Niko Kaarto

Varaverkonhallintakeskuksen käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

13.5.2013

Metropolia

Tekijä Otsikko Sivumäärä Aika	Niko Kaarto Varaverkonhallintakeskuksen käyttöönotto 30 sivua 13.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Yliopettaja Matti Puska Service deskin esimies Dan Strömberg

Tämä työ tehtiin Cygate Oy:lle. Verkonhallinta- ja valvontapalveluita tarjoavan yrityksen on hyvä ottaa huomioon erilaiset vika- ja katastrofitilanteet sekä niiden vaikutus verkonvalvontaan ja hallintaan. Cygaten on oltava valmis varautumaan tilanteisiin, joissa nykyinen verkonhallintakeskus menetetään pidemmäksi aikaa.

Työn tavoitteena oli tehdä käyttövalmis varaverkonhallintakeskus sekä päivittää Cygaten IT-palveluiden jatkuvuuden hallinnan dokumentit ajan tasalle varaverkonhallintakeskuksen osalta. Työn alussa kuvattiin IT-palveluiden jatkuvuudenhallinnanprosessia ITIL:n näkökulmasta sekä määriteltiin Cygaten prosessi varaverkonhallintakeskukseen siirtymiselle. Työn alussa esiteltiin myös erilaisia tekniikoita verkonvalvontaan ja –hallintaan (SNMP, RMON, Netflow) sekä esiteltiin Cygaten käyttämää verkonvalvontatekniikkaa.

Työn käytännön osuudessa laitettiin varaverkonhallintakeskuksen kytkimelle tarvittavat määritykset kytkemällä se Cygaten laboratorioverkkoon, minkä jälkeen se vietiin varaverkonhallintakeskukseen. Kytkimelle määriteltiin tarvittavat verkot, reitit ykset ja tietoturva-asetukset. Varaverkonhallintakeskus ja sen verkot liitettiin Cygaten olemassa olevaan verkkoon sekä asennettiin varaverkonhallintakeskuksen työasemiin tarvittavat sovellukset. Varaverkonhallintakeskuksen IP-puhelimet myös asennettiin tässä yhteydessä.

Lopuksi kaikkien yhteyksien ja työasemien toimivuus testattiin. Tämän jälkeen korjattiin kaikki testauksissa ilmenneet ongelmat. Valmiin työn tuloksena saatiin toimiva varaverkonhallintakeskus Cygate Oy:lle. Varaverkonhallintakeskus on käyttövalmiina, jos sinne siirtymiselle tulee tarve.

Avainsanat	verkonvalvonta, verkonhallinta, ITIL, SNMP, RMON, Netflow

Author Title Number of Pages Date	Niko Kaarto Implementing a backup network operations center 30 pages 13 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Matti Puska, Principal Lecturer Dan Strömberg, Service Desk Manager

A corporation such as Cygate Ltd that provides network monitoring and management services must take into account various setbacks that network monitoring and management might face. Cygate Ltd must be prepared for situations in which its network operations center is lost for a longer period.

The purpose of the project described in this thesis was to create and implement a ready-to-use backup network operations center and update the IT Services Continuity Management documents of Cygate regarding the backup network operations center. First, the Continuity Management process based on ITIL (Information Technology Infrastructure Library) and the relocating process of Cygate's network operations are described to give some basic information about the project. Secondly, different network monitoring and management protocols and the network monitoring and management method used by Cygate are introduced as well.

Finally, the thesis discusses the practical implementation of the backup network operations center. The network switch of the backup network operations center was configured in Cygate's laboratory network. All the necessary configurations were configured to this network switch. These configurations included basic, routing and security configurations. After configuration, the network switch was removed to the backup network operations center. The networks of the backup network operations center were connected to Cygate's current network. Installations of workstation applications and IP Phones were conducted after the switch configuration.

Subsequently, the functionality of all configurations and installations was tested. In conclusion, the backup network operations center is fully operational and ready for use.

Keywords	Network management, ITIL, SNMP, RMON, Netflow

Sisällys

Lyhenteet

BCM	*Business Continuity Management.* Liiketoiminnan jatkuvuuden hallinta.
BIA	*Business Impact Analysis.* Liiketoiminnan vaikutusanalyysi.
dot1x	Standardi porttikohtaiselle pääsynhallinnalle.
EAPOL	*Extensible Authentication Protocol Over LAN*. Verkkoporttiin liitettyjen laitteiden tunnistautumiseen käytettävä protokolla.
ECAB	*Emergency Change Advisory Board*. Kriisimuutosten johtoryhmä.
G.722	Laajakaistainen äänikodekki, joka pakkaa äänen pienempään datavirtaan ja voi tukea laajempaa taajuusaluetta.
ICMP	*Internet Control Message Protocol*. Internet kontrolli protokolla esimerkiksi ping.
IP	*Internet Protocol*. TCP/IP-mallin Internet kerroksen protokolla.
ITIL	*Information Technology Infrastructure Library.* IT-palveluiden hallintaan ja johtamiseen käytettävä kokoelma käytäntöjä.
ITSCM	*IT Services Continuity Management.* IT-palveluiden jatkuvuuden hallinta.
LACP	*Link Aggregation Control Protocol*. Protokolla, jonka avulla monesta fyysisestä portista voidaan tehdä yksi looginen portti.
MIB	*Management Information Base*. Hallittavien verkkoelementtien tietokanta.
MPLS	*Multiprotocol Label Switching*. IP-pakettien reititysmenetelmä.
NMS	*Network Management System.* Sovellus, jota käytetään hallinnoimiseen SNMP:ssä.
NOC	*Network Operations Centre.* Verkonvalvonta ja -hallinta keskus.

OSI	*Open System Interconnection model.* Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä eri kerroksessa.
OSPF	*Open Shortest Path First*. Dynaaminen reititysprotokolla.
QoS	*Quality of Services*. Liikenteen luokittelua ja priorisointia tarkoittava termi.
RADIUS	*Remote Authentication Dial In User Service*. Protokolla, joka tarjoaa keskitettyä pääsynhallintaa.
SCM	*Service Continuity Management.* Palveluiden jatkuvuuden hallinta.
SNMP	*Simple Network Management Protocol.* TCP/IP verkkojen hallinnassa käytettävä protokolla.
TCP/IP	*Transport Control Protocol/Internet Protocol*. Usean Internet-liikennöinnissä käytettävän protokollan yhdistelmä.
UDP	*User Datagram Protocol*. Yhteydetön protokolla, joka mahdollista tiedostojen siirron ilman, että yhteyttä muodostetaan laitteiden välille.
VLAN	*Virtual Local Area Network*. Virtuaalinen lähiverkko.
VoIP	*Voice over IP*. Tekniikka jonka avulla ääntä siirretään IP-verkon välityksellä.
VRF	*Virtual Routing and Forwarding*. Teknologia, joka sallii useamman instanssin IP-pakettien reitityksessä.

1 Johdanto

Tämä työ on tehty Cygate Oy:lle. Cygate-konsernissa työskentelee tällä hetkellä yli 500 henkilöä Suomessa ja Ruotsissa. Cygate tuottaa IP-teknologioihin (Internet Protocol) perustutuvia tietoverkko- ja tietoturvapalveluita. Nykyään palveluvalikoimaan kuuluvat myös palvelinjärjestelmät ja niiden hallinta.[1.]

Nykyajan IT-yrityksissä (Information Technology) on tärkeää ottaa huomioon palveluiden jatkuminen kriisi- ja katastrofitilanteissa. Tämä on erityisen tärkeää verkon valvonnan ja hallinnan osalta, koska tietoverkkojen toimivuudella on nykyaikana suuri vaikutus yritysten liiketoimintaan. Tietoverkkojen vikatilanteissa verkonvalvonnalla on tärkeä osuus vikatilanteiden havaitsemisessa. Täten on tärkeää taata toimivat verkon valvonta- ja hallintapalvelut asiakkaille kaikissa tilanteissa.

Tässä työssä toteutetaan varaverkonhallintakeskus Cygate Oy:lle paikkaan, joka sijaitsee eri kiinteistössä kuin nykyinen Cygaten verkonhallintakeskus. Tämä on erityisen tärkeää sen takia, jos nykyiselle kiinteistölle ja sen laitteille tapahtuu vahinkoja. Valmiin työn tavoite on, että varaverkonhallintakeskus on käyttövalmis tarpeen vaatiessa. Varaverkonhallintakeskus tulee liittymään yrityksen jo olemassa olevaan verkkoon. Laitteisto tulee koostumaan yhdestä kytkimestä, työasemista sekä kahdesta IP-puhelimesta.

Insinöörityön alkuosassa tutustutaan siihen mitä on IT-yritysten jatkuvuuden hallinta ITIL:n (Information Technology Information Library) näkökulmasta ja siihen mitä vaatimuksia ITIL antaa jatkuvuuden hallinnalle. Sitten kerrotaan, kuinka Cygaten verkon valvonta ja hallinta siirretään varapaikkaan. Varaverkonhallintakeskukseen tulevalle kytkimelle tehdään määritykset Cygate Oy:n laboratorioverkossa, jonka jälkeen se siirretään varapaikkaan. Tämän jälkeen kytkintä on myös mahdollista hallita etäkäytöllä.

2 IT-yrityksen jatkuvuuden hallinta

2.1 Jatkuvuuden hallinta ITIL:n näkökulmasta

ITIL on kokoelma eri käytäntöjä IT-palveluiden hallintaan. Kokoelmat sisältävät prosesseja ja erilaisia toimintoja, joita IT-palveluiden tarjoaja voi käyttää tuottamassaan palvelussa asiakkaille. ITIL:n on kehittänyt Central Computer and Telecommunications Agency Englannissa vuonna 1980. ITIL:in tavoitteena on muun muassa integroida IT-liiketoiminnan palveluihin, parantaa eri prosessien tehokkuutta ja tehdä toiminnasta riskittömämpää. ITIL:n tavoitteena on myös parantaa tuotettavien palveluiden tehokkuutta ja hinta-laatu suhdetta. ITIL v3 koostuu viidestä eri vaiheesta. Näitä vaiheita ovat: [2, s.6;9;11.]

