

Atte Sorvo

# Blade-järjestelmän käyttöönotto

Metropolia Ammattikorkeakoulu  
Insinööri (AMK)  
Tietotekniikan koulutusohjelma  
Insinöörityö  
19.8.2012

Tekijä Otsikko	Atte Sorvo Blade-järjestelmän käyttöönotto
Sivumäärä Aika	53 sivua + 1 liite 19.8.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Lehtori Tapio Wikström Lehtori Marko Uusitalo
<p>Tämän työn tavoitteena oli Blade-järjestelmän käyttöönotto. Metropolia Ammattikorkeakoulun Bulevardin toimipisteen luokassa U205 olevaan palvelihuoneeseen asennettiin Blade-järjestelmä. Kyseessä oli vanha tuotantoverkosta poistunut Blade-kehikko, johon käyttöönoton yhteydessä asennettiin Blade-palvelimia ja verkkomoduuleja. Työssä suunniteltiin ja toteutettiin verkkoyhteydet Blade-kehikkoon kytkimen avulla.</p> <p>Työssä asennettiin joihinkin Blade-palvelimiin käyttöjärjestelmiä ja testattiin niitä. Laitteiden ja käyttöjärjestelmien toimivuus testattiin. Kaikkiin Blade-palvelimiin ei kuitenkaan asennettu käyttöjärjestelmiä. Työssä kokeiltiin virtualisointiratkaisuja Blade-palvelimilla. Blade-kehikko tuli koulun käyttöön ja opiskelijat voivat käyttää siihen luotavia virtuaalikoneita koulun kursseilla tai omissa projekteissaan.</p> <p>Työn tulos on raportti, jonka avulla on helppo saada käsitys aiheesta. Työssä suoritettiin onnistuneesti Blade-järjestelmän käyttöönotto ja testaus. Työn alussa asetetut tavoitteet saavutettiin.</p>	
Avainsanat	Blade, palvelin, virtualisointi

Author Title	Atte Sorvo Deployment of Blade System
Number of Pages Date	53 pages + 1 appendix 19 August 2012
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data Networks
Instructors	Tapio Wikström, Senior Lecturer Marko Uusitalo, Senior Lecturer
<p>This bachelor thesis was made to Metropolia University of Applied Sciences. The school needed a new Blade system to be deployed. The intention was to deploy a Blade system and install some Blade servers and modules there. The thesis completed, Metropolia is going to use the Blade servers for their own purposes.</p> <p>The intention was to plan and implement a network between the switch and Blade enclosure. The study explains the installation of certain operating systems and how virtual machines were made to work in the Blade servers. One of the most important things to manage by the Blade system is remote administration. Therefore the enclosure was configured remotely and the whole Blade system was tested properly.</p> <p>The result of the thesis is a report giving a view about the topic. The deployment of Blade system was completed successfully and the Blade system was fully tested. The goals of the study were thus accomplished.</p>	
Keywords	Blade, server, virtualization

# Sisälllys

## Lyhenteet

1	Johdanto	1
2	Palvelin	1
2.1	Yleistä	1
2.1.1	Asiakas-palvelin-malli	2
2.1.2	Palvelinlaitteisto	3
2.1.3	Palvelinten vikasietoisuus	4
2.1.4	Palvelinkeskus	4
2.2	Blade-palvelin	5
2.3	Blade-kehikko	6
2.3.1	Blade-kehikon edut	6
2.3.2	Blade-kehikon haitat	7
3	Reititysprotokollat	7
3.1	Yleistä	7
3.2	Linkkitilaprotokolla	9
3.3	OSPF	10
3.3.1	Aluetyypit	10
3.3.2	Dijkstran algoritmi	12
4	Virtuaalilähiverkko	12
4.1	Yleistä	12
4.1.1	VLAN:ien toiminta	13
4.1.2	Trunk	14
4.2	Spanning tree -protokolla	15
4.3	Multiple Spanning Tree	16
4.3.1	MST-instanssit	17
4.3.2	MST-vyöhykkeet	18
5	HP BladeSystem	18
5.1	HP BladeSystem c-sarja	18
5.2	HP Onboard Administrator	22

5.3	HP Integrated Lights Out	24
5.4	HP Virtual Connect	24
5.5	HP Intelligent Power Discovery	25
5.6	HP Intelligent Power Distribution Unit	26
5.7	HP Insight Control	26
5.8	HP BladeSystem Insight Display	27
6	Virtualisointi	29
6.1	Yleistä	29
6.2	VMware	29
6.2.1	Yleistä	29
6.2.2	VMwaren toiminta	30
6.2.3	VMware ESX Server	30
6.2.4	VMware ESXi Server	31
6.3	Hyper-V	31
7	Työn vaiheet	32
7.1	Blade-järjestelmän asennus	32
7.1.1	Blade-kehikon fyysinen asennus	32
7.1.2	Blade-palvelimien fyysinen asennus	33
7.1.3	Virtalähteiden asennus	33
7.1.4	Tuulettimien asennus	33
7.1.5	Virtual Connect -moduulien asennus	34
7.1.6	OA-moduulien asennus	34
7.1.7	Virtakaapeleiden kytkeminen	35
7.2	Verkkoyhteydet	35
7.2.1	Verkkoyhteyksien suunnittelu	35
7.2.2	Kytkimen ohjelmistopäivitys	36
7.2.3	Kytkimen konfigurointi	37
7.2.4	Kytkimen asennus	38
7.3	Blade-kehikon error-ongelmat	39
7.3.1	BladeSystemin virheet	39
7.3.2	Virheiden selvittäminen	41
7.3.3	Virheiden korjaus	41
7.4	Etähallinta	42
7.4.1	Etähallinta HP Onboard Administratorin avulla	42
7.4.2	Etähallinta HP Virtual Connectin avulla	42
7.4.3	Firmware-päivitykset	44

7.5	Käyttöjärjestelmien asennus Blade-palvelimille	46
7.5.1	VMware ESXi	46
7.5.2	Windows Server 2008 R2	47
7.6	Virtuaalikoneet Blade-palvelimissa	47
7.6.1	VMware	47
7.6.2	Hyper-V	48
7.6.3	Virtuaalikoneiden testaus	49
8	Yhteenveto	50
	Lähteet	51
	Liitteet	
	Liite 1. HP 3500 -kytkimen konfiguraatio	

## Lyhenteet

ABR	Area Border Router. Reititin, joka sijaitsee yhden tai useamman OSPF-alueen reunalla ja yhdistää ne alueet backbone-alueeseen.
ASBR	Autonomous System Boundary Router. Reititin, joka sijaitsee OSPF-alueen ja jonkun muun alueen välissä.
BGP	Border Gateway Protocol. Internetin tärkein reititysprotokolla, joka reitittää tietoliikenteen autonomisten systeemien välillä.
BIOS	Basic Input-Output System. Tietokoneohjelma, joka lataa käyttöjärjestelmän keskusmuistiin.
BPDU	Bridge Protocol Data Unit. Erityinen datakehys, jolla vaihdetaan tietoja kytkinten välillä.
CST	Common Spanning Tree. Spanning Tree -versio, joka tunnetaan standardista IEEE 802.1D.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, joka muuttaa nimelliset verkko-osoitteet IP-osoitteiksi.
Domain	Domain on toimialue, jossa joukkoa verkon laitteita voidaan hallita keskitetysti yhdeltä palvelimelta.
ECC memory	Error-correcting code memory. Virheenkorjauskoodi, joka havaitsee virheet koodissa ja korjaa ne automaattisesti.
EGP	Exterior Gateway Protocol. Internetin reititysprotokolla autonomisten järjestelmien yhdistämiseen. BGP on nykyään syrjäyttänyt EGP:n lähes kokonaan.

EIGRP	Enhanced Interior Gateway Routing Protocol. Ciscon kehittämä etäisyysvektoriprotokolla.
Hot swap	Hot swap on tekniikka, joka mahdollistaa jonkin laitteen osan vaihtamisen siten, että laite voi jatkaa koko ajan toimintaansa.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö, joka kehittää mm. tietotekniikan standardeja.
IGP	Interior gateway protocol. Sisäinen reititysprotokolla, joka vaihtaa tietoa autonomisten järjestelmien sisällä.
IGRP	Interior Gateway Routing Protocol. Ciscon kehittämä etäisyysvektoriprotokolla.
IPD	Intelligent Power Discovery. HP:n kehittämä teknologia IT-järjestelmien automatisointia varten.
IS-IS	Intermediate System To Intermediate System. TCP/IP-verkkojen linkktilareititysprotokolla
ISP	Internet Service Provider. Internet-palveluntarjoaja.
Kernel	Kernel eli ydin on tietokoneen käyttöjärjestelmän alin osa mahdollistaen muiden ohjelmien toiminnan.
Linux	Avoimen lähdekoodin käyttöjärjestelmä.
Load balancing	Load balancing on keino, jolla voidaan vähentää verkon kuormitusta tasaamalla kuorma useammalle linkille.
LSA	Link-state advertisement. Reitittimien välisiä linkkitiloja mainostetaan LSA-viestien avulla muille reitittimille.



MAC-osoite	Media Access Control address. Verkkokortin osoite, joka yksilöi laitteen Ethernet-verkossa.
MAC OS X	MAC OS X. Unix-pohjainen käyttöjärjestelmä.
OSPF	Open Shortest Path First. TCP/IP-verkkojen linkkilareititysprotokolla.
PDU	Power Distribution Unit. Jakaja on laite joka jakaa virtaa. Käytetään esimerkiksi palvelinhuoneissa ja palvelinkeskuksissa.
Ping	Työkalu tietokoneverkossa, jonka avulla pystyy testaamaan verkon toimivuutta.
PLC	Power line communication. Datasähkö tarkoittaa datasiirtoa sähköverkossa.
Reititystaulu	Reititystaulu sisältää tietoa tietoliikenneverkon reitityksestä eri kohteisiin. Reititystauluja on esimerkiksi reitittimillä ja layer 3 –tason kytkimillä.
RIP	Routing Information Protocol. Sisäisten verkkojen reititysprotokolla. RIP kuuluu etäisyysvektoriprotokolliin.
RIPv2	Routing Information Protocol versio 2. Kehittyneempi versio RIP:stä, joka tukee luokatonta reititystä.
Räkki	Räkki on laiteteline, johon voi asentaa fyysisesti eri laitteita.
SCSI	Small Computer System Interface. Tietokoneen ja oheislaitteiden väliseen viestintää.
SUV	Serial, USB, VGA. SUV-kaapeli, jolla voidaan yhdistää Blade-palvelimeen video- ja USB-laitteita, kuten näyttö, USB-tikku tai ulkoinen DVD-asema.

TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jonka avulla luodaan yhteyksiä internettiin yhteydessä olevien tietokoneiden kesken.
Topologia	Tietoliikenneverkon perusrakenne, joka kuvaa miten verkon laitteet on liitetty toisiinsa.
UPS	Uninterruptible Power Supply. Laite, joka pystyy takaamaan tasaisen virransyötön lyhyiden katkosten ajan sekä syöttöjännitteen epätasaisuuden aikana
UUID	Universally unique identifier. Open Software Foundationin standardoima tunnistusstandardi, joka tunnistaa laitteet tai järjestelmät numeron perusteella.
VLAN	Virtual LAN. Virtuaalilähiverkko on tekniikka, joka mahdollistaa fyysisen tietoliikenneverkon jakamisen loogisiin osiin.
Windows	Windows on Microsoftin kehittämä maailman tunnetuin käyttöjärjestelmien perhe.

## 1 Johdanto

Työn tarkoituksena on ottaa käyttöön vanha tuotantoverkosta poistunut Blade-järjestelmä. Blade-järjestelmä tulee Metropolia Ammattikorkeakoulun käyttöön.

Metropolia Ammattikorkeakoulun Bulevardin toimipisteen luokan U205 palvelinhuoneen laitetelineeseen asennetaan Blade-järjestelmä. Työssä käytetään HP BladeSystem c7000 Enclosure -merkkistä Blade-kehikkoa. Blade-kehikkoon asennetaan Blade-palvelimia ja moduuleja. Käytössä on HP ProLiant BL460c G1 -merkkisiä Blade-palvelimia. Blade-järjestelmän tärkeä hallintakeino eli etähallinta on yksi asia, jota työssä vaaditaan. Tarkoitus on testata virtuaalikoneita Blade-palvelimissa ja lopuksi Blade-järjestelmän toimivuus testataan.

Teoriaosuudessa esitellään HP BladeSystemia ja virtualisointia. Käytännön osuus on pitkälti Blade-järjestelmän käyttöönottoa ja etähallinnan avulla Blade-järjestelmän konfigurointia.

## 2 Palvelin

### 2.1 Yleistä

Palvelin tarkoittaa tietokonetta, joka suorittaa palvelinohjelmistojen välityksellä erilaisia palveluja muille ohjelmille joko tietokoneverkon kautta tai paikallisesti samassa tietokoneessa. Palvelinta käyttävää tietokonetta tai sovellusta kutsutaan asiakkaaksi (client). Palvelimet tarjoavat hyödyllisiä palveluita ympäri tietoverkkoa, joko organisaation sisäiseen käyttöön tai yleiseen käyttöön internetissä. Palvelimesta käytetään myös nimeä serveri.

Palvelin-termiä käytetään yleisesti tietotekniikassa. Yleensä palvelimet määritellään ohjelmistojen isännöintilaitteiksi. Tietokone tai tietokoneohjelmisto jakaa tietoa keskenään yhden tietokoneen toimiessa isäntänä toisille tietokoneille. Teoriassa mikä tahansa tietokoneistettu prosessi, joka jakaa resursseja yhdelle tai useammalle asiakasohjelmalle, on palvelin. Näitä ei kuitenkaan aina kutsuta palvelimiksi. Lähestulkoon mikä

tahansa tietokone voi toimia verkkopalvelimena, mutta varsinaisina palvelimina myydyt laitteet sisältävät tuotantoympäristöönkin sopivia toimintoja.

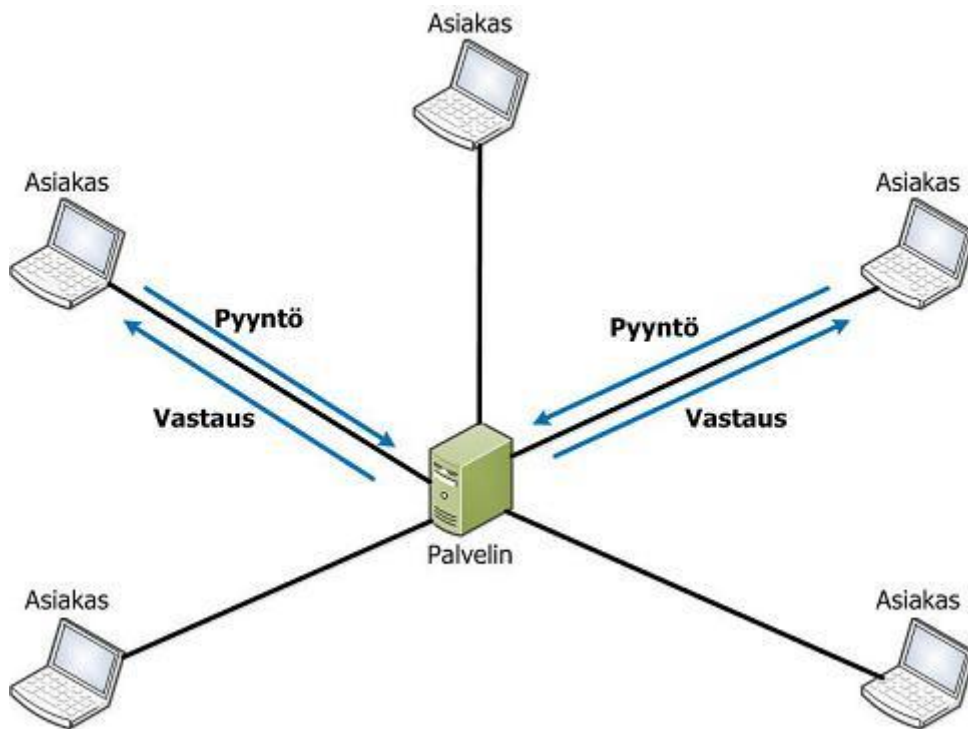
Monet palvelimet käynnistyvät ja lataavat käyttöjärjestelmän hitaasti. Palvelin suorittaa muistitarkastuksen ja etäpalveluiden varmistuksen. RAID tekee myös omat tarkastuksensa vikasietoisuuden tarkastamiseksi. Palvelimen käynnistys voi kestää useita minuutteja, mutta sen jälkeen se toimii pitkään ilman, että tarvitsisi käynnistää palvelinta uudelleen. Palvelimia ylläpitää yleensä jokin it-osasto, ylläpito voi olla ulkoistettu johonkin toiseen yritykseen.

Käyttöjärjestelmien suunnittelussa on pidetty mielessä asiakas-palvelin-malli. Nämä käyttöjärjestelmät mahdollistavat ohjelmistoille suoran pääsyn laitteen resursseihin. Käyttöjärjestelmää voidaan pitää käytettävää ohjelmistoa palvelevana laitteistona.

Yksi palvelimen tärkeistä ominaisuuksista on etähallinta. Laitteisiin on mahdollista saada erikseen etähallintakortteja. Palvelin voidaan sammuttaa, käynnistää uudelleen ja sitä voidaan hallita verkon yli etähallintakortin avulla, vaikka kone olisi kaatunut. [1.]

### 2.1.1 Asiakas-palvelin-malli

Tietotekniikassa tunnetaan asiakas-palvelin-malli (client-server), jossa palvelimen ja asiakkaan välinen kommunikaatio perustuu asiakkaan tekemään yhteydenottoon (request). Tässä mallissa asiakas tarkoittaa käyttäjän työasemassa toimivaa ohjelmaa. Palvelin on ohjelma, joka toimii tietokoneessa, joka tuottaa tietopalveluja. Palvelimella voi olla samaan aikaan monia yhteyksiä asiakkaisiin. Kaikki tietoliikenneverkossa olevat asiakasohjelmat voivat lähettää kyselyn palvelimelle. Palvelimen vastaus (response) kyselyyn on kertaluonteinen, eikä palvelin välttämättä muista kyseistä asiakasta enää sen jälkeen. Palvelimen ja asiakasohjelman välille ei siis synny erillistä istuntoa, vaan kyseessä on yhteydetön kummunkaatiotapa. Kommunikaatio ei perustu ennaltamääritettyyn kaksisuuntaiseen yhteyteen, vaan asiakkaan tekemään yhteydenottoon. Vapaasti käytettäviä tietopalveluja tarjoavassa koneessa ei käytetä käyttäjätunnuksia eikä salasanoja. Palvelu on tällöin julkinen eikä siihen tarvitse kirjautua käyttäjänä.



