KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Markus Varjola

Virtuaalisten verkkorajapintojen hallinta ja toteutus SimuNet-ympäristössä

Opinnäytetyö 2012

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

VARJOLA, MARKUS

Virtuaalisten verkkorajapintojen hallinta ja toteutus SimuNet-ympäristössä

Opinnäytetyö 52 sivua + 14 liitesivua
Työn ohjaaja yliopettaja Martti Kettunen
Toimeksiantaja KYMP Oy, SimuNet-hanke
Maaliskuu 2012
Avainsanat SimuNet, Nexus, VMware, EVC, Virtualisointi, EoMPLS

Virtualisoitujen ratkaisujen lisääntyessä tietoverkkojen ja palvelimien hallinta-alueiden rajat ovat alkaneet sekoittua. On tilanteita, joissa palvelimien ylläpitäjien pitäisi hallita myös tietoverkkotekniikoita. Ilmiö on herättänyt kysyntää ratkaisuille, jotka selkeyttäisivät hallinta-alueiden rajat.

Kymenlaakson ammattikorkeakoulun tiloissa toimii SimuNet-niminen tietoverkkojen kehitys- ja testausympäristö. SimuNet on toteutettu käyttäen moderneja operaattoriverkon tekniikoita ja menetelmiä. Työn tarkoituksena on tuottaa simuloitu tilanne, jossa SimuNet esittää palveluntarjoajaa ja tuottaa palveluna virtuaalisten verkkojen rajapintojen hallintaa kuvitteelliselle asiakkaalle. Verkkojen hallinta toteutetaan käyttäen Nexus 1000V -virtuaalikytkintä. Lisäksi asiakkaan toimipisteet sillataan käyttäen hyväksi SimuNet-verkon palveluita.

Asiakkaan toimipisteet sillattiin hyödyntäen SimuNet-verkon IP/MPLS-tekniikkaa. Menetelmäksi valittiin Layer 2 -tasolla toteutettu, EVC-pohjainen EoMPLS-tunnelointi. Nexus 1000V -virtuaalikytkimen komponentit sijoitettiin SimuNet-verkon VMware-klusteriin ja asiakkaan ESXi-palvelimiin. Työn alussa käydään läpi käytettyjä protokollia, esitellään asiakkaan verkon muutossuunnitelmat ja lopuksi käydään läpi tekninen toteutus vaihe vaiheelta.

Tuloksena kuvitteellisen asiakkaan toimipisteet saatiin sillattua Layer 2 -tasolla hyödyntäen SimuNetin MPLS-palveluja ja EVC-tekniikkaa. Siltauspalvelua täydennettiin siirtämällä asiakkaan virtuaalisten verkkojen rajapintojen hallinta palveluntarjoajan vastuulle hyödyntäen Nexus 1000V -virtuaalikytkintä. Ratkaisu todettiin kokonaisuutena toimivaksi, mutta tietyissä olosuhteissa epävarmaksi.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

VARJOLA, MARKUS	Management of Virtualized Network Edges and Implementation into SimuNet Environment
Bachelor's Thesis	52 pages + 14 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	KYMP Oy, SimuNet Project
March 2012	
Keywords	SimuNet, Nexus, VMware, EVC, Virtualization, EoMPLS

As virtualized solutions have increased, network and server management boundaries have begun to mix. There are situations when server administrators must know how to manage different network technologies. This phenomenon has given rise to the demand for solutions that clarify the management boundaries.

Kymenlaakso University of Applied Sciences hosts a development and testing network called SimuNet. SimuNet environment has been implemented using modern techniques and methods also used by network operators. The goal of this study was to produce a simulated situation where SimuNet presents the service provider and produces a service of managing virtualized network edges of a fictional client. Network management was carried out using the Nexus 1000V virtual switch. In addition, the client's branch offices were bridged by using SimuNet's network services.

At the beginning of the study the principles and protocols used in this study were explained, migration plans for the clients network were presented and then the technical implementation followed step by step. Client's branch offices were bridged by utilizing SimuNet's IP/MPLS network. Bridging was carried out at Layer 2 and achieved by EVC-based EoMPLS tunneling. The Nexus 1000V virtual switch components were installed in SimuNet's VMware cluster and the clients ESXi servers.

As a result, the fictitious client's branch offices were bridged over Layer 2 connection by utilizing SimuNet's MPLS services and EVC technology. The bridge service was supplemented by moving the client's virtualized network management responsibility to the service provider utilizing the Nexus 1000V virtual switch. The solution proved to be functional, but unstable under certain conditions.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

LYHENNELUETTELO 6

1 JOHDANTO 9

2 TYÖN RAJAUS JA TAVOITE 10

3 KÄSITTEITÄ 10

3.1 Virtual Local Area Network (VLAN) 11
3.2 Multiprotocol label switching (MPLS) 11
3.3 MPLS L2VPN-menetelmät 12

3.3.1 Virtual Private Lan Service (VPLS) 12
3.3.2 Ethernet Virtual Connection (EVC) 13
3.4 iSCSI-protokolla 14
3.5 MAC Pinning Port Channel 14

4 SIMUNET 15

4.1 Yleistä 15
4.2 Topologia 15

5 SUUNNITELMA 16

6 TEKNINEN TOTEUTUS 18

6.1 Verkon konfigurointi 18

6.1.1 EVC L2VPN 19
6.1.2 CE-kytkimet 20
6.2 Asiakkaan iSCSI konfiguraatio 21
6.3 SimuNet vSwitch konfigurointi 23
6.4 Virtual supervisor module (VSM) 24

6.4.1 Asennus 25
6.5 Virtual ethernet module (VEM) 28

6.5.1 Asennus 29
6.6 VMware vCenter 30
6.6.1 Asennus 30
6.6.2 VMware-klusteri 31
6.6.3 vSwitch:n konfigurointi 33
6.7 Nexus SVS -yhteys 36
6.8 Nexus Port profile 39
6.8.1 Konfigurointi 39
6.9 vCenter vNetwork Distributed Switch (vDS) migraatio 41
7 NEXUS 1000V ACCESS CONTROL LIST (ACL) 44
8 TODENTAMINEN 46
9 YHTEENVETO 48
LIITTEET
Liite 1. SimuNetin fyysinen kytkentä.
Liite 2. Asiakasverkon lähtötilanne
Liite 3. Asiakasverkon lopputilanne
Liite 4. CE1-laitteen konfiguraatio
Liite 5. CE2-laitteen konfiguraatio
Liite 6. PE3-laitteen konfiguraatio
Liite 7. PE4-laitteen konfiguraatio
Liite 8. Nexus 1000V:n konfiguraatio

LYHENNELUETTELO

API	Application programming interface; *Ohjelmointirajapinta*
CDP	Cisco Discovery Protocol; *Ciscon protokolla suoraan kytkettyjen laitteiden tunnistamista varten*
CE-laite	Customer Edge; *Asiakasverkon reunalaite*
dot1Q	IEEE 802.1Q; *Virtuaaliset lähiverkot ja runkolinkit mahdollistava verkkostandardi*
DRS	Distributed Resource Scheduler; *VMware-klustereiden resurssien osoittamisesta vastaava järjestelmä*
EAKR	*Euroopan aluekehitysrahasto*
EoMPLS	Ethernet over MPLS; *Tunnelointitekniikka Ethernetkehysten kuljettamiseen MPLS-verkossa*
EVC	Ethernet Virtual Circuit; *Operaattoriverkkojen virtuaaliverkkotekniikka*
HA	High Availablity; *Korkea saatavuus*
IEEE	Institute of Electrical and Electronics Engineers; *Maailmanlaajuinen standardien kehitysorgnasiaatio*
IGMP	Internet Group Management Protocol; *Multicast-ryhmien muodostamiseen käytetty protokolla*
IOS	Internetwork Operating System; *Cisco Systemsin verkkolaitteiden käyttöjärjestelmä*
IPv4	Internet Protocol version 4; *Internet-protokollan versio 4*
IPv6	Internet Protocol version 6; *Internet-protokollan versio 6*

iSCSI	Internet Small Computer System Interface; *Tiedon tallennusjärjestelmissä käytetty protokolla*
LAN	Local Area Network; *Lähiverkko*
LUN	Logical Unit Number; *Loogisten tallennusyksiköiden tunniste numero*
MAC-osoite	Media Access Control; *Ethernet-verkon laitteita yksilöivä Layer 2 -tason tunnus*
MPLS	Multiprotocol Label Switching; *Lippumerkintöihin perustuva pakettien kytkentätekniikka*
OSI-malli	Open Systems Interconnection; *Esitys tiedonsiirtoprotokollista seitsemässä eri tasossa*
PE-laite	Provider Edge; *Operaattoriverkon reunalaite*
P-laite	Provider; *Operaattoriverkon runkolaite*
pnic	Physical Network Interface Controller; *Ciscon termi VMware ESXi -palvelimen fyysisistä verkkokorteista*
QoS	Quality of Service; *Palvelun laatu*
RAID	Redundant Array of Independent Disks; *Usean kiintolevyn yhdistäminen loogisiksi levyiksi*
SDRS	Storage Distributed Resource Scheduler; *VMware-klustereiden tallennusresurssien osoitusjärjestelmä*
vDS	vNetwork Distributed Switch; *VMwaren hajautettu virtuaalikytkin, tai Nexus 1000V -virtuaalikytkin*
VEM	Virtual Ethernet Module; *Nexus 1000V:n virtuaalinen kytkinmoduuli*

VLAN	Virtual Local Area Network; *Virtuaalinen lähiverkko*
VM	Virtual Machine; *Virtuaalikone*
vnic	Virtual Network Interface Controller; *VMwaren termi VMware ESXi -palvelimen fyysisistä verkkokorteista*
VPN	Virtual Private Network; *Yleinen tunnelointikäsite*
VSM	Virtual Supervisor Module; *Nexus 1000V:n virtuaalinen hallintamoduuli*
vSwitch	Virtual Switch; *VMware-ympäristössä esiintyvä yksinkertainen virtuaalikytkin*

1 JOHDANTO

Tietoverkot ovat kasvaneet nopeasti viimeisten vuosien aikana ja niiden tärkeys suurille yrityksille ja laitoksille on kasvanut samalla vauhdilla. Vaatimusten taso on myös kasvanut ja tänä päivänä toimipisteet saattavat sijaita pitkien etäisyyksien päässä toisistaan. Tietoverkkojen on silti toimittava ja palveltava asiakkaita moitteettomasti. Nämä vaatimukset ovat tuoneet mukanaan uudenlaisia ja monimutkaisempia ratkaisuja, minkä seurauksena yritykset ovat alkaneet ulkoistaa tietoverkkopalvelujaan yhä enemmän. Kasvavat asiakasmäärät pakottavat verkko-operaattoreita hyödyntämään jo olemassa olevia verkkoja tehokkaammin. Tavoite on saavutettavissa hyödyntämällä virtualisointia, eikä virtualisointi ole ainoastaan tietoverkkoja varten. Virtualisointia voidaan käyttää myös tallennusjärjestelmien, palvelinten, tietoturvalaitteiden ja verkkoinfrastruktuurin kanssa (Kettunen 2009, 9).

Virtualisointi tuo myös mukanaan aivan uudenlaisia haasteita yrityksille ja verkko-operaattoreille. Merkittäväksi ongelmakohdaksi muodostuu raja, jossa fyysinen ja virtuaalinen verkko kohtaavat. Esimerkkinä yritys, joka haluaa ostaa tietoverkkojen hallinnan palveluna, mutta säilyttää omat virtualisoidut palvelimensa. Verkko-operaattori on kykenevä tarjoamaan palvelun aina verkkojen rajapinnalle saakka. Rajapinnan jälkeen verkko-operaattori menettää kaiken näkyvyyden ja hallinnan asiakkaan verkkoon. Palvelu jäisi vaillinaiseksi ja asiakkaan tulisi itse osata hallita ja ylläpitää verkon virtuaalista osuutta.

Cisco ja Vmware ovat yhdessä kehittäneet ratkaisua kyseiseen ongelmaan ja lopputuloksena on Cisco Nexus 1000V -sarja. Ratkaisu perustuu verkon rajapinnan siirtämiseen aina palvelimen ohjelmistoon saakka virtuaalisten kytkimien avulla (Bakke 2012). Näin verkko-operaattorin on mahdollista hallita koko verkkoa ja saavuttaa näkyvyys aina virtuaalikoneille saakka. Ratkaisu lisää myös asiakkaan näkyvyyttä verkon suuntaan, joka helpottaa vikatilanteiden selvittämistä.

Käytännön toteutus suoritettiin SimuNetin tiloissa, joka on Kymenlaakson ammattikorkeakoulun ja alueellisten yritysten testi- ja T&K-ympäristö (Kettunen 2009, 11). Laitteistona toimivat Kymenlaakson ammattikorkeakoulun tietohallinnon lainapalvelimet, SimuNet-ympäristön VMware-klusteri, SimuNetin runkoverkko ja Cisco Nexus 1000V. Kaikki työssä käytettävät ohjelmistot toimivat kokeilulisensseillä kustannussyistä ja termistö on suureksi osaksi Ciscon ja VMwaren omaa.

SimuNet-ympäristöön tehtyjen opinnäytetöiden lukumäärän vuoksi on mahdotonta välttää päällekkäisyyksiä edellisten opinnäytetöiden kanssa ja tämän vuoksi lähdeviittaukset edellisiin opinnäytetöihin on pyritty merkitsemään mahdollisimman selvästi.

2 TYÖN RAJAUS JA TAVOITE

Työssä on tarkoitus perehtyä tarkemmin Cisco Nexus 1000V -virtuaalikytkimen vaatimuksiin, toimintaan, asentamiseen ja käyttämiseen. Nexus 1000V -järjestelmän sulauttaminen SimuNet-verkkoon ja VMware-klusterin konfigurointi Nexuksen asennusta varten kuuluvat myös työn rajaukseen. SimuNetin toiminnan syvällisempi tutkiminen, työtä edeltäneet fyysiset asennustyöt ja VMware-palvelimien esiasennukset on rajattu työn ulkopuolelle. Kyseistä aiheesta ei löytynyt muita tehtyjä opinnäytetöitä, vaikka aihetta on sivuttu muutamassa työssä mainitsemalla Nexus-tuoteperhe.

Lähtötilanteessa kuvitteellisella asiakkaalla on kaksi toimipistettä, jotka sijaitsevat maantieteellisesti erotettuna toisistaan. Molemmilla toimipisteillä on oma virtualisointipalvelin ja tämän palvelimen paikallisessa käytössä oleva pieni iSCSI-tallennustila. Lähtötilanteessa palvelimet ja iSCSI-laitteet eivät hyödynnä keskitettyä hallinnointia.

Tavoitteena on tuottaa simuloitu tilanne, jossa asiakkaan kaksi toimipistettä yhdistetään toisiinsa palveluntarjoajan toimesta. Yhdistäminen toteutettaisiin hyödyntäen palveluntarjoajan MPLS-pilven mahdollistamia ratkaisuja. Toimipisteiden siltaamisen lisäksi tuotettaisiin palvelu, jossa palveluntarjoaja hyödyntää Nexus 1000V -virtuaalikytkintä ja poistaa asiakkaalta tarpeen hallita omien virtualisointipalvelimien verkkokonfiguraatiota. Simulaatiossa SimuNet-ympäristö edustaa palveluntarjoajaa ja asiakasta edustaa itsenäinen laiteräkki, jossa lainapalvelimet sijaitsevat. Alussa käsitellään työn kannalta oleellisia teorioita ja tämän jälkeen esitellään SimuNet lyhyesti. Teknisen toteutuksen järjestyskriittisyyden vuoksi asennus ja konfiguraatio toimenpiteet esitellään työvaiheittain.

3 KÄSITTEITÄ

Työssä esiintyy useita eri verkko- ja ohjelmistotekniikoita ja näistä oleellisimmat on käsitelty erikseen. Esimerkkinä työssä käytettävistä tekniikoista on MPLS, EVC, EoMPLS, VLAN, iSCSI ja MAC pinning. Useimmat työssä esiintyvistä termeistä ovat Ciscon tai VMwaren omia ja toiset valmistajat voivat puhua samoista asioista eri

termeillä. Vähemmän tärkeitä teoria- ja tekniikka-asioita käsitellään myöhemmin työn teknisen toteutuksen yhteydessä.

3.1 Virtual Local Area Network (VLAN)

Lähiverkko (LAN) käsittää kaikki laitteet samassa levitysviestialueessa (broadcast domain). Levitysviestialueeseen kuuluvat kaikki lähiverkkoon liitetyt laitteet, jotka voivat vastaanottaa muilta laitteilta lähetettyjä levitysviesti-kehyksiä. Lähiverkkoa ja levitysviestialuetta voi käytännössä ajatella samana asiana. Ilman virtuaalisia lähiverkkoja (VLAN) kytkin käsittelee kaikkia liityntäportteja yhtenä levitysviestialueena, toisin sanoen kaikki kytketyt laitteet ovat samassa lähiverkossa. VLAN-verkkojen avulla kytkin voi osoittaa liityntäportteja eri levitysviestialueille luoden kytkimen sisälle useita levitysviestialueita. Näitä kytkimen sisälle luotuja yksittäisiä levitysviestialueita kutsutaan VLAN-verkoiksi. (Odom 2008, 10.)

Työssä esiintyy erilaisia virtuaalisia verkkoja kuten MPLS- ja VLAN-verkkoja. Puhuttaessa virtuaalisista verkoista, kuitenkin viitataan perinteisiin VLAN-verkkoihin. Näitä käytetään pääsääntöisesti Nexus 1000V -virtuaalikytkimen erilaisten yhteyksien erottelemiseen toisistaan.

3.2 Multiprotocol label switching (MPLS)

MPLS-protokolla on lippukytkentäinen (label switching) mekanismi, jota MPLS-reitittimet ja -kytkimet voivat käyttää liikenteen kuljettamiseen. Hallintatasolla (control plane) MPLS-laite osoittaa tietylle liikenteelle lippumerkinnän ja näitä merkintöjä jaetaan eteenpäin käyttäen tehtävään tarkoitettuja protokollia. Jokainen laite jakaa paikallisesti osoitetut liput muille MPLS-laitteille ja vastaanottavat lipputietoja muilta laitteilta. Jokainen laite kokoaa näistä lipuista koostuvan tietokannan (LIB), jossa tiedot lipuista säilytetään. Jokainen laite suorittaa tiedon MPLS-enkapsuloinnin ennen liikenteen ohjaamista muille laitteille. MPLS-laitteen vastaanottaessa MPLS-enkapsuloitua liikennettä laite tekee välityspäätöksen MPLS-lipun otsikkotiedon perusteella. (Xu 2010, 6.)

Verrattuna tavalliseen Layer 3 -tason liikenteeseen MPLS on äärimmäisen tehokas ja monipuolinen tapa toteuttaa ja hallita operaattoriverkkoa. Layer 3 -tasolla operoidessa saapuvan paketin otsikko tarkistetaan reitityspäätöksen mahdollistamiseksi. Tällä tie-

dolla määritellään paketin seuraavan hypyn IP-osoite. Riippuen tilanteesta reititin voi joutua tarkastelemaan paketin muita kenttiä reitityspäätöstä varten, vaikka useimmiten vain IP-osoitetiedolla on merkitystä. Paketin matkan aikana jokainen reititin joutuu tutkimaan paketin IP-otsikon ja tämä toiminta tekee perinteisesti Layer 3 -tason liikennöinnistä hitaampaa. MPLS-verkossa paketin Layer 3 -otsikko joudutaan tutkimaan vain kerran, jonka jälkeen sille osoitetaan lippu ja tämän perusteella reitittimet voivat tehdä reitityspäätökset.

3.3 MPLS L2VPN-menetelmät

Operaattorin on mahdollista tarjota asiakkaille kahden tyyppisiä VPN-palveluita, jotka hyödyntävät MPLS-pilveä. OSI-mallin toisella kerroksella toimivat ratkaisut (Layer 2) ja kolmannella kerroksella toimivat ratkaisut (Layer 3). Työssä käytetään Layer 2 -tason ratkaisuja, jotka tunnetaan nimellä L2VPN ja näitä ratkaisuja ovat:

- Point-to-Point Virtual Leased Line (VLL) palvelu.
- Multipoint-to-Multipoint Ethernet Bridging Service, josta käytetään myös nimeä VPLS (Virtual Private LAN Service).

Layer 2 -tason ratkaisuja useimmiten tarjotaan asiakkaille, jotka haluavat hallita omaa verkkoa. Menetelmä tarjoaa yksinkertaisen ratkaisun verkko-operaattorille ja antaa asiakkaalle mahdollisuuden hallita itsenäisesti reitityspäätöksiä. (Xu 2010, 21)

3.3.1 Virtual Private Lan Service (VPLS)

VPLS on multipoint-to-multipoint tyyppinen ethernetsilta palvelu, joka kuljetetaan MPLS-pilven läpi. VPLS yhdistää useat maantieteellisesti erotetut sijainnit toisiinsa emuloimalla bridge domain -aluetta. Kaikki VPLS-palveluun liitetyt asiakkaan toimipisteet ovat näennäisesti samassa lähiverkkoalueessa. VPLS:stä käytetään myös termiä Transparent LAN Service (TLS).

