

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikka / Tietoverkkotekniikka

Mikko Lehtinen

DATAKESKUSTEN ARKKITEHTUURI JA SUUNNITTELU

Opinnäytetyö 2014

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikka

Lehtinen, Mikko	Datakeskusten arkkitehtuuri ja suunnittelu
Opinnäytetyö	35 sivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	Kymenlaakson ammattikorkeakoulu
Toukokuu 2014	
Avainsanat	datakeskukset, arkkitehtuuri, suunnittelu

Datakeskusten lisääntyminen maailmalla on seuraus kasvavasta tiedotatan tarpeesta ihmisten keskuudessa. Operaattorit ja yritykset tarvitsevat valtavasti tilaa säilöökseen tietoa, ja niiden on pystyttävä tarjoamaan palveluitaan ympärivuorokautisesti asiakkailleen.

Opinnäytetyön aiheena on perehtyä datakeskusten arkkitehtuuriin ja niiden suunnitteluun. Tavoitteena on antaa lukijalle laajamittainen kuva datakeskuksen toiminnasta sekä näyttää menetelmiä oikeaoppisen laitesalin suunnitteluun.

Opinnäytetyö jakautuu kahteen pääosioon, jotka ovat arkkitehtuuri ja suunnittelu. Arkkitehtuuri-osiossa käydään läpi erinäisiä datakeskustekniikoita sekä Ciscon suunnitteleman Virtualized Multi-tenant Data Center -mallin, jota käytetään pohjana datakeskusten arkkitehtuurissa. Suunnittelussa esitellään TIA-942-standardi, joka määrittää, kuinka suunnitella oikeiden asetusten mukainen datakeskus. Tämän lisäksi esitellään datakeskuksissa käytettyjä laitteistoja sekä järjestelmiä, joilla varmistetaan datakeskusten jatkuva toiminta.

Kymenlaakson ammattikorkeakoulun ICT-laboratorion tiloihin rakennetaan kesällä 2014 kyberturvallisuuslaboratorio. Tämä opinnäytetyö toimii apuna varsinaisessa kyberturvallisuuslaboratorion suunnittelu- ja rakennusvaiheessa.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Information Technology

Lehtinen, Mikko	Datacenter's Architecture and Design
Bachelor's Thesis	35 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Kymenlaakso's University of Applied Sciences
May 2014	
Keywords	data centers, architecture, planning

Continuous increase of data centers around the world is the result of the growing need for information data among the people. Operators and enterprises need a great deal of space to storage data and they need to be capable of offering services around the clock to their customers.

Objective of this study was to examine data center architecture and design. The objective was to present large-scale view on the function of a data center and to show proper methods for designing a server room.

This study was divided to two main sections which were architecture and design. On architecture section several data center technologies and The Virtualized Multi-tenant Data Center model designed by Cisco Systems which is used as basis on data center architecture were presented. On planning phase TIA-942 standard was presented which defines how to plan a data center properly. In addition to this facilities and systems which are needed to ensure data centers continuous operation were presented.

In summer 2014, cybersecurity laboratory in facilities of ICT-laboratory in Kymenlaakso's University of Applied Sciences will be built. This study will assist in the actual planning and implementation phase of a cybersecurity laboratory.

SISÄLLYS	
TIIVISTELMÄ	
ABSTRACT	
LYHENTEET	
1 JOHDANTO	9
2 DATAKESKUKSET SUOMESSA	10
3 DATAKESKUKSEN SUUNNITTELU	10
3.1 TIA-942-standardi	11
3.1.1 Tilan suunnittelu	11
3.1.2 Kaapelointi-infrastruktuuri	12
3.1.3 Datakeskuksen tasoluokitukset	13
3.2 Palvelintelineet ja laitteet	15
3.2.1 Rittal CMC III-kulunvalvontajärjestelmä	17
3.3 Datakeskuksen aktiivilaitteet	17
3.3.1 Cisco UCS 6200 Fabric Interconnect	17
3.3.2 Cisco Nexus 5000 -sarja	18
3.4 Jäähdytysjärjestelmät	18
3.5 Varasähköntuotanto	19
3.6 Palonestojärjestelmä	22
4 DATAKESKUSTEN ARKKITEHTUURI	23
4.1 Datakeskusten verkkoteknologiat	25
4.1.1 Fibre Channel	25
4.1.2 Fibre Channel over Ethernet	25
4.2 Virtualisoitu datakeskus moniasiakasympäristössä	25
4.2.1 Three-Layer Hierarchical Model	27
4.2.2 VMDC-tasot	29
5 YHTEENVETO JA POHDINTA	31
LÄHTEET	32

LYHENTEET

BGP	Border Gateway Protocol eli <i>autonomisten alueiden välinen reititysprotokolla.</i>
CNA	Converged network adapter eli <i>verkkokortti, jossa on myös Fibre Channelia tukeva hubi.</i>
DCB	Data Center Bridging eli <i>joukko standardeja, joilla mahdollistetaan konvergoitunut verkkoinfrastruktuuri.</i>
DMZ	Demilitarized Zone eli <i>eristetty alue julkisen ja yksityisen verkon välissä.</i>
DNS	Domain Name System eli <i>nimipalvelujärjestelmä.</i>
EIGRP	Enhanced Interior Gateway Routing Protocol eli <i>etäisyysvektorireititysprotokolla.</i>
FTP	File Transfer Protocol eli <i>tiedostojen siirtämisprotokolla.</i>
GigE	Gigabit Ethernet.

IDS	Intrusion Detection System eli <i>tunkeilijanhavaitsemisjärjestelmä.</i>
IN	Intelligent Network eli <i>verkkoarkkitehtuuri</i>
IPTV	Internet Protocol television eli <i>internetin yli kulkeva televisi-</i> <i>siopalvelu.</i>
iSCSI	Small Computer System Interface over IP eli <i>tiedonsäilömisjärjestelmien linkitystekniikka.</i>
IT	Information and Communication's Technology eli <i>informaatioteknologia.</i>
LCP	Liquid Cooling Package eli <i>nestejäähdytystekniikka.</i>
NAS	Network-attached storage eli <i>tallennusjärjestelmä, jolla</i> <i>voidaan jakaa tiedostoja verkossa.</i>
OSPF	Open Shortest Path First eli <i>linkkitilan reititysprotokolla.</i>
QoS	Quality of Service eli <i>palvelun laatu.</i>

RU	Rack Unit eli <i>Räkkiunitti</i> .
SAN	Storage Area Network eli <i>verkko, joka tarjoaa käyttäjille pääsyn tallennustiloihin.</i>
SMTP	Simple Mail Transfer Protocol eli <i>sähköpostiviestien välityspalvelu.</i>
TIA	Telecommunications Industry Association eli <i>instituutti, joka on kehittänyt TIA-942-standardin.</i>
UCS	Unified Computing System eli <i>Cisco Systemsin kokonaisuus, joka yhdistää verkkolaitteet ja palvelut samaan arkkitehtuuriin.</i>
UPS	Uninterruptible Power Supply eli <i>varasähköntuoton mahdollistava sähkölaitte.</i>
VM-FEX	Virtual Machine Fabric Extender eli <i>teknologia, jolla pystytään yhdistämään fyysinen ja virtuaalinen verkko yhdeksi infrastruktuuriksi.</i>

VoIP

Voice over IP eli *menetelmä, jolla voidaan siirtää ääntä*
verkon yli.

WAN

Wide Area Network eli *laajaverkko.*

1 JOHDANTO

Nykyaikana yhä useammat yritykset käyttävät tietoverkkopohjaisia ratkaisuja, joten datakeskukset ovat välttämätön osa yrityksiä. Asiakkaat vaativat entistä enemmän korkealaatuista palvelua, jota yrityksen tulee pystyä tarjoamaan luotettavasti. Tärkeä osa datakeskusta on SAN-ratkaisu, jossa säilytetään yrityksen dataa. Kuvien ja muun median koko on kasvanut laadun lisääntyessä, joten täytyy olla resursseja niiden säilyttämiseen. Jotta tietoliikenteen kulku olisi jatkuvaa, pitää datakeskuksen arkkitehtuurin sekä laitteiden olla mitoitettu optimaalisesti. Tähän käytetään apuna erinäisiä standardeja, jotka määrittävät datakeskuksen rakenteen.

Datakeskus on laitetila, joka keskittää yrityksen IT-operaatiot ja laitteistot sekä tallettaa dataa ja hallinnoi sitä. IT-laitteisto koostuu esimerkiksi palvelimista, tallennusjärjestelmistä sekä tietoliikennelaitteista. Käytännössä jokaisessa isossa yrityksessä on jonkinlainen datakeskus eli laitetila. Yritykset voivat hankkia datakeskusten tuottamat palvelut tänä päivänä myös pilvipalveluna, eli tarvittavat palvelut sijaitsevat palveluntarjoajan datakeskuksessa internetissä. Tämä opinnäytetyö ei kuitenkaan käsittele datakeskusten tuottamia palveluja.

Alun perin opinnäytetyön tarkoituksena on toimia esiselvityksenä ja tiedonhankintana Kymenlaakson ammattikorkeakouluun kesällä 2014 rakennettavalle uudelle kyberturvallisuuslaboratorion tarpeita palvelevalle datakeskukselle.

Kyberturvallisuuslaboratoriohanke on edennyt opinnäytetyön valmistumiseen mennessä kuitenkin vasta hankintaselvitys- ja tarjouskilpailuvaiheeseen. Tämän vuoksi päädyin opinnäytetyössäni käsittelemään datakeskusten arkkitehtuuria yleisellä tasolla. Sen lisäksi käyn läpi, kuinka rakennetaan datakeskus ja mitä asioita tulee ottaa huomioon sen suunnittelussa. Varsinaista käytännön osuutta opinnäytetyössäni ei ole.

