteella lopullinen suunnitelma tehdään.

Avainsanat	IP, verkko, verkkosuunnittelu, konesali

Metropolia

Abstract

Author Title Number of Pages Date	Heikki Salminen Designing customer network in data centre environment 25 pages + 5 appendices 7 May 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications
Instructors	Jerry Jalava, Chief Technical Officer Erik Pätynen, Senior Lecturer

This study was done for Nemein Ltd. to first implement a system based on a design by a third party, and then to create designs for a data centre network to improve on the current implementation. The goal was to phase the designs so that each of them would be economically viable to implement when the need arises.

The thesis starts by defining various network technologies which can be used to extract more potential out of the network. After that the current implementation was analyzed. The main focus was to introduce ways for the network to support and benefit the key elements of the system, such as fault-tolerance and high availability.

As a result, this thesis introduces three phases for upgrading the network. The first phase is the most complete one, with defined suggestions for equipment to invest in, and network visualizations that take into account the differences of topology with different suggested equipment. The second and third phase are introduced as principal designs, with some suggestions for the available options included in each phase. When upgrading their network, Nemein Ltd. can use these plans as they are, or as design guidelines for the final plans.

Keywords	IP, network, network design, data centre

Sisällys

Lyhenteet, käsitteet ja määritelmät

ACL	*Access Control List.* Verkon pääsylista.
CAM	*Content Addressable Memory.* Muisti, jossa haut tallennetulle datalle tehdään koko muistiin.
Cat6(a)/7	Kategoria on jaottelu, joka kuvaa parikaapelin laadukkuutta ja soveltuvuutta eri signalointinopeuksille.
CST	*Common Spanning Tree.* Useat STP-instanssit yhdistävä STP, osa MSTP:tä.
Ethernet	L2-tason protokolla, IEEE:n standardi 802.3, yleisin käytetyistä L2-tason protokollista
FastEthernet	Kytkimien porttityyppi, määrittää porttinopeutta. FastEthernetin tuetut nopeudet ovat 10Mb/s ja 100Mb/s
FC	*Fibre Channel.* SAN-verkkojen tiedonsiirtoprotokolla, vastaa TCP:tä IP-verkoissa, välittää SCSI-komentoja Fibre Channel-verkkojen yli.
FCIP	*Fibre Channel over IP.* SAN-verkkojen tiedonsiirtoprotokollan kerrostus IP:n päälle.
FCoE	*Fibre Channel over Ethernet.* Ethernet-kehystyksen päällä kuljetettavaa Fibre Channel protokollan dataa.
FCP	*Fibre Channel Protocol.* Protokolla Fibre Channel-tekniikan alla. Kts. FC - Fibre Channel.
Gb/s	*Miljardia bittiä per sekunti.* Tiedonsiirtonopeus mitattuna siirrettyjen bittien määrällä sekunnissa.
HSRP	*Hot Standby Routing Protocol.* Ciscon omistama redundanssi-protokolla, jonka avulla luodaan vikasietoinen oletusyhdyskäytävä liitäntälaitteille.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
IETF	*Internet Engineering Task Force.* Internet-protokollien standardoinnista vastaava organisaatio.
IP	*Internet Protocol.* L3-tason tiedonsiirtoprotokolla.
IPoFC	*Internet Protocol over Fibre Channel.* IP-verkkojen tiedonsiirtoprotokollan kerrostus FC:n päälle.
ISL	*Inter-Switch Link.* Kahden SAN-kytkimen välinen linkki.

L1	*Layer 1.* Tiedonsiirtoprotokollien ensimmäinen, fyysinen taso.
L2	*Layer 2.* Tiedonsiirtoprotokollien toinen, siirtoyhteystaso.
L3	*Layer 3.* Tiedonsiirtoprotokollien kolmas, verkkotaso.
LAN	*Local Area Network.* Lähiverkko, sisältää laitteet jotka kuuluvat samaan, pienellä alueella sijaitsevaan verkkoon, esimerkiksi toimisto.
MAC	*Media Access Control.* Fyysisen liitännän, esimerkiksi verkkokortin 48-bittinen osoite.
Mb/s	*Miljoonaa bittiä per sekunti.* Tiedonsiirtonopeus mitattuna siirrettyjen bittien määrällä sekunnissa.
MPLS	*Multiprotocol Label Switching.* Menetelmä, jolla kuljetetaan esimerkiksi IP-paketteja ennalta määriteltyjen yhteyksien yli ilman, että tarvitsee tehdä reititystä.
Mp/s	*Miljoonaa pakettia per sekunti.* Tiedonsiirtonopeus mitattuna siirrettyjen pakettien määrällä sekunnissa.
MSTP	*Multiple Spanning Tree Protocol.* IEEE:n standardi 802.1Q-2005, luo oman STP-instanssin jokaiselle VLAN:ille.
OSI	*Open Systems Interconnection.* Malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PVST	*Per-VLAN Spanning Tree.* Jokaiselle VLAN:ille oman instanssin luova, Ciscon omistama versio STP-protokollasta.
PVST+	*Per-VLAN Spanning Tree+.* 802.1q standardia tukeva protokollaversio PVST:stä. Ciscon omistama.
QoS	*Quality of Service.* Palvelunlaatu, määritellään eri tasoihin verkkoliikenteen priorisoimiseksi.
RFC	*Request For Comments.* tyypillisesti IETF:n muistio Internetin standardeista ja protokollista.
RPVST	*Rapid Per-VLAN Spanning Tree.* Nopeamman liitäntälaitteiden verkkoon liittymisen mahdollistava protokollaversio PVST:stä. Ciscon omistama.
SAN	*Storage Area Network.* Erillinen verkko, jolla tuotetaan yhteys keskitettyyn tietosäilöön, esimerkiksi kovalevyyn.
SCSI	*Small Computer System Interface.* Sarja standardeja tietokoneiden ja liitännäislaitteiden yhteyttä ja tiedonsiirtoa varten.
SFP	*Small Form-Factor Pluggable -transceiver.* Liitin, jolla voidaan liittää esimerkiksi valokuitua liitintyypille tarkoitettuihin kytkinportteihin.

SLA	*Service-level Agreement.* Palvelutasosopimus, asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot.
STP	*Spanning Tree Protocol.* Verkkoprotokolla, joka varmistaa silmukattoman topologian kaikissa sillatuissa lähiverkoissa.
SVI	*Switch Virtual Interface.* Virtuaalinen portti, joka prosessoi VLAN:eja L3-tasolla.
TRILL	*Transparent Interconnect of Lots of Links.* L2-tason päällä toimiva protokolla, IETF:n standardi, joka yhdistää siltojen ja reitittimien hyödyt linkkitason reitityksessä.
VLAN	*Virtual Local Area Network.* Virtuaalinen lähiverkko, fyysisestä yhteydestä riippumaton looginen verkko.
VPN	*Virtual Private Network.* Tapa, jolla kaksi tai useampia verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisen yksityisen verkon.
VRRP	*Virtual Router Redundancy Protocol*. IETF:n HSRP:n pohjalta kehittämä standardi, kuvaillaan dokumentissa RFC 5798.
WAN	*Wide Area Network.* Laajaverkko, käytetään tässä työssä ainoastaan kuvaamaan yhteyttä Internetiin.

1 Johdanto

Tässä insinöörityössä on tarkoitus käsitellä konesaliverkon suunnittelua pienen asiakasyrityksen tarpeisiin. Työn alussa esitellään yleisesti eri verkkotekniikoita OSI-mallin (Open Systems Interconnection. Malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä tasossa) eri tasoilla ja käydään läpi yleisiä huomioon otettavia asioita konesaliympäristöistä ja niiden verkkosuunnitteluun vaikuttavista erityispiirteistä. Seuraavaksi käsitellään verkon nykytilannetta, yrityksen tarpeiden suhteuttamista ehdotettaviin laitehankintoihin ja vaatimuksia, jotka tulevat hankinnat asettavat yritykselle. Lopuksi esitellään vaiheittain verkon parannusta ja laajennusta käsittelevät suunnitelmat.

Insinöörityö tehdään Nemein Oy:lle, joka on kasvava ohjelmistotalo, joka erikoistuu web-pohjaisiin ratkaisuihin, sekä erilaisiin intranet- ja ekstranet-ratkaisuihin. [1.] Insinöörityöstä halutaan saada asiantuntevaa näkemystä erilaisista mahdollisista verkkoratkaisuista yrityksen omiin tarpeisiin. Työssä esitellyt suunnitelmat pohjautuvat sekä eri laitevalmistajien esittämiin suunnittelumalleihin että omaan työkokemukseen verkkojen parissa yli kolmen vuoden ajalta.

