

Tatu Hirvikoski

# Virtualisoitu palvelinympäristö

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

05.06.2013

Tekijä Otsikko	Tatu Hirvikoski Virtualisoitu palvelinympäristö
Sivumäärä Aika	43 sivua 05.06.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoliikenneverkot
Ohjaajat	yliopettaja Matti Puska Mgr Technical Services Markku Kankaala
<p>Insinöörityön toimeksiantaja on yhdysvaltalainen telekommunikaatiolaitteita valmistava Tellabs Oy. Työssä perehdyttiin virtualisoinnin hyötyihin ja riskeihin sekä selvitettiin käytännössä kuinka virtualisointi vaikuttaa työskentelytehokkuuteen hotline-testausympäristössä.</p> <p>Insinöörityön teoriaosuudessa avataan virtualisointia käsitteenä ja pohditaan sen merkitystä nykypäivän IT-maailmassa sekä perehdytään VMwaren virtualisointiohjelmistoihin.</p> <p>Käytännön osuudessa luotiin laboratorioverkon tarpeisiin kartoitettu määrä virtuaalikoneita sekä testattiin niiden nopeutta ja vikasietoisuutta. Laboratorioprojektin avulla Tellabs pyrkii kartoittamaan virtualisoinnin etuja ja haittoja tulevia laitehankintoja silmällä pitäen.</p> <p>Tellabsilla on käytössä VMwaren virtualisointiohjelmisto vSphere Enterprise Plus edition 5.0. Virtualisoinnin laskentatehon tarjoavat blade-palvelimet ovat Tellabsin IT-osaston hallinnoimia, joten oikeudet toimintojen testaamiseen olivat rajalliset.</p> <p>Projektille määritellyt tavoitteet saavutettiin ja halutut ominaisuudet virtualisoiduissa palvelimissa saatiin toimimaan. Projektin pohjalta on helpompi suunnitella tulevia laitehankintoja teknisen tuotetuen laboratorioympäristöön.</p>	
Avainsanat	virtualisointi, ESXi, vSphere, INM, palvelin

Author Title	Tatu Hirvikoski Virtualized server environment
Number of Pages Date	43 pages 5th June 2013
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Networks
Instructors	Matti Puska, Principal Lecturer Markku Kankaala, Mgr Technical Services
<p>The study examines the risks and benefits of moving to virtualized server environment. The thesis also evaluates how virtualization affects working efficiency using the hotline test environment. The mandator of the thesis was the U.S based telecommunication equipment manufacturer Tellabs Oy.</p> <p>Tellabs uses the VMware vSphere Enterprise Plus product suite, edition 5.0, as virtualization platform. The blade-servers powering the virtualization are administrated by the Tellabs IT department so the rights to test different functionalities were quite limited.</p> <p>In the theoretically section of the thesis virtualization is discussed as a concept and its effect on the modern IT world is analyzed. Some additional functionalities of the VMware product suite are also reviewed and how they boost working efficiency, fault tolerance and overall product value is studied.</p> <p>In the practical section of the thesis, the hardware needs for a hotline-network are mapped and how much virtualization could be utilized is documented. With this project Tellabs wanted to determine the advantages and disadvantages of virtualization to ease the decision making when buying new hardware for the laboratory. Old hardware based servers were tested against the virtualized servers using custom built macro as a benchmarking tool.</p> <p>The project achieved the objectives set and the desired properties of virtualized servers were obtained. On the basis of the project, it is easier to plan for future equipment purchases in laboratory environment.</p>	
Keywords	Virtualization, ESXi, vSphere, INM, Server

## Sisällys

1	Johdanto	1
2	Virtualisointi	2
2.1	Virtualisoinnin toteutus	2
2.1.1	Täysvirtualisointi	3
2.1.2	Paravirtualisointi	4
2.2	Virtualisoinnin historia	4
2.3	Virtualisoinnin nykytilanne	6
2.4	Virtualisoinnin ja emuloinnin erot	7
2.5	Virtualisoinnin hyödyt	8
2.6	Virtualisoinnin haasteet ja riskit	10
3	Tellabsin verkkolaitteet ja verkonhallintatyökalut	12
3.1	N-1 Hotline verkon laitekoonpano	12
3.2	N-1 Verkkoelementit	19
4	VMware ohjelmistot	23
4.1	VMware vSphere product suite	23
4.2	Virtuaaliset levyjärjestelmät	28
4.3	Virtuaalikytkin	30
5	Toteutus	32
5.1	Ohjeistusta hotline-verkon suunnitteluun	33
5.2	Mallipohjan luonti	34
5.3	Virtuaalipalvelimen käyttöönotto ja suorituskyvyn määrittäminen	35
5.4	INM-roolit ja asennus	36
5.5	Suorituskykymittaukset	38
5.6	Virtualisointiprojektin haasteet	40
5.7	Vikatilanteesta toipuminen	41
6	Yhteenveto	43
	Lähteet	44

## Lyhenteet

AMD-V	<i>AMD Virtualization.</i> AMD:n kehittämä laitetason tuki virtualisoinnille.
CLI	<i>Command Line Interface.</i> Komentoliittymä, joka mahdollistaa käskyjen syöttämisen hallinoitavalle laitteelle.
CMS	<i>Conversational Monitor System.</i> IBM:n kehittämä varhainen versio hypervisorista.
CPU	<i>Central Processing Unit.</i> Tietokoneen keskusyksikkö.
CIR	<i>Customer Introduction Release.</i> Ohjelmistoversio, joka julkaistaan ainoastaan tietyille asiakkaille ennen virallista julkaisuajankohtaa.
GA	<i>General Availability.</i> Yleisesti asiakkaille saatavilla oleva ohjelmistoversio
DEP	<i>Data Execution Prevention.</i> Turvaominaisuus, jolla estetään ohjelmistoa ajamasta koodia muistin alueelta, mistä ei normaalisti voi lukea tietoa.
DNS	<i>Domain Name System.</i> Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
DPM	<i>Distributed Power Management.</i> VMwaren virransäästöön suunnattu järjestelmä, joka tehon tarpeen mukaan käynnistää tai sammuttaa fyysisiä palvelinlaitteita.
DRS	<i>Distributed Resource Scheduler.</i> VMwaren järjestelmä, joka dynaamisesti ohjaa laiteresurssien käyttöä eri palvelimien välillä.
ESXi	<i>Virtualization Platform.</i> VMwaren kehittämä virtualisointialusta.
FC	<i>Fibre Channel.</i> Verkkotallennusjärjestelmissä gigabittisillä yhteyksillä usein käytetty teknologia.
HA	<i>High Availability.</i> Tietojärjestelmien suunnittelussa käytettävä käytäntö, jolla pyritään aina käytettävissä olevaan järjestelmään.

HW	<i>Hardware.</i> Laitetaso eli koneen fyysiset komponentit.
INM	<i>Intelligent Network Manager.</i> Tellabsin kehittämä verkonhallintaohjelmisto.
Intel-VT	<i>Intel Virtualization Technology.</i> Intelin kehittämä laitetason tuki virtualisoinnille.
I/O	<i>Input-Output.</i> Tarkoittaa sekä tiedon siirtämistä tietokonelaitteiston ja komponenttien välillä että myös siirräntälaitteita.
kbps	Kilobittiä sekunnissa, tiedonsiirtonopeuden mittayksikkö.
LAN	<i>Local Area Network.</i> Rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko.
MAC	<i>Media Access Control.</i> Verkkosovittimen Ethernet-verkossa yksilöivä osoite.
NAS	<i>Network Attached Storage.</i> Verkkoon liitetty tallennusjärjestelmä.
NMRS	<i>Tellabs 8000 Network Manager Resilience Service.</i> Tellabsin kehittämä ratkaisu virhetilanteesta palautumiseen.
OS	<i>Operating System.</i> Käyttöjärjestelmä
SW	<i>Software.</i> Tietokoneohjelma
SAN	<i>Storage Area Network.</i> Tallennusverkko, joka koostuu useista NAS-laitteista. Arkkitehtuuri tiedostopalvelimien yhdistämiseksi.
SCSI	<i>Small Computer System Interface.</i> Protokolla tiedon välittämiseen tietokoneen ja oheislaitteen välillä.
SNMP	<i>Simple Network Management Protocol.</i> TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla.

SRM	<i>Site Recovery Manager.</i> VMwaren kehittämä järjestelmä, jolla voidaan replikoida ohjelmistoja ja siirtää ohjelmistot toiselle palvelimelle.
SSC	<i>Single Server Configuration.</i> Yhden palvelimen kokoonpanolla ajettava INM toimintaympäristö.
STP	<i>Spanning Tree Protocol.</i> Verkkoprotokolla, joka estää silmukoiden syntymisen kytkinten välille.
TAC	<i>Tellabs Technical Assistance Center.</i> Tellabsin tekninen tuotetuki.
USB	<i>Universal Serial Bus.</i> Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen.
VMFS	<i>Virtual Machine File System.</i> VMwaren kehittämä tiedostojärjestelmä virtuaalikoneiden levykuvauksille sekä snapshot-tiedostoille.
VM	<i>Virtual Machine.</i> Virtuaalikone.
VPN	<i>Virtual Private Network.</i> Tekniikka, jolla kaksi tai useampia yrityksen verkoista voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

## 1 Johdanto

Opinnäytetyön toimeksiantaja on yhdysvaltalainen Tellabs Oy. Yhtiön liiketoimiala on televerkkolaitteiden kehitys. Vuonna 1993 Tellabs osti espoolaisen 1976 perustetun Martis Oy:n. Suomessa Tellabsilla työskentelee yhteensä noin 450 työntekijää, joista suurin osa toimii tuotekehitystehtävissä. Yritys suunnittelee, kehittää ja valmistaa tietoliikennereitittimensä itse alusta loppuun. Tellabsilla on varteenotettava asema markkinoilla ja se lukeutuu suurimpiin tietoliikennereititinvalmistajiin. Tellabsin asiakaskunta muodostuu pääosin kansainvälisesti merkittävistä teleoperaattoreista ympäri maailmaa. [1.]

Insinöörityö on suunniteltu ja toteutettu Tellabs Oy:n Suomen yksikköön. Idea virtualisointiin tuli työnantajan toimesta. Osastomme TAC (*Tellabs Technical Assistance Center*) Tier 2 on luopumassa useista vanhoista fyysisistä palvelimista ja tilalle on hankittu keskitettyä laskentatehoa blade-palvelimien muodossa. Laskentateho on tarkoitus allokoida useiden virtuaalipalvelimien käyttöön.

Palvelinvirtualisointiprojektissa on tarkoitus hyödyntää yrityksessä jo käytössä olevaa virtuaalikoneverkkoa ja virtualisoida verkkolaboratorion hotline-verkkoympäristön hallinto- ja kommunikointipalvelimet, jotka toimivat tällä hetkellä fyysisillä palvelinlaitteilla. Työssä käydään läpi verkon käyttöönotto ja sen tuomat hyödyt sekä mahdolliset haasteet. Työssä avataan myös tarkemmin virtualisoinnin käsitettä teoriatasolla.

Tellabsilla on jo käytössä VMware ESXi 5.0:lla toteutettu virtuaaliympäristö, mutta virtuaalipalvelimia ei ole vielä otettu käyttöön TACin hotline-verkoissa. Hotline-verkolla tarkoitetaan pienehköä eristettyä verkkoaluetta, jossa on kiinteä laitekoonpano verkkoreitittimiä sekä palvelinkoneita. TAC:lla on käytössä kolme hotline-verkkoa ja neljännen hankinta on työn alla. TAC-insinöörit pyrkivät uudelleenluomaan asiakkaan kohtaamat ongelmat laboratorioympäristössä ja tätä varten heillä on käytettävissä hotline-verkot, missä asiakasverkon toimintaa pystytään simuloimaan. Asiakasverkoissa saattaa olla käytössä mikä tahansa INM (*Intelligent Network Manager*)-verkonhallintatyökalun ohjelmistoversioista, joten jokaiselle tuetulle versiolle



on luotu oma hotline-verkko. Työn toiminnallinen osuus tehtiin toimeksiantajan tiloissa sen tarjoamalla laite- ja ohjelmistoresursseilla.

## 2 Virtualisointi

### 2.1 Virtualisoinnin toteutus

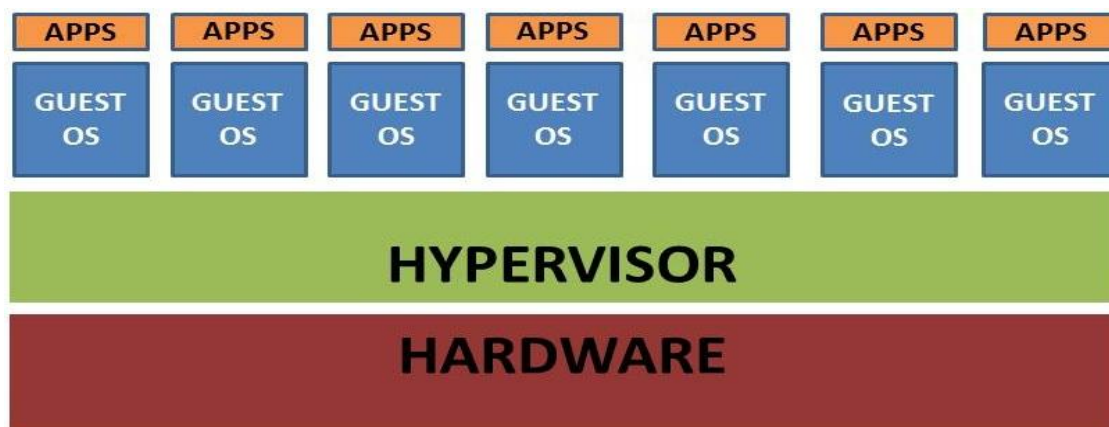
Virtualisointi on tietokoneen laitteiston jakamista moninkertaisiin toteutusympäristöihin käyttämällä yhtä tai useampaa konseptia tai teknologiaa, kuten laitteiston tai ohjelmiston jakamista, osituskäyttöä, osittaista tai täydellistä tietokoneen simuloimista tai jäljittelemistä. [18.]

Virtualisointi hyödyntää käytävissä olevaa jaettua laskentatehoa sekä tallennuskapasiteettiä, joka mahdollistaa käyttöjärjestelmän asentamisen laitteistoon, jota ei fyysisesti ole olemassa. Samalla fyysisellä laitteistolla virtualisoidut tietokoneet voivat toimia yhteisessä ympäristössä tai täysin erillään toisistaan. Virtuaalikoneelle asennetusta käyttöjärjestelmästä käytetään nimitystä vieraskäyttöjärjestelmä. [9.]

Palvelinten keskittäminen ja tehokas resurssien jakaminen ovat nykypäivän edelleen nouseva trendi IT-alalla. Virtuaalikoneet ovat houkutteleva ratkaisu etenkin palvelimia silmällä pitäen. Hypervisorin eli virtualisointikerroksen avulla jokaiselle virtuaalikoneelle luodaan illuusio, jossa kone luulee olevansa täysin dedikoitu ja muista virtuaalikoneista eristetty fyysinen suoritin. Täysvirtualisointiohjelmistot mahdollistavat fyysisten palvelinlaitteiden korvaamisen virtuaalisilla versioilla lähes olemattomalla suorituskykyerolla. Hallinnointi helpottuu ja säästöjä syntyy, kun useampi pieni palvelinlaite saadaan keskitettyä muutamaaan paljon laskentatehoa tarjoavaan yksikköön. [7;18.]

### 2.1.1 Täysvirtualisointi

Virtualisointitekniikat on jaettu kahteen päätyyppiin, ensimmäisen tyyppin virtualisoinnilla tarkoitetaan täysvirtualisointia ja toisen tyyppin virtualisoinnilla paravirtualisointia. Ensimmäisen tyyppin järjestelmä ei vaadi toimiakseen isäntäkäyttöjärjestelmää, jonka päälle vieraskäyttöjärjestelmät asennettaisiin. Vieraskäyttöjärjestelmien hallinnoinnista ja kommunikoinnista laskentatehon tarjoaman laitteiston kanssa vastaa hypervisor (virtualisointikerros). Ensimmäiset hypervisorit olivat IBM:n 1960-luvulla kehittämät CP/CMS sekä testityökalu SIMMON. Moderneja hypervisoreita on tarjolla useamman yrityksen toimesta muunmuassa Oracle VM Server, Citrix XenServer, Microsoft Hyper-V sekä VMware ESXi. Hypervisor antaa komennot laitetasolle kääntämättä tai emuloimatta koodia tapahtuman aikana ja tästä syystä virtuaalipalvelimet kykenevät keskustelemaan suoraan fyysisen laitteiston kanssa kierrättämättä komentoja isäntäkäyttöjärjestelmän kautta kuten paravirtualisoinnissa. Kuvassa 1 on nähtävissä täysvirtualisoitu arkkitehtuuriratkaisu. [25;15.]

