LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Yrityksen verkonvalvonnan hälytysten kehittäminen

Raunio, Ville

2017 Laurea

Laurea-ammattikorkeakoulu

Yrityksen verkonvalvonnan hälytysten kehittäminen

Raunio Ville
Tietojenkäsittely koulutus
Opinnäytetyö
Helmikuu, 2017

Laurea-ammattikorkeakoulu
Koulutus
Tietojenkäsittely

Tiivistelmä

Ville Raunio

Yrityksen verkonvalvonnan hälytysten kehittäminen

Vuosi 2017 Sivumäärä 43

Opinnäytetyö toteutettiin toimeksiantona Helsingin kaupungin liikennelaitoksen Metron Infra- ja kalustoyksikölle. Opinnäytetyön tarkoituksena oli kehittää ja tutkia Metro-lan verkon verkonvalvonnan hälytyksiä. Tehtävinä oli muun muassa saada verkonvalvonta lähettämään hälytyksestä tieto sähköpostitse reealiajassa kohdennetuille käyttäjille ja selvittää mistä laitteista halutaan saada hälytystieto. Lisäksi tavoitteena oli luoda käyttöopas, jolla työntekijät pystyvät luomaan hälytyksiä.

Teoreettisessa osuudessa käsiteltiin yleisiä asioita verkonhallinnasta ja verkonvalvonnasta, joka on vain yksi osa verkonhallintaa. Lisäksi osiossa käytiin läpi aiheeseen liittyviä protokollia ja tutustuttiin lyhyesti verkonvalvontaohjelmistoihin.

Opinnäytetyössä käytettiin empiiristä tutkimusmenetelmää. Aineisto kerättiin tutkimalla yrityksen verkonvalvontaohjelmistoa, josta sai kerättyä tarvittavan tutkimusaineiston. Verkonvalvontaohjelmistolle pystyttiin suorittamaan erilaisia simuloituja tapauksia ja saatujen tuloksien avulla pystytiin saavuttamaan tavoitteet.

Opinnäytetyön tavoitteet saavutettiin. Tutkimustulosten perusteella yritykselle ehdotettiin muutoksia verkkoprosesseihin. Ehdotetut muutokset otettiin käyttöön yrityksessä. Empiirisen tutkimuksen avulla saatiin kerättyä lisää tietoa verkonvalvontaohjelmistosta, jota voidaan hyödyntää jatkossa verkonvalvontaa kehitettäessä. Käyttöopasta voidaan hyödyntää jatkossa, jos yrityksen työntekijä haluaa luoda omia hälytyksiä verkonvalvontaan.

Asiasanat: verkonvalvonta, protokolla, ohjelmistot, hallinta

Laurea University of Applied Sciences
Degree Programme in Business Information Technology
Bachelor's Thesis

Abstract

Ville Raunio

Improving company's Network Monitoring alerts

Year 2017 Pages 43

This Bachelor's thesis was commissioned by Helsinki City Transport's Infra and Rolling Stock. The aim of this thesis was to improve the company's network monitoring alerts. These tasks included getting the network monitoring software to send event information by e-mail to targeted users and also investigate which devices will be selected to send event information through e-mail. In addition, the aim was also to create a user manual for employees to create their own alerts with the network monitoring software.

The theoretical part discusses some general aspects in network management and networking monitoring, which is only one part of network management. In addition this section also describes related protocols to network management as well as briefly explores network monitoring software.

Empirical research method was used in this thesis. The data was collected by investigating the company's network monitoring software, which provided all needed research information. Network monitoring software allowed to simulate different kind events and with the results obtained from events, it was possible to achieve the aims of the thesis.

The thesis aims were achieved and the changes made are in use in the company. With the use of empirical research method new information about the network monitoring software was also collected, which can be used in the future for developing the company's network monitoring. The user guide can be utilized in the future, if an employees want to create their own alerts into network monitoring.

Keywords: network monitoring, protocol, software, management

Sisällys

1 Johdanto 6
2 Työn tarkoitus ja tavoite 6
2.1 Keskeiset käsitteet 7
2.2 Yrityksen esittely 8
2.3 Tutkimusmenetelmä 9
3 Verkonvalvonta 10
3.1 Verkonvalvonta kokonaisuus 10
3.1.1 Vikojen valvonta 11
3.1.2 Käytön hallinta 11
3.1.3 Kokoonpanon hallinta 12
3.1.4 Suorituskyvyn hallinta 12
3.1.5 Turvallisuuden hallinta 13
3.2 Verkonhallinnan protokollia 13
3.2.1 SNMP 13
3.2.2 SNMPv2 15
3.2.3 SNMPv3 16
3.2.4 TCP/IP, UDP ja OID 18
3.2.5 SMI ja SMIv2 19
3.2.6 MIB ja ICMP 20
3.2.7 OSI-malli 21
3.2.8 RMON, Syslog ja CIM 23
3.2.9 WMI ja WBEM 25
4 Verkonvalvontaohjelmistot 25
4.1 Vapaan lähdekoodin valvontaohjelmistot 26
4.1.1 Nagios 26
4.1.2 Nino 26
4.2 Solarwinds Orion NPM 27
4.2.1 Kyselyjärjestelmä 28
4.2.2 Hälytysjärjestelmä 29
4.2.3 Raportointijärjestelmä 29
5 Tutkimuksen toteutus 30
6 Yhteenveto ja johtopäätökset 33
Lähteet 35
Kuviot.. 36
Liitteet 37

1 Johdanto

Tämän opinnäytetyön tavoitteena on saada yrityksen verkonvalvontaa kehitettyä, koska laiteympäristö on kasvava ja nykytilanne, jossa esimerkiksi tärkeistä laitteista ei saada tietoa halutulla tavalla, on kankea. Kehitys suoritetaan Solarwinds Orion NPM ohjelmiston avulla, joka on yrityksen tällä hetkellä käyttämä verkonvalvontaohjelmisto. Ohjelmisto sisältää kaikki vaadittavat toiminnot, jotta tarvittavat kehitystoimenpiteet saadaan suoritettua. Tässä opinnäytetyössä käsiteltävät kehittämistoimenpiteet tehdään HKL:n metrovarikolla, jossa on ohjelmiston ylläpitopalvelin.