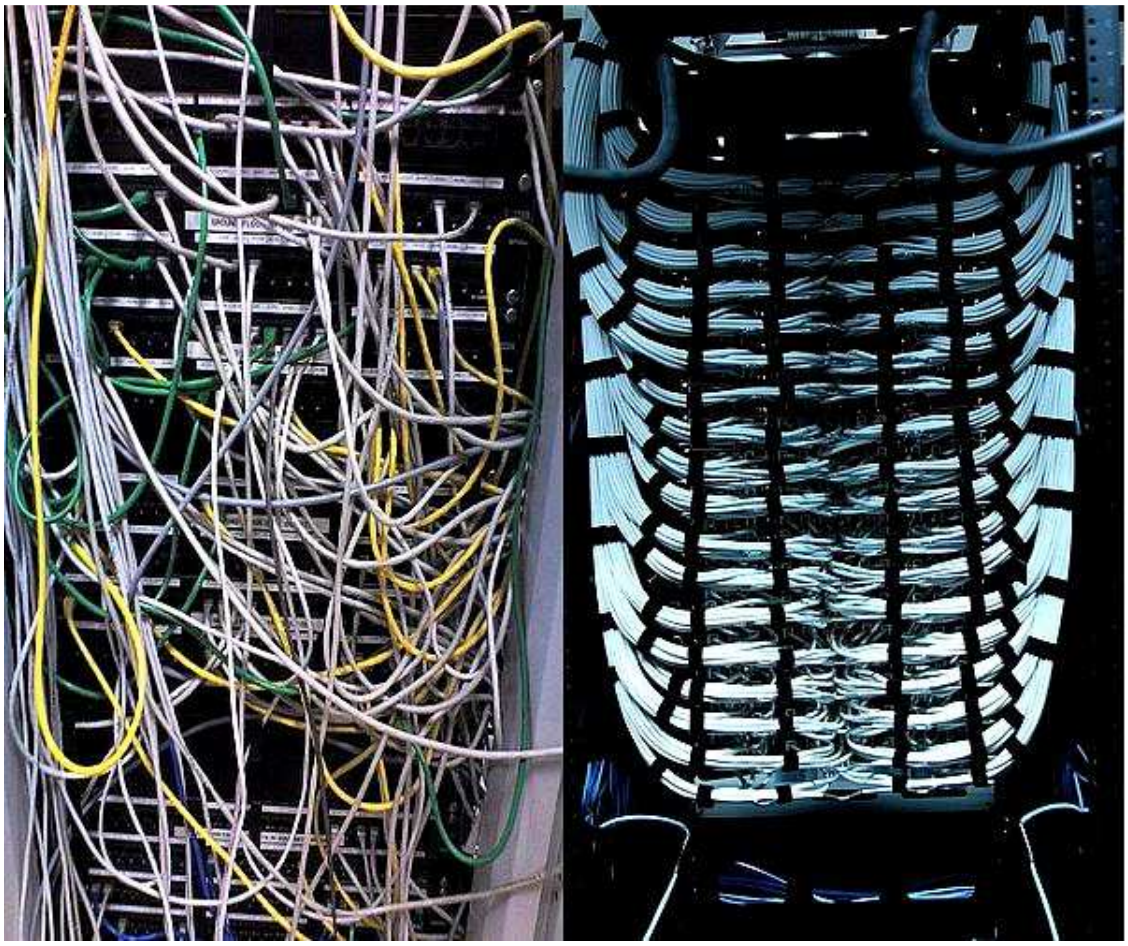
2 Verkkotekniikoiden teoria

2.1 Fyysisen tason kytkennät

Fyysisen tason kytkennät vaikuttavat suoraan laitevalintoihin, ja niitä harkittaessa tulee ottaa huomioon sekä kytkennässä tarvittava kapasiteetti että valitun median pituus. Kuparimediat eli nykyään pääasiassa Cat6-, Cat6a- ja Cat7- Ethernet-kaapelit hävittävät kuparin sähköisessä signaalissa aiheuttaman resistanssin takia dataa jo hyvinkin lyhyillä matkoilla. Cat eli kategoria on jaottelu, joka kuvaa parikaapelin laadukkuutta ja soveltuvuutta eri signalointinopeuksille. 10 Gb/s (Miljardia bittiä per sekunti) siirtonopeuksilla suurimmat mahdolliset etäisyydet suojaamattomilla kaapeleilla ovat 55 m/100 m (Cat6/Cat6a), ja tällöin puhutaan yksittäisestä kaapelista. Laitekaappikaappiin niputettuna kaapelit aiheuttavat häiriöitä myös toisilleen, jolloin mahdolliset kytkentäetäisyydet lyhenevät entisestään. Häiriöiden vaikutusta voi pienentää vähentämällä tarvittavien kytkentöjen määrää tai käyttämällä suojattuja kaapeleita, jotka taas vastaavasti tuottavat lisäkustannuksia. Kuparin häiriöalttiuden takia sitä pyritään käyttämään ainoastaan lyhyissä, laitekaapin sisäisissä kytkennöissä.

Toinen konesaliympäristössä mahdollinen kytkentämedia on valokuitu. Valokuidun hyviä puolia ovat sen häiriöttömyys ja korkea siirtokapasiteetti. Valokuidun huono puoli on sen herkkyys fyysiselle rasitukselle ja lialle. Kaapeli ei kestä juurikaan taitoksia tai vetorasitusta, ja pienikin määrä likaa kaapelin päässä saattaa estää optiikkaa toimimasta kunnolla. Lyhyillä, alle 300 metrin kytkentämatkoilla, ja vastaavasti konesaliympäristössä laitekaappien välillä ja pitkissä kytkennöissä laitekaappien sisällä käytetään yleisesti monimuotokuitua, kun taas vastaavasti pitkillä etäisyyksillä käytetään yksimuotokuitua. Yksimuotokuidulla voidaan tehdä kymmenien kilometrien pituisia, jopa 100 Gb/s nopeudella toimivia kytkentöjä. Tämän kapasiteetin kytkennät ovat tällä hetkellä pääasiassa operaattoreiden käytössä, joskin hiljalleen myös konesalien sisällä aletaan siirtyä vastaaviin kapasiteettivaatimuksiin. [2.]

Kun laitekaappi on kalustettu ja kytkentöjä aletaan tehdä, tulee asentajan ottaa huomioon hyvä kytkentätapa. Esimerkki hyvästä ja huonosta kytkentätavasta on nähtävissä kuvassa 1.



Kuva 1. Huono kytkentätapa esitettynä vasemmalla, hyvä oikealla. [3.]

Kytkentöjen sijoittelu tulee ottaa huomioon jo verkkoa suunnitellessa, jotta tulevat laajennukset voidaan toteuttaa purkamatta olemassa olevia kytkentöjä uusien liittämiseksi. Kaapelit tulee ohjata kytkentäkohdasta laitekaapin sivulle kaapelijohtimeen, ja mieluiten niputtaa yhteen sopivista kohdista. Kaapeleita käsitellessä tulee ottaa huomioon käyttöön valittu media, sillä valokuitu hajoaa herkästi. Kuparikaapelit kestävät hieman kovempaa käsittelyä, mutta niitäkään ei tule taivutella liian tiukoille mutkille. Kun kytkennät tuodaan kaapelijohtimesta seuraavaan kytkentäpisteeseen, toistetaan sama prosessi toisin päin. Tässä vaiheessa pyritään myös poistamaan mahdollinen liika pituus kaapeleista jättäen kuitenkin tarpeeksi vapaata kaapelia, jotta kytkinmoduuli voidaan poistaa kehikosta irrottamatta kaapeleita. [4, s. 46.]

2.2 Siirtoyhteystason kytkennät

L2-tason eli siirtoyhteystason kytkennät kehystävät ylempien OSI-mallin tasojen tietoliikennepaketit L1-tason eli fyysisen tason siirtoa varten. Tällä tasolla on myös mahdollista havaita ja tarvittaessa korjata fyysisellä tasolla ilmeneviä virheitä. L2-tasolla voidaan myös jakaa fyysisiä kytkentöjä omiin loogisiin kokonaisuuksiinsa VLAN:ien avulla. VLAN eli Virtual Local Area Network on virtuaalinen lähiverkko, fyysisestä yhteydestä riippumaton looginen verkko. Siirtotasolla laitteet tunnistavat toisensa fyysisten, 48-bittisten MAC-osoitteiden perusteella. MAC eli Media Access Control on fyysisen liitännän, esimerkiksi verkkokortin osoite. Kytkimet tallentavat tiedot MAC-osoitteiden sijainneista portti- ja VLAN-kohtaisesti CAM-taulukkoon ja ohjaavat jatkossa kyseiseen MAC-osoitteeseen kohdennetut paketit ulos siitä portista, josta kyseinen MAC-osoite on opittu. CAM on lyhenne sanoista Content Addressable Memory eli kyseessä on muisti, jossa haut tallennetulle datalle tehdään koko muistiin. [5.]

Jokainen VLAN muodostaa oman loogisen verkkonsa, jonka jäsenet voivat olla yhteydessä toisiinsa riippumatta niiden fyysisestä sijainnista. Näin voidaan säilyttää looginen kokonaisuus kullekin verkolle vaikka laitteiden sijainnit vaihtelisivat esimerkiksi asennushetkestä riippuen. Lisäksi tämä mahdollistaa yksinkertaisen redundanssin eri palveluita tarjottaessa. Mikäli palvelin A, jossa suoritetaan asiakkaan X palvelua Ö jää esimerkiksi sähkönsyöttöjärjestelmän vikaantumisen vuoksi virroitta, voi samassa VLAN:ssa, mutta eri laitekaapissa toimiva palvelin B omaksua sen roolin, kunnes palvelin A ja sen palvelut on jälleen saatu toimintakuntoon.

Kun portit jaetaan omiin toiminnallisiin ryhmiinsä, saadaan lisättyä myös verkon tietoturvaa. Tällöin kukin portti toteuttaa omaa toiminnallisuuttaan, eikä toisesta VLAN:sta ole ilman erillisiä toimia mahdollista kommunikoida toiseen. Tietyissä tilanteissa voidaan haluta eri VLAN:ien voivan kommunikoida keskenään, ja tällöin jossain verkon pisteessä luodaan L3-tasolla eli verkkotasolla reitti kahden VLAN:n välille, ja rajoittaa edelleen laitteiden välistä kommunikaatiota erillisillä pääsylistoilla.

Hyvä tapa määritellä verkkoon tarvittavat VLAN:t on valita jokaiselle toiminnallisuudelle yksi satunnainen VLAN, ja näiden lisäksi ottaa yksi tyhjä VLAN käytettäväksi vapaille porteille. Kehystyksessä käytetään yleisesti IEEE:n standardia 802.1q. IEEE tarkoittaa Institute of Electrical and Electronics Engineersiä, joka on kansainvälinen tekniikan alan järjestö. [6; 7.]

Kun tehdään redundanttisia kytkentöjä yhteyksien varmistamiseksi, tarvitaan jokin mekanismi varmistamaan, etteivät kahdennetut yhteydet aiheuta silmukoita, joihin paketit jäävät kiertämään. Tähän tarkoitukseen käytetään yleisesti STP-protokollaa, joka on IEEE:n standardi 802.1d. Spanning Tree Protocol on verkkoprotokolla, joka varmistaa silmukattoman topologian kaikissa sillatuissa lähiverkoissa. Protokolla laskee tunnisteen jokaiselle linkille, joka muodostuu linkin nopeuden arvosta sekä erikseen määritellystä tunnisteesta. Näiden perusteella pienimmän tunnisteen saanut linkki valitaan juureksi, jonka perusteella muodostetaan linkkien lopullinen topologia. Koska erillisen tunnisteen voi määritellä käsin, on tärkeä valita juurilinkki laitteesta, joka on mahdollisimman lähellä verkon runkoa, ja suuren kapasiteetin linkkejä. Kun juuriportti on määritelty, laskevat kaikki linkit arvot matkalla juuriportille kaikilla mahdollisilla reiteillä, joista ne valitsevat pienimmän arvon saavat ja sulkevat muut. Näin varmistetaan, ettei topologiassa ole loogisia silmukoita, ja mahdollistetaan redundanttisten linkkien olemassaolo.

Koska STP jättää käyttämättä osan mahdollisista poluista, verkon kapasiteettia menee väistämättä hukkaan. STP:stä on kuitenkin olemassa eri versioita, jotka mahdollistavat yhden STP-instanssin yhtä VLAN:a kohden. Verkkolaitevalmistaja Ciscolla on kolme omaa malliaan, PVST, PVST+ ja RPVST. Per-VLAN Spanning Tree on jokaiselle VLAN:ille oman instanssin luova, Ciscon omistama versio STP-protokollasta. Per-VLAN Spanning Tree+ on myös Ciscon omistama, erona tavalliseen on tuki 802.1q standardille. Rapid Per-VLAN Spanning Tree on myös Ciscon omistama, nopeamman liitäntälaitteiden verkkoon liittymisen mahdollistava protokollaversio PVST:stä. Suurin osa muista laitevalmistajista ei tue näitä, vaan ne käyttävät IEEE:n standardia 802.1s (myöhemmin sisällytetty standardiin 802.1q-2005), MSTP. Multiple Spanning Tree Protocol on IEEE:n standardi 802.1Q-2005, joka luo oman STP-instanssin jokaiselle VLAN:ille.

MSTP:llä voidaan luoda useita STP-alueita, jotka voidaan yhdistää yhdeksi yleiseksi STP:ksi, CST:ksi eli Common Spanning Tree:ksi, joka on useat STP-instanssit yhdistävä STP, osa MSTP:tä. Näin saadaan käyttöön sekä topologian redundanttisuus, että koko kapasiteetti. [8.]