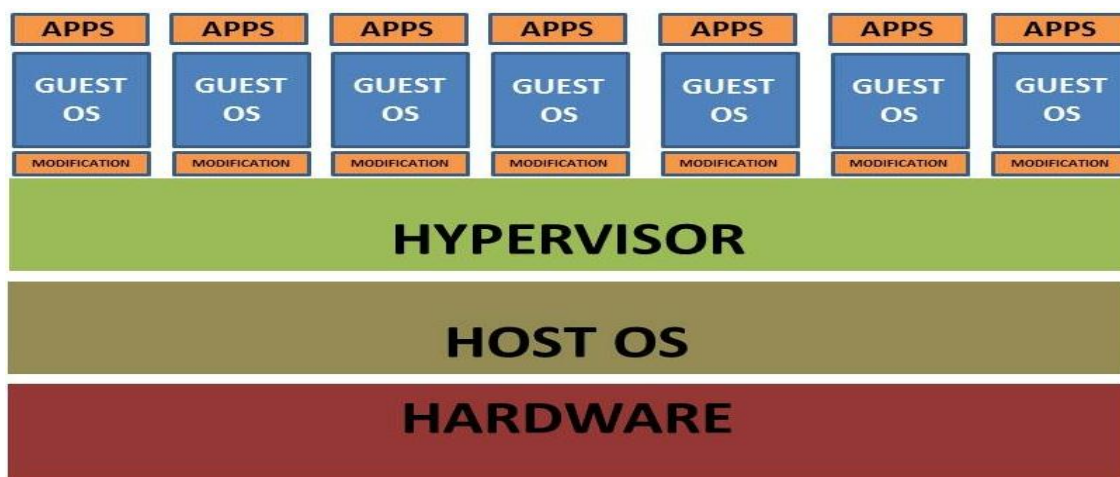


Kuva 1 Täysvirtualisointi [4].

Nykyaikaisilla hypervisoreilla täysvirtualisoidut palvelimet ovat lähes tulkoon yhtä nopeita kuin vertailukohteina käytetyt fyysiset palvelimet. Täysvirtualisointi vaatii fyysisen keskusyksikön, joka tukee virtualisointia laitetasolla. Intel-VT tai AMD-V ovat nykyisin tuettuna kaikissa markkinoilta löytyvissä keskusyksiköissä ja myöskin vanhemmissa malleissa tuki löytyy todennäköisesti, koska tekniikka lähti yleistymään hurjaa vauhtia vuodesta 2006 eteenpäin. [18;15.]

### 2.1.2 Paravirtualisointi

Paravirtualisoinnissa asennetaan isäntäkäyttöjärjestelmä laskentatehon tarjoaman laitteiston päälle. Hypervisor hallinnoi virtuaalikoneita toimien isäntäkäyttöjärjestelmän ja vieraskäyttöjärjestelmien välisessä kerroksessa. Paravirtualisointiratkaisua käyttäviä ohjelmistoja ovat mm. VMware Workstation ja VirtualBox. Paravirtualisointiohjelmat ovat äärimmäisen helppoja asentaa sekä yleensä ilmaisia ja tukevat isäntäkäyttöjärjestelmänä joko Windowsia tai Linuxia. Yrityskäyttöön suositellaan kuitenkin täysvirtualisoituja ohjelmistoratkaisuja niiden keskitetyn hallittavuuden vuoksi. Kuvassa 2 on esitelty paravirtualisoitu kerrosrakenne. [10;11;20.]



Kuva 2 Paravirtualisointi [4].

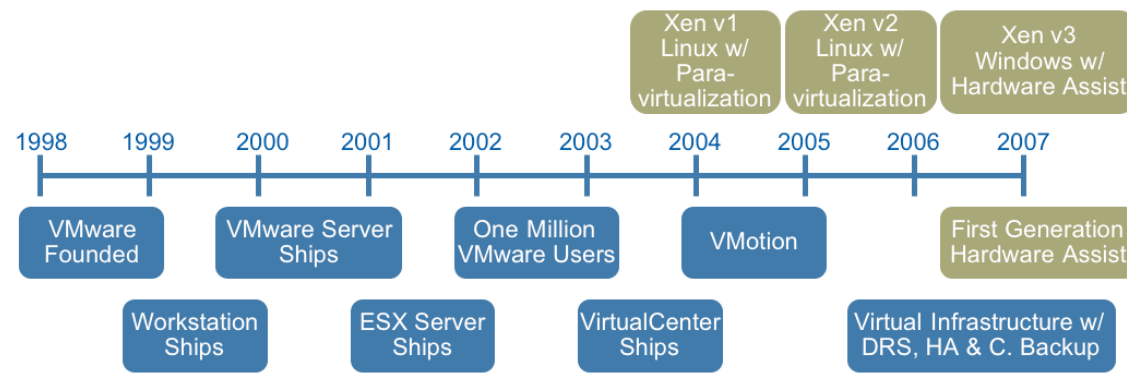
### 2.2 Virtualisoinnin historia

Virtualisointi on saavuttanut nykyisen valtaisan suosion etenkin palvelinpuolella hyvin pitkälti VMwaren kehittämän x86- ja x86-64-arkkitehtuureille yhteensopivan ohjelmistoratkaisun myötä. Virtualisointi ei ole käsitteenä mikään uusi asia vaan siihen liittyviä projekteja käynnisteltiin jo 1960-luvun lopulla. Tuohon aikaan korkean suorituskyvyn tietokoneen hinta liikkui miljoonissa dollareissa eikä kotikone-käsitettä vielä ollut keksitty. Suurista kustannuksista haluttiin ottaa irti maksimaalinen hyöty, ja ratkaisuksi kaavailtiin saman suurkoneen sisällä tapahtuvia rinnakkaisia laskutoimituksia eri osioiden sisällä, jolloin kapasiteetti saatiin hyödynnettyä tehokkaammin. [27.]

1960-luvulla usean yliopiston yhteistyössä kehittämä Atlas ja IBM:n M44/44X olivat ensimmäisiä tietokoneita, joissa käytettiin professori Christopher Stracheryn kehittämää Time Sharing -tekniikkaa. Time Sharingia voidaan pitää virtualisoinnin esiasteena, sillä se mahdollisti multiohjelmoinnin. Multiohjelmoinnissa yksi ohjelmoija tuottaa omassa konsolissaan koodia, jota toinen ohjelmoija tarkistaa virheitä etsien käyttämällä samaa laskentayksikköä mutta syöttää käskyt henkilökohtaisesta konsolistaan. Atlas-supertietokone oli ensimmäinen virtuaalista muistia hyödyntävä laite.

1960-luvun lopulla IBM kehitti System/360 tietokoneelle CP-40-käyttöjärjestelmän, jolla oli mahdollista ajaa yhtäaikaisesti useaa täysin virtualisoitua käyttöympäristöä. Virtual Machine Monitor (VMM) on ohjelmistokerros, joka virtualisoi fyysiset laitteistoresurssit ja valjastaa vieraskäyttöjärjestelmälle fyysisiä resursseja kuvastavan virtuaalisen laiterajapinnan. CP-40 simuloi alla pyörivän laitetason laitteistoa vieraskäyttöjärjestelmille (mm. täydellinen käskykanta, I/O-operaatiot, keskeytykset, muistinkäyttö sekä kaikki elementit mitä normaali käyttöjärjestelmäinstanssi vaatisi) [7.]. IBM System/360 -tietokoneella ajettava CP-67-hypervisor oli ensimmäinen laajemmin kaupallisesti saatavilla oleva virtuaalikoneeratkaisu, jossa jokaisella käyttäjällä oli oma CMS-instanssi eli yhden käyttäjän hallinnoima käyttöjärjestelmä. CP-67 hypervisor tarjosi laskentaresurssit sekä jokaiselle käyttäjälle allokoitun virtuaalimuistin, ja CMS mahdollisti time-sharing ominaisuudet. [12;27.]

VMware-yhtiö perustettiin vuonna 1998. Perustajajäseniä olivat Diane Greene ja hänen miehensä tohtori Mendel Rosenblum sekä kaksi opiskelijaa Stanfordin yliopistosta. Samana vuonna yrityksen perustajat hakivat patenttia uusille virtualisointitekniikoille, jotka pohjautuivat Stanfordin yliopistossa tehtyihin tutkimuksiin. Moderneista virtualisointiohjelmistoista ensimmäisenä markkinoille saapui 1999 VMwaren Workstation 1.0. Workstation 1.0 oli ensimmäinen virtualisointiohjelma, joka osasi hyödyntää x86-proessoriarkkitehtuuria, ja siinä oli tuki Windowsille sekä Linuxille. Virtualisoinnin juuret löytyvät IBM:stä mutta virtualisointi nousi valtavirran suosioon vasta, kun VMware toi virtualisoinnin x86-proessoriarkkitehtuurille. X86-arkkitehtuuriin siirryttäessä virtualisointi helpottui suuresti, koska virtualisointiratkaisu ei enää vaadikaan varta vasten sille suunniteltua isäntäkäyttöjärjestelmää kuten IBM:n kulta-aikoina. [14;27.]



Kuva 3 x86 virtualisoinnin aikajana [20].

Intelin ja AMD:n keskusyksiköissä ei alun perin ollut huomioitu virtualisointia mitenkään suoritinarkkitehtuuria suunnitellessa. X86-käskykannan ongelmallisimmat käskyt jouduttiinkin aluksi korvamaan virtualisointiohjelmissä toteutetuilla emuloinneilla. Vuonna 2005 julkaistu Intel-VT sekä 2006 AMD-V toivat mukanaan myös laitetason virtualisointituen, mikä yhtenäisti käskykanta ja nopeutti virtualisointiohjelmien ajamista merkittävästi. Kuvasta 3 on nähtävissä, kuinka virtualisointiohjelmistot rupesivat hyödyntämään laitetason tukea vuodesta 2007 eteenpäin. Virtualisoinnin toteuttamiseen ei enää tarvittu täydellistä isäntäkäyttöjärjestelmää, vaan kevyt ja kompakti virtualisointikerros, jota VMware kutsui hypervisoriksi. Nykyään kolme yleisimmin käytössä olevaa virtualisointiohjelmistoa ovat VMwaren lisäksi Microsoftin Windows Server 2008:n yhteydessä lanseeraama Hyper-V sekä Linux-lähtöinen Oracle VM. Kaikki kolme edellämainittua virtualisointiohjelmistoa tukevat sekä Windows että Linux vieraskäyttöjärjestelmiä. [8; 16; 27.]

### 2.3 Virtualisoinnin nykytilanne

Ajanjaksolla 2008—2012 virtualisointi on ollut IT-alan infrastruktuuriratkaisuihin ja käyttötoimintoihin syvimmin vaikuttanut ilmiö. 1990-luvulla Internetin laajenemisen myötä palvelinkeskusten fyysisten palvelimien määrä lähti eksponentiaaliseen kasvuun, mikä taas loi kysyntää yhä suuremmille ja suuremmille konesalihalleille. Nykyään varsinkin palvelinkeskukset ovat omaksuneet virtualisoinnin salat ja vaativat asiakkailta mahdollisesti erityisperusteluja fyysistä palvelinta tilattaessa. Virtualisointiratkaisut soveltuvat niin suurille kuin pienillekin yrityksille yksittäisiä käyttäjiä unohtamatta. Perustietokoneen keskusmuistin ja prosessoriytimien lisääntynyt määrä mahdollistaa usean virtuaalikoneen ajamisen tavallisella koti-pc:llä.

Hypervisoreita myydään nimelliseen hintaan tai tarjotaan ilmaiseksi ladattavina versioina. Näillä voi toteuttaa yhden fyysisen palvelimen virtualisointiratkaisuja. Voitollinen liiketoiminta rakennetaankin lisäarvoa tuovien hallintaohjelmistojen ja palvelujen varaan. [7.]

#### 2.4 Virtualisoinnin ja emuloinnin erot

Virtualisointi ja emulointi jakavat samoja piirteitä, mutta suorituskyky näiden tekniikoiden välillä on suuri virtualisoinnin eduksi. Emuloitaessa ohjelma muuntaa ajettavan koodin ja arkkitehtuurin emuloitavalle käskykannalle sopivaksi. Emulointi mahdollistaa esimerkiksi Android-ohjelmien ajamisen Windowsista käsin ajamalla ensin Android-sovellukset Windowsissa pyörivän emulointiohjelman läpi, jolloin koodi muuntuu luettavaksi kahden eri arkkitehtuurin välillä. Virtualisoinnilla pyritään ennemminkin asettamaan virtuaalisia rajoja useiden samalla fyysisellä alustalla ajettavien käyttöjärjestelmien välille. Virtualisoitavat käyttöympäristöt perustuvat lähes aina samaan prosessoriarkkitehtuuriin kuin fyysinen alusta, mikä tarjoaa niille laskentatehon. Tästä syystä koodi ajetaan natiivisti eli sitä ei tarvitse muuntaa toiselle arkkitehtuurille ymmärrettävään muotoon, jolloin saavutetaan huomattava nopeusero emulointiin verrattaessa.

Emuloinnilla pyritään saamaan tietyn käskykannan käyttöjärjestelmä käyttäytymään kuin eri käskykantaan perustuva käyttöjärjestelmä. Emulointi mahdollistaa täysin epäyhteensopivan käskykannan ohjelmien ajamisen ympäristössä, joka ei ole millään tasolla suunniteltu tehtävää varten. Emuloinnin yhteydessä tapahtuvat käskykantamuutokset kuitenkin verottavat järjestelmän nopeutta ja suorituskykyä merkittävästi. Virtualisointiohjelmien rajoitteista mainittakoon esimerkiksi VMware, joka vaatii toimiakseen fyysisen x86-arkkitehtuurin perustuvan PC-alustan. Emulointiohjelmista voidaan ottaa esimerkiksi pSX emulator, mikä mahdollistaa Playstation-pelikonsolille tehtyjen pelien ajamisen PC:llä. [33; 34.]

## 2.5 Virtualisoinnin hyödyt

Palvelimien virtualisoinnilla saavutetaan monia etuja normaaliin fyysiseen palvelinratkaisuun verrattuna. Esimerkkitapaukseksi voidaan ottaa tilanne, jossa yritykseen tarvitaan useita uusia palvelimia. Perinteisesti hanke lähtee liikkeelle, kun IT-osasto tilaa uudet palvelimet ja odottaa osien saapumista, jonka jälkeen päästään asentamaan palvelimet palvelinkaappeihin ja kaapeloimaan ne. Tämän jälkeen voidaan asentaa tarvittavat käyttöjärjestelmät ja päivittää ne uusimpaan versioon sekä asentaa palvelimissa käytettävät ohjelmistot, jonka jälkeen viimein päästään käyttämään palvelimia. Toinen lähestymistapa on käyttää virtualisointia ja allokoida uusille palvelimille tarvittava määrä laskentatehoa ja keskusmuistia, jonka jälkeen asennetaan käyttöjärjestelmä ja päivitykset yhdelle virtuaalikoneelle sekä tehdään kyseisestä koneesta template. Tätä templatea käyttäen voidaan helposti luoda joukko vastaavia palvelimia muutamassa minuutissa. Myös käytössä olevan palvelimen ohjelmistopäivitys voidaan huoletta suorittaa kunhan tallennetaan koneen nykyinen tila snapshot-toiminnolla ennen päivittämistä. Mahdollisen vikatilanteen ilmetessä voidaan helposti palauttaa palvelin päivitystä edeltävään tilaansa eikä ohjelmistoja tarvitse asentaa uudelleen. [2.]

Laitetasolla tuettu virtualisointi yhdenmukaistaa käskykanta Hypervisorin kanssa, jolloin käskyjä ei tarvitse erikseen kääntää. Laitetasolla tuettu virtualisointi esiteltiin ensimmäisen kerran vuonna 1972 IBM:n virtuaalikonekäyttöjärjestelmässä nimeltä System/370. Vuosien 2005 ja 2006 aikana Intel, AMD sekä Sun Microsystems toivat myös virtualisointituen laiteratkaisuilleen. Nykyisin lähes kaikki myynnissä olevat keskusyksiköt tukevat laitetasolla virtualisointia. [15.]

Muutaman ajanmukaisen palvelinlaitteen ylläpito ja resurssien jakaminen on huomattavasti helpompaa kuin useiden erillisten ja mahdollisesti eri ikäisten palvelimien kanssa toimiminen. Nykyään palvelimien keskusmuistin ja laskentaydinten määrä on kasvanut merkittävästi ja fyysisen palvelimen laskentatehosta saatetaan hyödyntää ainoastaan 10—20% tai jopa vähemmän. Rasittamaton fyysinen palvelin vaatii silti tilaa ja jäähdytystä lähes samoissa määrin kuin rasiattu palvelin. Virtualisoidulla palvelimella voidaan laskentatehosta hyödyntää 80% tai enemmän kuitenkin käyttämättä sen enempää tilaa tai jäähdytystä. Virtualisointi on selkeästi

energiatehokkaampi vaihtoehto yrityksille, koska sama määrä asioita saadaan tehtyä huomattavasti pienemmällä määrällä palvelinlaitteita. [7.]

Virtualisoinnin avulla fyysisten palvelinlaitteiden määrä vähenee huomattavasti ja käytettävissä olevien palvelinlaitteiden käyttöaste saadaan tehokkaammaksi. Virtualisointi on ajankohtainen asia myös ympäristönäkökulmasta katsottuna, sillä palvelinhuoneet kuluttavat paljon sähköä. Fyysisten palvelinlaitteiden väheneminen johtaa myös tila- ja ilmastointitarpeen vähenemiseen, jolloin sähkönkulutus laskee huomattavasti. Virtualisointi myös nopeuttaa ongelmatilanteista toipumista, yksinkertaistaa järjestelmänhallintaa ja mahdollistaa minimaaliset käyttökatkokset. [7.]