2 DATAKESKUKSET SUOMESSA

Suomesta on viime vuosina tullut Euroopan parhaimpia paikkoja isojen yritysten datakeskuksille. Tämän ovat esimerkiksi huomanneet Google, Microsoft ja Yandex, joista Google on perustanut jo datakeskuksen Haminaan vanhaan paperitehtaan tiloihin. Microsoft rakentaa datakeskuksensa Ouluun tai Kajaaniin ja Yandex rakentaa omansa Mäntsälään. Jotta datakeskus voisi toimia, se tarvitsee sähköä, hyvät jäähdytysmahdollisuudet, korkeat verkkoyhteydet ja ammattimaista työvoimaa. Suomi takaa kaikki edellä vaadittavat ominaisuudet. (Suomi on datakeskusten luvattu maa... yksi pieni ongelma.) Huhtikuussa 2014 tuli voimaan laki, joka vähensi datakeskusten sähkölaskutusta 1,703 sentistä/kWh 0,703 senttiin/kWh. Sähköhinnan muutos parantaa Suomen asemaa huomattavasti globaalien yritysten silmissä. (Cheaper electricity for data centers in Finland 3/2014.)

3 DATAKESKUKSEN SUUNNITTELU

Suunnitteluvaihe on tärkeä osa kokonaisuutta; sillä maksimoidaan hyöty ja minimoidaan vastaisuudessa mahdollisesti tapahtuvat haitat. Datakeskus pitää suunnitella skaalautuvuutta ajatellen, joten laitetila on syytä ylimitoitaa, jotta tulevaisuudessa tarvittavat muutokset olisi mahdollista toteuttaa. Datakeskuksessa on useita muuttuvia tekijöitä, jotka pitää ottaa huomioon. (Use Best Practices to Design Data Center Facilities 4/2005.)

Huomioitavia muutoksia ovat muun muassa seuraavat:

- laajennukset ja tilojen yhdistyminen
- uudet laitehankinnat
- redundanttisuus
- muuttuvat tehovaatimukset
- muuttuvat jäähdytystarpeet
- rajoittunut lattiatila
- muuttuvat turvallisuusmääritelmät
- muutokset toimintaprotokollassa.

3.1 TIA-942-standardi

Alkuaan kun ensimmäisiä datakeskuksia rakennettiin, ei ollut olemassa määräyksiä, joiden mukaan olisi pitänyt menetellä suunnitteluvaiheessa. Nykyään Telecommunications Industry Association-instituutti on kehittänyt TIA-942-standardin, joka määrittelee rakennettavan datakeskuksen infrastruktuurin. TIA-942-dokumentti jakautuu neljään eri kategoriaan, jotka ovat tilasuunnittelu, kaapelointi-infrastruktuuri, datakeskuksen tasoluokitukset ja huomioon otavat ympäristövaikutukset. Ympäristövaikutuksiin kuuluvat jäähdytys, varasähköntuotanto ja palonestojärjestelmä. (Smith L.)

3.1.1 Tilan suunnittelu

Standardin mukaisella tilan suunnittelulla varmistetaan jatkossakin skaalautuva ja ympäri vuorokauden toimiva toimintaympäristö. On tärkeää jättää tyhjää tilaa, jos yrityksen tulevaisuudessa halutaan laajentaa laitetilaa uusilla laitekaapeilla. TIA-942-standardissa suositellaan, että yrityksen laitteet olisi jaoteltu hierarkkisesti erillisiin tiloihin. Ne jakautuvat neljään pakolliseen tilaan, mutta tarpeen tullen on myös mahdollista lisätä tilojen määrää. Pakolliset tilat on esitelty seuraavasti:

Hallintakeskus – Datakeskuksella on oltava yksi tai useampi hallintakeskus. Hallintakeskus toimii liitäntäpisteenä datakeskuksen palvelimille ja se voi sijaita joko laitetilan sisällä tai mieluiten erillisenä tilana, jolloin se on turvallisempi. Tämän lisäksi teknikkojen ei tarvitse astua sisään laitetilaan ja he välttyvät laitteiden mahdollisesti aiheuttamilta kuulovaurioilta. (TIA-942 Data Center Standards Overview 4/2006.)

Pääjakelukeskus – Pääjakelukeskus on datakeskuksen tärkein tila, joka keskittää datakeskuksen päälaitteet, kuten Core-reitittimet ja kytkimet LAN- ja SAN-infrastruktuuria varten. Se toimii kaapeloinnin keskustana, joka yhdistää rakennuksen laitetilat yhtenäiseen verkkoon. (Data Center Spaces 2013.)

Horisontaalinen jakelukeskus – Horisontaalinen jakelukeskus toimii välikappaleena esimerkiksi kerrosten välillä. Tätä keskusta ei välttämättä tarvitse olla, etenkin pienemmissä datakeskuksissa. Horisontaalinen kaapelointi on toteutettu laiterasioiden avulla, jotka helpottavat laitteiden kytkeytymistä verkkoon jättämällä kaapeloinnin

välimatkan pieneksi. Yleisesti horisontaalinen jakelukeskus koostuu LAN-, SAN- ja KVM-kytkimistä. (Data Center Spaces 2013.)

Equipment Distribution Area – Equipment Distribution Arealla säilytetään datakeskuksen päätelaitteet kuten palvelimet. Tässä tilassa horisontaalista kaapelointia käyttävät laitteet yhdistyvät laitekaapissa olevaan ristikytkentäpaneeliin. (TIA-942 Data Center Standards Overview 1/2006.)

3.1.2 Kaapelointi-infrastruktuuri

Oikeanmukaisella kaapeloinnilla ehkäistään tulevat viat ja helpotetaan ongelmien tunnistamista, koska TIA-942-standardia käytetään maailmanlaajuisesti. TIA-942-standardi määrittää datakeskuksessa käytettävien kaapeleiden rakenteen ja sen ominaisuudet. Kaapeleiden sijoittaminen on tärkeää moninaisista syistä. Esimerkiksi virta- ja yhteyskaapelien pitää olla erotettuna toisistaan sähköhäiriöiden minimoimiseksi. Lisää tietoa kaapeloinnista on luvussa 3.2 Palvelintelineet ja laitteet. Kaapelointi jaetaan kahteen osaan, jotka ovat runkoverkko ja horisontaalinen kaapelointi. (TIA-942 Data Center Standards Overview 1/2006.)

TIA-942-standardi suosittelee runkoverkossa käytettäväksi optista monimuotoista kuitukaapelia, koska se tukee suuria tiedonsiirtonopeuksia pitkillä matkoilla. Runkoverkossa kuitukaapelin maksimimitaksi on määritetty 300 metriä. (Best Practices Guide: Cabling the Data Center 2007.)

Horisontal-kaapeloinnissa, jossa kaapelointi on toteutettu kaapelikouruja pitkin, suositellaan käytettäväksi Cat6 Rj45-kaapeleita. Kaapelikouruilla pystytään piilottamaan muuten näkyvissä kulkevat verkkokaapelit. Suunnittelijan on tärkeää valita kaapeli, joka pystyy tarjoamaan tiedonsiirtonopeudet, jotta vältetään tulevilta fyysisiltä muutoksilta. Horisontal-kaapeloinnin maksimipituus on 300 metriä. (Best Practices Guide: Cabling the Data Center 2007.)

Datakeskukset käyttävät laitesaleissa korotettuja lattioita, joilla mahdollistetaan kaapeleiden piilottaminen ja jäähdytysreitit. Lattian tilalla on kehikko, joka on päällystetty laatoilla, joiden alla on tyhjää tilaa kaapeleita ja jäähdytystä varten. (Use Best Practices to Design Data Center Facilities 4/2005.) Kuvassa 1 on esitelty mallin mukainen toteutus.



Kuva 1. Datakeskuksen korotettu lattia. (Perforated-Ventilating-raised-access-floor-tiles.)

3.1.3 Datakeskuksen tasoluokitukset

Datakeskukset ovat rakenteeltaan erilaisia, joten Uptime Institute -yhtiö on kehittänyt sitä varten sertifikaattijärjestelmän, jolla pystytään määrittelemään rakennettu datakeskus kuuluvaksi ansaittuun luokkaan. Luokat jakautuvat seuraavasti: taso I, taso II, taso III ja taso IV. Mitä suurempi saatavuus datakeskuksella on, sitä ylempään tasoon se kuuluu. Tasojen erot saatavuudessa ovat 99,995 % (taso 4) – 99,671 % (taso 1). Prosenttimäärä ilmoittaa, kuinka kauan laitesali on toiminnassa vuoden aikana. Vaikka prosenttimäärän erot tasojen välillä vaikuttavat pieniltä, eron huomaa vasta, kun tarkastelee tulosta tuntien perusteella. Esimerkiksi tasolla 4 laitesali ei ole toiminnassa 26,3 minuuttia vuodessa, kun taas tasolla 1 laitesali ei ole toiminnassa 28,8 tuntia vuodessa. (Tier Standards Overview .)

Tasoluokitus annetaan seuraaville datakeskuksen infrastruktuurin osille: mekaaniset järjestelmät, sähköjärjestelmät, televiestintäjärjestelmät sekä sisäinen arkkitehtuuri. Jokaisella järjestelmällä voi olla saavutettu eri taso, mutta pääasiallisesti yleisen tason datakeskukselle määrittää huonoin arvosana. (TIA-942 Data Center Standards Overview 1/2006.)