- Palvelustrategia (eng. Service Strategy)
- Palvelun suunnittelu (eng. Service Design)
- Palvelun siirtymisvaihe (eng. Service Transition)
- Palveluoperaatiot (eng. Service Operations)
- Jatkuva palveluiden kehitys (eng. Continual Service Improvement)

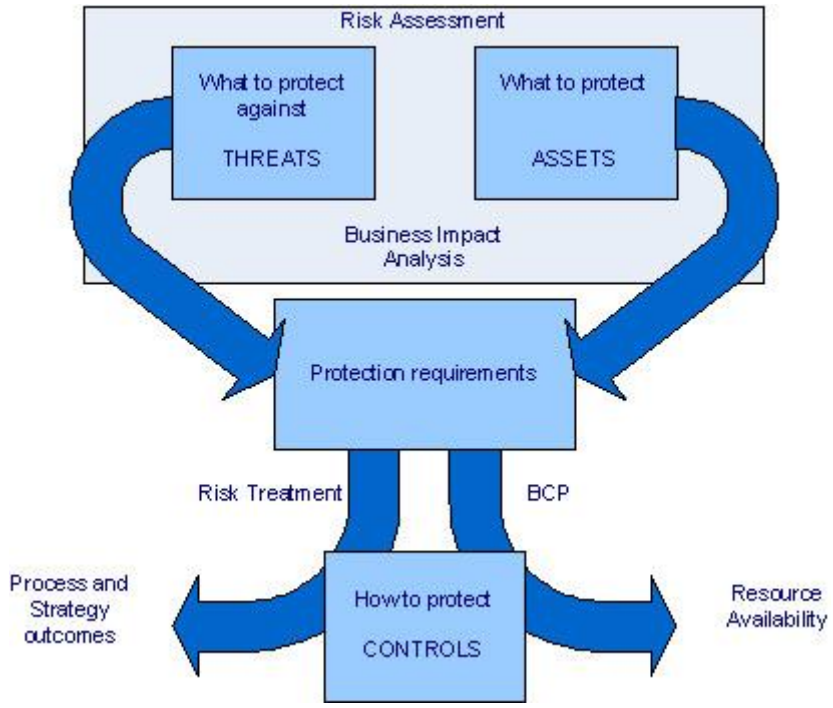
IT-palveluiden jatkuvuuden hallinta eli ITSCM (IT Services Continuity Management) on ITIL:n määrittelemä prosessikuvaus. Jatkuvuuden hallinnan tarkoitus on ylläpitää kykyä toipua yllättävistä vastoinkäymisistä IT-palveluissa. Varsinkin IT-alalla voi tulla yllättäviä haasteita tai vastoinkäymisiä, joita ei ole välttämättä osattu ennustaa. Organisaation on tärkeää ymmärtää, mitä vaikutuksia palvelun epäonnistumisella voi olla yrityksen liiketoiminnalle. Tämän takia on tärkeää ottaa huomioon jatkuvuuden hallinnan prosessi IT-palveluissa. Teknologia on tehnyt organisaatioiden liiketoiminnasta entistä tehokkaampaa. Tämän johdosta organisaatioiden jatkuvuuden hallinnan epäonnistuessa voivat seuraukset olla liiketoiminnan kannalta vakavat.

IT-palveluiden jatkuvuuden hallinnan päämääränä on tukea liiketoiminnan jatkuvuuden hallintaa eli BCM (Business Continuity Management). Tällä tarkoitetaan, että IT-

palvelut palautuvat sovituissa aikarajoissa aiheuttaen näin mahdollisimman pienen katkoksen palveluille. Hyvään IT-palveluiden jatkuvuuden hallintaan kuuluu suunnitelmat palveluiden palauttamiseksi sekä suorittaa säännöllisiä liiketoiminnan vaikutusanalyysejä BIA (Business Impact Analysis). Tähän kuuluu säännöllinen riskien analysointi ja hallinta harjoitukset, joilla varmistetaan prosessin toimivuus. [3, s.207–208.]

On tärkeää ottaa huomioon myös mahdollisten muutosten vaikutus jatkuvuuden hallinnan suunnitelmissa erityisesti liiketoiminnan kannalta tärkeissä kohteissa. Jos muutos epäonnistuu, pystytään tällöin nopeasti palauttamaan IT-palveluiden taso hyväksyttävälle tasolle. Mahdollisten ulkopuolisten alihankkijoiden kanssa kannattaa myös tehdä tarvittavat sopimukset, jos palveluiden jatkuvuuden takaaminen vaatii tätä. [3, s. 208.]

IT-palveluiden jatkuvuuden hallinta käsittelee laajempialaisempia tapahtumia, joilla on suurempi vaikutus liiketoimintaan kuin yksittäisillä tapauksilla. Liiketoiminnan vaikutusanalyysin testaus on hyvä tapa mitata taloudellista menetystä liiketoiminnalle. Tällöin pystytään määrittämään riittävät vaatimukset IT-palveluiden jatkuvuuden hallinnan kannalta. Mikä on jatkuvuuden hallinnan laajuus, riippuu täysin muun muassa organisaation rakenteesta, kulttuurista ja strategiasta. Kuvassa 1 kuvataan yleisesti jatkuvuuden hallinnan vaiheet. [2, s.209–210.]



Kuva 1. Jatkuvuuden hallinnan eri vaiheita [4].

2.2 Jatkuvuuden hallinnan toteutus oikeassa tilanteessa

Kun halutaan palautua IT-palveluita koskettavasta katastrofista, jatkuvuudenhallinta-prosessi nojautuu IT-laitteiden määrittelyjen kokonaisuuksiin ja IT-varoihin, jotka tukevat liiketoimintaprosessia. Jos organisaation täytyy siirtyä uuteen sijaintiin katastrofin sattuessa, jatkuvuudenhallintaprosessi määrittelee, kuinka esimerkiksi henkilöstö siirtyy uuteen sijaintiin tai missä säilytetään kopioita kriittisistä asiakirjoista. Prosessi ei kata suoraan pitkäaikaisia riskejä, vaikka ne vaikuttaisivat IT-palveluihin. Tämä johtuu siitä, että aina ei ole aikaa tunnistaa ja arvioida pitkäaikaisia riskejä. Pitkäaikaisia riskejä varten luodaan omat strategiat ja prosessit. IT-palveluiden jatkuvuuden hallinta ei myöskään kata pieniä teknisiä vikoja, ellei niillä sitten ole merkittävää vaikutusta liiketoimintaan. Pienet tekniset viat hoidetaan häiriönhallinnan prosessin puitteissa. [3, s. 210.]

Pienet välikohtaukset tulisi hoitaa organisaation IT-palvelukeskuksessa. Organisaatio voi hoitaa tai sisällyttää nämä riskit ja välikohtaukset myös seuraaviin prosesseihin:

- Saatavuuden hallinta
- Ongelmien hallinta
- Muutosten hallinta
- Laitteiden määrittelyjen hallinta
- Operatiivinen hallinta

ITIL tarjoaa vain oman näkemyksensä prosessista kuinka toimia. Se miten oikeassa tilanteessa toimitaan, riippuu paljon organisaatiosta ja siitä, kuinka kriittistä IT-palveluiden jatkuvuuden hallinta organisaatiolle on. Organisaatiot, joissa palveluiden tuotanto nojaa IT:seen, tulisi ottaa jatkuvuuden hallinta huomioon tarpeellisella vakavuudella. [3, s.210]

2.3 Jatkuvuuden hallinnan liiketoiminta-arvo ja elinkierto

Jatkuvuuden hallinnalla on tärkeä rooli tukea liiketoimintaa sekä sen jatkuvuutta. IT-palveluiden jatkuvuuden hallintaa käytetään luomaan tietoisuutta jatkuvuudesta ja siitä mitä tarvitaan palveluiden palautumiseen kriisitilanteista normaaliin tilanteeseen. Ideaalisessa tilanteessa liiketoiminnan jatkuvuuden täytyy ohjata IT-palveluiden jatkuvuutta. IT-palveluiden jatkuvuuden hallinta tarjoaa palautumisjärjestelyt IT-palveluille. Näiden järjestelyiden täytyy olla synkronoitu tunnistettujen liiketoimintavaikutusten, riskien ja tarpeiden kanssa. [3, s. 211.]

2.3.1 Elinkierron eri vaiheet

Organisaation kannattaa ottaa käyttöönsä jatkuvuuden elinkaari lähestymistapa, kun otetaan käyttöön IT-palveluiden jatkuvuuden hallinta prosessia. Jatkuvuuden hallinta takaa sen, että palveluiden jatkuminen ja palautumissuunnitelmat ovat yhdenmukaisia organisaation liiketoiminta-arvojen kanssa läpi prosessin elinkaaren. Jatkuvuuden hallinnan elinkaari alkaa suunnitelmien alullepanosta ja menee tämän jälkeen läpi kolme eri vaihetta [3, s.213.]

Näitä vaiheita ovat:

- Alullepano
- Tarpeet ja strategia
- Käyttöönotto
- Ylläpito

Edellä olevat vaiheet ovat palveluiden jatkuvuuden hallinnan vaiheita eli (SCM Service Continuity Management), joita IT-palveluiden jatkuvuuden hallinta tukee. Alullepano-, strategia- ja tarpeiden määrittelyvaiheet ovat osa liiketoiminnan jatkuvuuden hallintaa. Näiden vaiheiden aikana IT-palveluiden jatkuvuuden hallinnassa pitää ymmärtää liiketoimintaprosessien välinen suhde ja mikä vaikutus IT-palveluiden menettämisellä on tälle suhteelle. Liiketoiminnan tarveanalyysi ja riskianalyysi suoritetaan näiden vaihei-

den aikana, jotta voidaan tuottaa IT- ja liiketoiminnan jatkuvuuden strategiat. [3, s. 213–214.]

Elinkierron ensimmäinen vaihe on alullepano. Vaihe kattaa koko organisaation. Alullepanovaiheessa on tarkoitus määrittää erilaiset politiikat sekä se mitä resursseja tarvitaan. Tässä vaiheessa määritellään myös jatkuvuuden hallinnan laajuus, määritellään projektin organisaatio ja rakenne. Alullepanovaiheen jälkeen täytyy olla yhteisymmärrys edellä mainituista asioista. [3, s. 215–216.]

Elinkierron toinen vaihe kattaa tarpeet ja strategian. Vankka tarveanalyysi on avainasemassa liiketoimintaa kohtaavan kriisin käsittelyssä. Täytyy osata arvioida liiketoiminnan vaatimukset ja tarpeet IT-palveluiden jatkuvuudelle, jotta osataan arvioida, miten organisaatio selviää kriisitilanteesta. Huonosti toteutetulla tarveanalyysillä voi olla vakavat vaikutukset IT-palveluiden jatkuvuuden hallinnalle. [3, s. 217–218.]

Kolmantena vaiheena elinkierrossa on käyttöönotto. Kun strategia on viimeistelty, täytyy luoda IT-palveluiden jatkuvuussuunnitelmat. Näissä suunnitelmissa tulee huomioida liiketoiminnan jatkuvuus. Suunnitelmat tarjoavat tietoa kriittisistä systeemeistä, palveluista ja tiloista, jotka tulisi palauttaa käyttöön mahdollisimman nopeasti. Liiketoiminnan palvelut ovat yleensä hyvin riippuvaisia IT-palveluista, minkä takia jatkuvuussuunnitelmat tulee olla sellaiset, että liiketoiminta ei kärsi suurta vahinkoa häiriötilanteista. Suunnitelmien tulisi myös olla aina saatavilla avainhenkilöille. Kopioita suunnitelmista tulisi pitää erillisessä sijainnissa. [3, s. 246–247.]

Neljäs vaihe elinkierrossa on ylläpito. Tässä vaiheessa on tärkeää, että henkilöstö ja erityisesti IT-henkilöstö ovat tietoisia rooleistaan kriisin sattuessa. Tietoisuutta voidaan lisätä erilaisilla koulutuksilla ja harjoituksilla. Prosessin komponentit tulisi arvioida tasaisin väliajoin, jotta varmistetaan niiden ajantasaisuus. Aloitustestausten jälkeen olisi hyvä ylläpitää tasaista testausaikataulua. Suunnitelmia olisi myös hyvä testata suurien muutosten jälkeen. Näin varmistetaan, että muutokset on otettu huomioon jatkuvuuden hallinnan suunnitelmissa. Jos jatkuvuuden hallinnan suunnitelma ei toimi suunnitellulle muutokselle, tulee suunnitelmaa muuttaa ennen kuin tehdään muutos. [3, s. 253–254.]

Kuva 2. Elinkierron eri vaiheet.

2.3.2 Jatkuvuuden hallinnan tehokkuus elinkierron aikana

Kuvassa 2 esitetyt jatkuvuuden hallinnan elinkierron vaiheet antavat valmiin perusmallin jatkuvuuden hallinnan toteutukseen. Jatkuvuuden hallinnan tehokkuus riippuu enemmän siitä, kuinka sitoutuneita sen toteuttamisessa ollaan kuin siitä miten hyvin valmista mallia seurataan. Jos prosessiin ei olla tarpeeksi sitoutuneita tai se on huonosti suunniteltu, niin suuretkaan resurssit ei takaa prosessin onnistumista ja tehokkuutta. Jatkuvuuden hallinnasta voidaan saada toimivaa ja tehokasta käyttämällä siihen osoitettuja resursseja oikealla tavalla. Tähän voidaan päästä huolellisella suunnittelulla sekä tarkalla tarpeiden ja strategioiden kartoituksella.