Laajoissa konesaliympäristöissä L2-taso saattaa kasvaa hyvinkin suureksi, joka muodostaa omia ongelmiaan. MAC-osoitteita on niin paljon, että se muodostuu ongelmaksi, ja sen ympärille on kehitetty erilaisia ratkaisuita, joista tässä yhteydessä mainittakoon esimerkkeinä Brocaden TRILL-protokollaan perustuva ratkaisu ja Juniperin oma QFabric. TRILL eli Transparent Interconnect of Lots of Links on L2-tason päällä toimiva protokolla, IETF:n standardi, joka yhdistää siltojen ja reitittimien hyödyt linkkitason reitityksessä. Molemmat protokollat käsittelevät MAC-osoitteita kuin L3-tason IP-osoitteita eli niitä reititetään, joka mahdollistaa useiden eri linkkien käytön ohjattaessa paketteja lähettäjältä vastaanottajalle. Internet Protocol eli IP on L3-tason tiedonsiirtoprotokolla. [9; 10; 11; 12.]

2.3 Verkkotason kytkennät

L3-tasolla kytkennät tapahtuvat IP-osoitteiden perusteella. Toisin kuin L2-tasolla, jossa liikenne tapahtuu verkon sisällä, L3-tasolla liikennöidään eri verkkojen välillä, eli reititetään paketteja. Konesaliympäristössä L3-tason protokollia tarvitaan välittämään liikennettä ulkoverkon ja palvelimien välillä, laitteiden etähallintaan sekä mahdollisesti L2-verkkojen väliseen kommunikointiin. Palveluntarjoajan tulisi mainostaa asiakkaille laitekaappeihin asti ainoastaan oletusreitti kohti ulkoverkkoa ja varmistaa, etteivät eri asiakasverkot pääse kommunikoimaan keskenään niin, että paketit ohittavat palomuurin.

Lisäksi voidaan lisätä verkkokytkentöjen redundanssia käyttämällä protokollia kuten Ciscon omistama HSRP tai yleinen standardi VRRP. Hot Standby Routing Protocol on Ciscon omistama redundanssi-protokolla, jonka avulla luodaan vikasietoinen oletusyhdyskäytävä liitäntälaitteille.

Sen pohjalta on kehitetty Virtual Router Redundancy Protocol, joka on IETF:n HSRP:n pohjalta kehittämä standardi, joka kuvaillaan dokumentissa RFC 5798. IETF eli Internet Engineering Task Force on internet-protokollien standardoinnista vastaava organisaatio, ja RFC on Request For Comments-nimellä kulkeva dokumenttityyppi jota IETF käyttää protokollia kehittäessään. Tällöin L3-tason liikennettä välittävät laitteet mainostavat yhdessä virtuaalista oletusyhdyskäytävää (default gateway) kyseiseen verkkoon kuuluville laitteille, jolloin linkin katketessa sillä hetkellä liikennettä välittävälle laitteelle varalla oleva laite omaksuu liikennettä välittävän roolin. Kuten STP, tämäkin muodostaa kapasiteettihäviötä, mikäli vain yhtä laitetta käytetään liikenteen välittämiseen. Kummassakin edellä mainitussa protokollassa on mahdollista jakaa verkkoja eri prioriteeteille, jolloin varmistetaan koko käytössä olevan kapasiteetin hyödyntäminen. [13; 14.]

L3-tasolla päätetään myös pakettien ohjaamisesta QoS-tasojen mukaisesti. Quality of Service eli palvelunlaatu määritellään eri tasoihin verkkoliikenteen priorisoimiseksi. QoS:a hyväksikäyttämällä voidaan määrittää korkeamman prioriteetin paketeille etuoikeus käyttää kaistaa muuhun liikenteeseen verrattuna. Sitä voidaan käyttää myös ylimyytäessä kapasiteettia, jolloin ruuhka-aikana heikomman tason palveluun kuuluvat paketit saatetaan pudottaa jonosta kokonaan. QoS:n avulla voidaan myös varmistaa, että hallintayhteyksille ja esimerkiksi HSRP:n ylläpitoviesteille on aina varattuna riittävä määrä kapasiteettia, riippumatta muun verkon kuormituksesta. Tällä estetään turhat verkon konvergoitumiset tilanteessa, jossa ylläpitoviestit eivät pääse jonosta läpi ja varalla oleva laite tulkitsee primäärilaitteen kadonneen verkosta. [15.]

L3-tasolle luodaan ACL:ejä eli Access Control List:ejä, verkon pääsylistoja, joilla määritellään tarkemmin eri verkkoelementtien oikeuksia kommunikoida toisilleen. Voi ilmetä tarve reitittää kahden VLAN:n liikennettä keskenään, esimerkiksi mahdollistamaan palvelinten kommunikointi tietokantaan tai tiedostopalvelimelle. Mikäli tietoturvataso halutaan pitää hyvänä, tulisi ACL:n määritellä tarkasti, mistä verkon A IP–osoitteista on luvallista kommunikoida verkon B tiettyihin osoitteisiin ja tarvittaessa toisin päin. Tällä varmistetaan, ettei mikään ylimääräinen laite pääse olemaan yhteydessä minnekään, mihin sen ei pitäisi. ACL:t voidaan luoda hyvinkin täsmällisesti, jolloin sallittu liikenne rajoitetaan tiettyihin, erikseen määriteltyihin portteihin.

Tällöin liikenteen suodatusta korotetaan tarvittaessa kuljetustasolle (jatkossa L4-taso). Pääsylistoja voidaan luoda tarvittaessa myös L2-tasolle, jolloin suodatus tapahtuu MAC-osoitteiden perusteella. [16.]

2.4 Storage Area Network

SAN eli Storage Area Network on erillinen verkko, jolla tuotetaan yhteys keskitettyyn tietosäilöön, esimerkiksi kovalevyyn. Sitä käytetään pääasiassa tekemään erilaisista tallennusmedioista palvelimille saatavilla olevia siten, että ne näyttävät olevan käyttöjärjestelmän kiinteitä osia. Käyttöjärjestelmät ylläpitävät omia tiedostojärjestelmiään omilla loogisilla levyillään, aivan kuten ne olisivat paikallisia niille itselleen. Näiden loogisten yksiköiden jakaminen eri palvelinten kesken ei onnistu ilman korkeamman tason ratkaisuja, kuten SAN-tiedostojärjestelmiä. Ongelmista huolimatta SAN:it helpottavat datakapasiteetin käyttöä, sillä useat palvelimet keskittävät oman tallennustilansa levypakoille. Yleisiä käyttötarkoituksia SAN:ille ovat nopeaa kahdensuuntaista liikennettä kovalevyille vaativat järjestelmät, kuten tietokannat, sähköpostipalvelimet ja paljon käytetyt tiedostopalvelimet. SAN:ien hyviä puolia ovat muun muassa tallennustilan hallinnan yksinkertaistuminen ja joustavuus, sillä kaapeleita ja tallennusmedioita ei tarvitse siirtää kun tallennustila siirretään palvelimelta toiselle. Muita hyötyjä ovat esimerkiksi palvelinten mahdollisuus käynnistyä suoraan SAN:sta. Tämä mahdollistaa nopean ja helpon vikaantuneiden palvelimien vaihdon, sillä SAN voidaan konfiguroida niin, että uusi palvelin voi käyttää vikaantuneen palvelimen loogista yksikköä.

SAN:it mahdollistavat myös tehokkaamman kriittisestä vauriosta palautumisen. SAN voidaan levittää kauas toisesta tallennustilasta, joka mahdollistaa tallennustilan kahdennuksen, esimerkiksi FCIP:llä, siinä missä perinteinen fyysinen SCSI tuki ainoastaan muutaman metrin etäisyyksiä. SCSI eli Small Computer System Interface on sarja standardeja tietokoneiden ja liitännäislaitteiden yhteyttä ja tiedonsiirtoa varten. FCIP tarkoittaa Fibre Channel over IP:tä, jossa SAN-verkkojen tiedonsiirtoprotokollan kerrostetaan IP:n päälle. SAN:a käytetään yleisesti FC-teknologian avulla.

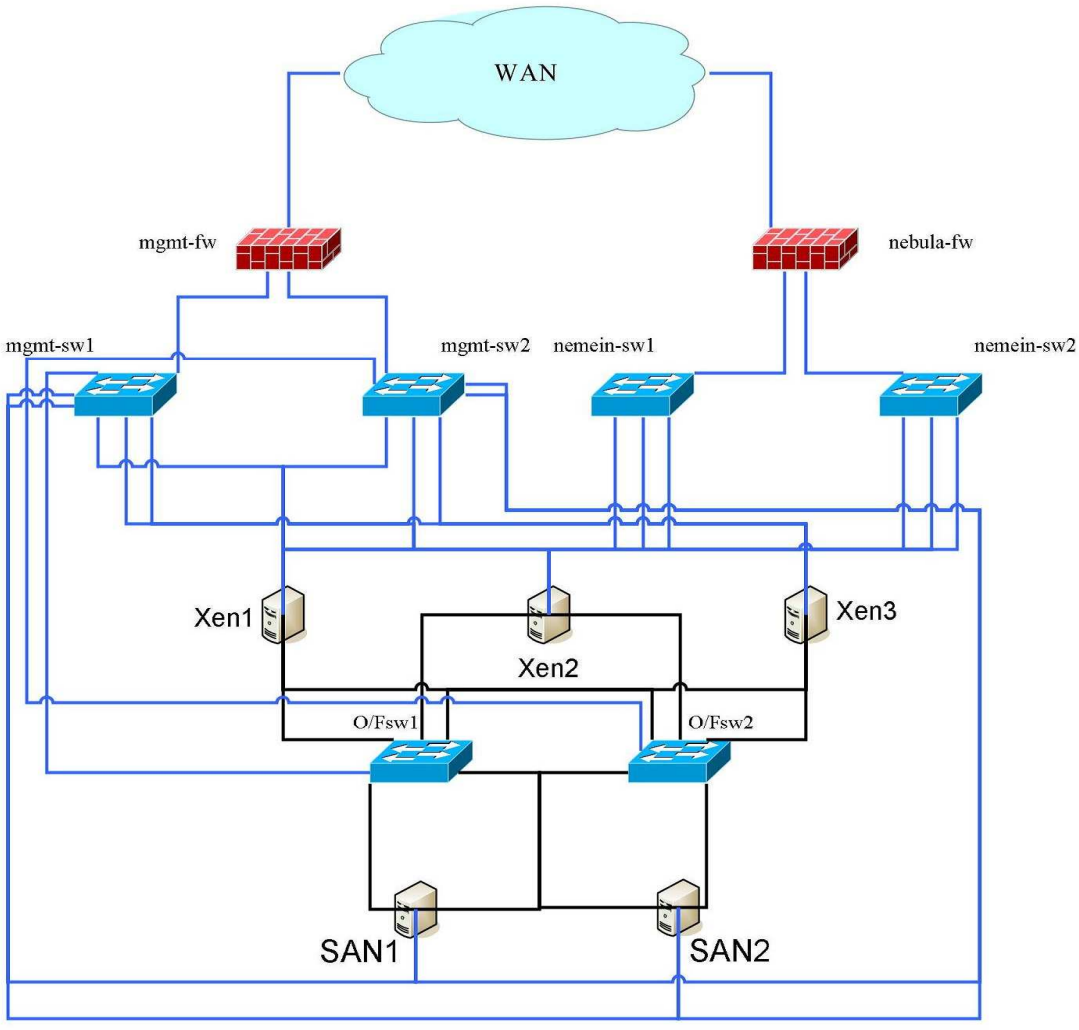
FCP on TCP:tä IP-verkoissa vastaava siirtoprotokolla, joka siirtää SCSI-komentoja FC-verkkojen yli. Fibre Channel on SAN-verkkojen tiedonsiirtoprotokolla, vastaa TCP:tä IP-verkoissa, välittää SCSI-komentoja Fibre Channel-verkkojen yli. Se käyttää Fibre Channel Protokollaa, joka on protokolla Fibre Channel-tekniikan alla. [17; 18; 19.]