Kuvio 1. Asiakas-palvelin-malli

### 2.1.2 Palvelinlaitteisto

Palvelinkone poikkeaa jokseenkin laitteistopuolen osalta normaalista pöytäkoneesta. Edulliset palvelimet saattavat olla melko samanlaisia kuin pöytäkoneet. Isoissa palvelimissa laitteistossa saattaa olla useita rinnakkaisia prosessoreita, kaksi virtalähdettä, monta verkkoyhteyttä, SCSI ja RAID-levyjärjestelmä, jossa on useita rinnakkaisia levyjä.

Palvelimen laitteistovaatimukset vaihtelevat palvelinohjelmistosta riippuen. Prosessorin nopeus ei ole niin tärkeä tekijä palvelimissa kuin puolestaan pöytäkoneissa. Palvelimen velvollisuudet tarjota palveluita käyttäjille verkon yli johtavat erilaisiin vaatimuksiin, kuten nopeaan internet-yhteyteen ja korkeaan I/O -läpisyöttöön.

Palvelimet ovat yleensä yhteydessä verkkoon siten, ettei niissä ole näyttö kytkettynä. Monilla palvelimilla ei yleensä ole graafista käyttöliittymää, koska se kuluttaa resursseja eikä ole pakollinen palvelimen toiminnan kannalta. [1.]

### 2.1.3 Palvelinten vikasietoisuus

Yleensä palvelimet ovat päällä pitkään ilman katkoja. Palvelimen toiminnan luotettavuus on todella tärkeää, sillä palvelinten saatavuuden pitää olla hyvä. Yritysten kriittisille palvelimille pyritään takaamaan hyvä vikasietoisuus ja kenties laadukkaampaa laitteistoa, jotta voidaan maksimoida laitteen yhtäjaksoinen käyttöaika. Kriittisten palvelinten hankinnoissa ei kannata säästää rahaa virheiden uhalla, sillä lyhytaikaisetkin seisonnajat voivat tulla kalliiksi kriittisillä palvelimilla.

Palvelimet saattavat sisältää nopeita, korkean kapasiteetin kiintolevyjä, isoja tuulettimia tai vesijäähdytysratkaisuja lämpötilan säätelyn vuoksi. Palvelimissa saatetaan käyttää myös UPS:ja, jotka pystyvät takaamaan tasaisen virransyötön lyhyiden katkosten ajan sekä syöttöjännitteen epätasaisuuden aikana. Luotettavuutta parantavia tekijöitä on myös kiintolevyjen ja virtalähteiden tuplaaminen, jolloin laitteiston vikasietoisuus kasvaa. ECC-muisti, joka on on virheenkorjaavaa muistia, on yksi tapa, jolla voi välttää datassa ilmeneviä virheitä. Nämä komponentit nostavat hintaa, mutta mikä tärkeintä, suorituskyky ja luotettavuus säilyy korkealla tasolla. Joissakin palvelimissa on hot swap -mahdollisuus, joka mahdollistaa kiintolevyn tai virtalähteen vaihdon ilman palvelimen sammuttamista.

Vikasietoisuuden kasvattaminen onnistuu RAID-levyjärjestelmää käyttäen. RAID-levyjärjestelmässä on useita rinnakkaisia levyjä, jotka voidaan yhdistää yhdeksi loogiseksi levyksi. Täten saadaan levyjen vastaajat ja virheettömyys varmasti optimitasolle. RAID-levyjärjestelmässä on eri vaihtoehtoja varmistukseen, kuten RAID0 (lomitus), RAID1 (peilaus), RAID0+1 (lomitus ja peilaus), RAID5 (pariteettidatan käyttö) ja RAID6 (pariteettidatan käyttö), jossa RAID6-pakasta voi hajota kaksi levyä ilman datan menetystä. [1.]

### 2.1.4 Palvelinkeskus

Palvelimet vaativat fyysistä turvaa ja pitävät huomattavaa meteliä, joten palvelimet sijaitsevat yleensä erillisissä huoneissa tai palvelinkeskuksissa. Yleensä palvelimet sijaitsevat laitetelineissä tai muissa niille varatuissa paikoissa. Koska palvelinkeskuksessa voi olla tuhansia palvelimia, täytyy huolehtia lämpötilasta ja ilmastoinnista. Palvelinhuoneissa pitää olla sopiva lämpötila toimivuuden takaamiseksi. Täten huoneissa on

yleensä ilmastointi- tai jäähdytyslaitteita. Palvelinkeskukset jäähdytetään yleensä ilma-jäähdytyksellä, mutta myös vesijäähdytys on käytössä joissain palvelinkeskuksissa.

Palvelimia on eri mallisia ja kokoisia. Yleisimmät fyysiset palvelintyypit ovat rakkipalvelin, tornipalvelin, minirakkipalvelin ja Blade-palvelin. Palvelimet kiinnitetään laitetelineeseen tai vastaavaan jollain sopivalla keinolla. Koska palvelinhuoneissa ja -keskuksissa voi olla satoja tai tuhansia palvelimia, niin huoneet voivat olla hyvinkin täynnä laitetelineitä, jotka ovat täynnä palvelimia.

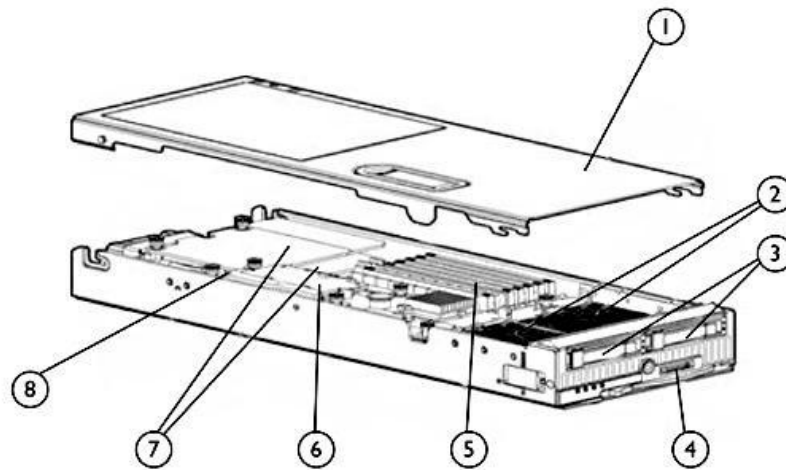
## 2.2 Blade-palvelin

Blade-palvelin on korttipalvelin, jossa palvelimen komponentit on mahdutettu pieneen tilaan. Sen kaikki komponentit ovat yhdellä piirilevyllä. Blade-palvelimet tuottavat enemmän virtaa pienemmässä tilassa ja niissä on yleensä edullisemmat hallintakustannukset kuin tavallisissa yhden yksikön palvelimissa. Blade-kehikossa kaapelointia on yksinkertaistettu huomattavasti. Blade-kehikossa säästetään virtaa, kun virtalähteet ovat automatisoituja ja tuottavat virtaa tarpeen mukaan.

Blade-palvelimet fyysiset komponentit on helppo päivittää. Vikatilanteissa Blade-järjestelmä ilmoittaa virheestä ja siitä, miten virhe voidaan korjata. Blade-palvelimet tukevat hot swap -tekniikkaa eli ne voi poistaa tai vaihtaa laitteen ollessa päällä. Vaikka verkkoyhteys Blade-palvelimen IP-osoitteeseen olisi mennyt poikki, Blade-palvelimeen pääsee käsiksi etänä iLO-hallintaosoitteen kautta. iLO tarkoittaa palvelimen etähallinta-ominaisuutta.

### HP ProLiant BL460c

HP ProLiant BL460c -palvelin on pieneen tilaan rakennettu Blade-palvelin eli korttipalvelin. HP ProLiant BL460c -korttipalvelimista on eri versioita. Tässä työssä käytettiin HP ProLiant BL460c G1 -korttipalvelimia. Nämä korttipalvelimet ovat puolikorkeita laitteita, eli kun ne asennetaan Blade-kehikkoon, täytyy kehikossa olla välilevyjä, jotta kehikon tilan voi hyödyntää täysin.



HP ProLiant BL460c Server Blade	
1. Access Panel	5. Eight (8) PC2-5300, Fully Buffered DIMMs (DDR2-667) Memory Slots
2. Up to two Intel® Xeon® 5000 Sequence processors	6. HP Smart Array E200i Controller with optional battery-backed write cache (standard BTO models)
3. Small form factor (SFF) hot-plug drive bays (standard BTO models)	7. Two Mezzanine slots
4. Local I/O connector	8. Internal USB Connector (standard BTO models)

Kuvio 2. HP ProLiant BL460c -korttipalvelin. [2.]

### 2.3 Blade-kehikko

Blade-kehikko on tyhjä runko, johon voidaan fyysisesti asentaa Blade-palvelimia, verkkomoduuleja, virtalähteitä ja tuulettimia. Blade-palvelimet asennetaan fyysisesti Blade-kehikkoon, jossa niitä ei tarvitse erikseen kaapeloida, koska kaikki kytkennät on tehty Blade-kehikon sisällä. Kehikon sisällä on liitäntöjä Blade-palvelinten ja moduulien välillä. Blade-palvelimille ei kytketä virtajohtoja ja verkkokaapeleita suoraan, vaan kaikki kytkennät tehdään Blade-kehikkoon. Kehikkoon voi asentaa useita palvelimia, verkkomoduuleita, virtalähteitä ja tuulettimia. Täten saadaan useita palvelimia samaan tilaan yksinkertaisella ratkaisulla.

#### 2.3.1 Blade-kehikon edut

Työssä käytettyyn Blade-kehikkoon mahtuu 16 Blade-palvelinta. Jos tavallisia yhden yksikön palvelimia laitettaisiin 16 kappaletta, ne veisivät huomattavasti enemmän tilaa ja verkkokaapeleita jouduttaisiin käyttämään huomattavasti enemmän, kun jokaiseen Blade-palvelimeen pitäisi kytkeä oma verkkokaapeli. Blade-kehikossa riittää uplinkit



molempiin ethernet-moduuleihin ja OA-moduuleihin. Mikäli käytetään kuitukytkimiä, niin siinä tapauksessa myös niihin kytketään verkkokaapelit.

### 2.3.2 Blade-kehikon haitat

Blade-järjestelmän hankinta ei ole edullista mikäli Blade-kehikkoon laitetaan vain muutama Blade-palvelin, koska Blade-järjestelmän runko on melko hintava. Blade-palvelimet eivät sovi kaikkiin it-ratkaisuihin. Väylän leveys ja muistin rajoittuneisuus saattavat muodostua pullonkaulaksi suurissa liiketoiminnan prosesseissa. Kun yritykseen on hankittu yhden valmistajan Blade-järjestelmä, sen vaihtaminen toisen valmistajan laitteisiin voi muodostua ongelmaksi, sillä toisen valmistajan laitteissa ei välttämättä ole kaikkia samoja elementtejä, joita yrityksessä tarvitaan.

## 3 Reititysprotokollat

### 3.1 Yleistä

Reititysprotokollat määrittelevät, miten reitittimet kommunikoivat keskenään. Reititysprotokollien avulla voidaan levittää tietoa siitä, miten tietoverkossa pääsee johonkin tiettyyn verkkoon. Reititysprotokollat valitsevat tietyn reitin tietoverkossa perustaen valinnan reititysalgoritmeihin. Reitittimet ja kolmostason kytkimet pystyvät suorittamaan IP-tason reititystä.

Reitittimet käyttävät reititysprotokollia vaihtaakseen tietoja internetin verkkojen rakenteesta. Reititysprotokollat jaetaan sisäisiin ja ulkoisiin reititysprotokolleihin. Yleisimmät sisäiset reititysprotokollat ovat RIP, RIPv2, IGRP, EIGRP, OSPF ja IS-IS. Ulkoisia reititysprotokollia ovat BGP ja EGP. Näistä EGP-protokollaa ei kuitenkaan käytetä juuri missään.

### Classification of routing protocols

	Interior Gateway Protocols				Exterior Gateway Protocols	
	Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector	
	<b>Classful</b>	RIP	IGRP			EGP
<b>Classless</b>	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4	
<b>IPv6</b>	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP for IPv6	

Kuvio 3. Ulkoiset ja sisäiset reititysprotokollat. [3.]

Reititysprotokollat käyttävät erilaisia metriikkoja, joiden perusteella reititin valitsee sopivimman reitin kohdeverkkoon. Metriikkaan voivat vaikuttaa esimerkiksi kapasiteetti, pituus, luotettavuus, viive tai hinta. Reititysprotokollat saattavat ilmoittaa metriikoiksi eri arvoja ja tämän takia valittava reitti ratkaistaan käyttäen hallinnollisen etäisyyden arvoa. Taulukossa 1 näkyy reititysprotokollien hallinnolliset etäisyydet. Hallinnollinen etäisyys merkitsee esimerkiksi silloin, kun reititin tekee päätöstä reittivalinnasta kahden eri reitin viedessä samaan kohteeseen. Hallinnollinen etäisyys määrittää reititysprotokollan luotettavuutta. [4.]

Taulukko 1. Reititysprotokollat ja niiden hallinnolliset etäisyydet. [5.]

Protokolla	Hallinnollinen etäisyys
Suoraan kytketty	0
Staattinen reitti	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
DHCP-learned	254
Tuntematon	255

Reititysprotokolla jakaa tietoa ensin suoraan kytketyille (directly connected) laitteille ja sen jälkeen edelleen verkon muihin laitteisiin. Tällä tavalla reititin saa tietoa verkon rakenteesta myös muilta reitittimiltä, kun muut reitittimet lähettävät omat reititysmainostuksensa. Lopulta kaikki verkon laitteet, joihin reititysprotokollat on konfiguroitu, tietävät verkon rakenteen ja voivat kommunikoida keskenään.

On olemassa sisäisiä ja ulkoisia reititysprotokollia. IGP (Interior gateway protocol) käyttää etäisyysvektoriprotokollaa (distance vector protocol) sekä linkkitilaprotokollaa (link state protocol). EGP (Exterior Gateway Protocol) käytetään BGP:ssä, jota käytetään ydintason (core) reititykseen internetissä.

### 3.2 Linkkitilaprotokolla

Linkkitilaprotokollan ominaisuuksiin kuuluu, että jokainen reititin näkee verkon kokonaistopologian ja pystyy itsenäisesti tekemään reitityspäätökset perustuen verkkotopologiaan. Tämän vuoksi jokaisen reitittimen täytyy pitää kirjaa sen naapurireitittimistä ja myös muista tietoverkon tai sen alueen reitittimistä ja niiden verkoista. Tämän lisäksi reitittimellä on jokaiseen verkkoon yksi reitti, jota se käyttää (best path).

Linkkitilaprotokolla vastaa nopeasti tietoverkon muutoksiin. Se lähettää päivityksen aina silloin, kun verkossa tapahtuu jokin muutos. Tällä vältetään turhat päivitysviestit, kun taas jossakin reititysprotokollissa lähetetään määräajoin viestejä, vaikkei muutoksia olisi tapahtunut. Tällaisissa tapauksissa jonkin yhteyden katkeaminen huomataan vasta, kun tasaisin väliajoin lähetetty viesti saapuu reitittimelle. Linkkitilaprotokollan tietokantaan lähetetään LSA-mainostuksia, jolla vahvistetaan, ettei topologiassa ole tapahtunut muutoksia. Tällä estetään tiedon vanheneminen. [6.]

#### LSA

LSA eli Link-state advertisement tarkoittaa linkkitilan mainostusta. LSA:t ovat tietokantojen tietoa, jotka muodostavat kokonaisen OSPF-alueen topologian, kun kaikki LSA:t yhdistetään. LSA-tyyppejä on kaikkiaan 11 kappaletta. Kun verkossa tapahtuu muutos verkkotopologiassa, reititin, johon muutos vaikuttaa, luo LSA:n koskien kyseistä linkkiä. LSA:ta kutsutaan myös nimellä PDU. LSA lähetetään multicastina kaikkiin samassa OSPF-alueessa oleviin naapurilaitteisiin käyttäen osoitetta 224.0.0.5 tai 224.0.0.6. Rei-

tittimet, jotka vastaanottavat LSA:n, lähettävät sen kaikille omille naapurilaitteilleen, pois lukien sille, josta se on vastaanotettu. Reitittimet, jotka vastaanottavat LSA:n, liisäävät ne omiin linkkitilietokantoihinsa (LSDB). LSDB:ta käytetään parhaan reitin laskemiseen. Parhaan reitin laskeminen perustuu Dijkstran shortest path first -algoritmiin. [4.]

### 3.3 OSPF

OSPF eli Open Shortest Path First on link-state-reititysprotokolla. OSPF perustuu avoimiin standardeihin ja on organisaation sisäinen TCP/IP-verkkojen reititysprotokolla. OSPF käyttää Dijkstran algoritmia löytääkseen optimaalisimman reitin. OSPF on kenties kaikista yleisimmin käytetty IGP-protokolla suurissa yritysverkoissa. Nykyään IPv4-osoitteiden käyttämä OSPF-versio on numeroltaan 2. IPv6-osoitteita varten on kehitetty OSPFv3.

OSPF:ssa samassa broadcast domainissa olevat reitittimet muodostavat naapurisuhteita (neighbor relationships) huomatessaan toisensa. Reititin tunnistaa itsensä ja muut hello-paketeilla. Ethernet ja frame-relay -verkoissa olevat reitittimet valitsevat joukostaan DR:n ja BDR:n, jotka toimivat keskuksena vähentääkseen reitittimien välistä liikennettä. Point-to-point-verkoissa ei tehdä DR/BDR-valintoja. OSPF pystyy käsittelemään eripituisia aliverkkomaskeja ja osaa yhdistää useita alueita yhdeksi loogiseksi alueeksi.

OSPF lähettää reititystaulut naapurireitittimille vain silloin, kun reititystauluissa tapahtuu muutoksia. OSPF tarjoaa ratkaisun vikasietoisen reititinverkon rakentamiseen. Linkin statuksesta eli tilasta huomataan, jos linkki katoaa. Oletusaika on nyt 10 sekuntia. Tätä aikaa on mahdollista säätää pienemmäksi, jolloin linkin puuttuminen havaittaisiin aikaisemmin. [4.]

#### 3.3.1 Alueityypit

OSPF-domain on jaettu alueisiin 32-bittisillä aluetunnisteilla. Aluetunnisteet kirjoitetaan yleensä esimerkiksi 0.0.0.1 -muodossa, mutta saman voi myös kirjoittaa pelkällä numerolla 1. Aluetunnisteita ei pidä sekoittaa IP-osoitteisiin. IP-osoitteet ja aluetunnisteet

voivat olla samoja lukuja ilman, että niistä olisi haittaa kummankaan toiminnalle. Alueet ovat laitteiden ja verkkojen loogisia ryhmiä. Jokainen OSPF-alue ylläpitää omaa linkkitietokantaansa.

OSPF:n alueella on olemassa erityyppisiä reitittimiä, kuten sisäinen reititin, alueen reunareititin (ABR) ja autonomisen järjestelmän rajareititin (ASBR). OSPF:n normaali alue tarkoittaa jotakin muuta kuin runkoverkon aluetta, mutta se ei kuitenkaan ole mitenkään rajoitettu.