Prosessin tehokkuutta voidaan testata riittävän säännöllisesti toteutetuilla harjoituksilla. Jos tehokkuudessa havaitaan puutteita harjoituksen aikana, on nämä puutteet helpompi korjata etukäteen kuin kriisin aikana. Kriisin aikana kaiken tulisi toimia saumattomasti ja mahdollisimman tehokkaasti, jotta katkoksesta ei aiheutuisi liiketoiminnalle suurta haittaa. Jatkuvuuden hallinnan prosessin heikko tehokkuus voi pahimmillaan aiheuttaa suuria taloudellisia menetyksiä organisaatioille, jotka nojaavat toimintansa IT:hen. Ennen kaikkea tehokkaalla toiminnalla saadaan kulutkin pidettyä kurissa. [3, s. 262–263.]

2.4 Yrityksen verkonhallinnan siirtyminen varasijaintiin

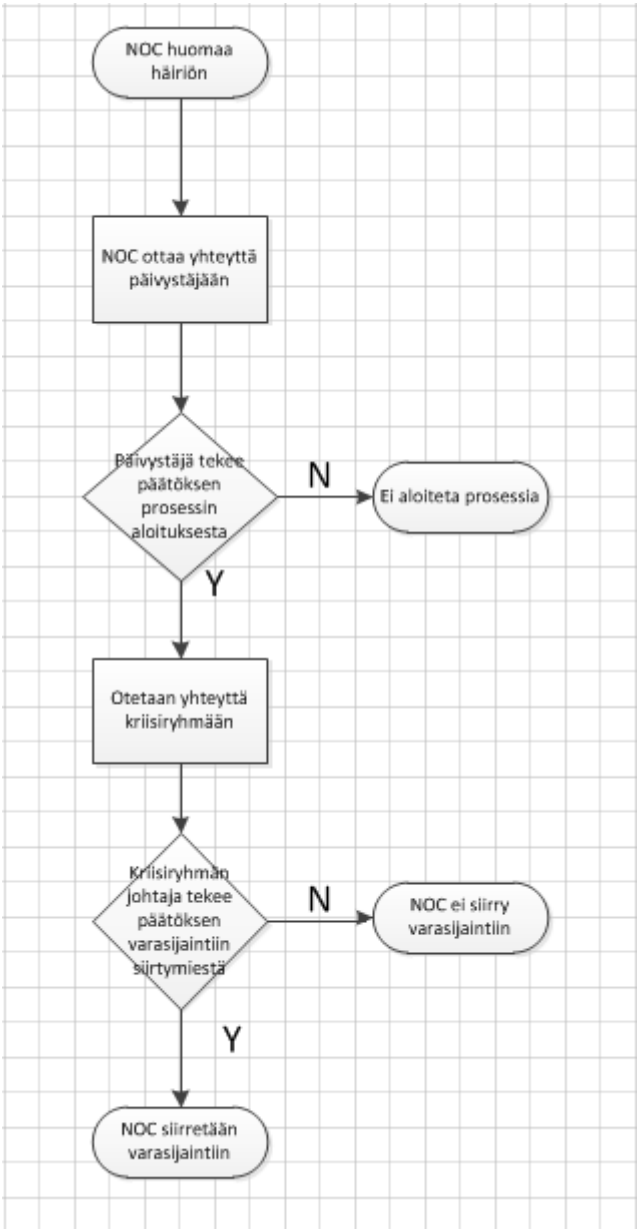
Yrityksen verkonvalvonnan ja hallinnan siirtämisessä varasijaintiin tulee huomioida monia tekijöitä. Tärkein asia, minkä pitää olla kunnossa siirrettäessä verkon valvontaa ja hallintaa varasijaintiin, on siirtymiselle suunniteltu prosessi. Ainakin verkonhallintakeskuksen eli NOC-henkilöstön (Network Operations Centre), erikseen nimetyn kriisiryhmän sekä järjestelmäkehitysryhmän täytyy olla tietoisia prosessin etenemisvaiheista. Cygate Oy:llä on erikseen nimetty kriisiryhmä kriisitilanteiden varalle. Tämä ryhmä koostuu viidestä henkilöstä. Jatkuvuudenhallinnanprosessi etenee näiden henkilöiden kautta, ja he organisoivat tarvittavan henkilöstön hoitamaan kriisiä.

Prosessi lähtee käyntiin siitä, kun NOC huomaa nykyisen verkonhallintakeskuksen toimimattomuuden, jonka on aiheuttanut esimerkiksi sähkökatko tai joku muu häiriö. Havaitsemisen jälkeen NOC ottaa yhteyttä päivystäjään, joka tekee päätöksen, laitetaanko jatkuvuuden hallinnan prosessi käyntiin. Jos prosessi päätetään laittaa käyntiin, soittaa NOC kriisiryhmän jäsenille, kunnes joku jäsenistä on saatu kiinni. Kun joku kriisiryhmän jäsenistä on saatu kiinni, tehdään puhelun aikana päätös kriisiryhmän kokoonpanosta. Tavoitettu kriisiryhmän jäsen voi tarvittaessa toimia yksin ECAB:n (Emergency Change Advisory Board) jäsenenä. Kriisiryhmän johtaja tekee päätöksen verkon hallinnan ja valvonnan siirtämisestä varasijaintiin. Hänen täytyy seurata tilannetta niin kauan, kunnes NOC on toimintakykyinen varasijainnissa. Kriisiryhmän johtaja tekee myös päätöksen, miten kommunikointi hoidetaan kriisin aikana ja kuinka viestintä hoidetaan asiakkaiden suuntaan.

Siirtyminen varasijaintiin suoritetaan joko omilla henkilöautoilla tai taksilla. NOC-henkilöstön siirtyminen varasijaintiin määräytyy tilanteen mukaan. Sähkökatkon tapauksessa yksi NOC-työntekijä siirretään varasijaintiin noin 90 minuutin kuluttua tai siinä vaiheessa, kun NOC menettää sähköt kokonaan. Tässä tapauksessa oletetaan, että verkonhallintakeskus on menetetty pidemmäksi aikaa. Jos verkonhallintakeskus on menetetty pidemmäksi aikaa, siirtyy myös muu NOC-henkilöstö varasijaintiin.

Pääsy varaverkonhallintakeskukseen on järjestetty asiaankuuluvilla tunnisteilla. Pääsy varaverkonhallintakeskukseen tulee olemaan NOC-henkilöstöllä, 2-tason asiantuntijoilla, järjestelmäkehitysryhmällä sekä kriisiryhmällä. Tarvittavat dokumentaatiot prosessista löytyvät Cygaten tuotannon sisäverkosta sekä erillisiltä salatuilta USB-muistitikuilta, jotka ovat kriisiryhmän jäsenten hallussa.

Varaverkonhallintakeskuksen työasemat ja puhelimet ovat käyttövalmiina. Työasemia käydään päivittämässä kerran kuukaudessa. Tämä kierto perustuu Windowsin päivitysten aikatauluun. Päivityskäynneistä tehdään oma lista Cygaten tuotannon sisäverkkoon. Myös ohjeistus prosessista tullaan lisäämään tuotannon sisäverkkoon. Kuvassa 3 kuvataan ITSCM-prosessin etenemistä. [5.]



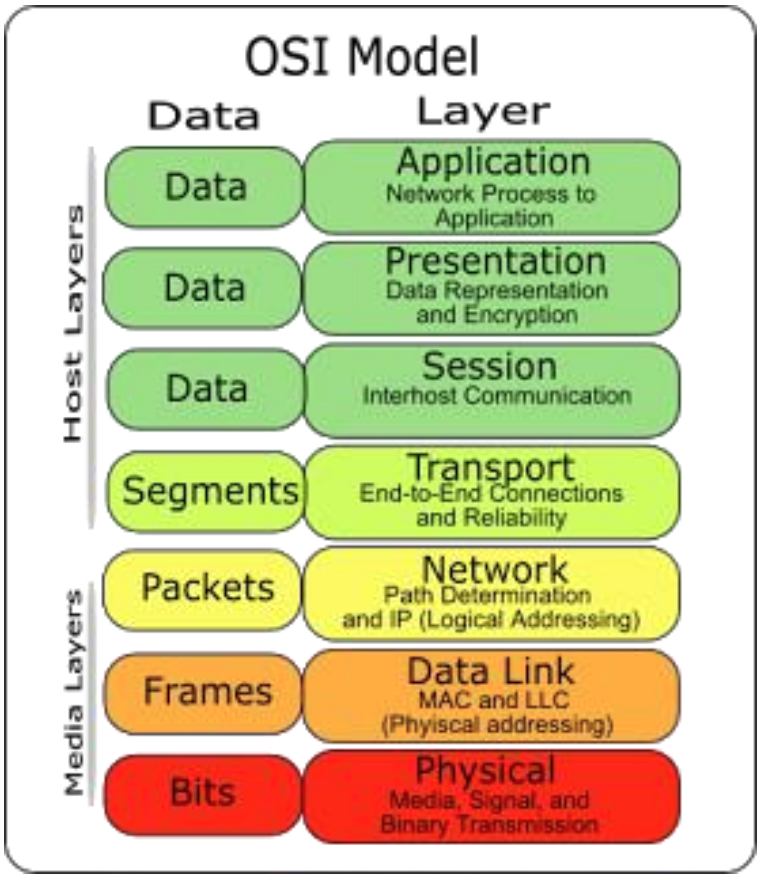
Kuva 3. ITSCM-prosessin vaiheet.

3 Verkon valvonnassa ja hallinnassa käytettäviä tekniikoita

Organisaatioiden verkkojen ja verkkolaitteiden määrän kasvaessa on tärkeää, että näitä valvotaan. Verkon valvonnan tärkeys korostuu sitä enemmän, mitä yrityksellä on erilaisia verkkolaitteita ja kuinka riippuvainen se on niistä. Jo pienikin katkos verkkolaitteissa voi aiheuttaa isoja taloudellisia menetyksiä organisaatiolle. Tämän vuoksi verkonvalvonnan tärkeyttä ei kannata vähätellä. Verkonvalvonnan avulla vikatilanteisiin osataan reagoida nopeammin ja näin minimoida viasta aiheutuvat mahdolliset haitat. Tässä luvussa käydään läpi yleisimpiä verkon valvonta- ja hallintatekniikoita. [6.]

3.1 SNMP-protokolla

SNMP-protokolla eli Simple Network Management Protocol perustuu reititinpohjaisiin valvontatekniikoihin. Sillä voidaan kysellä verkossa olevan laitteen tilaa. Tämä laite voi antaa hälytyksiä esimerkiksi, jos laitteen tilanne on muuttunut. SNMP-agentti sisältää sovelluksen, jolla on tietoa hallittavista laitteista. Agentti kääntää tämän tiedon SNMP-protokollalle luettavaan muotoon. SNMP on sovellus tason protokolla OSI-mallissa eli Open System Interconnection model, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä eri kerroksessa. Kuvassa 3 Esitellään OSI-mallin seitsemän eri kerrosta, jossa SNMP-protokolla sijoittuu Transport-kerroksen päälle. SNMP-sanoma kehystetään kuljetuskerroksen UDP-otsikolla (User Datagram Protocol). TCP/IP-arkkitehtuurissa (Transport Control Protocol/Internet Protocol) SNMP sijoittuu sovellustasolle [6.]