VPLS on pseudowire-pohjainen Layer 2 -tason VPN-palvelu, joka perustuu MPLS-tekniikkan. VPLS-ratkaisut on määritelty RFC 4761 ja RFC 4762 standardeissa. VPLS-palvelut voivat olla paikallisia tai hajautettu useamman PE-laitteen välille.

Paikallisessa ratkaisussa kaikki asiakkaan toimipisteet on yhdistetty yhteen PE-laitteeseen. Vain yksi PE-laite osallistuu VPLS-palvelun luomiseen ja vain yksi VPLS-instanssi on määritelty. VPLS-palveluun on määritelty vähintään kaksi SAP (Service access point) -liitosta. Paikalliseen VPLS-palveluun ei kuulu pseudowire-tekniikkaa, joten asiakkaan liikenteeseen ei liitetä VPN- tai MPLS-enkapsulointimerkintää.

Hajautetussa VPLS-palvelussa asiakkaan toimipisteet ovat yhdistetty useammalla PE-laitteella. PE-laitteet yksilöidään ja assosioidaan tiettyyn VPLS-palveluun. Jokaisella palveluun osallistuvalla PE-laitteella on määriteltynä kyseinen VPLS-instanssi. Palvelu käsittää yhden tai useamman SAP- ja pseudowire-liitoksen, joiden avulla yhdistäminen muihin PE-laitteisiin tapahtuu. Hajautettu VPLS vaatii jaetun pseudowire -infrastruktuurin PE-laitteiden kesken. (Xu 2010, 463)

3.3.2 Ethernet Virtual Connection (EVC)

EVC on Cisco Systemsin operaattoreita varten kehittämä ohjelmistoarkkitehtuuri. Metro Ethernet Forum (MEF) -liiton termistössä EVC tarkoittaa virtuaalista ethernet yhteyttä (Virtual Ethernet Connection / Circuit), mutta tässä tapauksessa EVC edustaa Ciscon kehittämää ohjelmistoarkkitehtuuria kokonaisuutena. EVC-tekniikassa on monia etuja, kuten kyky tukea useita erilaisia palveluilta liityntäporttia kohden. Yhtä fyysistä liityntäporttia kohden voi käyttää kaikkia seuraavia palveluita sekoitettuna keskenään:

- 802.1q trunk (runkolinja)
- 802.1q tunnel (runkolinjatunnelointi)
- Local connect (paikallinen siltaus)
- Scalable EoMPLS (EoMPLS xconnect)
- Multipoint Bridging (Layer 2 -tason siltaus)
- Multipoint Bridging (VPLS, SVI-pohjainen EoMPLS)
- L3 termination (Layer 3 -tason päättäminen

EVC-arkkitehtuuri toimii luomalla Service Instance -palvelu, joka liitetään fyysiseen liityntäporttiin. Service Instance hyväksyy tai hylkää sisälle tulevan liikenteen VLAN-merkintöjen perusteella. Sisälle tulevaa liikennettä voidaan manipuloida monipuoli-

sesti, mutta oletusarvoisesti Service Instance ei tee liikenteelle mitään, kunnes toisin määritellään. Esimerkkejä tavasta manipuloida sisälle tulevaa liikennettä, on VLAN-merkintöjen poisto, muokkaus ja lisäys. Service Instance voidaan myös päättää VPLS-palveluun hyödyntämällä Bridge Domain -alueita. (Chatzithomaoglou 2009.)

3.4 iSCSI-protokolla

Internet Small Computer System Interface (iSCS) on yleinen standardi, jota käytetään liittämään IP-pohjaisia tiedon tallennuslaitteita erilaisiin järjestelmiin. iSCSI mahdollistaa tiedon siirtämisen kuljettamalla SCSI-komentoja IP-verkon yli, joka useimmissa tapauksissa on yrityksen sisäinen tietoverkko. Vaikka iSCSI-standardia hyödynnetään pääsääntöisesti lähiverkoissa, skaalaa se myös alueverkkoihin tai jopa pitkän matkan siirtoihin hyödyntämällä erilaisia tunnelointitekniikoita. (Ferguson 2012, 164.)

3.5 MAC Pinning Port Channel

Port channel -kanava on usean fyysisen liityntäportin muodostama looginen liityntäportti. Kaistan ja vikasietoisuuden kasvattamiseksi on mahdollista muodostaa enintään kahdeksan aktiivista linkkiä käsittävän port channel -kanavan. Kuorma jaetaan port channel -kanavan muodostamiseen osallistuvien fyysisten liityntäporttien kesken. Port channel -kanava säilyttää toimintakykynsä niin kauan, kun yksikin fyysinen liityntäportti on toiminnassa. Nexus 1000V -virtuaalikytkin on kykenevä muodostamaan kahdenlaisia port channel -kanavia.

- Perinteinen port channel -kanava, joka konfiguroidaan Nexus 1000V -virtuaalikytkimeen, sekä upstream-kytkimeen.
- Port channel -kanava, joka konfiguroidaan vain Nexus 1000V -virtuaalikytkimeen.
  (Cisco Systems 2012, 5-1.)

MAC pinning port channel -kanava on suositeltava vaihtoehto tilanteessa, jossa upstream-kytkimet eivät tue port channel -kanavia. MAC pinning -menetelmä jakaa palvelimien liityntäportit yksittäisiksi linkeiksi ja kiinnittää (pins) MAC-osoitteet näille linkeille round-robin-menetelmällä. Tämä varmistaa, ettei virtuaalikoneen MAC-osoitetta näy useammassa, kuin yhdessä upstream-kytkimessä kerralla. Upstream-kytkimiä ei tarvitse konfiguroida VEM-moduulin liittämistä varten. MAC pinning ei

luota mihinkään protokollaan upstream-kytkimien tunnistamiseksi, joten konfiguraatio on riippumaton laitteesta ja valmistajasta. Vian ilmetessä Nexus 1000V -virtuaalikytkin lähettää ARP-paketteja upstream-kytkimelle, ilmoittaakseen VEM-moduulin MAC-osoitteen vaihtavan linkkiä. Menetelmä mahdollistaa vikaantuneen linkin vaihtamisen toimivaan alle sekunnissa. (Cisco Systems 2012, 5-4.)

4 SIMUNET

SimuNet on EAKR-hanke, joka on syntynyt Kymenlaakson ammattikorkeakoulun ja Kaakkois-Suomen verkko- ja palveluoperaattoreiden yhteistyöstä (Kettunen 2009, 1). Hanke käynnistettiin vuonna 2009 ja seurauksena Kymenlaakson ammattikorkeakoulun tiloihin on rakennettu palveluntarjoajan verkkoa muistuttava SimuNet-verkko. Tämän työ hyödyntää kyseistä verkkoa teknisen toteutuksen alustana.

4.1 Yleistä

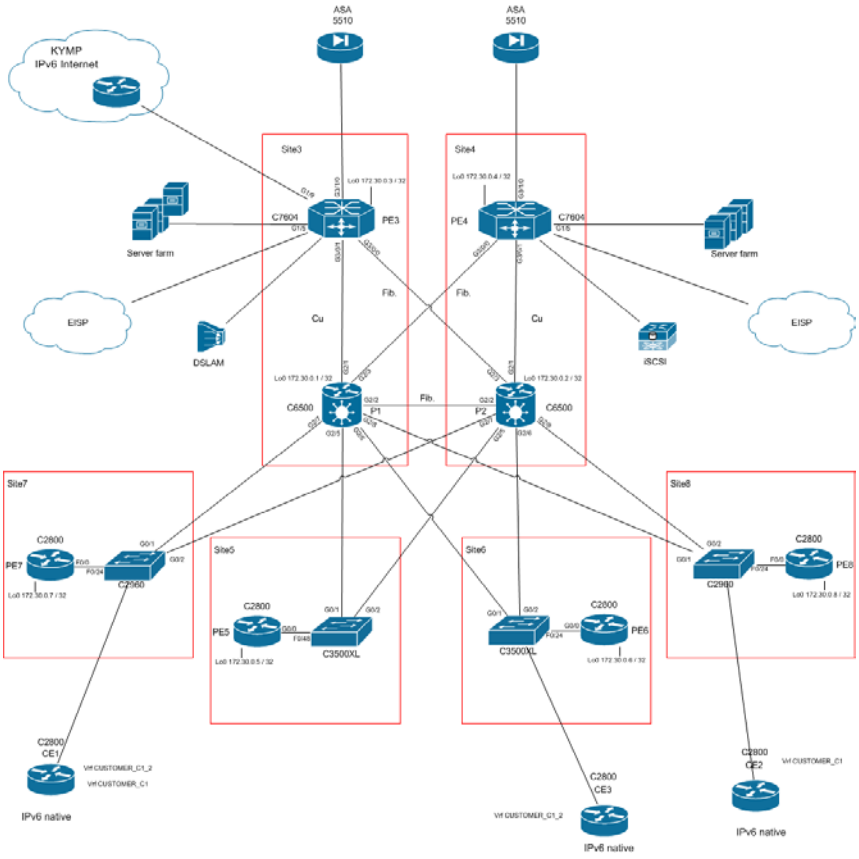
SimuNet on testausalusta, joka simuloi modernin palveluntarjoajan konesalin ratkaisuja. Ympäristö tarjoaa uusia mahdollisuuksia opiskelijoille ja hankkeessa mukana oleville yrityksille. On olemassa paljon asioita, joita verkko-operaattorit haluaisivat simuloida ja harjoitella ennen muutoksien suorittamista omassa tuotantoverkossa. SimuNet-ympäristössä voidaan suorittaa myös opiskelijoiden omia projekteja simuloidussa operaattoriverkossa ilman kriittisten palveluiden vaarantamista. Eniten SimuNet-verkkoa on käytetty juuri opiskelijoiden opinnäytetöissä, sekä erinäisissä projekteissa (Oinonen 2011, 21).

4.2 Topologia

SimuNet oli aluksi Kymenlaakson ammattikorkeakoulun verkoista eristetty ympäristö hallintayhteyksiä lukuun ottamatta. Tähän tuli muutos keväällä 2011, kun SimuNet valjastettiin tuottamaan ipv6-palveluita ICT-laboratorion verkkoon. Kaikki yhteydet kulkevat oletusarvoisesti ipv6-liikenteenä SimuNetin lävitse. Vian ilmetessä liikenne vaihtuu takaisin vanhaksi ipv4-liikenteeksi, joka kulkee ICT-laboratorion oman verkon kautta.

Työn kannalta olennaista on SimuNetin runko, reuna ja niiden toimintaperiaate. Verkko koostuu useasta simuloidusta laitetilasta, joiden välillä on kuvitteellinen maantie-

teellinen etäisyys. SimuNet-verkon runkolinjat ovat toteutettu suurimmaksi osaksi kuitulinkeillä ja muuten toteutuksessa on käytetty kuparilinjoja.



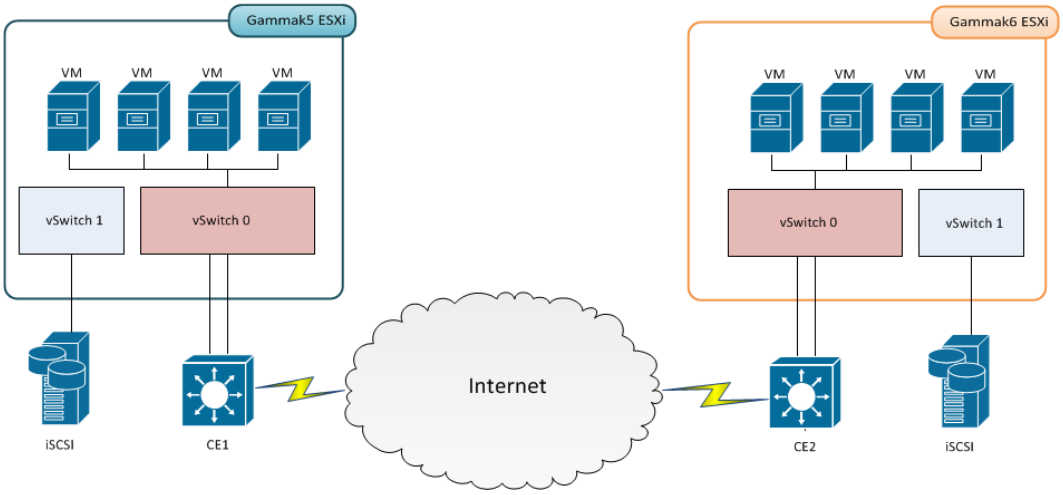
Kuva 1. SimuNetin fyysinen kytkentä (Tuntematon 2012). Kuva mukana isompana liitteenä

5 SUUNNITELMA

Opinnäytetyössä kuvitellaan tilanne, jossa asiakkaalla on omia virtualisoituja palvelimia. Asiakkaalla on myös kaksi toimipistettä, jotka ovat erillään toisista. Asiakas haluaa ostaa palveluntarjoajalta palvelun, joka vapauttaisi asiakkaan verkon hallinnoimisesta ja yhdistäisi kaksi toimipistettä toisiinsa. Virtualisoitujen palvelimien ongelmana on tarve tietynasteiselle verkko-osaamiselle. Palveluntarjoajalla on seuraavia vaihtoehtoja käytettävissä. Toimipisteiden yhdistämiseksi voidaan hyödyntää palveluntarjoajan MPLS-pilveä ja sen avulla toimivaa L2VPN-tekniikkaa. Tämä mahdollistaisi asiakkaan virtuaalisten palvelimien klusteroinnin, jota Layer 3 -tason ratkaisu ei sallisi. Virtualisoitujen palvelimien verkkojen hallitsemiseksi palveluntarjoaja voi hyödyntää Nexus 1000V -sarjan ratkaisua. Tämäkin tekniikka mahdollistaa porttiprofiileiden syöttämistä asiakkaan palvelimille, eikä asiakkaan tarvitse tehdä muuta, kuin ilmoittaa

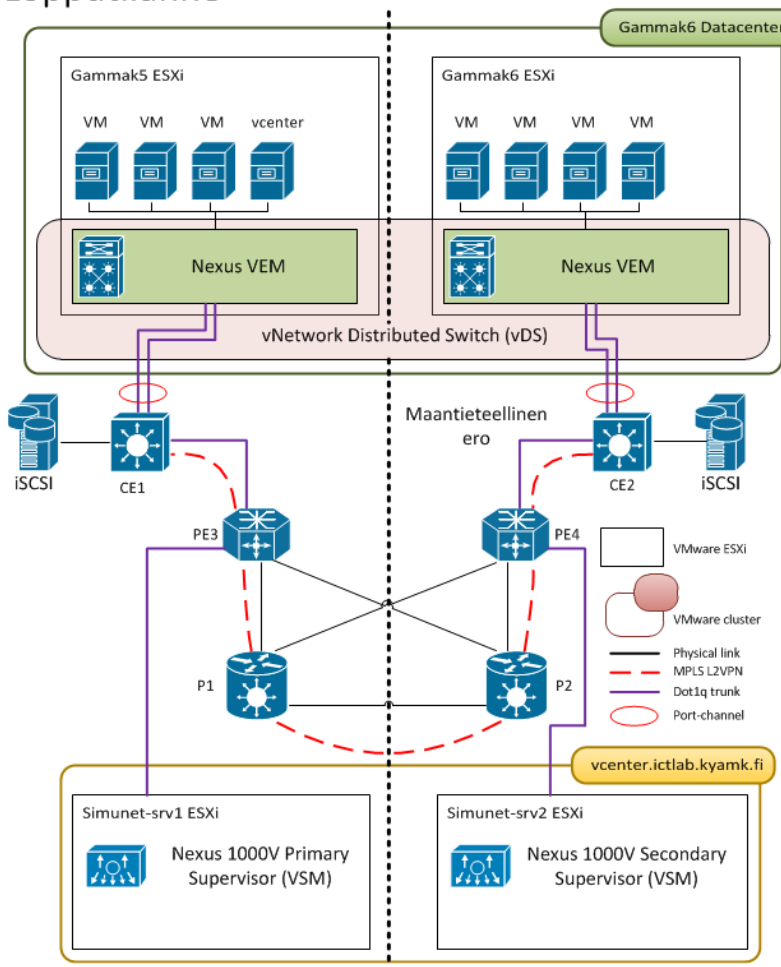
tarpeensa palveluntarjoajalle. Tämän pohjalta laadittiin kaaviot nykytilanteesta ja toivotusta lopputuloksesta.

Lähtötilanne



Kuva 2. Asiakasverkon lähtötilanne. Kuva mukana isompana liitteenä

Lopputilanne



Kuva 3. Asiakkaan verkko muutosten jälkeen. Kuva mukana isompana liitteenä

Lopputilannetta esittävä kuva osoittaa osittain fyysistä ja osittain loogista kytkentää. Kuvasta näkyy, miten L2VPN-tunneli kiertää SimuNet-verkon MPLS-pilven runkolaitteiden läpi ja asiakkaan reunalla päättyy runkolinjaporttiin. Asiakkaan VMware-ympäristö on klusteroitu ja iSCSI-palvelimet on siirretty suorasta yhteydestä kytkimen puolelle, jotta klusteri voi paremmin hyödyntää tallennustilat. Kuva osoittaa myös, miten VMwaren yksinkertaiset vSwitch-kytkimet on vaihettu Ciscon VEM-moduuleihin ja niiden muodostamaan loogiseen vDS-virtuaalikytkimeen (Nexus 1000V). Palveluntarjoajan päädyssä VSM-moduulit sijaitsevat palveluntarjoajan VMware-klusterissa.

6 TEKNINEN TOTEUTUS

Opinnäytetyön tekninen osuus suoritetaan Kymenlaakson ammattikorkeakoulun ICT-laboratorion ja SimuNet-hankkeen tiloissa. Teknisessä toteutuksessa käydään läpi kaikki merkittävät vaiheet, jotka Nexus 1000V -virtuaalikytkimen käyttöönotto vaatii. Tähän sisältyy asiakkaan VMware-ympäristön konfigurointi ja muutostyöt, SimuNet-verkon reunalle tehtävät konfiguraatiot ja Nexus 1000V -virtuaalikytkimen asennus ja konfigurointi. Teknisen toteutuksen järjestyskriittisyyden vuoksi työvaiheet käydään läpi järjestyksessä, jossa ne alun perin toteutettiin. Kappaleet saattavat käsitellä teoria-asioita, joita teoriaosuudessa ei esitelty.

6.1 Verkon konfigurointi

Työn sijoittaminen SimuNet-ympäristöön vaatii olemassa olevan verkon hyödyntämistä muutamin muutoksin. Liite 1. esittää SimuNetin fyysistä kytkentää ja kuvasta selviää eri laitetilojen kytkentäpisteet ja niiden suhteet toisiinsa nähden. Alun perin työn oli tarkoitus sijoittua internetreunan ja asiakasreunan (PE-laite 3 ja PE-laite 5) päihin, mutta laitteiston rajoitteiden vuoksi suunnitelmaa jouduttiin muuttamaan. Lopullisessa suunnitelmassa kuvitteellisen asiakkaan verkot sijaitsevat internetreunojen päädyissä (PE3 ja PE4). Näiden reunojen väliin haluttiin muodostaa Layer 2 -tasolla toimiva virtuaalinen tunneli, jotta asiakas näkisi verkkonsa yhtenä isona kokonaisuutena. Layer 2 -taso on myös Nexus-kytkimen kannalta otollinen tapa yhdistää maantieteellisesti erotetut verkot toisiinsa. Tunneli rakennettiin käyttäen EVC-portteja ja skaalattavaa EoMPLS-tekniikkaa.