Suuri OSPF-alue jaetaan yleensä pienemmiksi alueiksi. Alueen sisällä olevan reitittimen muistissa on alueen sisäinen topologiakuvaus. Alueen ulkopuolisen liikenteen ohjaamiseen käytetään reunareitittimien antamia tietoja. Reitittimien ei tarvitse pitää muistissa niin laajaa reititystaulua ja topologiatietoja, kun alue pilkotaan pienemmiksi alueiksi, jolloin reittien laskeminen käy reitittimiltä nopeammin. Kun OSPF-verkko jaetaan alueisiin, on myös helpompaa ylläpitää verkkoa. Reitittimiä ei suositella liitettäväksi useisiin eri alueisiin, koska tällöin reitittimen kuormitus kasvaa. Alueen reunareititin pyörittää samaan aikaan kahta eri OSPF-prosessia. OSPF-reititysprotokollassa on mahdollista konfiguroida eri alueita ja tehdä niistä erilaisia. OSPF-alueita ovat runkoverkkoalue, stub area ja NSSA. Näiden lisäksi OSPF-alueita ovat totally-stubby area ja NSSA totally-stubby area, mutta niitä voi käyttää vain Ciscon laitteilla. [4.]

#### Backbone area

Runkoverkkoalue tunnetaan yleisemmin nimellä backbone area. Tämä tarkoittaa siis aluetta 0.0.0.0 eli 0. Runkoverkkoalue muodostaa OSPF-verkon ytimen. Kaikki muut alueet on yhdistetty siihen. Alueiden välistä reititystä (inter-area routing) tapahtuu runkoverkkoalueeseen ja toiseen alueeseen kytkettyjen reitittimien kautta. Tämä on OSPF-domainin looginen ja fyysinen rakenne.

Runkoverkkoalue on vastuussa reititystiedon jakamisesta muiden aluiden välillä. Runkoverkkoalueen täytyy olla toisen alueen viereinen alue, mutta toisen alueen ei tarvitse olla fyysisesti yhdistetty suoraan runkoverkkoalueeseen. Yhteys runkoverkkoalueeseen voidaan tehdä virtuaalilinkkejä hyväksi käyttäen. [7.]

#### Stub area

Stub area eli tynkä alue ei vastaanota ulkoisia reititysmainostuksia, reititys alueen sisältä ulospäin perustuu täysin oletusreittiin. Alue ei vastaanota summary-reittejä muilta reititysprotokollilta paitsi OSPF:lta. Stub-alueella pitää siis olla oletusreitti, jotta paketit kulkevat alueelta ulospäin. Stub-alueita käytetään yleensä hub-and-spoke-verkoissa.

Not-so-stubby area

Not-so-stubby area eli NSSA on laajennus stub-alueesta. NSSA on stub-alue, johon tuodaan alueiden ulkopuoliset reitit ja ne lähetetään muiden alueiden reitittimille. NSSA ei voi vastaanottaa alueen ulkopuolisia reittejä muilta reitittimiltä.

### 3.3.2 Dijkstran algoritmi

Dijkstran algoritmia käytetään OSPF:ssa optimaalisimman reitin löytämiseen. Dijkstran algoritmi etsii lyhyimmän polun (shortest path) yhdestä pisteestä muihin pisteisiin. Täten muodostuu shortest path tree, jossa yhdestä pisteestä on selvitetty lyhin reitti kaikkiin muihin pisteisiin.

Algoritmi laskee reittejä pisteestä toiseen. Ensin algoritmi etsii polun, jolla on pienin kustannus. Jos lähdetään pisteestä A, niin kaikki siitä lähtevät reitit alkavat pisteestä A ja kulkevat pisteen A jonkun viereisen pisteen kautta eteenpäin. Ensimmäinen polku pisteestä A on helppo nähdä, sillä se on suoraan se polku, jonka kustannus on pienin. Sen jälkeen reittien kustannukset lasketaan laskemalla polkujen kustannukset yhteen. Reitti tiettyyn pisteeseen valitaan käyttäen pienimmän kustannuksen aiheuttavaa reittiä kyseiseen pisteeseen. [8.]

## 4 Virtuaalilähiverkko

### 4.1 Yleistä

Virtuaalilähiverkko eli VLAN on tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin. Esimerkiksi yrityksessä voidaan haluta jakaa tietoliikenneverkkoja eri osastojen kesken. Tämä onnistuu helposti virtuaalilähiverkoilla. Virtuaalilähiverkkoon voi liittää tietokoneita, ja ne toimivat kuin ne olisivat fyysisesti samassa verkossa riip-

pumatta niiden fyysisestä sijainnista. Virtuaalilähiverkolla on samoja ominaisuuksia kuin lähiverkolla ja tietokoneet toimivat virtuaalilähiverkossa samalla tavalla kuin lähiverkossa, vaikka tietokoneita ei olisikaan kytketty samaan kytkimeen.

Virtuaalilähiverkot vaativat toimiakseen sitä tukevat kytkimet ja reitittimet. Virtuaalilähiverkkoja tukevat laitteet merkitsevät lähetettyihin kehyksiin tunnukset, joista tietää, mihin virtuaalilähiverkkoon kyseinen paketti kuuluu. Laitteelta lähtevät broadcast- ja multicast-paketit lähetetään vain niihin kytkimen portteihin, jotka kuuluvat samaan virtuaalilähiverkkoon. Koska jokainen päätelaite käsittelee broadcast-kehukset, virtuaalilähiverkkojen käyttö nopeuttaa verkon toimintaa, kun broadcast-viestit eivät välity turhiin päätelaitteisiin eivätkä täten kuormita verkkoa.

Kytkimet vastaavat VLAN:ien määrittämisestä porttien, osoitteiden tai käyttäjien perusteella. Kytkimet välittävät VLAN-tiedon trunk-porttien välityksellä. Virtuaalilähiverkkojen välinen liikenne reititetään ja sen turvallisuutta pystytään parantamaan tekemällä suodatuslistoja. Eri virtuaalilähiverkot voivat kommunikoida keskenään reitittimen välityksellä.

Virtuaalilähiverkkojen avulla aliverkot ovat virtuaalisia, konfiguraatiomuutokset vähenevät ja verkkojen hallinta on keskitettyä. Virtuaalilähiverkon tuomat edut ovat kustannusten väheneminen, turvallisuus, parempi hallittavuus ja korkeampi suorituskyky.

Valmistajien välisen yhteensopivuuden takaamiseksi virtuaalilähiverkon laitteissa noudatetaan määrättyjä protokollia. Yleisin virtuaalilähiverkkoprotokolla on IEEE 802.1Q, joka tunnetaan myös nimellä Dot1q. Ciscon ISL-protokolla on toinen käytössä oleva standardi, jonka merkitys tosin on vähenemässä. [9.]

#### 4.1.1 VLAN:ien toiminta

VLAN:t toimivat access-kerroksella. Niiden ei pidä yltää muihin kerroksiin (distribution, core), paitsi distribution-kerroksen kytkimeen. Liikenne reititetään paikallisesta VLAN:sta distribution-kerroksen kautta core-kerrokselle. Jos VLAN-porttiryhmä on olemassa vain yhdessä laitteessa, VLAN-ryhmien portteja ei tarvitse merkitä taggediksi, vaan ne portit ovat untagged. Tagged mahdollistaa useamman VLAN:n liikenteen kulun toiseen laitteeseen jonkin portin kautta.

Jos kytkimelle ei ole konfiguroitu VLAN:ja, niin kytkimellä ei ole yhtään VLAN:ia, mikäli VLAN:ia ei ole otettu käyttöön. Jos VLAN on otettu käyttöön, mutta kytkintä ei ole konfiguroitu, niin kytkimeltä löytyy oletus-VLAN (default VLAN), johon kuuluvat kaikki kytkimen portit. Oletus-VLAN:n ID on numeroltaan yleensä 1.

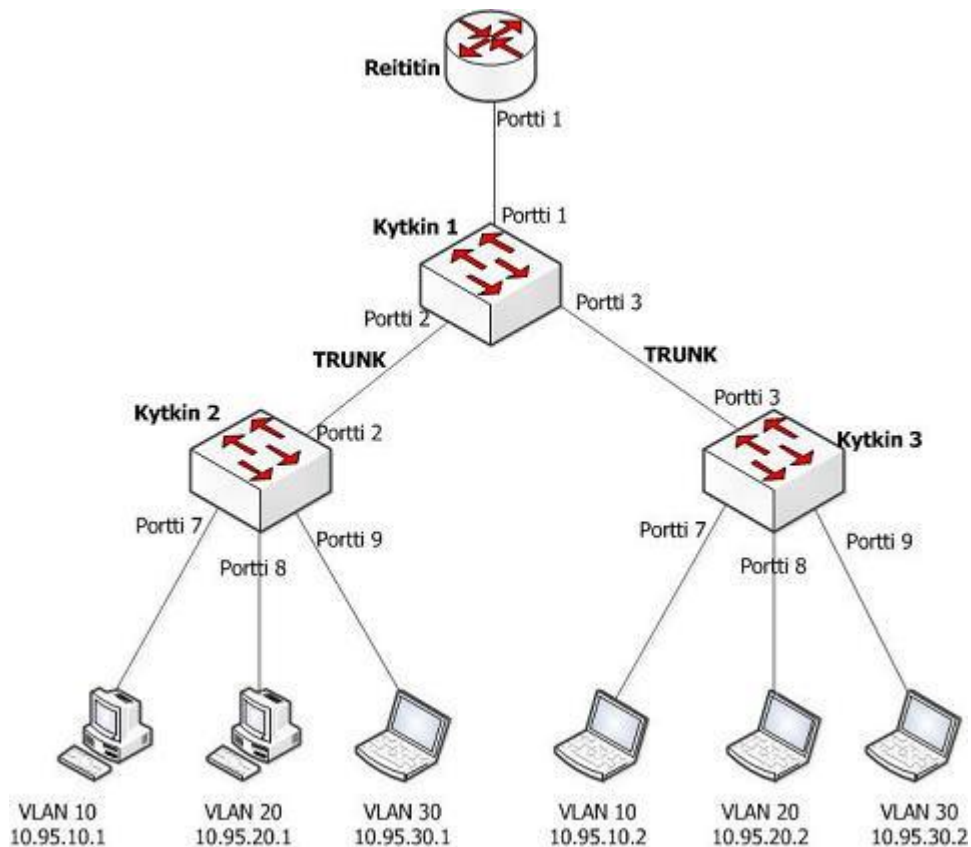
Kun ensimmäinen VLAN luodaan ja siihen lisätään siihen kuuluvat portit, niin kyseiset portit poistetaan samalla oletus-VLAN:n porteista. Tämä ensimmäinen konfiguroitu VLAN on itse asiassa laitteen toinen VLAN, koska oletus-VLAN luodaan aina automaattisesti kytkimeen. VLAN voidaan nimetä helpommin tunnistettavalla nimellä. Kaikki käsittely tehdään kuitenkin numeron perusteella. [9.]

#### 4.1.2 Trunk

Trunk-linkit voivat välittää kaikkien VLAN:ien liikenteen yhden fyysisen linkin kautta trunking-protokollaa käyttäen. VLAN voi kommunikoida samaan VLAN:iin kuuluvan laitteen kanssa trunk-linkin välityksellä, vaikka ne sijaitsisivat fyysisesti eri lähiverkoissa.

Yksilöllisistä VLAN:eista tulevat kehykset täytyy tunnistaa, jotta useat VLAN:t voidaan sallia yhdellä linkillä. IEEE 802.1Q on yleisin ja suosituin keino tähän. Se lisää ethernet-kehukseen tagin, leimaten sen kuuluvaksi tiettyyn VLAN:iin. 802.1Q käyttää siis kehyksen sisäistä tag-merkintää ja muokkaa näin ethernet-kehystä. Tämän takia 802.1Q toimii sekä access- että trunk-linkeissä. Koska 802.1Q on avoin standardi, sen ainoana vaihtoehtona on ympäristö, joka käy useammalle laitteelle. Ciscon ISL on myös trunking-protokolla, mutta se toimii vain Ciscon laitteissa.





Kuvio 4. Esimerkkikuva VLAN-verkosta.

Kuviossa 4 näkyy, miten trunk-linkkien on tarkoitus toimia. Kuvan trunk-linkit kuljettavat VLAN:ien 10, 20 ja 30 liikennettä. IP-osoitteen 10.95.10.1 tietokone voi kommunikoida 10.95.10.2 tietokoneen kanssa trunk-linkkien välityksellä. Trunk-linkit täytyy konfiguroida samalla tavalla molemmista päistä. Ciscon ja HP:n kytkimien konfiguroinnissa on tiettyjä eroja trunk-linkkien kohdalla. Ciscon konfigurointikomento trunk tarkoittaa HP:n tagged porttia. HP:n trunk puolestaan tarkoittaa Ciscon Etherchannelia.

#### 4.2 Spanning tree -protokolla

Spanning tree -protokollaa käytetään kytkimissä mahdollisten silmukoiden ja broadcast-myrskyjen estämiseksi. Spanning tree -protokollasta käytetään lyhennettä STP. STP:n avulla saadaan aikaan verkko, johon ei muodostu silmukoita, vaan verkko toimii järkevästi ilman turhaa liikennettä. Kytkimet suorittavat neuvottelut STP:n avulla. IEEE:n standardi 802.1D määrittää Spanning tree -protokollan. STP on TCP/IP-

protokollan linkkikerroksen protokolla. STP toimii ainoastaan access- ja distribution-kerrosten kytkimillä.

Kytkimet välittävät verkkoliikennettä tiettyyn porttiin MAC-osoitteiden perusteella. Jos kytkin ei tunne kehyksen kohde-MAC-osoitetta, kehys tulvii kytkimen kaikkiin portteihin paitsi siihen porttiin, josta se on tullut. Samoin käy, mikäli kehys on tyypiltään broadcast tai multicast. Silmukoita ja broadcast-myrskyjä muodostuu helposti, mikäli kehykset tulvivat.

STP sallii vikasietoiset varayhteydet, jotka otetaan automaattisesti käyttöön, mikäli aktiivinen yhteys katkeaa. Kytkinten konfiguraatiossa on määritelty varayhteydet, eikä niitä tarvitse ottaa käyttöön manuaalisesti, vaan toiminta on automatisoitua. Varayhteydet on oletuksena kytketty pois päältä eikä niitä voi silloin käyttää. [10.]

Taulukko 2. Spanning tree –protokollat. [10.]

Protokolla	Lyhenne	Standardi	Kattavuus	Toiminta
Common Spanning Tree	CST	802.1D	Kaikki VLAN:t	Hidas
PerVLAN Spanning Tree Plus	PVST+	Cisco	Per VLAN	Hidas
Rapid Spanning Tree Protocol	RSTP	802.1w	Kaikki VLAN:t	Nopea
PerVLAN Rapid Spanning Tree Plus	PVRST+	Cisco	Per VLAN	Nopea
Multiple Spanning Tree Protocol	MSTP	802.1s	VLAN-lista	Nopea

### 4.3 Multiple Spanning Tree

Multiple Spanning Tree eli IEEE 802.1s on laajennos IEEE 802.1w RST -algoritmista. Multiple Spanning Tree tunnetaan nimellä MST. MST:ssa yhdistyy PVST+:n ja 802.1Q:n parhaat ominaisuudet. MST on monimutkaisempi kuin normaali spanning tree. MST:n tarkoitus on vähentää spanning tree -instanssien määrää, jotta kytkimien prosessorien kuormitus vähenisi ja se täsmäisi fyysisen topologian kanssa. VLAN:t voidaan kartoittaa

spanning tree -instansseihin, koska suurin osa tietoliikenneverkoista ei tarvitse kuin muutaman loogisen topologian. MSTP eli Multiple Spanning Tree Protocol on samanlainen kuin Ciscon Multiple Instances Spanning Tree Protocol (MISTP). MSTP on muodostunut STP:n ja RSTP:n (Rapid Spanning Tree Protocol) kehityksen johdosta.

Perinteinen STP toimii kunnolla, jos verkossa on vain yksi VLAN. MSTP sallii useiden MST-vyöhykkeiden muodostamisen, jotka pystyvät käyttämään useita MST-instansseja. Useat vyöhykkeet ja STP-kytkimet on kytketty keskenään käyttäen common spanning tree:ta (CST). Kaikki MSTP:n spanning tree -data on yhdessä BPDU-formaatissa.

#### 4.3.1 MST-instanssit

MST pystyy kartoittamaan useita VLAN:ja yhteen spanning-tree -instanssiin. MST spanning tree -instanssin voi konfiguroida vain kytkimiin, jotka ovat siihen yhteensopivia. Konfiguroimalla kytkimet samalla MST-konfiguraatiolla, ne voivat osallistua samaan spanning tree -instanssien joukkoon.

Jokaisella instanssilla voi olla oma topologiansa, joka on riippumaton muista spanning tree -instansseista. MST-arkkitehtuuri parantaa verkon vikasetoisuutta. Tämä arkkitehtuuri mahdollistaa dataliikenteelle useat polut ja load balancingin käytön. Verkkoyhteyden katkeaminen yhdeltä reitiltä ei vaikuta toisiin instansseihin, joilla on toiset reitit. Eri VLAN:ien ja spanning tree -topologioiden käyttö tekee verkon ylläpidosta helpompaa isoissa verkoissa.

MST sallii usean spanning tree:n rakentamisen trunk-linkkien yli ryhmittämällä VLAN:t ja liittämällä ne spanning tree -instansseihin. Verkossa voi olla esimerkiksi 1000 VLAN:ia, jotka on jaettu kahden kytkimen välille tasan. Tällöin molemmilla kytkimillä on 500 VLAN:ia. MSTP asettaa tällöin vain kaksi instanssia, jolloin jokaisella kytkimellä suoritetaan vain kahta instanssia. Kaksi erillistä STP-topologiaa vaatii kaksi MST-instanssia. Tässä tapauksessa on vain kaksi loogista topologiaa, joten kaksi spanning tree -instanssia riittää mainiosti. Täten ei tarvitse pyörittää tuhatta instanssia.

### 4.3.2 MST-vyöhykkeet

MST-vyöhyke tarkoittaa joukkoa keskenään kytkettyjä kytkimiä, joilla on sama MST-konfiguraatio. Kytkimillä pitää olla samat määrittymiset konfiguroituna ollakseen osa yhteistä MST-vyöhykettä. Jotta kytkimet tietävät, missä instansseissa VLAN:t toimivat, niiden konfiguraatioiden täytyy täsmätä nimen, tarkastusnumeron ja 4096-elementtitaulun osalta. 4096-elementtitaulu liittää mahdolliset 4096 VLAN:t instanssiin. Näiden määrittysten monistaminen kaikkiin vyöhykkeen kytkimiin on verkon ylläpitäjän vastuulla.