Virtualisoinnista saatavat säästöt tulevat hyvin esille, kun tarkastellaan palvelinsovelluksia. Palvelinsovellukset eivät useinkaan kuormita laitteistoa kuin muutaman prosentin edestä, mutta ohjelmistotalot eivät yleensä takaa sovelluksensa toimintaa, jos samalla koneella ajetaan muitakin sovelluksia. Kun jokaiselle sovellukselle annetaan oma käyttöjärjestelmätapahtuma, saadaan samassa koneessa toimivat sovellukset eristettyä toisistaan ja laitteistojen käyttöastetta kohotettua. Tällä toimintamallilla säästöä syntyy muunmuassa laitekustannuksissa, konesalien kehikkotilassa, energiankulutuksessa sekä jäähdytyskuluissa. Nykyisin suurimmat virtualisointiohjelmien kehittäjät kuten VMware, Microsoft ja Oracle tarjoavat ohjelmistojensa perusversiot ilmaiseksi, mutta parempi hallittavuus, skaalautuvuus ja vikasietoisuus saadaan aikaiseksi maksullisilla ohjelmistolisensseillä ja laajennuksilla. Säästöjen realisointi vaatii kuitenkin virtualisointiin perehdytetyn henkilökunnan ja mahdollisesti mittavia remontteja perusratkaisuihin sekä laitekannan uusimista virtualisoinnin laitetasolla mahdollistaviin laitteisiin.

Iso yritys hyötyy virtualisoinnista eniten hallittavuuden ja vikasietoisuuden paranemisen myötä. Kahdennettu tallennusverkko ja virtualisoidut palvelimet tarjoavat katastrofista toipumiseen helpommin määriteltävän ja testattavan tavan. Mitä suurempi määrä fyysisiä palvelimia saadaan keskitettyä virtualisoinnilla, sitä suuremmat säästöt saadaan pidemmällä ajanjaksolla seurattuna. Harva yritys kuitenkaan virtualisoi koko palvelinkantaansa kerralla siitä koituvien suurten kustannusten takia. Yleisin tapa on ottaa virtualisointi käyttöön fyysisten palvelinten rinnalle ja laajentaa virtuaalipalvelimien osuutta pikkuhiljaa.



Pienikin yritys voi hyötyä virtualisoinnista. Itsenäiseen työskentelyyn ja testaamisen riittää varsin hyvin ilmaiseksi tarjolla oleva paravirtualisointiohjelmisto. Esimerkiksi ohjelmistotalo saa virtualisoimalla käyttöönsä joustavat kehitys- ja testausympäristöt huomattavasti edullisemmin kuin fyysisillä palvelimilla toteutettuna. Eri ohjelmistoversioiden ajaminen samalta fyysiseltä laitteelta mahdollistaa todella joustavan testiympäristön. Virtuaaliseen testausympäristöön ei välttämättä ole tarvetta hankkia lisenssejä kaikille käytössä oleville ohjelmille, kun kokeiluversiokin riittää käytön väliaikaisuuden johdosta. VMwaren kehittämä snapshot-ominaisuus on erittäin hyödyllinen ohjelmistotestausta silmällä pitäen, koska sen avulla voidaan helposti testauksen jälkeen palauttaa vieraskäyttöjärjestelmä alkuperäiseen tilaan.

Hyvin suunniteltu ja toteutettu virtuaaliympäristö mahdollistaa palveluiden toimimisen ilman käyttökatkoksia. Esimerkiksi Microsoftin Live Migration sekä VMwaren vMotion mahdollistavat virtuaalikoneiden siirtämisen isäntäkoneelta toiselle ilman käyttökatkoa. Uuden virtuaalipalvelimen käyttöönotto on tehty erittäin helpoksi templatien avulla. Template luodaan olemassa olevasta virtuaalikoneesta ja jatkossa uuden koneen luonti tapahtuu templatea käyttämällä. Uudelle virtuaalikoneelle tarvitsee määrittää isäntäkone, haluttu klusteri, lisenssiavain sekä verkkoasetukset ja loput asennuksesta hoituu automaattisesti. Esimerkiksi palvelinvirtualisointiprojektissa työntekijä oli epähuomiossa poistanut väärän virtuaalikoneen ja korvaavan Windows 2008 Server -käyttöjärjestelmällä varustetun virtuaalikoneen luontiin mallipohjaa käyttäen kului ainoastaan 15 minuuttia. [17.]

## 2.6 Virtualisoinnin haasteet ja riskit

Virtualisointiin siirtyminen on usein haasteellista, kun pyritään ottamaan vanhasta laitteistosta kaikki hyöty irti ja lähdetään käyttämään sitä virtualisoinnissa. Vanhan palvelinlaitteiston muuntaminen virtualisoiduksi laskentatehoksi tulee harvoin kysymykseen 32-bittisen muistiavaruuden takia sekä mahdollisen laitetason virtualisointituen puuttuessa. Virtualisointi vaatii palvelimelta suorituskykyä useamman prosessoriytimen voimin ja varsinkin keskusmuistin määrä on ratkaisevassa asemassa. Koska virtualisoidun laitteiston resurssit allokoidaan usealle erilliselle käyttöjärjestelmäinstanssille, yksi merkittävimmistä pullonkauloista on isäntäpalvelimen keskusmuistin määrä. Tästä syystä on erityisen tärkeää tarkastella 64-bittisen

prosessoriarkkitehtuurin tuomaa hyötyä virtualisoinnissa. 64-bittinen arkkitehtuuri voi käsitellä paljon suurempaa muistiavaruutta kuin 32-bittinen arkkitehtuuri, jossa muistiavaruuden määrä rajoittuu hieman alle neljään gigatavuun. Useita virtuaalikoneita isännöivällä palvelimella voi olla allokoitavanaan kymmeniä gigatavuja keskusmuistia, joten 32-bittisyys ei tule kuuloonkaan. [17, s.46]

Suurempaan skaalaan siirryttäessä virtualisoinnista hyötyäkseen tarvitsee tietenkin tehdä suurempia investointeja lisensseihin ja laitekantaan. Erillinen verkkotallennusratkaisu ei ole halpa investointi eivätkä edistyneempien virtualisointiohjelmien ja hallintatyökalujen lisenssit ole ilmaisia. Virtuaaliympäristöä hallinnoivan henkilökunnan koulutukseen kuuluu myös aikaa ja rahaa. Tuotantoympäristön ohjelmistohankinnoissa ei myöskään synny merkittäviä säästöjä, koska virtuaalikoneissa käytettävät käyttöjärjestelmät ja sovellukset vaativat toimiakseen lisenssit samaan tapaan kuin fyysiseen laitteeseen asennettuna. Ohjelmistotalot ovat kuitenkin heräämässä haasteeseen ja esimerkiksi Microsoft on kehittänyt palvelinohjelmistojensa lisensointia virtualisointiyhtävällisemmäksi. [7.]

Virtuaalikoneita on äärimmäisen helppo ja nopea luoda, mutta täytyy muistaa, että niiden tuhoaminen onnistuu myös muutamalla napsautuksella, joten yrityksen täytyy valvoa tarkkaan, kenellä on pääsy hallinointiohjelmaan. On myös huomioitava, ettei virtualisoitu palvelin kykene tarjoamaan kaikkia ominaisuuksia ja liitäntöjä kuin fyysinen vastaava. Tämä kävi selväksi myös laboratorioprojektissa dxx-palvelimen virtualisointiongelmien yhteydessä.

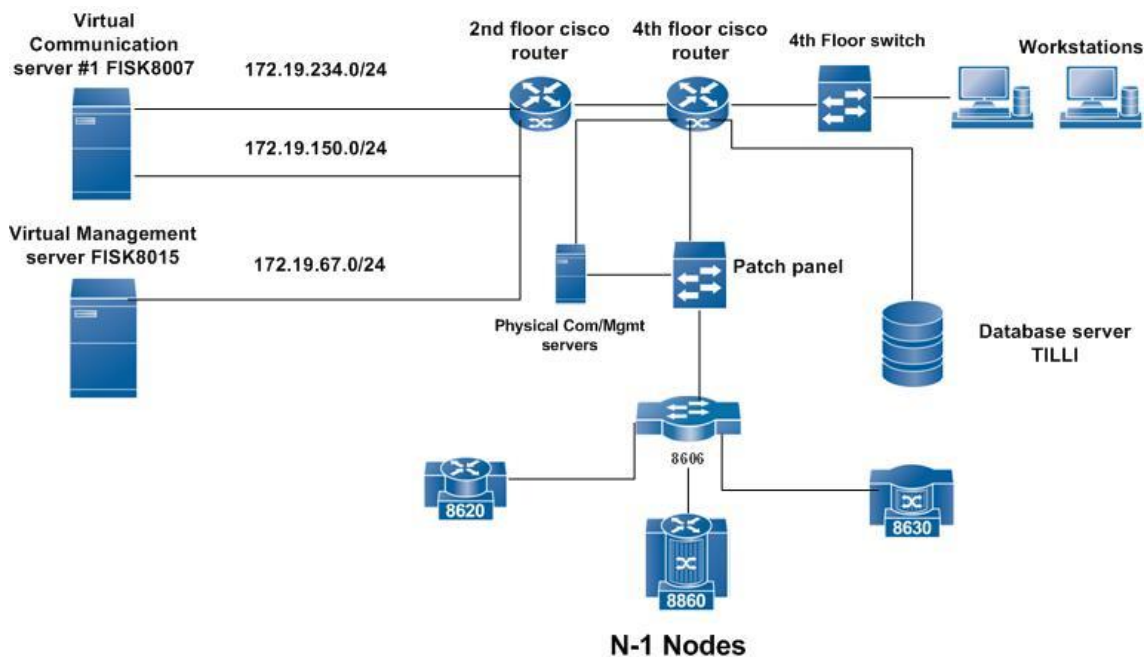
Virtuaalikoneet altistuvat viruksille, madoille sekä troijalaisille siinä missä fyysisten tietokoneet. Saastunut vieraskäyttöjärjestelmä kykenee harvoin levittämään viruksen isäntäkäyttöjärjestelmään mutta sekin onnistuu mikäli isäntä- ja vieraskäyttöjärjestelmillä on käytössä keskenään jaettuja kansioita. Vieraskäyttöjärjestelmän saa eristettyä isäntäkäyttöjärjestelmästä, kun kytketään jaetut kansiot kokonaan pois päältä. Ykköstyyppin virtualisointi eli täysvirtualisointi on erittäin turvallinen tekniikka eikä viruksen leviäminen saastuneesta virtuaalikoneesta ole todennäköistä. Kakkostyyppin virtualisoinnissa eli paravirtualisoinnissa vieraskäyttöjärjestelmällä on mahdollisuus saastuttaa myös isäntäkäyttöjärjestelmä mutta tämä edellyttää molemmilla käyttöjärjestelmille määritettyjen jaettujen kansioden käyttämistä.

### 3 Tellabsin verkkolaitteet ja verkonhallintatyökalut

Tellabsin teknisellä tuotetuella on käytössä kolme hotline-verkkoympäristöä ja neljättä ollaan rakentamassa parasta aikaa. Jokainen hotline-verkko käyttää eri versioita Tellabs Intelligent Network Manager -verkonhallintatyökalusta. Hotline-verkkojen nimeämiskäytäntö noudattaa sääntöä, missä uusimmalla INM-versiolla ajettava verkko on nimeltään N ja vanhemmilla ohjelmistoversioilla asennetut verkot N-1, N-2 jne. Laboratorioprojektissa virtualisoidaan N-1 verkon laitteita ja kyseisessä hotline-verkossa ajettava INM-versio on SR3.0.

#### 3.1 N-1 Hotline verkon laitekoonpano

Virtualisoitu N-1 hotline laboratorioverkko käyttää Tellabs 8000 Intelligent Network Manager -ohjelman SR3.0-versiota. Tellabs 8000 INM SR3.0:n vähimmäislaitevaatimukset hallinointipalvelimelta ovat 64-bittinen käyttöjärjestelmä sekä 8 GB keskusmuistia. Keskusyksikön tehovaatimukset skaalautuvat verkon hallittavien laitteiden määrän mukaan. Eniten laskentatehoa vaativat hallinointipalvelin sekä kommunikointipalvelin. Kumpaankin palvelimeen suositellaan vähintään neliytimistä Xeon-suoritinta tai sitä nopeampaa ratkaisua. Tuetut käyttöjärjestelmät ovat: Windows XP, Windows 7, Windows Server 2003 & 2008 sekä Solaris tietokantapalvelimelle. Kuvassa 4 on esitetty yksinkertaistettu malli, josta käy ilmi virtuaalipalvelimien ja verkkolaitteiden kytkennät. [5; 3.]

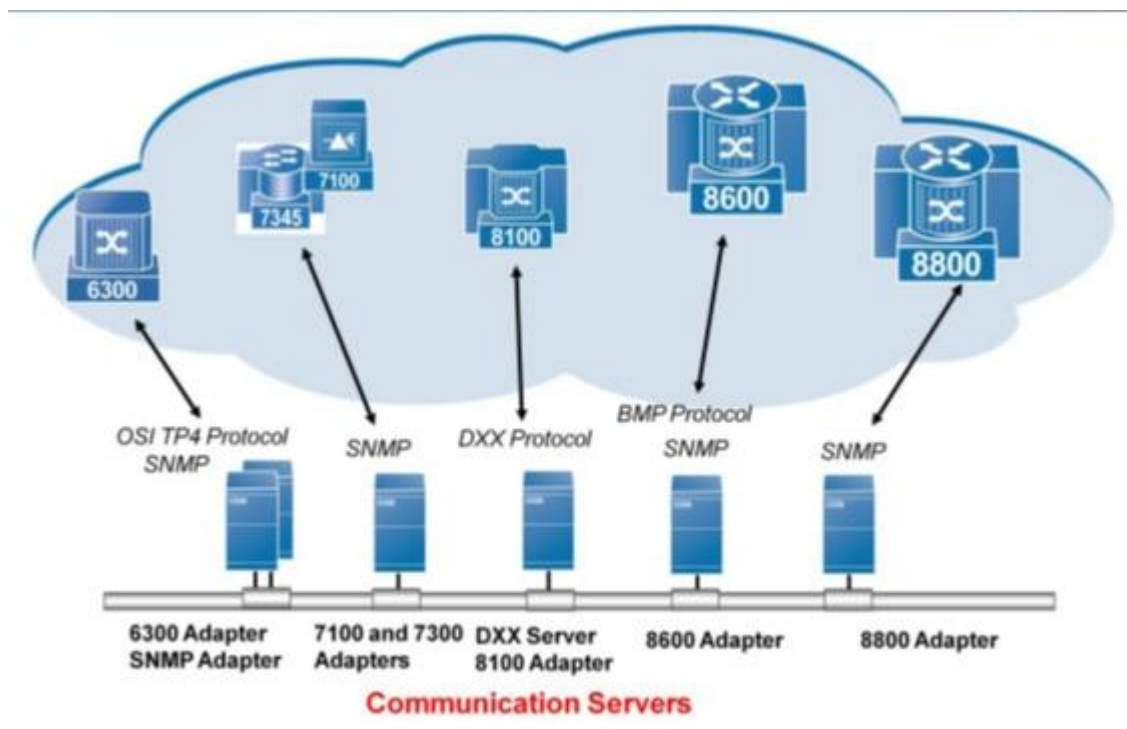


Kuva 1 Hotline N-1 verkkotopologia [4].

### Kommunikointipalvelin

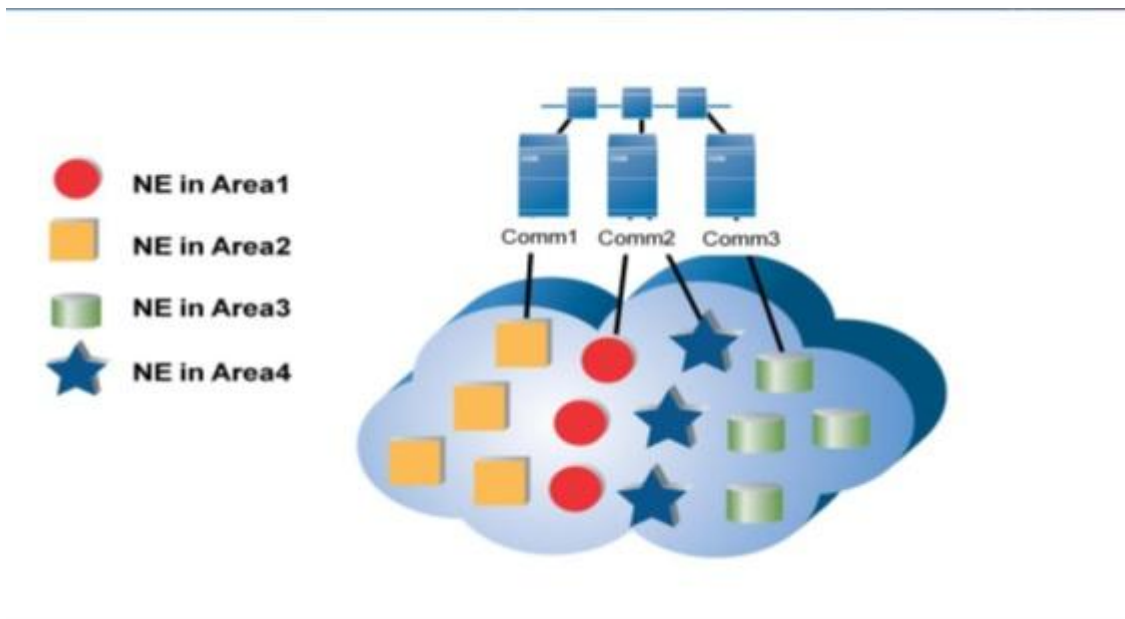
Kommunikointipalvelimella on mahdollista hallinoida Tellabs 5500-, 6300-, 7100-, 7300-, 8600-, 8800- sekä SmartCore 9100 -verkkoelementtejä. Hotline-laboratorioverkossa hallittavien verkkoelementtien määrä on verrattaen pieni ja tuoteperheistä on mukana ainoastaan 6300-, 8100- sekä 8600-sarjan verkkoelementtejä. Käytössä on yksi ensisijainen kommunikointipalvelin sekä fyysinen varapalvelin paremman vikasietoisuuden saavuttamiseksi.