6.1.1 EVC L2VPN

PE-laitteet ovat jo toimivan MPLS-konfiguraation seurauksena tietoisia toisistaan. Laitteiden välille tarvitsee vain luoda Layer 2 -tasoinen VPN-tunneli. Tätä varten hyödynnetään PE-laitteiden SIP-400 -moduuleita, jotka tukevat EVC-tekniikkaa. Liityntäporttien alle konfiguroidaan service instance -palveluita, jotka ovat yksilöllisiä liityntäporttia kohden. Tällä menetelmällä palveluntarjoajan verkosta ei tuhlaannu resursseja asiakkaan verkkojen läpivientiin. Ilman service instance -palveluita palveluntarjoajan verkosta jouduttaisiin osoittamaan resursseja, kuten VLAN-verkkoja, asiakkaan verkkojen kuljettamiseen. Service instance -palveluiden sisälle konfiguroidaan yksinkertainen skaalattava EoMPLS (Ethernet over MPLS), joka kytkee service instance -palvelun MPLS-verkon ylitse. PE-laitteisiin konfiguroidaan seuraavat komennot:

PE3(conf)#interface GigabitEthernet3/0/3
PE3(conf-if)#service instance 140 ethernet
PE3(conf-if-srv)#encapsulation dot1q 69
PE3(conf-if-srv)#xconnect 172.30.0.4 140 encapsulation mpls
PE3(conf-if-srv)#service instance 141 ethernet
PE3(conf-if-srv)#encapsulation dot1q 150
PE3(conf-if-srv)#xconnect 172.30.0.4 141 encapsulation mpls
PE3(conf-if-srv)#service instance 142 ethernet
PE3(conf-if-srv)#encapsulation dot1q 160
PE3(conf-if-srv)#xconnect 172.30.0.4 142 encapsulation mpls
PE3(conf-if-srv)#service instance 143 ethernet
PE3(conf-if-srv)#encapsulation dot1q 167
PE3(conf-if-srv)#xconnect 172.30.0.4 143 encapsulation mpls

PE4(conf)#interface GigabitEthernet3/0/3
PE4(conf-if)#service instance 140 ethernet
PE4(conf-if-srv)#encapsulation dot1q 69
PE4(conf-if-srv)#xconnect 172.30.0.3 140 encapsulation mpls
PE4(conf-if-srv)#service instance 141 ethernet
PE4(conf-if-srv)#encapsulation dot1q 150

PE4(conf-if-srv)#xconnect 172.30.0.3 141 encapsulation mpls

PE4(conf-if-srv)#service instance 142 ethernet

PE4(conf-if-srv)#encapsulation dot1q 160

PE4(conf-if-srv)#xconnect 172.30.0.3 142 encapsulation mpls

PE4(conf-if-srv)#service instance 143 ethernet

PE4(conf-if-srv)#encapsulation dot1q 167

PE4(conf-if-srv)#xconnect 172.30.0.3 143 encapsulation mpls

Varmistetaan tunneleiden ylösnouseminen:

PE3#sh mpls l2transport vc

Local intf	*Local circuit*	*Dest address*	*VC ID*	*Status*
VFI FW_OUT_10	*VFI*	*172.30.0.4*	*10*	*UP*
VFI FW_OUT_20	*VFI*	*172.30.0.4*	*20*	*UP*
VFI INTERNET_C1	*\ VFI*	*172.30.0.4*	*81*	*UP*
Vl100	*Eth VLAN 100*	*172.30.0.4*	*100*	*UP*
Vl101	*Eth VLAN 101*	*172.30.0.4*	*101*	*UP*
VFI NAGIOS	*VFI*	*172.30.0.4*	*120*	*UP*
Gi3/0/3	*Eth VLAN 69*	*172.30.0.4*	*140*	*UP*
Gi3/0/3	*Eth VLAN 150*	*172.30.0.4*	*141*	*UP*
Gi3/0/3	*Eth VLAN 160*	*172.30.0.4*	*142*	*UP*
Gi3/0/3	*Eth VLAN 167*	*172.30.0.4*	*143*	*UP*

Alleviivatut kohdat osoittavat kaikkien neljän tunnelin onnistuneen muodostamisen.

6.1.2 CE-kytkimet

Asiakkaan tiloissa toimivat CE (Customer Edge) -kytkimet, joiden avulla asiakas liittyy operaattoriverkon reunaan. Operaattorin verkossa (SimuNet) tehdyt asetukset ovat täysin läpinäkyviä asiakkaalle, joten asiakkaan päädyssä konfiguraatio on yhtä yksinkertainen, kuin liittäisi kaksi tavallista kytkintä toisiinsa runkolinjan avulla. CE-kytkimiin tehtiin seuraava konfiguraatio:

switch(config)#interface GigabitEthernet0/9

switch(config-if)#switchport trunk encapsulation dot1q

switch(config-if)#switchport trunk allowed vlan 1,69,150,160,170

switch(config-if)#switchport mode trunk

switch(config-if)#interface GigabitEthernet0/10

```
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport trunk allowed vlan 1,69,150,160,170
switch(config-if)#switchport mode trunk
switch(config)#interface GigabitEthernet0/11
switch(config-if)#switchport access vlan 150
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport trunk allowed vlan 1,69,150,160,170
switch(config-if)#switchport mode trunk
switch(config)#interface GigabitEthernet0/12
switch(config-if)#switchport access vlan 150
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport trunk allowed vlan 1,69,150,160,170
switch(config-if)#switchport mode trunk
switch(config)#interface GigabitEthernet0/13
switch(config-if)#switchport access vlan 160
switch(config-if)#switchport mode access
switch(config)#interface GigabitEthernet0/14
switch(config-if)#switchport access vlan 160
switch(config-if)#switchport mode access
switch(config)#interface GigabitEthernet0/15
switch(config-if)#switchport access vlan 160
switch(config-if)#switchport mode access
```

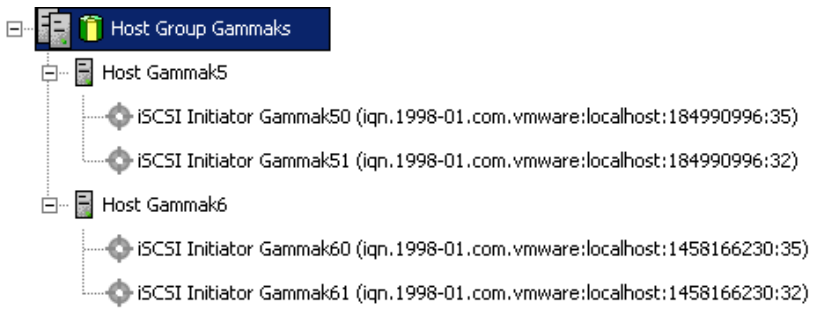
Yliviivattu osuus on olennainen operaattorin verkkoon liittymistä varten. Loput konfiguraatiot ovat esivalmistelua Nexus 1000V:n liittämistä varten. Tässä vaiheessa todennettiin tunnelin toiminta luomalla jokaiselle vlan-alueelle, kumpaankin kytkimeen oma virtuaalinen liityntäportti ja sille ip-osoite. Liityntäporteilla suoritettiin ping-komentoja tunnelin läpi. Koska ping-komennot toimivat moitteettomasti, voitiin tunnelit todeta toimiviksi.

6.2 Asiakkaan iSCSI konfiguraatio

VMwaren vikasietoinen klusteri on tarkka redundanttisuuden vaatimuksista. Jokaista klusteria kohtaan on oltava vähintään kaksi jaettua datastore-sijaintia. Oikeassa tilanteessa tämä tarkoittaisi kahta erillistä tallennuslaitetta. Nämä kaksi erillistä tallennus-

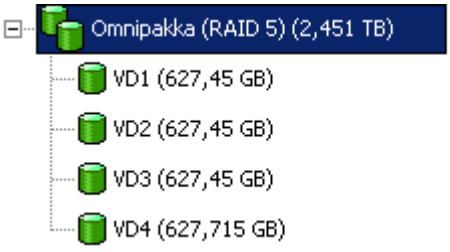
laitetta peilaisivat toisiaan ja toisen vikaantuessa, olisi toinen laitteista vielä käyttökelpoinen. Resurssien puutteen vuoksi tämä vaatimus voidaan kiertää ja tilanne on toteutettavissa yhdellä laitteella. Laitteelle määritellään ensin yksi iso RAID5 (redundant array of independent disks) -tila, joka pilkotaan kahdeksi virtuaalilevyksi. Jokaisella virtuaalilevyllä on oma LUN (logical unit number) -tunnus, joten palvelimen järjestelmä kuvittelee käsittelevänsä kahta erillistä fyysistä levyä. Kyseinen konfiguraatio ei kuitenkaan tarjoa todellista redundanttisuuta, joten sen soveltamista oikeaan tuotantoympäristöön ei suositella.

iSCSI-laitteen on ensimmäiseksi tunnistettava palvelimet, jotka aikovat sitä käyttää. Palvelimien tunnistaminen tapahtuu iSCSI initiator -nimen perusteella. Palvelimien nimet ovat seuraavat:



Kuva 4. iSCSI initiator -nimet

Palvelimia varten on osoitettava virtuaalilevyt. Tämä tapahtuu host-to-virtual disk -kartoituksen avulla. Kummallekin palvelimelle on osoitettava samat virtuaalilevyt, muuten klusterin muodostamisen aikana ilmenee ongelmia oikeuksien kanssa. Molemmat palvelimet on osoitettu ryhmään, joten helpointa on osoittaa virtuaaliset levyt myös kyseiselle ryhmälle.



Kuva 5. Virtuaalilevyjen allokointi

Virtual Disk Name	Accessible By	LUN
Access	Host Group Gammaks	31
VD1	Host Group Gammaks	0
VD2	Host Group Gammaks	1
Access	Storage Array	31

Kuva 6. Host-to-virtual disk kartoitus

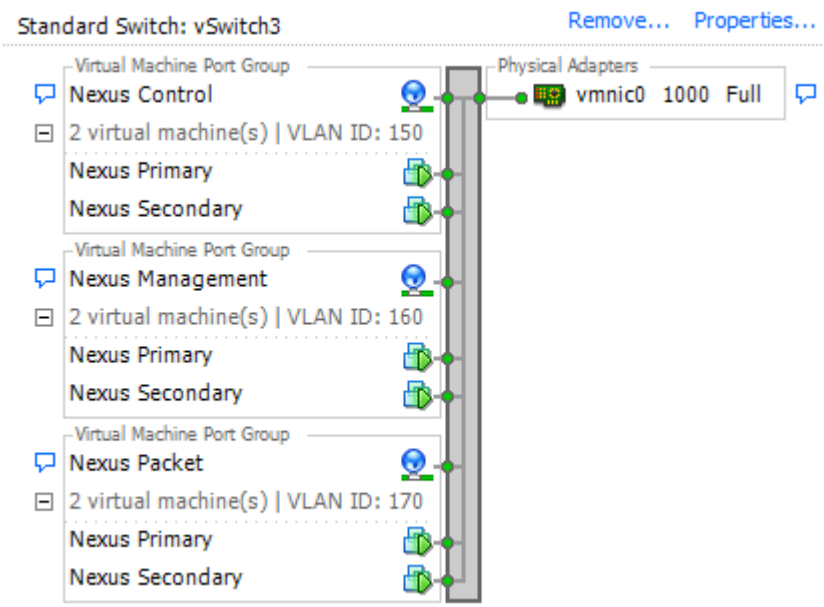
Viimeisenä suoritetaan verkon konfigurointi iSCSI-kohteille. iSCSI-laite alun perin käytti hallintaverkkona ip-osoiteavaruutta 192.168.128.0/24, joten iSCSI-kohteet päätettiin sijoittaa samaan osoiteavaruuteen. Laitteen ip-osoitteet ovat seuraavanlaiset:

- Hallinta - 192.168.128.101
- iSCSI Target 0 - 192.168.128.201

Toimenpiteiden jälkeen iSCSI-laite on valmis ottamaan vastaan yhteyksiä palvelimilta.

6.3 SimuNet vSwitch konfigurointi

Asiakkaan verkko ja ESXi-palvelimet ovat jo tietoisia kaikista tarpeellisista verkkoon liittyvistä asioista, mutta SimuNetin palvelinklusteri ei ole vielä konfiguroitu ottamaan yhteyksiä vastaan. SimuNetin vSwitch-kytkimet on ehdottomasti konfiguroitava ennen Nexus 1000V:n asentamisen aloittamista. SimuNetin ESXi-palvelimissa oli kummassakin yksi vapaa verkkokortti, jotka valjastettiin pelkästään Nexus 1000V:n yhteyksiä varten. SimuNetin vSwitch konfiguraatio näyttää valmiina tältä. Kuva 12 on myös otettu migraation jälkeen, joten Nexus 1000V:n ensisijainen ja toissijainen VSM-moduuli on näkyvissä.



Kuva 7. SimuNet Nexus 1000V vSwitch-kytkin

6.4 Virtual supervisor module (VSM)

Cisco Nexus 1000V sarjan Virtual Supervisor Module (VSM) -moduuli hallitsee useampaa VEM -moduulia yhtenä loogisena ja modulaarisena kytkimenä. Perinteisten linjakorttimoduulien sijasta VSM-moduuli tukee useita ohjelmistopohjaisia VEM-moduuleja fyysisten ESXi-palvelimien sisällä. Konfiguroiminen tapahtuu VSM-moduulin välityksellä ja tehdyt konfiguraatiot siirtyvät automaattisesti VEM-moduuleille. Ohjelmistopohjaisten vSwitch-kytkimen asetusten muuttamisen sijasta verkon ylläpitäjä voi tehdä muutoksia kaikkiin VEM-moduuleihin käyttäen hyväksi VSM-moduulin tarjoamaa keskitettyä konfigurointipistettä. (Corbin, Fuller & Jansen 2011, 378.)

VSM- ja VEM-moduulin väliseen kommunikointiin käytetään kahta tarkoin määriteltyä VLAN-verkkoa. VLAN-verkkojen on oltava Layer 2 -tasoisia ja niiden on sijaittava VSM- ja VEM-moduuleiden välissä. Nämä kaksi VLAN-verkkoa ovat Nexuksen Control ja Packet VLAN-verkot. Control-verkkoa käytetään:

- VSM- ja VEM-moduulien pitkien matkojen yhteydenpitoon samalla tavalla, kuin Nexus 7000 ja Catalyst 6500 malleissa.
- Kuljettamaan alhaisen tason viestejä VEM-moduulille varmistaen konfiguraation eheyden.

- Ylläpitämään kahden sekunnin sykettä VSM-moduulilta VEM-moduulille. (6 sekunnin aikakatkaisu)
- Ylläpitämään ensisijaisen ja toissijaisen VSM-moduulin välistä synkronointia.

Packet-verkkoa käytetään verkkopakettien kuljettamista VEM-moduulilta VSM-moduulille, kuten Cisco Discovery Protocol (CDP) ja Interior Gateway Management Protocol (IGMP). (Corbin, Fuller & Jansen 2011, 378.)

Alun perin Cisco suositteli VSM- ja VEM-moduulin välille Layer 2 -tasoa jokaista VLAN-verkkoa varten, mutta Nexus 1000V version 4.2(1)SV1(5.2) yhteydessä on alettu suosittelemaan Layer 3 -tasoa Control-verkolle. Tässä työssä kuitenkin käytettiin edelleen Layer 2 -tasoa vanhojen suositusten mukaan.

6.4.1 Asennus

Nexus 1000V VSM-moduuli on mahdollista asentaa usealla eri tavalla. Java-pohjainen asennusohjelma, manuaalinen asennus käyttäen Open Virtualization Appliance (OVA)- / Open Virtualization Format (OVF) -menetelmää tai manuaalinen asennus käyttäen levykuvaa (.iso). (Corbin, Fuller & Jansen 2011, 382.)

Helpoin tapa asentaa Nexus 1000V järjestelmä kokonaisuutena on käyttää java-pohjaista asennusohjelmaa. Tämä vaihtoehto ei kuitenkaan soveltunut tähän työhön, sillä asennusohjelma ei ymmärtänyt vaihtoehtoa, että hallittavat ESXi-palvelimet eivät sijaitse saman vCenterin alaisuudessa, mihin VSM-moduuli asennetaan.

Seuraavaksi helpoin vaihtoehto olisi käyttää OVA/OVF menetelmää, mutta tämäkään ei luonnistunut. Jostain syystä, OVA ja OVF tiedostot vaikuttivat korruptoituneilta, eivätkä suostuneet edes aloittamaan asennusprosessia. Asennustiedostojen uudelleen lataaminen ei auttanut asiaa, joten jäljelle jäi vain manuaalinen asennus levykuvaa käyttäen.

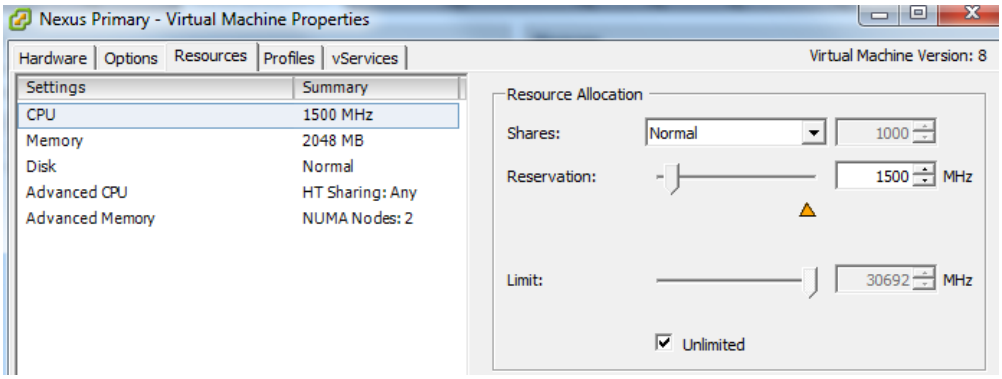
Levykuvaa käyttäessä on tärkeää luoda virtuaalikone, jolla on oikeat asetukset. Nexus 1000V on hyvin kriittinen omien resurssejansa saatavuudesta ja virtuaalikone voi alkaa käyttäytyä hyvin omituisesti, jos esimerkiksi muistia ei ole saatavilla oikeaa määrää. Siksi on äärimmäisen tärkeää painottaa virtuaalikoneen asetuksia laittaessa, että resurssit ovat taattuja. VSM-moduulin virtuaalikoneen vaatimukset ovat seuraavat:

- VM-tyyppi: Other 64-bit linux
- 1 Prosessori (taattu 1,5 Ghz)
- 2Gb Muistia (varattu ja taattu)
- 3 Verkkokorttia
- Minimi 3 GB SCSI kovalevytilaa
- LSILogic levyohjain

  (Corbin, Fuller & Jansen 2011, 382.)

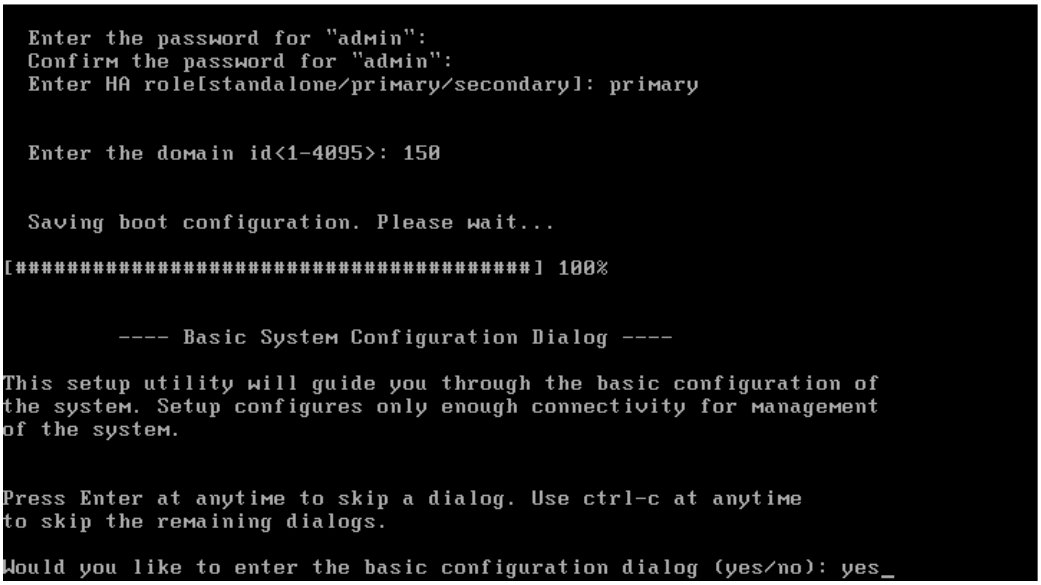
Avataan yhteys ICT-laboratorion vCenter-palvelimeen käyttäen vSphere Client -ohjelmaa ja aloitetaan uuden virtuaalikoneen luominen. Asennuksessa tehtiin seuraavat valinnat:

- Konfiguraatio: custom
- VM nimi: Nexus Primary
- Datastore: Sun iSCSI
- VM versio: Virtual Machine Version: 8
- Asiakasjärjestelmä: Other 64-bit Linux
- Suoritin: 1 virtual socket, 1 virtual core per socket
- Muisti: 2 Gb
- Verkko
  - NIC1 = Nexus Control, adapter E1000
  - NIC2 = Nexus Management, adapter E1000
  - NIC3 = Nexus Packet, adapter E1000
- SCSI ohjain: LSILogic parallel
- Kovalevy: Luo uusi levy
- Kovaley koko: 3Gb, Thin provision

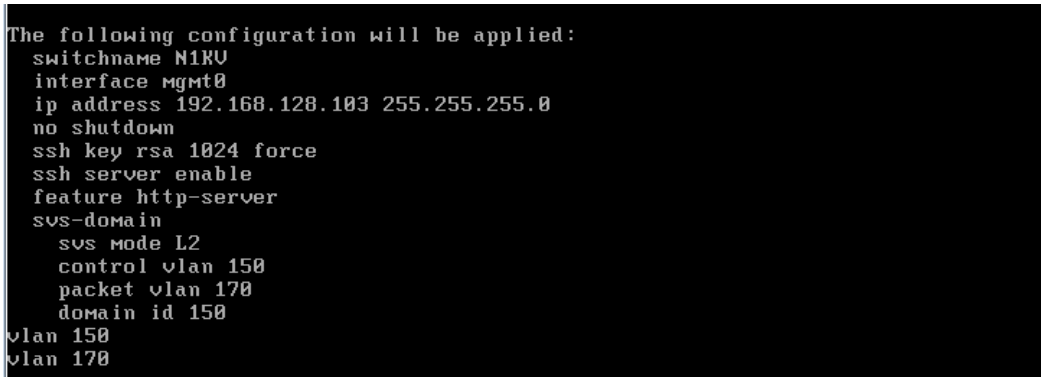


Kuva 8. VSM-moduulin resurssivaraukset

Virtuaalikoneen luomisen jälkeen oli vielä varattava muistia ja suoritinaikaa tarpeeksi vakaan toiminnan takaamiseksi. Tämän jälkeen virtuaalikone voitiin käynnistää ja yhdistää levykuva koneeseen. Avattiin konsoliyhteys virtuaalikoneeseen ja käynnistyessä valittiin käynnistysvalikosta asennusvaihtoehto ja aloitettiin asennus.