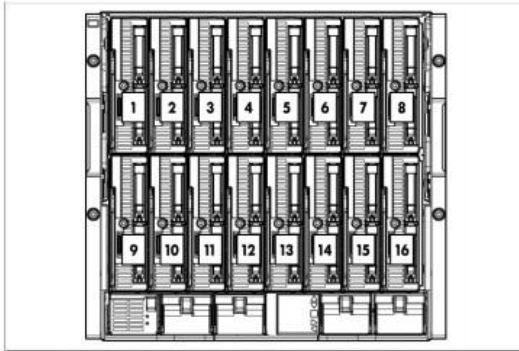
Protokollan täytyy tunnistaa vyöhykkeiden rajat, jotta se pystyy suorittamaan johdonmukaisen kartoituksen VLAN:t instansseiksi. Kytkimien täytyy tietää, mitkä naapurikytkimet ovat niiden kanssa samalla vyöhykkeellä. Kytkimet lähettävät vain digest:n, jossa on ainoastaan tarpeelliset tiedot verkon kuormituksen välttämiseksi. MST-vyöhykkeen ominaisuudet sisältyvät BPDU-kehysiin. Kytkimen vastaanottaessa BPDU:n se purkaa message digest:n, joka on matemaattisella funktiolla saatu numeerinen arvo. Arvoa verrataan sen omaan laskettuun digestiin. Jos digestit eroavat toisistaan, niin portti, joka vastaanottaa BPDU-kehymen, on vyöhykkeen reunalla. Eli portti on vyöhykkeen reunalla, jos sen segmentin designated-kytkin on eri vyöhykkeellä tai jos vastaanotettu kehys on jokin vanhemman tyylinen STP-kehys.

## 5 HP BladeSystem

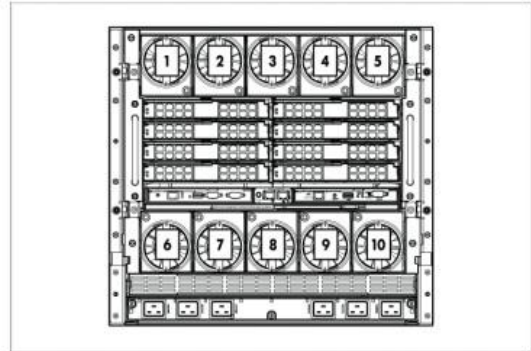
### 5.1 HP BladeSystem c-sarja

HP BladeSystem mahdollistaa palvelinteknologian tehokkaan käyttöönoton, hyvä resurssien jakamisen ja hallinnan. HP BladeSystem c-sarja on tuonut uusia ominaisuuksia, joita ei aikaisemmin ole korttipalvelimissa ollut. Korttipalvelimissa ja kehikoissa niiden ominaisuudet on yhdistetty luovasti. HP BladeSystem c-sarjassa on automatisoituja ratkaisuja, joiden avulla järjestelmänvalvojat voivat hallita c-sarjan tuotteita vaivattomasti. C-sarjan kehikkoa voi käyttää 1-16 korttipalvelimella tai tallennusjärjestelmäkortilla. Kehikko mukautuu automaattisesti kyseisten korttien mukaan.

Half-height device bay numbering



Fan bay numbering



Kuvio 5. Puolikorkeiden laitteiden Blade-palvelinpaikat (vas.) ja tuuletinpaikat (oik.). Tuuletinpaikkojen välissä moduulipaikat. [12.]

Täyteen asennettu BladeSystem c-sarjan kehikko vie ainoastaan noin 60 prosenttia siitä tilasta, minkä veisi vastaava määrä yhden yksikön palvelimia. HP BladeSystem c-sarjan kehikoissa on parannettu jäähdytysominaisuuksia. Virrankulutuksessa on selvää säästöä, ja entistä kehittyneemmät hallintatyökalut säästävät aikaa ja kokonaiskustannuksia. Kehikossa säästetään fyysisen kaapeloinnin määrässä jopa 94 prosenttia verrattuna vastaavaan määrään yhden yksikön palvelimia. Blade-järjestelmäratkaisut on helppompi ja nopeampi ottaa käyttöön, kun aikaa säästetään suunnittelussa ja toteutuksessa edellä mainittujen asioiden osalta.

Kehikossa on toteutettu virtualisointia, ja kehikon elementit voidaan koota yhteen, jolloin niitä voi käyttää yhdessä virtuaaliresursseina. Nämä resurssit näkyvät muulle konealille yhtenä näkymänä. HP Onboard Administrator on hallintaliittymä, jonka avulla saa tiedot koko BladeSystem-ympäristöstä ja hallinta tehostuu. HP Virtual Connect -teknologian avulla voidaan yksinkertaistaa liitäntöjä lähi- ja tallennusalueverkkoihin. BladeSystem-kehikon kaikki komponentit on kahdennettu vikasietoisuuden lisäämiseksi. [11.]

Taulukko 3. HP BladeSystemin hallintatyökalut. [11.]

Työkalu	Kuvaus
Onboard Administrator	Portaali kokonaisvaltaiseen c-Class hallintaan
Insight Display	Konfigurointi- ja hallintänäyttö
Rapid Deployment Pack	Palvelimien asennus ja hallintatyökalu
iLO 2	Etähallintatyökalu
Systems Insight Manager	Hallinta- ja valvontatyökalu
Performance Management Pack	Selvittää palvelimen pullonkaulat
Vulnerability and Patch Management Pack	Tietoturva-aukkojen etsintä ja paikkaus työkalu

#### HP BladeSystem c7000 Enclosure

Työssä käytetty HP BladeSystem c7000 Enclosure on Blade-kehikko, joka tarjoaa virtaa, jäähdytystä ja I/O–infrastruktuurin, jolla pystytään tukemaan palvelimia ja ylläpitämään niitä tulevina vuosina. Kehikon etupuolella on 16 paikkaa puolikorkeille Blade-palvelimille tai kahdeksan paikkaa täyskorkeille Blade-palvelimille. Jos haluaa käyttää kehikkoa puolikorkeille Blade-palvelimille, täytyy kehikkoon laittaa välilevyjä, jotta voi hyödyntää kaikkia paikkoja. Kehikon etupuolen alaosassa on kuusi paikkaa virtalähteille. Kehikon takapuolella on 10 paikkaa tuulettimille. Blade-kehikon takapuolelta löytyy myös kahdeksan paikkaa verkkomoduuleille ja kaksi paikkaa OA-moduuleille. Kehikko on 10U (unit) korkea.

Uusi HP Single Phase AC Intelligent Power Module, HP Intelligent PDU ja HP Platinum virtalähteet mahdollistavat Intelligent Power Discovery -nimisen ohjelman, joka automaattisesti kartoittaa palvelimet niiden virtalähteisiinsä. HP:n teknologiat toimivat automaattisesti HP BladeSystem c7000 -kehikossa. [12.]



Kuvio 6. Työssä käytetty Blade-kehikko edestäpäin kuvattuna.

Kuviossa 6 on kuvattu Blade-kehikko edestäpäin katsottuna. Blade-kehikkoon on asennettu 10 Blade-palvelinta kiinni ja loppuille paikoille on laitettu tyhjät peitelevyt. Kuvan alaosassa näkyy HP Insight Display -näyttö, jossa on Health Summary -näkyvä.

Kuviossa 7 puolestaan Blade-kehikko on kuvattu takaapäin katsottuna. Ylhäällä näkyy viisi tuuletinta. Niiden alapuolella on kaksi ethernet-moduulia, joiden alla on kaksi kuumomoduaalia. Alaosassa on vielä viisi tuuletinta ja niiden yläpuolella on OA1- ja OA2 -hallintamoduulit.



Kuvio 7. Työssä käytetty Blade-kehikko takaapäin kuvattuna.

## 5.2 HP Onboard Administrator

HP Onboard Administrator on c-sarjan aivot HP BladeSystem c7000 -kehikolle. Kehikon HP Insight Displayn kanssa Onboard Administrator on suunniteltu HP BladeSystem c-sarjan paikalliseen hallintaan ja etähallintaan. Onboard Administratorista käytetään lyhennettä OA. Blade-kehikkoa voi hallita Onboard Administratorin kautta selaimen avulla. Onboard Administratorin avulla pystyy muuttamaan Blade-kehikon asetuksia, kuten Blade-kehikon nimeä, laitetelineen nimeä, Blade-palvelinten iLO-osoitteita, ethernet- ja FC-moduulien iLO-osoitteita. Blade-palvelimia pystyy käynnistämään ja sammuttamaan etänä Onboard Administratorin kautta. Onboard Administratoriin avulla ja Web Administrator -ikkunaan kirjautumalla pystyy mm. vaihtamaan Blade-palvelimen nimeä ja päivittämään firmwaren eli laiteohjelmiston etänä.



HP BladeSystem Onboard Administrator - Mozilla Firefox

HP BladeSystem Onboard Administrator

10.95.241.101 https://10.95.241.101

User: admin Home | Sign Out

### Device Bay Summary

Device List

Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
1	OK	Off	Off	10.95.241.1	home1	Disconnected
2	OK	Off	Off	10.95.241.2	ILOCZJ804015A	Disconnected
3	OK	Off	Off	10.95.241.3	ILOCZJ804017H	Disconnected
4	OK	Off	Off	10.95.241.4	ILOCZJ74504JH	Disconnected
5	OK	Off	Off	10.95.241.5	ILOCZJ74504J1	Disconnected
6	OK	Off	Off	10.95.241.6	ILOCZJ74501WH	Disconnected
7	OK	Off	Off	10.95.241.7	ILOCZJ804015S	Disconnected
8	OK	Off	Off	10.95.241.8	ILOCZJ74504JL	Disconnected

Refresh

Front View

Rear View

Systems and Devices

Rack Overview

Rack Firmware

Primary: bulelab-c1

- Enclosure Information
- Enclosure Settings
- Active Onboard Administrator
- Standby Onboard Administrator
- Device Bays
  - 1. Server-1
  - 2. Server-2
  - 3. Server-3
  - 4. Server-4
  - 5. Server-5
  - 6. Server-6
  - 7. Server-7
  - 8. Server-8
- Interconnect Bays
- Power and Thermal
- Users/Authentication
- Insight Display
- Virtual Connect Manager ...

Kuvio 8. HP Onboard Administrator -hallintaikkunan näkymä.

HP Onboard Administrator -hallintaikkunan vasemmassa laidassa on listattu mm. kehikon asetukset, OA-moduulit, laitepaikat ja moduulipaikat. Näiden alta löytyy tarkempaa tietoa kyseisistä asioista. Kuvion 8 oikeassa reunassa näkyy kehikon nykyinen tilanne. Siitä näkee mitkä palvelinpaikat, moduulipaikat, tuuletinpaikat ja virtalähdepaikat ovat käytössä.

Blade-kehikoiden mukana tulee yleensä OA-moduulit ja laiteohjelmistot. Ne tarjoavat yhdessä Blade-kehikolle helpon ja nopean konfiguroinnin, turvallisen pääsyn HP BladeSystem -infrastruktuuriin, automatisoidut virta- ja jäähdytysratkaisut Blade-kehikolle ja tietoa Blade-kehikon lämpötilasta. Blade-järjestelmä tukee hot swap -tekniikkaa ja Onboard Administrator havaitsee komponenttien lisäykset ja poistot Blade-kehikossa heti muutoksen jälkeen.

HP BladeSystem c7000 -kehikossa on kaksi paikkaa OA-moduuleille. Ne toimivat yleensä siten, että toinen moduuleista on aktiivisena ja toinen on standby-tilassa. Näin OA-moduulit tarjoavat lisää vikasietoisuutta Blade-kehikkoon. Standby-tilassa oleva moduuli on pois käytöstä niin kauan, kunnes aktiivisena oleva OA-moduuli lopettaa toimintansa. Tällöin standby-tilassa oleva OA-moduuli siirtyy aktiiviseen tilaan, jolloin Blade-kehikon toiminta voi jatkua normaalina. [13.]

### 5.3 HP Integrated Lights Out

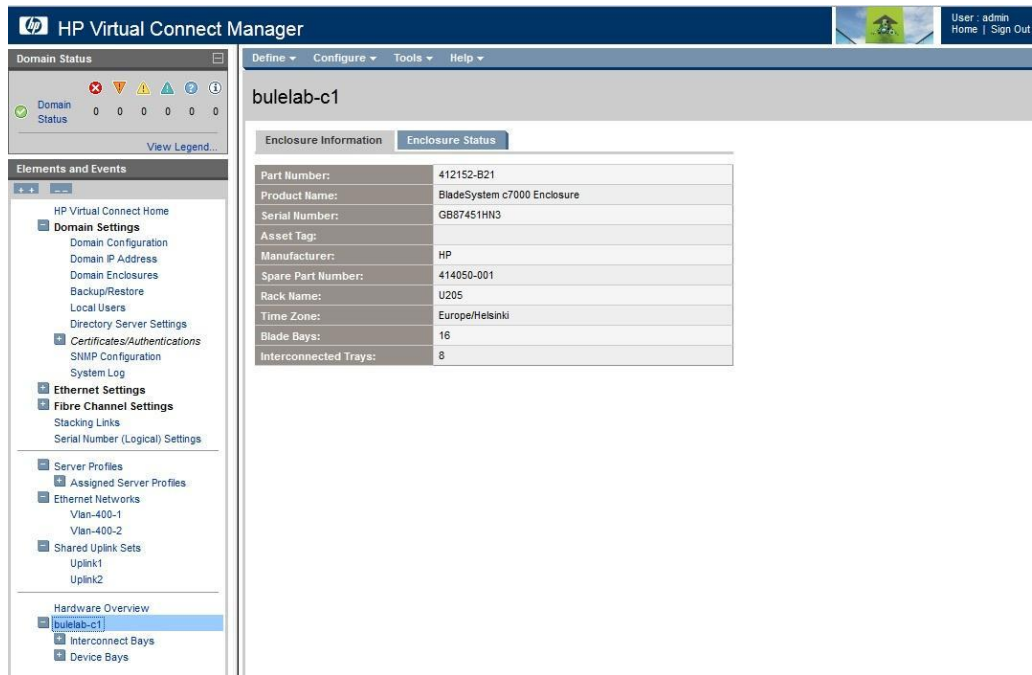
HP Integrated Lights Out eli iLO on palvelimella oleva komponentti, joka mahdollistaa palvelimen etähallinnan, vaikka palvelin ei olisikaan toiminnassa. iLO:lla on oma verkkoyhteysensä, jonka kautta voidaan nähdä integrated management logs. iLO:n avulla voidaan nähdä, mitä palvelimen näytöllä on ja käyttää sitä samalla tavalla kuin terminaalipalveluja ja uudelleen käynnistää palvelin.

iLO:lla on oma IP-osoite. Se ei siis ole sama kuin palvelimen IP-osoite. iLO:a käytetään selaimella syöttämällä IP-osoite tai DNS-nimi selaimen osoitekenttään. iLO vaatii kirjautumisen turvallisuussyistä ja kirjautumisessa pitää syöttää käyttäjänimi ja salasana.

Kun selaimella on otettu iLO:n kautta yhteys ja kirjaututtu sisään, näkyy neljä välilehteä, joista kaikki kontrolloivat palvelimen eri osia. Palvelimia pystyy hallitsemaan iLO:n kautta aivan samalla tavalla kuin paikallisesti pystyisi.

### 5.4 HP Virtual Connect

HP Virtual Connect -teknologialla pystytään erottamaan korttipalvelimet, lähiverkko ja tallennusverkko erilleen toisistaan. HP Virtual Connect pystyy virtualisoimaan seuraavat palvelimen ominaisuuksia, kuten palvelimen nimi, Fibre Channel-kortin WWN-osoitteet, verkkokortin MAC-osoitteet, verkkomääritykset, boot-From-SAN-määritykset ja FC-kortin Bios-asetukset. Virtual Connectista käytetään lyhennettä VC.



Enclosure Information	
Part Number:	412152-B21
Product Name:	BladeSystem c7000 Enclosure
Serial Number:	GB87451HN3
Asset Tag:	
Manufacturer:	HP
Spare Part Number:	414050-001
Rack Name:	U205
Time Zone:	Europe/Helsinki
Blade Bays:	16
Interconnected Trays:	8

Kuvio 9. HP Virtual Connect Manager -hallintaikkuna.

HP Virtual Connect Manager on selaimen avulla käytettävä hallintaohjelma. Sen avulla voidaan hallita Blade-kehikon verkkoyhteyksiä. HP Virtual Connect Managerissa voi määrittellä palvelinprofiilit, ethernet- ja kuituverkkoasetukset ja jaetut uplinkit. Alkuasetusten jälkeen Virtual Connet Managerissa ei tarvitse muuttaa oikeastaan kuin palvelinprofiileja.

## 5.5 HP Intelligent Power Discovery

HP Intelligent Power Discovery (IPD) on ensimmäinen teknologia, joka luo automaattisen, energiatietoisien tietoverkon tietotekniikan systemien ja laitteistojen välille. Tämän avulla yritykset voivat säästää huomattavasti virrankulutuksessa ja seisontakustannuksissa. Intelligent Power Discovery maksimoi datakeskuksen tehokkuuden. Intelligent Power Discovery avulla saadaan tarkkaa tietoa palvelintelineiden virrankulutuksesta, jotta pystytään tunnistamaan ja eliminoimaan alueet, joilla virtaa on mennyt hukkaan. Täten energiaa säästämällä voi pidentää datakeskuksen käyttöikää.

Kun HP ProLiant -palvelin otetaan käyttöön, Intelligent Power Discovery havaitsee palvelimet automaattisesti ja kartoittaa ne oikeaan virtalähteeseen. IPD varmistaa virran vikasietoisuuden tekemällä vikasietoiset liitännät myös toiseen PDU:hun ja huolehtii,

että kaikki on kytketty oikein säästään aikaa ja eliminoiden kaikki ihmisille mahdolliset virheet. Ihmisten virheet häviävät täten kokonaan ja yritys tietää, paljonko mikäkin palvelinteline kuluttaa virtaa. Näin ollen voidaan lisätä palvelimia, eikä tarvitse huolehtia sähkökatkoksista.

Intelligent Power Discovery:ssa yhdistyvät HP Intelligent Power Distribution Unit (iPDU), HP Platinum power supplies ja HP Insight Control -ohjelmisto. Intelligent Power Discoveryn avulla pystytään tarjoamaan uuden palvelimen sähköjakeluun täsmällistä hallintaa ja automatisointia. HP Intelligent Power Discovery käyttää HP Common Slot Platinum -virtalähdettä, joka on yksi maailman tehokkaimmista virtalähteistä. Sen avulla on mahdollista säästää sähkökustannuksissa.

PLC-teknologiaa käyttävissä HP ProLiant G6- ja G7-palvelimissa on tunnistuspalvelu, joka määrittää palvelimen nimen, UUID-numeron ja IP-osoitteen Intelligent PDU:hun ja HP Insight Control -virranhallintaohjelmistoon. Virranjakeluohjelmiston ja -laitteiston konfigurointi ei vie täten niin paljoa aikaa. IPD havaitsee itsekseen vikasietoiset virtalähteet ja varmistaa, että ne ovat toisessa PDU:ssa. Näin ollen datakeskuksen suurimmat ongelmat eli ihmisten virheet ja suunnittelemattomat katkokset vähenevät. [14.]