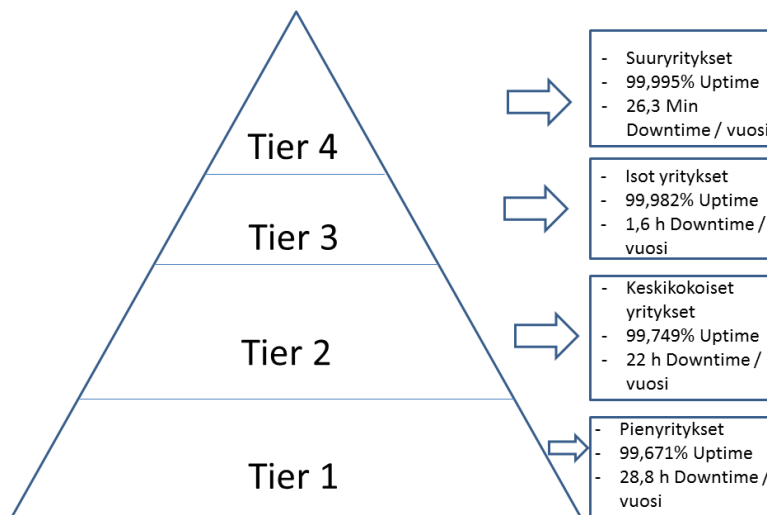
Taso 1 on TIA-942-standardiin pohjautuvan tasoluokituksen alin taso. Vaatimukset ovat vähäisiä, mutta datakeskuksessa / laitetilassa pitää olla vähintään virransyöttö ja jonkinlainen jäähdytyslaitteisto. Jos järjestelmässä on UPS-laite, se ei ole modulaarinen. Tason 1 saavuttamiseen datakeskuksen ei tarvitse olla redundanttinen. Tasolla 1 toimivan laitesalin laitteet pitää päivittäin sulkea huollon ajaksi. Suurimmalta osin kaikki laitesalit täyttävät tason 1 vaatimukset, ja se on yleisin taso maailmalla. Tason 1 laitesaleja käytetään pienissä yrityksissä, eivätkä nämä vaadi jatkuvaa ylläpitoa. (Designing the Physical Infrastructure.)

Taso 2 sisältää redundanttiset komponentit, jotka käyttävät vain yhtä yhtä yhteistä virranjakelujärjestelmää. Taso 2 vaatii, että datakeskuksessa on korotetut lattiat ja UPS-laite. Tasovaatimukset nousevat porrastetusti, joten esimerkiksi tason 2 pitää täyttää samat vaatimukset kuin taso 1, tason 3 pitää täyttää samat vaatimukset kuin taso 2 jne. Koska laitesalilla on redundanttinen UPS-laite, kokonaisuutta kutsutaan merkinnällä $N + 1$, jossa N merkitsee komponentteja ja $+1$ varmuuksien määrää. Tason 2 datakeskuksia näkee useimmiten keskikokoisissa yrityksissä, joissa toimintakatkokset eivät haittaa merkittävästi yrityksen toimintaa. (Data Center Construction Costs.)

Tason 3 datakeskuksen tulee tarjota monta vaihtoehtoista virransyötön reittiä redundanttisille laitteille. Tällöin ei tarvitse tukea kuin ainoastaan yhtä sähkönsyöttöä kerralla. Tason 3 datakeskuksia näkee käytettävän isoissa yrityksissä. (Designing the Physical Infrastructure 11/2010.)

Tasolla 4 vaaditaan minimissään saatavuusprosentti 99,995, joka tarkoittaa sitä, että datakeskus saa olla pois käytöstä enintään 26,3 minuuttia vuodessa. Taso 4 on tasoista vikasietoisin, ja tämän tason datakeskuksia käyttävät vain suuryritykset. Datakeskukselta vaaditaan seuraavia ominaisuuksia: virranjakelu monesta reitistä, redundanttiset laitteet ja datanjakelu on mahdollistettu monia reittejä pitkin. Datakeskuksessa pitää olla polttoainetta generaattoria varten jatkuvasti, jotta sähkökatkoksen tapahtuessa voidaan datakeskusta pyörittää generaattorilla ainakin 12 tuntia. Jäähdytysjärjestelmien pitää pyöriä kokopäiväisesti, koska laitteiston ylikuumentumiselta halutaan välttyä. Näillä menetelmillä ja varokeinoilla mahdollistetaan datan kulkeminen verkossa kokoaikaisesti. Yksittäisen tahallisen tai tahattoman ongelman tapahtuessa järjestelmän toiminta ei lakkaa. Suuryrityksissä

datakeskuksen sammuminen vain minuuteiksi voi tarkoittaa jo suurien rahasummien menettämistä, joten taloudellisesta näkökulmasta datakeskuksen jatkuva toiminta on elintärkeää. Kuvassa 2 on esiteltyä eri tasot pyramidikuvana.



Kuva 2. Data Center Tierit vertailussa.

3.2 Palvelintelineet ja laitteet

Palvelintelineet eli laitekaapit toimivat rakenteena laitesalin verkkolaitteille kuten blade-palvelimille ja reitittimille, joten niiden valinta on tärkeä osa suunnittelua. Laitesalin koosta riippuen pitää miettiä, montako laitekaappia tilaan halutaan asennettavan. Laitekaappien sijoittamiseen vaikuttaa tilan arkkitehtuuri ja jäähdytysjärjestelmä. Laitekaapit pitää sijoittaa organisoidusti, jotta jäähdytyslaitteistot pystyvät toteuttamaan parhaan mahdollisen jäähdytyksen verkkolaitteille. Laitekaappien valmistajien pitää pystyä tarjoamaan helppokäyttöisiä laitekaappiratkaisuja asiakkaille, jottei jatkossa tarvitse turvautua ulkopuoliseen apuun. Laitekaapit jakautuvat osiin, jotka on esitelty seuraavaksi.

Kotelon valinta perustuu kahteen asiaan: Mitä laitekaappiin asennettava laite vaatii ja kuinka paljon laitteita asennetaan laitekaappiin? Kotelo kannattaa ja pitää ylimitoittaa, koska jatkossa kotelon korkeutta ei pystytä laajentamaan. Laitekaapin lopullinen koko voi osoittautua ongelmaksi, kun laitekaappi viedään haluttuun asennuspaikkaan. Miten menetellään jos laitekaappi ei mahdu ovesta sisään laitesaliin? Laadukas laitekaappiratkaisu mahdollistaa myös organisoidun laitekaapeloinnin, joka parantaa

käyttäjäkokeemusta. (Server Rack Ordering Guide.) Laitekaappien koot ovat standardisoituja ja niitä on lukuisia. Kuitenkin 19 ja 23 tuuman koot ovat käytetyimpiä mittoja yritysten keskuudessa. RU-merkinnällä tarkoitetaan laitekaappiin asennettavan laitteen korkeutta, joka määritellään standardissa EIA-310.

Kotelon sivuissa oleviin asennusrimoihin kiinnitetään asennettavat moduulit ruuveilla. Moduulit pitää asentaa tukevasti etu- sekä takapuolelta, jotta ne eivät paina alla olevia verkkolaitteita. Oikeanlaisella asennusmetodilla moduulien väliin jää tilaa jolloin ilma pääsee kiertämään eivätkä laitteet myöskään aiheuta resonointia. Laitekaapin sivuun asennetaan jännitekiskot, joista laitteet saavat tarvitsemansa virran. Normaalien jännitekiskojen lisäksi voi myös olla ns. ”älykkäitä jännitekiskoja”, joita pystyy käyttämään etänä verkon kautta. Esimerkkinä ”älykkästä jännitekiskosta” on Rittalin CMC III- ratkaisu. CMC III-jännitekiskon avulla pystytään esimerkiksi sammuttamaan laitekaapin osia erillisestä tilasta. (Server Rack Ordering Guide.)

Laitekaapin päällä oleva paneeli estää pääsyn verkkolaitteisiin ja mahdollistaa kaapeloinnin pois pääsyn. Paneeleissa voi olla myös lisäosana tuuletin, joka kuljettaa lämmön laitekaapin sisältä ulos. Koteloon kiinnitetyillä ovilla minimoidaan verkkolaitteiden aiheuttama melu ja suljetaan pääsy asiaankuulumattomilta laitesalin käyttäjiltä. Kaikki ratkaisut eivät ole suljettuja, vaan on haluttu saada aikaiseksi optimaalinen ratkaisu ilmanvaihdon ja melun suhteen. Näin ollen esimerkiksi Rittalin TS-IT-laitekaappien ovet on rei’itetty molemmilta puolilta. Seuraavaksi kuva Rittalin 19” 42U TS-IT-mallista.



Kuva 3. Rittal TS-IT-laitekaappi. (Rittal TS-IT-laitekaappi.)

3.2.1 Rittal CMC III-kulunvalvontajärjestelmä

Rittal CMC III on laitekaappiin kiinnitettävä moduuli, joka tarkkailee automaattisesti laitesalin toimintaa. Siihen voidaan kytkeä laitesalin jäähdytyslaite, virranjakelujärjestelmä, laitekaappien valaistus ja yleinen turvajärjestelmä. Keskitetyllä kulunvalvontajärjestelmällä saavutetaan laitesalin optimoidumpi energianhallinta. Järjestelmän mukana tulee anturit, jotka asetetaan haluttuun kohteeseen mittaamaan lämpötilaa. Lämpötilan muuttuessa arvot kirjataan automaattisesti järjestelmän lokiin. Tietoturvaa ajatellen on mahdollista asentaa liikeanturi tilan oviin, jotta huomataan mahdollinen tietomurto ajoissa. Ongelman tai mahdollisen tietoturvauhan ilmetessä CMC III-järjestelmä ilmoittaa RiZone-ohjelmalla ylläpitäjälle tapahtuneesta virheestä. (Rittal CMC III.) CMC III-järjestelmään kuuluu 3-vaiheinen laitekaappiin asennettava virranmittauskisko, josta pystytään tarkastelemaan laitteiden virrankäyttöä ja havaitaan mahdolliset virtapiikit. Virranmittauskisko osaa tarvittaessa lähettää tiedot sähköpostiin SMTP-protokollan avulla.