2.5 Muita konesalien verkkojen erityispiirteitä

Suunniteltaessa verkkoa konesaliympäristöön tulee muutamia toimistoverkoista poikkeavia erityispiirteitä ottaa huomioon. Ensimmäinen syy valita konesaliympäristö palvelimien sijoituspaikaksi on niiden tarkoituksenmukainen suunnittelu. Konesaleissa on kiinnitetty erityistä huomiota sekä virransyötön että riittävän jäähdytyksen varmistamiseksi kaikissa tilanteissa. Tämä tarkoittaa tiettyä tapaa, jolla kytkennät tulee kussakin ympäristössä suorittaa, riippuen konesalin suunnittelusta. Lattia voi esimerkiksi olla korotettu, jolloin kullakin laitekaapilla on tietty maksimipaino, jota siihen kytkettävät laitteet eivät saa ylittää. Jäähdytyksen ja virransyötön toteutuksen mukaan kukin laitekaappi saattaa olla rajoitettu myös suurimman sallitun tehon suhteen. Lisäksi tulee ottaa huomioon verkon kapasiteetin rajoitukset sekä konesalin sisällä että liikenteessä ulkoverkkoon. [3, s. 11–13; s. 26–27.] Verkon suunnittelussa tulee ottaa huomioon verkkoon asennettavien järjestelmien, palvelimien ja levyjärjestelmien, erityispiirteet. Tässä työssä asiakkaan fyysiset palvelimet kahdentavat virtuaalipalvelimien osalta toisiaan ja luovat oman virtuaalisen verkkonsa tätä varten. Tämän verkon toimintaa voidaan tukea tietyillä verkon piirteillä, joita on esitelty jo aiemmin, kuten verkkojen jakamisella omiin loogisiin osiinsa, VLAN:ihin, täyden kapasiteetin paremmaksi hyödyntämiseksi ja liikenteen erottamiseksi ulkoverkkoon suuntautuvasta asiakasliikenteestä. Tämän lisäksi asiakas tuottaa joitakin vasteaikatasoltaan kriittisiä järjestelmiä, joiden jatkuva saatavuus ja nopea palautuminen mahdollisista virhetilanteista on äärimmäisen tärkeää. Tätä ajatellen verkon olisi hyvä sisältää mahdollisimman paljon redundanssia lisääviä komponentteja ja tekniikoita, kuten aiemmin mainitut VRRP ja HSRP, ja kaikkien yhteyksien kahdentamisen.

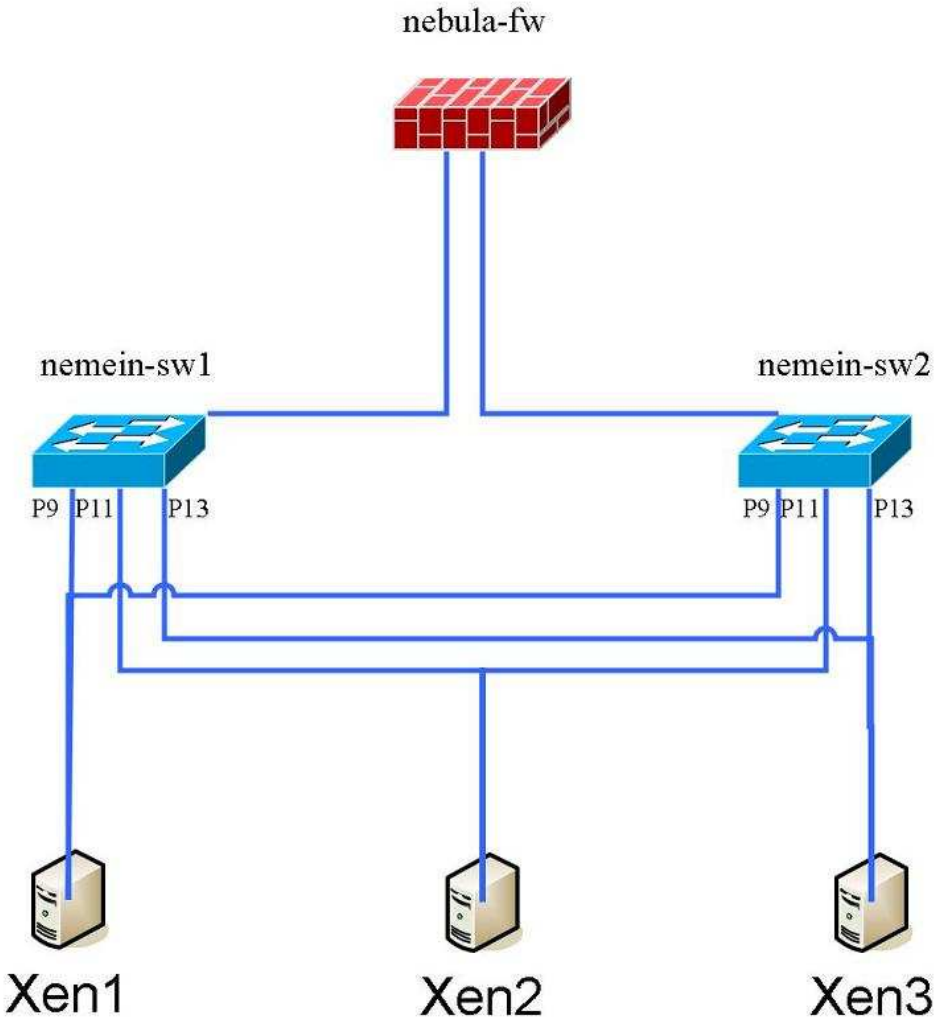
3 Asiakkaan järjestelmän asennus konesaliin

Työn ensimmäinen vaihe oli asiakkaan järjestelmän asennus konesaliin syksyllä 2011, ja tämän toteutuksen verkon suunnittelusta vastasi kolmas osapuoli. Järjestelmä sisälsi kolme Xen-palvelinta, kaksi SAN-kehikkoa, neljä hallitsematonta Hewlett Packardin 1410-kytkintä, ja kaksi Brocaden 300-sarjan SAN-kytkintä, ja hallintayhteyksiä varten ZyXEL ZyWALL USG 20-palomuuri. Laitekaapin kaikki L1-kytkennät ilman porttitietoja ovat nähtävissä kuvassa 2.



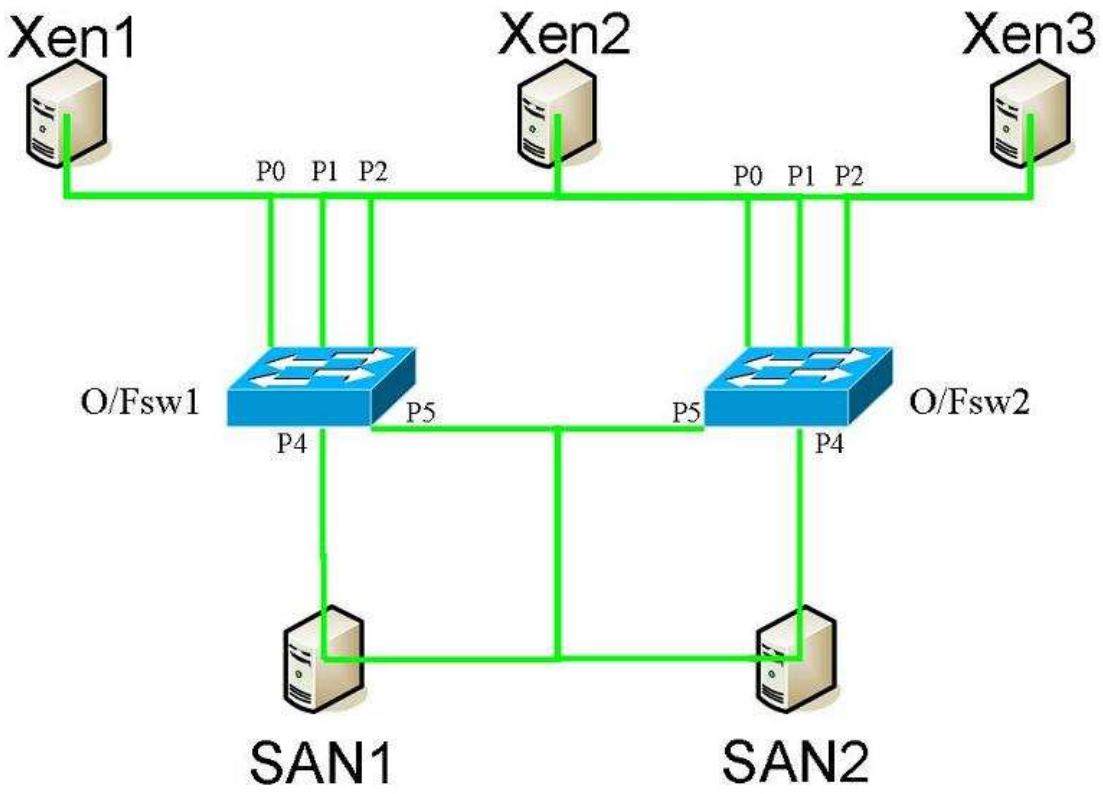
Kuva 2. Laitekaapin L1-tason kytkennät

Laitteiden yhteys WAN-verkkoon kytkettiin palveluntarjoaja Nebulan kytkimeen, josta yhteys ohjattiin palveluntarjoajan palomuurialustalle. WAN eli Wide Area Network on yhteys laajaverkkoon, tässä työssä käytetään kuvaamaan yhteyttä julkiseen verkkoon. Nebulan kytkin on kuvien yksinkertaistamiseksi jätetty pois kuvista. Palvelimet pyörittävät joukkoa virtuaalipalvelimia, joiden kaikkien yhteydet ohjataan palvelinten fyysisistä verkkoliitännöistä ulkoverkkoon. WAN-verkkoon välitettävien yhteyksien L1-kytkennät ovat nähtävillä kuvassa 3, mukana ovat porttitiedot kytkinten osalta.