Kuva 4. OSI-mallin eri kerrokset [7].

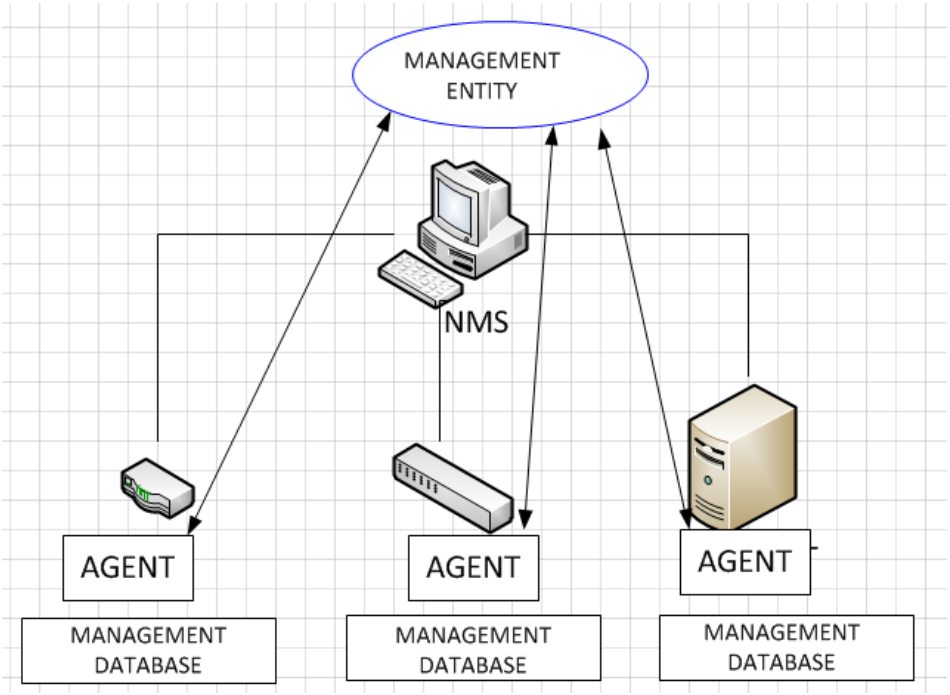
SNMP:stä on olemassa kolme eri versiota.

- SNMPv1
- SNMPv2
- SNMPv3

SNMPv3 ei ole kuitenkaan laajalti käytössä. SNMP voidaan jakaa kolmeen eri komponenttiin. Ensimmäinen komponentti on hallinnoidut laitteet. Hallinnoidut laitteet sisältävät SNMP-agentin, joka on hallinnoiduissa laitteessa pyörivä ohjelma. Tällä ohjelmalla on paikallinen tietous hallintatiedoista, jotka se kääntää SNMP-protokollalle luettavaan muotoon. Hallinnoituja laitteita voivat olla muun muassa erilaiset verkossa olevat laitteet. Kolmas komponentti on NMS eli Network Management System. Tämä on sovellus, jota ajetaan tietokoneissa, joilla hallitaan valvottavaa verkkoa. Hallittavassa kokonaisuudessa täytyy olla ainakin yksi NMS. SNMP käyttää neljää eri operaatiota toiminnassaan. Nämä operaatiot ovat Get, GetNext, Set ja Trap. [6.]

- Get-operaatiota käytetään, kun NMS pyytää tietoa hallinnoidusta laitteesta.
- GetNext-operaatiota käytetään, jos hallinnoitu laite ei palauta mitään arvoa Get kyselyyn. Tällöin GetNext-operaatio palauttaa seuraavan objekti-instanssin arvon.
- Set-operaatio on NMS:n lähettämä pyyntö agentille, jolla asetetaan arvoja agentissa.
- Trap-operaatio on agentin lähettämä ilmoitus NMS:lle muuttuneesta tilasta.

SNMP on hyödyllinen työkalu verkonvalvonnassa ja -hallinnassa. SNMP käyttää mallia, jossa saatavilla oleva informaatio määritellään MIB:ssä (Management Information Base). MIB on tietokanta, jolla hallitaan laitteita verkossa. MIB koostuu eri objekteista, jotka muodostavat hierarkkisen rakenteen. SNMP:n heikkoutena ovat puuttuvat autentikointiominaisuudet. Tämä tekee siitä haavoittuvaisen verkkohyökkäyksille. Kuvassa 5 on esitelty SNMP:n rakenne. [8.]



Kuva 5. SNMP:n rakenne.

3.2 Etämonitorointi

RMON (eng. Remote Monitoring) eli etämonitorointi on SNMP:ssä käytettävän MIB:n laajennus. RMON on kykeneväinen asettamaan hälytyksiä, joilla valvotaan verkkoa perustuen määriteltyihin kriteereihin. Se sallii järjestelmänvalvojan hallita etäverkkoja samalla tavalla kuin paikallisia verkkoja yhdestä sijainnista. RMON:sta on kaksi eri versiota: RMON ja RMON2. RMON2:lla pystytään valvomaan paketteja OSI-mallin kaikista seitsemästä tasosta, mikä tekee siitä monipuolisemman valvonta ja -hallintatyökalun kuin SNMP. [6.]

RMON koostuu kahdesta komponentista. Nämä komponentit ovat valvontalaite (eng. probe) ja hallintapääte (eng. client). RMON-valvontalaite kerää ja varastoi tietoa valvottavasta verkosta. Valvontalaite on verkkolaitteistoon integroitu sovellus, jota voidaan ajaa myös työasemassa. Hallintapääte kommunikoi valvontalaitteen kanssa SNMP:llä, jonka avulla hallintapääte saa RMON-dataa valvontalaitteelta. RMON käyttää yhdeksää eri valvontaryhmää saadakseen tietoa verkosta. Nämä valvontaryhmät ovat esitelty taulukossa 1. [6.]

Taulukko 1. RMON:n valvontaryhmät

Statistics	Valvontalaitteen mittaamaa tilastoa valvotuista laitteista
History	Tallentaa historiatietoja valituista statistiikoista
Alarm	Ottaa jaksollisesti näytteitä ja vertaa niitä kynnysarvoihin.
Host	Sisältää statistiikkaa verkon päätelaitteista
HostTopN	Pitää kirjaa aktiivisimmista yhteyksistä
Filters	Asettaa filtereitä määritetyille kaavoille
Packet capture	Kerää ja edelleen lähettää datapaketteja
Events	Kontrolloi tapahtumien luontia ja niistä lähteviä ilmoituksia
Token Ring	Tukee Token Ring teknologiaa

3.3 Netflow

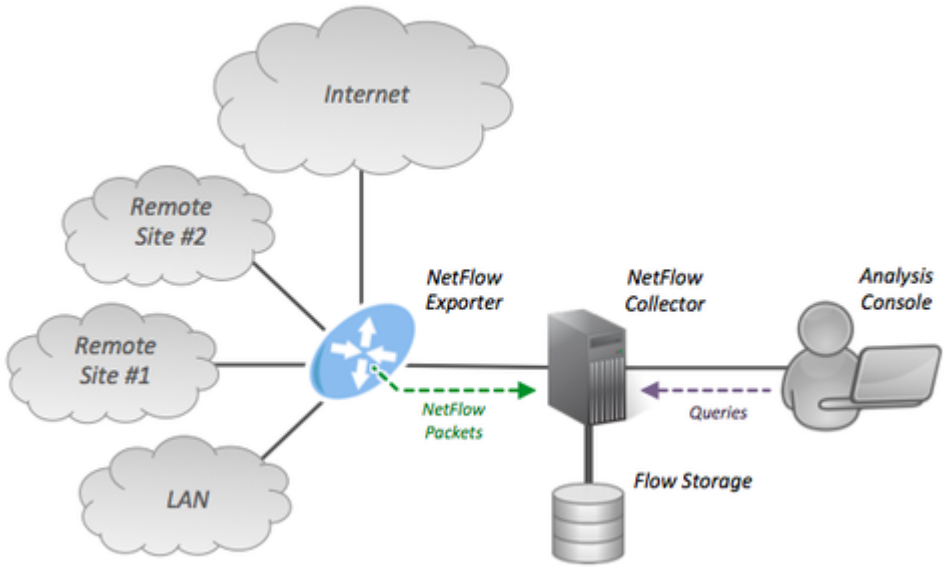
Netflow on ominaisuus, joka on ensimmäisenä esitelty Cisco reitittimissä. Netflowsta kerätyllä datalla järjestelmänvalvoja pystyy muun muassa määrittämään verkkoliikenteen lähteen, kohteen, palveluluokan ja mahdollisen ruuhkan aiheuttajan verkossa.

Netflowssa Netflow Exporter kerää vuotaulukkoa, jonka se lähettää kerääjälle määräajoin. Netflow koostuu kolmesta eri komponentista.

- Flow Caching
- Flow Control
- Data Analyzer

Flow Caching eli pakettivirran tallennus välimuistiin, on operaatio, jossa ensimmäisenä reitityspolun läpäisseen paketin vuo ja sen laskurit tallentuvat välimuistiin. Välimuistin tietoja siirretään säännöllisesti Flow Collectoriin, joka on vastuussa datavirtauksen keräämisestä, suodattamisesta ja varastoinnista. Se sisältää historiatietoja portin läpi menneistä datavirroista. Flow Collector hoitaa myös datan koon muokkausta valittujen suodattimien avulla. Data Analyzer analysoi kerättyä dataa. Kerättyä dataa voidaan käyttää moniin eri tarkoituksiin. Sitä voidaan käyttää esimerkiksi verkon suunnitteluun ja laskutukseen.

Netflown etu verrattuna muihin valvontatyökaluihin on sen monipuoliset verkkoliikenteen analysointityökalut. Kerätty data pystytään esittelemään käyttäjäystävällisemmin kuin SNMP:ssä ja RMON:ssa. Käyttämällä verkon analysointiin tarkoitettuja ohjelmia voidaan luoda erilaisia kaavioita ja taulukoita kerätystä datasta. Hyvä työkalu saadun datan analysointiin on Netflow Analyzer. Kuvassa 6 kuvataan Netflown arkkitehtuuri. [6.]