## 5.6 HP Intelligent Power Distribution Unit

HP Intelligent Power Distribution Unit:n (iPDU) avulla on mahdollista hallita laitetelineeseen asennettuja sähköjakeluyksiköitä, jolla voidaan vähentää datakeskuksen kasvun aiheuttamaa virran kuormitusta.

HP Modular PDU line käyttää core and stick -arkkitehtuuria. HP Intelligent PDU:n avulla voi tarkkailla virran kulutusta ytimessä, lohossa, tikussa ja ulostulossa täsmällisesti. Siinä on sisäänrakennettu etähallintamahdollisuus ja laitetelineen jokaisen komponentin virrankulutus tiedetään tarkalleen. [15.]

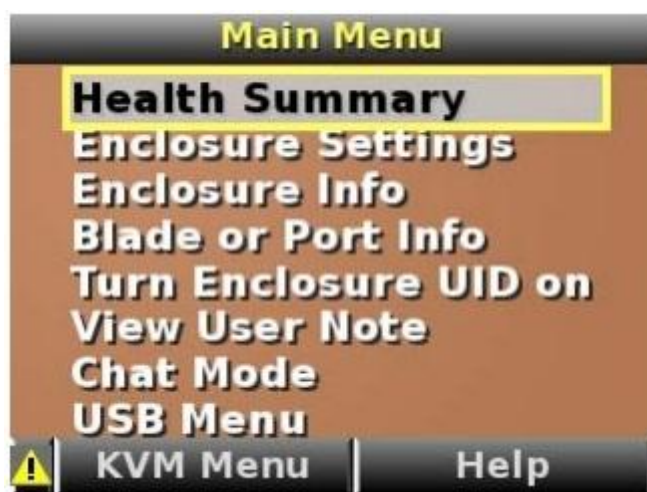
## 5.7 HP Insight Control

HP Insight Control on oleellinen palvelimen hallintakeino, jonka avulla HP ProLiant-palvelimia pystytään hyödyntämään täysin. HP Insight Control:lla pystytään hallitse-

maan HP:n palvelimia seuraavissa ympäristöissä: Microsoft Windows, VMware ESX, Microsoft Hyper-V, Red Hat ja SUSE Linux.

## 5.8 HP BladeSystem Insight Display

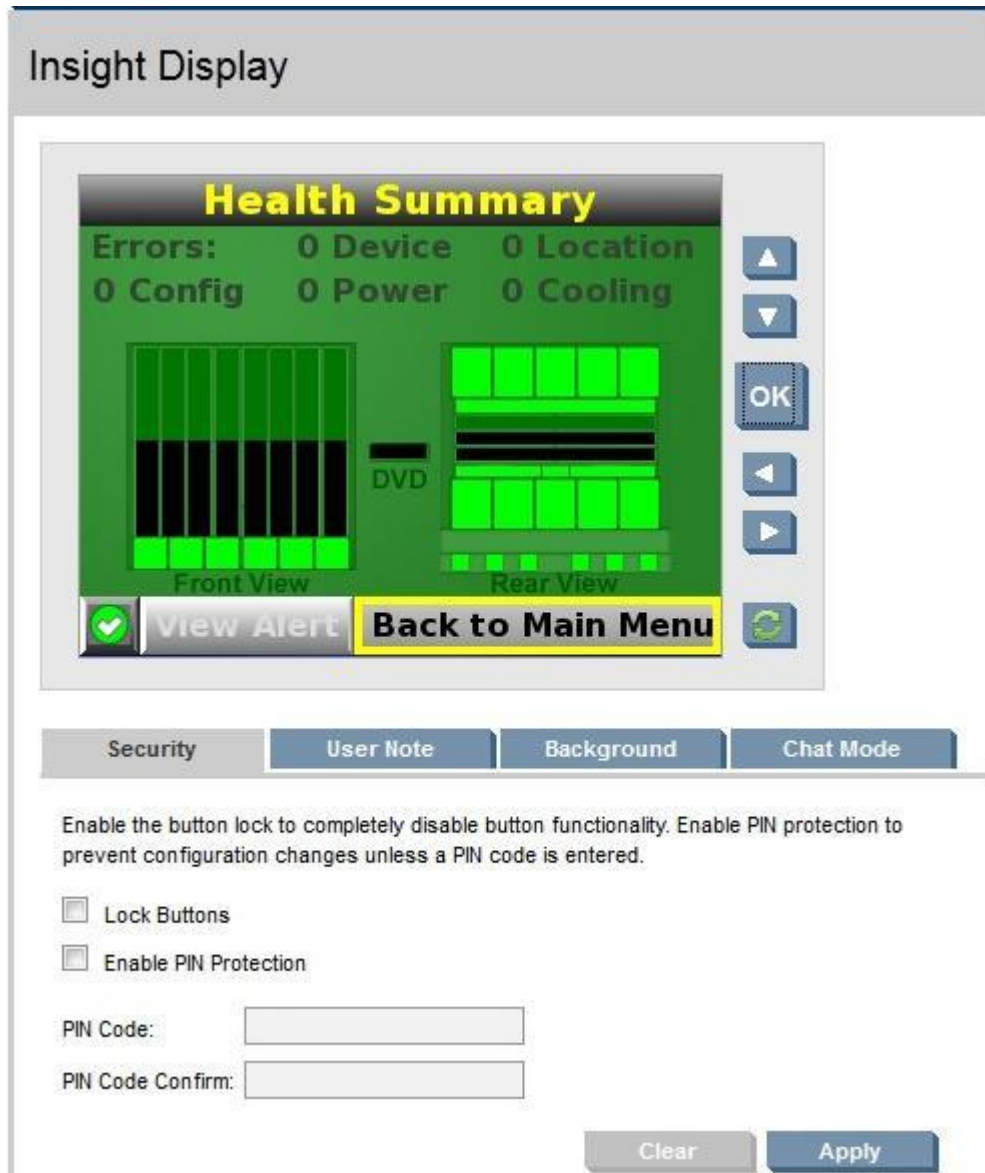
HP BladeSystem Insight Display on eräs HP BladeSystemin hallintatyökaluista. Insight Display on Blade-kehikon etuosassa oleva hallinta- ja konfigurointinäyttö. Näyttö tarjoaa tietoa Blade-kehikon tilasta ja sen toiminnasta. Näytön taustaväri kertoo, missä tilassa Blade-kehikko on, ja taustaväri vaihtelee kehikon kunnon mukaan. Insight Displayn taustaväri on sininen UID-valon ollessa päällä. UID-valo (Unit Identification) on LED-valo, jonka avulla palvelinhuoneessa voi havaita tietyt palvelimen tai laitteiston. Tausta on väriltään vihreä, kun Blade-kehikossa ei ole virheitä ja se toimii normaalisti. Näyttö on ruskean värinen, kun OA havaitsee virheitä tai hälytyksiä Blade-kehikossa. Väri on tumma, kun näyttö ei ole aktiivinen eli se on sammutettu tai ollut vähintään kaksi minuuttia käyttämättömänä.



Kuvio 10. HP BladeSystem Insight Displayn päävalikko. [16.]

Näytön vasemmassa alareunassa oleva ikoni (enclosure health) näkyy jokaisella eri ruudulla ja kertoo kehikon kunnon. Kyseistä ikonia painamalla pääsee Health Summary -näytölle. Kehikon toiminnasta vastaava henkilö voi konfiguroida Blade-kehikon toimintaa näytön avulla.

Myös Onboard Administratorin kautta voi hallita Insight Displayta. Selaimessa näkyy samanlainen näyttö, joka toimii samalla tavalla kuin kehikon alareunassakin oleva fyysinen näyttö. Kun Insight Displayta käytetään selaimen avulla, siinä on pieni viive. Mikäli Blade-kehikossa olisi virheitä, ne näkyisivät kuviossa 11. Näkymästä ilmeni minkälainen virhe on kyseessä ja millä paikalla virhe esiintyy.



Kuvio 11. HP Onboard Administrator -hallintaikkunan kautta käytettävän HP Insight Displayn Health Summary -näkyvä.

## 6 Virtualisointi

### 6.1 Yleistä

Virtualisointi tarkoittaa tietotekniikassa fyysisten resurssien piilottamista sovelluksilta ja loppukäyttäjältä. Virtuaalikoneiden ollessa käytössä voidaan laitteistoresursseja jakaa usealle loppukäyttäjälle toisin kuin ilman virtuaalikoneita, jolloin yhdellä käyttöjärjestelmällä on käytössä kaikki laitteistoresurssit.

Virtualisoinnissa voidaan luoda virtuaalikoneita käyttöjärjestelmän päällä toimiviksi. Virtuaalikone on virtualisoitu ympäristö, jossa voidaan suorittaa ohjelmia tietokoneen tapaan. Yhden paikallisen tietokoneen päällä voidaan ajaa useita virtuaalikoneita. Täten yksi henkilö voi käyttää samalta tietokoneelta useaa eri tietokonetta samaan aikaan. Tätä hyödynnetään esimerkiksi tietyissä työtehtävissä. Virtuaalikoneet näyttävät tavallisilta ohjelmilta, koska ne avautuvat omissa pikakuvakkeissaan.

### 6.2 VMware

#### 6.2.1 Yleistä

VMware tarjoaa virtualisointiohjelmistoja. VMwaren tärkeimmät tuotteet ovat VMware Server, VMware ESX Server, VMware Workstation ja VMware Player. VMwaren työpöytäohjelmistoa voi käyttää Microsoft Windowsilla, Linuxilla ja Mac OS X:lla. VMware ESX Server ja VMware ESXi Server eivät tarvitse erillistä käyttöjärjestelmää toimiakseen, vaan ne voi ajaa laitteiston päällä itsenäisenä käyttöjärjestelmänä.

VMware vSphere Client on ohjelma, jonka voi asentaa VMware ESXi Serverin päälle. Sen avulla voi hallita ja käyttää virtuaalikoneita. VMware vSphere Client toimii siten, että kyseinen sovellus käynnistetään, jonka jälkeen kirjaudutaan halutulle palvelimelle. Tämän jälkeen ohjelma avautuu omassa ikkunassaan ja virtualisointia voidaan toteuttaa halutulla tavalla.

### 6.2.2 VMwaren toiminta

Isännät eli hostit ovat tietokoneita, jotka käyttävät VMware-ohjelmistoja ja käyttöjärjestelmiä. Ohjelmien sisällä toimii virtuaalikoneita, joita kutsutaan vieraksi eli guesteiksi. Vieraita voi siirtää isäntien välillä riskittä. Virtuaalikoneissa on simuloidut laitteet, jotka VMware on sille virtualisoinut.

Fyysisellä tietokoneella voidaan käyttää yhtä tai useampaa virtuaalista tietokonetta samanaikaisesti. Eli isäntäkoneen käyttöjärjestelmän päällä voidaan ajaa useampaa virtuaalikonetta omilla käyttöjärjestelmillään. Virtuaalikoneiden avulla on mahdollista käyttää useaa konetta samanaikaisesti yhdeltä fyysiseltä tietokoneelta. Virtuaalikoneita voi käyttää VMwaren kautta tai ottamalla verkkoyhteyden virtuaalikoneeseen. [17.]

### 6.2.3 VMware ESX Server

VMware ESX on yrityskäyttöön tarkoitettu tietokoneiden virtualisointiohjelma. VMware ESX toimii omana käyttöjärjestelmänä, eikä sitä tarvitse suorittaa toisen käyttöjärjestelmän päällä toisin kuin monia muita VMwaren virtualisointituotteita. VMware ESX toimii VMkernelillä, joka on VMwaren omaa tuotantoa. VMware ESX:n ollessa itsenäinen käyttöjärjestelmä, se on myös turvallisempi ja sen resurssien jakoa voi kontrolloida helpommin. VMware käyttää toiminnassaan hyväksi VMotionia, VirtualCenteriä ja Linuxin Service Consolea. VMwaren ESX Server käyttää Linux-pohjaista virtuaalikonetta (Service Console) tuottaakseen käyttöliittymäpalveluita. VMotion-työkalu sallii virtuaalikoneiden siirtämisen isäntäpalvelinten välillä niiden toiminnan jatkuessa koko siirron ajan. VirtualCenterin avulla voidaan puolestaan tarkkailla VMware ja ESX Serveriä samaan aikaan.

Kernel, joka on VMware ESX -palvelimen ydin, hoitaa ainoastaan virtuaalikoneiden toiminnallisuuden ja resurssien hallinnan. Kernelin yhteydessä toimii Console Operating System, joka mahdollistaa ESX-palvelimen hallinnan ja käyttöjärjestelmien palvelut. ESX nimi juontaa juurensa sanoista Elastic Sky X. [17.]



#### 6.2.4 VMware ESXi Server

VMware ESXi poikkeaa VMware ESX -käyttöjärjestelmästä siten, että Console Operating Systemin tarjoamat palvelut on tuotu kerneliin. ESXi:ssa on tarkkaan vianselvitykseen oma komentorivinsä, joka on nimeltään ESXi Shell. ESXi Shell sisältää ESXCLI-komentoja mm. vian etsintään ja korjaukseen. ESXi Shelliin pääsy täytyy ottaa käyttöön joka järjestelmällä erikseen.

VMware ESXi voidaan integroida Active Directoryyn, jossa sille määritellään käyttöoikeudet. VMware vSphere Clientin hallinnassa voi määrittää oikeuksia tarkemmin. Uusimmassa ESXi-versiossa (5.0) virtuaalikoneiden laitteistotasot voi päivittää versioon 8. Tässä versiossa on mahdollista tuoda enemmän tehoa virtuaalikoneelle ja siitä löytyy myös USB 3.0 -tuki.

Käyttöjärjestelmien asennuksen voi suorittaa skriptien avulla, jolloin asennus helpottuu, kun itse ei tarvitse tehdä jokaista asennuksen vaihetta jokaisen palvelimen kohdalla erikseen.

VMware ESXi vaatii toimiakseen melko suorituskykyisen tietokoneen tai palvelimen. Yksiytiminen prosessori riittää, mutta olisi hyvä olla vähintään kaksiytiminen prosessori. Neliytimisen prosessoria suositellaan. Mitä enemmän ytimiä prosessorissa, sitä enemmän virtuaalikoneita on mahdollista pyörittää kyseisen prosessorin kanssa. Keskusmuistin minimivaatimus on 1 GB, mutta suositeltavaa on olla enemmän, esimerkiksi 8 GB, jotta useita virtuaalikoneita voidaan suorittaa samaan aikaan. Minimivaatimus VMware ESXi:lle on yksi verkkokortti ja 80 GB kiintolevytilaa. Ideaalitalanne on jos olisi peilattuja kiintolevyjä, esimerkiksi RAID5-konfiguraatiolla olevia kiintolevyjä. [18.]

#### 6.3 Hyper-V

Hyper-V on Microsoftin kehittämä palvelinvirtualisointiratkaisu. Windows Server 2008 -käyttöjärjestelmässä voidaan ottaa Hyper-V käyttöön suoraan rooleista, jossa ensin asennetaan Hyper-V-rooli ja sitten määritellään sen yleisasetukset.

Hyper-V on tarkoitettu etenkin palvelinten virtualisointiin. Hyper-V poikkeaa toisesta työssä käytetystä virtualisointiratkaisusta, VMware ESXi Serveristä. VMware ESXi:n pys-

tyi asentamaan suoraan palvelimen raudan päälle, jolloin se toimi omana käyttöjärjestelmänään. Hyper-V puolestaan asennetaan käyttöjärjestelmän päälle. Ensin palvelimeen asennetaan jokin käyttöjärjestelmä, jonka jälkeen asennetaan Microsoft Hyper-V, joka toimii virtualisointialustana. Tämän jälkeen virtualisointialustan päälle voidaan luoda virtuaalikoneita.

Hyper-V:ssä luodaan virtuaalikoneita ja niihin määritellään halutut asetukset, jonka jälkeen virtuaalikoneet saa käyntiin. Virtuaalikoneisiin täytyy asentaa vielä käyttöjärjestelmät, jonka jälkeen niitä voi alkaa käyttämään.

## 7 Työn vaiheet

### 7.1 Blade-järjestelmän asennus

#### 7.1.1 Blade-kehikon fyysinen asennus

Koululle tuotiin HP BladeSystem c7000 Enclosure Blade-kehikko Espoon Leppävaarasta. Blade-kehikon fyysinen asennus suoritettiin yhdessä koulun laboratorioassistentin kanssa, koska kehikko oli painava ja olisi ollut todella vaikeaa suorittaa kehikon fyysinen asennus yksin. Metropolia Ammattikorkeakoulun Bulevardin toimipisteen luokassa U205 on palvelinkoppi, jonka yhteen laitetelineeseen Blade-kehikko asennettiin.

Vanha Blade-kehikko otettiin pois laitetelineestä, jotta työssä käytetty Blade-kehikko saatiin mahtumaan laitetelineeseen. Vanhasta kehikosta oli jo irrotettu virtakaapelit ja verkkokaapelit, joten täytyi ainoastaan ottaa Blade-kehikko ja siinä olevat Blade-palvelimet pois laitetelineestä. Ensin otettiin Blade-palvelimet irti Blade-kehikosta, jotta kehikko olisi kevyempi nostaa laitetelineestä pois. Blade-palvelimet irrotettiin Blade-kehikosta painamalla Blade-palvelimen etuosassa olevaa salpaa, jolloin salpa vapautui ja Blade-palvelin vedettiin kehikosta ulos. Blade-kehikosta oli aikaisemmin irrotettu virtalähteet, joten kehikko oli tyhjä palvelimien poiston jälkeen. Seuraavaksi ruuvattiin irti ruuvit, jotka pitivät kehikon laitetelineessä paikallaan. Sitten tyhjän kehikon pystyi irrottamaan laitetelineestä.

Seuraavaksi asennettiin työssä käytettävä Blade-kehikko fyysisesti paikoilleen. Tämä sujui samaan tyyliin kuin vanhan Blade-kehikon poisto. Ainoastaan järjestys tässä oli päinvastainen. Blade-kehikko saatiin paikallaan nostamalla se oikealle korkeudelle ja työntämällä se laitetelineeseen, jonka jälkeen se ruuvattiin paikoilleen.

#### 7.1.2 Blade-palvelimien fyysinen asennus

Blade-palvelimet asennettiin Blade-kehikon etupuolelle, niille varatuille paikoille. Blade-palvelimien fyysinen asennus Blade-kehikkoon oli helppoa, sillä palvelimet täytyi ainoastaan työntää paikoilleen ja varmistaa, että palvelimet menivät perille asti, jolloin ne lukittuivat kiinni kehiikkoon. Blade-kehikossa oli 16 paikkaa Blade-palvelimille ja käytössä oli kymmenen Blade-palvelinta. Käytetyt Blade-palvelimet olivat HP ProLiant BL460c G1 -merkkisiä. Kymmenen Blade-palvelinta asennettiin paikoilleen ja kuusi paikkaa jäi tyhjäksi ja niille paikoille laitettiin peitelevyt, jotka ovat Blade-kehikon etuosaa peittäviä muovilevyjä, jotka suojaavat kehiikon sisätiloja pölyyntymiseltä.