Kuva 9. Nexus 1000V setup script



Kuva 10. Konfiguraation lopputulos

Konfiguroinnin aikana Nexus 1000V kytkimelle määritetään useita asetuksia. Osa määrityksistä on samoja, kuin millä tahansa kytkimellä, esimerkiksi ”switchname”-komento, joka vastaa IOS (Internetwork Operating System) -komentoa ”hostname”. Tärkeimmät määritteet ovat kuitenkin domain-id, svs mode, control vlan ja packet vlan.

Domain id on Nexus-järjestelmälle tunnistetieto, jonka avulla VSM- ja VEM-moduulit voivat päätellä kenelle tieto kuuluu. VEM-moduulin saadessa komentoja VSM-moduulilta, joka ei jaa samaa domain id -numeroa, komennot jätetään suoritta-

matta. Tällä menetelmällä voidaan varmistaa komentojen vastaanotto ympäristössä, jossa toimii useampi VSM-moduuli.

Control- ja packet-VLAN tiedot yhdistävät VSM-moduulin oikeisiin vnic-verkkokortteihin ja samalla oikeisiin VLAN-verkkoihin, jotka määriteltiin aikaisemmin. SVS mode määrittelee verkkokerroksen, jonka avulla VSM- ja VEM-moduulit vaihtavat tietoja. Työssä käytetään vanhaa Layer 2 -tason suositusta, mutta myös Layer 3 -tasoa on mahdollista käyttää. Layer 3 -tasolla toimiessa jokaiselle ESXi-palvelimelle tulisi määrittää yksi ylimääräinen vmkernel-liityntä ja luoda sille tarkoitettu l3control-parametrillä varustettu vethernet-porttiprofiili. Layer 3 -tasolla toteutettu control-verkko on myös valmistajien mukaan helpompi diagnosoida ongelmatilanteen ilmetessä.

Ensisijaisen VSM-moduulin asentamisen jälkeen on asennettava toissijainen VSM-moduuli. Asennus toteutetaan vastaavasti, kuin ensisijaisen VSM-moduulin, mutta roolin valintakohdassa valitaan primary-vaihtoehdon sijasta secondary. Samalla Layer 2 -tasolla sijaitsevat VSM-moduulit synkronoituvat keskenään automaattisesti.

6.5 Virtual ethernet module (VEM)

Cisco Nexus 1000V Virtual Ethernet Module (VEM) suoriutuu osana Vmware ESX tai ESXi:n ydintä (kernel). VEM-moduuli hyödyntää VMwaren vNetwork Distributed Switch (vDS) -kytkimen ohjelmointirajapintaa (API). Ohjelmointirajapinta tarjoaa edistyksellisiä ominaisuuksia virtuaalikoneille ja sallii VEM -moduulin integroitumisen VMwaren vMotion- ja Distributed Resource Scheduler (DRS) -tekniikan kanssa. VEM-moduuli saa konfiguraatiotiedot Virtual Supervisor Module (VSM) -moduulilta ja niiden perusteella suorittaa Layer 2 -tason kytkemistä ja muita verkotustekniikoita, kuten:

- Port channel
- Quality of service (QoS)
- Tietoturvaominaisuuksia, kuten Private VLAN ja pääsylistat
- Monitorointi, kuten NetFlow, Switch Port Analyzer (SPAN) ja Encapsulated Remote SPAN (ERSPAN) (Corbin, Fuller & Jansen 2010, 376.)

6.5.1 Asennus

VEM-moduuli on mahdollista asentaa usealla eri tavalla. Käyttäjäystävällisin tapa on hyödyntää VMware Update Manager -ohjelmistoa, mutta näin pienessä toteutuksessa helpointa oli asentaa VEM-moduulit manuaalisesti SSH (Secure Shell) -protokollan välityksellä. Oikean asennustiedoston valitseminen tapahtuu Ciscon kotisivuilta löytyvän tuotematriisin avulla.

Palvelimien versio on ESXi 5.0.0, alaversio 623860, jonka perusteella oikea asennustiedosto on cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.1.vib. Tiedostot siirrettiin käyttäen WinSCP ohjelmistoa ja ne sijoitettiin /tmp hakemistoon (ESXi käyttää Linux-pohjaista käyttöjärjestelmää). Varsinaista asentamista varten otettiin uusi SSH-yhteys PuTTy-ohjelmiston avulla ja suoritettiin seuraavanlainen komento:

```
~ # esxcli software vib install -v /tmp/cross_cisco-vem-v140-
4.2.1.1.5.2.0-3.0.1.vib

    Installation Result
           Message: Operation finished successfully.
           Reboot Required: false
           VIBs Installed: Cisco_bootbank_cisco-vem-v140-
           esx_4.2.1.1.5.2.0-3.0.1
           VIBs Removed:
           VIBs Skipped:
```