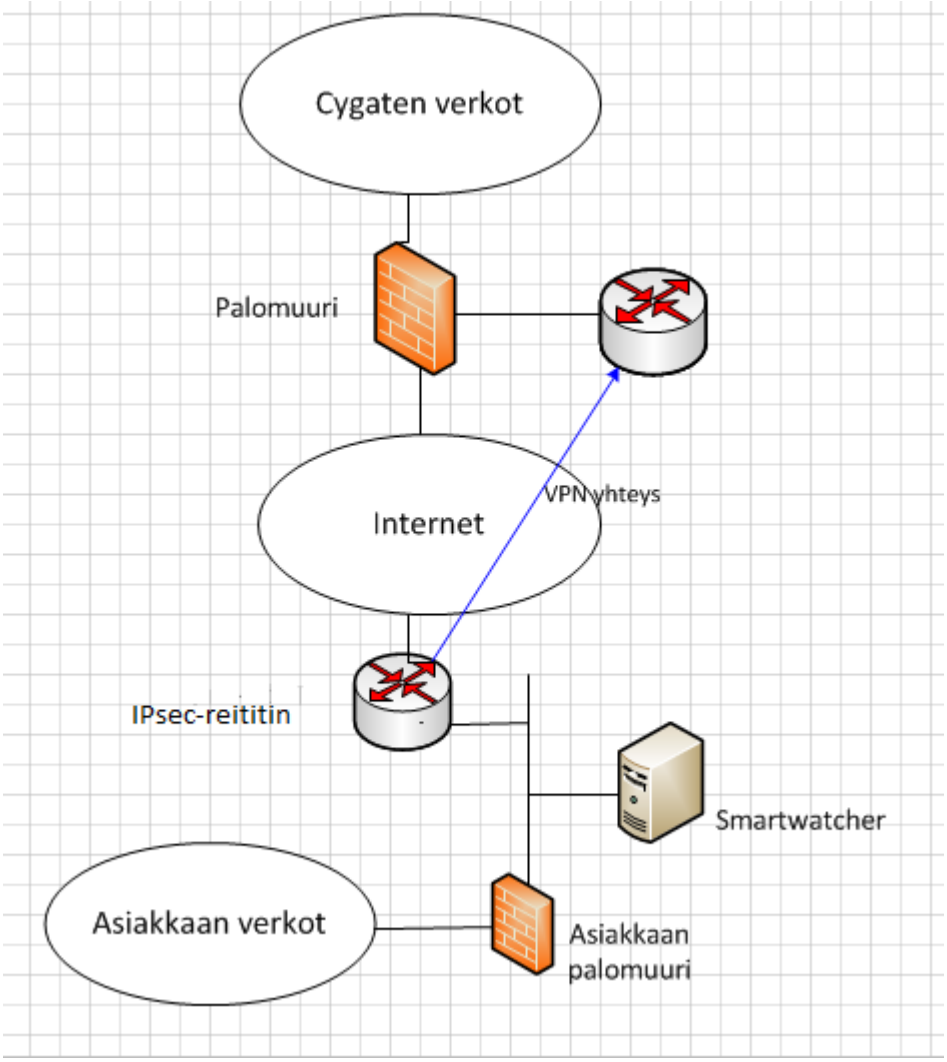


Kuva 6. Netflown arkkitehtuuri [9].

3.4 Cygaten käyttämä verkonvalvontatekniikka

Cygaten tuottaa verkon valvonta- ja hallintapalveluja, koska verkkolaitteet ovat tärkeitä komponentteja nykypäivänä kaikissa yrityksissä. Tämän takia niitä on tärkeää valvoa. Cygaten verkonvalvonta valvoo sekä Cygaten omia verkkolaitteita että asiakkaiden verkkolaitteita. Verkkolaitteiden valvontaa suoritetaan verkonhallintakeskuksessa.

Cygaten nykyiset valvontaratkaisut perustuvat Smartwatcherin käyttöön. Smartwatcher on Linux-pohjainen palvelin, jonka avulla voidaan valvoa asiakkaan verkon laitteita. Tällaisia laitteita ovat muun muassa reitittimet, kytkimet, palvelimet ja palomuurit. Smartwatcher on sijoitettu asiakkaan verkkoon. Valvonta- ja hallintamenetelmät, joita Smartwathcer käyttää ovat muun muassa ICMP eli Internet Control Message Protocol ja SNMP. ICMP Echo -pyyntöjä (Ping) Smartwatcher lähettää valvottavaan IP-osoitteeseen, jolloin pystytään valvomaan laitteen saavutettavuutta. Tällä menetelmällä voidaan valvoa myös viivettä ja pakettihävikkiä. SNMP:llä saadaan taas muuta statistiikkaa valvottavista laitteista. SNMP:n avulla laitteista voidaan ottaa myös varmuuskopiot laitteille määritellyistä asetuksista. Kuvassa 7 havainnollistetaan Smartwatcher-valvontaratkaisua.



Kuva 7. Esimerkki Smartwatcher-valvontaratkaisusta.

4 Verkonhallintakeskuksen tekninen toteutus

Verkonhallintakeskuksen tekninen toteutus tehtiin yhteistyössä Cygaten sisäisen IT:n ja asiantuntijoiden kanssa. Tässä luvussa kerrotaan, miten varaverkonhallintakeskus asettuu Cygaten olemassa olevaan tuotannon verkkoon ja miten laitteet on määritelty. Tässä luvussa mainitut VLAN-id:t (Virtual Local Area Network) ja IP-osoitteet on muutettu tietoturvasyistä.

4.1 Verkon liittyminen muuhun Cygaten verkkoon

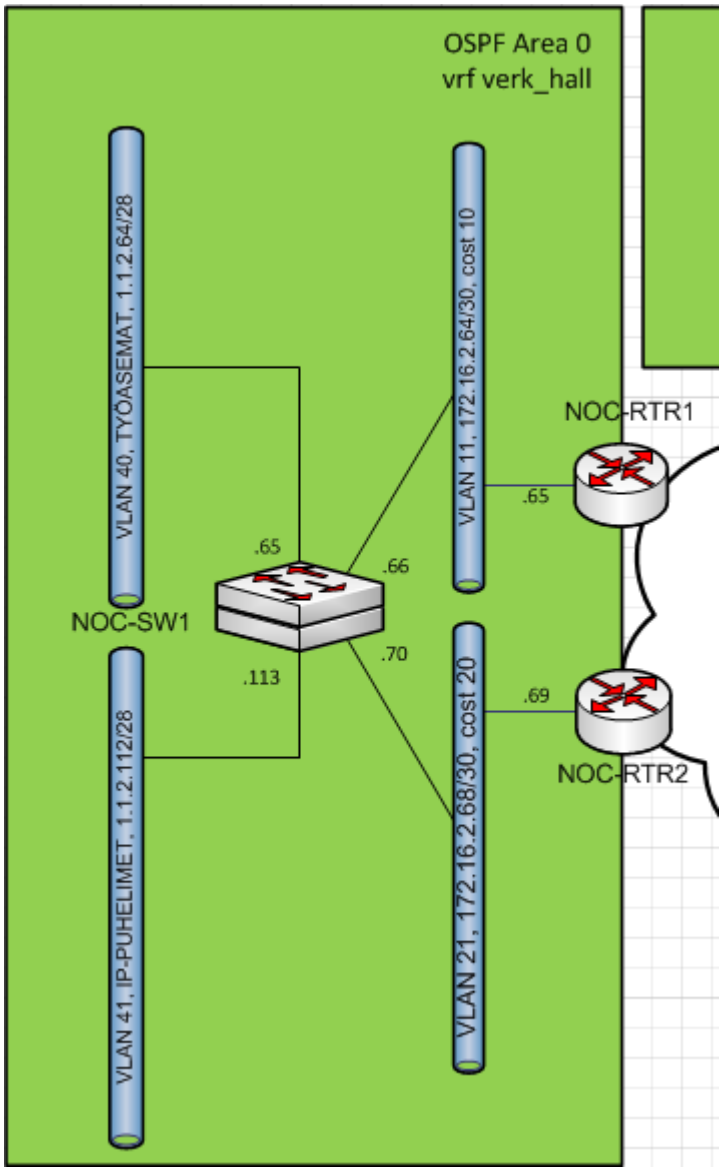
Varaverkonhallintakeskuksen verkko liitettiin olemassa olevaan Cygaten verkkoon. Tämä oli helpoin toteutustapa tälle työlle. Cygaten tämän hetkinen verkonhallintakeskuksen verkko koostuu kahdesta reitittimestä ja niiden takana olevasta neljästä eri VLAN:sta:

- VLAN 40, verkko verkonhallintakeskuksen työasemille
- VLAN 41, verkko verkonhallintakeskuksen IP-puhelimille
- VLAN 11 ja 21, transit VLAN:it muihin Cygaten tuotannon verkkoihin

Nämä verkot ovat yhteydessä Cygaten VRF:ään (Virtual Routing and Forwarding) nimeltä verk_hall. VRF:llä tarkoitetaan virtuaalista reititysinstanssia. VRF verk_hall muodostaa oman reititysinstanssin, joka liittää Cygaten tuotannon verkot toisiinsa. Reititysprotokollana tässä instansissa käytetään MPLS:ää eli Multi Protocol Label Switching. MPLS on reititysteknologia, jolla on helppo hallita IP-liikennettä isoissa verkoissa. MPLS:ssä IP-paketit merkitään omalla leimalla (eng. encapsulate) ensimmäisessä MPLS-laitteessa. Tämän jälkeen paketit reititetään leiman mukaan. [10;11.]

Reititysprotokollana edellä mainittujen VLAN:ien reitityksessä käytetään OSPF:ää eli Open Shortest Path First. OSPF on dynaaminen reititysprotokolla, jossa IP-paketin reitti määränpäähän määräytyy Dijkstran algoritmin mukaan. Tässä algoritmissa otetaan huomioon muun muassa reitin varrella olevien linkkien siirtonopeus, kun valitaan parasta reittiä määränpäähän. OSPF on laitevalmistajasta riippumaton reititysprotokolla, minkä takia sitä on hyvä käyttää verkoissa, joissa on eri laitevalmistajien laitteita. Sen takia sitä käytetään myös tässä työssä.

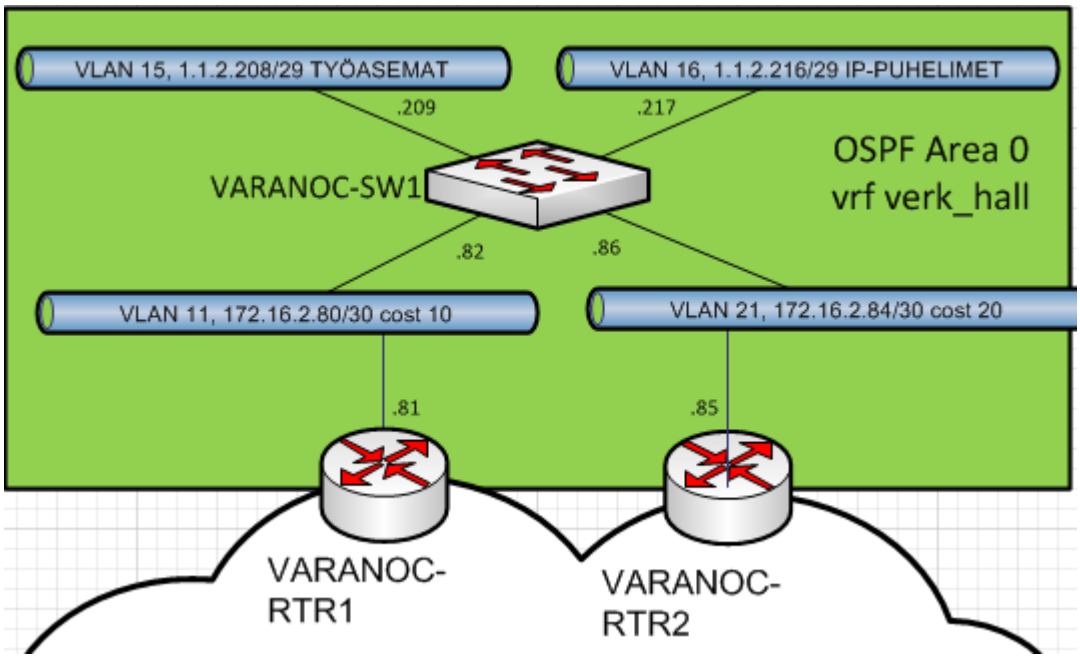
VLAN:issa 11 ja 21 käytetään OSPF:n point-to-point -tyyppiä. Tällä tyypillä tarkoitetaan sitä, että OSPF muodostaa vain yhden naapuruuden (eng. adjacency). VLAN:ssa 40 ja 41 on määriteltynä passiivinen OSPF. Tämä tarkoittaa sitä, että VLAN:it mainostavat verkkojansa ilman, että ajavat itse OSPF-reititysprotokollaa. Kytkimen määritykset käydään tarkemmin läpi seuraavassa alaluvussa. Kuvassa 8 näkyy nykyinen verkonhallintakeskus ja sen VLAN:it. [10;12.]