#### 7.1.3 Virtalähteiden asennus

Blade-kehikon etupuolen alareunassa oli kuusi paikkaa virtalähteille. Virtalähteiden asennus oli käytännössä samanlaista kuin Blade-palvelimien asennus. Virtalähteet työnnettiin Blade-kehikon etupuolen alareunaan niille varatuille paikoille ja lukittiin kiinni kehiikkoon. Työssä käytettiin kuutta virtalähdettä, jotta Blade-järjestelmä saa varmasti tarpeeksi virtaa.

#### 7.1.4 Tuulettimien asennus

Blade-kehikon takapuolella oli kymmenen paikkaa tuulettimille. Viisi tuuletinpaikkaa oli kehiikon yläosassa ja viisi kehiikon alaosassa. Yläosaan asennettavat tuulettimet piti asentaa siten, että tuulettimen LED-valo oli tuuletinpaikan oikeassa alakulmassa. Alaosaan asennettavat tuulettimet puolestaan täytyi asentaa siten, että LED-valo osoitti vasemmalle ylös. Käytössä oli kymmenen tuuletinta, jotka asennettiin paikoilleen työntämällä. Tuulettimet lukittiin paikoilleen kääntämällä tuulettimessa olevasta kahvasta.

### 7.1.5 Virtual Connect -moduulien asennus

Moduuleille oli kehikossa yhteensä kahdeksan paikkaa kehikon takapuolella. Blade-kehikkoon asennettiin neljä Virtual Connect -moduulia, joista kaksi oli ethernet-moduuleja ja kaksi FC-moduuleja eli kuitumoduuleja. Ethernet-moduulit olivat mallia HP 1/10Gb VC-Enet Module ja kuitumoduulit olivat mallia HP 4 Gb VC-FC Module. Ethernet-moduulit laitettiin paikoille 1 ja 2 ja kuitumoduulit paikoille 3 ja 4. Moduulit työnnettiin paikoilleen, jolloin ne lukittuivat kiinni kehikkoon.

Neljä moduulipaikkaa jäi tyhjäksi ja niihin laitettiin moduulipaikkoihin sopivat peitepaikat. Kuitumoduulit eivät olleet käytössä, joten ne sammutettiin myöhemmin OA:n kautta. Kytkimen trunk-porteista kytkettiin verkkokaapelit ethernet-moduulien ensimmäisiin portteihin.

Interconnect Bay Summary							
Interconnect List							
Virtual Power		UID State					
Bay	Status	UID	Power State	Module Type	Management URL *	Product Name	
1	OK	Off	On	Ethernet	<a href="http://10.95.241.21/">http://10.95.241.21/</a>	HP 1/10Gb VC-Enet Module	
2	OK	Off	On	Ethernet	<a href="http://10.95.241.22/">http://10.95.241.22/</a>	HP 1/10Gb VC-Enet Module	
3	OK	Off	On	Fibre Channel		HP 4Gb VC-FC Module	
4	OK	Off	On	Fibre Channel		HP 4Gb VC-FC Module	

\* The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.

Kuvio 12. Interconnect Bay Summary eli ethernet- ja kuitumoduulit OA-hallintaikkunassa.

### 7.1.6 OA-moduulien asennus

Blade-kehikon takapuolella oli kaksi paikkaa OA-moduuleille. Käytössä oli kaksi OA/iLO -moduulia, jotka asennettiin niille varatuille paikoille. OA-moduulit lukittuivat kiinni Blade-kehikkoon. Vasemmanpuoleinen OA-moduuli on aktiivinen ja oikeanpuoleinen OA-moduuli on standby-tilassa. Molempiin OA-moduuleihin kytkettiin verkkokaapelit kytkimen porteista, jotka oli konfiguroitu VLAN 401:lle.

### 7.1.7 Virtakaapeleiden kytkeminen

Virtakaapeleiden kytkeminen oli seuraavaksi vuorossa. Blade-kehikossa oli kuusi virtalähdettä, joten kehikkoon piti kytkeä kuusi virtakaapelia. Virtakaapeleiden kytkeminen suoritettiin koulun hiihtolomaviikolla, koska haluttiin käyttää tiettyjä virtakaapeleita ja muutamaa virtakaapelia jouduttiin siirtämään paikasta toiseen aiheuttaen katkon siihen kytketyn laitteen käytössä.

## 7.2 Verkkoyhteydet

### 7.2.1 Verkkoyhteyksien suunnittelu

Blade-järjestelmästä piti päästä koulun verkkoon kytkimen kautta. Työhön saatiin käyttöön kytkin, joka oli HP Procurve Switch 3500yl-24G. HP Procurve Switch 3500yl-24G on kolmostason kytkin, eli se kykenee IP-reititykseen. Kytkimessä on 24 porttia. Kytkimeen tuli OSPF-konfiguraatio ja siinä käytettiin aluetta 0.0.0.0. Koulun verkkoon yhteydessä oleville porteihin piti konfiguroida VLAN 50. Työhön varattiin käyttöön VLAN:t 400-407 ja kerrottiin myös, mitä IP-osoitteita niissä voi käyttää. IP-osoitteiden piti olla sellaisia, että niitä ei ole käytössä koulun verkossa, jotta reititys toimisi täysin normaalisti.

Taulukko 4. Koulun verkosta varatut IP-osoitteet.

VLAN	IP-osoite	Maski
400	10.95.240.0	/24
401	10.95.241.0	/24
402	10.95.242.0	/24
403	10.95.243.0	/24
404	10.95.244.0	/24
405	10.95.245.0	/24

406	10.95.246.0	/24
407	10.95.247.0	/24

### 7.2.2 Kytkimen ohjelmistopäivitys

Kytkin HP Procurve 3500 piti päivittää uusimpaan ohjelmistoversioon. Tietokoneelta otettiin konsolilyhteys kytkimeen ja tarkastettiin ohjelmistoversion, joka oli K.12.57. Uusin saatavilla oleva ohjelmistoversio oli K.15.06.0008. Päivitys ei onnistunut, koska kytkimessä ollut versio oli liian vanha. Kytkin ilmoitti, että BootROM-version täytyy olla K.12.17 tai uudempi, jotta ohjelmistoversio K.15 voidaan ladata kytkimeen. Internetistä ladattiin hieman kytkimessä ollutta versiota uudempi versio, joka oli K.13.25 ja kytkin päivitettiin sillä. Nyt kytkimen ohjelmistoversio ilmoitti, että primary image on K.13.25.

Ohjelmistoa uusimpaan versioon päivittäessä huomattiin, että kytkin ilmoitti edelleen ohjelmistoversion olevan liian vanha. Tällöin huomattiin, että BootROM-versio ei ollut päivittynyt, vaan se oli edelleen sama eli K.12.12. Ohjelmistopäivitys päivitti siis vain primary imagen. Internetistä etsittiin versiota, joka päivittäisi myös BootROM-version. Sellainen löytyi HP:n sivuilta. Primary image päivitettiin versioon K.13.68, jolloin BootROM-versio päivittyi samalla.

Kun primary image päivitettiin K.13.68-versioon, niin BootROM-versio päivittyi samalla versioon K.12.17. Primary image kopioitiin secondary imageksi. Nyt kun BootROM-versio oli tarpeeksi uusi, ohjelmisto pystyttiin päivittämään suoraan uusimpaan versioon, joka oli K.15.06.0008. Kytkimeen päivittyi uusien ohjelmistoversio, ja BootROM-versio päivittyi samalla versioon K.15.19.

Kytkimen ohjelmistopäivitystiedostot ovat.swi-tiedostoja. Kytkimen ohjelmistopäivitykset hoidettiin siten, että ensin ladattiin haluttu tiedosto internetistä ja se sijoitettiin tietokoneen C-aseman juureen eli kohteeseen C:\. Sitten käynnistettiin ohjelma nimeltä TFTP Server ja ohjelman asetuksista varmistettiin, että TFTP Server on päällä. Palvelimen IP-osoitteen pystyi tarkastamaan kohdasta Server interfaces: 10.95.1.89. Ohjel-

mistoversion pystyi päivittämään komennolla: `copy tftp flash 10.95.1.89 K_15_06_0008.swi`. Primary imagen pystyi kopioimaan secondary imageksi komennolla: `ProCurve Switch 3500yl-24G# copy flash flash secondary`.

```

HP-E3500yl-24G# show version
Image stamp: /sw/code/build/btm(K_15_06)
             Oct 8 2011 17:39:18
             K.15.06.0008
             85
Boot Image:  Primary

HP-E3500yl-24G# show flash
Image      Size (bytes) Date   Version
-----
Primary Image  : 14844423 10/09/11 K.15.06.0008
Secondary Image.: 7566208 07/30/09 K.13.68
Boot ROM Version : K.15.19
Default Boot   : Primary

```

Kuvio 13. Kytkimelle ohjelmistopäivityksen jälkeen syötetyt show-komennot.

### 7.2.3 Kytkimen konfigurointi

Kun kytkimeen oli päivitetty uusi ohjelmistoversio, oli vuorossa kytkimen konfigurointi. Ensin poistettiin olemassa oleva konfiguraatio ja käynnistettiin kytkin uudestaan, jolloin päästiin konfiguroimaan oletuskonfiguraation päälle. HP:n laitteiden konfiguroinnista ei ollut juurikaan aiempaa kokemusta, joten HP Procurve -kytkimien konfigurointiin tutustuminen vei hieman aikaa.

Kytkimeen luotiin VLAN:t 50, 400, 401 ja 402. Koulun verkkoon menevät portit konfiguroin VLAN 50:lle. Kytkimeen konfiguroitiin VLAN:t 400-402, kuten alemmassa kuvassa näkyy. Tarkoitus oli jaotella eri tarpeet eri verkkoihin. VLAN 400 oli tarkoitettu Blade-palvelimien IP-osoitteille. VLAN 401 oli tarkoitettu Blade-palvelimien iLO-osoitteille, joiden avulla Blade-palvelimia voidaan hallita. VLAN 402 oli tarkoitettu Blade-palvelimiin luotujen virtuaalikoneiden IP-osoitteille. Kytkimen kaksi viimeistä porttia konfiguroitiin trunk-linkeiksi. VLAN:t 403-407 oli myös varattu työhön, mutta niitä ei tässä työssä tarvittu.

Kytkimeen konfiguroitiin spanning tree. Spanning treen tyypiksi laitettiin MST. Tarvittavat tiedot MST-konfiguraatiosta saatiin työn ohjaajalta. Reititysprotokollaksi konfiguroitiin OSPF. OSPF:ssa käytettiin aluetta 0.0.0.0. Kun OSPF oli konfiguroitu, alkoivat reiti-

tysmainostukset liikkua ja pian reititystauluun oli tullut OSPF:n kautta joukko verkkoja. Kytkimeltä pystyi pingaamaan ulospäin verkkoon, joka tarkoitti, että yhteys toimii.

VLAN:ien konfiguraatiot testattiin pingaamalla niiden osoitteita kytkimeltä. Myös yhteyttä ulospäin verkkoon testattiin laittamalla halutun VLAN:n staattinen IP-osoite yhdelle laboratorioluokan tietokoneelle ja yhdistämällä se kytkimeen, jonka kautta yhteys koulun verkkoon muodostui. Kaikki kytkimen testaukset toimivat ja konfiguraatio vaikutti hyvältä.

Taulukko 5. HP Procurve 3500 -kytkimen portit.

VLAN	Portit
50	1-4
400	11-20
401	5-10
402	-
TRUNK	23-24

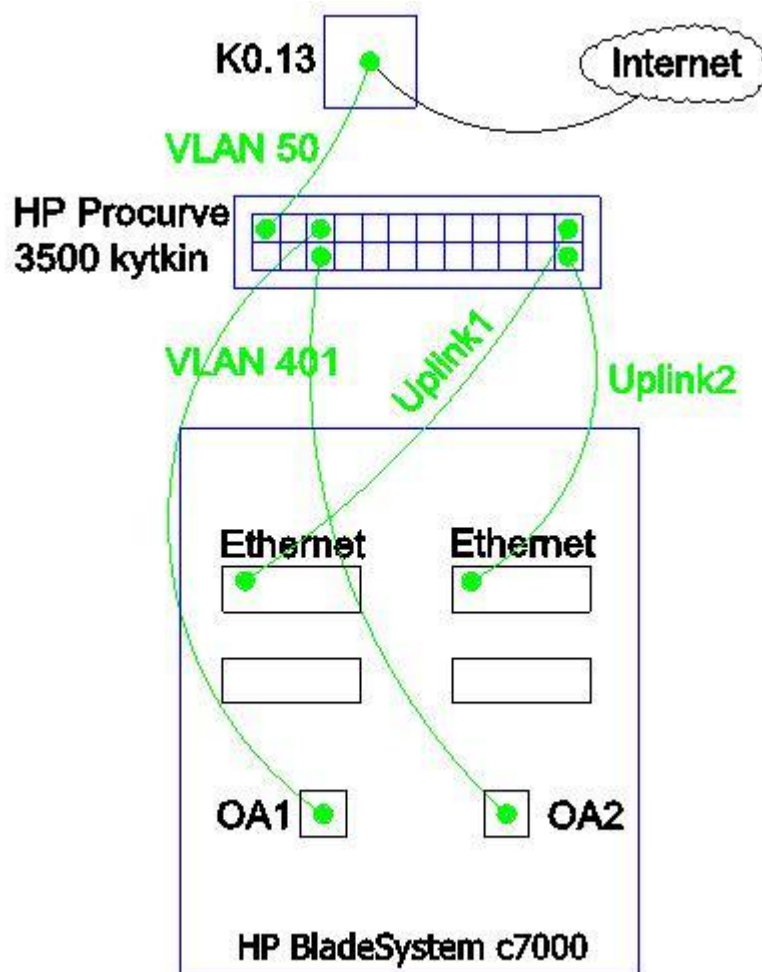
#### 7.2.4 Kytkimen asennus

HP Procurve Switch 3500yl-24G piti asentaa U205-huoneen palvelinkaapin laitetelineeseen. Kytkin ruuvattiin kiinni laitetelineen sivussa oleviin ruuvipaikkoihin, jolloin kytkin pysyi tukevasti paikoillaan. Virtakaapeli kytkettiin kiinni ja verkkokaapeli laitettiin kytkimen ensimmäiseen porttiin, joka oli konfiguroitu VLAN 50:ksi. Verkkokaapelin toinen pää kytkettiin laitetelineen takana seinässä olevaan paikkaan K0.13, joka oli kiinni koulun verkossa. Kytkimen toimivuutta testattiin eräältä U205-luokan tietokoneelta Tera Term -ohjelmaa käyttäen. Kytkimeen pääsi käsiksi ottamalla telnet-yhteyden kytkimen VLAN 50:n IP-osoitteeseen. Yhteys toimi, ja kytkin toimi halutulla tavalla koulun verkossa.

Kuviossa 14 näkyy Blade-järjestelmän ympärillä olevan verkon rakenne. OA1- ja OA2-paikat ovat HP Onboard Administrator -hallintaan tarkoitettuja paikkoja. OA1 on aktiivinen ja OA2 on standby-tilassa. OA1- ja OA2-paikat yhdistettiin verkkokaapelin avulla HP Procurve 3500 -kytkimen portteihin 5 ja 6 eli VLAN 401:n portteihin. Uplink1:n ja Uplink2:n verkkokaapelit kytkettiin kytkimen portteihin 23 ja 24, jotka olivat trunk-



portteja. Uplinkkien toiset päät kytkettiin Blade-kehikon ethernet-moduulien ensimmäisiin portteihin.

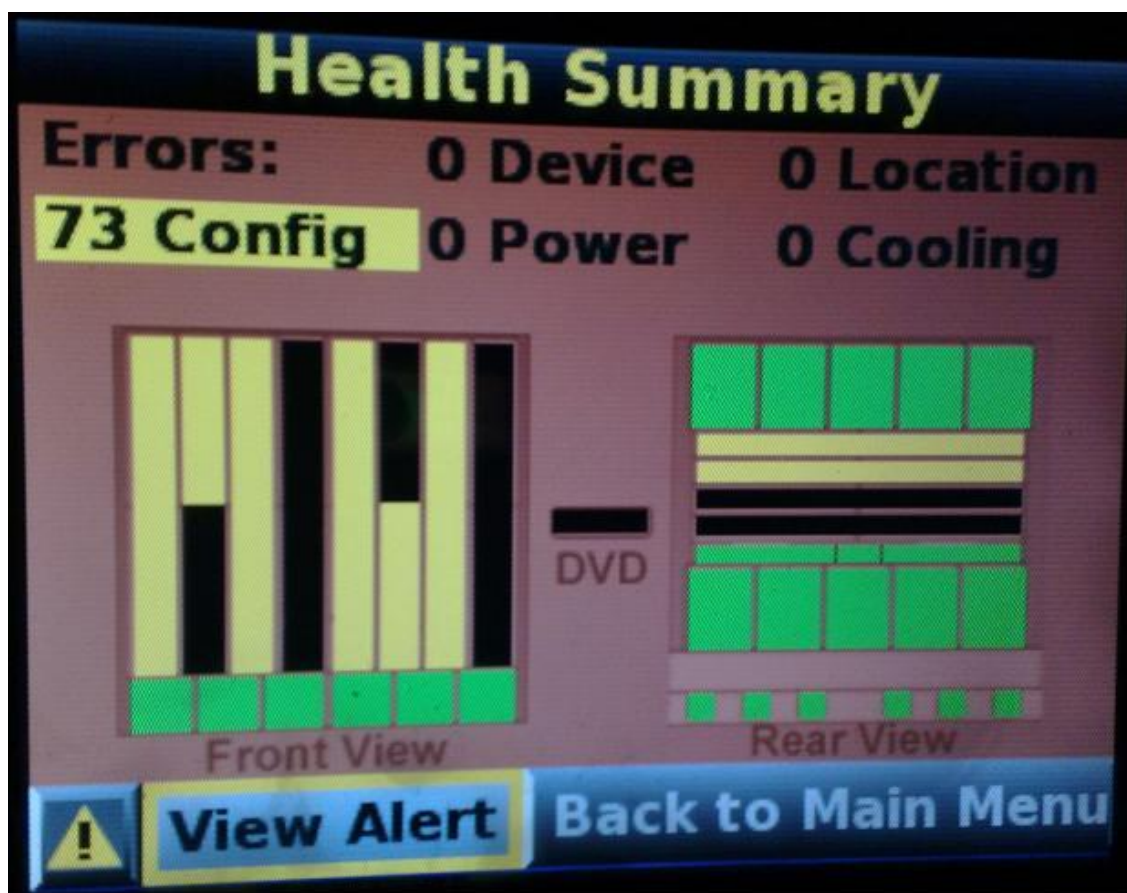


Kuvio 14. Verkon rakenne.