Moduulin toimivuus varmistettiin seuraavalla komennolla:

```
~ # vem status -v

Package vssnet-esxmn-ga-release
Version 4.2.1.1.5.2.0-3.0.1
Build 1
Date Mon Oct 18 12:38:49 PST 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name    Num Ports   Used Ports  Configured Ports MTU  ….
```

```
vSwitch0        128         3           128               1500 …
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Toimenpide suoritettiin kummallekin palvelimelle. Yliviivattu rivi osoittaa VEM-moduulin toimivan.

6.6 VMware vCenter

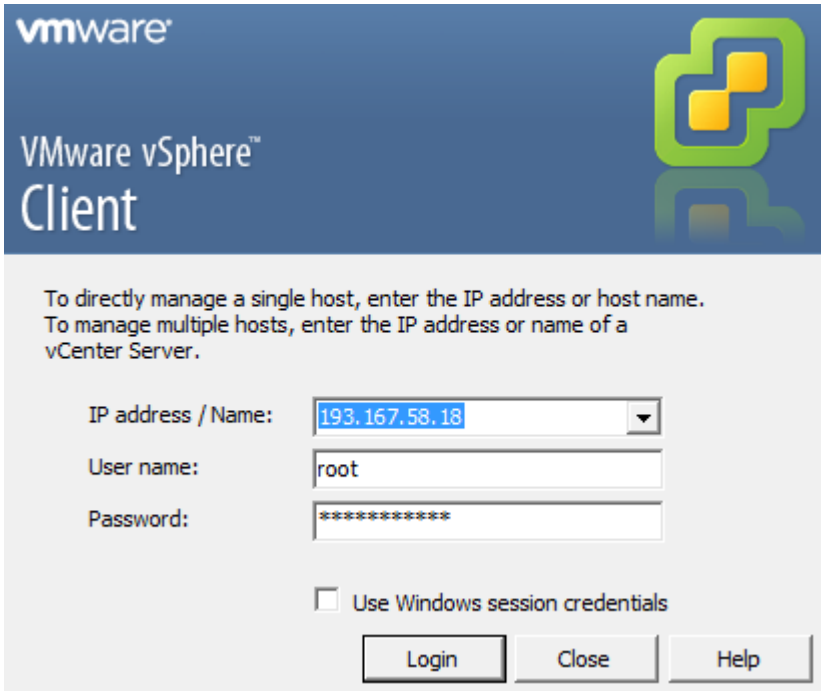
vCenter-palvelimesta tulee asiakkaan vSphere ympäristön keskitetty komento-, hallinta- ja kommunikaatiokeskus. Organisaatioiden tarpeiden vaihdellessa suuresti VMware tarjoaa useita eri vaihtoehtoja ohjelmistosta. Jokainen vaihtoehto ohjelmistosta tarjoaa erilaisen kokoonpanon työkaluja, joilla hallita virtuaalikoneita (VM) ja palvelimia (ESXi). (Ferguson 2012, 6.)

Työn kannalta vSphere-ympäristön varustelutaso on olennainen, koska Nexus 1000V vaatii toimiakseen tuen vNetwork Distributed Switch (vDS) -virtuaalikytkimelle. Ominaisuus on saatavilla vain VMware Enterprise Plus -varustelutasossa. Lisenssin puuttumisen vuoksi vSphere asennetaan kokonaisuutena kokeilulisensseillä. Lisenssit toimivat oletusarvoisesti korkeimmalla varustelutasolla ja takaavat tarvittavan ominaisuuden saatavuuden.

6.6.1 Asennus

vCenter on mahdollista asentaa virtuaalikoneena tai fyysiselle palvelimelle. Resurssien rajoittaman työssä käsitellään vCenteriä virtuaalikoneena. Asentaminen vaatii käyttöjärjestelmän, joka voi olla Windows 2008 R2 tai WMwaren oma vCenter appliance-järjestelmä, joka on rakennettu SUSE Linuxin varaan. Tuotannossa pienien yrityksien on hyvä turvautua vCenter appliance -ohjelmistoon, joka ei tuota lisäkustannuksia. Windows 2008 R2 vaatii oman lisenssin, joka tuo lisäkustannuksia järjestelmän pystyttämiseen. Työssä käytetään Windows 2008 R2:sta, koska se on entuudestaan tuttu järjestelmä ja teknisen toteutuksen aikarajoitteiden vuoksi lisensointi ei ole ongelma.

Virtuaalikone päätettiin asentaa Gammak5 palvelimelle käyttäen hyväksi VMware vSphere client -ohjelmistoa. Sisään kirjautuminen tapahtuu antamalla palvelimen osoitteen ja käyttäjätunnuksen.



Kuva 11. Gammak5 palvelimen sisään kirjautuminen

Palvelimelta valittiin toiminto ”luo uusi virtuaalikone” ja suoritettiin ohjattu asennustoiminto. Virtuaalikoneen onnistumisen luomisen jälkeen virtuaalikoneeseen asennettiin Windows 2008 R2, jonka asentamista ei käsitellä tarkemmin sen jäädessä työn rajauksen ulkopuolelle.

Windows 2008 R2 asentamisen jälkeen asennetaan varsinainen vCenter-ohjelmisto. VMware mahdollistaa kokeiluversion lataamisen ilmaiseksi rekisteröitymistä vastaan. Ohjelma on ladattavissa useassa eri muodossa ja tässä työssä käytettiin .iso formaattista levykuvaa, joka purettiin käyttäen WinRAR -ohjelmistoa. Asennus oli suoraviivainen prosessi, joka noudatteli ohjattua asennusta ilman ylimääräisiä komentoja tai määritteitä.

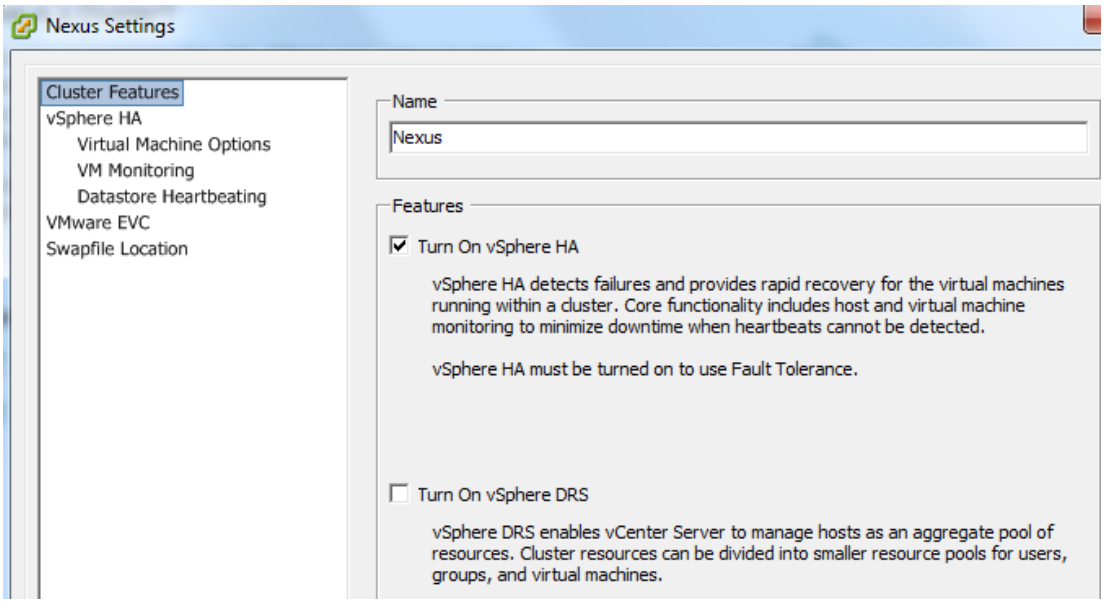
6.6.2 VMware-klusteri

Klusteri on ryhmä ESX- tai ESXi-palvelimia ja virtuaalikoneita. Kaikki fyysiset resurssit, kuten muisti ja laskentateho, ovat klusterin omaisuutta ja vCenter hallitsee tätä kokonaisuutta. (Bowling 2011.)

VMware kykenee käsittelemään kahdenlasia klustereita, DRS/HA (Distributed Resource Scheduler / High Availability) ja SDRS (Storage Distributed Resource Scheduler). DRS/HA klusteri on vastuussa palvelinten muistin ja laskentatehon hallinnoin-

nista ja SDRS on vastuussa tallennustilan hallinnasta. Kahta palvelinta ei tavallisesti tarvitse asettaa klusteriin, mutta vCenterin virtuaalisuuden vuoksi on hyvä varmistaa sen korkea saatavuus, joka saavutetaan konfiguroimalla palvelimet käyttämään HA-klusteria.

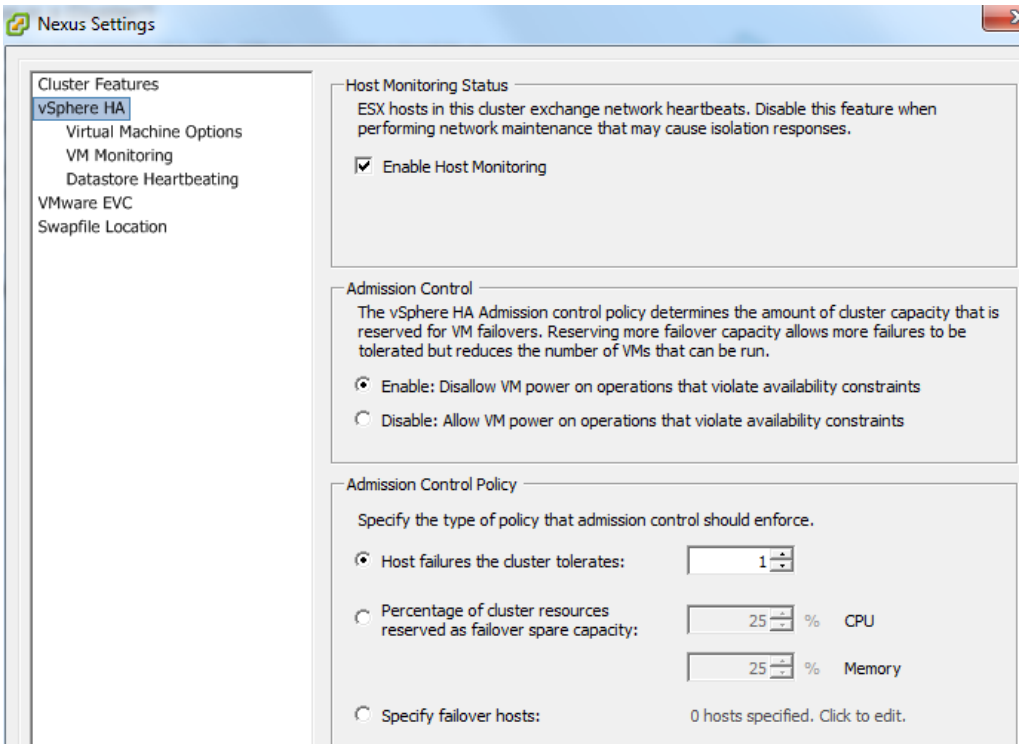
Ensimmäisenä palvelimet täytyi liittää vCenterin hallintaan. Tämä tapahtui luomalla uusi Datacenter -objekti, johon palvelimet liitettiin käyttäen New Host -toimintoa. Palvelimen tuomista vCenteriin varten täytyy tietää palvelimen ip-osoite ja root-tunnuksen salasana. Palvelimien tuomisen jälkeen oli mahdollista aloittaa klusterin luominen, joka tapahtuu valitsemalla Datacenter-objekti ja suorittamalla New Cluster -toiminto. Toiminnon aikana klusteri nimetään ja halutut tehtävät valitaan aktiivisiksi. Aikaisemmin mainittiin klusterin suorittavan vain korkean saatavuuden virkaa, joten se on ainoa toiminto, joka valitaan aktiiviseksi.



Kuva 12. Nexus klusterin ominaisuudet

Klusterin luomisen jälkeen palvelimet voi yksinkertaisesti maalata, vetää ja tiputtaa klusterin päälle. Toiminto lisää palvelimet automaattisesti klusterin jäseniksi. Jotta klusterista olisi jotain hyötyä, oli sille konfiguroitava määritteet, jonka perusteella klusteri toimii toisen palvelimen vikaantuessa. Klusteri määriteltiin kestämään yhden palvelimen vikaantumisen. Virtuaalikoneita ei siis voi olla päällä enempää, kuin mitä yksi palvelin jaksaa yksin suorittaa. Palvelimissa on identtiset suorittimet, mutta muistin määrät eroavat toisistaan. Virtuaalikoneiden maksimimäärä lasketaan siis hei-

koimman palvelimen mukaan. Tämän vuoksi VMware suosittelee, että klusterissa toimivat palvelimet olisivat laitteiston puolesta identtiset.



Kuva 13. Nexus klusterin vikatilanneasetukset

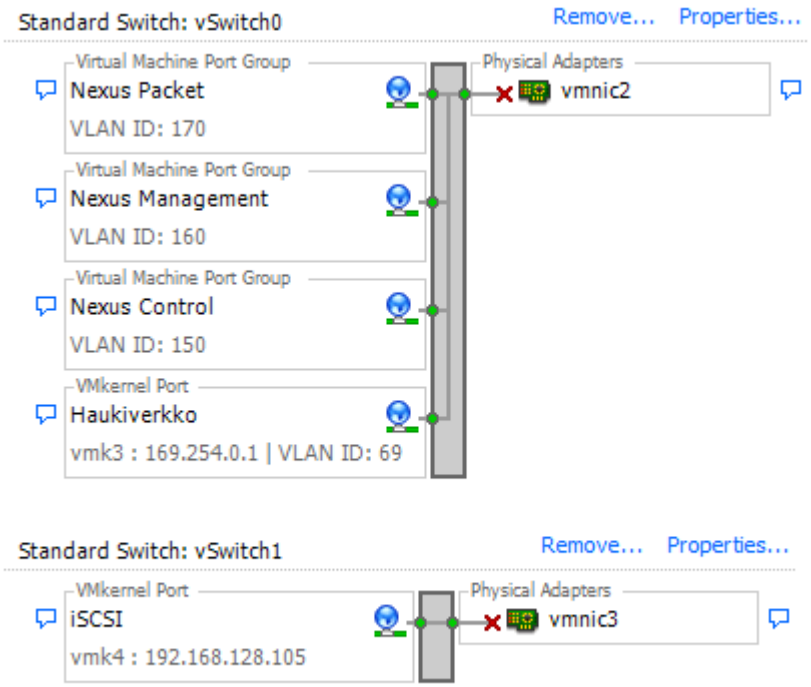
6.6.3 vSwitch konfigurointi

Virtuaalisten verkkojen rakentaminen ja suunnittelu vSphere ympäristössä sisältää paljon yhtäläisyyksiä oikeiden verkkojen rakentamisen ja suunnittelun kanssa, mutta eroavaisuuksiakin on myös paljon. ESXi palvelimien verkkoarkkitehtuuri keskittyy vSwitch -virtuaalikytkimien luomisen ja konfiguroimisen ympärille. Kyseisiä virtuaalikytkimiä on kahdenlaisia, on vSphere Standard Switch - tai vSphere Distributed Switch -kytkimiä. (Lowe 2011, 171-172.)

vSwitch on yksinkertaisin verkon komponentti, jota ESXi palvelin voi käyttää. Nämä virtuaalikytkimet tarjoavat vSphere ympäristölle perusominaisuuksia, kuten yhteydet virtuaalikoneiden, ESXi-palvelimien, fyysisten laitteiden ja VMKernel toimintojen välillä. Oli tilanne mikä tahansa, ESXi palvelimien verkkotoiminnot on aina ajettava alkuun näiden yksinkertaisen virtuaalikytkimien avulla. Alustavan verkonkonfiguroinnin jälkeen on mahdollista konfiguroida käyttöön edistyksellisempi vDS-virtuaalikytkin, tai kuten tässä työssä Nexus 1000V -pohjainen vDS-virtuaalikytkin.

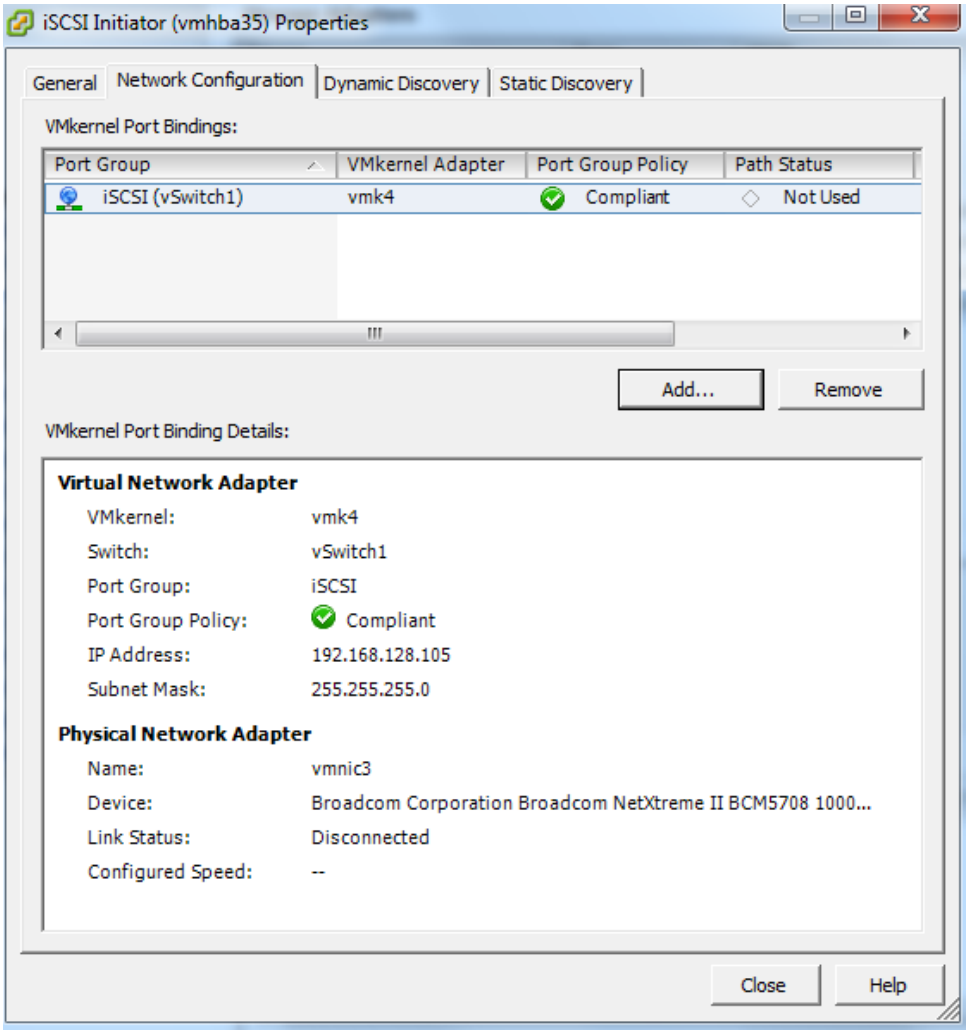
VMKernel luo ja hallitsee virtuaalikytkimiä, jotka ovat ESXi-palvelimien sisällä. Virtuaalikytkimet tai vSwitch-kytkimet eivät ole hallittuja kytkimiä, eivätkä ne tarjoa kaikkia edistyksellisiä ominaisuuksia, joita monet fyysiset kytkimet tarjoavat. Esimerkiksi vSwitch-kytkimeen ei voi ottaa telnet-yhteyttä ja konfiguroida sitä komentoriviltä, mukaan lukematta paria komentoa, jotka on mahdollista ajaa ESXi-palvelimen komentoriviltä. Silti vSwitch-kytkin toimii monella tavalla, kuten fyysinen kytkin. Fyysisen vastineen tavoin vSwitch-kytkin toimii Layer 2 -tasolla, säilyttää MAC-osoite taulukkoa, tukee VLAN-verkkoja, kykenee käsittelemään tagged liikennettä käyttäen 802.1q protokollaa ja pystyy luomaan port channel -väyliä. vSwitch-kytkin konfiguroidaan aina käyttämään tiettyä porttimäärää, kuten fyysiset kytkimetkin. Yhtäläisyyksistä huolimatta vSwitch-kytkimet eroavat fyysisistä vastineistaan merkittävästi. vSwitch-kytkin ei tuo dynaamisia neuvotteluprotokollia, kuten Dynamic Trunking Protocol (DTP) tai Port Aggregation Protocol (PAgP). Port channel -väylien tai 802.1q trunk -väylien konfigurointi täytyy tehdä manuaalisesti. vSwitch-kytkintä on mahdotonta kytkeä toiseen vSwitch-kytkimeen, joka poistaa täysin silmukoiden mahdollisuuden. Tämän vuoksi vSwitch kytkimellä ei ole mitään tarvetta käyttää Spanning Tree Protocol (STP) -protokollaa. Verkkojen silmukoituminen on todellinen ongelma, joten tämä on suuri etu vSwitch-kytkimelle. (Lowe 2011, 173.)

Asiakkaan ESXi-palvelimet tarvitsevat liitettävyyttä useaan eri verkkoon, joista yksinkertaisin on suora yhteys iSCSI-palvelimeen. Alussa tärkeintä oli pitää kytkentä mahdollisimman yksinkertaisena, jotta myöhemmin tehtävä migraatio vDS-kytkimeen olisi mahdollisimman helppo. Tämän vuoksi alussa käytettiin vain kahta verkkokorttia ja kahta vSwitch-kytkintä. Toinen vSwitch-kytkin on kaikkia VLAN-verkkoja varten ja toinen on yksinomaan omistettu iSCSI-liikenteelle. Kumpikin ESXi-palvelin konfiguroitiin identtisillä asetuksilla ja lopputulos oli seuraavanlainen.



Kuva 14. ESXi-palvelimien vSwitch-asetukset

Kuvan 9 mukainen asettelu ei varsinaisesti vaadi suurempaa asetusten muuttamista. Fyysinen verkkokortti vmnic2 muuttuu automaattisesti 802.1q trunk -väyläksi, kun sen käsiteltäväksi konfiguroidaan useampi VLAN-verkko. Ainoa muutos asetuksiin tehtiin iSCSI-yhteyksiä hallitsevaan vmk4 VMKernel-ytimeen, joka asetettiin käsittelemään iSCSI-liikennettä. vSwitch-kykimiä koskevat kuvat on otettu migraation jälkeen. Siksi kaikki verkkokortit ilmoittavat liitettävyyden puutteesta.

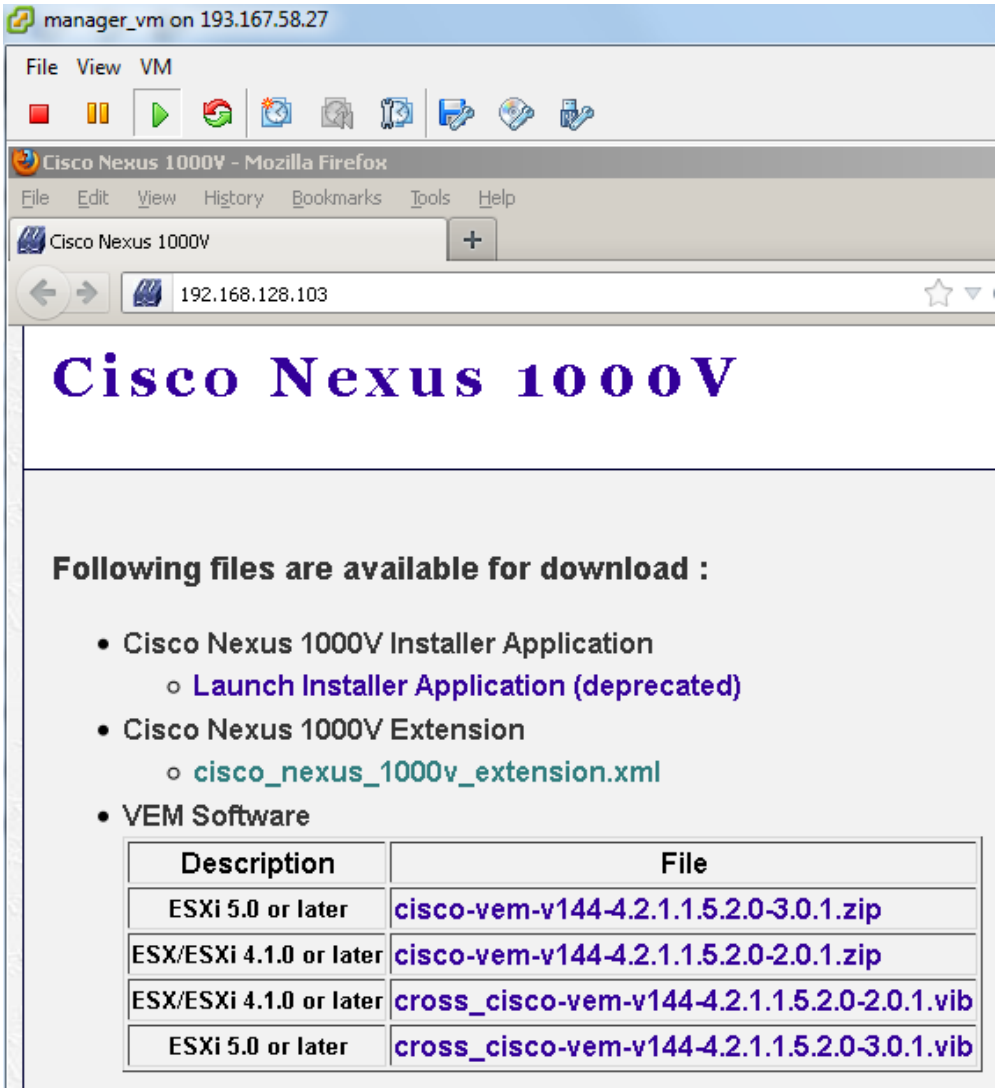


Kuva 15. Vmnic3 ja vmk4:sen iSCSI-asetukset

6.7 Nexus SVS -yhteys

VSM-moduuli säilyttää jatkuvan yhteyden vCenter-palvelimeen. Yhteyttä käytetään ylläpitämään määritteitä ja siirtämään muutoksia porttiprofiileissa vCenter-palvelimelle. Nexus 1000V käyttää vCenter-palvelimelle tarkoitettua liitännäistä (plugin) yhteyden muodostamiseen ja ylläpitämiseen. Nexus 1000V liitännäinen on XML-tiedosto, jonka voi ladata VSM-moduulin hallintaverkon osoitteesta (Nexus Management). XML-liitännäinen täytyy asentaa ennen yhteyden muodostamista VSM-moduulin ja vCenter-palvelimen välille. VSM-moduulin ja vCenter-palvelimen välisen yhteyden katketessa uusia asetuksia on mahdotonta tehdä. VEM-moduulit jatkavat kuitenkin toimintaansa ja välittävät paketteja eteenpäin, vaikka yhteys VSM-moduuliin on poikki. Katkon aikana tehdyt muutokset välittyvät VEM-moduuleille välittömästä yhteyden palattua. VSM-moduuli pitää tästä huolen. (Corbin, Fuller & Jansen 2011, 390.)

vCenter-palvelimen liitännäisen lataamista varten oli siirrettävä yksi virtuaalikone Nexus Management -verkon puolelle, koska tällä verkolla on ainoastaan virtuaalinen liitettävyys. Samalta http-alustalta saa myös ladattua VEM-moduulin ESXi-palvelimia varten.



Kuva 16. vCenter-palvelimen liitännäisen lataus

Liitännäisen lataamisen jälkeen virtuaalikone siirretään toiseen verkkoon, jonka kautta tiedosto voidaan siirtää fyysiselle tietokoneelle. Tämän kautta liitännäinen voidaan vihdoin asentaa vCenter-palvelimeen. Liitännäisen asentaminen vie vain hetken ja tämän jälkeen vCenter-palvelin on valmis kekustelemaan VSM-moduulin kanssa. VSM-moduuli täytyy vielä tehdä tietoiseksi vCenter-palvelimesta. Suoritetaan seuraava konfigurointi Neuxs 1000V kytkimellä:

N1KV#cconf t

N1KV(config)#svs connection gammak6

N1KV(config-svs-conn)#protocol vmware-vim

N1KV(config-svs-conn)#vmware dvs datacenter-name Gammak6

N1KV(config-svs-conn)#remote ip address 192.168.128.106

N1KV(config-svs-conn)#connect

N1KV(config-svs-conn)#exit

N1KV(config)#copy run start

Yhteyden voi varmistaa seuraavalla komennolla:

N1KV# sh svs connections gammak6

connection gammak6:
ip address: 192.168.128.106
remote port: 80
protocol: vmware-vim https
certificate: default
datacenter name: Gammak6
admin:
max-ports: 8192
DVS uuid: d8 cd 01 50 86 21 70 0b-1f 26 4d b7 b0 5d 74 c5
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 5.1.0 build-799731
vc-uuid: B51ACDEE-A709-4303-99E5-764162FE62A6

Onnistuneen yhteydenmuodostamisen jälkeen on vuorossa VLAN-verkkojen konfigurointi:

N1KV#cconf t

*N1KV(config)#*vlan 69

*N1KV(config-vlan)#*name haukiverkko

*N1KV(config-vlan)#*vlan 150

*N1KV(config-vlan)#*name Nexus_Control

*N1KV(config-vlan)#*vlan 160

*N1KV(config-vlan)#*name Nexus_Management

*N1KV(config-vlan)#*vlan 170

*N1KV(config-vlan)#*name Nexus_Packet

6.8 Nexus Port profile

Nexus 1000V käyttää niin sanottuja porttiprofiileita (port profile) VEM-moduulien liitäntöjen (interface) konfiguroimiseen. Samaa porttiprofiilia voidaan käyttää useassa eri liitännässä ja tämä mahdollistaa standardoidut liitännät eri VEM-moduuleiden välillä. Kaikki saman porttiprofiilin alla olevat liitännät hyväksyvät automaattisesti porttiprofiiliin tehdyt muutokset. vCenter-palvelimessa porttiprofiileja edustavat porttiryhmät (port group). vCenter-palvelimella vethernet- ja ethernet-liitännät liitetään porttiprofiileihin ja näin voidaan määrittää suuri määrä portteja yhdellä säännöllä. Palvelimen ylläpitäjän on mahdollista liittää uplink-määritteellä varustetut porttiprofiilit fyysisiin verkkokortteihin, vmnic (VMware termi) tai pnic (Cisco termi). Porttiprofiilit joilla ei ole uplink-määritettä, ovat virtuaalikoneita varten. (Corbin, Fuller & Jansen 2011, 429.)

Porttiprofiileja luodessa on otettava huomioon muutamia seikkoja. ESXi-palvelimia liitettäessä vDS-kytkimeen, palvelimien tulisi saada tieto porttiprofiileista, mutta saadakseen tämän tiedon porttiprofiileista, palvelimien tulisi käyttää porttiprofiileita. Ongelman kiertämiseksi käytetään system vlan -määritettä. Kun VLAN-verkko merkitään system vlan-määritteellä, siirtyy tieto ESXi-palvelimille vCenterin kautta ennen kuin palvelimet ovat kykeneviä muodostamaan yhteyden itse VSM-moduulin. Näin mahdollistetaan järjestelmän toimivuus alkutilanteessa ja tilanteissa, joissa VSM-moduuli on mahdollisesti tavoittamattomissa. Kaikkia VLAN-verkkoja ei tule merkitä system vlan -määritteellä, koska se muuttaa oleellisesti tapaa, jolla Nexus 1000V kohtelee VLAN-verkkoa ja toiseksi system vlan -määritettä on äärimmäisen hankala poistaa. Tärkeimmät VLAN-verkot, jotka tulisi merkitä system vlan -määritteellä ovat:

- Nexus Management VLAN
- Nexus Control VLAN
- iSCSI-verkon VLAN

(Bakke 2012.)

6.8.1 Konfigurointi

Aloitetaan porttiprofiileiden määrittäminen uplink-profiilista. Asiakas liittää tähän profiiliin kaikki ESXi-palvelimien käyttöön otettavat liitännät. Uplink-profiiliin täytyy

ehdottomasti merkitä system vlan -määritteet. Uplink-profiili määritettiin seuraavalla tavalla:

N1KV#conf t
N1KV(config)#port-profile type ethernet system-uplink
N1KV(config-port-prof)#vmware port-group
N1KV(config-port-prof)#switchport mode trunk
N1KV(config-port-prof)#switchport trunk allowed vlan 1,69,150,160,170
N1KV(config-port-prof)#channel-group auto mode on mac-pinning
N1KV(config-port-prof)#no shutdown
N1KV(config-port-prof)#system vlan 150,160,170
N1KV(config-port-prof)#state enabled

Channel-group -komento laittaa kaikki porttiprofiiliin liitetyt liitännät suorittamaan automaattisesti mac-pinning -toimintoa. Näin saavutetaan jonkun asteinen kuormajako ilman asiakkaan kytkimien konfiguroimista. Seuraavaksi luodaan vethernet-profiilit virtuaalikoneita varten, joihin myös tulee luoda system vlan -määritteet, niitä tarvitseville VLAN-verkoille.

N1KV(config)#port-profile type vethernet Nexux_Control
N1KV(config-port-prof)#vmware port-group
N1KV(config-port-prof)#switchport mode access
N1KV(config-port-prof)#switchport access vlan 150
N1KV(config-port-prof)#no shutdown
N1KV(config-port-prof)#system vlan 150
N1KV(config-port-prof)#state enabled

Tässä kohtaa tulee huomioida iSCSI-yhteyksien tarpeita. iSCSI-yhteydet ovat luonnostaan suoria yhteyksiä yhdestä fyysisestä liitännästä toiseen. Tämän vuoksi iSCSI-yhteydet sisältävään vethernet-profiiliin tulee sisällyttää iscsi-multipath -komento. Tämä mahdollistaa iSCSI-yhteyksien yhdistäminen useamman fyysisen pnic-adapterin läpi. Ilman komentoa vCenter ei anna määrittää verkkosovitinta iSCSI kykeneväksi.

N1KV(config)#port-profile type vethernet Nexus_Management
N1KV(config-port-prof)#vmware port-group
N1KV(config-port-prof)#switchport mode access

N1KV(config-port-prof)#switchport access vlan 160
N1KV(config-port-prof)#capability iscsi-multipath
N1KV(config-port-prof)#no shutdown
N1KV(config-port-prof)#system vlan 160
N1KV(config-port-prof)#state enabled

N1KV(config)#port-profile type vethernet Nexus_Packet
N1KV(config-port-prof)#vmware port-group
N1KV(config-port-prof)#switchport mode access
N1KV(config-port-prof)#switchport access vlan 170
N1KV(config-port-prof)#no shutdown
N1KV(config-port-prof)#system vlan 170
N1KV(config-port-prof)#state enabled

N1KV(config)#port-profile type vethernet haukiverkko
N1KV(config-port-prof)#vmware port-group
N1KV(config-port-prof)#switchport mode access
N1KV(config-port-prof)#switchport access vlan 69
N1KV(config-port-prof)#no shutdown
N1KV(config-port-prof)#state enabled

6.9 vCenter vNetwork Distributed Switch (vDS) migraatio

Nexus 1000V on konfiguroitu valmiiksi ja ESXi-palvelimet voidaan siirtää käyttämästä yksinkertaisia vSwitch-kytkimiä ja siirtää verkon toiminnallisuus vDS-kytkimen puolelle. Aloitetaan lisäämällä molemmat ESXi-palvelimet vDS-kytkimen puolelle. Tässä kohtaa ei kuitenkaan vielä siirretä yhtään vmnic-adapteria kytkimelle. Näin voidaan varmistaa osa verkon konfiguraatiosta ilman toiminnallisuuden vaarantamista. Lisätään ESXi-palvelimet vDS-kytkimeen ja jos vCenter ei anna virheilmoituksia, suoritetaan VSM-moduulista komento: **show module**

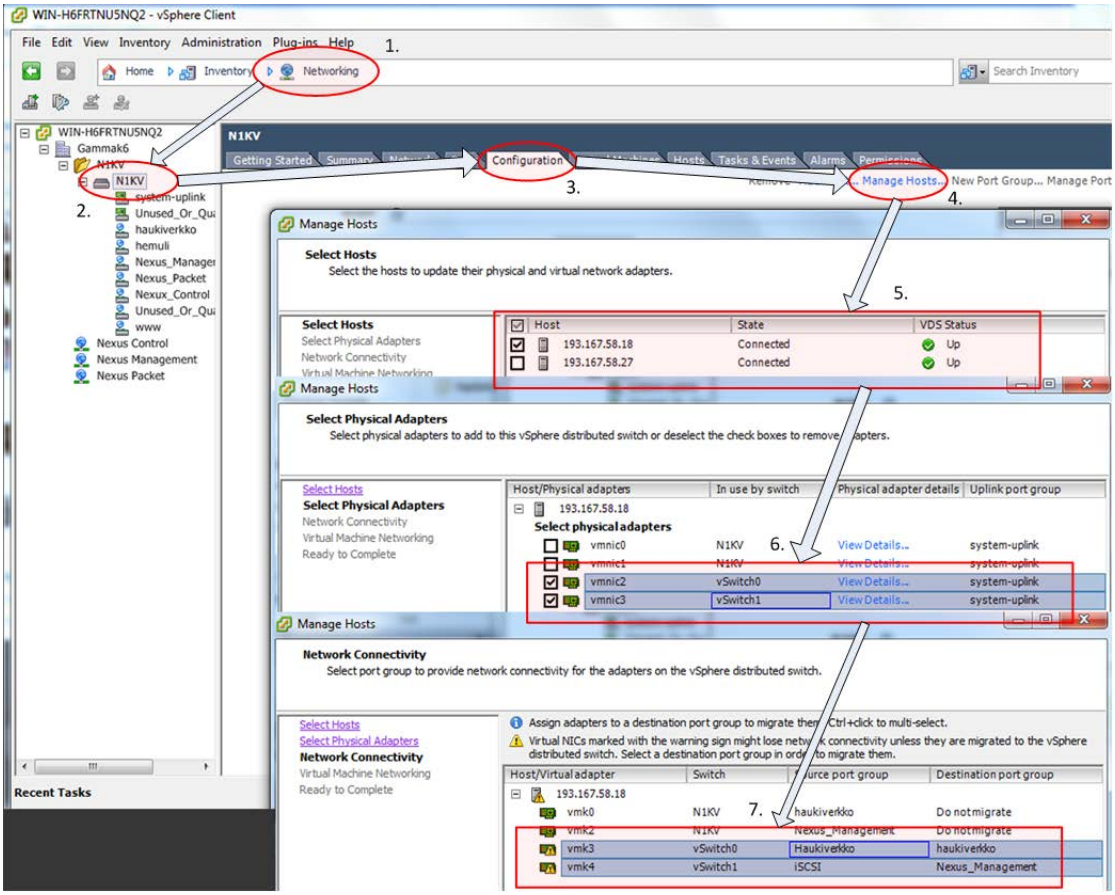
N1KV# show module

Mod	Ports	Module-Type	Model	Status
1	0	Virtual Supervisor Module	Nexus1000V	active *
2	0	Virtual Supervisor Module	Nexus1000V	ha-standby