Kommunikointipalvelin lähettää konfiguraatiokomentoja verkkoelementeille, suorittaa vikakyselyitä sekä kerää suorituskykydataa. Kommunikointipalvelimella on oma adapteri jokaista Tellabsin tuoteperhettä varten. Adapterit keskustelevat verkkoelementin kanssa käyttäen kullekin tuoteperheelle määriteltyä protokollaa. Kuvasta 5 on nähtävissä, että yleisimmin käytössä on SNMP (*Simple Network Management Protocol*) -protokolla.



Kuva 2 Kommunikointipalvelimen adapterit [3].

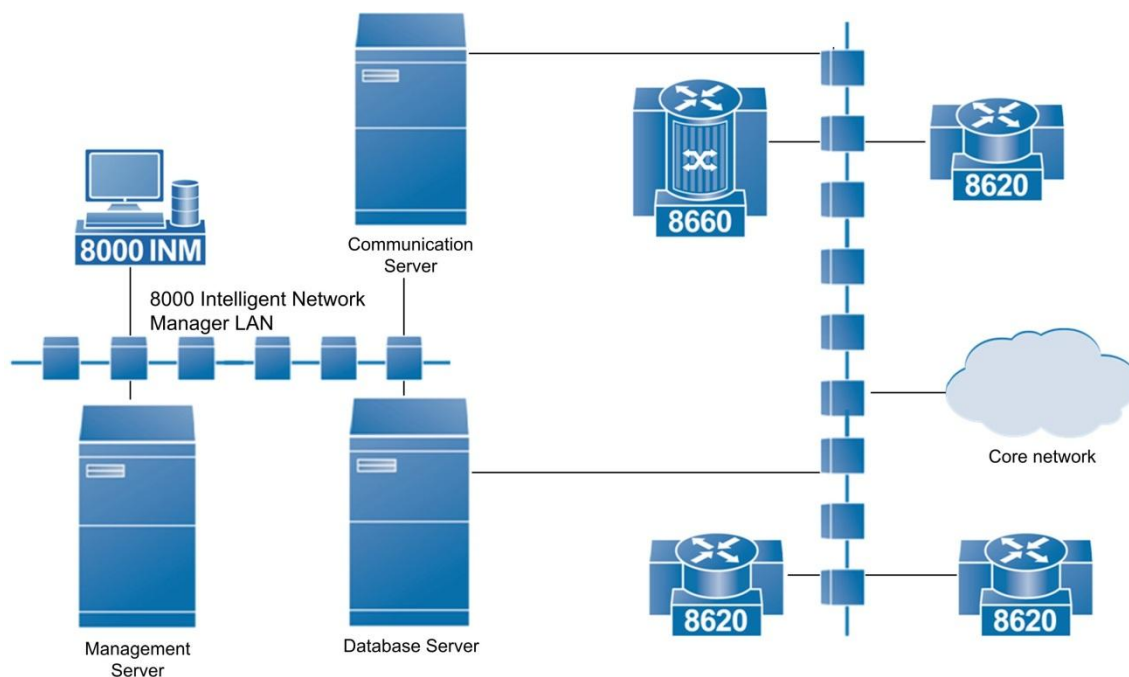
Tellabs 8000 INM -ohjelmassa hallinnoitavat verkkoelementit jaetaan aina ennaltamääräytyihin alueisiin. Kuvasta 6 on nähtävissä, kuinka jokaisella alueella on oma kommunikointipalvelin sekä mahdollisesti varmistava kommunikointipalvelin vikasietoisuuden parantamiseksi. Vikatilanteen sattuessa varmentava kommunikointipalvelin siirtyy automaattisesti hallinnoimaan alueen verkkoelementtejä. Samalla kommunikointipalvelimella voi olla useita eri alueita hallinnoitavana samaan aikaan. [3.]



Kuva 3 Kommunikointipalvelimen alueet [3].

### Hallinnointipalvelin

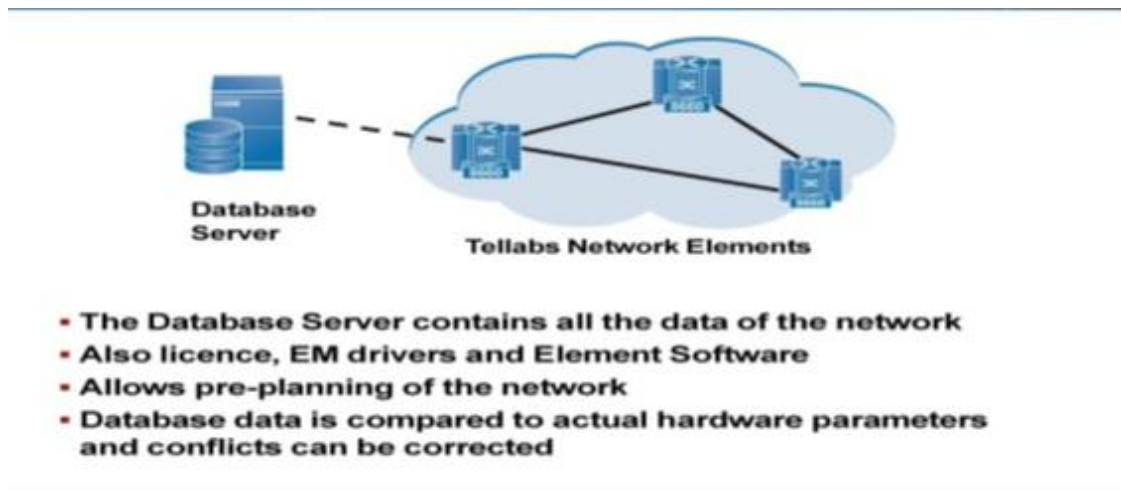
Hallinnointipalvelin toimii runkona Tellabs 8000 INM -ohjelmiston hajautetuille sovelluksille, jotka toimivat kukin omana prosessinaan. Tietyt palvelut on ajettava ainoastaan yhtenä instanssina mutta joitakin palveluita on myös mahdollista suorittaa toiselta palvelimelta varmistavana palveluna tai kuormituksen jako (load balancing)-tekniikkaa käyttäen. Hallinnointipalvelimella ajettavia prosesseja voidaan käynnistää ja sammuttaa helposti käyttämällä Server Command Center -monitorointityökalua, joka listaa palvelimella ajettavat palvelut. Hotline N-1 -verkossa on ensisijaisena käytössä yksi virtualisoitu hallinnointipalvelin ja varalla fyysinen hallinnointipalvelin vikasietoisuuden parantamiseksi. Kuvassa 7 on esitetty tyypillinen palvelinratkaisu 8600-tuoteperheen verkkoelementtien hallinointia varten. [3.]



Kuva 4 Tyypillinen palvelinratkaisu Tellabs 8000 INM-verkkoon [32].

### 3.1.1 Tietokantapalvelin

Tietokantapalvelin sisältää Sybasen relaatiotietokannan, johon kaikki Tellabs 8000 INM -työkalut tallentavat datan. Uudemmat INM-versiot tuovat mukanaan tuen myös Oraclen tietokantaratkaisulle. Tietokantapalvelimen laitteistovaatimukset vaihtelevat verkon koon mukaan mutta kokoonpanon minimivaatimukset x86-arkkitehtuurille ovat Intel Xeon quad-core 2,2 GHz CPU, 8 GB RAM. Mikäli käytössä on Oraclen SPARC-palvelinlaite, minimivaatimukset ovat SPARC VII quad-core CPU ja 8 GB RAM. [3.]



Kuva 5 Tietokantapalvelin [3].

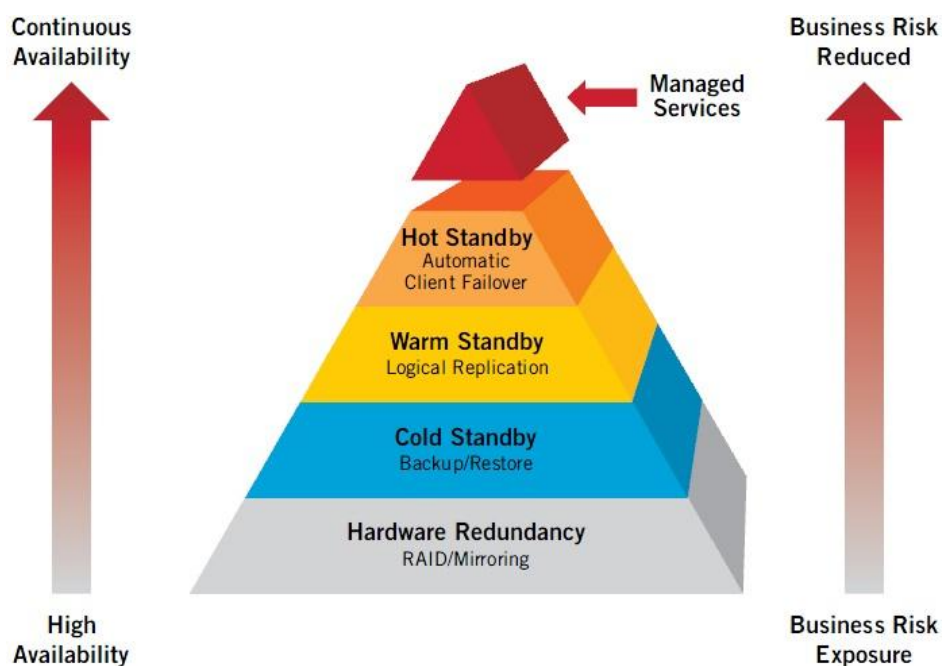
Tellabs 8000 INM -verkkoympäristö vaatii toimiakseen tietokantapalvelimen, joka saattaa olla kahdennettu vikasietoisuuden parantamiseksi. Kuvassa 8 on esitetty yksinkertaistettu malli tietokantapalvelimen sijoittelusta ja päätehtävistä. Tellabs on kehittänyt tietokantapalvelimia silmällä pitäen katastrofista toipumista nopeuttavan NMRS-järjestelmän (Network Manager Resilience Service), joka muodostuu useasta eri tasosta. Jokainen taso on teknisesti edeltäjäänsä haasteellisempi toteuttaa, ja myöskin kustannukset kasvavat vikasietoisuuden paranemisen myötä.

Tellabs 8000 NMRS -järjestelmän ensimmäinen taso eli Cold Standby hyödyntää kahta tietokantapalvelinta, jotka tekevät tietokannoistaan varmuuskopioita jaksotetusti. Kaksi fyysistä palvelinta tallentavat varmuuskopiot kukin omaan levyjärjestelmäänsä. Varmentava tietokantapalvelin ei ole aktiivisena muulloin kuin jaksotetun varmuuskopioinnin aikana.

Tellabs 8000 NMRS -järjestelmän toinen taso eli Warm Standby vaatii lisää laitteita Cold Standbyhyn verrattuna. Erillinen replikointipalvelin seuraa Tellabs 8000 INM-liikennettä ja tallentaa muutokset automaattisesti varatietokantaan. Varatietokanta on täydellinen kopio ensisijaisesta, ja virhetilanteen tai huoltoikkunan aikana se voidaan nostaa manuaalisesti ensisijaiseksi palvelimeksi.



Tellabs 8000 NMRS -järjestelmän kolmas taso eli Hot Standby lisää kokoonpanoon palvelimen, jonka tehtävä on virhetilanteen sattuessa automaattisesti kytkeä toimimaton tietokantapalvelin pois käytöstä ja uudelleenohjata INM käyttämään edelleen toiminnassa olevaa tietokantapalvelinta. Hot standby vaatii toimiakseen Warm Standby -valmiudessa olevan laitteiston, jotta tietokanta saadaan pidettyä synkronoituna. Automatisoidun vaihdoksen johdosta INM:n käyttökatkosta ei pitäisi ilmetä mutta hetkellinen toiminnan hidastuminen on mahdollista vaihdoksen aikana. [33.]



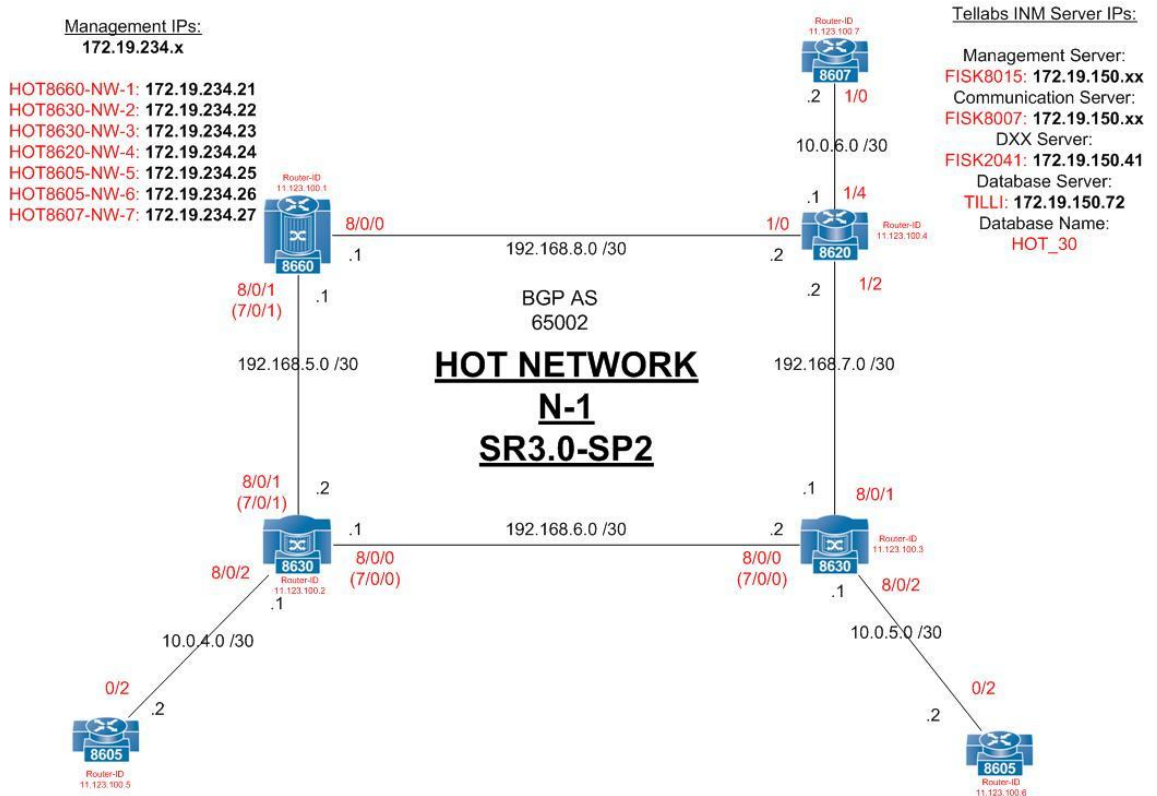
Kuva 6 NMRS tasot [33].

### DXX-palvelin

DXX-palvelin toimii kuten kommunikointipalvelin mutta se kommunikoi ainoastaan Tellabs 8100 -tuoteperheen verkkoelementtien kanssa. DXX-palvelin ohjaa liikennettä verkkoelementtien ja tietokantapalvelimen välillä. Tausta-ajossa palvelin suorittaa myös suorituskyky- ja virhekyseilyjä sekä HW/DB (Hardware / Database), yhtäpitävyystarkastuksia. Mikäli verkkoalue pitää sisällään 8100-tuoteperheen verkkoelementtejä, täytyy niille määrittää hallinoinva DXX-palvelin samaan tapaan kuin muiden tuoteperheiden laitteille kommunikointipalvelin.

### 3.2 N-1 Verkkoelementit

Hotline N-1 -verkko koostuu useista eri tyyppisistä reitittimistä. Verkossa on myös 8100 sekä 6300-tuoteperheen verkkoelementtejä mutta suurin osa laitteista koostuu 8600-sarjan reitittimistä. Kuvassa 10 on esitetty 8600-reitittimien kytkennät sekä osoitteistus.



Kuva 7 N-1 verkkotopologia

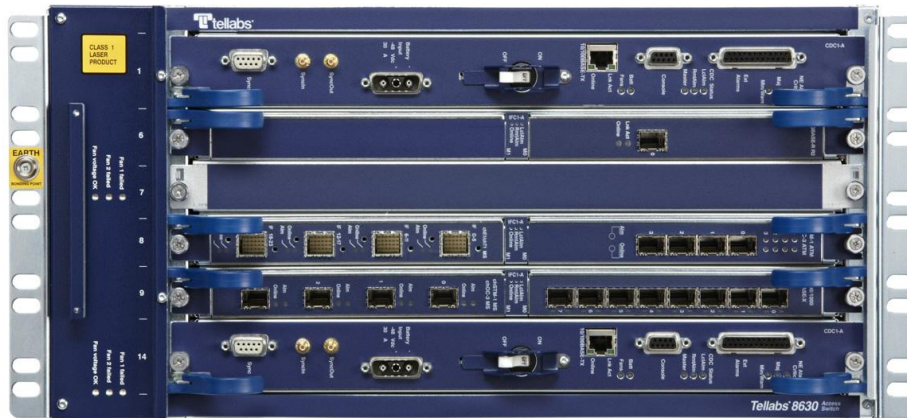
## Tellabs 8660 Smart Router



Kuva 8 8660 Smart Router [32].