3.3 Datakeskuksen aktiivilaitteet

3.3.1 Cisco UCS 6200 Fabric Interconnect

Cisco UCS 6200 -sarjan Fabric Interconnect-kytkimet kuuluvat Ciscon UCS-alustaan ja tarjoavat helpompaa palvelimien hallintaa verkon ylläpitäjille. Kytkin yhdistää kaikki siihen kytketyt laitteet samaan hallinta-alueeseen. Tällä ratkaisulla voidaan muuntaa datakeskuksen arkkitehtuuri yksinkertaisemmaksi, joten laitekustannusten määrä pienenee huomattavasti. Cisco UCS 6200 -sarjan kytkimet tarjoavat LAN- ja SAN-liitettävyyden kaikille blade-palvelimille, jotka ovat samassa domainissa. Virtuaalisoinnin osalta se tukee VM-FEX-arkkitehtuuria, joka tarjoaa käytännön mukaisen virtuaalilaitteiden liitettävyyden. Cisco UCS Manageri mahdollistaa jopa satojen palvelimien ja muiden verkkolaitteiden hallinnan ohjelmallisesti. (Cisco UCS 6200 Series Fabric Interconnects 7/2013.)

3.3.2 Cisco Nexus 5000 -sarja

Ciscon Nexus 5000 -sarjan kytkimillä pystytään muodostamaan vakaa ja skaalautuva verkko datakeskuksen infrastruktuurille. Ne on suunniteltu datakeskuskäyttöön, minkä huomaa liitännäporttien paikoista ja uusien verkkoteknologioiden tuesta. Tuettuja teknologioita ovat esimerkiksi Data Center siltaus (DCB), Virtual Port Channel, Fabric Extender ja tietovarastojen keskittäminen. Nexus-kytkimet vähentävät energiankulutusta ja kaapeloinnin määrää I/O-yhtenäistymisellä. Laitteet tukevat 10 Gbit/s nopeuksia kaikissa liitännäporteissa, mikä on välttämätöntä kuitukaapeloinnin kannalta. Nexus 5500 -sarjan laitteet tukevat myös Fiber Channel over Ethernet-teknologiaa. Kytkimiin voi asentaa moduuleja, joilla saadaan lisättyä esimerkiksi liitännäporttien määrää ja tarjota myös parempia tiedonsiirtonopeuksia. (Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches 5/2013.)

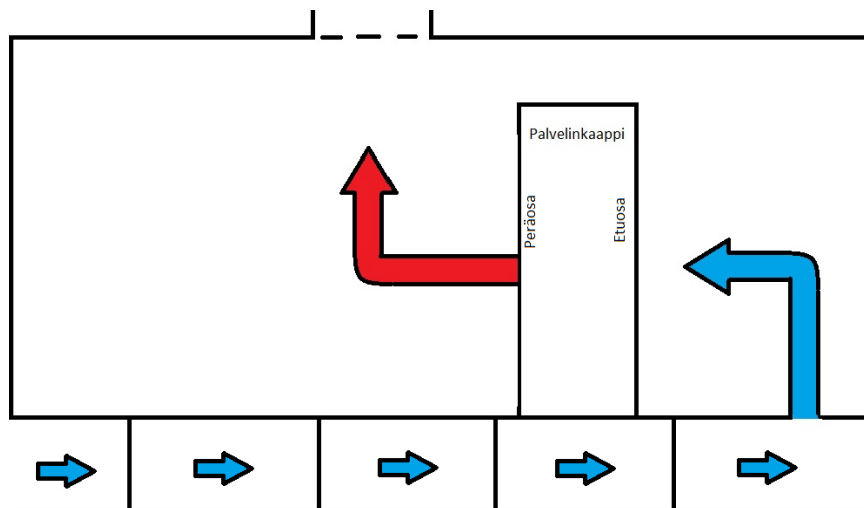
3.4 Jäähdytysjärjestelmät

Tärkeä osa datakeskustekniikkaa on jäähdytys, ja sitä ei voi jättää huomiotta suunnitteluvaiheessa. Datakeskuksen tietoverkossa kulkee huomattava määrä dataa, joka kuumentaa tietotekniikkalaitteita ja näin ollen voi aiheuttaa moninaisia häiriöitä laitteisiin. Tämä estetään laskemalla laittilan lämpötilaa tarvittavaan pisteeseen. (Data Center Power and Cooling 8/2011.)

Laittilalle halutaan löytää mahdollisimman kustannustehokas ratkaisu, joka tarjoaa parhaan jäähdytystehon ja halvat käyttökulut. Useimmissa datakeskuksissa laittilan lämpötila on 70 astetta tai pienempi. Korottamalla lämpötilaa vain kymmenellä asteella voidaan päästä jopa satojen tuhansien säästöihin vuodessa riippuen laittilan koosta. (Google: Raise Your Data Center Temperature.)

Korotetulla lattialla mahdollistetaan toimiva järjestelmä laitekaappien optimaaliseen jäähdytykseen. Jäähdytyksen pääperiaate toimii seuraavanlaisesti: Lattian alla oleva putki puhalttaa kylmää ilmaa ylöspäin laitesaliin palvelinkaappin laitteille.

Palvelintelineiden laitteissa olevat tuulettimet puhaltavat niiden muodostaman lämpöenergian pois laitekaappin perältä ylös, jossa ilmastointilaitte kuljettaa kuumaa ilman putkistoa pitkin ulos. Kuvassa 4 on esimerkki jäähdytyksen toiminnasta.



Kuva 4. Laitesalin yksinkertainen jäähdytysmenetelmä.

Mahdollinen jäähdytysratkaisu laitesalille on Rittalin LCP-rivijäähdytin.

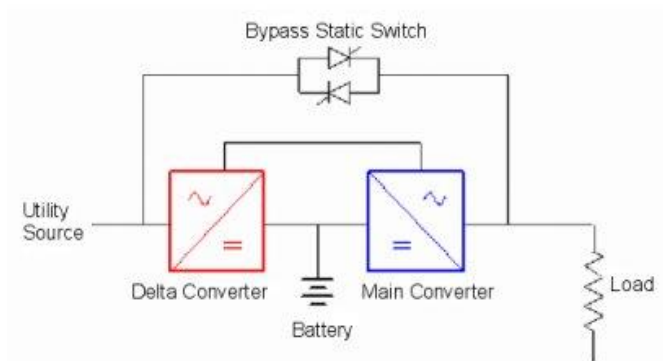
Palvelinkaappien välissä oleva Rittalin LCP-rivijäähdytin imee ilmaa palvelinkaapin takaa ja jäähdyttää sen erillisessä tilassa olevalla lämmönvaihdinkennolla, minkä jälkeen jäähdytetty ilma kulkee laitesalin alla putkia pitkin vedessä ja ilma puhalletaan palvelinkaapin etuosaan.

3.5 Varasähköntuotanto

Kun halutaan saada järjestelmän saatavuus mahdollisimman lähelle 100 %:a, on tärkeää huomioida tulevaisuudessa tapahtuvat mahdolliset sähkökatkokset. Tällä varatoimella turvataan datakeskuksen data, joka olisi menetetty sähkökatkon tapahtuessa. Tätä varten on olemassa UPS-laite, joka takaa tasaisen virransyötön lyhyiden katkojen tapahtuessa. UPS-laite suojaa myös tietotekniikkalaitteistoa satunnaisilta virtapiikeiltä ja ali- ja ylijännitteiden aiheuttamilta vaurioilta. Suunnittelun alkuvaiheessa pitää huomioida, halutaanko jokaiselle laitekaapille oma UPS vai panostetaanko yhteen erilliseen yksikköön, joka takaa varasähköntuotannon kaikille laitetilan laitteille. Fyysisesti pienelle laitetilalle on järkevämpää valita hajautettu järjestelmä, jotta kokonaisuuden hallinta olisi helpompaa. Molempia ratkaisuja voidaan myös käyttää yhtenä kokonaisuutena, jotta saadaan toteutettua laitetilalle redundanttinen suojaus. (UPS-käsikirja 2012.)

UPS:t eroavat toisistaan seuraavien ominaisuuksien osalta: fyysinen koko, paino, rakenne, kapasiteetti, tuetut virtalähteet ja hinta. Näiden ominaisuuksien lisäksi UPS

jaetaan kolmeen eri topologiaan, jotka ovat Passiivinen off-line, Line-interaktiivinen ja Double conversion - kaksoismuunnos teknologia. Koska datakeskuksen virransyötön pitää olla jatkuvaa, tähän käyttöön tärkein topologia on Double conversion -kaksoismuunnos. Double conversion -kaksoismuunnosmenetelmässä tasamuuntaja muuntaa vaihtovirran tasavirraksi ja tämän jälkeen vaihtomuuntaja muuntaa tasavirran vaihtovirraksi. Menetelmä poistaa järjestelmässä tapahtuvat mahdolliset virtapiikit ja muut sähköhäiriöt. (UPS-käsikirja 2012.) Kuvassa 5 kuvataan Double conversion -topologia, joka esittelee sen keskeisen toimintatavan.