```
3    248    Virtual Ethernet Module          NA              ok
4    248    Virtual Ethernet Module          NA              ok

Mod  Sw              Hw
---  --------------  ------------------------------------------------
1    4.2(1)SV1(5.2)    0.0
2    4.2(1)SV1(5.2)    0.0
3    4.2(1)SV1(5.2)    VMware ESXi 5.0.0 Releasebuild-623860 (3.0)
4    4.2(1)SV1(5.2)    VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP       Server-UUID                          Server-Name
---  --------------  -----------------------------------  --------------------
1    192.168.128.103  NA                                   NA
2    192.168.128.103  NA                                   NA
3    193.167.58.18    44454c4c-5900-1044-8037-c3c04f53334a  193.167.58.18
4    193.167.58.27    44454c4c-5900-1044-8037-c4c04f53334a  193.167.58.27
```

Yliviivatut merkinnät kuuluvat ESXi-palvelimien VEM-moduuleille. Niiden näkyminen show module -komennolla tarkoittaa, että system vlan -määritteet ja VLAN-verkkojen asetukset, ovat molemmat oikein. Varmistamisen jälkeen voidaan varsinaiset verkon komponentit siirtää vDS-kytkimen puolelle.

Tämä työvaihe on hyvin kriittinen. Jos konfiguraatioissa on tehty jotain väärin, on ESXi-palvelimien hallinnan menettäminen hyvin todennäköistä. ESXi-palvelimet ovat kuitenkin helposti palautettavissa takaisin vSwitch-kytkimen varaan kirjautumalla jokaiselle palvelimelle paikallisesti ja suorittamalla ”palauta alkuperäinen vSwitch” -toiminto. Migraatio on järkevintä suorittaa ESXi-palvelin kerrallaan ja aloittaa palvelimesta, jolla ei ole yhtään virtuaalikonetta hallittavana. Jos migraation jälkeen ESXi-palvelin vastaa vCenterin komentoihin, voidaan suorittaa vMotionin avulla virtuaalikoneen siirtäminen jo muutetulle palvelimelle. Jos tämäkin sujuu ongelmitta, voidaan konfiguraatio todeta toimivaksi kaikin puolin. Seuraava kuva osoittaa, miten migraatio aloitetaan. Kuva on myös mukana isompana liitteenä.

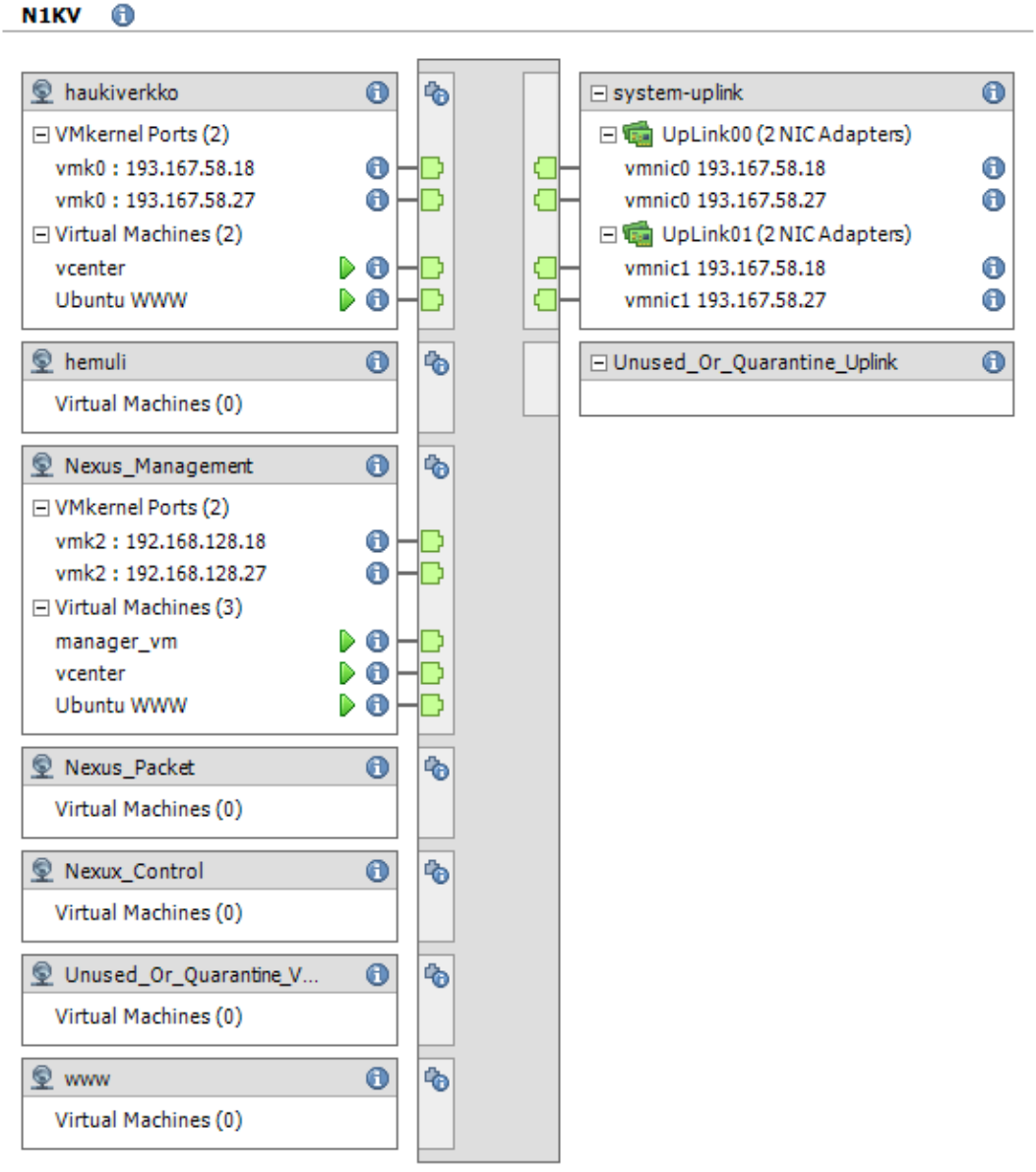


Kuva 17. vDS-kytkimen migraatio

Avataan kuvan esittämää toimintajärjestystä.

1. Valitaan vCenterin hallintanäkymistä verkkoja käsittelevä hallintanäkymä.
2. Valitaan objektiluettelosta Nexus 1000V:n luoma N1KV vDS -kytkin.
3. Valitaan vDS-kytkimen konfiguraationäkymä.
4. Aloitetaan palvelimien hallintatoiminto.
5. Valitaan ensimmäinen siirrettävä palvelin, jolla ei ole virtuaalikoneita hallitta-vana.
6. Valitaan siirrettävät fyysiset verkkokortit ja määritetään niille porttiprofiiliksi valmiiksi luotu system-uplink -porttiprofiili.
7. Määritetään vSwitch-kytkimien verkot siirrettäväksi vethernet porttiprofiilei-hin. ESXi-palvelimen hallintaliikenteestä vastaava vSwitch-kytkin siirretään haukiverkkoon kytkettyyn porttiprofiilin ja iSCSI-yhteyksille tarkoitettu vSwitch-kytkin siirretään Nexus Management -porttiprofiiliin, joka on samassa verkossa, kuin iSCSI-palvelin.

Koska ensimmäisellä palvelimella ei ole yhtään virtuaalikonetta, ei niitä tarvitse siirtää migraatiotyökalun avulla. Tämän jälkeen jos ESXi-palvelin ei menetä yhteyttä vCenter-palvelimeen, voidaan virtuaalikoneet siirtää yksitellen vMotion-tekniikan avulla jo siirretylle koneelle. Tämän jälkeen suoritetaan jäljelle jääneelle ESXi-palvelimelle sama siirtotoimenpide. Nexus 1000V -virtuaalikytkin on alustavasti konfiguroitu, otettu käyttöön ja lopputuloksena on seuraavannäköinen vDS-kytkin.



Kuva 18. Valmis vDS-kytkin

7 NEXUS 1000V ACCESS CONTROL LIST (ACL)

Nexus 1000V ei vasta asennettuna tarjoa varsinaisesti mitään uutta, mitä VMwaren oma vDS-kytkin ei tarjoaisi. Jotta Nexus 1000V:n toiminnasta saisi jotain käsitystä,

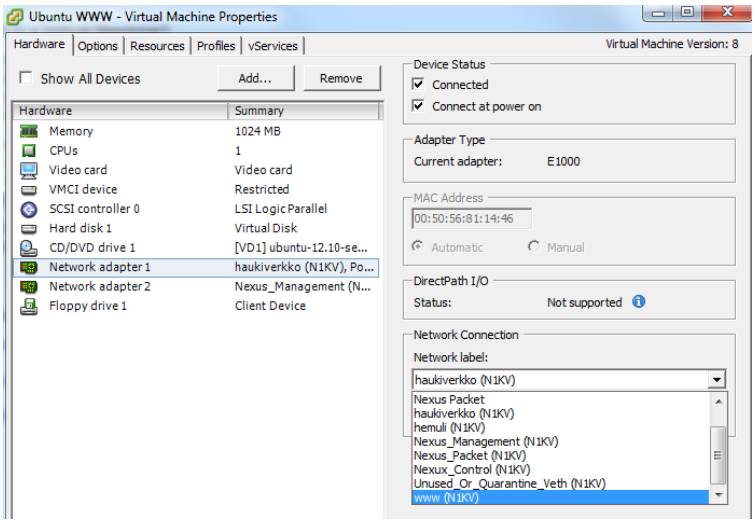
päätettiin kokeilla pääsylistojen luomista ja toimintaa. Tätä ominaisuutta ei löydy VMwaren omasta vDS-kytkimestä. Pääsylistan tarkoitus on suodattaa virtuaalikoneelta kaikki verkkoliikenne, paitsi http- ja dhcp-protokolla. Pääsylistaa sovelletaan yksinkertaiseen linux-pohjaiseen www-palvelimeen. Aloitetaan luomalla pääsylista.

N1KV#conf t
N1KV(config)#ip access-list www
N1KV(config-acl)#permit tcp any eq www any
N1KV(config-acl)#permit udp any eq bootpc any

Seuraavaksi pääsylista liitetään porttiprofiiliin ja koska muita virtuaalikoneita ei haluta rampauttaa asettamalla pääsylistaa yleiseen haukiverkon porttiprofiiliin, luodaan pääsylistaa varten uusi porttiprofiili.

N1KV#conf t
*N1KV(config)#*port-profile type vethernet www
*N1KV(config-port-prof)#*vmware port-group
*N1KV(config-port-prof)#*switchport mode access
*N1KV(config-port-prof)#*switchport access vlan 69
*N1KV(config-port-prof)#*ip port access-group www in
*N1KV(config-port-prof)#*no shutdown
*N1KV(config-port-prof)#*state enabled

Liitetään virtuaalinen www-palvelin käyttämään luotua porttiprofiilia.



Kuva 19. WWW-palvelimen porttiprofiilin vaihto

8 TODENTAMINEN

Kaikki tarpeellinen on konfiguroitu, lisäominaisuuksia on otettu käyttöön, mutta toimiiko kaikki? Kysymys tarvitsee ehdottomasti vastauksen ja siihen lähdetään vastaamaan aloittamalla pääsylistan toiminnan varmentamisella.

Nollataan tilanne ja siirretään virtuaalikone takaisin alkuperäiseen porttiprofiiliin, jossa ei ole yhtään estoa tai rajausta. Varmistetaan, että www-palvelimella on muitakin palveluja päällä, kuten SSH. Käytetään hyväksi ilmaisia nettipohjaisia verkkoskannereita ja todennetaan porttien olevan auki.

Scanning ports on 193.167.58.14

```
193.167.58.14 is responding on port 22 (ssh).
193.167.58.14 is responding on port 80 (http).
```

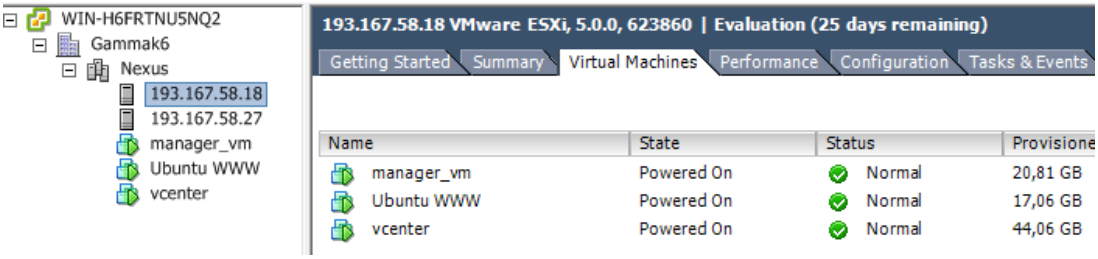
Palvelin vastaa kummassakin portissa, joissa tiedetään olevan palvelu. Siirretään palvelin takaisin sille tarkoitettuun www-porttiprofiiliin, joka suodattaa kaiken liikenteen paitsi www- ja dhcp-protokollan. Dhcp:n toimintaa ei voida kyseisellä skannerilla varmentaa, koska se tukee vain TCP-protokollaa. Virtuaalikone voidaan kuitenkin käynnistää uudelleen, koska verkon konfiguraatio on asetettu automaattiseen tilaan. Jos kone käynnistyessään saa verkkoliitettävyyden, tarkoittaa se porttiprofiilin toimivan. Käynnistetään virtuaalikone uudelleen ja suoritetaan porttien skannaus.

Scanning ports on 193.167.58.14

```
193.167.58.14 isn't responding on port 22 (ssh).
193.167.58.14 is responding on port 80 (http).
```

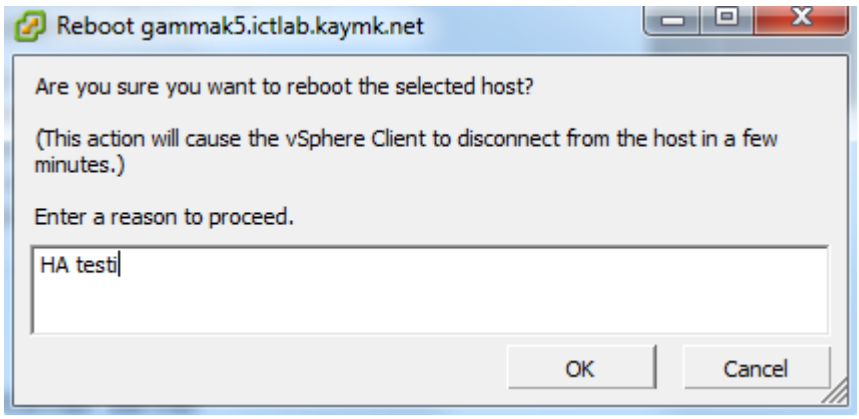
Virtuaalikone sai dhcp-palvelimelta verkon asetukset ja suodatti onnistuneesti SSH-liikenteen pois. Porttiprofiili voidaan todeta toimivaksi. Seuraavaksi todennetaan korkean saatavuuden ja sääntöjen siirtyvyyden toiminta. Pakotetaan kaikkia virtuaalikoneita sisältävä palvelin käynnistymään uudelleen, tarkastellaan siirtyykö virtuaalikoneet oikein palvelimelta toiselle ja todennetaan porttiprofiileiden toiminta siirtymisen

jälkeen. Koska myös vCenter-palvelin sammuu, on koko järjestelmän rampautuminen mahdollista. Aloitetaan testaus varmistamalla kaikkien virtuaalikoneiden sijainti.



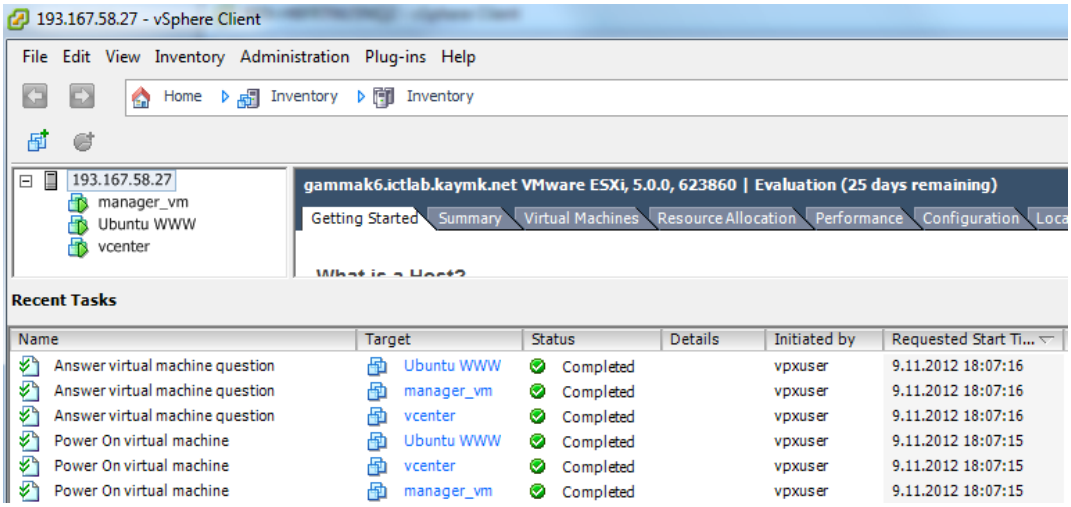
Kuva 20. Virtuaalikoneet gammak5-palvelimella

Kirjaudutaan sisälle gammak5-palvelimelle ja pakotetaan palvelimen uudelleen käynnistys. Tätä kautta tehtynä vCenter-palvelin ei saa tietoa uudelleenkäynnistyksestä ja näin simuloidaan vikatilannetta.



Kuva 21. Gammak5-palvelimen uudelleenkäynnistys

Koska vCenter-palvelin sammuu myös tilapäisesti, on kirjauduttava gammak6-palvelimelle tilanteen tarkkailemiseksi.



Kuva 22. Virtuaalikoneiden onnistunut ylösnosto

Virtuaalikoneiden onnistuneen siirtymisen jälkeen tarkastetaan vielä nopeasti portti-profiileiden toiminta suorittamalla www-palvelimen porttien skannaus.

Scanning ports on 193.167.58.14