Kuvassa 11 esiintyy 8600-tuoteperheen lippulaivamalli, Smart Router 8660. Reititin voidaan varustaa 14 linjakortilla, joista reunimaiset ovat ohjaukskortteja, mitkä kontrolloivat virransyöttöä muille linjakorteille sekä hallinnoivat yleisiä reitittimen toiminnallisuuksia. Muut 12 korttipaikkaa voidaan täyttää linjakorteilla ja jokaiseen linjakorttiin voidaan asentaa kaksi moduulia. Valittavana on monia erityyppisiä moduuleja riippuen siitä mikä verkkoratkaisu kulloinkin on kyseessä. Hot-swappable -ominaisuus mahdollistaa linjakorttien sekä tuuletinyksikön vaihtamisen lennosta eikä reititintä tarvitse sammuttaa toimenpiteen ajaksi. 8660 -verkkoelementtiin on tarkoitus keskittää suuri määrä liikennettä ja uudelleenreitittää se eteenpäin. Hallitut Ethernet- sekä IP VPN (Virtual Private Network) -palvelut ovat reitittimen päätehtäviä ja se pystyy reitittämään sekä 2G- että 3G -liikennettä. [32.]

## Tellabs 8630 Smart Router



10407

## Kuva 9 8630 Smart Router [32].

Kuvassa 12 esiintyy Smart Router 8630. Smart Router 8630 on käytännössä puolikas 8660, siinä on kuusi korttipaikkaa joista ylin ja alin on varattu CDC-hallintakorteille ja neljä väliin jäävää paikkaa on täytettävissä linjakorteilla. Hot swapping -ominaisuus on tuettuna linjakorttien ja jäähdytyksen osalta. Reititysominaisuuksiltaan 8630 on täysin identtinen 8660:n kanssa. 8630 sijoitetaan verkossa usein keskittämään liikennettä kohti 8660:ta, ja mikäli kapasiteettitarve on pienempi, voidaan 8660 korvata kokonaan pikkuvelimallilla. [32.]

## Tellabs 8620 Smart Router



Kuva 10 8620 Smart Router [6].

Kuvassa 13 esiintyy Smart Router 8620. Smart Router 8620 on isoveljiinsä nähden jo paljon pienemmän kokoluokan reititin ja se voidaan varustaa kahdella moduulikortilla. Tällä tavoin siitä on helppo tehdä kustannustehokkaasti tarkoitukseen soveltuva reititin. 8620:n lisäksi 8611, 8607 ja 8605 ovat pienimpiä Tellabsin valmistavia MPLS/IP-kykeneviä reitittimiä. Niitä käytetään yleensä välittämään liikennettä tukiasemilta kohti runkoverkkoa. [6.]

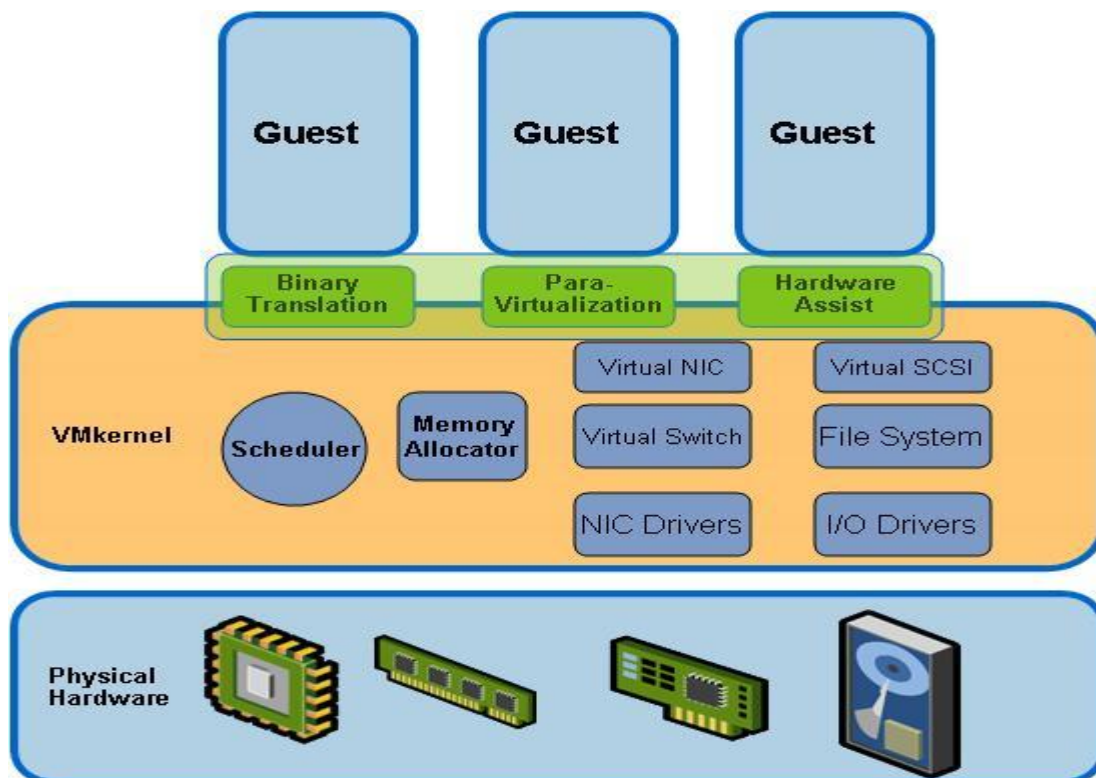
## 4 VMware ohjelmistot

### 4.1 VMware vSphere product suite

vSphere product suite sisältää useita VMware -ohjelmistoratkaisuja, jotka kaikki pohjautuvat saman virtualisointikerroksen eli hypervisorin käyttöön. VMware vSphere suite 5.0 tarjoaa virtualisointikerrokseksi ainoastaan ESXi:tä, mikä on merkittävä muutos aikaisempiin versioihin, joissa valittavana oli myös ESX. vSphere 5 on täysvirtualisointiohjelmisto, jonka keskeisin osa on ESXi 5 hypervisor, joka sisältää oleellisen VMkernelin eikä se tarvitse isäntäkäyttöjärjestelmää toimiakseen. Tellabsilla on käytössä vSphere Enterprise Plus edition versio 5.0. [2, s.17]

#### VMware ESXi 5.0

vSphere -ohjelmistopakettin ydin on hypervisor, joka toimii virtualisointikerroksena ja perustana muille VMware-ohjelmistoille. vSphere 5:n virtualisointikerroksena toimii ESXi. Aikaisemmissa versioissa valittavana oli joko ESXi tai ESX, jotka äkkiseltään vaikuttavat hyvin samankaltaisilta ominaisuuksien ja lisenssien osalta. ESX käytti Linux-pohjaista konsolia, jolla käyttäjä pystyi hallinnoimaan hypervisoria. Linux-pohjainen Service Console sisälsi myös käyttöjärjestelmälle tavanomaisia ominaisuuksia, kuten palomuurin, SNMP-agentin ja web-palvelimen. VMware ESXi edustaa uudemman sukupolven virtualisointiratkaisua, eikä se tarvitse erillistä Linux-pohjaista konsolia asennukseen tai hallinnoimiseen. ESXi kykenee silti tarjoamaan kaikki ominaisuudet joita ESX sisälsi, koska siinä on edistynyt VMkernel. Virtuaalikoneet pääsevät käsiksi hypervisorin alla toimivaan laitteistoon VMkernelin kautta. Kuvasta 14 on nähtävissä kuinka VMkernel allokoii prosessorin laskenta-aikaa, ylläpitää muistinhallintaa ja virtuaalikytkimen dataprosessointia. [2, s.39]



Kuva 11 VMkernel [25].

ESXi host tukee korkeintaan 2048:aa virtuaalista prosessoria, 160:tä ydintä, 160:tä loogista prosessoria, 25:tä virtuaalista prosessoria ydintä kohti sekä maksimissaan 2 TB RAM-muistia isäntää kohden. [2.]

### VMware vCenter Server

VMware vCenter Serverin toiminnallisuutta voidaan verrata Microsoftin Active Directoryn toimintamalliin, joka sisältää käyttäjätietokannan sekä hakemistopalvelun sisältäen tiedot verkon resursseista ja tietokoneista. Vcenter Server mahdollistaa keskitetyn virtuaalikoneiden sekä ESXi-isäntien resurssien jakamisen ja hallinnoimisen, oli kyseessä sitten yksittäinen virtuaalikone tai kokonainen klusteri. vCenter Server hakee datan ESXi-isännistä sekä virtuaalikoneista tietokannasta ja tuettuja tietokantaratkaisuja on nykyisessä versiossa muunmuassa Oracle ja Microsoft SQL server.

Tietokantaan tallennetaan isäntien ja virtuaalikoneiden data. Nykyisessä ohjelmistoversiossa on myös Linux-tuki, joten Windows-palvelimien käyttö ei ole enää

välttämättömyys. vCenterin Serverin avulla on mahdollista luoda virtuaalikoneen kloonin sijaan erillinen template-tiedosto, jota käytetään pohjana uusia virtuaalikoneita luotaessa. Templaten pohjalta saadaan helposti luotua uusi virtuaalikone perusasetuksilla ja puhtaalla käyttöjärjestelmäasennuksella, mistä onkin helppo jatkaa laitteen kustomointia tarpeen mukaan. vCenteristä on myös erittäin vaivatonta muokata jo olemassa olevien virtuaalikoneiden resursseja eli allokoida lisää laskentatehoa, keskusmuistia tai lisätä verkkokortteja sekä levytilaa. [2.]

### vCenter Update Manager

vCenter Update Manager (VUM) on vCenter Serverin liitännäisohjelma, joka mahdollistaa VMware -ohjelmistojen päivitysten keskitetyn sekä automatisoidun asennuksen. Update Manager varmistaa automaattisesti, että VMware-ohjelmistopäivitykset ovat ajan tasalla. Update Manager myös ilmoittaa, mikäli jokin systeemi ei ole yhteensopiva uusimman päivityksen kanssa. [2.]

### VMware vMotion ja Storage vMotion

VMware vMotionin avulla on mahdollista manuaalisesti tasoittaa resurssien käyttöä kahden ESXi-isännän välillä. vMotionia hyödyntäen voidaan esimerkiksi siirtää virtuaalikone fyysiseltä palvelimelta toiselle ilman uudelleenkäynnistystä tai verkkoyhteyden katkeamista eikä käyttäjä huomaa katkosta käynnissä olevien ohjelmien suorittamisessa. Siirrettäessä virtuaalikone ESXi-isännältä toiselle siirtyvät myös sille allokoitu määrä laskentatehoa ja keskusmuistia toisen palvelimen allokoitavaksi. Tämän takia vMotion on erityisen hyödyllinen työkalu ylikuormitetun ESXi-isännän laskentataakan helpottamiseen ja huoltokatkosten minimoimiseen. Yksinkertaistetusti vMotionin toiminta perustuu käytössä olevan virtuaalikoneen muistin sisällön siirtämiseen ESXi-isännältä toiselle sekä mahdollisesti levytallennusjärjestelmän kontrollin siirtoon. [2.]

Storage vMotion toimii teknisesti aivan kuten vMotion mutta se jättää CPU- ja keskusmuistiallokoinnit olemassa olevalle ESXi-isännälle siirtäen ainoastaan levytilan tallennusjärjestelmältä toiselle ilman käyttökatkosta virtuaalikoneelle. StorageMotionia käytetään jaettujen tallennusratkaisujen kanssa. StorageMotion ei rajoitu ainoastaan

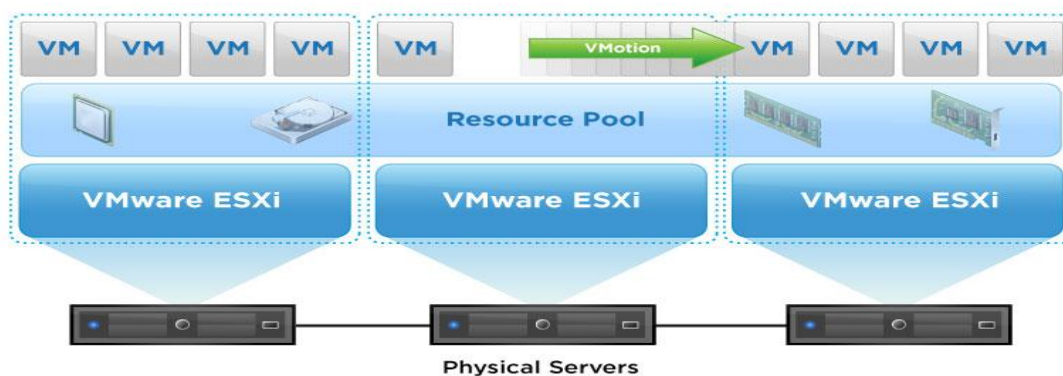


yksittäisten virtuaalikoneiden siirtoon vaan kokonainen SAN-verkkotallennusjärjestelmä on siirrettävissä kerrallaan tarpeen vaatiessa.

Toimiessaan oikein vMotion on vaikuttava ominaisuus mutta ennakoasetelmat ja konfiguraatio täytyy olla hyvin suunniteltu. Sekä lähde- että kohde-ESXi-isännillä täytyy olla pääsy verkkotallennusjärjestelmään, jossa virtuaalikoneen tiedostot sijaitsevat. Sujuvaa käyttökokemusta haettaessa ESXi-isännillä tulisi olla käytettävissä Gigabit Ethernet -verkkoliitäntä sekä siihen määritetty VMkernel-portti, jotta vMotion-toiminto voidaan ottaa käyttöön. [2, s.10]

### vSphere Distributed Resource Scheduler & Distributed Power Management

Distributed Resource Scheduler (DRS) tarkkailee jatkuvasti käyttöastetta vSphere-palvelimien välillä ja tasapainottaa käytettäviä resursseja virtuaalikoneiden kesken. DRS:llä on oma resurssiallas jokaista klusteria kohden, kuten kuvasta 15 on nähtävissä. DRS hyödyntää vMotionin toiminnallisuutta mutta sen toiminta on automaattista, joten virtuaalikoneita liikutellaan ESXi-isäntien ja tallennusjärjestelmien välillä, mikäli määritetyt kynnyksarvot käyttöasteessa ylittyvät. Distributed Power Management (DPM) puolestaan kykenee optimoimaan virrankulutusta sulkemalla alhaisen käyttöasteen isäntiä ja siirtämällä toiminnan aktiivisemmalle isännälle. [2.]



Kuva 12 DRS [26].

## VMware vSphere Client 5.0

vSphere-asiakasohjelma mahdollistaa ESXi-isäntien hallinnoinnin. vSphere-asiakasohjelma yhdistetään joko suoraan ESXi-isäntään tai vaihtoehtoisesti hallinnointi voidaan suorittaa yhdistämällä asiakasohjelma vCenteriin. Yhteyden ottaminen suoraan ESXi-isäntiin vaatii määritellyn käyttäjätunnuksen, joka luodaan ESXi-isännän asennusvaiheessa. vCenteriin yhdistettäessä voidaan käyttää Windows-tilin kirjautumistunnuksia. Suurin osa hallinnointimahdollisuuksista on käytettävissä suoraan ESXi-isännälle yhdistettäessä mutta vCenterin yhdistämällä on mahdollista hallinnoida useita ESXi-isäntiä samassa istunnossa. Suurta virtuaalikoneverkkoa konfiguroitaessa onkin suositeltavaa käyttää vCenteriä pelkän asiakasohjelman sijaan. [2.]

## VMware High Availability & Fault Tolerance

Virtuaalikoneet lähettävät heartbeat-signaalia isäntäpalvelimelle ilmoittaakseen kaiken olevan kunnossa. Käyttöjärjestelmän tai fyysisen laitteen vikaantuessa heartbeat-signaali katkeaa ja aktivoitunut High Availability (HA) -toiminto käynnistää virtuaalikoneen toiselta fyysiseltä isäntäpalvelimelta. Siirto aiheuttaa muutaman minuutin palvelukatkoksen. VMware HA on klusterikohtainen ominaisuus, joten kaikki klusteriin luotavat virtuaalikoneet perivät myös HA -asetuksen. HA on suositeltavaa kytkeä pois käytöstä, mikäli suunniteltuja käyttökatkoksia on tiedossa esimerkiksi verkon huoltoikkunoiden ajaksi.

Fault Tolerance (FT) luo peilatus virtuaalikoneen toiselle fyysiselle isäntälaitteelle, jotta tärkeimmät virtuaalikoneet voidaan kahdentaa vikasetoisuuden parantamiseksi. Vain rajattu määrä virtuaalikoneita isäntää kohden voidaan kahdentaa, joten ominaisuutta on käytettävä ainoastaan tärkeimpien virtuaalikoneiden yhteydessä. Kahdennetuilla virtuaalikoneilla ei synny palvelukatkoksia vikatilanteessakaan eikä dataa katoa, vaikka varakone jouduttaisiin aktivoimaan. [2; 23.]

## Snapshot

Virtuaalikoneesta voidaan luoda palautuspisteitä snapshot-toiminnon avulla. Snapshot tallentaa virtuaalikoneen senhetkisen tilan muistaen myös avoinna olleet prosessit ja tallentaa ”tilannevedoksen” omaksi tiedostoksi, josta se voidaan tarvittaessa ladata

käyttöön. Snapshot toimii ikään kuin Windowsin System Restore Point, mutta ei ole käyttöjärjestelmäriippuvainen, koska hypervisor osaa tallentaa virtuaalikoneen tilan oli käytössä sitten mikä tahansa tuetuista käyttöjärjestelmistä. Snapshot tallentaa ainoastaan virtuaalikoneelle tehdyt muutokset eikä suinkaan koko koneen tilaa, joten snapshotin luoma .vmsn-tiedoston koko on murto-osa koko virtuaalikoneen vaatimasta levytilasta. Ohjelmistopäivitystä tehtäessä on hyvä luoda snapshot ennen päivityksen asentamista, joten vikatilanteen ilmaantuessa voidaan palata vanhoihin ajuri- ja ohjelmistoasetuksiin muutamalla hiiren painalluksella. [19.]