### 7.3 Blade-kehikon error-ongelmat

#### 7.3.1 BladeSystemin virheet

Blade-kehikossa ilmeni virheitä, jonka vuoksi Blade-palvelimet eivät aluksi käynnistyneet lainkaan. Blade-palvelimissa paloi vihreiden valojen sijasta oranssi valo, joka tarkoittaa, että palvelin on sammuksissa, mutta saa kuitenkin virtaa. HP Insight Displayn vasemmassa alakulmassa näkyi virhetilanteista ilmoittava keltainen varoituskolmio. Health Summary -näkyessä ilmoitettiin, että virheitä on yhteensä peräti 73. Virheet olivat samanlaisia, ainoastaan eri paikoille tulleita virheilmoituksia.



Kuvio 15. HP Insight Displayn Health Summary –näkyvän virheilmoitukset.

Blade-järjestelmässä ilmenneitä virheilmoituksia:

Svr Bay 13 iLO Network Problem

I/O Keying Mismatch for Svr Bay 15 Emb NIC 2

I/O Keying Mismatch for IO Module Slot 2 Port 15

I/O Keying Mismatch for Svr Bay 14 Mezz 1 Port 2

### 7.3.2 Virheiden selvittäminen

HP Insight Displayn Health Summary -näkylässä oikein toimivat komponenttipaikat näkyvät vihreinä, virheitä sisältävät komponenttipaikat näkyvät keltaisina ja tyhjät komponenttipaikat näkyvät mustina. Tumman vihreä tarkoittaa, että komponentti ei ole päällä, mutta siinä ei kuitenkaan esiinny virheitä.

Health Summary -näkylässä tarkastelemalla pystyi päättelemään, että virtalähteet, tuuletin ja OA-moduulit on oikein asennettu eivätkä aiheuttaneet virheitä. Virheilmoitukset johtuivat Health Summary -ikkunan mukaan Blade-palvelimista sekä Ethernet- ja FC-moduuleista.

Johtopäätös virheistä oli se, että todennäköisesti Ethernet- ja FC-moduulit oli asennettu väärin moduulipaikkoihin. FC-moduulit olivat moduulipaikoilla 1 ja 2. Ethernet-moduulit olivat paikoilla 3 ja 4. Pääteltiin, että moduulivirheet todennäköisesti poistuisivat Ethernet- ja FC-moduulien paikkaa vaihtamalla. Kehikkoon saattaisi kuitenkin jäädä vielä virheitä.

### 7.3.3 Virheiden korjaus

Virheiden korjaamiseksi ethernet- ja FC-moduulit irrotettiin keihikon takaosan moduulipaikoista. Ethernet-moduulit laitettiin nyt paikoille 1 ja 2, kun taas FC-moduulit laitettiin paikoille 3 ja 4. Kun Blade-kehikko oli päivittänyt muutokset, HP Insight Displayn Health Summary -näkyssä ilmoitti yhden virheen. Kyseinen virhe oli "Svr Bay 13 iLO Network Problem". Kyseisen palvelinpaikan Blade-palvelimessa paloi punainen varoitusvalo NIC1-tekstin kohdalla. Myöhemmin selvisi, että kyseisessä palvelinpaikassa ollut Blade-palvelin oli rikki eikä sitä voinut Insight Displayn tarjoamien ohjeiden perusteella saada toimintakuntoon.

Virheiden korjauksen jälkeen kaikki neljä moduulipaikkaa näkyi Health Summary -näkylässä vihreinä eli ne toimivat. Kehikon takapuolella kyseisissä moduuleissa paloi myös vihreät valot.

## 7.4 Etähallinta

### 7.4.1 Etähallinta HP Onboard Administratorin avulla

Blade-kehikon etähallinta on mahdollista HP Onboard Administratorin ja HP Virtual Connectin avulla. Blade-kehikon HP Insight Displayta käyttäen vaihdettiin Blade-kehikon OA1:n IP-osoitteeksi 10.95.241.101 /24. OA2:n IP-osoitteeksi vaihdettiin 10.95.241.102 /24. Molemmat OA-moduulit yhdistettiin verkkokaapelilla kytkimen VLAN 401 -portteihin. Tämän jälkeen selaimella sai muodostettua etäyhteyden HP Onboard Administratoriin. HP Onboard Administratorin käyttö vaatii sisäänkirjautumisen, jossa vaaditaan käyttäjätunnus ja salasana. OA-moduuleihin oli kiinnitetty lappu, jossa oli kahdet oletustunnukset, joista toinen oli käytössä aktiivisessa OA-moduulissa. Näin kehikkoa pystyi hallitsemaan etänä. HP Onboard Administratoriin luotiin uudet tunnukset järjestelmänvalvojan oikeuksilla. Tästä lähtien työssä käytettiin vain näitä tunnuksia oletustunnusten sijaan.

Blade-kehikon asetukset käytiin läpi ja asetuksista muutettiin mm. Blade-kehikon nimi, laitetelineen nimi, Blade-palvelinten iLO-osoitteet, ethernet- ja FC-moduulien iLO-osoitteet. Blade-palvelimille täytyi syöttää IP-osoite, aliverkkomaski, gateway-osoite, domainin nimi ja DNS-palvelinten osoitteet. iLO-osoitteiksi laitettiin VLAN 401:n IP-osoitteita eli osoitteet verkosta 10.95.241.0 /24. Kun palvelimille syötti uudet hallinta-osoitteet ja hyväksyi muutokset, iLO-proessorit käynnistyivät uudelleen uusilla asetuksilla. Interconnect Bays -välilehdelle piti syöttää ethernet- ja kuitumoduulien hallinta-osoitteet. Tarvittavat osoitteet olivat IP-osoite, aliverkkomaski, gateway-osoite, domain, DNS-palvelimet ja NTP-palvelimet. NTP-palvelinten osoitteiksi laitettiin 193.167.197.100 ja 195.148.144.100.

### 7.4.2 Etähallinta HP Virtual Connectin avulla

HP Virtual Connect Managerin avulla pystyy hallitsemaan Blade-kehikon verkkoyhteyksiä. HP Virtual Connect Managerissa määriteltiin ensin halutut alkuasetukset, jonka jälkeen siirryttiin muokkaamaan palvelinprofileja, ethernet-verkkoja ja jaettuja uplinkkejä. Kuituyhteyksien asetuksia ei muokattu, koska työssä ei ollut käytössä kuitukytkimiä.

## Server Profiles

Server Profiles -välilehdellä määriteltiin palvelinprofiilit. Jokaiselle Blade-palvelimelle piti luoda oma palvelinprofiili. Jokaiselle palvelinprofiilille määriteltiin nimi, mitä VLAN:ia kyseinen palvelin käyttää ja missä palvelinpaikassa Blade-palvelin on kiinni. Työssä luotiin palvelinprofiilit palvelinpaikoille 1-8. Nämä asetukset ovat palvelinkohtaisia, joten ne pitää määrittää jokaiselle palvelimelle erikseen.

**Edit Server Profile: Server-2**

**Profile**

Profile Name	Status
Server-2	✓

**Ethernet Adapter Connections**

Port	Network Name	Status	Port Speed	Allocated Bandwidth	PXE	MAC	Mapping
1	Vlan-400-1	✓	PREFERRED	1 Gb	DISABLED	00-17-A4-77-00-04	LOM:1 => Bay 1
2	Multiple Networks	?	PREFERRED	1 Gb	DISABLED	00-17-A4-77-00-06	LOM:2 => Bay 2

**FC HBA Connections**

Port	Connected To	FC SAN Name	Status	Port Speed	WWPN	Mapping
1	Bay 3	Unassigned	☑	AUTO	HW-DEFAULTS	MEZZ1:1 => Bay 3
2	Bay 4	Unassigned	☑	AUTO	HW-DEFAULTS	MEZZ1:2 => Bay 4

Fibre Channel Boot Parameters

**Assign Profile to Server Bay**

Enclosure	Server	Model	SN	Status	Power	UD
bulelab-c1	Bay 2	ProLiant BL460c G1	CZJ804015A	✓	✓	⊘

Apply Cancel

Kuvio 16. Kuva Server-2:n palvelinprofiilista.

Tässä työssä käytettiin palvelimia Server-2 ja Server-3, joiden palvelinprofiileihin määriteltiin Ethernet Adapter Connections -kohtaan port 1: Vlan-400-1 ja port 2: Multiple Networks, johon sisältyi Vlan-400-2 ja Vlan-402-2. Täten oli mahdollista käyttää palvelimia VLAN:eissa 400 ja 402. FC HBA Connections -kohdat oli tarkoitettu kuitumoduuleille, joita tässä työssä ei käytetty, joten ne kohdat jätettiin tyhjiksi. Assign Profile to Server Bay -kohdassa määriteltiin palvelinprofiili tietylle palvelinpaikalle.

## Ethernet Networks

Ethernet Networks -välilehdellä määriteltiin halutut VLAN:t. Työssä luotiin Vlan-400-1, Vlan-400-2, Vlan-402-1 ja Vlan-402-2. Tämä mahdollisti VLAN 400:n ja VLAN 402:n käytön Blade-palvelimilla. VLAN 401 ei luotu tähän kohtaan, koska VLAN 401 on käytössä iLO-hallintaosoitteissa eikä sitä tarvita Blade-palvelimien ja muun verkon väliseen liikenteeseen.

## Shared Uplink Sets

Shared Uplink Sets -välilehdellä määriteltiin Vlan-400-1 ja Vlan 402-1 Uplink1:lle. Vlan 400-2 ja Vlan 402-2 määriteltiin Uplink2:lle. Blade-kehikkoon tulevat uplinkit kytkettiin molempien ethernet-moduulien porttiin 1. Verkkokaapelin toiset päät kytkettiin HP 3500 -kytkimen portteihin 23 ja 24, jotka olivat trunk-portteja.

Kun Blade-kehikkoa oli konfiguroitu HP Onboard Administratorin ja HP Virtual Connect Managerin avulla, oli mahdollista käynnistää Blade-palvelimet ja alkaa suorittaa niille haluttuja toimenpiteitä.

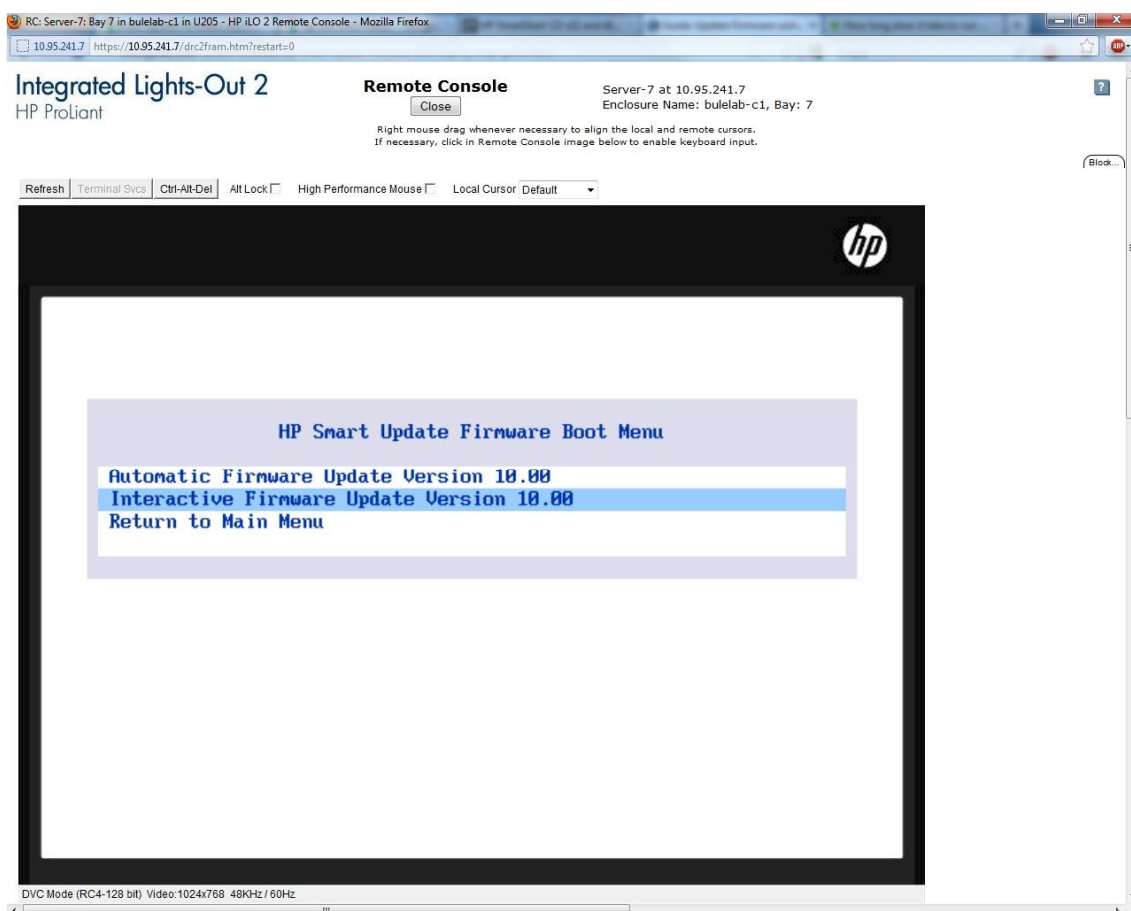
Uplink Set	Status	Network		Settings	
		sharedNetworkName	VLAN ID	Smart Link	Private network
Uplink1	OK	Vlan-402-1	402	<input type="checkbox"/>	<input type="checkbox"/>
	OK	Vlan-400-1	400	<input type="checkbox"/>	<input type="checkbox"/>
Uplink2	OK	Vlan-400-2	400	<input type="checkbox"/>	<input type="checkbox"/>
	OK	Vlan-402-2	402	<input type="checkbox"/>	<input type="checkbox"/>

Kuvio 17. Shared Uplink Sets, jossa näkyy uplinkit sekä niiden käyttämät VLAN:t.

### 7.4.3 Firmware-päivitykset

Internetistä ladattiin firmware-päivitys ja HP USB Key Utility -ohjelmaa käyttäen tehtiin USB-tikusta firmwarepäivityksen sisältävä boottaava USB-tikku. Firmwarepäivitys oli täten mahdollista suorittaa suoraan usb-tikulta. USB-tikku yhdistettiin Blade-

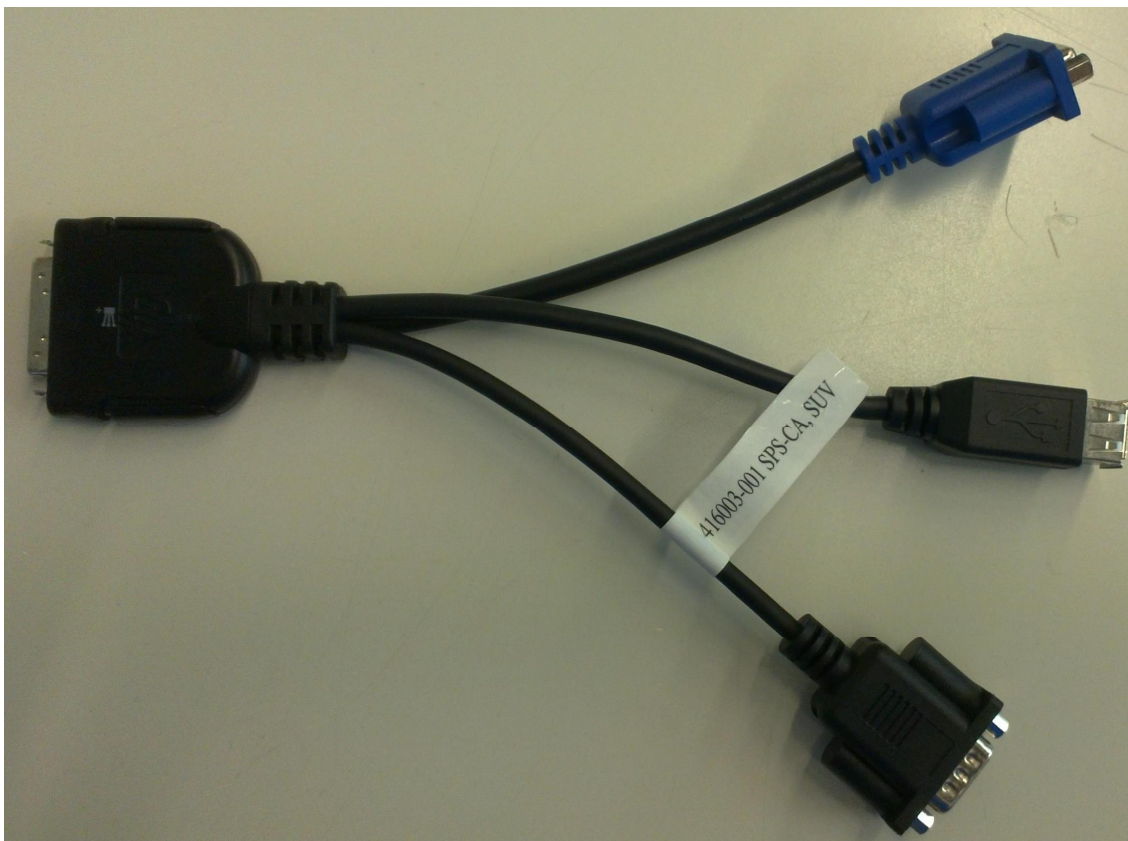
palvelimeen käyttäen SUV-kaapelia, jonka avulla voidaan yhdistää video- ja USB-laitteita Blade-palvelimeen. USB-tikku kiinnitettiin palvelimeen ja internetin välityksellä otettiin Remote Console -yhteys OA:n kautta, josta näkyi, mitä palvelimen näytöllä tapahtui. BIOS:sta säädettiin USB-laitteen bootin ykkösprioriteetiksi ja sitten blade-palvelin käynnisti päivitysohjelman suoraan USB-tikulta. Firmwarepäivitys alkoi HP USB BOOT Menusta, josta sai valita automaattisen ja interaktiivisen päivityksen väliltä. Firmwarepäivitys päivitti iLO:n versioon 2.07 ja palvelimen laiteohjelmisto päivittyi samalla versioon 5.03.15.



Kuvio 18. HP iLO Remote Console -hallintaikkunassa näkyvä firmware-päivityksen valikko.

OA:n puolelta Blade-palvelimia käytettiin iLO:n kautta Remote Console -etäyhteydellä, joka ei ole kovin käyttäjäystävällinen. Kun Blade-palvelimeen oli asentanut käyttöjärjestelmän ja laittanut verkkoyhteydet kuntoon, pystyi Blade-palvelinta hallitsemaan Remote Desktop Connectionin avulla, joka on huomattavasti mukavampi tapa hallita Blade-palvelinta.





Kuvio 19. SUV-kaapeli, jolla voi yhdistää video- ja USB-laitteita Blade-palvelimeen.

## 7.5 Käyttöjärjestelmien asennus Blade-palvelimille

Koska tässä työssä ei ollut käytössä ulkoista levyjärjestelmää, piti huolehtia, että Blade-palvelimissa on kiinni kiintolevyt. Suurimmassa osassa Blade-palvelimia RAID-ohjain ei ollut päällä, joten se laitettiin BIOS:sta käsin päälle. Blade-palvelimen käynnistyessä uudelleen käynnistettiin RAID-ohjaimen valikko, josta poistettiin vanha RAID ja luotiin uusi RAID1+0.