```
193.167.58.14 isn't responding on port 22 (ssh).
193.167.58.14 is responding on port 80 (http).
```

Järjestelmä on VMwaren puolesta luokiteltu kestämään yhden palvelimen vikaantuminen ja testi osoittaa järjestelmän kestävän suunnitelman mukaisesta. Nexus 1000V ylläpitää myös toimintansa vikatilanteen aikana ja suorittaa uudelleen synkronoinnin heti ESXi-palvelimen yhdistäessä takaisin vCenter-palvelimeen. Näin ollen toteutus voidaan todeta onnistuneeksi.

9 YHTEENVETO

SimuNet tarjoaa valtavan määrän vaihtoehtoja ja mahdollisuuksia toteuttaa erilaisia simulaatioita ja projekteja, mutta se on myös ympäristönä äärimmäisen haastava. Opinnäytetyö käsittelee pääasiallisesti VMwaren ja Cisco Systemsin yhteistyötä ja Nexus 1000V -sarjan ratkaisuja. Eniten aikaa kului SimuNet-ympäristön toimintaa selvittäessä.

Alun perin asiakkaan verkon siltaamista MPLS-verkon yli lähdettiin toteuttamaan multipoint-to-multipoint -ajatuksella ja toteutuksessa käytettiin hyväksi VPLS- ja QinQ-tekniikkaa. Ratkaisun toimiessa keskityttiin olennaisempiin asioihin, kuten

VMware-ympäristöön ja Nexus 1000V:hen. Työn loppuvaiheilla, kerrattaessa ratkaisuja, huomattiin alkuperäisen verkkoratkaisun olevan kaikkea muuta kuin moderni operaattoriverkon ratkaisu. QinQ-tekniikka pakottaa varaamaan vähintään yhden VLAN-alueen operaattorin verkosta. Nykypäivän standardien mukaan tämä ei ole tarpeeksi skaalautuva menettelytapa. Lisäksi VPLS-tekniikka suorittaa operaattorin verkossa asiakkaan MAC-osotteiden oppimista, jota oikeasti halutaan vain muutamissa tapauksissa. Kyseisten tekniikoiden yhdistelmä ei siis ollut järkevä operaattoritason ratkaisu.

Verkon toimintaa korjattiin ja päädyttiin point-to-point -tyyliseen ratkaisuun kahden internetreunalaitteen (PE3 ja PE4) välille. Point-to-point -ratkaisu on laiteresurssien sanelema, koska vain kyseiset reunalaitteet pystyvät luomaan service instance -palveluja. EVC-pohjainen ratkaisu, jonka avulla käytetään skaalattavia EoMPLS-tunneleita, oli merkittävä parannus alkuperäiseen suunnitelmaan.

VMwaren ja Nexuksen osalta kaikki onnistui ja toimi suunnitelmien mukaan, mutta lopputulos ei ollut täysin tyydyttävä. Palvelu, joka luodaan helpottamaan asiakkaan taakkaa ja yksinkertaistamaan toimintaa, on ainakin tässä tapauksessa harvinaisen monimutkainen ottaa käyttöön. Myös toteutuksen vakaus jätti epäilyille sijaa. Verkon muutostöiden aikana Nexus 1000V -järjestelmä purkautui melkein alkutekijöihinsä. VEM-moduulit kadottivat osittain konfiguraationsa ja yhteyksien palautuessa verkon osalta, eivät ESXi-palvelimet osanneet enää keskustella VSM-moduulien kanssa. Tästä seurasi osittain Nexus 1000V:n uudelleen käyttöönotto.

Asetelmassa ilmeni lisää ongelmia liittyen vikatilanteisiin. Väärissä olosuhteissa, on mahdollista ajautua niin sanottuun Split Brain -tilanteeseen. Tämä tarkoittaa VSM-moduuleiden välistä kommunikaatiokatkosta, jonka seurauksena molemmat VSM-moduulit menevät aktiivitilaan. Tilanteeseen voidaan ajautua, jos VSM-moduulit ovat VMware-klusterissa eri palvelimilla ja niiden väliset hallinta- ja kontrolliverkko katkeavat. Tämä tilanne osoitti puutteita hallintaverkon suunnittelussa. Edellä mainituista syistä Cisco ei virallisesti tue suunnitelman mukaista konfiguraatiota.

Suunnitelman mukaista asetelmaa on kuitenkin mielestäni mahdollista vakauttaa merkittävästi, sillä suurin ongelma tuntuu olevan liiallinen virtualisointi. vCenter-palvelimen ja VSM-moduulin siirtäminen pois virtuaalisesta ympäristöstä ja asentaminen fyysisiksi laitteiksi esim. Nexus 1010, auttaisi merkittävästi vikatilanteissa. Täl-

lä tavalla uskon palvelun olevan jossain määrin käyttökelpoinen, vaikka lisensoinnin ja fyysisten VSM-moduuleiden hinta arveluttaakin.

Opinnäytetyön aikarajoitusten takia Nexus 1000V järjestelmästä jäi tutkimatta merkittäviä ominaisuuksia, kuten virtuaalikoneiden QoS ja SPAN-toiminnot. Lyhyesti tiivistettynä Nexus 1000V -sarja tarjoaa ehdottomasti etuja pelkistettyyn VMwaren vDS-kytkimeen nähden. Pienin varauksin ja huolellisen suunnittelun avulla Nexus 1000V -sarjan ratkaisut voivat tarjota asiakkaille uudenlaista helpotettua virtuaalipalvelinten hallintaa.

LÄHTEET

Bakke, M. 2012. Advanced - Deploying and Troubleshooting the Nexus 1000v virtual switch. Lontoo 2012. Cisco Systems. Cisco Live 2012 tapahtuman seminaaritaltiointi. [viitattu 1.11.2012]

Bowling, J. 2011. Should servers in a cluster have the same everything? Blogi. Saatavissa: http://vsential.com/2011/03/should-servers-in-a-cluster-have-the-same-everything [viitattu 6.11.2012]

Chatzithomaoglou, A. 2009. EVC: Flexible Service Mapping. Blogi. Saatavissa: http://ccie-in-3-months.blogspot.fi/2009/09/evc-flexible-service-mapping.html [viitattu 13.11.2012]

Cisco Systems. 2012. Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3). Verkkojulkaisu. Saatavissa: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/port_profile/configuration/guide/n1000v_portprof.pdf [viitattu 5.11.2012]

Corbin, K., Fuller, R., Jansen, D. 2010. NX-OS and Cisco Nexus Switching. Indianapolis: Cisco Press.

Ferguson, B. 2012. The official VCP5 certification guide. Massachusettes: Pearson plc.

Kettunen, M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana. Verkkojulkaisu. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/SimuNet%20artikkeliv6a.pdf [viitattu 28.10.2012]

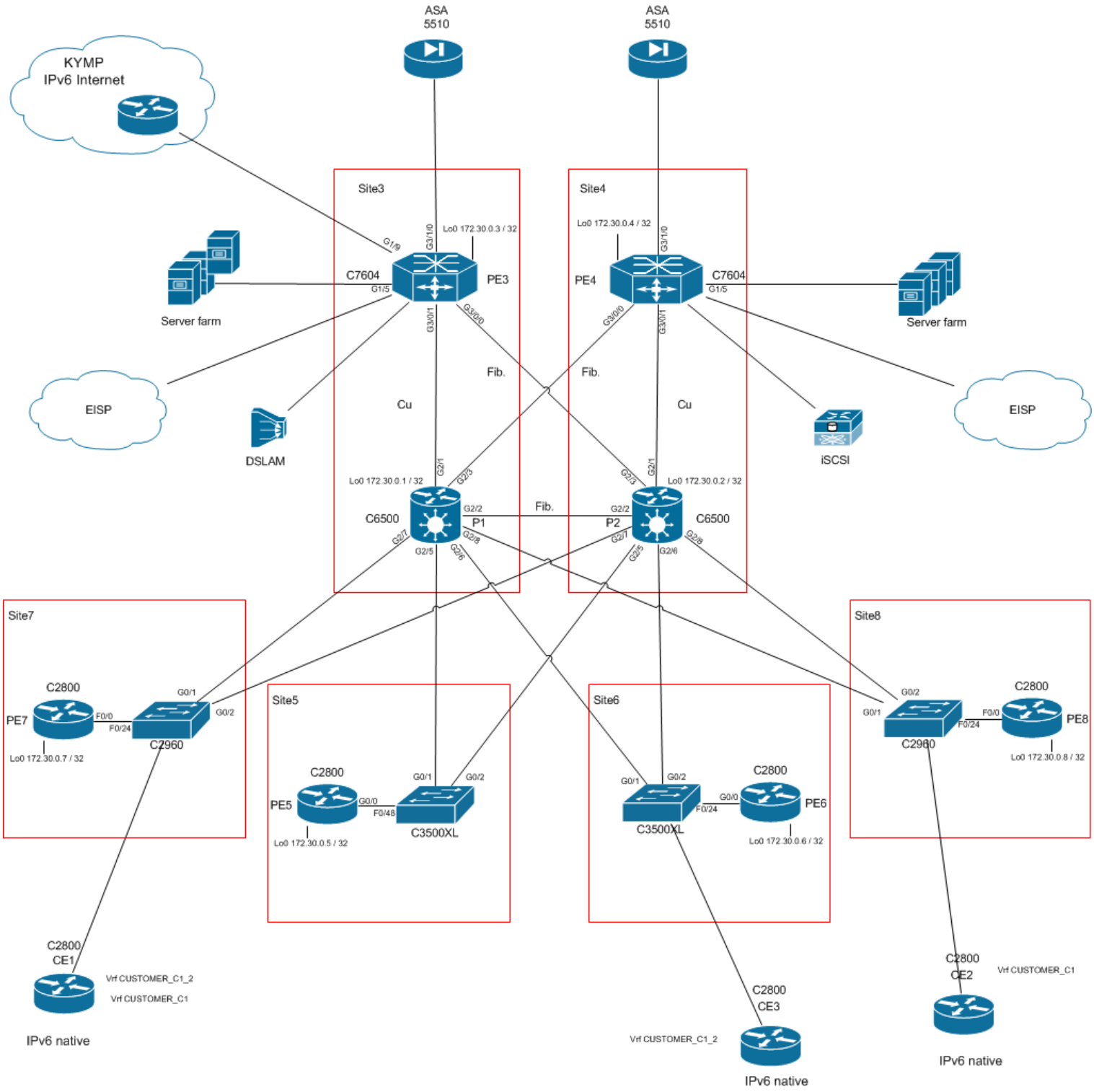
Lowe, S. 2011. Mastering Vmware vSphere 5. Indianapolis: John Wiley & Sons Inc.

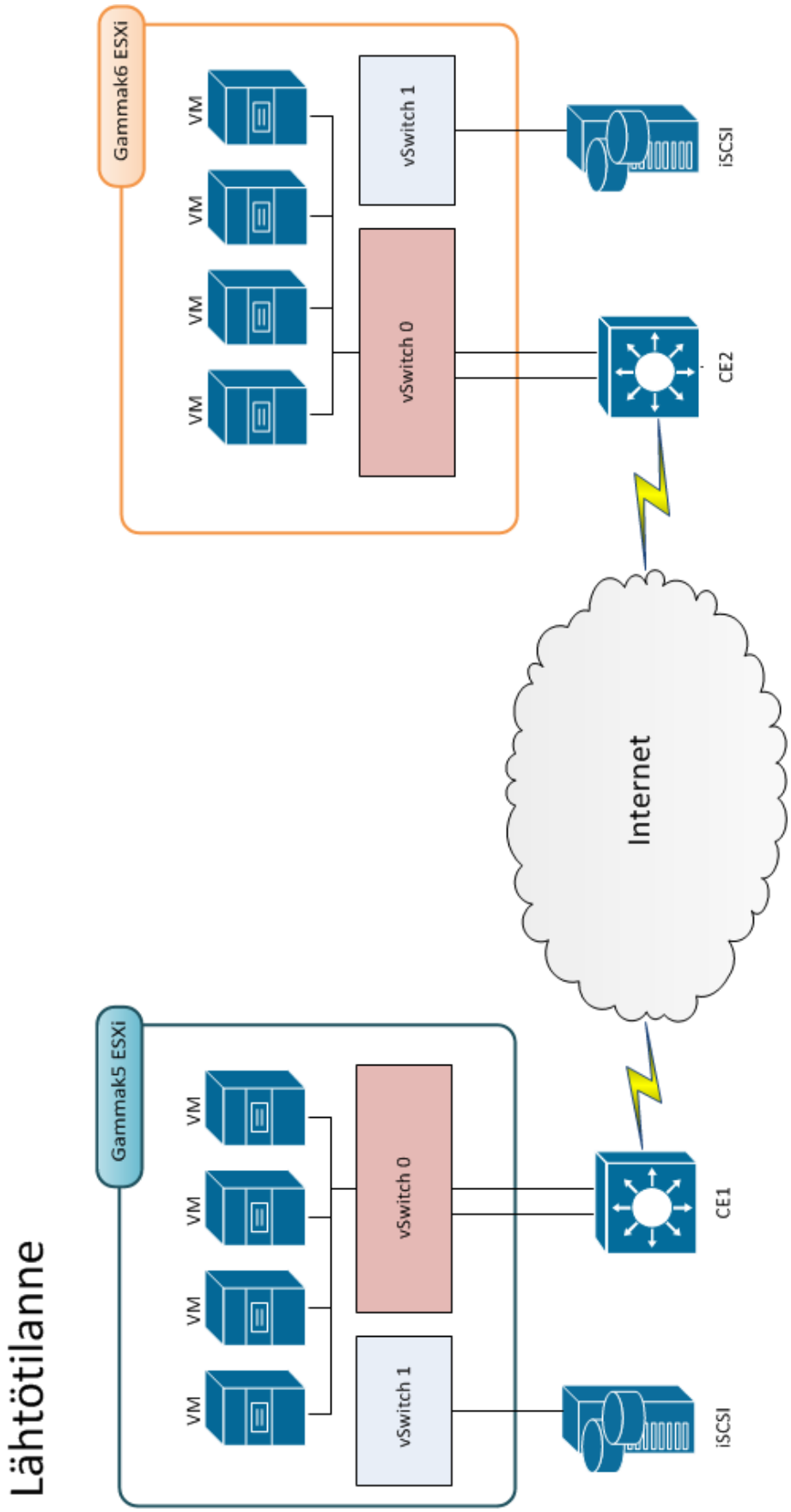
Odom, W. 2008. CCNA ICND2 Official Exam Certification Guide, Second Edition. Indianapolis: Cisco Press.

Oinonen, R. 2011. MPLS L2VPN ja operaattoriverkon kahdennetut palvelut. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/Riku%20Oinonen%20thesis.pdf [viitattu 28.10.2012]

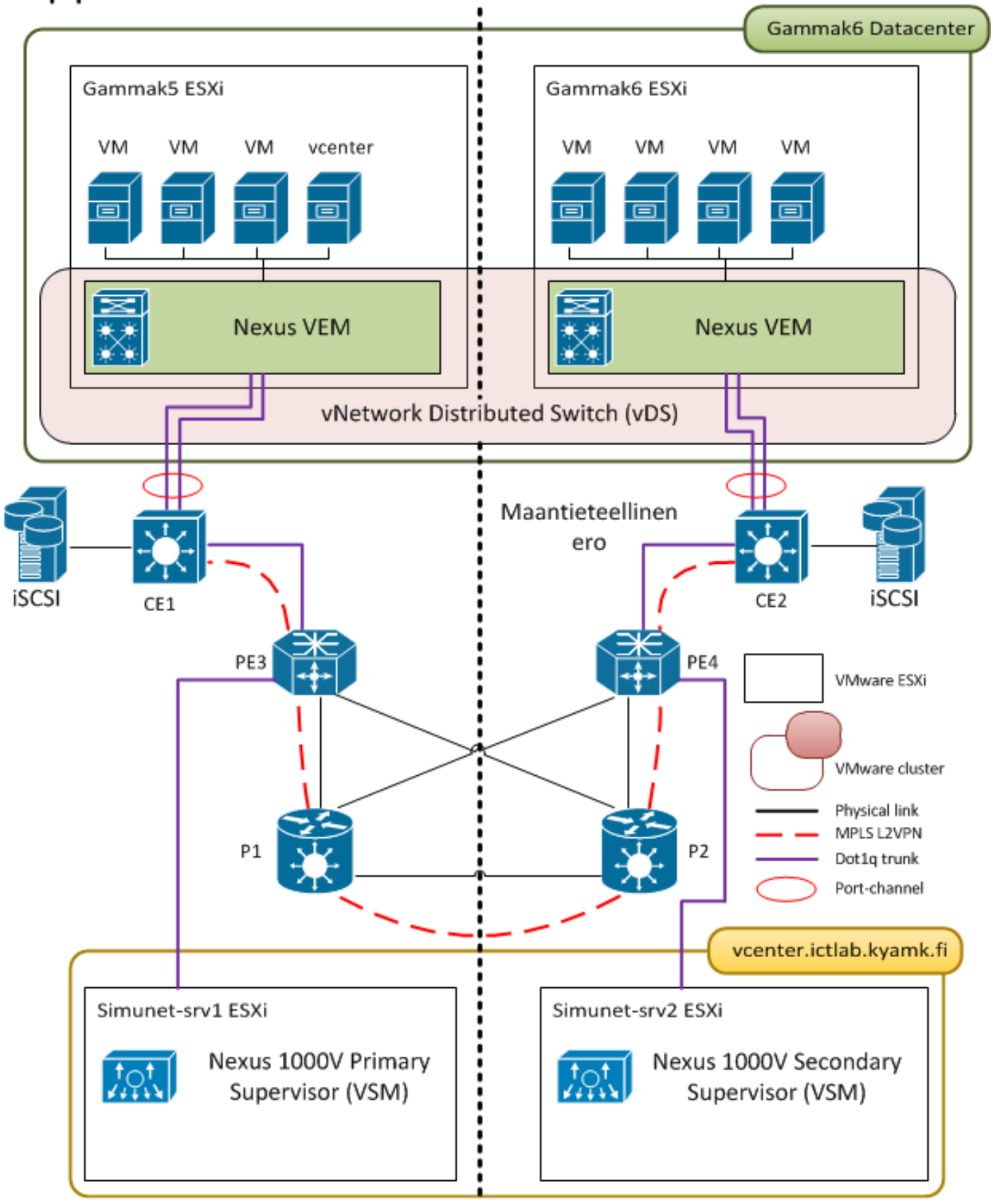
Tuntematon. 2012. SimuNetin fyysinen kytkentä. Kaavio. Saatavissa: Kymenlaakson Ammattikorkeakoulun ICT-Laboratorion sisäverkko.

Xu, Z. 2010. Design and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services. Indianapolis: Wiley Publishing, Inc.


ASA
5510
ASA
5510
KYMP
IPv6 Internet
Site3
Site4
Lo0 172.30.0.4 / 32
G1/8
G3/1/0
Lo0 172.30.0.3 / 32
C7604
G1/5
PE3
PE4
C7604
G1/5
Server farm
Server farm
G3/0/1
G3/0/0
G3/0/0
G3/0/1
Fib.
Fib.
EISP
Cu
Cu
EISP
DSLAM
iSCSI
G2/1
G2/3
G2/3
G2/1
Lo0 172.30.0.1 / 32
Lo0 172.30.0.2 / 32
C6500
G2/2
P1
Fib.
P2
G2/2
C6500
G2/7
G2/5
G2/8
G2/6
G2/5
G2/7
G2/6
G2/8
Site7
Site8
C2800
G0/1
G0/2
G0/2
C2800
PE7
F0/0
F0/24
G0/1
F0/0
F0/24
PE8
C2960
C2960
Lo0 172.30.0.7 / 32
Lo0 172.30.0.8 / 32
Site5
Site6
C2800
C2800
G0/1
G0/2
G0/1
G0/2
PE5
G0/0
F0/48
C3500XL
G0/0
F0/24
PE6
C3500XL
Lo0 172.30.0.5 / 32
Lo0 172.30.0.6 / 32
C2800
CE1
Vrf CUSTOMER_C1_2
Vrf CUSTOMER_C1
IPv6 native
C2800
CE3
Vrf CUSTOMER_C1_2
IPv6 native
C2800
CE2
Vrf CUSTOMER_C1
IPv6 native


Lähtötilanne
Gammak6 ESXi
VM
VM
VM
VM
vSwitch 1
vSwitch 0
iSCSI
CE2
Internet
Gammak5 ESXi
VM
VM
VM
VM
vSwitch 0
vSwitch 1
CE1
iSCSI

Lopputilanne



```
CE1#sh run
Building configuration...