Mikäli virtuaalikone joudutaan palauttamaan snapshottia edeltävään tilaan kaikki snapshotin luonnin jälkeen kirjoitettu uusi data katoaa prosessissa. Myöskin snapshotin jälkeen asennetut ohjelmat poistuvat virtuaalikoneesta. Tämän takia on hyvä kartoittaa kuinka paljon luotua dataa tullaan menettämään palauttaessa kone snapshotia edeltäneeseen tilaan ja mahdollisesti varmuuskopioida tärkeät tiedot ennen palautusprosessia. [2, s.498—503.]

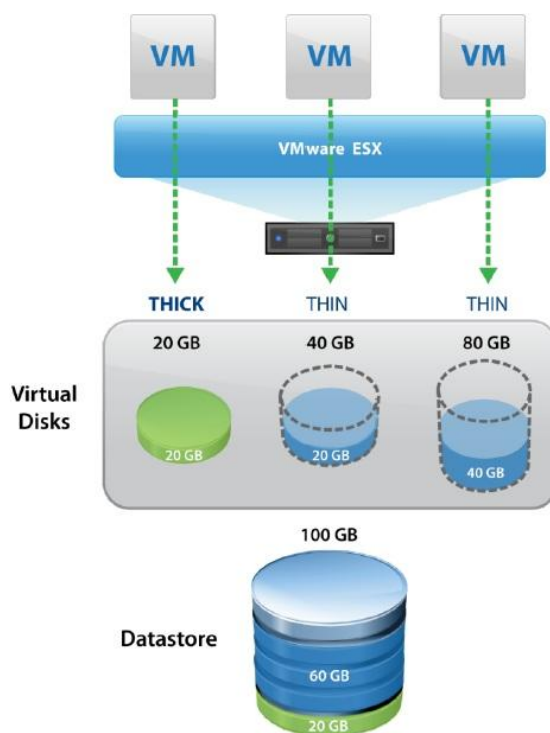
#### 4.2 Virtuaaliset levyjärjestelmät

vSphereä tukeva levyjärjestelmä on avainasemassa virtualisointia toteuttaessa. Monet VMwaren kehittyneistä työkaluista (mm. vMotion, HA, DRS sekä FT) vaativat jaetun verkkotallennusjärjestelmän toimiakseen. [2.]

##### Thin Provisioning

Thin provision -toiminto helpottaa järjestelmänhaltijan työtä ja tuo lisää joustavuutta virtuaalikoneen levytilaa mitoittaessa. Aluksi virtuaalikoneelle määritetään käytettävän levytilan yläraja, mutta virtuaalikone käyttää tilaa ainoastaan sillä hetkellä tarvitsemansa määrän eikä se alusta tai varaa käytettävissä olevaa levytilaa ennen kuin dataa kirjoitetaan lisää. Kuvassa 16 levytilan varaus on esitetty katkoviivoja käyttäen ja alustettu osuus kuvataan sinisellä värillä. Thin-provisioitu 100 GB:n levy on käytännössä vmdk-tiedostona ainoastaan sen suuruinen mitä käyttöjärjestelmäasennus sekä ohjelmat vaativat eli tässä tapauksessa helposti alle puolet määritetystä levytilasta. Thin-provisioinnin etuja muihin levytilanjakotekniikoihin verrattuna ovat muunmuassa alhaisempi sähkönkulutus, tehokkaampi tilankäyttö ja pienempi lämmöntuotto seurauksena levykiekkojen vähäisemmästä määrästä.

Suorituskykyä verrattaessa thin provisioning on thick provisioningia nopeampi ottaa käyttöön mutta esimerkiksi suuria tiedostoja siirrettäessä thick-provisoidut osiot toimivat nopeammin. [24.]



Kuva 13 Thin provisioning [24].

### Thick Provisioning

Thick provisioning käyttää tekniikkaa, jossa levytilaa allokoidaan yli nykyisten tarpeiden silmälläpitäen tulevia levytilavaatimuksia. Vertailukohtaksi voidaan ottaa vaikkapa kovalevy Windows-ympäristössä, missä se ensin osioidaan ja sen jälkeen määritetty osio alustetaan käytettäväksi. Alustettu osio varaa sille määrätyn verran gigatavuja levyiltä vaikka sille ei vielä olisikaan kirjoitettu dataa. Tästä syystä allokoitun levytilan käyttöaste saattaa jäädä varsin alhaiseksi. Taulukossa 1 on esitetty suorituskykymittauksia thin ja thick provisioningin välillä. [2.]

Taulukko 1 Levyjärjestelmien vertailu [31].

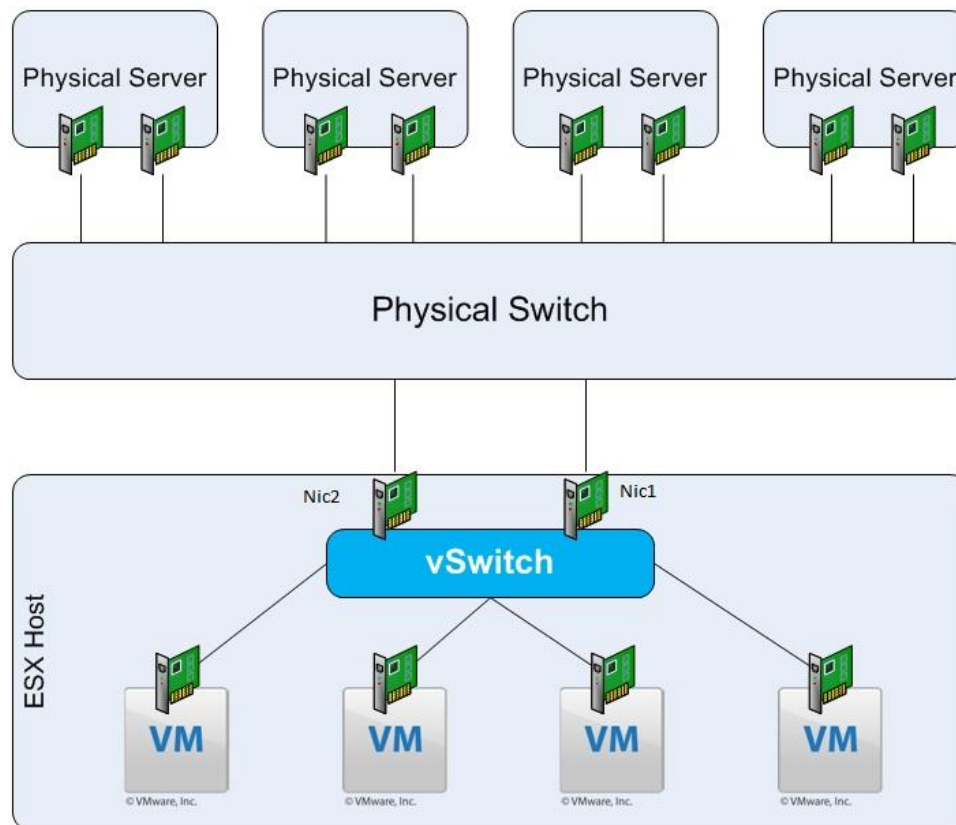
VM Type	Overview		Space Usage (Example 50GB VM with 10GBs Actual Data)					Performance		VM Creation Time		
	Space Allocated	Blocks Zeroed	On the Storage Array					Disk-Based Storage Array	Pure Storage FlashArray	Disk-Based Storage Array	Disk-Based Storage Array w/ VAAI	Pure Storage FlashArray w/ VAAI
			In VMFS	Thick Provisioned Array	Thin Provisioned Array	Thin Prov Array With Zero Reclaim	Pure Storage FlashArray					
Eager Zero Thick	At VM creation	At VM creation	50GB	50GB	50GB	10GB	2GB	Same (Disk Latency)	Same (Flash Latency)	~10 mins	< 30 sec	4 sec
Lazy Zero Thick	At VM creation	When block first written	50GB	50GB	10GB	10GB	2GB	Same (Disk Latency)	Same (Flash Latency)	~ 1 min	< 30 sec	0.2 sec
Thin	When block first written	When block first written	10GB	10GB	10GB	10GB	2GB	Same (Disk Latency)	Same (Flash Latency)	< 30 sec	< 30 sec	0.1 sec

### 4.3 Virtuaalikytkin

Virtuaalikytkimet eivät ole hallinnoitavia kytkimiä ainakaan samassa mielessä kuin fyysiset kytkinlaitteet. Virtuaalikytkimeen ei esimerkiksi voi ottaa Telnet-yhteyttä asetuksia muokatakseen. vSwitcheissä ei myöskään ole CLI:tä (*Command Line Interface*), lukuun ottamatta muutamia vSpheren CLI-komentoja. Toimintatavallaan virtuaalikytkin on hyvin samanlainen fyysiseen verrattuna. vSwitch toimii OSI-taso 2:lla mutta itse kytkimen sijaan MAC (*Media Access Control*) -osoitekantaa ylläpitää hypervisor. vSwitch välittää paketteja kytkinportista toiseen MAC-osoitteen perusteella, tukee VLAN-osoitteistusta ja kykenee luomaan porttikanavia (port channel) ja syöttölinjayhteyksiä IEEE 802.1Q -leimoilla. vSwitcheissä on sisäänrakennettu järjestelmä, mikä estää silmukoiden syntymisen. vSwitchin uplinkiin saapuvaa liikennettä ei koskaan ohjata ulos toiseen uplinkiin, joten STP:lle (*Spanning Tree Protocol*) ei ole tarvetta. [2 ; 29.]

Uutta virtuaaliporttia luodessa ohjelma kysyy luotavan kytkimen roolia eli hoitaako kytkin virtuaalikoneiden verkkoliikennettä, VMkernel-liikennettä vai ainoastaan isäntäkoneen verkkoliikennettä. Mikäli virtuaaliportin on tarkoitus hoitaa muita tehtäviä kuin virtuaalikoneiden verkkoliikennettä, on sille määritettävä oma IP-osoite. Virtuaalikytkimen asetuksia voidaan säätää isäntäkoneen edit settings -valikosta. Virtuaalikytkimen asetuksista voidaan määrittää kytkimen porttien määrä, verkon nimi, VLAN-tunnus sekä valitaan käyttöön otettava virtuaalikoneen verkkokortti ja määritetään sen nopeus. VMwaren vSwitch mahdollistaa eritasoisten

tietoturvaluokitusten määrittämisen samalta fyysiseltä laitteelta ajettaville virtuaalikoneille. Kuvassa 17 esitelly usealla virtuaaliportilla varustettu virtuaalikytkin. [2.]

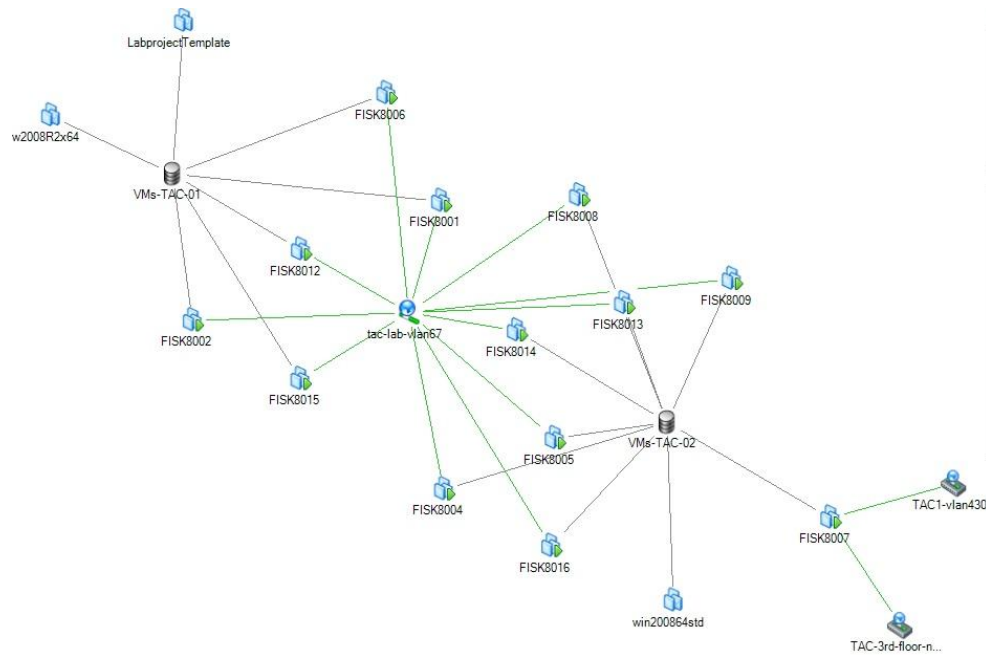


Kuva 17 vSwitch [30].

## 5 Toteutus

Virtualisoitu hotline-verkko suunniteltiin vanhan fyysisen toteutuksen pohjalta ja komponenttien rooli sekä konfigurointi pyrittiin pitämään mahdollisimman samanlaisena. Heti alkuvaiheessa kävi selväksi, ettei DXX-palvelimen virtualisoiminen onnistu, koska palvelinlaite pitäisi pystyä fyysisesti kytkemään sarjaliitännällä verkkoon eikä tätä voida emuloida Ethernet-kytkennällä tai vSwitchiä konfiguroimalla. Ensimmäinen virtualisoitu hotline-verkko, N-1, sisältää virtuaalisen kommunikointipalvelimen, virtuaalisen hallinnointipalvelimen sekä fyysisen tietokanta- ja DXX-palvelimen. N-1 hotline-verkossa on useita verkkoelementtejä 6300-, 8100- ja 8600-tuoteperheistä, joten toimivuuden takaamiseksi tarvitaan sekä kommunikointipalvelin että DXX-palvelin. Valmis virtuaaliratkaisu mahdollistaa asiakkaan ongelmatilanteen uudelleenluomisen turvallisesti rajatussa työympäristössä, jotta insinöörit voivat kehittää siihen toimivan ratkaisun.

Kuvassa 18 on nähtävissä TAC (Technical Assistance Center) -osaston virtuaalikoneklusterin, joka pitää sisällään työntekijöiden luomia virtuaalikoneita ja kaksi käytössä olevaa levypinoa sekä virtuaalikoneiden luomiseen käyteyt mallipohjat. Kommunikointipalvelimen virkaa hoitava FISK8007-virtuaalikone on liitetty useampaan verkkoon vSwitch konfiguraatioilla.



Kuva 18 TAC virtuaalikoneklusteri

### 5.1 Ohjeistusta hotline-verkon suunnitteluun

Teknisen tuotetuen hotline-verkkoja hyödynnetään asiakasverkkojen ongelmatilanteiden ratkaisemiseen. Hotline-verkkojen täytyy tukea kaikkia asiakkaille yleisesti saatavilla olevia (Generally Available, GA) verkkoelementti- ja INM-ohjelmistoversioita, jotta voidaan luoda asiakasverkon kaltainen työympäristö. Uusia INM-versioita julkaistaan kausittain, joten hotline-verkkoja täytyy myös päivittää aktiivisesti, ettei laitteilla ajeta liian vanhaa versioita, johon ei tehdä enää ohjelmistopäivityksiä. Hotline-verkon päivittäminen tulisi aloittaa hyvissä ajoin ennen ohjelmistopäivityksen yleistä julkaisuajankohtaa, jotta ehditään tarvittaessa tilata lisää uusia laitteita ja varmistaa niiden yhteensopivuus. Tellabsin tuotekehitysosasto informoi teknistä tukea, kun seuraava INM-ohjelmistoversio saavuttaa CIR (Customer Introduction Release) -vaiheen. CIR-vaiheessa tuote julkaistaan rajatulle asiakaskunnalle käyttöön ja tällöin myös teknisen tuen pitää saada tuote testattavaksi, jotta hotline verkon valmistelu voidaan aloittaa. CIR julkaisun aikaan saataville tulee myös INM 3<sup>rd</sup> Party Guide Manual, jota tuotetuen insinöörit voivat hyödyntää työssään.