Kuva 5. Double conversion -topologia. (Lessons on ups topologies.)

Valittaessa sopivaa UPS:ää datakeskukseen, valinta yleensä keskittyy kahden tyypin välille: 3-vaiheinen staattinen UPS ja rotary UPS. Staattinen UPS hallitsee kuitenkin noin 90%:a markkina-alueesta ja on täten käytetyin arkkitehtuuri. Se on korvannut melkein kokonaan rotary UPS:n nykypäivänä. (Comparison of Static and Rotary UPS 2011.)

Staattista UPS:ää kutsutaan staattiseksi, koska siinä ei ole liikkuvia osia pois lukien lisälaitteet kuten tuulettimet. Double conversion -topologiaa käytetään staattisen UPS:n pohjana. Pääperiaatteena UPS lataa sen sisällä olevat akut ja virran katketessa tämä tarjoaa akuissa olevan virran laitteille. Tyypillisesti useimmat varasähkölaitteet pystyvät syöttämään virtaa laitteille 5 – 30 minuuttia. Syöttöajan pituuteen vaikuttavat tarvittava virran määrä ja akkujen kapasiteetti. (Comparison of Static and Rotary UPS 2011.) Kuvassa 6 on esiteltyä tyypillinen laitekaapeissa käytettävä Cisco Catalyst 6500 -sarjan staattinen UPS-laite.



Kuva 6. Static UPS Cisco Catalyst 6500. (Cisco Catalyst 6500.)

Ennen Static UPS:n yleistymistä datakeskukset käyttivät varasähkölaitteina Rotary UPS -tekniikkaa. Silti nykypäivänä esimerkiksi Cisco Systems käyttää Rotary UPS-laitteita osana vuonna 2011 valmistuneessa Greenfieldin datakeskuksessa. Sen vahvuutena on huomattava suoritusteho verrattuna Static UPS-laitteeseen.

Heikkouksiin puolestaan kuuluvat käytöstä aiheutuva melu johtuen liikkuvista osista, ympäristöongelmat ja käyttökulut. Rotary UPS-laitteesta puhuttaessa yleensä tarkoitetaan moottorigeneraattorilla toimivaa UPS-laitetta. Se ei käytä ollenkaan akkuja kuten Static UPS-laite, vaan sähkökatkoksen tapahtuessa sähkömoottori pyörittää vauhtipyörää, joka antaa virtaa muutamia minuutteja UPS-laitteeseen kytketyille laitteille. Sähkömoottorin tilalla voi käyttää myös polttomoottoria, joten laitetta voi käyttää siihen asti, kunnes polttoaine loppuu. (Rotary 2014.)

Kuvassa 7 on Ciscon Greenfieldissä sijaitsevan datakeskuksen käyttämä Rotary UPS-laite.



Kuva 7. Rotary UPS-laite Ciscon datakeskuksessa. (Cisco Allen Rotary UPS.)

3.6 Palonestojärjestelmä

Palonestojärjestelmä on tärkeä osa datakeskuksen infrastruktuuria ja on tärkeää selvittää, millaisen järjestelmän laitetilalleen haluaa. Koska datakeskuksen sähkölaitteet ovat jatkuvassa käytössä vuorokauden ympäri, ne saattavat ylikuumentua, minkä seurauksena voi syntyä tulipalo. Tulipalosta aiheutuvat ongelmat, kuten tiedon menetys, laiteuudistukset ja ihmishenkien menetys, vaikuttavat yrityksen tulevaisuuteen negatiivisesti, ja siksi tulipalo on pystyttävä estämään. Nykytekniikalla pystytään myös ennaltaehkäisemään tulipalo alentamalla hapen määrää tilassa ihmishenkiä vaarantamatta. Laitetilan ilmaan lisätään typpeä, joten tulen syttyminen ei ole mahdollista. (Olzak, T.)

Palonestojärjestelmät jaetaan viiteen alaluokkaan, joita ovat:

- Tulipalon havaitsemisjärjestelmä - Laite huomioi mahdollisen tulipalon laitehuoneessa ja ilmoittaa siitä keskukselle tai palovastaavalle. Havaitsemisjärjestelmän on oltava laadukas, jotta turhilta hälytyksiltä vältyttäisiin.
- Palohälytin - Jotta taattaisiin myös työntekijöiden turvallisuus työpaikalla, pitää pystyä varoittamaan laitetilassa tapahtuvasta tulipalosta äänisummerilla.
- Kannettavat palonsammuttimet – Tulipalon etenemistä voidaan estää kannettavilla palonsammuttimilla, joita henkilökunta pystyy käyttämään ensitoimena.
- Virtakatkaisin - Monissa datakeskuksissa käytetään virtakatkaisinta, jolla pystytään katkaisemaan virta kaikista sähköverkkoon kytketyistä sähkölaitteista. Tältä tilanteelta halutaan kuitenkin välttyä, koska tällöin voidaan menettää tärkeää tietoa laitteista varmuuskopioiden puuttuessa.
- Tulipalon sammutusaine - Sammutusaineet jakautuvat kahteen olomuotoon: veteen ja kaasuun. Maailmalla eniten käytetty menetelmä rakennuksissa on katossa oleva vesisprinklerijärjestelmä, joka palon syttyessä ruiskuttaa vettä ympäri huonetta ja näin ollen sammuttaa tulipalon. Datakeskuskäytössä tätä menetelmää ei voi käyttää, koska sähkölaitteet eivät kestä vettä. Joutuessaan veden kanssa kosketuksiin ne rikkoutuvat ja voivat aiheuttaa pahemman ongelman kuin tulipalo, jota varten ne on tilaan hankittu. Tulipalon leviäminen voidaan estää

myös kaasujärjestelmällä. Kaasujärjestelmät käyttävät erilaisia kaasuja, jotka vaikuttavat tuleen eri tavoilla. Hiilidioksidi ja Inergen-kaasut poistavat hapen laitetilasta ja näin ollen tukahduttavat tulen. Kaasumainen palonsammutusjärjestelmä poistaa hapen kokonaan laitetilasta, joten henkilöiden liikkumisen tilassa pitää olla rajattua. Vaihtoehtoisesti voidaan myös käyttää esimerkiksi FM-200-palonsammutusjärjestelmää, joka imee lämmön pois tulesta ja aiheuttaa sen sammumisen. Tämän jälkeen imetty lämpö kuljetetaan ilmanvaihdon kautta ulos. (The mystical world of data center fire suppression.) Kuvassa 8 on esiteltyä kaasumainen palonestojärjestelmä.

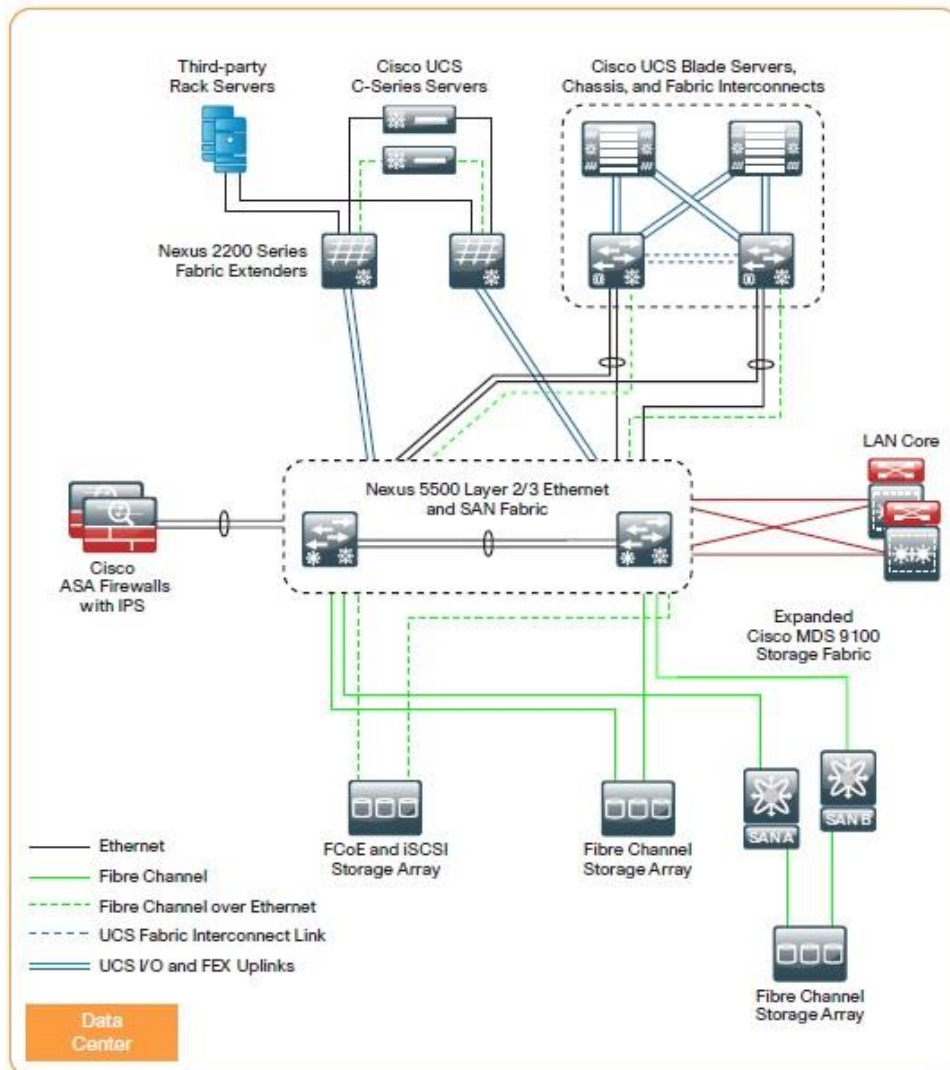


Kuva 8. Datakeskuksissa käytettävä kaasumainen palonestojärjestelmä. (Gas-Fire-Suppression.)