Kuva 3. WAN-yhteyksien L1-kytkennät

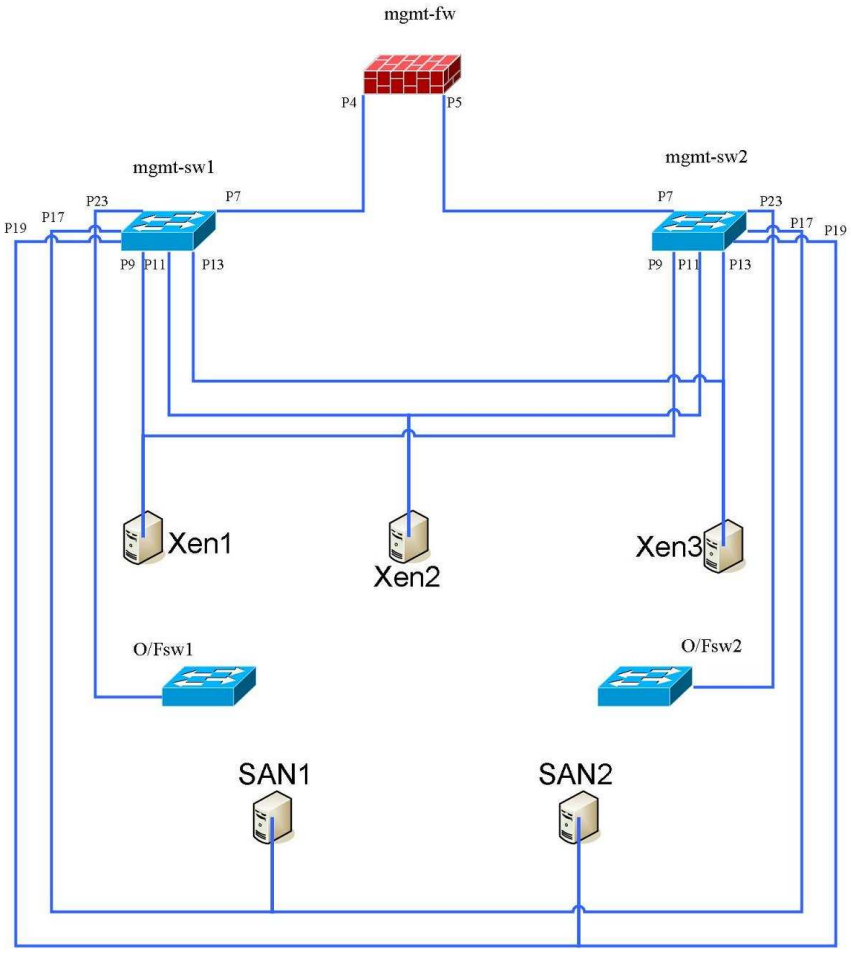
Palvelimet ja SAN-kehikot asennettiin kaapin pohjalle ja verkkolaitteet toistaiseksi niiden päälle. SAN-verkon L1-kytkennät ovat nähtävillä kuvassa 4, porttitiedot ovat merkittynä kytkinten osalta.



Kuva 4. SAN-verkon L1-tason kytkennät

Verkkolaitteet oli lopulta tarkoitus sijoittaa laitekaapin yläosaan, kun loput palvelimet saataisiin asennettua. Ongelma verkkolaitteiden väliaikaisessa sijoituksessa keskelle laitekaappia on kaapelointi. Mikäli laitteet olisi asennettu oikeille paikoilleen heti aluksi, lisälaitteiden kaapelointi olisi ollut helpompi ohjata kaapelijohtimiin laitekaapin reunoilla ja alkuperäiset kytkennät olisi voinut mitoittaa sopiviksi välittömästi asennuksen yhteydessä.

Toinen ilmeinen ongelma muodostuu verkkolaitevalinnoista, joita kolmas osapuoli oli suositellut asiakkaalle hankittavaksi. Hallitsemattomat kytkimet eivät mahdollista täyttä redundanssia L1- ja L2–tasoilla, eikä niiden avulla ole mahdollista ottaa käyttöön tietoturvaa ja saatavuutta parantavia konfiguraatioita. Lisäongelma on SAN-kytkimien puutteelliset hallintaverkon liittimet, sillä laitteissa on ainoastaan yksi FastEthernet-portti hallintayhteyksiä varten. Ongelmaa on mahdollista pienentää lisäämällä LAN-verkkojen 802.1q-trunkkia vastaavan, SAN-verkoissa käytetyn ISL-trunkin, eli kahden SAN-kytkimen välisen Inter-Switch Linkin kytkimien välille tai käyttämällä tätä linjaa IPoFC-protokollan (IP-protokollan kerrostus FC:n päälle.) avulla laitteen toissijaisena hallintayhteytenä. L1-tason hallintayhteyksien kytkennät ovat nähtävillä kuvassa 5.



Kuva 5. Hallintayhteyksien L1-tason kytkennät

Kolmas ongelma ilmeni palveluntarjoajan kytkimen suhteen. Vaikka laitteen virransyöttö oli kahdennettu, laite itsessään oli Ciscon C2960G-työryhmäkytkin, jolloin pienikin laiterikko, esimerkiksi varavirtalähteen tai tuulettimen hajoaminen, tarkoittaa automaattisesti kaikkien yhteyksien katkeamista huollon ajaksi.

4 Verkon suunnittelu

4.1 Ensimmäinen vaihe

4.1.1 Suositukset laitehankinnoista

Verkon tietoturvaa, hallittavuutta ja kapasiteettia parantaakseni otin lähtökohdaksi verkkosuunnittelulle laitehankinnat. Ehdottomalla etukäteen mahdollisia laitemalleja ja niihin perustuvia ratkaisuja on asiakkaan helpompi saada ilman laajaa verkkotietämystä kuva vaadittavista muutoksista. Ryhmittelin ehdottamani laitteet ominaisuuksien mukaan, jonka jälkeen tein verkkosuunnitelmat kullekin ehdotukselle.

Mikäli L3-tason ominaisuudet halutaan jättää käyttämättä (mm. HSRP, VRRP, SVI), on suositeltavaa päivittää kaikki kytkimet kahteen tai useampaan seuraavista kahdesta mallista: Cisco Nexus 5010 tai Brocade 8000. SVI eli Switch Virtual Interface on virtuaalinen portti, joka prosessoi VLAN:eja L3-tasolla.

Ciscon Nexus-kytkimen L2-tason välityskapasiteetti on 520 Gb/s tai 386,9 Mp/s (miljoonaa pakettia per sekunti). [20.]

Brocaden 8000-kytkimestä ei valmistajan sivuilla ollut välityskapasiteettitietoja, mutta kapasiteetin pitäisi olla samaa luokkaa Nexuksen kanssa. Niputettaessa portteja laitteella on mahdollista saavuttaa 128 Gb/s välitysnopeus kytkimeltä kytkimelle ja 40 Gb/s välitysnopeus palvelimelle. [21.]

Mikäli L3-tason ominaisuuksia halutaan ottaa käyttöön, voidaan Brocaden 300-sarjan SAN-kytkimet jättää välittämään SAN-verkon liikennettä, ja tällöin voidaan keskittyä LAN-kytkimiin. Tällöin hyviä vaihtoehtoja ovat esimerkiksi Ciscon 3750-X -sarjan tuotteet, Alcatel-Lucentin OmniSwitch 6850- ja 6855-kytkimet, tai Juniper Networksin EX4200-kytkimet.

Kaikkien laitteiden välityskyky on noin 101 Mp/s, joka on noin kolminkertainen tämän hetkisiin HP:n hallitsemattomiin kytkimiin verrattuna. Kaikissa malleissa on 48 porttia ja moduulipaikka erilaisille lisäporteille, esim. 10 Gb/s SFP-porteille. SFP eli Small Form-Factor Pluggable -transceiver on liitin, jolla voidaan liittää esimerkiksi valokuitua liitintyypille tarkoitettuihin kytkinportteihin.

Laitteiden hintataso vapailla markkinoilla on samaa luokkaa kaikilla valmistajilla. Kaikki mallit ovat pinottavia, joten kapasiteettia voi tarvittaessa päivittää lisäämällä uuden kytkimen pinoon. Pinojen suurimmat mahdolliset koot vaihtelevat valmistajien välillä, Ciscon laitteita voi pinota yhdeksän, Alcatelin kahdeksan, ja Juniperin kymmenen. Kaikki pinot käyttäytyvät yhtenä kytkimenä, johon voidaan lisätä ja poistaa laitteita tarpeen mukaan. Mikäli päälaite hajoaa, otetaan jokin toinen laite korvaamaan sen toimintaa. [22; 23; 24.]

Mikäli pelkkä hallittava L2-taso riittää, hyviä vaihtoehtoja on tarjolla kaikilta valmistajilla. Laitteiden hintataso vapailla markkinoilla on noin puolet monitasokytkinten hinnoista, ja pakettien välityskyky on samalla tasolla. Ciscolla paras vaihtoehto on 2960S-sarja, Alcatelilla 6400, ja Juniperilla EX3200. Nämä kytkimet eivät enää ole pinottavia, joten kytkimien lisäysmahdollisuus ja modulaarisuus heikkenee suorassa suhteessa hinnan mukana. Lisäksi näihin malleihin ei ole saatavilla 10 Gbps-linkkejä, toisin kuin monitasokytkinmalleihin. [25; 26; 27.]

Brocaden 300-sarjan kytkimissä oli asennushetkellä käytössä ainoastaan kahdeksan portin lisenssi, joten niissä on laajennusvaraa vielä 16 portin verran. Välityskyvyn pitäisi riittää pelkkää SAN–verkon liikennettä varten. Jos hallittavuutta halutaan parantaa, ensimmäisinä mainitut Ciscon Nexus 5010- ja Brocaden 8000-kytkimet tarjoavat mahdollisuuden käyttää FCoE-tekniikkaa eli Fibre Channel over Ethernetiä, jossa Ethernet-kehystyksen päällä kuljetetaan Fibre Channel protokollan dataa uusien SAN-laitteiden kytkemiseksi muihinkin kuin FC-portteihin.

Tämän lisäksi nämä kytkimet mahdollistavat SAN-verkon laajennuksen muihin konesaleihin FCIP-tekniikan avulla, ja ne voidaan kytkeä osaksi muuta kytkinverkkoa.

4.1.2 VLAN-suunnitelma ja verkkokuvat

Suunniteltaessa VLAN:eja on tietoturvan kannalta parasta valita VLAN:ien numerotunnisteet satunnaisesti. Tämän lisäksi on suositeltavaa luoda vähintään yksi ylimääräinen VLAN vapaiksi jääviä kytkinportteja varten. 802.1q-kehystystä on hyvä käyttää aina kuin mahdollista. Muuten VLAN:eja voidaan luoda tarpeen mukaan lisää. Tämän työn yhteydessä ei alustavasti ole verkon osalta tarvetta kuin kahdelle VLAN:ille, WAN-yhteyksien ja hallintayhteyksien välittämiseen. VLAN-suunnitelma on nähtävillä taulukossa 1. Käytetyt IP-alueet ovat esimerkkejä, ja ne tulevat käyttöön ainoastaan tapauksessa, jossa asiakas valitsee monitasokytkimet korvaaviksi laitteiksi.

Taulukko 1. VLAN-suunnitelma

VLAN	VLAN ID	IP-verkko	Aliverkon maski
inet	83	160.43.42.0	255.255.255.128
mgmt	107	10.50.12.0	255.255.255.0
dummy-port	401	-	-

VLAN:ien nimet on hyvä valita kuvaavasti, jottei laitteita konfiguroidessa joudu turvautumaan selventäviin dokumentteihin jokaisella kerralla. Seuraavana on esimerkkejä eri VLAN:ien käytöstä eri porteissa Ciscon IOS-käyttöjärjestelmässä. Esimerkkikonfiguraatio 1 on WAN-liikenteelle määritetty portti. Tähän porttiin voidaan kytkeä esimerkiksi uusi palvelin.

```
interface GigabitEthernet0/3
 description inet-connection
 switchport
 switchport mode access
 switchport access vlan 83
end
```

Esimerkkikonfiguraatio 2. inet-VLAN portti.