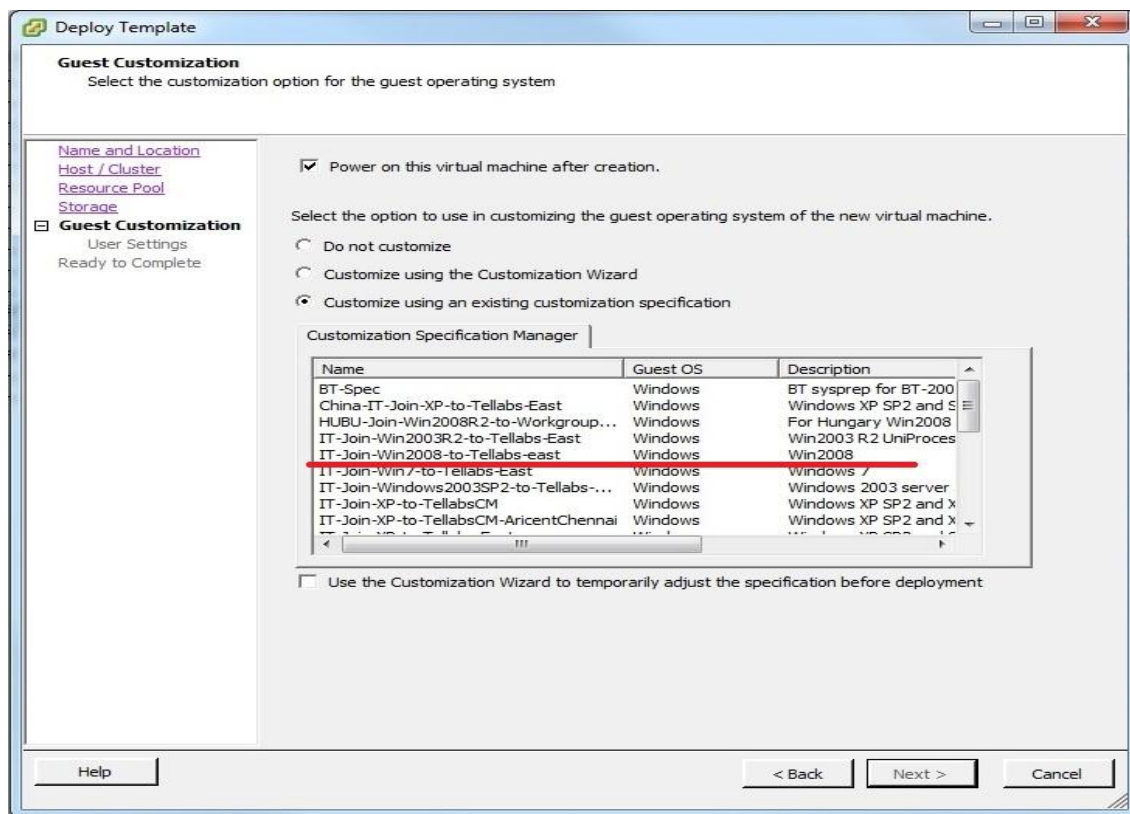
Merkittäviin ohjelmistojulkaisuihin tulee lähes aina myös päivityksiä sekä service pack -julkaisuja. Service packien asennusajankohta hotline-verkoissa ei ole niin kriittinen ja yleensä päivitysajankohta päätetään viikkokouksissa ja sovitetaan tuotetuen osastolle sopivaan ajankohtaan. Lähtökohtaisesti TAC hotline-verkoista pitäisi löytyä yleisimmät asiakkaiden käyttämistä ohjelmistoversioista.

Tällä hetkellä N-1 -verkossa on käytössä virtualisoitu kommunikointipalvelin sekä hallintopalvelin mutta taustalla toimii edelleen varavaihtoehtona fyysiset palvelinlaitteet. Tulevaisuudessa suurin osa TAC:in hotline-palvelimista tullaan virtualisoimaan ja fyysisistä varapalvelimista luovutaan pikkuhiljaa. Jatkossa ensisijaisena käytettävät virtuaalipalvelimet täytyy kahdentaa FT-ominaisuudella, jotta vikatilanteessa palvelin saataisiin nopealla aikataululla takaisin käyttöön eikä asetuksia jouduttaisi uudelleenkonfiguroimaan.

Virtualisoituihin hotline-verkkoihin siirryttäessä ilmenee myös uudenlaisia riskejä. Mikäli kriittinen virhetilanne sattuisi yöaikaan eivätkä hotline-verkon palvelimet olisi käytettävissä, saattaisi vian selvittämiseen kulua normaalia pidempi aika, koska Tellabsin IT-osastolla ei ole henkilökuntaa päivystämässä yöaikaan. Sähkökatkoksen sattuessa totaaliseltsä pimennolta on mahdollista välttyä, koska Tellabsin tiloihin tulee sähköä useammalta toimittajalta. TAC:n työntekijöiden täytyy pystyä hallinnoimaan oman klusterin virtuaalikoneita mutta esimerkiksi levyjärjestelmän hallinnointiin oikeuttavat tunnukset tulisi jakaa vain tarkasti valituille henkilöille, koska kaikkia virtuaalikoneita ei voida resurssien puolesta kahdentaa ja olemassa olevien koneiden poistaminen levyjärjestelmästä on turhankin helppoa.

## 5.2 Mallipohjan luonti

Muokkasin Tellabsilla käytössä olevaa Windows Server 2008 SP2 64-bit -mallipohjaa lisäämällä siihen pääte-emulaattoriohjelma Puttyn sekä Wiresharkin verkkoliikenteen seuraamista varten. Virtuaalikoneen luonti mallipohjasta on äärimmäisen helppo toimenpide, jossa täytyy nimetä luotava virtuaalikone sekä valita sille klusteri ja käytettävä verkkolevyjärjestelmä. Kuvasta 19 on nähtävissä lista Tellabsin IT-osaston luomista vieraskäyttöjärjestelmäasetuksista, joista täytyy olla valittuna asennettavalle käyttöjärjestelmälle räätälöity asetus, mikäli kone halutaan liittää Tellabsin verkko-osoiteavaruuteen.



Kuva 19 Vieraskäyttöjärjestelmän asetukset

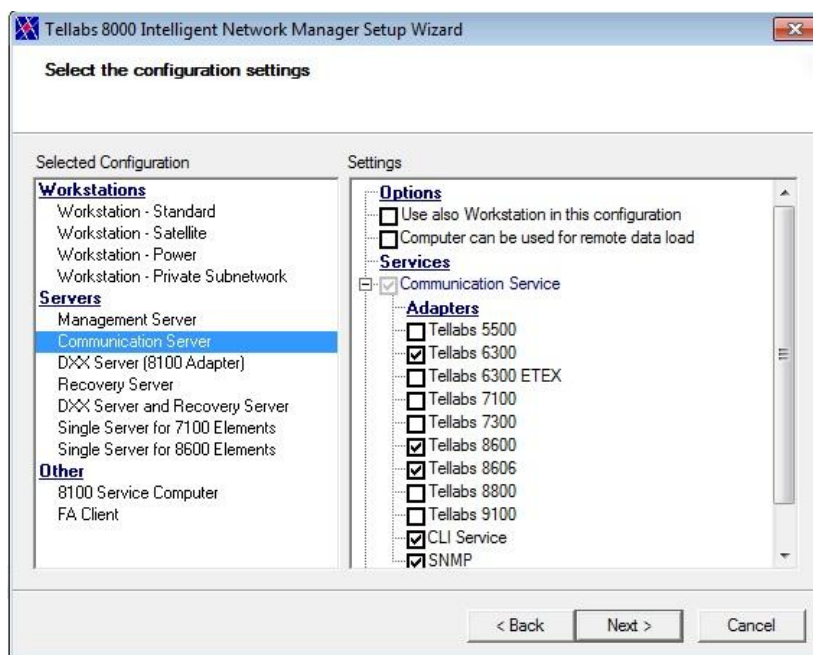
### 5.3 Virtuaalipalvelimen käyttöönotto ja suorituskyvyn määrittäminen

Ensimmäisessä vaiheessa määritin allokoitavan laskentatehon sekä keskusmuistin määrän virtuaalipalvelinta kohden noudattaen 3<sup>rd</sup> Party Installation Manual -ohjeistusta laitteiston minimivaatimuksista. Virtualisoidun palvelimen resurssien hallinta on huomattavasti yksinkertaisempaa kuin fyysisten palvelimien, joten päätin luoda myös toisen testiskenaarion, jossa pyrin määrittämään virtuaalikoneille lähes samanlaisen kokoonpanon, kuin fyysisillä laitteilla on käytössä. Rajoittamalla virtuaalikoneen resursseja pystyn paremmin vertailemaan vanhan fyysisen palvelimen ja uuden virtuaalipalvelimen nopeuseroa INM-ohjelmalla suoritettussa rasiustestissä.

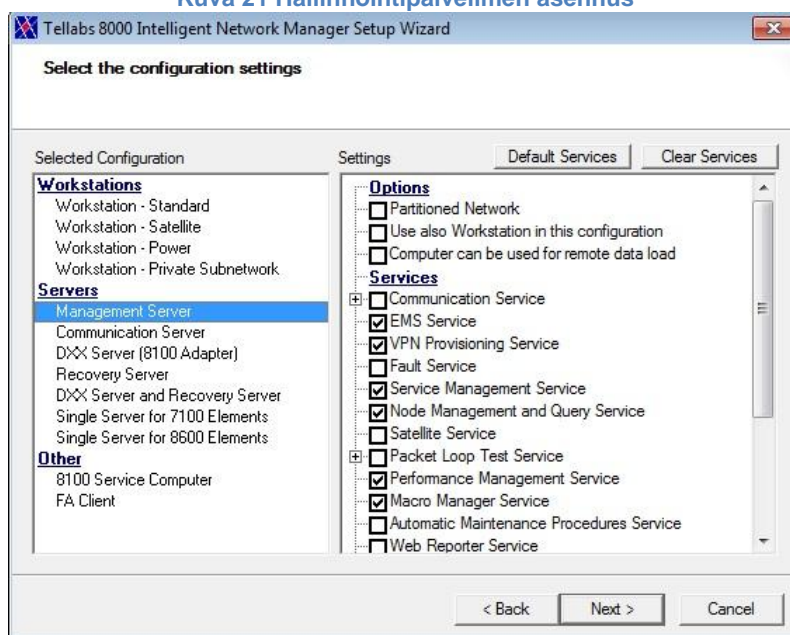
Palvelinasennuksen ensimmäisessä vaiheessa luodaan template eli asennuspohja tuleville virtuaalikoneille. Asennuspohjan avulla on helppoa ja nopeaa luoda useita samanlaisia virtuaalikoneita samoilla perusasetuksilla sekä ohjelmistolla varustettuna. Seuraavassa vaiheessa asennuspohjalta asennettu virtuaalikone kustomoidaan rooliansa varten esimerkiksi tietyn tyyppisellä INM-asennuksella.

## 5.4 INM-roolit ja asennus

Luodaan virtuaalikoneista kommunikointi- ja hallinnointipalvelimet. Mallipohjasta luotuun virtuaalikoneeseen FISK8007 asennetaan INM-ohjelmistoversio 3.0 SP2. Kuvasta 21 sekä 22 on nähtävissä asennuksen alkuvaiheessa esiintyvä lista, josta valitaan haluttu rooli ja mahdolliset adapterit sekä lisätoiminnot.

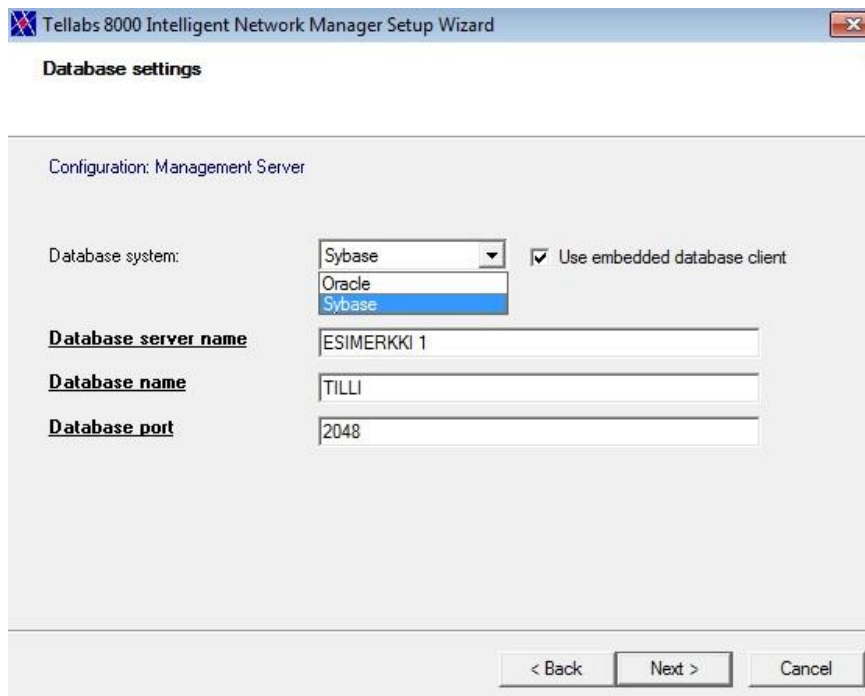


Kuva 21 Hallinnointipalvelimen asennus



Kuva 22 Kommunikointipalvelimen asennus

Kuva 23 näyttää INM-ohjelmiston asennuksen seuraavan vaiheen, missä asennusohjelma kysyy käytetäänkö Oraclen vai Sybasen tietokantaa sekä käytettävän tietokantapalvelimen sekä tietokannan nimen ja porttinumeron.



The screenshot shows a window titled "Tellabs 8000 Intelligent Network Manager Setup Wizard" with a "Database settings" tab. The window content is as follows:

Configuration: Management Server	
Database system:	Sybase <input checked="" type="checkbox"/> Use embedded database client
<b>Database server name</b>	ESIMERKKI 1
<b>Database name</b>	TILLI
<b>Database port</b>	2048

At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

#### Kuva 23 Tietokantapalvelimen asetukset

Asennuksen päätteeksi avataan INM toolbox ja kirjaututaan sisään lisenssiin määritetyillä kirjautumistunnuksilla.

## 5.5 Suorituskykymittaukset

Suorituskykymittauksissa vertaillaan INM:n vastaanottavuutta fyysisten ja virtuaalisten hallinnointi- ja kommunikointipalvelimien välillä. Taulukossa 2 esitellään fyysisten sekä virtuaalisten palvelinlaitteiden kokoonpanot.

**Taulukko 2 Laboratoriokoneiden laitekuvaus**

<b>Rooli</b>	<b>Malli</b>	<b>CPU-tyyppi</b>	<b>RAM</b>
Kommunikointipalvelin FIVI2047	<b>IBM x3250M2</b>	<b>2,4 GHz 2-core</b>	<b>8 GB</b>
Hallinnointipalvelin FIVI2074	<b>IBM x3250M3</b>	<b>2,4 GHz 4-core</b>	<b>8 GB</b>
Virtuaalinen Kommunikointipalvelin FISK8007	<b>Intel Xeon E7-L8867</b>	<b>2,13 GHz 4-core</b>	<b>8 GB</b>
Virtuaalinen Hallinnointipalvelin FISK8015	<b>Intel Xeon E7-L8867</b>	<b>2,13 GHz 4-core</b>	<b>12 GB</b>

Ensimmäisenä testinä suoritetaan INM-ohjelmalla yhtäpitävyystarkastus, joka käy läpi valitun verkkoelementin kaikki liitännät sekä testaa niiden toimivuuden. Testit ajettiin läpi Tellabs Smart Router 8630 -reitittimellä käyttäen ensin fyysistä kommunikointi- ja hallinnointipalvelinta, jonka jälkeen sama testi ajetaan virtuaalisilla laitteilla. Fyysiset palvelinlaitteet suoriutuivat yhtäpitävyystarkastuksesta 18 minuutissa, ja virtuaalisilla laitteilla sama hoitui 15 minuutissa. Ajettaessa useita yhtäpitävyystarkastuksia samaan aikaan huomataan, kuinka virtuaalinen hallinnointipalvelin käyttää tasaisesti nousevaan tahtiin resursseja sitä mukaan, mitä enemmän tarkistuksia on käynnissä. Isäntäkoneen keskusyksikön kellotaajuus yhdellä tarkistuksella vaihteli välillä 700—900 MHz ja nousi kuutta tarkistusta ajettaessa 2800 MHz:iin. Tarkistuksien määrästä riippumatta muistin käyttöaste pysyi tasaisesti 8 GB:ssä.

Seuraavaksi pyrin rasittamaan virtuaalista hallinointipalvelinta ajamalla raskasta makro-ohjelmaa INM:ssä. Makro-ohjelma lisää verkkoon 8630-reitittimen ja kalustaa sen korttipaikka kerrallaan, jonka jälkeen korttipaikat tyhjennetään ja laite poistetaan järjestelmästä. Lisää / poista-silmukkaa jatketaan niin monta kertaa kuin käyttäjä on makroon määrittänyt.

Ajoin neljä instanssia makrosta käyttämällä jokaisessa makrossa eri node id:tä, jotta jokainen makro luo uniikin laitteen verkkoalueeseen. Makrot lisäävät ja poistavat täysin kalustetun 8630 reitittimen 10 kertaa. Virtuaalinen hallinointipalvelin suoritti makrot 27 minuutissa keskusyksikön kellotaajuden vaihdella 2100—4300 MHz välillä. Fyysiseltä hallinointipalvelimelta samaan tehtävään kului 38 minuuttia eli 11 minuuttia pidempään.

Seuraavaksi otetaan käyttöön ensisijaiseksi kommunikointipalvelimeksi fyysinen palvelin FISK2059 ja ajetaan makrot läpi virtuaalisella hallinointipalvelimella FISK8015. Suorituskykyeroa ei syntynyt virtuaalisen ja fyysisen kommunikointipalvelimen välille, koska makro luo ja poistaa verkkoelementit käyttäen koko prosessin ajan "Planned"-tilaa, mikä mahdollistaa verkkoelementin lisäämisen INM-ohjelmaan, vaikka sitä ei oikeasti olisi olemassa. Mikäli reitittimen liitäntää ei nosteta "In-use"-tilaan, se ei edes yritä luoda yhteyttä kommunikointipalvelimeen, vaan liikennöinti tapahtuu ainoastaan tietokannan ja hallinointipalvelimen välillä.

Testien perusteella virtuaalinen hallinointipalvelin on selkeästi vanhaa fyysistä palvelinta ripeämpi. Testitulokset on perusteltavissa selkeällä resurssierolla virtuaalisen ja fyysisen palvelimen välillä. Fyysinen hallinointipalvelimen keskusyksikkö toimii koko ajan 2,4 GHz:n kellotaajudella, kun taas virtuaalipalvelimen prosessorin käyttö saattoi parhaimmillaan käväistä jopa 4,3 GHz:ssa.