Kuva 8. Verkonhallintakeskuksen verkko [10].

Varaverkonhallintakeskuksen verkko tulee olemaan rakenteeltaan samantyylinen kuin pääverkonhallintakeskuksen verkko. Ainoastaan työasemien ja IP-puhelinten VLAN:ien nimet, numerot ja IP-osoitteet muuttuvat. Varaverkonhallinnan VLAN:it 15 ja 16 vastaavat VLAN:eja 40 ja 41. Myös näihin VLAN:eihin on määritelty passiivinen OSPF. Työasemat ja IP-puhelimet on laitettu omiin verkkoihin pääverkonhallintakeskuksen tapaan, koska niiden liikennettä ei haluta sekoittaa keskenään. Erityisesti IP-verkossa kulkeva ääni on hyvä määritellä omaan verkkoonsa, koska se vaatii enemmän verkkokaistaa. Transit VLAN:it 11 ja 21 on määritelty samoilla parametreillä kuin pääverkonhallintakeskuksessa. Transit VLAN:lla tarkoitetaan VLAN:ia, joka on 3-tason (eng. Layer-3) laitteiden välillä. 3-tason laitteella tarkoitetaan verkkolaitetta, joka välittää IP-

liikennettä. Varaverkonhallintakeskuksen työasemat tullaan liittämään Cygaten tuotannon toimialueeseen. Kuvassa 9 näkyy varaverkonhallintakeskus ja sen VLAN:it.



Kuva 9. Varaverkonhallintakeskuksen verkko [10].

4.2 Varaverkonhallintakeskuksen kytkimen määrittely

Tässä aliluvussa kerrotaan, miten varaverkonhallintakeskuksen kytkin ja verkot on määritelty keskittyen varaverkonhallintakeskuksen kannalta olennaisimpiin määrittelyihin. Kytkimenä käytettiin Juniperin 48-porttista kytkintä, joka voi toimia reitittimen tavoin 3-tason laitteena. Kytkimestä lähtee valokuitukaapelit toimipisteen kahteen reitittimeen, jotka ovat yhteydessä Cygaten VRF:ään nimeltä verk_hall.

Ensiksi kytkimeen määriteltiin kytkimen perusasetukset. Näihin kuuluivat esimerkiksi järjestelmän asetukset, aikavyöhykeasetukset, pääsynhallinta-asetukset ja pääkäyttäjän (eng. root) salasana. Tässä yhteydessä määriteltiin myös käyttäjä kytkimelle. Suurin osa kytkimen perusasetuksista saatiin kopioitua pääverkonhallintakeskuksen kytkimeltä. Kytkimeen määriteltiin hallintayhteys ja se lisättiin verkonvalvonnan piiriin. [13;16.]

Kytkimeen täytyi määritellä kaksi porttia runkoyhteyksille (eng. trunk-port), joista lähtee yhteydet toimipisteen reitittimille. Runkoyhteysportilla tarkoitetaan porttia, jonka läpi voi

kulkea useamman VLAN:in liikenne. Transit VLAN:ien 11 ja 21 liikenne määriteltiin kulkemaan näistä porteista. Runkoyhteysporttien määritykset tehtiin niihin portteihin, joista haluttiin useamman VLAN:in verkkoliikenteen kulkevan. Tähän käytettiin kytkimen valokuituportteja nopeiden yhteyksien takaamiseksi. Runkoyhteysportit määriteltiin kytkimelle seuraavilla komennoilla: [14]

```
set interfaces ge-0/1/0 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/1/0 unit 0 family ethernet-switching vlan members verk_hall-transit
```

Kytkin määriteltiin käyttämään LACP:tä (Link Aggregation Control Protocol). LACP:llä voidaan sitoa monta fyysistä porttia yhdeksi loogiseksi portiksi. Tämä tuo luotettavuutta yhteyteen, jos joku fyysinen portti ei enää pysty kuljettamaan verkkoliikennettä. LACP-portiksi voidaan määritellä sekä VLAN-merkittyjä että ei-VLAN-merkittyjä portteja. Kytkimeen määriteltiin LACP aktiiviseksi eli LACP-portti vaihtaa LACP-paketteja toiseen päähän määritellyn LACP-portin kanssa. LACP määriteltiin kytkimelle koskemaan kaikkia VLAN:eja. Määritykset tehtiin seuraavilla komennoilla [15.]:

```
set interfaces ae0 aggregated-ether-options lacp active

set interfaces ae0 aggregated-ether-options lacp periodic fast

set interfaces ae0 unit 0 family ethernet-switching port-mode trunk

set interfaces ae0 unit 0 family ethernet-switching vlan members all
```

Kytkimeen täytyi määritellä myös omat portit VLAN:eille. Tämä tehtiin sen takia, että verkkoliikenne kulkisi VLAN:eissa. VLAN-portit määriteltiin seuraavalla komennolla:

```
set interfaces vlan unit <id> family inet address <ip-address>/<mask>
```

Yllä olevaa komentoa käytettiin kaikkien VLAN:ien konfigurointiin. Edellä olevassa komennossa `<id>` korvattiin VLAN:in id:llä ja `<ip-address>/<mask>` korvattiin IP-osoitteella ja aliverkon peitteellä. Molemmissa VLAN:eissa käytettiin aliverkon peitteenä 255.255.255.248 -osoitetta. Tämä tarkoittaa, että verkkoon mahtuu korkeintaan

kuusi laitetta. Tällä aliverkotuksella pyrittiin säästämään IP-osoitteita. Jos verkkoon tulevaisuudessa halutaan enemmän laitteita, täytyy osoiteavaruutta laajentaa. Kytkimeen määriteltiin seuraavat VLAN-portit:

- VLAN 15, VLAN varaverkonhallintakeskuksen työasemille
- VLAN 16, VLAN varaverkonhallintakeskuksen IP-puhelimille
- VLAN 11, Transit VLAN VRF instanssi verk_hall muihin osiin
- VLAN 21, Transit VLAN VRF instanssi verk_hall muihin osiin

Kytkimeen määriteltiin vielä VLAN-portit toimistoyhteyksiä varten ja erillinen vierailija VLAN. Näitä ei kuitenkaan käsitellä tässä työssä. Kaikki edellä mainitut VLAN:it määriteltiin 3-tason porteiksi vierailija VLAN:ia lukuun ottamatta. VLAN:it määriteltiin 3-tason porteiksi, koska niiden haluttiin välittävän IP-liikennettä. VLAN:it määriteltiin 3-tason porteiksi seuraavilla komennoilla [17.]:

```
set vlans <VLAN name> vlan-id <id>

set vlans <VLAN name> l3-interface vlan.<id>
```

Fyysiset portit, joihin liitettiin työasemat ja IP-puhelimet tuli määritellä se VLAN, jonka liikenne porttiin haluttiin kulkevan. Kytkinportit, joihin kytkettiin työasemat, määriteltiin VLAN 15:een. Kytkinportit IP-puhelimia varten määriteltiin VLAN 16:een.

Kytkimeen tuli määritellä reititys, jotta verkonhallintakeskuksen yhteydet toimisivat sisäverkkoon sekä ulkomaailmaan. Kytkimeen määriteltiin reititysinstanssi verk_hall, jonka jälkeen määriteltiin reititysprotokollaksi OSPF. Reititysinstanssi verk_hall toimii ikään kuin omana loogisena reitittimenä. Yhdessä fyysisessä laitteessa voi olla useita virtuaalisia reititysinstansseja. Tämä on mahdollista sen takia, että verkkopolut muodostavat omat segmenttinsä. Tämä tehtiin sen takia, että Cygaten eri verkkojen liikenne saadaan erotettua toisistaan, mikä lisää tietoturvallisuutta. VRF:ää määriteltäessä täytyi ensin määrittää kuvaus sekä instanssin tyyppi. Kuvauksena käytettiin jo olemassa olevaa instanssia verk_hall ja tyyppinä virtuaalireititintä. Reititysinstanssiin kuuluvat portit täytyi myös määritellä. Reititysinstanssiin määriteltiin kuuluvaksi työasema, IP-

puhelin ja transit VLAN:it. Reititysinstanssi sekä siihen kuuluvat VLAN:it määriteltiin kytkimelle seuraavilla komennoilla [18.]:

```
set routing-instances verk_hall description "Cygate verk_hall"

set routing-instances verk_hall instance-type virtual-router

set routing-instances verk_hall interface vlan.<id>
```

Reititysprotokolla OSPF määriteltiin reititysinstanssin sisään, jotta varaverkonhallintakeskuksen verkot reitittyisivät reititysinstanssin sisällä ja sitä kautta Cygaten muihin reititysinstansseihin. Työasemien ja IP-puhelimien VLAN:hin määriteltiin passiivinen OSPF. Passiivinen OSPF määriteltiin, koska verkot joiden takana on vain päätelaitteita, ei tarvitse lähettää reitityspäivityksiä. Transit VLAN:hin 11 ja 21 määriteltiin OSPFn point-to-point-tyyppi. Tämä tyyppi määriteltiin, koska VLAN:it 11 ja 21 muodostavat vain yhden naapuruuden. VLAN:iin 11 määriteltiin OSPF metric-arvoksi 10 kun taas VLAN:iin 21 määriteltiin arvoksi 20. Tällä määrityksellä OSPF käyttää IP-pakettien reitityksessä sitä reittiä, jolla on pienempi metric-arvo. VLAN 11 määriteltiin tällä tavoin pääreitiksi ja VLAN 21 varareitiksi siltä varalta jos VLAN 11 epäonnistuu.

OSPF-määrityksiin VLAN:lle 11 ja 21 määriteltiin arvot myös hello-intervallille ja dead-intervallille. Hello-interval tarkoittaa aikaväliä hello-pakettien välissä, joita lähetetään OSPF naapurille. Dead-interval on ajanjakso, jonka jälkeen naapuruuden tila muuttuu FULL-tilasta DOWN-tilaan. Tämä arvo on oletuksena neljä kertaa suurempi kuin hello-interval. Tässä määrityksessä käytettiin kolme kertaa suurempaa arvoa. Tämä tehtiin sen takia, että OSPF-topologiassa havaitut muutokset halutaan huomata nopeammin. Huonona puolena tästä saattaa aiheutua lisääntynyt reititysliikenne. OSPF määriteltiin seuraavilla komennoilla: [18]

```
set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.15 passive

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.16 passive

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.11 point-to-point
```

```
set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.11 metric 10

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.11 hello-interval 1

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.11 dead-interval 3

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.21 point-to-point

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.21 metric 20

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.21 hello-interval 1

set routing-instances verk_hall protocols ospf area 0.0.0.0 in-
terface vlan.21 dead-interval 3
```

4.3 Varaverkonhallintakeskuksen työasemat ja niissä käytettävät ohjelmat

Verkonhallintakeskusta varten hankittiin neljä kannettavaa työasemaa. Kannettavat työasemat hankittiin Cygaten sisäisen IT:n toimesta. Tässä aliluvussa kerrotaan, mitä eri ohjelmia työasemille asennettiin ja kuinka ne liitettiin Cygaten toimialueeseen.

Varaverkonhallintakeskuksessa käytettävät työasemat liitettiin telakoihin, joten niitä ei tarvitse kytkeä erikseen verkkovirtajohtoon. Jokaiseen telakkaan liitettiin myös 22-tuumainen näyttö, näppäimistö ja hiiri parantamaan työskentelymukavuutta. Työasemissa on tarpeeksi tehoa verkonhallinnassa ja valvonnassa käytettäviin sovelluksiin. Tämän mahdollistaa Intelin i7-neliydinprosessori ja 8 GB keskusmuistia. Käyttöjärjestelmänä työasemissa käytetään 64-bittistä Windows 7 Enterprisea. Työasemille annettiin kiinteät IP-osoitteet työasemille allokoidusta verkosta.