Current configuration : 2001 bytes

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

hostname CE1


no aaa new-model
system mtu routing 1500
ip subnet-zero



no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id

vlan internal allocation policy ascending


interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface GigabitEthernet0/3

interface GigabitEthernet0/4

interface GigabitEthernet0/5

interface GigabitEthernet0/6

interface GigabitEthernet0/7

interface GigabitEthernet0/8

interface GigabitEthernet0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/11
 switchport access vlan 150
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/13
 switchport access vlan 160
 switchport mode access

interface GigabitEthernet0/14

interface GigabitEthernet0/15

interface GigabitEthernet0/16

interface GigabitEthernet0/17

interface GigabitEthernet0/18

interface GigabitEthernet0/19

interface GigabitEthernet0/20

interface GigabitEthernet0/21

interface GigabitEthernet0/22

interface GigabitEthernet0/23

interface GigabitEthernet0/24

interface GigabitEthernet0/25

interface GigabitEthernet0/26

interface GigabitEthernet0/27

interface GigabitEthernet0/28

interface Vlan1
 no ip address

interface Vlan150
 ip address 192.168.150.1 255.255.255.0
```

```
interface Vlan160
 ip address 192.168.128.231 255.255.255.0

ip classless
ip http server



control-plane


line con 0
line vty 0 4
 login
line vty 5 15
 login

end
```

```
CE2#sh run
Building configuration...

Current configuration : 2753 bytes

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

hostname CE2


no aaa new-model
system mtu routing 1500
vtp domain testi
vtp mode transparent
ip subnet-zero
ip routing



no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id

vlan internal allocation policy ascending

vlan 69
 name Clustervlan

vlan 150
 name Nexus_Control

vlan 160
 name Nexus_Management

vlan 170
 name Nexus_Packet


interface GigabitEthernet0/1
 switchport access vlan 69
 switchport mode access

interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150-170
 switchport mode trunk

interface GigabitEthernet0/3
 switchport access vlan 69
 switchport mode access

interface GigabitEthernet0/4
 switchport access vlan 69
 switchport mode access

interface GigabitEthernet0/5

interface GigabitEthernet0/6

interface GigabitEthernet0/7

interface GigabitEthernet0/8

interface GigabitEthernet0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/11
 switchport access vlan 150
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,69,150,160,170
 switchport mode trunk

interface GigabitEthernet0/13
 switchport access vlan 160
 switchport mode access

interface GigabitEthernet0/14
 switchport access vlan 160
 switchport mode access

interface GigabitEthernet0/15
 switchport access vlan 160
 switchport mode access

interface GigabitEthernet0/16

interface GigabitEthernet0/17
```

```
interface GigabitEthernet0/18

interface GigabitEthernet0/19

interface GigabitEthernet0/20
 switchport access vlan 69

interface GigabitEthernet0/21
 switchport access vlan 69

interface GigabitEthernet0/22
 switchport access vlan 69

interface GigabitEthernet0/23
 switchport access vlan 69

interface GigabitEthernet0/24
 switchport access vlan 69

interface GigabitEthernet0/25

interface GigabitEthernet0/26

interface GigabitEthernet0/27

interface GigabitEthernet0/28

interface Vlan1
 no ip address

interface Vlan69
 description clusterin hallinta osoitteiden vlan
 no ip address

interface Vlan150
 ip address 192.168.150.2 255.255.255.0

interface Vlan160
 ip address 192.168.128.230 255.255.255.0

ip classless
ip http server


control-plane


line con 0
line vty 0 4
 login
line vty 5 15
 login

end
```

```
PE3#sh run
Building configuration...

Current configuration : 12532 bytes

 Last configuration change at 23:32:22 UTC Wed Nov 14
2012

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver

hostname PE3

boot-start-marker
boot-end-marker

no aaa new-model

ip source-route

ip name-server 2A00:1DD0:100:C1::100
ip name-server 172.16.91.92
ip multicast-routing
ip dhcp excluded-address 172.20.99.1 172.20.99.100
ip dhcp excluded-address 172.20.99.254

ip dhcp pool HALLINTA
 network 172.20.99.0 255.255.255.0
 default-router 172.20.99.1

ip dhcp pool VLAN2001
 network 10.10.11.0 255.255.255.0
 default-router 10.10.11.1

ip dhcp pool VLAN2000
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1

ipv6 unicast-routing
ipv6 dhcp pool vlan2000
 prefix-delegation pool VLAN2000ipv6
 dns-server 2A00:1DD0:0:1::32
 dns-server 2A00:1DD0:0:1::132
 domain-name kymp.net

vtp mode transparent
mpls label protocol ldp
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated




spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
username HALLINTA secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
username simunet secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

redundancy
 main-cpu
  auto-sync running-config
 mode sso

vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000

interface Loopback0
 ip address 172.30.0.3 255.255.255.255

interface Loopback5
 no ip address
 ip pim sparse-mode
 ip igmp version 3

interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::3/128

interface GigabitEthernet1/5
 description simunet-srv
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan
90,91,100,101,110,120,150,200
 switchport mode trunk

interface GigabitEthernet3/0/0
 description P2-PE3 fiber
 dampening
 mtu 1600
 ip address 192.168.23.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 ip ospf cost 1
 carrier-delay msec 0
 negotiation auto
 mpls ip
 bfd interval 100 min_rx 100 multiplier 3

interface GigabitEthernet3/0/1
 description P1-PE3 copper
 dampening
 mtu 1600
 ip address 192.168.13.3 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 carrier-delay msec 0
 speed 1000
 no negotiation auto
 mpls ip
 no mpls ldp igp sync
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
```

```
 ip rsvp bandwidth 512 512

interface GigabitEthernet3/0/2
 no ip address
 speed 1000
 negotiation auto
 service instance 30 ethernet
  encapsulation dot1q 30
  xconnect 172.30.0.4 30 encapsulation mpls

 service instance 40 ethernet
  encapsulation dot1q 40
  xconnect 172.30.0.4 40 encapsulation mpls

interface GigabitEthernet3/0/3
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 140 ethernet
  encapsulation dot1q 69
  xconnect 172.30.0.4 140 encapsulation mpls

 service instance 141 ethernet
  encapsulation dot1q 150
  xconnect 172.30.0.4 141 encapsulation mpls

 service instance 142 ethernet
  encapsulation dot1q 160
  xconnect 172.30.0.4 142 encapsulation mpls

 service instance 143 ethernet
  encapsulation dot1q 167
  xconnect 172.30.0.4 143 encapsulation mpls

router ospf 1
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet3/0/0
 no passive-interface GigabitEthernet3/0/1
 network 172.16.50.0 0.0.0.3 area 0
 network 172.20.99.0 0.0.0.255 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 172.30.101.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
 neighbor 2A00:1DD0:0:200::1 remote-as 65000
 neighbor 172.30.0.4 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO

 address-family ipv4
  network 172.30.0.0 mask 255.254.0.0
  neighbor 2A00:1DD0:0:200::1 activate
  neighbor 172.30.0.4 activate
  neighbor 172.30.0.6 activate
 exit-address-family

 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100::/48
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  neighbor SISAVERKKO send-label
  neighbor 2A00:1DD0:0:200::1 activate
  neighbor 172.30.0.4 activate
 exit-address-family

no ip http server
no ip http secure-server
ip pim ssm default
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1

ip explicit-path name pe3top1tope4 enable
 next-address 192.168.13.1
 next-address 192.168.14.4

logging esm config
access-list 1 permit 172.31.1.2
access-list 100 permit ip host 172.31.1.2 host 172.31.1.3
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100::/48 Null0
ipv6 local pool VLAN2000ipv6 2A00:1DD0:100:4000::/56 64
ipv6 local pool VLAN2000ipv7 2A00:1DD0:100:4200::/56 64

mpls ldp router-id Loopback0 force
snmp-server community public RO
snmp-server host 172.16.120.10 version 2c public

ipv6 access-list testilista
 permit udp any any eq domain
 permit udp any eq domain any

control-plane

line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 session-timeout 60
 login local
 transport input ssh
line vty 5 15
 session-timeout 60
 login local
 transport input ssh

end
```

```
PE4#sh run
Building configuration...

Current configuration : 12068 bytes

 Last configuration change at 23:32:01 UTC Wed Nov 14
2012

version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service counters max age 10
service unsupported-transceiver


hostname PE4


boot-start-marker
boot-end-marker


mls ipv6 vrf

 address-family ipv6
  route-target export 6:6
  route-target import 6:6
 exit-address-family


no aaa new-model


ip source-route


no ip domain lookup
ip domain name ictlab.kyamk.fi
ip multicast-routing
ip dhcp excluded-address 172.21.99.1 172.21.99.100
ip dhcp excluded-address 172.21.99.254




ip dhcp pool HALLINTA
 network 172.21.99.0 255.255.255.0
 default-router 172.21.99.1

ipv6 unicast-routing

vtp mode transparent
clns routing
mls flow ip interface-full
no mls flow ipv6
mls cef error action reset
multilink bundle-name authenticated

spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic bootup level minimal
no errdisable detect cause gbic-invalid
username simunet secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

redundancy
 main-cpu
  auto-sync running-config
 mode sso

vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000

interface Loopback0
 ip address 172.30.0.4 255.255.255.255

interface Loopback6
 no ip address
 ipv6 address 2A00:1DD0:100::4/128

interface GigabitEthernet1/5
 description simunet-srv
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan
90,91,100,101,110,120,150,200
 switchport mode trunk
 no keepalive

interface GigabitEthernet3/0/0
 description P1-PE4 fiber
 dampening
 mtu 1600
 ip address 192.168.14.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 negotiation auto
 mpls ip
 no mpls ldp igp sync
 mpls traffic-eng tunnels
 bfd interval 100 min_rx 100 multiplier 3
 ip rsvp bandwidth 512 512

interface GigabitEthernet3/0/1
 description P2-PE4 copper
 dampening
 mtu 1600
 ip address 192.168.24.4 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 speed 1000
 no negotiation auto
 mpls ip
 no mpls ldp igp sync
 bfd interval 100 min_rx 100 multiplier 3

interface GigabitEthernet3/0/2
 description ASA5510 Kalaverkkoon
 no ip address
 speed 1000
 no negotiation auto
 ipv6 address 2A00:1DD0:100:F001::1/64
 ipv6 enable
```

```
interface GigabitEthernet3/0/3
 mtu 1600
 no ip address
 speed 1000
 no negotiation auto
 service instance 140 ethernet
  encapsulation dot1q 69
  xconnect 172.30.0.3 140 encapsulation mpls

 service instance 141 ethernet
  encapsulation dot1q 150
  xconnect 172.30.0.3 141 encapsulation mpls

 service instance 142 ethernet
  encapsulation dot1q 160
  xconnect 172.30.0.3 142 encapsulation mpls

 service instance 143 ethernet
  encapsulation dot1q 167
  xconnect 172.30.0.3 143 encapsulation mpls

router ospf 1
 auto-cost reference-bandwidth 10000
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet3/0/0
 no passive-interface GigabitEthernet3/0/1
 no passive-interface GigabitEthernet3/0/4
 network 172.16.50.0 0.0.0.3 area 0
 network 172.21.99.0 0.0.0.255 area 0
 network 172.30.0.0 0.0.0.255 area 0
 network 172.30.101.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
 bfd all-interfaces
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

router bgp 65001
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor SISAVERKKO peer-group
 neighbor SISAVERKKO remote-as 65001
 neighbor SISAVERKKO update-source Loopback0
 neighbor SISAVERKKO version 4
 neighbor 10.0.0.2 remote-as 65100
 neighbor 10.0.0.2 version 4
 neighbor 172.30.0.3 peer-group SISAVERKKO
 neighbor 172.30.0.5 peer-group SISAVERKKO
 neighbor 172.30.0.6 peer-group SISAVERKKO
 neighbor 172.30.0.7 remote-as 65001
 neighbor 172.30.0.7 update-source Loopback0
 neighbor 172.30.0.8 remote-as 65001
 neighbor 172.30.0.8 update-source Loopback0

 address-family ipv4
  network 172.30.0.0 mask 255.254.0.0
  neighbor 10.0.0.2 activate
  neighbor 172.30.0.3 activate
  neighbor 172.30.0.5 activate
  neighbor 172.30.0.6 activate
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.8 activate
 exit-address-family

 address-family ipv6
  redistribute connected
  network 2A00:1DD0:100:B1::/64
  network 2A00:1DD0:100:B2::/64
  network 2A00:1DD0:100:100::/56
  neighbor SISAVERKKO send-label
  neighbor 172.30.0.3 activate
 exit-address-family

 address-family vpnv6
  neighbor 172.30.0.7 activate
  neighbor 172.30.0.7 send-community extended
  neighbor 172.30.0.8 activate
  neighbor 172.30.0.8 send-community extended
 exit-address-family

 address-family ipv6 vrf CUSTOMER_C1
  redistribute connected
  redistribute static
 exit-address-family

no ip http server
no ip http secure-server
ip pim ssm default
ip route profile
ip route 172.30.0.0 255.255.255.0 Null0
ip route 172.30.2.0 255.255.255.0 172.30.1.1
ip route 172.31.2.0 255.255.255.0 172.31.1.1

ip explicit-path name pe4top1tope3 enable
 next-address 192.168.13.1
 next-address 192.168.13.3

logging esm config
ipv6 route 2A00:1DD0:100:B1::/64 Vlan10 FE80:A1::1
ipv6 route 2A00:1DD0:100:B2::/64 Vlan20 FE80:A2::1
ipv6 route 2A00:1DD0:100:100::/56 GigabitEthernet3/0/2
2A00:1DD0:100:F001::2
ipv6 route vrf CUSTOMER_C1 2A00:1DD0:100:10C3::/64
2A00:1DD0:100:F310::2
ipv6 router ospf 6

mpls ldp router-id Loopback0 force

control-plane

line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 session-timeout 60
 login local
 transport input ssh
line vty 5 15
 session-timeout 60
 login local
 transport input ssh

end
```

```
N1KV# sh run

!Command: show running-config
!Time: Wed Nov 14 23:58:57 2012

version 4.2(1)SV1(5.2)
no feature telnet

username admin password 5
$1$XwLyxOKW$YlUdQSp2SlTBWFJwvAkgK1  role
network-admin

banner motd #Nexus 1000v Switch#

ip domain-lookup
ip host N1KV 192.168.128.103
switchname N1KV
errdisable recovery cause failed-port-state
ip access-list www
  10 permit tcp any any eq www
vem 3
  host vmware id 44454c4c-5900-1044-8037-
c3c04f53334a
vem 4
  host vmware id 44454c4c-5900-1044-8037-
c4c04f53334a
snmp-server user admin network-admin auth
md5 0x5782c74d9f1506f258de49f4939f6d2a
 priv 0x5782c74d9f1506f258de49f4939f6d2a
localizedkey

vrf context management
vlan 1,69,150,160,170
vlan 1
vlan 69
  name haukiverkko
vlan 150
  name Nexus_Control
vlan 160
  name Nexus_Management
vlan 170
  name Nexus_Packet

port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile default port-binding static
port-profile type ethernet
Unused_Or_Quarantine_Uplink
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V
internal usage. Do not use.
  state enabled
port-profile type vethernet
Unused_Or_Quarantine_Veth
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V
internal usage. Do not use.
  state enabled
port-profile type ethernet system-uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1,69,150,160,170
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 150,160,170
  state enabled
port-profile type vethernet Nexux_Control
  vmware port-group
  switchport mode access
  switchport access vlan 150
  no shutdown
  system vlan 150
  state enabled
port-profile type vethernet Nexus_Management
  vmware port-group
  switchport mode access
  switchport access vlan 160
  capability iscsi-multipath
  no shutdown
  system vlan 160
  state enabled
port-profile type vethernet Nexus_Packet
  vmware port-group
  switchport mode access
  switchport access vlan 170
  no shutdown
  system vlan 170
  state enabled
port-profile type vethernet haukiverkko
  vmware port-group
  switchport mode access
  switchport access vlan 69
  no shutdown
  state enabled
port-profile type vethernet www
  vmware port-group
  switchport mode access
  switchport access vlan 69
  ip port access-group www in
  no shutdown
  state enabled
```

```
system storage-loss log time 30
vdc N1KV id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0
maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0
maximum 768
  limit-resource u4route-mem minimum 1
maximum 1
  limit-resource u6route-mem minimum 1
maximum 1
  limit-resource m4route-mem minimum 58
maximum 58
  limit-resource m6route-mem minimum 8
maximum 8


interface port-channel1
  inherit port-profile system-uplink
  vem 3

interface port-channel2
  inherit port-profile system-uplink
  vem 4

interface mgmt0
  ip address 192.168.128.103/24

interface Vethernet1
  inherit port-profile Nexus_Management
  description manager_vm, Network Adapter 1
  vmware dvport 64 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74 c5"
  vmware vm mac 0050.5681.6405

interface Vethernet2
  inherit port-profile haukiverkko
  description VMware VMkernel, vmk0
  vmware dvport 160 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74 c5"
  vmware vm mac 0015.C5F9.E78E

interface Vethernet3
  inherit port-profile Nexus_Management
  description VMware VMkernel, vmk3
  vmware dvport 65 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74 c5"
  vmware vm mac 0050.5679.FA2A

interface Vethernet4
  inherit port-profile haukiverkko
  description VMware VMkernel, vmk0
  vmware dvport 161 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74c5"
  vmware vm mac 0015.C5F9.E6E4

interface Vethernet5
  inherit port-profile Nexus_Management
  description VMware VMkernel, vmk2
  vmware dvport 66 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74 c5"
  vmware vm mac 0050.5675.2856

interface Vethernet6
  inherit port-profile haukiverkko
  description vcenter, Network Adapter 1
vmware dvport 162 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74c5"
  vmware vm mac 000C.29B7.CE8D

interface Vethernet7
  inherit port-profile Nexus_Management
  description vcenter, Network Adapter 2
  vmware dvport 68 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74 c5"
  vmware vm mac 0050.5681.0B94

interface Vethernet9
  inherit port-profile www
  description Ubuntu WWW, Network Adapter 1
  vmware dvport 256 dvswitch uuid "d8 cd 01 50
86 21 70 0b-1f 26 4d b7 b0 5d 74c5"
  vmware vm mac 0050.5681.1446

interface Ethernet3/1
  inherit port-profile system-uplink

interface Ethernet3/2
  inherit port-profile system-uplink

interface Ethernet4/1
  inherit port-profile system-uplink

interface Ethernet4/2
  inherit port-profile system-uplink

interface control0
line console
boot kickstart bootflash:/nexus-1000v-
kickstart.4.2.1.SV1.5.2.bin sup-1
boot system bootflash:/nexus-
1000v.4.2.1.SV1.5.2.bin sup-1
```

```
boot kickstart bootflash:/nexus-1000v-
kickstart.4.2.1.SV1.5.2.bin sup-2
boot system bootflash:/nexus-
1000v.4.2.1.SV1.5.2.bin sup-2
svs-domain
  domain id 150
  control vlan 150
  packet vlan 170
  svs mode L2
svs connection gammak6
  protocol vmware-vim
  remote ip address 192.168.128.106 port 80
  vmware dvs uuid "d8 cd 01 50 86 21 70 0b-1f 26
4d b7 b0 5d 74 c5" datacenter-n
ame Gammak6
  max-ports 8192
  connect
vservice global type vsg
  tcp state-checks
vnm-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level info
```