4 DATAKESKUSTEN ARKKITEHTUURI

Datakeskus on perusta laskentateholle, tiedontallennukselle ja sovelluksille, jotka ovat oleellinen osa yritysten liiketoimintaa. Datakeskuksen infrastruktuuri on keskeinen osa IT-arkkitehtuuria, jossa kaikki tiedonvaihto tapahtuu. Oikeanlainen suunnittelu datakeskuksen infrastruktuurissa on kriittistä, joten esimerkiksi suorituskyky ja järjestelmän skaalautuvuus pitää ottaa huomioon. Datakeskukset sisältävät kriittisiä laskentaresursseja kontrolloidussa ja keskitetyssä ympäristössä, joka mahdollistaa yritysten toimimisen kellon ympäri (Arregoces & Portolani 2003, 5).

Yksi tärkeä tekijä datakeskuksen suunnittelussa on joustavuus, jotta uusia palveluita voitaisiin jatkossa tukea. Joustavan arkkitehtuurin suunnittelun tuloksena voi olla huomattava etuasema kilpailijoihin verrattuna. Jotta arkkitehtuuri olisi joustava, vaaditaan alustavaa suunnittelua sekä seuraavat asiat on syytä ottaa huomioon: tietotekniikkalaitteiden porttien määrä, liityntäkerroksen laitteiden kaistanopeus, virtuaalisointi sekä palvelimien maksimikapasiteetti. Virtuaalisoinnilla voidaan luoda monia näennäisiä laitteita ja järjestelmiä niitä tukeviin verkkolaitteisiin. Virtuaalilaitteilla voidaan kokeilla ja toteuttaa suunnitelmia turvallisesti säästämällä samalla rahaa. Eräs suunnittelumalli on Ciscon Virtualized Multi-Tenant Data Center -malli joka määrittelee verkkolaitteiden toiminnot ja missä lokaatiossa ne sijaitsevat. (Cisco Data Center Infrastructure 2.5 Design Guide 12/2007.) Kuvassa 9 esitellään Cisco Systemsin ajankohtainen ratkaisu datakeskuksen arkkitehtuurin suunnittelulle.



Kuva 9 Datakeskuksen laitetopologia kuva (Data Center Technology Design Guide.)

4.1 Datakeskusten verkkoteknologiat

4.1.1 Fibre Channel

Fibre Channel -tekniikkaa (kuitukanavatekniikkaa) käytetään datakeskuksissa tiedon siirtämiseen tietovarastosta muuhun tietoverkkoon. Se pystyy tarjoamaan jopa 40 gigabitin/s tiedonsiirtonopeuden, joka eroaa vanhasta Ethernet-tekniikan tarjoamasta nopeudesta huomattavasti. Kuitukanavatekniikan heikkoudeksi muodostuu kuitenkin kaapelin maksimipituus, joka voi olla enintään 10 kilometriä. Tästä ei ole kuitenkaan haittaa datakeskuskäytössä, koska etäisyydet laitteiden välillä ovat vähäiset.

Tiedonsiirtonopeuden lisäksi kuitua käyttämällä säästetään tilaa verrattuna vanhoihin Ethernet Cat6 -kaapeleihin. (Two revolutionary optical technologies 10/2009.)

Kuitukanavatekniikassa käytetään fyysisellä tasolla optisia kuitukaapeleita, joissa hiuksen paksuiset lasista valmistetut putket kuljettavat valoa kaapelin päästä päähän. Kuten Ethernet-tekniikassa, kuitukanavatekniikassa on myös mahdollista kuljettaa sähköä laitteille verkon yli. Tätä tekniikkaa kutsutaan Power Over Fiber -tekniikaksi (Two revolutionary optical technologies 10/2009.)

4.1.2 Fibre Channel over Ethernet

Fibre Channel over Ethernet -teknologialla mahdollistetaan kuitukanavaliikenteen kuljettaminen jo valmiin Ethernet-infrastruktuurin päällä verkossa. Normaalisti datakeskuskäytössä verkko on jaettu Ethernet LANiin ja Fibre Channel SANiin. FCoE-teknologialla saadaan aikaiseksi konvergoitunut verkko, jota ylläpitäjän on helpompi hallita. Tätä voidaan kutsua myös I/O consolidationiksi. Menetelmällä mahdollistetaan vähäisempi kaapeleiden ja CNA-laitteiden määrä. (Fibre Channel over Ethernet (FcoE).)

4.2 Virtualisoitu datakeskus moniasiakasympäristössä

Eräs mahdollinen vaihtoehto kyberturvallisuuslaboratorion datakeskuksen toimittajaksi on Cisco Systems. Seuraavaksi tarkastelen pilvipalveluja tarjoavien datakeskusten suunnittelua tarkemmin juuri Cisco Systemsin suunnitteludokumenttien näkökulmasta.

Virtualized Multi-tenant Data Center -malli on syrjäyttänyt aikaisemmin käytetyn Ciscon Data Center Multi-Tier -mallin nykypäivänä pilvipalveluiden yleistymisen seuraksena. Pilviratkaisuilla parannetaan yrityksen kustannustehokkuutta sekä mahdollistetaan palveluiden skaalautuvuus jatkossakin. Kustannustehokkuutta parantaakseen yritys voi ulkoistaa toimintoja ulkopuolisen tahon hallittavaksi, joita ovat esimerkiksi palvelimet ja tietoturvalaitteet. Tätä menetelmää kutsutaan julkiseksi pilvimalliksi. (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

Virtualized Multi-tenant Data Center malli määrittää ”päästä päähän”-järjestelmän, joka on sopiva sovelluksen käyttöönottoon sekä julkisessa että yksityisessä pilvimallissa. ”Päästä päähän” – järjestelmä jakautuu osiin, jotka ovat datakeskus, runkoverkko, julkinen internet-yhteys, asiakas ja tiedonhallinta. Tenant-termillä tarkoitetaan asiakasyrityksen ryhmää eli hallintoaluetta. Hallintoalue voi sijaita yksittäisenä alueena tai yhdistää monta fyysistä aluetta saman pilven alle. (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

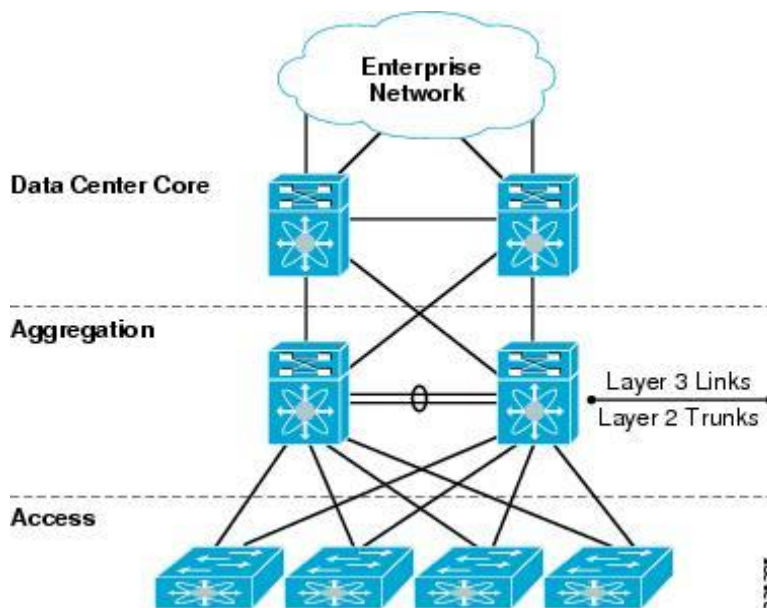
Jotta pystyttäisiin jakamaan dataa hallitusti eri hallintoalueiden välillä, datakeskukset luovat virtuaalisia verkkokortteja (vNIC), joista jokainen edustaa eri hallintoaluetta. Näiden lisäksi myös VLAN-tekniikka on tärkeä osa virtualisointia. VMware vSphere -ohjelmistolla hallitaan virtuaalisia palvelinklustereita datakeskuksen sisällä. Datakeskuskäytössä halutaan estää pääsy palvelimiin suoraan julkisesta verkosta. Tätä varten on kehitetty julkisen ja yksityisen verkon väliin DMZ-alue, jossa oleva välityspalvelin reitittää paketit palvelimelle ja päinvastoin. Välityspalvelimen toimintatapa on rinnastettavissa palomuriin, joten sitä voi käyttää rinnakkain jo valmiina olevan palomuurin kanssa. Tällä menetelmällä saadaan merkittävä lisäturva yrityksen datalle. (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

Redundanttisuus on tärkeä osa datakeskustekniikkaa. Sillä mahdollistetaan jatkuva datan kulku verkossa ja minimoidaan vikojen vaikuttaminen järjestelmän toimivuuteen. Sitä varten on kehitetty reitittimiin redundanttinen HSRP-protokolla. Sillä voidaan luoda kahteen reitittimeen sama virtuaalinen oletusyhdyskäytävä, joka ottaa reititystaulun hallinnan toisen mennessä vikatilaan. Reitittimet vaihtavat tilaviestejä toistensa kanssa, joten vian ilmetessä päällä olevasta reitittimestä tulee hallitseva reititin. Redundanttisuutta voidaan parantaa myös fyysisesti lisäämällä

jokaiselle yhteyslinkille monta liitäntäporttia käyttöön. (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

4.2.1 Three-Layer Hierarchical Model

Nykyisin datakeskuksissa käytetty VMDC -malli pohjautuu Ciscon vanhaan Three-Layer Hierarchical Modeliin. Datakeskuksen suunnittelijan on ymmärrettävä infrastruktuurin kokonaiskuva, joten on syytä selvittää, mitä eri kerroksilla tapahtuu. Kuvassa 10 on esiteltyä Cisco Three-Layer Hierarchical-malli.