Esimerkkikonfiguraatio 2 on vapaasta portista, joka on merkitty käyttämään tyhjää VLAN:a. Vaikka portin sulkeva *shutdown*-komento jäisi epähuomiossa pois, tämän tyhjän VLAN:n avulla ei pysty liikennöimään tuotannossa oleviin verkkoihin. Lisäksi tämän VLAN:n liikenne ei ole sallittua trunk-linkkien kautta, joten yhteydet rajautuvat edelleen ainoastaan kytkimelle, josta potentiaalinen tunkeutuja on löytänyt avonaisen portin.

```
interface GigabitEthernet0/12
 description FREE PORT
 switchport
 switchport mode access
 switchport access vlan 401
 shutdown
end
```

Esimerkkikonfiguraatio 2. Vapaa portti.

Esimerkkikonfiguraatio 3 on trunk-linkki kytkimeltä kytkimelle. Liikenne kehystetään, ja ainoastaan VLAN:ien 83 ja 107 liikenne sallitaan linkin kautta. Portteja voidaan myös niputtaa yhteen, jolloin luodaan yksi virtuaalinen portti, jonka kapasiteetti vastaa kaikkien nipussa olevien porttien kapasiteettia. Ciscon kytkimissä tätä virtuaalista porttia kutsutaan nimellä Port-Channel, jonka esimerkki seuraavaksi.

```
interface GigabitEthernet0/48
 description link to nemein-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 83,107
 switchport mode trunk
end
```

Esimerkkikonfiguraatio 3. Trunk-linkki.

Ensimmäisenä luodaan virtuaalinen porttikanava, jolle annetaan tässä tapauksessa tunnistenumeroksi 1. Se esitetään esimerkkikonfiguraatiossa 4.

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk encapsulation dot1q
switch(config-if)# exit
```

Esimerkkikonfiguraatio 4. Virtuaalinen porttikanava.

Tämän jälkeen valitaan joukko fyysisiä portteja, jotka liitetään luodun virtuaalisen kanavan ryhmään ja asetetaan trunk-linkeiksi. Esitetty esimerkkikonfiguraatiossa 5.