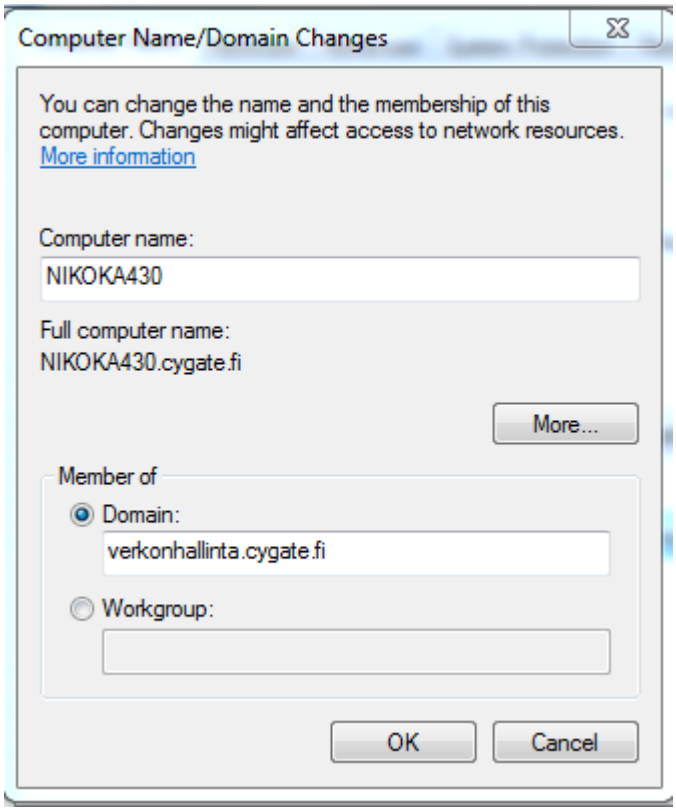
Ensin työasemille asennettiin puhdas Windows 7 Enterprise, joka Windows -komponenttien lisäksi ainoastaan Office 2010 paketin. Office-pakettiin kuuluu Word, Excel, PowerPoint ja Outlook. Tämän jälkeen yhdelle työasemalle asennettiin tarvittavat ohjelmat. Ohjelmien asennuksen jälkeen työasemalle ajettiin sysprep-komento ja

otettiin levykuvasta kopio. Sysprep-komennolla tarkoitetaan sitä, että levykuvasta eli kopiosta poistetaan kaikki uniikit asetukset ja rekisterit. Tämä täytyy tehdä, jos halutaan käyttää yhden asennuksen levykuvaa useissa työasemissa. Levykuvasta otettu kopio asennettiin sitten kolmeen muuhun työasemaan. Levykuva luotiin ja asennettiin Cygaten sisäisen IT:n avustuksella. Työasemille asennettiin seuraavat sovellukset [20.]:

- Office 2010 Standard (Word, Excel, PowerPoint, Outlook)
- Checkpoint Smart Console versiot r75.20, r75.40, r76 ja r77 (Checkpoint palomuurien hallintatyökalu)
- Juniper Network and Security Manager versiot 2010.3 ja 2010.4 (Juniper Netscreen palomuurien keskitetty hallintatyökalu)
- VMWare ViewClient (VMWare virtuaalikoneiden client-ohjelma)
- Cisco CallManager Agent (Client-ohjelma Ciscon IP-puhelimille)
- FileZilla (FTP client-ohjelma tiedostojen siirtämiseen)
- Notepad++ (Monipuolisempi Notepad)
- Pidgin (Pikaviesti client-ohjelma)
- WireShark (Verkkoliikenteen seuranta ja analysointi ohjelma)
- Xmanager (Ohjelma valvontanäkymää varten)
- SecureCRT ja PuTTy (SSH-client ohjelmia etähallintaa varten)
- Citrix receiver (Sovellus IT-palveluiden jakamiseen)
- WinRar (Tiedostojen purkutyökalu)
- Thunderbird (Sähköpostiohjelma)

Työasemille oli tarkoitus myös asentaa NetOp Guest -niminen palvelinten ja työasemien etähallintatyökalu. Tähän ohjelmaan ei kuitenkaan löytynyt sarjanumeroa, joten ohjelmaa ei asennettu tässä yhteydessä. Ohjelman voi asentaa helposti jälkikäteen, jos sen käytölle tulee tarvetta.

Ennen työasemien käyttöönottoa koneet tuli liittää vielä Cygaten toimialueeseen. Toimialueeseen lisääminen tehtiin jokaisessa työasemassa Ohjauspaneelissa System-valikon alla System properties -välilehdellä, jossa lisättiin työasema toimialueeseen. Kuvassa 11 käytin esimerkkinä havainnollistamiseen omaa työasemaani.



Kuva 10. Työaseman liittäminen toimialueeseen.

4.4 Varaverkonhallintakeskuksen IP-puhelimet

Varaverkonhallintakeskuksessa otettiin käyttöön Ciscon IP-puhelimet. Puhelimissa on muun muassa viiden tuuman näytöt sekä tuki viidelle eri äänikoodekille mukaan lukien

G.722-laajakaistakoodekki. Kaiutin tukee kaksisuuntaista liikennettä akustisella kaiunpoistolla. IP-puhelin tukee myös liikenteen luokitusta ja priorisointia (eng. Quality of Services). Liikenteen luokittelulla tarkoitetaan sitä, että osa liikenteestä voidaan luokitella tärkeämmäksi kuin toinen. Liikenteen luokittelun avulla voidaan priorisoida erityyppistä liikennettä. Tämä on tärkeää erityisesti dataliikenteessä, joka sisältää puhetta. IP-puhelimille täytyi hankkia käyttäjälisenssit erikseen. IP-puhelimet määriteltiin käyttämään kiinteitä IP-osoitteita IP-puhelimille allokoidusta verkosta. IP-puhelimien asetukset määriteltiin Cygaten VoIP-tiimin (Voice over IP) avustuksella. Virtaa IP-puhelimet saavat suoraan Ethernet-liitännästä, johon ne on kytkettynä. Kytkimen portit täytyi määritellä tukemaan Power over Ethernet -toimintoa. Se tehtiin seuraavalla komennolla kytkimelle [21; 22.]:

```
set poe interface all
```

5 Verkonhallintakeskuksen tietoturva

Verkonhallintakeskuksen tietoturvassa täytyi ottaa huomioon useita eri tekijöitä. Eri asiakkailla on omia vaatimuksia tietoturvan suhteen. Varaverkonhallintakeskuksen tuli vastata näihin vaatimuksiin. Tässä luvussa käydään läpi, mitä asioita täytyi ottaa huomioon tietoturvan kannalta ja mitä määrityksiä kytkimelle laitettiin tietoturvan parantamiseksi.

5.1 Tietoturvan huomioonottaminen käyttöönotossa

Varaverkonhallintakeskuksen käyttöönotossa täytyi asiaankuuluvalle henkilöstölle hankkia tarvittavat kulkutunnisteet tiloihin pääsyä varten. Cygaten henkilöstöosasto toimitti nämä asiaankuuluvalle henkilöstölle. Tällä varmistettiin, että vain asiaankuuluvilla on pääsy varaverkonhallintakeskuksen tiloihin. Kiinteistössä oli jo valmiiksi kameravalvonta ja se kuuluu vartioinnin piiriin. Jos tiloihin yritetään esimerkiksi murtautua, siitä lähtee hälytys vartiointiyritykselle. Kaikki tuotannon verkot sijaitsevat palomuurin takana, jonne täytyi tehdä avauksia liikenteelle varaverkonhallintakeskukseen. Cygaten tuotantoverkosta vastaavat asiantuntijat tekivät nämä avaukset palomuurille.

5.2 Tietoturva kytkimessä ja työasemissa

Tietoturvan parantamiseksi kytkimissä on käytetty dot1x-pääsynhallintaa, josta käytetään myös nimitystä 802.1x. 802.1x on standardi, jolla määritellään porttikohtainen pääsynhallinta. Tällä estetään kytkimen porttien luvaton käyttö. Kun laite lisätään kytkinporttiin, tulee sen ensin tunnistautua. Tunnistautuminen tapahtuu esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmällä tai laitekohtaisella sertifikaatilla. Tunnistautuminen voi tapahtua keskitetysti palvelimella. Tässä kytkimessä tunnistautumiseen käytettiin olemassa olevaa RADIUS-pääsynhallintapalvelinta (Remote Authentication Dial In User Service). RADIUS on verkkoprotokolla, joka tarjoaa keskitettyä pääsynhallintaa verkon käyttäjille. [23; 24.]

Kun laite liitetään dot1.x-pääsynhallintaa käyttävään kytkinporttiin, vastaa kytkin tähän EAPOL-identiteettikyselyllä (Extensible Authentication Protocol Over LAN). EAPOL on verkkoporttien pääsynhallintaan käytettävä protokolla. Kytkettävä laite vastaa tähän kyselyyn EAPOL-vastauksella, joka voi olla esimerkiksi käyttäjätunnus. Kytkin ohjaa tämän vastauksen RADIUS-pääsynhallintapalvelimelle, joka varmistaa identiteetin lähettämällä takaisin haastekyselyn (eng. access challenge). Laite vastaa tähän kyselyyn esimerkiksi salasanalla tai varmenteella. Jos RADIUS-pääsynhallintapalvelin hyväksyy tunnistautumisen, pystyy laite kytkeytymään verkkoon. RADIUS-pääsynhallintapalvelimen hylätessä tunnistautumisyrityksen portti pysyy estettynä. RADIUS-pääsynhallintapalvelinta määriteltäessä täytyi asettaa muun muassa eri portteja, salasana ja IP-osoitteet. Tietoturvan parantamiseksi aikakatkaisun arvoksi asetettiin viisi sekuntia ja uudelleen yritysten määräksi kolme. Määritykset tehtiin seuraavilla komennoilla [24.];

```
set system radius-server <ip-address> port 1812

set system radius-server <ip-address> accounting-port 1813

set system radius-server <ip-address> secret <password>

set system radius-server <ip-address> timeout 5

set system radius-server <ip-address> retry 3

set system radius-server <ip-address> source-address <ip-
address>
```

```
set system radius-options attributes nas-ip-address <ip-address>
```

Määriteltäessä dot1x:ää kytkimelle täytyi ensin määritellä dot1x-ryhmä ja asetukset. Dot1x määriteltiin koskemaan kytkimen kaikkia portteja. Kytkimen portit määriteltiin käyttämään dot1x multiple supplicant -asetusta. Tällä tarkoitetaan, että yhteen porttiin voi tunnistautua useita päätelaitteita. Tämä asetus tehtiin sen takia, koska samaa kytkintä käyttää myös toimipisteen toimistotyöasemat. Porteille määriteltiin uudelleenyritysten määrä sekä aika, jonka portti odottaa, ennen kuin siihen voidaan yrittää kytkeä laitetta uudestaan. Tätä ajanjaksoa käytetään silloin, kun maksimi pyyntöjen määrä on ylittynyt. Porteille määriteltiin ajanjakso, kuinka kauan portti odottaa ennen kuin se lähettää ensimmäisen EAPOL-paketin uudestaan. [24; 25; 26.]