Myöhemmin suoritin uudet mittaukset siten, että virtuaalikoneen resurssit rajattiin 2,4 GHz:iin, mikä vastaa lähemmin fyysistä verrokkilaitetta. Fyysistä palvelinta vastaavaksi mitoitettu virtuaalikone nähtävissä kuvasta 24. 2,4 GHz maksimikellotaajuudelle rajattu virtuaalikone suoritti macron 10 kertaa ajassa 36 min eli muutamaa minuuttia nopeammin kuin fyysinen hallinointipalvelin samalla kellotaajudella. Pieni nopeusero virtuaalikoneen eduksi saattaa selittyä virtuaalikoneiden laskentatehon tarjoaman

laitteiston uudemmalla tekniikalla verrattaessa fyysiseen palvelimeen. Testillä todistettiin, ettei virtualisointi ainakaan hidasta prosessia.

Name	State	Status	Host	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
FISK8001	Powered On	Normal	Unknown	112,05 GB	39,05 GB	510	6331	2
FISK8002	Powered On	Normal	Unknown	54,05 GB	35,88 GB	85	1528	2
FISK8004	Powered On	Normal	Unknown	53,88 GB	34,33 GB	850	2205	11
FISK8005	Powered On	Normal	Unknown	54,28 GB	41,10 GB	340	1950	8
FISK8006	Powered On	Normal	Unknown	54,12 GB	34,20 GB	2360	696	14
FISK8007	Powered On	Normal	Unknown	44,05 GB	41,30 GB	148	1808	6
FISK8008	Powered On	Normal	Unknown	21,05 GB	20,96 GB	106	543	11
FISK8009	Powered On	Normal	Unknown	66,05 GB	48,12 GB	510	3121	3
FISK8012	Powered On	Normal	Unknown	52,05 GB	42,00 GB	127	757	0
FISK8013	Powered On	Normal	Unknown	44,05 GB	43,37 GB	212	1604	5
FISK8014	Powered On	Normal	Unknown	44,05 GB	41,01 GB	127	1840	9
FISK8015	Powered On	Normal	Unknown	97,75 GB	58,61 GB	0	0	0
FISK8016	Powered On	Normal	Unknown	62,06 GB	47,46 GB	361	943	0

Kuva 24 Fyysistä palvelinta vastaavaksi mitoitettu hallinnointipalvelin

## 5.6 Virtualisointiprojektin haasteet

Virtuaalikoneiden luonti kustoimoidusta mallipohjasta oli aluksi ongelmallista, koska konetta ei saanut liitettyä verkko-osoitevaruuteen asennuksen päätyttyä. Syy tähän oli ohjeistuksen puute IT:n puolesta. Vika selvisi, kun otin käyttöön valmiiksi kustomoidut verkkoasetukset vieraskäyttöjärjestelmälle.

Kommunikointipalvelimen OSITP4-liikenne vaatii suoran verkkoyhteyden virtuaalikoneelta laboratorioverkkoon. OSITP4 -verkkoliikenne ei välittynyt kerrosten välisten reitittimien läpi oikein ennen kuin virtuaalisen kommunikointipalvelimen vSwitch-asetuksia muutettiin laboratorion aliverkkoon sopiviksi.

Virtuaalikoneiden resurssien muuttaminen lennosta on ongelmallista, koska hallinnoitava laitteisto on IT-osaston hallussa eivätkä oikeudet TAC:issa riitä asetusten muuttamiseen. Tämän vuoksi virtualisoidun hallinnointipalvelimen laskentateho ylitti selkeästi fyysisen verrokkipalvelimen resurssit ja erot makroja ajettaessa olivat huomattavat.

Suorituskykyä mitattaessa aikaa vievin osuus oli saada makro-ohjelmat toimimaan oikein. Sain käyttöni valmiin pohjan makrolle mutta se oli luotu täysin eri ympäristöä varten. Makro ei myöskään kalustanut 8630-noodia oikein, joten lisää/poista-toiminnallisuus piti luoda jokaiselle linjakortille alusta alkaen.

Virtuaalisella kommunikointipalvelimella ajossa olleet palvelut keskeytyivät alle viikon käytön jälkeen yllättäen ja myös remote desktop -yhteys palvelimeen katosi. Kommunikointipalvelinta pystyttiin edelleen hallinoimaan vSpheren konsoliyhteyden kautta mutta INM-prosessien vikasietoisuutta täytyy seurata tarkasti. Pidemmällä aikavälillä seurattuna ongelma ei onneksi uusiutunut.

Koko talon virtualisoitua verkkoa ei kannattaisi liittää laboratorioverkkoihin, koska käytössä oleva lähiverkko on aikaisemmin kaatunut väärin asennettujen tai viallisten verkkolaitteiden aiheuttaman yleislähetysryöpyn seurauksena. Yleislähetysryöppy syntyy, kun verkkolaitteiden välittämät tason 2 yleislähetykset ja ryhmälähetykset välittyvät eteenpäin kytkimien jokaisesta portista. Verkko tukkeutuu nopeasti, kun kytkimet uudelleenlähettävät yleislähetyspaketteja jokaista porttia käyttäen. Itse kytkimet ja reitittimet eivät tukkeudu yleislähetysryöpyssä, mutta mikäli luodut virtuaalikoneet alkavat vastailta kyselyihin, on lopputulos katastrofaalinen ja verkko kaatuu. Myöskin IP-puhelinyhteydet talossa menevät alas mikäli vastaava yleislähetysryöppy toteutuu. [16.]

## 5.7 Vikatilanteesta toipuminen

Virtualisoidussa ympäristössä voi esiintyä useita erilaisia vikatilanteita mutta vikatilanteesta toipuminen on usein nopeampaa kuin fyysisten palvelinlaitteiden kanssa. Tellabsilla on käytössä hyvin vikasietoinen virtuaalikoneympäristö, jossa on kahdennettuna verkkokytkimet, kuitukytkimet, blade-palvelimet sekä verkkotallennusjärjestelmä. Laskentatehon tarjoavat kolme blade-palvelinta on mitoitettu siten, että yhden palvelimen vikaantumisen seurauksena kaksi jäljelle jäävää kykenevät tarjoamaan tarvittavan laskentatehon kunnes korjaukset on tehty. Järjestelmää pyöritetään kirjoitushetkelläkin ainoastaan kahdella palvelimella, koska kolmannelle palvelimelle suoritetaan keskusmuistin lisäys.

Kytkimen tai isäntäpalvelimen vikaantuessa Tellabsin nykyinen virtuaalikone-infrastruktuuri kykenee uudelleenreitittämään ja käynnistämään virtuaalikoneen hyvin nopeasti. Levyjärjestelmän hajoamisen yhteydessä olisi virtuaalikoneiden data silti luettavissa peilatulta verkkolevyiltä eikä tietoa katoa prosessin aikana. Helpon korjattavissa oleva vikatilanne syntyy yksittäisen virtuaalikoneen hajoamisen yhteydessä. Virtuaalikoneen käyttämä vieraskäyttöjärjestelmä saattaa aiheuttaa



virheen, joka korjaantuu käyttöjärjestelmän uudelleenkäynnistyksellä. Mikäli virtuaalikone ei edelleenkään toimi oikein, VMware HA -toiminto siirtää sen käynnistettäväksi toisella fyysisellä host-laitteella, jotta saadaan suljettua pois mahdollinen fyysinen laitevika.

Viimeisen kolmen vuoden aikana IT-osaston hallinnoima virtuaalikoneinfrastruktuuri on viidesti joko kaatunut tai hidastunut selkeästi yleislähetysryöpyn johdosta. Vikatilanne on syntynyt aina päivällä ja syy on lähes poikkeuksetta ollut työntekijän väärin konfiguroima fyysinen laite. Vikatilanteen sattuessa ilta-aikaan joudutaan paikalle hälyttämään IT-henkilökunnan jäsen tai vaihtoehtoisesti voidaan neuvotella rajoitettujen oikeuksien antamisesta TAC-henkilökunnalle, jotta virtuaalikoneiden hallinnoiminen onnistuisi. IT-osasto kehittää parhaillaan ratkaisua, jolla eliminoidaisiin tason 2 ongelmat sekä yleislähetysryöpyt. [16.]

Virtuaalipalvelimen vikaantuessa käyttökatkoksen pituus lasketaan kuitenkin vain minuuteissa. Vian ilmetessä fyysisessä palvelinlaitteessa voidaan yleensä laskea käyttökatkos tunneissa tai jopa päivissä ja korjaustoimet vaativat manuaalisia toimenpiteitä IT-henkilöstöltä.

Merkittävimmät vikasietoisuutta parantavat tekijät kahdennettujen laitteiden ohella ovat VMwaren HA- ja FT-toiminnot. HA mahdollistaa fyysisistä laitevioista toipumisen muutamissa minuuteissa, ja FT mahdollistaa käyttökatkottoman vikasietoisuuden kriittisille virtuaalipalvelimille. [2.]

## 6 Yhteenveto

Työn tarkoituksena oli selvittää hyötyjä, haittoja sekä kustannuksia virtuaalipalvelimiin siirryttäessä. Tutkimuskohteena oli eritoten Tellabsin hotline-verkon palvelinlaitteet ja niiden virtualisoiminen. Virtualisoidun palvelimen käyttö INM-verkonhallintaohjelman kommunikointi- tai hallinnointipalvelimen roolissa antoi paremman kuvan siitä, mitä voidaan jatkossa toteuttaa virtualisoiduilla laitteilla. Suorituskyky mittaukset antoivat positiivisen kuvan virtuaalipalvelimista.

Projekti oli hyvin ajankohtainen, koska Tellabsin TAC-osasto on sijoittanut suuren summan rahaa kevään aikana virtualisointihankkeeseen mutta läheskään kaikkea laskentatehoa ei ollut vielä syksyyn mennessä valjastettu hyötykäyttöön. Projektin lopussa laskentatehoa on edelleen käyttämättä, joten osaston virtuaalikoneiden osuutta suhteessa fyysisiin laitteisiin voidaan edelleen kasvattaa. Suunnitelmat uusimman hotline-verkon virtualisoinnista ovat myös käynnistyneet.

Projektin eteenpäin vieminen oli ajoittain haasteellista, koska laitteisiin ja hallintatyökaluihin ei aina päässyt käsiksi oikeuksien rajallisuuden vuoksi. Esimerkiksi mallipohjan luonti ja uuden virtuaalikoneen asentaminen olisivat sujuneet huomattavasti nopeammin, jos Tellabsille kustomoidut asetukset olisi opastettu heti kättelyssä IT-osaston puolesta. Tilanne olisi varmasti ollut toisenlainen, mikäli blade-palvelimet olisivat TAC:n omistuksessa eikä IT-osaston hallinnoimia. Toisaalta hallinnoimisen rajallisuus on ymmärrettävää, kun laitteita käytetään ainoastaan työn tekemiseen ja vikasietoisuuden voi jättää täysin IT-osaston huoleksi.

Testien perusteella voin ehdottomasti suositella virtualisointia tulevaisuuden laitehankintoja suunniteltaessa. Keskitetty hallinnointi, työympäristön muunneltavuus sekä erittäin hyvä vikasietoisuus ovat virtuaaliympäristön valttikortteja fyysiseen ratkaisuun verrattaessa. Hallinnoinnin helppous ja merkittävä nopeusero aikaisemmin käytössä olleisiin fyysisiin palvelimiin olivat vaikuttavia tekijöitä laitehankintoja suunniteltaessa. Riskitekijöitä arvioitaessa päädyttiin lopputulokseen, jossa riskit kohdistuvat yhtä lailla virtuaalisiin kuin fyysisiin palvelimiin, mutta vikatilanteesta palautuminen on poikkeuksetta nopeampaa ja automaattisempaa virtuaalipalvelimia käytettäessä.

## Lähteet

- 1 Tellabs Oy Suomessa. (Verkkodokumentti.) Tellabs Oy. <http://www.tellabs.com/fi/>. Luettu 8.10.2012. Päivitetty 20.09.2012
- 2 Scott Lowe. 2011. Mastering VMware vSphere 5, (Kirja.).
- 3 Tellabs 8000 INM Software Installation and Maintenance Tellabs® 8000 Intelligent Network Manager SR4.0 System Description. Luettu 1.11.2012
- 4 Hirvikoski Tatu, MS PowerPoint 2010 piirretyt kuvat.
- 5 Tellabs 8000 Third party software installation manual. Luettu 2.10.2012
- 6 <http://www.tellabs.com/products/8000/tlab8620sr.pdf> (Verkkodokumentti, kuva). Luettu 1.11.2012. Päivitetty 15.01.2012
- 7 Tietokone 2/2009. (Lehtiartikkeli). Luettu 20.8.2012
- 8 [www.tietokone.fi/lehti/tietokone\\_3\\_2009/kaikki\\_virtualisoinnista\\_osa\\_2\\_4\\_408](http://www.tietokone.fi/lehti/tietokone_3_2009/kaikki_virtualisoinnista_osa_2_4_408) (Verkkodokumentti). Luettu 21.8.2012. Päivitetty 20.04.2011
- 9 <http://fi.wikipedia.org/wiki/Virtualisointi> (Verkkodokumentti). Luettu 19.8.2012. Päivitetty 2.7.2012.
- 10 <http://en.wikipedia.org/wiki/Paravirtualization> (Verkkodokumentti). Luettu 24.8.2012. Päivitetty 25.05.2012
- 11 <https://www.virtualbox.org/> (Verkkodokumentti). Luettu 11.10.2012. Päivitetty 09.09.2012
- 12 <http://www.ibm.com/developerworks/aix/library/au-aixhpvirtualization/index.html> (Verkkodokumentti). Luettu 5.11.2012. Päivitetty 01.06.2012

- 13 [http://technet.microsoft.com/en-us/library/cc794868\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc794868(v=ws.10).aspx) (Verkkodokumentti). Luettu 15.10.2012. Päivitetty 01.09.2012
- 14 [http://en.wikipedia.org/wiki/Timeline\\_of\\_virtualization\\_development](http://en.wikipedia.org/wiki/Timeline_of_virtualization_development) (Verkkodokumentti). Luettu 20.11.2012. Päivitetty 01.02.2012
- 15 [http://en.wikipedia.org/wiki/Hardware\\_virtualization](http://en.wikipedia.org/wiki/Hardware_virtualization) (Verkkodokumentti). Luettu 26.8.2012. Päivitetty 03.03.2011
- 16 [http://en.wikipedia.org/wiki/Broadcast\\_radiation](http://en.wikipedia.org/wiki/Broadcast_radiation) (Verkkodokumentti). Luettu 17.11.2012. Päivitetty 04.05.2012
- 17 Ruest, D. & Ruest, N. 2009. Virtualization: a beginner's guide (Kirja).
- 18 <http://www.waldspurger.org/carl/papers/esx-mem-osdi02.pdf> (Verkkodokumentti). Luettu 9.11.2012. Päivitetty 05.06.2012
- 19 [http://www.vmware.com/support/ws55/doc/ws\\_learning\\_files\\_in\\_a\\_vm.html](http://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm.html) (Verkkodokumentti). Luettu 8.10.2012. Päivitetty 06.08.2012
- 20 [http://www.vmware.com/files/pdf/VMware\\_paravirtualization.pdf](http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf) (Verkkodokumentti). Luettu 9.11.2012. Päivitetty 03.09.2012
- 21 <http://www.vmware.com/company/mediaresource/milestones.html> (Verkkodokumentti). Luettu 10.10.2012 Päivitetty 01.10.2012
- 22 <http://blog.ioshints.info/2010/11/vmware-virtual-switch-no-need-for-stp.html> (Verkkodokumentti). Luettu 14.11.2012. Päivitetty 29.11.2010
- 23 <http://www.vmware.com/products/datacenter-virtualization/vsphere/high-availability.html#technical> (Verkkodokumentti). Luettu 15.10.2012. Päivitetty 01.08.2012
- 24 [http://www.vmware.com/pdf/vsp\\_4\\_thinprov\\_perf.pdf](http://www.vmware.com/pdf/vsp_4_thinprov_perf.pdf) (Verkkodokumentti). Luettu 7.11.2012. Päivitetty 01.09.2012

- 25 [http://communities.vmware.com/servlet/JiveServlet/showImage/102-5501-7-3049/multi\\_mode\\_monitor.JPG](http://communities.vmware.com/servlet/JiveServlet/showImage/102-5501-7-3049/multi_mode_monitor.JPG) (Kuva). Katsottu 17.11.2012. Päivitetty 05.07.2012
- 26 [http://www.vmware.com/files/images/vsphere\\_imgs/VMW-DGRM-vSPHR-DRSOVERVIEW-101-800x600.jpg](http://www.vmware.com/files/images/vsphere_imgs/VMW-DGRM-vSPHR-DRSOVERVIEW-101-800x600.jpg) (Kuva). Katsottu 19.10.2012. Päivitetty 02.06.2012
- 27 <http://www.networkworld.com/news/2009/043009-ibm-virtualization.html> (Verkkodokumentti). Luettu 9.11.2012. Päivitetty 30.04.2009
- 28 <http://stackoverflow.com/questions/6044978/full-emulation-vs-full-virtualization> (Verkkodokumentti). Luettu 20.9.2012 Päivitetty 18.05.2011
- 29 <http://blog.ioshints.info/2010/11/vmware-virtual-switch-no-need-for-stp.html> (Verkkodokumentti). Luettu 14.11.2012. Päivitetty 29.11.2010
- 30 <http://kensvirtualreality.files.wordpress.com/2009/03/fault-tolerance-the-difference.png> (Kuva). Katsottu 23.11.2012.
- 31 <http://www.purestorage.com/blog/wp-content/uploads/2012/02/Screenshot-2012-02-02-at-3.03.28-PM.jpg> (Kuva). Katsottu 23.11.2012
- 32 Tellabs® 8000 Intelligent Network Manager SR4.0 System Description
- 33 Tellabs® 8000 Network Manager Resilience Service