```
switch(config)# interface range GigabitEthernet0/41-48
switch(config-if-range)# channel-group 1 mode on
switch(config-if-range)# switchport
switch(config-if-range)# switchport trunk encapsulation dot1q
switch(config-if-range)# switchport mode trunk
switch(config-if-range)# end
```

Esimerkkikonfiguraatio 5. Porttien liittäminen osaksi porttikanavaa

Kaikkia edellä esimerkein esitettyjä kytkentätapoja esiintyy suunnittelun ensimmäisen vaiheen verkkokuvissa. Päätelaitekytkennät toimivat yhden VLAN:n porttikonfiguraatioilla, ja verkkolaitteiden välisissä linkeissä käytetään joko yksinkertaisia trunk-linkkejä, tai niputettuja, virtuaalisia Port-Channeleita. Tämän lisäksi kuvissa on otettu huomioon SAN-verkko, ja sen tarvitsemat erilliset kytkennät.

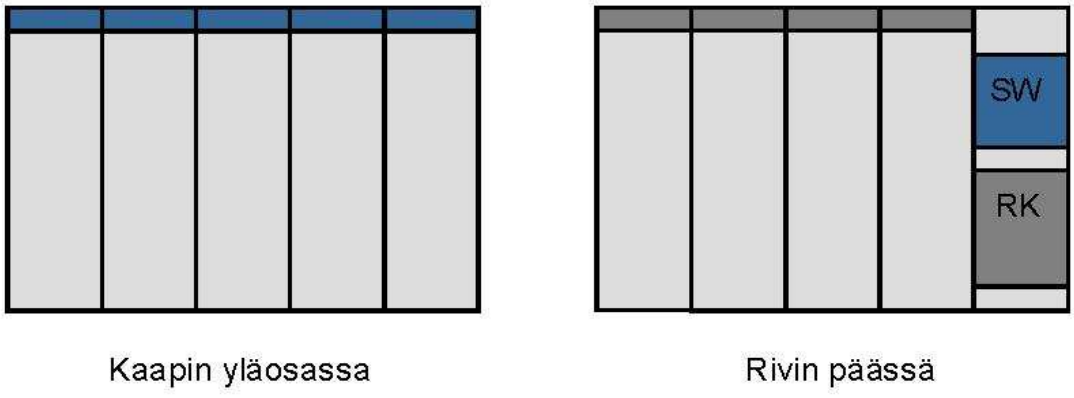
Liitteissä 1 ja 2 kuvatuissa kytkennöissä käytetään jo olemassa olevia Brocaden 300-sarjan SAN-kytkimiä, joista liitteessä 1 vaihtoehdoksi esitetään hallittavia L2-kytkimiä ja liitteessä 2 sekä L2- että L3-tason monitasokytkimiä. Molemmissa liitteissä on yhteistä kahden fyysisen kytkimen vähennys laitekaapista. Liitteessä 3 esitellään kolmas ehdotus, jossa kaikki kuusi kytkintä korvataan kahdella sekä L2-tason Ethernet:iä että FC:a ymmärtävillä laitteilla. Asiakkaalle esitetyt laitevaihtoehdot ovat luvussa 4.1.1.

Ensimmäisen vaiheen tarkoituksena on ensisijaisesti joko mahdollistaa tai parantaa verkon hallintaa sekä lisätä redundanssia ja tietoturvaa. Ehdotetut laitteet ja niiden konfiguraatiot ovat tarpeeksi yksinkertaisia siihen, että kouluttautumalla oman ydinosaamisalueen ulkopuolelle asiakkaan on vielä mahdollista ylläpitää verkkoa ja sen laitteita itsenäisesti. Tämän lisäksi laitteiden hintataso on niin alhainen, että asiakkaan ei vielä tarvitse investoida suuria summia saavuttaakseen hyvän lähtötason seuraavalle suunnitteluvaiheelle. Malli antaa hyvän lähtökohdan seuraavien suunnitteluvaiheiden verkkojen ja niiden laitteiden hankintojen, sekä vaativamman osaamisen kartoitukselle, jotka verkon laajentuminen aiheuttaa.

Koska asiakkaalla ei kuitenkaan ole asiantuntemusta verkoista, verkkolaitteista tai verkkotekniikoista, eikä asiakkaan liiketoiminta suuntaudu verkkoihin, koko verkon hallinnan ja ylläpidon ulkoistaminen on varteenotettava vaihtoehto jo tässä vaiheessa. Tällöin asiakas voi keskittyä palvelimien ja niiden ylläpitämien palveluiden ylläpitoon ja jättää verkon toisen osapuolen vastuulle.

4.2 Toinen vaihe

Verkon laajennuksen toisessa vaiheessa verkkoa kasvatetaan sivusuunnassa konesalin sisäisesti ottamalla käyttöön lisää laitekaappeja. Kun verkko laajentuu huomattavasti sivusuunnassa, hallittavien verkkolaitteiden määrä lisääntyy tarpeettoman suureksi. Tästä syystä on hyvä toimintamalli muuttaa verkkolaitteiden asennustapaa niin, että laitekaapin yläosan sijasta verkkolaitteilla hankitaan oma laitekaappi rivin päästä ja sen kautta tehdään ristiinkytkennät muille laitekaapeille. Kuvassa 6 on esitetty molemmat asennustavat. Asennettaessa kytkimiä kaappien yläosaan on kaapelointi helppoa, ja mahdolliset viat yhteyksissä on tästä syystä helppo rajata. Huonona puolena on hallittavien laitteiden suuri määrä. Asennettaessa kytkimet rivin päähän erilliseen verkkolaitekaappiin vähennetään hallittavien laitteiden määrää, ja ristiinkytkennät on edelleen helppo toteuttaa. Huonona puolena on asennettavien kaapeleiden suuri määrä. [28, s. 38.]



Kuva 6. Verkkolaitteiden asennustavat

Tässä vaiheessa verkkolaitteiden kapasiteettivaatimuksia ovat ensisijaisesti tiedonsiirtokapasiteetti ja liitäntämäärät. Paras vaihtoehto on hankkia modulaarisia kytkinrunkoja, joihin voidaan tarpeen mukaan hankkia erillisiä kytkinmoduuleja. Mahdollisia vaihtoehtoja LAN-verkon laitehankinnoiksi ovat esimerkiksi Ciscon 6500- tai Nexus -sarjojen tuotteet, Juniperin EX6200 tai EX8200 -sarjat, ja Alcatelin OmniSwitch 9000 -sarjan tuotteet.

SAN-verkon tarpeisiin voidaan harkita esimerkiksi Ciscon MDS 9000 -sarjaa tai Ciscon Nexus- ja Juniperin EX -sarjojen kytkimien käyttämistä myös SAN-verkon tarpeisiin. Viimeistään toisen vaiheen tarpeiden määrittelyn yhteydessä on tarpeellista harkita ensimmäisestä vaiheesta kerätyn tiedon perusteella asiakkaan kykyä hallita ja ylläpitää verkkoa. Mikäli se on asettanut haasteita jo ensimmäisen vaiheen yhteydessä, laajentuvan ja monimutkaistuvan verkon ylläpidon ulkoistaminen on viimeistään tässä vaiheessa ajankohtaista. Palveluita tarjoavilla yrityksillä pitäisi jo lähtökohtaisesti olla asiantuntemusta vaativienkin verkkojen hallintaan, ja useimmilla suuremmilla toimijoilla on usein mahdollisuus liittää uudet järjestelmät jo olemassa oleviin valvonta- ja hallintajärjestelmiin, mikä nopeuttaa palveluiden käyttöönottoa. Toinen huomioitava kohta palvelun ulkoistamisessa ovat taloudelliset seikat. Sopimalla asianmukaiset SLA-tasot toisen osapuolen kanssa voidaan mahdollisista virhetilanteista aiheutuvia tappioita siirtää palveluntarjoajan maksettavaksi. SLA eli Service-level Agreement on palvelutasosopimus, asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot.

Verkon laajentumisen toinen vaihe ei ole asiakkaalle vielä millään tasolla ajankohtainen, joten suunnitelmana on esitetty ainoastaan periaatekuva mahdollisesta toteutuksesta. Tämä kuva on nähtävillä liitteessä 4. Samasta syystä etenkään mahdollisia laitehankintoja ei ole esitelty tuoteryhmien nimiä pidemmälle. Asiakas saattaa hankkia sekä laitteet että palvelun kokonaisratkaisuna, ja palveluntarjoajilla on usein mahdollisuus hankkia laitteita suoraan valmistajilta tai maahantuojilta listahintoja pienemmillä summilla.

4.3 Verkon laajennuksen kolmas vaihe

Seuraava vaihe laajennettaessa verkkoa on kahden tai useamman erillisen konesalin käyttö samassa järjestelmässä. Tällä voidaan ehkäistä katastrofitilanteita, joissa yhden konesalin täydellinen tuhoutuminen katkaisee asiakkaan palvelutuotannon kokonaan. Konesalien sisäisiä verkkoja ei tarvitse muuttaa, vaan eri konesalien verkot yhdistetään keskenään.

Konesalien välisien yhteyksien tulisi aina olla maantieteellisesti kahdennettuja siten, ettei yhteen kaapeliin kohdistuva vaurio tai häiriötilanne katkaise yhteyksiä kokonaan. Mahdollisia ratkaisuja konesalien välisille yhteyksille ovat suorat yhteydet, joissa palveluntarjoajalta ostetaan suora kytkentä konesalien välille, tai esimerkiksi L2 tai L3 MPLS VPN -yhteydet, joissa tietoliikenne kuljetetaan operaattorin runkoverkon päällä. Periaatekuva kolmannelle vaiheelle esitetään liitteessä 5. Multiprotocol Label Switching on menetelmä, jolla kuljetetaan esimerkiksi IP-paketteja ennalta määriteltyjen yhteyksien yli ilman, että tarvitsee tehdä reititystä. Virtual Private Network on tapa, jolla kaksi tai useampia verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisen yksityisen verkon.

Viimeistään tässä vaiheessa asiakkaan täytyy ainakin osittain ulkoistaa osa verkon hallinnasta, eli konesalien väliset yhteydet, palveluntarjoajalle, ja käytettävien verkkotekniikoiden monimutkaistuminen entisestään vaikeuttaa asiakkaan mahdollisuuksia onnistuneesti ylläpitää koko verkkoa. Verkko voi myös olla maantieteellisesti laaja, mikä vaikeuttaa asiakkaan omien palveluiden SLA-tasoissa pysymistä mahdollisten virhetilanteiden sattuessa.