Kuva 10. Ciscon Three-Layer Hierarchical-malli. (The Hierarchical Model in a Datacenter Network Switching Architecture.)

Core layer on järjestelmän runko, joka on suunniteltu vaihtamaan paketteja mahdollisimman nopeasti Aggregation-moduulien välillä. Laitteiden tulee tarjota paras mahdollinen saatavuus, jotta yhteydet pysyisivät koko ajan päällä. Core layer käyttää pakettien vaihtamiseen autonomisessa järjestelmässä verkon sisäistä reititysprotokollaa, joita ovat esimerkiksi OSPF, EIGRP ja BGP. Koko taso toimii pelkästään Layer3-ympäristössä. (Datacenter Core and Aggregation Design 12/2012.) Se toimii oletusyhdyksikäytävänä Campus Corelle, johon muut moduulit yhdistyvät, kuten esimerkiksi intranet ja WAN. Kaikki linkit Data Center Corelle terminoidaan Layer 3-tasolla, ja se yleensä käyttää 10 GigE:tä tukevia liitäntöjä, jotta suoritusteho olisi mahdollisimman optimaalinen. Datakeskuksen Core Layer eroaa Campus Core layerista ja sillä on erilaiset tarkoitusperät sekä vastuut. Se ei ole välttämätön osa

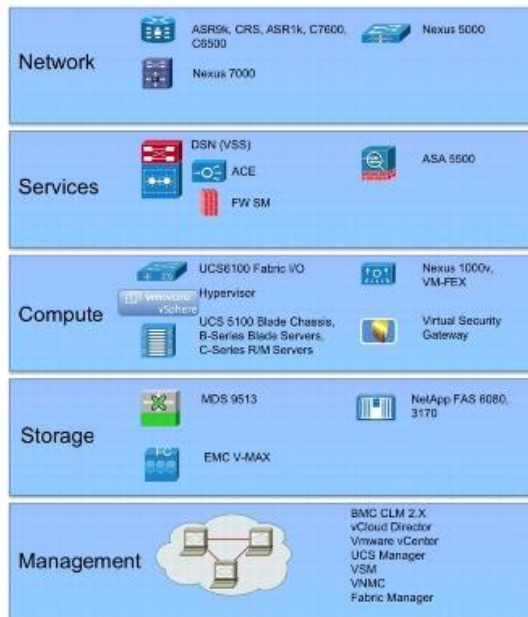
datakeskusta, mutta on silti suositeltavaa, että sitä käytetään. Erilliset Core layerit kuitenkin auttavat eristämään Campus Distribution layerit ja Data Center Aggregation layerit hallinnon ja politiikan mukaan. Näitä tekniikoita ja määreitä ovat esimerkiksi QoS, pääsylistat ja vianmääritys. (Data Center Multi-Tier Model Design.)

Aggregation layer on yhdistymispiste laitteille, jotka tarjoavat palveluita kaikille palvelinfarmeille. Esimerkkejä tarjotuista palveluista ovat palvelumoduulien integraatio, kuormanjako, Spanning Tree-prosessointi ja redundanttisuus. Aggregation layer toimii rajana Layer 2- ja Layer 3 -laitteiden välillä. Jotta yrityksen data kulkisi nopeasti ja estottomasti, Aggregation-kytkimien pitää tukea useita 10 GigE:n nopeuksia. Aggregation layer yhdistyy Core layeriin käyttäen edellä mainittuja 10 GigE:n portteja. Lisähyötynä Aggregation-kytkimien käyttämisessä on se, että polut dataliikenteelle ovat odotettuja, ja näin ollen niitä on yksinkertaisempi hallita. Aggregation layer tarjoaa myös palomuurauksen, jotta verkossa kulkeva data saataisiin suojattua kaikkiin suuntiin. (Cisco Data Center Infrastructure 2.5 Design Guide 12/2007.)

Access layer on arkkitehtuurin alin kerros, jossa kaikki palvelinfarmit ja muut päätelaitteet yhdistyvät verkkoon, ja se huolehtii verkossa kulkevien pakettien päätyemisestä loppukäyttäjille.

4.2.2 VMDC-tasot

Kuten Cisco Three-Layer Hierarchical -mallissa, Virtualized Multi-tenant Data Center -malli jakautuu tasoihin. Tasot määrittävät, mitkä verkon toiminnot tapahtuvat eri osa-alueilla, ja mahdollistavat tehokkaan ja skaalautuvan työympäristön, jota on helppo hallita. Kuvassa 11 ovat VMDC-tasot esittelyssä.



Kuva 11. VMDC tasot. (VMDC_2-2_DG_1-03.)

Network Layer - Sisältää verkon PE-reunalaitteet, jotka muodostavat kehän yrityksen verkon ympärille. Reunalaitteet hoitavat ulkoverkkoon menevän reitityksen ja tukevat myös Layer 2 -linkkiyhteyttä yrityksen datakeskuksien välillä. VMDC-arkkitehtuuri koostuu Nexus 7000 -kytkimistä, jotka toimivat core ja aggregation layerillä. Access layerin toiminnot hoitaa Nexus 5000 -sarjan laitteet.

Services Layer – Sisältää yrityksen verkon tietoturvalaitteet ja –palvelut, kuten kuormanjaon, palomuurauksen ja pääsyylistat. Tietoturvan lisäksi taso toimii päätepisteenä VPN-etäyhteyksille. Tärkeimpinä verkkolaitteina Services tasolla toimivat Cisco ASA 5500 -sarjan palomuurit. Palomuurauksella estetään verkkoon pääsy ulkopuolisilta tahoilta ja voidaan monitoroida jälkeenpäin verkkoon otettuja etäyhteyksiä. Cisco ASA 5500 -sarjan laitteet tukevat VRF-tekniikkaa, jonka avulla voidaan luoda laitteen sisälle virtuaalisia palomuuureja (Context). Tällä menetelmällä

parannetaan esimerkiksi yrityksen kustannustehokkuutta ja hallittavuutta. (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

Compute Layer - Compute layer jakautuu kolmeen osaan. Ensimmäinen on Virtual access switching taso, joka mahdollistaa L2-verkon ulottumisen fyysisiin laskentajärjestelmiin. Näihin lukeutuvat esimerkiksi fyysisissä palvelimisissa sijaitsevat virtuaalipalvelimet. Toisessa osassa sijaitsevat sovelluspohjaiset palvelut, joihin lukeutuu esimerkiksi Ciscon Virtual Security Gateway -palvelu. Ciscon Nexus-sarjan kytkimissä oleva VSG -palvelu tai toisin sanoen virtuaalinen palomuuuri mahdollistaa pakettien turvallisen kuljettamisen virtuaalikoneiden välillä. Kolmas osa käsittelee tietojenkäsittelyresursseja, joihin kuuluvat verkossa sijaitsevat fyysiset sekä virtuaaliset palvelimet. Cisco Unified Computing -järjestelmällä voidaan keskittää fyysiset ja virtuaaliset palvelimet yhdeksi kokonaisuudeksi, jotta hallittavuus olisi järjestelmällisempää. (Cisco Virtual Security Gateway 1/2014.)

Storage Layer – Tässä lohossa sijaitsevat tietoverkon niin sanotut tietovarastot. SAN-tietovarastot voidaan yhdistää yhdeksi kokonaisuudeksi FCoE-tekniikalla tason sisällä. Yleisimpiä tallennusjärjestelmiä ovat NAS ja SAN. Tallennusjärjestelmät pystyvät jakamaan tiedostoja verkon yli käyttäjille ilman, että datan pitäisi olla fyysisesti käyttäjien tietokoneilla. Tuettuja laitteita on esimerkiksi Ciscon MDS 9513 SAN-laite, joka tarjoaa verkon käyttäjille vakaan ja skaalautuvan ympäristön tiedostonjaolle.

Management Layer – Management layer sisältää ”loppupään” verkkolaitteet ja ohjelmistot, joilla voidaan hallita verkon infrastruktuuria. Hallintaohjelmiin kuuluvat esimerkiksi Ciscon UCS Manager (palvelimien hallinta), VMware Vcenter (virtuaalilaitteiden hallinta) ja Cisco Fabric Manager (tietovarastojen hallinta). (Cisco Virtualized Multi-Tenant Data Center 3/2013.)

5 YHTEENVETO JA POHDINTA

Oli ajoittain haastavaa saada näin valtavasta aiheesta johdonmukainen kokonaisuus aikaiseksi. Opinnäytetyön rakenne muuttui moneen otteeseen kuukausien aikana, ja etenkin yliopettaja Martti Kettusen neuvot rakenteen suhteen olivat todella tärkeitä. Datakeskuksen rakennosaa varten perehdyin Ciscon Virtualized Multi-Tenant Data Center -malliin. Tähän löytyi Cisco Systemsin sivuilta dokumentti, josta sai huomattavan määrän informaatiota, josta kertoa opinnäytetyössäni. Suunnitteluosaa varten materiaalia löytyi erinäisiltä internet-sivuilta, jotka toimivat tekniikassa ajankohtaisempina lähteinä. Etenkin Cisco Systemsin internet-sivuilta löytyi luotettavaa tietoa josta voi opiskella datakeskuksen toimintaa ja sen tarvittavia järjestelmiä.