Käyttöjärjestelmien asennuksessa käytin ulkoista kovalevyä, joka oli kytketty SUV-kaapelia käyttäen Blade-palvelimeen. Blade-palvelimien IP-osoitteet oli tarkoitus määrittellä verkkoon VLAN 400 eli 10.95.240.0 /24.

### 7.5.1 VMware ESXi

Blade-palvelimeen Server-2 asennettiin VMware ESXi -käyttöjärjestelmä. Työssä käytettiin VMware ESXi:n ilmaisversiota, joka rajoittaa käytön vain yhteen palvelimeen eikä



sisällä kaikkia kehittyneimpiä ominaisuuksia. Kun asennus oli valmis, verkkoyhteydet valmisteltiin kuntoon. Server-2:n IP-osoiteeksi määriteltiin 10.95.240.2 ja kyseistä palvelinta pystyi käyttämään Remote Desktop Connection -ohjelman avulla.

### 7.5.2 Windows Server 2008 R2

Blade-palvelimeen Server-3 asennettiin Windows Server 2008 R2 -käyttöjärjestelmä. Kaikista vaihtoehdoista asennettavaksi valittiin Enterprise-vaihtoehto. Server Managerin avulla pystyy lisäämään erilaisia rooleja ja tähän palvelimeen lisättiin virtuaalikoneisiin tarkoitettu ohjelma nimeltä Hyper-V. Server-3:n IP-osoiteeksi määriteltiin 10.95.240.3 ja kyseistä palvelinta pystyi käyttämään Remote Desktop Connection -ohjelman avulla.

## 7.6 Virtuaalikoneet Blade-palvelimissa

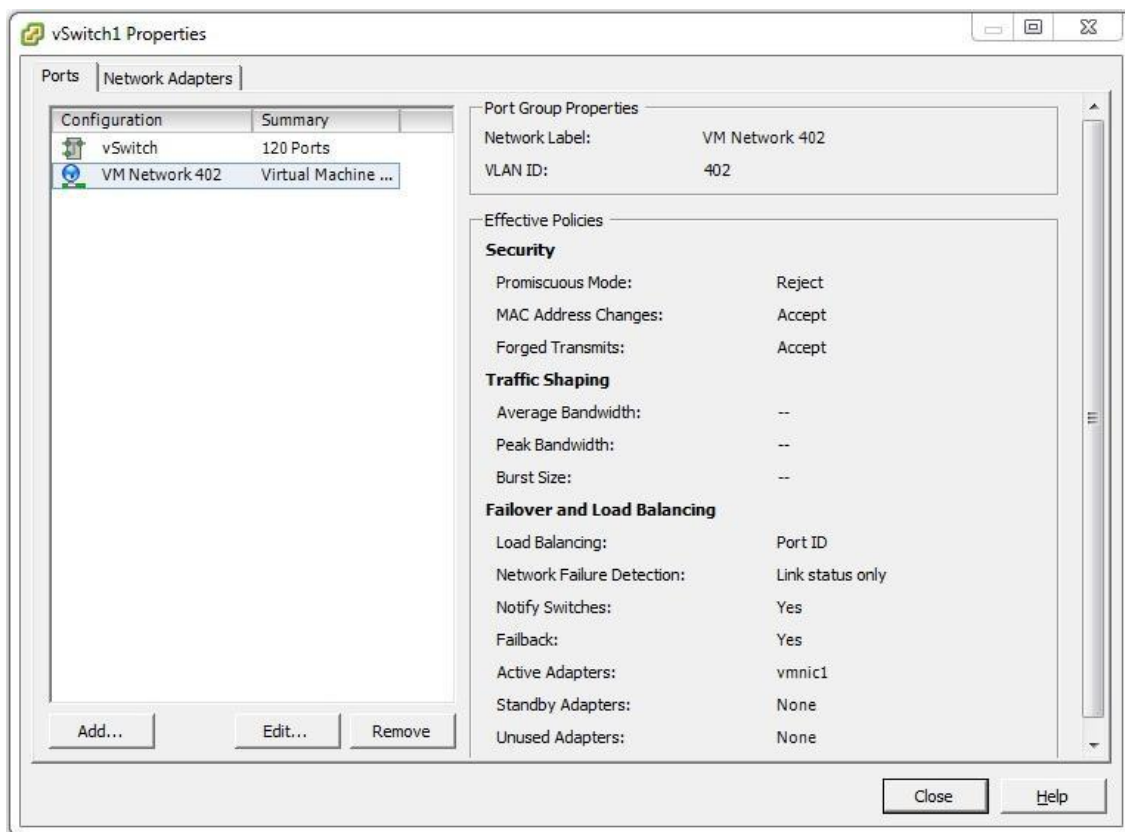
Tarkoituksena oli testata virtuaalikoneiden toimivuutta Blade-palvelimissa ja kokeilla miten virtuaalikoneet ja Blade-palvelimet saa eri verkkoon. Blade-palvelimien IP-osoitteet olivat VLAN 400:ssa, niiden iLO-hallintaosoitteet olivat VLAN 401:ssa, kun taas Blade-palvelimien virtuaalikoneiden IP-osoitteet oli tarkoitus määrittellä verkkoon VLAN 402 eli 10.95.242.0 /24. Jotta virtuaalikoneet toimivat Blade-palvelimissa, piti BIOS:sta laittaa virtualisointituki päälle. BIOS:ssa otettiin käyttöön No-Execute Memory Protection ja Intel ® Virtualization Technology.

### 7.6.1 VMware

Server-2:lle oli asennettu VMware ESXi, jota pystyi käyttämään VMware vSphere Clientin avulla kirjautumalla Blade-palvelimen IP-osoitteeseen 10.95.240.2. VMware vSphere Clientilla luotiin yksi virtuaalikone. Käyttöjärjestelmäksi tähän ladattiin internetistä Ubuntu 12.04 desktop (i386) .iso -image, joka asennettiin virtuaalikoneeseen. Virtuaalikoneeseen asennettu Ubuntu-käyttöjärjestelmä konfiguroitiin VLAN 402:n verkkoasetuksilla.

Jotta virtuaalikoneen verkkoyhteys saatiin toimimaan VLAN 402:ssa, piti tehdä muutoksia vSphere Client:n konfigurointi-välilehdellä, jossa luotiin uusi verkko, jonka yhteystyyppiä valittiin Virtual Machine. Network Access -kohdassa piti tehdä uusi vSphere

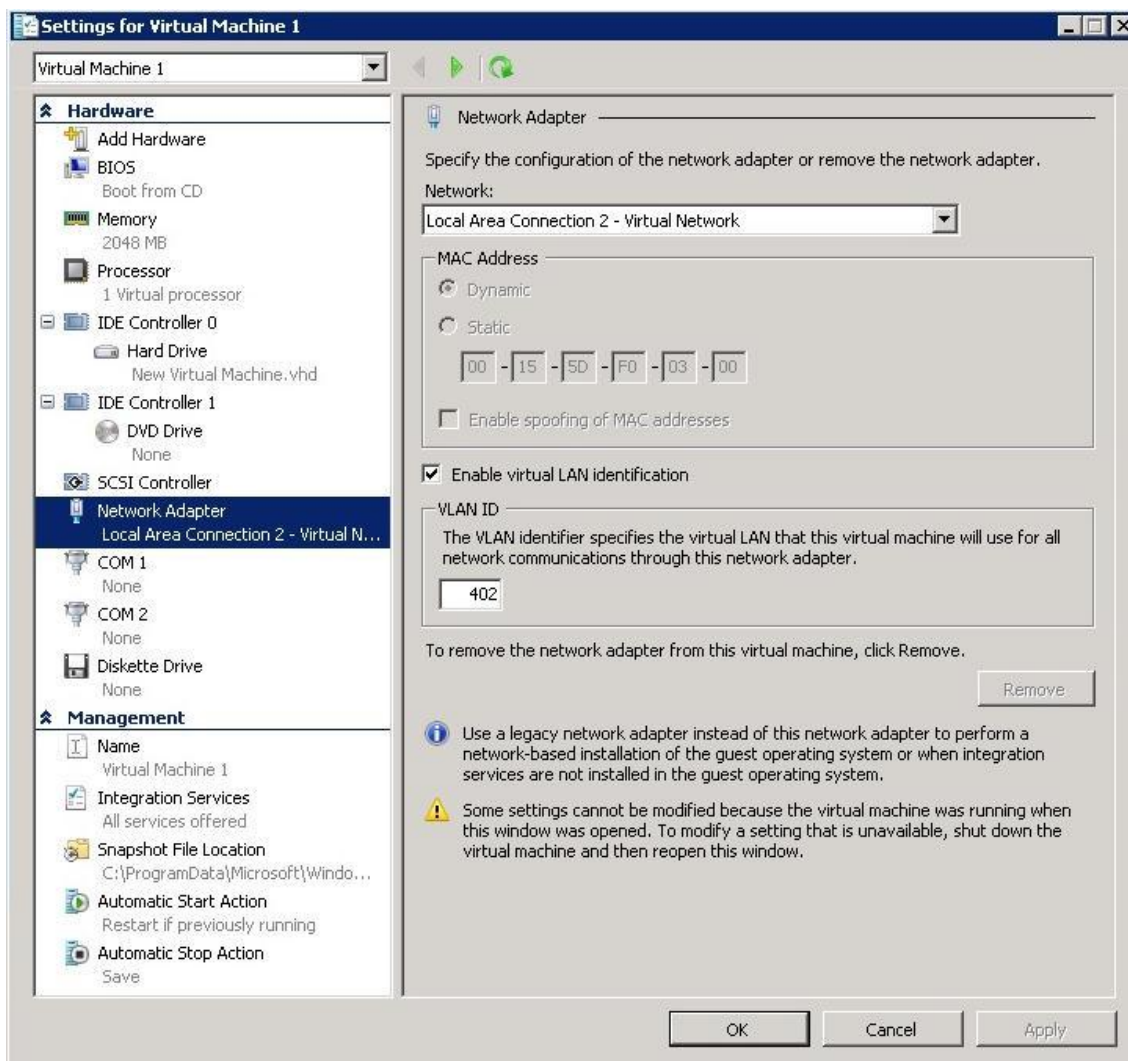
standard switch ja lopuksi määriteltiin haluttu VLAN, jota uusi verkko käyttää eli VLAN 402. Virtuaalikoneen ominaisuuksista valittiin verkko, jota virtuaalikone käyttää. Tähän valittiin juuri luotu verkko eli VLAN 402:ksi nimetty verkko. Näillä asetuksilla virtuaalikoneen verkkoyhteydet toimivat oikein.



Kuvio 20. VM Network 402:n asetukset, jossa valittuna VLAN ID 402.

## 7.6.2 Hyper-V

Hyper-V:hen luotiin kaksi uutta virtuaalikonetta, joihin molempiin asennettiin Windows Server 2008 R2. Virtuaalikoneisiin konfiguroitiin verkkoasetukset VLAN 402 -verkosta.



Kuvio 21. Virtuaalikone VM1:n Network Adapter -asetukset Hyper-V:ssa.

Hyper-V:n virtuaalikoneen asetuksista otettiin käyttöön VLAN-tunnistus, jonka alle määriteltiin haluttu VLAN ID-numero. Kun VLAN ID-numeroksi laittoi 402, ja virtuaalikoneen verkkoasetukset oli konfiguroitu VLAN 402:n IP-osoitteille, verkkoyhteydet toimivat halutussa verkossa täysin.

### 7.6.3 Virtuaalikoneiden testaus

Tarkoituksena oli testata, että virtuaalikoneet toimivat jossakin toisessa VLAN:ssa, joka on eri VLAN kuin Blade-palvelinten hallintaosoitteille tarkoitettu VLAN. Nyt lopullisessa verkossa on siis VLAN:t 400, 401 ja 402. Näistä VLAN 401 on HallintaVLAN, VLAN 400 on PalvelutVLAN ja VLAN 402 on virtuaalikoneille varattu verkko.

Kaikkien virtuaalikoneiden verkkoyhteydet testattiin ja ne toimivat halutulla tavalla. Virtuaalikoneiden verkkoyhteydet toimivat halutun verkon IP-osoitteilla. Tämä testattiin VLAN:eilla 400 ja 402.

## 8 Yhteenveto

Tässä insinööriyössä otettiin Blade-järjestelmä käyttöön Metropolia Ammattikorkeakoulun tiloihin. Työssä suoritettiin Blade-järjestelmän asennus, konfigurointi ja testaus. Blade-kehikkoon asennettiin Blade-palvelimia ja eri verkkomoduuleita työn suorittamiseksi.

Insinööriyön raportissa kerrottiin Blade-tekniikoista, joita Blade-kehikossa on käytössä. Blade-järjestelmän etähallinta oli tärkeä osa tätä insinööriyötä, ja sitä käytettiin paljon hyödyksi työtä tehdessä. Työssä tutustuttiin Blade-järjestelmän etähallintaan Onboard Administratorin ja Virtual Connectin avulla. Työssä luotiin katsaus virtualisointiin ja testattiin virtuaalikoneita Blade-palvelimissa.

Kaikki tarvittavat työvaiheet saatiin suoritettua ja Blade-järjestelmä testattiin onnistuneesti, joten työ onnistui kokonaisuudessaan hyvin. Mikäli työtä haluaisi vielä kehittää eteenpäin, voisi työssä tutustua johonkin levyjärjestelmään ja suorittaa sen käyttöönoton. Tähän vaadittaisiin kuitenkin lisää asiaan perehtymistä ja lisää aikaa.

## Lähteet

- [1] Server (computing). Verkkodokumentti. Viitattu: 22.3.2012  
Saatavissa:  
[http://en.wikipedia.org/wiki/Server\\_%28computing%29](http://en.wikipedia.org/wiki/Server_%28computing%29).
- [2] HP Proliant BL460c G1 QuickSpecs. Verkkodokumentti. Viitattu 21.4.2012.  
Saatavissa:  
[http://www.harddrivesdirect.com/quickspecs\\_proliant\\_BL460c.php](http://www.harddrivesdirect.com/quickspecs_proliant_BL460c.php).
- [3] CCNA2: Chapter 10. Oppimateriaali. Viitattu: 24.3.2012.
- [4] Odom, Wendell. CCNP route 642-902 official certification guide, 2010.  
Oppikirja. Viitattu 25.3.2012.
- [5] Administrative distance. Verkkodokumentti. Viitattu: 24.3.2012  
Saatavissa:  
[http://en.wikipedia.org/wiki/Administrative\\_distance](http://en.wikipedia.org/wiki/Administrative_distance).
- [6] Link-state routing protocol. Verkkodokumentti. Viitattu 25.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/Link\\_state\\_routing\\_protocol](http://en.wikipedia.org/wiki/Link_state_routing_protocol).
- [7] Open Shortest Path First. Verkkodokumentti. Viitattu 24.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/Open\\_Shortest\\_Path\\_First](http://en.wikipedia.org/wiki/Open_Shortest_Path_First).
- [8] Dijkstra's algorithm. Verkkodokumentti. Viitattu 26.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/Dijkstra%27s\\_algorithm](http://en.wikipedia.org/wiki/Dijkstra%27s_algorithm).
- [9] Virtual LAN. Verkkodokumentti. Viitattu 26.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN).

- [10] Spanning Tree Protocol. Verkkodokumentti. Viitattu 29.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](http://en.wikipedia.org/wiki/Spanning_Tree_Protocol).
- [11] HP BladeSystem c-Class. Verkkodokumentti. Viitattu 2.4.2012.  
Saatavissa:  
[http://www.bcc.fi/Suomeksi/Jarjestelmat\\_ja\\_palvelut/Palvelimet/HP\\_BladeSystem\\_c-Class](http://www.bcc.fi/Suomeksi/Jarjestelmat_ja_palvelut/Palvelimet/HP_BladeSystem_c-Class).
- [12] HP BladeSystem c7000 Enclosure - Quick Setup Instructions. Verkkodokumentti. Viitattu 22.4.2012.  
Saatavissa:  
<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00698534/c00698534.pdf>.
- [13] HP BladeSystem - Onboard Administrator. Verkkodokumentti. Viitattu 22.4.2012.  
Saatavissa:  
[http://h18004.www1.hp.com/products/blades/components/onboard/index.html?jumpid=reg\\_R1002\\_USEN](http://h18004.www1.hp.com/products/blades/components/onboard/index.html?jumpid=reg_R1002_USEN).
- [14] HP Intelligent Power Discovery. Verkkodokumentti. Viitattu 18.3.2012.  
Saatavissa:  
<http://h18004.www1.hp.com/products/servers/rackandpower/powersupplies/ipd/overview.html>.
- [15] HP Intelligent Power Distribution Unit. Verkkodokumentti. Viitattu 18.3.2012.  
Saatavissa:  
<http://h18004.www1.hp.com/products/servers/rackandpower/powersupplies/ipdu/index.html>.

- [16] HP BladeSystem c7000 Enclosure Setup and Installation Guide. Verk  
kodokumentti. Viitattu 26.4.2012.  
Saatavissa:  
[http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00698286  
/c00698286.pdf](http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00698286/c00698286.pdf).
- [17] VMware. Verkkodokumentti. Viitattu 18.3.2012.  
Saatavissa:  
<http://en.wikipedia.org/wiki/VMware>.
- [18] VMware ESXi Server. Verkkodokumentti. Viitattu 18.3.2012.  
Saatavissa:  
[http://en.wikipedia.org/wiki/VMware\\_ESXi\\_Server](http://en.wikipedia.org/wiki/VMware_ESXi_Server).

## HP 3500 -kytkimen konfiguraatio

Startup configuration: 28

; J8692A Configuration Editor; Created on release #K.15.06.0008

; Ver #01:0d:0c

hostname "HP-E3500yl-24G"

module 1 type J86xxA

ip routing

vlan 1

name "DEFAULT\_VLAN"

untagged 21-22

ip address dhcp-bootp

no untagged 1-20,23-24

exit

vlan 50

name "VLAN50"

untagged 1-4

ip address 10.95.0.111 255.255.254.0

tagged 23-24

exit

vlan 400

name "PalvelutVLAN"

untagged 11-20

ip address 10.95.240.254 255.255.255.0

tagged 23-24

exit

vlan 401

name "HallintaVLAN"

untagged 5-10

ip address 10.95.241.254 255.255.255.0

tagged 23-24



```
exit
vlan 402
  name "VLAN402"
  ip address 10.95.242.254 255.255.255.0
  tagged 23-24
exit
router ospf
  area backbone range 10.95.240.0 255.255.252.0 type summary
  redistribute connected
  redistribute static
  enable
exit
snmp-server community "public" unrestricted
spanning-tree
spanning-tree config-name "Bulelab"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 1-4093
vlan 50
  ip ospf 10.95.0.111 area backbone
exit
password manager
password operator
```