5 Yhteenveto

Insinöörityön tehtävänä oli toteuttaa ja suunnitella asiakkaan konesaliverkko. Työn lähtökohtana oli konesaliverkon toteutus kolmannen osapuolen tekemän suunnitelman ja laitevalintojen pohjalta, jonka jälkeen tuli tehdä jatkosuunnitelmat verkon kehittämiseksi. Jo konesaliverkon toteuttamisen aikana havaittiin useita ongelmia kytkennöissä ja verkkolaitteiden valinnoissa sekä molempien yhteisvaikutuksesta johtuvista rajoituksista verkon hallittavuuteen ja kapasiteetin hyödyntämiseen.

Verkon laajentamisen ensimmäisen suunnitteluvaiheen aikana keskityttiin sekä parantamaan välittömiä nykyisen verkkoratkaisun muodostamia ongelmia että lisäämään kapasiteettia tulevaa kasvua varten. Tältä pohjalta esitettiin joitakin eri mahdollisuuksia laitevaihtoehdoiksi ja eri laitevaihtoehtojen pohjalta kuvattiin tulevan verkon rakennetta verkkokuvilla. Toisen verkonlaajennusvaiheen suunnittelussa ei verkon tämänhetkisen kasvuvauhdin takia tehty täsmällisiä suunnitelmia tai esitelty laitevaihtoehtoja eri tuoteperheiden nimiä syvemmällä tasolla.

Tulevaisuuden varalle verkon mahdollisesta rakenteesta tehtiin kuitenkin periaatekuva, jonka pohjalta voi aloittaa yksityiskohtaisemman suunnittelun sen hetkisten tarpeiden mukaan. Kolmatta verkonlaajennusta käsiteltiin ainoastaan konesalien välisten yhteyksien näkökulmasta ja siihen esitettiin muutamaa erilaista vaihtoehtoa, joilla yhteydet voi toteuttaa. Yhteyksien erilaisista toteutustavoista luotiin esimerkiksi periaatekuva.

Työssä käsiteltiin osana kaikkia suunnitteluvaiheita asiakkaan mahdollista tarvetta ulkoistaa verkon hallinta ja ylläpito, joko joiltain osin tai kokonaisuudessaan. Asiakkaan oman palvelutarjonnan kannalta ulkoistaminen on mahdollista missä tahansa toteutusvaiheessa, ja siitä tulee tehdä päätökset viimeistään samassa yhteydessä, kun toisen vaiheen tarkempi suunnittelu aloitetaan.

Ensimmäisen laajennuksen suunnittelun venyminen myöhästytti työn valmistumista, eikä asiakkaalta saatu kunnollista arviota verkon kasvun nopeudesta lähitulevaisuudessa. Tämän takia toisen ja kolmannen laajennusvaiheen suunnitelmat jäivät periaatteellisiksi. Toisen vaiheen suunnitelmaa on mahdollista käyttää pohjana, kun harkitaan tulevan verkon rakennetta niin loogisesti kuin kytkennällisestikin. Kolmannen vaiheen suunnitelman tarkoitus on hahmottaa asiakkaalle erilaisia mahdollisuuksia verkkoyhteyksien kahdennuksia ja toisiaan kahdentavien konesalien jatkosuunnittelua varten. Seuraava työvaihe tulee olemaan uuden verkkolaitteiden asennus ja yliheitto sekä verkkolaitteiden konfigurointi, kunhan asiakas on saanut tehtyä päätökset tarvittavista laitehankinnoista. Tämä osuus jää tämän työn ulkopuolelle, eikä mahdollisesta konsultoinnista ole vielä sovittu asiakkaan kanssa. Tämän raportin kirjoittaminen paransi näkemystäni konesaliverkoista ja yleisesti verkkojen suunnitteluun liittyvästä työstä, ja siten parantaa kykyäni toimia asiantuntijana.

Lähteet

1 Yritys. 2012. Verkkodokumentti. Nemein Oy. http://nemein.com/fi/company/. Luettu 30.4.2012.

2 Cabling for Next Generation Data Centre Technologies. 2009. Luentokalvo. Cisco Inc. Ei julkinen dokumentti.

3 Laitekaapin kaapelointi. 2011. Kuva. Integrated Data Storage. http://www.integrateddatastorage.com/wp-content/uploads/2011/12/Final-Cable-Picture.jpg

4 Sippola, Juha. 2009. Konesalirakentaminen ja laiteasennukset. Insinöörityö. Metropolia ammattikorkeakoulu.

5 MAC Address. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/MAC_address. Luettu 2.5.2012.

6 802.1Q. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/802.1Q. Luettu 2.5.2012.

7 Virtual LAN. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Vlan. Luettu 2.5.2012.

8 Spanning Tree Protocol. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Spanning_tree_protocol. Luettu 2.5.2012.

9 TRILL. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/TRILL_(computing). Luettu 2.5.2012.

10 Industry Trends and Vision: Evolution toward Data Center Virtualization and Private Clouds. 2012. Verkkodokumentti. Brocade. http://www.brocade.com/downloads/documents/technical_briefs/DataCenter_Virtualization_GA-TB-277-00.pdf. Luettu 2.5.2012.

11 QFabric System. 2012. Verkkodokumentti. Juniper Networks. http://www.juniper.net/us/en/products-services/switching/qfx-series/qfabric-system/#overview. Luettu 2.5.2012.

12 A Tale of Two FCoEs. 2011. Verkkodokumentti. http://datacenteroverlords.com/2011/11/21/a-tale-of-two-fcoes/. Luettu 2.5.2012.

13 Virtual Router Redundancy Protocol. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Vrrp. Luettu 3.5.2012.

14 Hot Standby Routing Protocol. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/HSRP. Luettu 3.5.2012.

15 Quality of service. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Quality_of_service. Luettu 3.5.2012.

16 Access control list. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Access_control_list. Luettu 3.5.2012.

17 Storage Area Network. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Storage_area_network. Luettu 3.5.2012.

18 Fibre Channel. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Fibre_Channel. Luettu 3.5.2012.

19 Small Computer System Interface. 2012. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/Small_Computer_System_Interface. Luettu 3.5.2012.

20 Cisco Nexus 5010 & 5020 datasheet. 2012. Verkkodokumentti. Cisco. http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/data_sheet_c78-461802.html. Luettu 3.5.2012.

21 Brocade 8000 specifications. 2012. Verkkodokumentti. Brocade. http://www.brocade.com/products/all/switches/product-details/8000-switch/specifications.page. Luettu 3.5.2012.

22 Cisco 3750-X and 3560-X Series Switches datasheet. 2012. Verkkodokumentti. Cisco. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/data_sheet_c78-584733.html. Luettu 3.5.2012.

23 Alcatel-Lucent OmniSwitch 6850. 2011. Verkkodokumentti. Alcatel-Lucent. http://enterprise.alcatel-lucent.com/includes/doclinkPostEloq.cfm?id=15908. Luettu 3.5.2012.

24 Juniper Networks EX4200 Series Specifications. 2012. Verkkodokumentti. Juniper Networks. http://www.juniper.net/us/en/products-services/switching/ex-series/ex4200/#specifications. Luettu 3.5.2012.

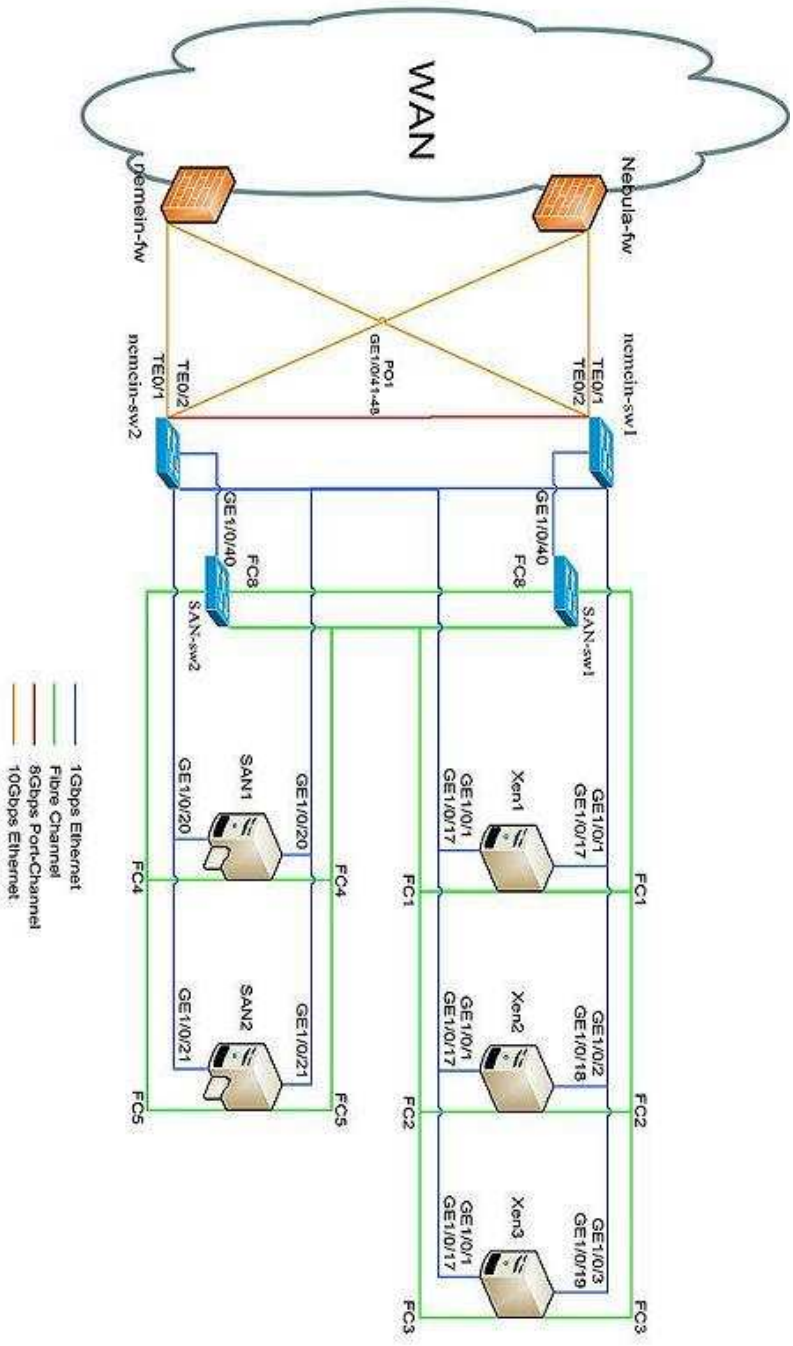
25 Cisco Catalyst 2960-S and 2960 Series Switches with LAN Base Software datasheet. 2012. Verkkodokumentti. Cisco. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.html. Luettu 3.5.2012.

26 Alcatel-Lucent OmniSwitch 6400 Technical. 2012. Alcatel-Lucent. http://enterprise.alcatel-lucent.com/?product=OmniSwitch6400&page=technical. Luettu 3.5.2012.

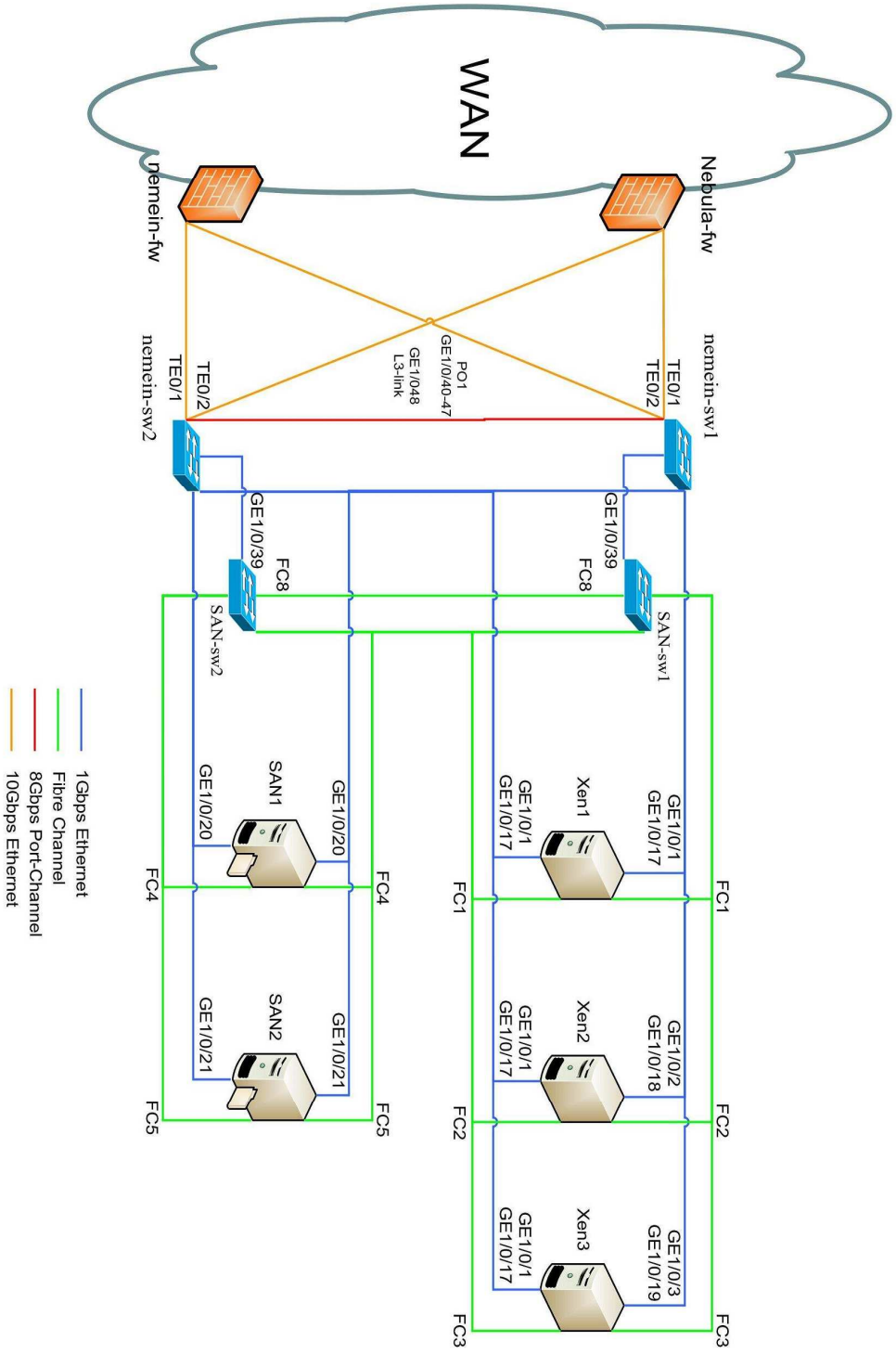
27 Juniper Networks EX3200 Series specifications. 2012. Juniper Networks. http://www.juniper.net/us/en/products-services/switching/ex-series/ex3200/. Luettu 3.5.2012.

Liitteet

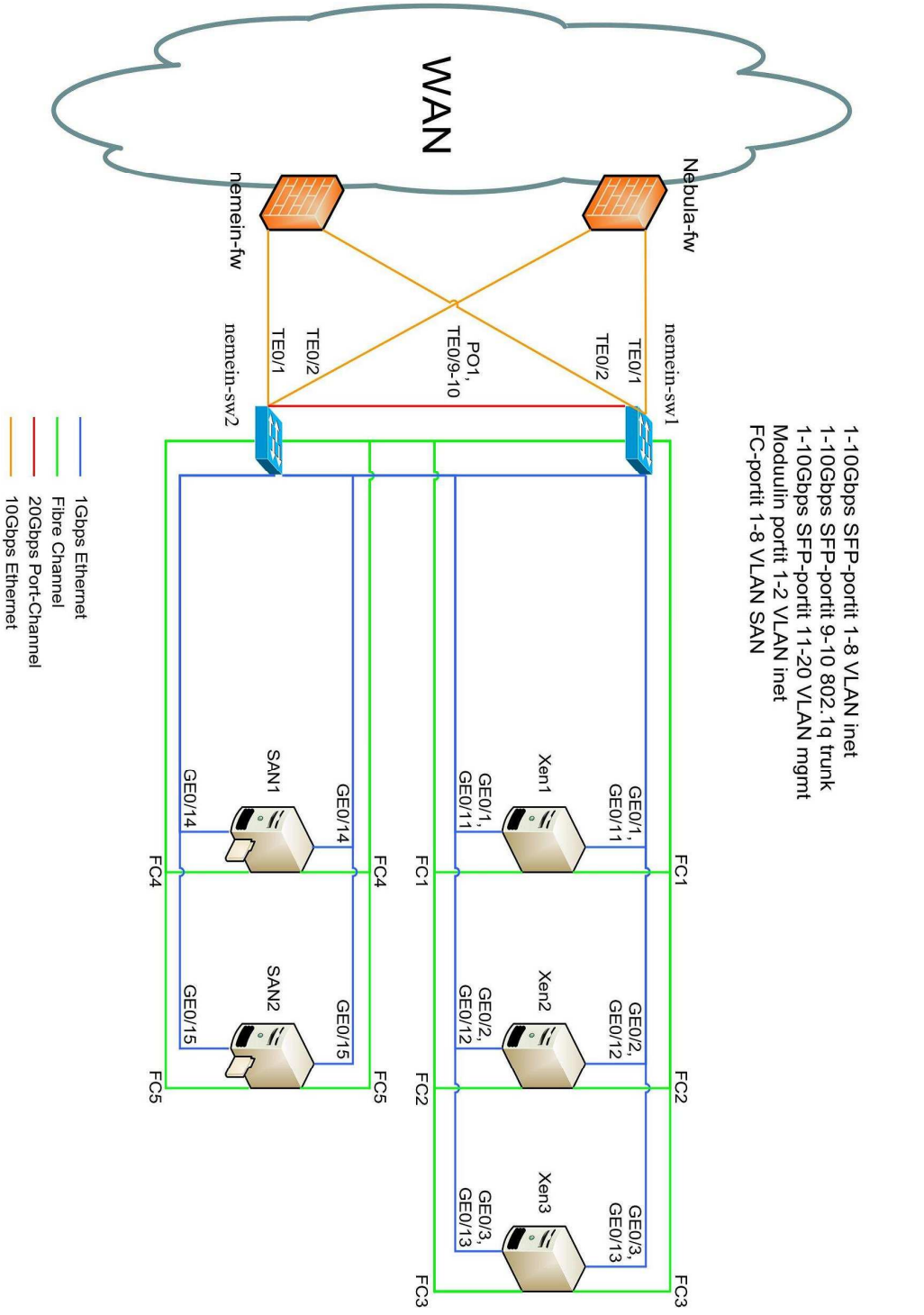
Liite 1. Verkon ensimmäinen laajennusvaihe, L2-tason hallittavat kytkimet



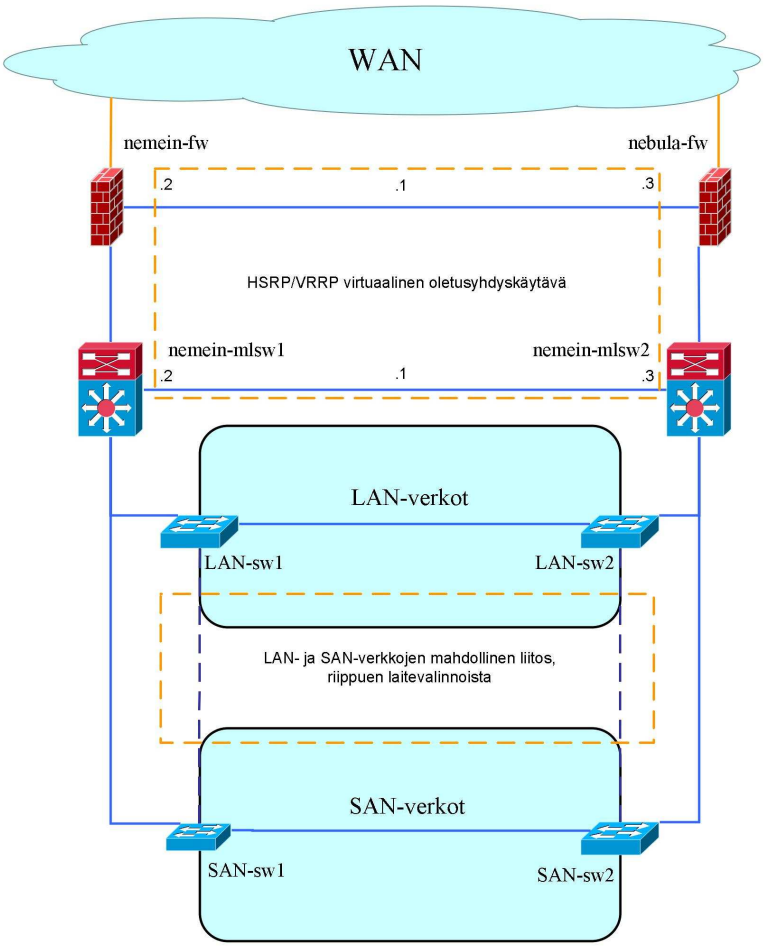
Liite 2. Verkon ensimmäinen laajennusvaihe, monitasokytkimet



Liite 3. Verkon ensimmäinen laajennusvaihe, LAN/SAN-kytkimet



Liite 4. Verkon laajentamisen toisen vaiheen periaatekuva



Liite 5. Verkon laajentamisen kolmannen vaiheen periaatekuva