Datakeskusten suunnittelijoiden on huomioitava kasvava ala ja sen tuomat haasteet. Virtuaalisointiin ja tietoturvallisuuteen on panostettava entistä enemmän. Ihmiset haluavat pääsyn ympärivuorokautisesti palveluihin ja tiedostoihin, joten pilvipalveluiden lisääntyminen on välttämätöntä tulevaisuudessa. Nykyaikana yhä useammat rikollisuusorganisaatiot keskittävät osan toimintaansa globaaliin tietoverkkoon, joten datakeskusten tietoturvan on oltava ajan tasalla. Suuret pörssiyritykset säilyttävät asiakkaiden henkilötietoja datakeskusten tietovarastoissa, ja niiden menettäminen on yritykselle sekä talouden, että maineen kannalta kriittistä.

Tekninen osaamiseni kasvoi valtavasti opinnäytetyötä tehdessäni ja mielestäni saavutin asetetun tavoitteeni opinnäytetyön lopussa. Opinnäytetyötä tehdessä ongelmia ei liiemmin syntynyt, mikä todennäköisesti johtui käytännön osan puutteesta. Datakeskus on laaja aihe, joten uskon, että kyberturvallisuuslaboratorion hankkeesta moni muukin tuleva neljännen vuoden opiskelija saa opinnäytetyön aiheen jatkossa itselleen. Toivonkin, että tätä tutkielmaa käytetään hyödyksi, kun tulevaisuudessa asennetaan fyysisesti sekä ohjelmallisesti varsinainen kyberturvallisuuslaboratorio ICT-laboratorion tiloihin.

LÄHTEET

Arregoces, M. & Portolani, M. 2003. Data Center Fundamentals. Cisco Press.

Best Practices Guide: Cabling the Data Center. Brocade 2007. Saatavissa:
http://www.brocade.com/downloads/documents/best_practice_guides/Cabling_Best_Practices_GA-BP-036-02.pdf [viitattu 12.4.2014].

Cheaper electricity for data centers in Finland. Tredea 3/2014. Saatavissa:
<http://www.tredea.fi/en/news/cheaper-electricity-for-data-centers-in-finland/> [viitattu 10.4.2014].

Cisco Allen Rotary UPS. Saatavissa: <http://www.datacenterknowledge.com/wp-content/uploads/2011/04/cisco-allen-rotaryups.jpg> [viitattu 2.4.2014].

Cisco Catalyst 6500. Cxtec. Saatavissa:
http://images.cxtec.com/ITEM_IMG/CISCO_6000W.jpg [viitattu 12.3.2014].

Cisco Data Center Infrastructure 2.5 Design Guide. Cisco Systems 12/2007.
Saatavissa:
https://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a008073377d.pdf [viitattu 1.3.2014].

Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches. Cisco Systems 5/2013.
Saatavissa: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/data_sheet_c78-618603.pdf [viitattu 8.5.2014]

Cisco UCS 6200 Series Fabric Interconnects. Cisco Systems 7/2013. Saatavissa:
http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-6200-series-fabric-interconnects/at_a_glance_c45-675242.pdf [viitattu 7.4.2014].

Cisco Virtual Security Gateway. Cisco Systems 1/2014. Saatavissa:
http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/virtual-security-gateway-nexus-1000v-series-switch/data_sheet_c78-618244.pdf [viitattu 8.5.2014]

Cisco Virtualized Multi-Tenant Data Center. Cisco Systems 3/2013. Saatavissa:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-2/design_guide/vmdcDesign22.pdf [viitattu 8.5.2014]

Comparison of Static and Rotary UPS. Carl Cottuli 2011. Saatavissa:
http://www.apcmedia.com/salestools/DBOY-78KRZE/DBOY-78KRZE_R2_EN.pdf
[viitattu 14.3.2014].

Datacenter Core and Aggregation Design. Cisco Systems 12/2012. Saatavissa:
<https://supportforums.cisco.com/docs/DOC-28501> [viitattu 1.3.2014].

Data Center Multi-Tier Model Design. Cisco Systems. Saatavissa:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_2.html [viitattu 6.3.2014].

Data Center Power and Cooling. Cisco Systems 8/2011. Saatavissa:
http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/white_paper_c11-680202.pdf [viitattu 27.3.2014].

Data Center Spaces. Standards Informant 2013. Saatavissa:
<http://blog.siemon.com/standards/tia-942-data-center-spaces> [viitattu 9.4.2014].

Data Center Technology Design Guide. Cisco Systems 8/2013. Saatavissa:
<http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-DataCenterDesignGuide-AUG13.pdf> [viitattu 8.5.2014]

Designing the Physical Infrastructure. Corning 11/2010. Saatavissa:
<http://www.corning.com/WorkArea/showcontent.aspx?id=34833> [viitattu 3.4.2014].

Fibre Channel over Ethernet (FCoE). Cisco Systems. Saatavissa:
<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/fibre-channel-over-ethernet-fcoe/index.html#~overview> [viitattu 10.4.2014].

Gas-Fire-Suppression. Saatavissa: <http://www.solarvps.com/wp-content/uploads/2013/12/Gas-Fire-Suppression.jpg> [viitattu 19.3.2014].

Google: Raise Your Data Center Temperature. Datacenter Knowledge 10/2008.

Saatavissa: <http://www.datacenterknowledge.com/archives/2008/10/14/google-raise-your-data-center-temperature/> [viitattu 27.3.2014].

Lessons on ups topologies. Reliable Resources. Saatavissa:

<http://www.relres.com/news/91/lessons-on-ups-topologies> [viitattu 12.3.2014].

Olzak, T. The mystical world of data center fire suppression. Saatavissa:

<http://www.techrepublic.com/blog/it-security/the-mystical-world-of-data-center-fire-suppression/> [viitattu 19.3.2014].

Perforated-Ventilating-raised-access-floor-tiles. Archiexpo. Saatavissa:

http://img.archiexpo.com/images_ae/photo-g/perforated-ventilating-raised-access-floor-tiles-56607-1844695.jpg [viitattu 12.4.2014].

Rittal CMC III. Rittal. Saatavissa: <http://www.rittal.com/content/en/webspecial/CMCIII.jsp> [viitattu 15.4.2014].

Rittal TS-IT-laitekaappi. Rittal. Saatavissa: [http://www.rittal.com/fi-](http://www.rittal.com/fi-fi/content/media/embilder/0home/fri120338900_ts-it_home_540x380_540x380.jpg)

[fi/content/media/embilder/0home/fri120338900_ts-it_home_540x380_540x380.jpg](http://www.rittal.com/fi-fi/content/media/embilder/0home/fri120338900_ts-it_home_540x380_540x380.jpg) [viitattu 16.4.2014].

Rotary. Storage Battery Systems 2014. Saatavissa:

<http://www.sbsbattery.com/products-services/by-application/critical-power/critical-power-products/ups-systems/rotary.html> [viitattu 15.4.2014].

Server Rack Ordering Guide. SRO. Saatavissa: <http://www.server-rack-online.com/server-rack-information.html> [viitattu 16.4.2014].

Smith, L. Data Center Construction Costs. Saatavissa:

<http://www.abrconsulting.com/UptimeDoc.htm> [viitattu 3.4.2014].

Suomi on datakeskusten luvattu maa... yksi pieni ongelma. Tietokone.fi 11/2013.

Saatavissa:

http://www.tietokone.fi/artikkeli/uutiset/suomi_on_datakeskusten_luvattu_maa_yksi_pieni_ongelma [viitattu 28.2.2014].

The Hierarchical Model in a Datacenter Network Switching Architecture. Pluribus Networks. Saatavissa: <http://pluribusnetworks.com/media/uploads/2014/01/29/The-Hierarchical-Model-in-Network-Switching-Architecture.jpg> [viitattu 8.5.2014].

TIA-942 Data Center Standards Overview. ADC Telecommunications 1/2006. Saatavissa: <http://www.te.com/content/dam/te/global/english/industries/enterprise-network-solutions/knowledge-center/documents/enterprise-white-paper-tia-942-data-center-standards-overview-102264ae.pdf> [viitattu 6.4.2014].

Tier Standards Overview. Colocation America. Saatavissa: <http://www.colocationamerica.com/data-center/tier-standards-overview> [viitattu 3.4.2014].

Two revolutionary optical technologies. The royal Swedish academy of sciences 10/2009. Saatavissa: http://web.archive.org/web/20110629061117/http://nobelprize.org/nobel_prizes/physics/laureates/2009/sciback_phy_09.pdf [viitattu 10.4.2014].

UPS-käsikirja. Eaton 2012. Saatavissa: http://pqlit.eaton.com/ll_download_bylitcode.asp?doc_id=24030 [viitattu 2.3.2014].

Use Best Practices to Design Data Center Facilities. Gartner 4/2005. Saatavissa: http://www.it.northwestern.edu/bin/docs/DesignBestPractices_127434.pdf [viitattu 14.4.2014].

VMDC_2-2_DG_1-03. Cisco Systems. Saatavissa: http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-2/design_guide/VMDC_2-2_DG_1.fm/_jcr_content/renditions/VMDC_2-2_DG_1-03.jpg [viitattu 8.5.2014].