Portteihin määriteltiin myös aikajakso, jonka jälkeen porttiin yhdistetyn päätelaitteen täytyy tunnistautua uudelleen. Tämä asetus määriteltiin sen takia, että voidaan tarkastaa porttiin kytketyn laitteen varmenteen oikeellisuus. Tässä käytettiin oletusarvoa, joka on 3600 sekuntia. Lopuksi määriteltiin vielä uudelleenyritystenmäärä sekä ajanjakso jonka portti odottaa ennen kuin uudelleen tunnistautuminen on mahdollista. Edellä mainituilla asetuksilla pyrittiin siihen, että kytkin olisi mahdollisimman tietoturvallinen, eikä siihen pääse kytkeytymään vieraita laitteita. Kytkinporttien dot1x-asetukset määriteltiin seuraavilla komennoilla: [24; 27.]

```
set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> supplicant multiple

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> retries 2

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> quiet-period 5

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> transmit-period 5

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> reauthentication 3600

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> supplicant-timeout 60

set groups dot1x-authenticate protocols dot1x authenticator in-
terface <*> maximum-requests 5
```

Kytkimelle määriteltiin palomuuriasetukset, jotka saatiin kopioitua suoraan pääverkonvalvontakeskuksen kytkimeltä. Palomuurimäärityksissä määriteltiin erilaisia suodattimia protokollille ja palveluille, jotta haluttiin sallia tai estää kytkimellä. Palomuurimääritysten tarkoitus on kontrolloida kytkimelle tulevaa liikennettä ja estää mahdollisesti haitallinen liikenne.

Työasemissa tietoturva otettiin huomioon siten, että koneille kirjautuessa täytyy ensin purkaa levynsalaus. Salaus puretaan kirjoittamalla oikea salasana. Levynsalauksen purkuun tarvittava salasana on asiaankuuluvan henkilöstön tiedossa. Tämän jälkeen koneille pääsee kirjautumaan henkilökohtaisilla tunnuksilla. Työasemilla on myös viruksentorjuntaohjelmisto. Kaikkiin tärkeisiin järjestelmiin kirjaudutaan niihin vaadituilla tunnuksilla. Työasemilla on varmenteet, joilla ne pystyvät tunnistautumaan varaverkonhallintakeskuksen kytkimen portteihin.

6 Yhteyksien ja laitteiden testaus

Varaverkonhallintakeskuksen yhteyksiä testattiin viemällä työasemat ja IP-puhelimet paikan päälle. Yhteyksiä testattiin aluksi sillä, että pääseekö koneilla Internetiin. Yhdistäminen Internetiin onnistui sen jälkeen, kun palomuurille lisättiin tarvittavat reitit. Tämä tehtiin Cygaten verkkoasiantuntijoiden toimesta. Tämän jälkeen yhdelle koneelle asetettiin staattinen IP-osoite työasemille allokoidusta verkosta ja testattiin kirjautumista työasemalle omalla henkilökohtaisella tunnuksella. Kirjautuminen työasemalle onnistui ilman ongelmia. Jokaisella työasemalla lisättiin NOC-henkilöstölle järjestelmänvalvojanoikeudet, jotta työskentely olisi helpompaa.

Seuraavana testattiin IP-puhelimien toimivuus. Testaus tehtiin siten, että puhelimella soitettiin ensin ulospäin suuntautuva puhelu ja sitten sisäinen puhelu. Molemmat puhelut onnistuivat. Tämän jälkeen testattiin vielä puhelun vastaanottoa. Testaus suoritettiin soittamalla ulkoa päin tuleva puhelu siten, että puhelu ohjautui varaverkonhallintakeskuksen toiseen puhelimeen. Tätä varten kaikkien muiden puhelinten täytyi olla not ready -tilassa, kun puhelu tehtiin. Tällä varmistettiin, että puhelu tulee varmasti varaverkonhallintakeskuksen puhelimeen. Tämäkin testaus suoritettiin onnistuneesti.

Työasemien testauksessa täytyi testata eri ohjelmien toimivuutta. Suurin osa ohjelmista toimi testauksessa niin kuin piti. Muutamien ohjelmien kohdalla ilmeni pieniä ongelmia toimivuudessa. Ensimmäinen ongelma ilmeni Xmanager-valvontaohjelman kanssa. Ohjelman asennuskansiosta puuttui yksi sessio-tiedosto. Tiedoston lisäämisen jälkeen ohjelma alkoi toimia. Thunderbird-sähköpostiohjelman kanssa ilmeni myös ongelmia. Sovellus ei näyttänyt sähköpostikansioita ollenkaan profiilien latauksen jälkeen. Tämä ongelma saatiin korjattua päivittämällä Thunderbird uusimpaan versioon. Juniperin Network and Security Managerin kanssa ilmeni ongelmia version 2010.3 kanssa. Ohjelma ei avautunut normaalin asennuksen jälkeen. Ongelma saatiin korjattua asentamalla ohjelma järjestelmän valvojana.

Työn päätteeksi päivitettiin Cygaten IT-palveluiden jatkuvuuden hallinnan dokumentit ajantasaisiksi. Dokumentteihin päivitettiin uuden varaverkonhallintakeskuksen sijainti ja kuinka siirtyminen sinne tapahtuu. Nämä päivitykset tehtiin yhteistyössä Cygaten IT-palveluiden jatkuvuuden hallinnasta vastaavan kanssa.

7 Yhteenveto

Työn tarkoituksena oli luoda Cygate Oy:lle varaverkonhallintakeskus, jotta Cygate Oy pystyisi vastaamaan paremmin asiakkaidensa verkonhallinnan ja valvonnan tarpeisiin. Jotkut Cygaten asiakkaat vaativat varaverkonhallintakeskuksen olemassaoloa. Tämä työ tukee myös Cygaten liiketoiminnan tarpeita.

Projektin eteenpäin vieminen oli sulavaa, koska Cygaten asiantuntijoilta sai tarvittaessa hyvin tukea työn suorittamiseen ja ongelmatilanteiden ratkomiseen. Lähdemateriaalia oli hyvin saatavilla Cygaten puolesta sekä verkosta. Työn alussa haasteellisinta oli aiheen rajaaminen. Myös muutaman työasemien ohjelmistojen kanssa koetut ongelmat veivät hieman aikaa.

Työ täytti sille asetetut tavoitteet, vaikka aikataulu venyi hieman tavoitellusta. Cygate Oy:lle saatiin toimiva varaverkonhallintakeskus, joka on käyttövalmiina tarpeen tullen. Työn yhteydessä saatiin päivitettyä Cygaten ITSCM-prosessikuvaukset. Cygaten verkonvalvonta on nyt vikasietoisempi kuin se oli ennen työn valmistumista. Tämä tarkoittaa sitä, että verkon valvontaa ja hallintaa pystytään jatkamaan, vaikka nykyinen verkonhallintakeskus menisi käyttökelvottomaan kuntoon.

Lähteet

1 Yritys. 2013. Verkkodokumentti. Cygate Oy.< http://www.cygategroup.com/cy_templates/Page.aspx?id=304>. Luettu 31.10.2013.

2 Ellis Hollman, Karla Houser. 2011. ITSCM (IT Service Continuity Management) Overview:ITIL®'s IT Disaster Recovery and Business Continuity Management.

3 ITpreneurs Nederland B.V. 2010. ITILv3 Intermediate Planning, Protection,and Optimization.

4 European Union Agency for Network and Information Security. 2005. Verkkodokumentti. < https://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience/bc-rm-interfaces>. Luettu 3.12.2013.

5 Harjunen, Timo. 2014. Cygate IT Services Continuity Management Process. Cygate Oy.

6 Alisha Cecil. 2006. A Summary of Network Traffic Monitoring and Analysis Technique. Verkkodokumentti. < http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html>. Luettu 5.1.2014.

7 OSI Model. 2011. Verkkodokumentti. Jz. Arisar. Data Communiation Networking. < http://datacombasic.blogspot.fi/2011/03/v-behaviorurldefaultvmlo.html>. Luettu 10.1.2014.

8 MIB (SNMP) FAQ. 2011. Verkkodokumentti. DPS. < http://www.dpstele.com/dpsnews/techinfo/mib_snmp.php>. Luettu 10.1.2014

9 NetFlow. 2014. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Netflow>. Luettu 15.1.2014.

10 Eskelinen, Aleksi. 2014. Cygaten tuotannon verkot. Cygate Oy.

11 Multi-Protocol Label Switching (MPLS). 2012. Verkkodokumentti. RadCom. < http://www.protocols.com/papers/mpls.htm>. Luettu 20.1.2014.

12 OSPF. 2014. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Open_Shortest_Path_First>. Luettu 20.1.2014.

13 Eskelinen, Aleksi. 2014. Kytkinten peruskonfiguraatiot. Cygate Oy.

14 Configuring VLANs and Trunking on the EX-series Switch. 2012. Verkkodokumentti. Juniper. < http://kb.juniper.net/InfoCenter/index?page=content&id=KB11013>. Luettu 7.11.2014.

15 Configuring Aggregated Ethernet LACP. 2014. Verkkodokumentti. Juniper. < http://www.juniper.net/techpubs/en_US/junos13.3/topics/usage-guidelines/interfaces-configuring-aggregated-ethernet-lacp.html>. Luettu 7.11.2013.

16 SRX Getting Started – Configure admin user. 2012. Verkkodokumentti. Juniper. < http://kb.juniper.net/InfoCenter/index?page=content&id=KB16657>. Luettu 10.10.2013.

17 How to configure routed VLAN interfaces (RVI) for inter VLAN routing on an EX switch. 2012. Verkkodokumentti. Juniper. < http://kb.juniper.net/InfoCenter/index?page=content&id=KB11000>. Luettu 2.12.2013.

18 Eskelinen, Aleksi. 2014. VRF- ja OSPF-konfiguraatiot. Cygate Oy.

19 Lenovo ThinkPad T430. 2014. Misco UK Limited. Verkkodokumentti.< http://www.misco.co.uk/Product/200061/Lenovo-ThinkPad-T430-Intel-Core-i5-3320M-14-0inch-4GB-500GB-Windows-7-Pro-Laptop-Notebook-PC>. Luettu 4.2.2014.

20 Tuure, Aaro. 2014. Profiilien luonti ja hallinta AD-ympäristössä. Opinnäytetyö.

21 Cisco Unified IP Phone 7942G. 2014. Verkkodokumentti. Cisco. < http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7942g/product_data_sheet0900aecd8069bb68.html>. Luettu 19.2.2014.

22 Wideband Audio and IP Telephony. 2014. Verkkodokumentti. Cisco. < http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7965g/prod_white_paper0900aecd806fa57a.html>. Luettu 19.2.2014.

23 RADIUS. 2014. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/RADIUS>. Luettu 26.2.2014.

24 Chapter 14. 802.1x Port Access Control. 2007. Verkkodokumentti. Foundry Networks. < http://www.foundrynet.com/services/documentation/EIUserProj/b14_8021x%20Port%20Security.html#999919>. Luettu 26.2.2014.

25 Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch. 2012. Verkkodokumentti. Juniper. < http://www.juniper.net/techpubs/en_US/junos12.2/topics/example/802-1x-pnac-single-supplicant-multiple-supplicant-configuring.html>. Luettu 4.3.2014.

26 transmit-period. 2010. Verkkodokumentti. Juniper. < http://www.juniper.net/techpubs/en_US/junos10.4/topics/reference/configuration-statement/transmit-period-edit-protocols-dot1x.html>. Luettu 4.3.2014.

27 supplicant-timeout. 2011. Verkkodokumentti. Juniper. < http://www.juniper.net/techpubs/en_US/junos11.4/topics/reference/configuration-statement/supplicant-timeout-802-1x.html>. Luettu 5.3.2014.