Verkonvalvonta on aiheena mielenkiintoinen, koska ympäristönä se on haastava ja valvonnansuunnittelu vaatii paljon pohdintaa. Yrityksen laiteympäristö lisää myös haasteita runsaan laitemäärän ja laitteiden sijaintien vuoksi. Laitteet ovat sijoiteltu laajasti erilaisiin olosuhteisiin, kuten metrovaunut, rata-alue, metroasemat ja tunnelit. Tämänkaltaiset olosuhteet vaikuttavat suuresti siihen, miten verkonvalvontaa tulisi suorittaa.

Metrovaunuissa olevat tukiasemat käynnistyvät ja sammuvat metrovaunun käynnistymisen ja sammumisen mukaan. Tämä aiheuttaa esimerkiksi turhan hälytyksen verkonvalvonnassa, koska on luonnollista, että laitteet sammuvat metrovaunun sammuessa. Tällainen tilanne tapahtuu esimerkiksi, kun metrovaunu on huollossa, jossa käynnistämistä ja sammuttamista tapahtuu jatkuvasti metrovaunulle. Rata-alueella olevat tukiasemat ovat jatkuvasti erilaisten sääolosuhteiden armoilla, minkä vuoksi tukiasemat aiheuttavat viikoittain hälytyksiä. Metroasemalla oleviin tukiasemiin kohdistuu ajoittain ilkivaltaa. Tämä voi myös aiheuttaa hälytyksen laitteen mennessä rikki. Tunneliolosuhteissa olevat laitteistot menevät yleensä ajan kanssa rikki ja se aiheuttaa aina hälytyksen. Verkonvalvonnassa on laajasti myös erilaisia toimintoja, kuten hälytykset. Tässä opinnäytetyössä rajataan tutkimuskohteeksi vain hälytysten kehittäminen ja suunnittelu.

2 Työn tarkoitus ja tavoite

Työn tarkoitus oli kehittää verkonvalvonnassa olevien laitteiden hälytyksiä. Verkonvalvonnassa on lukuisia eri tietoliikennelaitteita, jotka vaativat verkonvalvontaa, kuten palvelimia, kytkimiä ja tukiasemia. Opinnäytetyössä keskitytään kehittämään ja suunnitelmaan näiden laitteiden hälytyksiä. Hälytykset luodaan tai muokataan Solarwinds Orion NPM ohjelmistolla, jossa on tarvittavat toiminnallisuudet valmiina.

Toimeksiantajan kanssa on yhdessä valittu kriittisimmät tietoliikennelaitteet, jotka ovat Metro-lan verkossa. Valituista laitteista oli tarkoitus saada reealiajassa tieto sähköpostitse niiden häiriöistä ja vikaantumisista.

Opinnäytetyön tavoitteena on parantaa verkonvalvonnan aiheuttamia hälytyksiä. Hälytyksistä olisi tarkoitus tulla tieto verkon ylläpitäjille reaaliajassa ja siten, että hälytyksen aiheuttanut laite itse vaatii toimenpiteitä. Verkonvalvonta aiheuttaa tällä hetkellä lukuisia hälytyksiä, jotka eivät vaadi reagointia. Tällaiset hälytykset tulisi saada minimoitua. Hälytykset rakennetaan ja suunnitellaan siten, että turhia ja tarpeettomia hälytyksiä ei tulisi valittujen laitteiden kohdalta. Päätavoitteena on saada hälytykset sähköpostitse kohdennetuille käyttäjille.

Tutkimuskysymyksiä opinnäytetyössä ovat, miten laitteet määritetään lähettämään reealiaikainen hälytystieto sähköpostitse kohdennetuille käyttäjille sekä mitkä laitteet määritetään lähettämään hälytystieto ja miten hälytys luodaan ja miten se tulisi suunnitella. Järjestelmien ja verkon ylläpitäjien työtä saadaan helpotettua selvittämällä vastaukset näihin kysymyksiin. Verkon luotettavutta ja toimintavarmuutta pystytään parantamaan, kun toimintahäiriöt havaitaan nopeammin ja niihin voidaan reagoida hallitusti.

Tämä opinnäytetyö rajataan koskemaan verkonvalvonnan hälytyksiä. Verkonvalvonta on yleisesti ottaen, jokaisella yrityksellä tai muulla, joka sitä toteuttaa, määritetty täysin sen omien vaatimusten mukaisesti. Tämän vuoksi aineistoa ei käytännössä pysty saamaan kuin yrityksen omista lähteistä. Aineistoa kerätään tutkimalla muun muassa, miten verkonvalvontaohjelmisto toimii, mitä ohjelmistolla voi tehdä ja mikä on verkonvalvonnan nykyinen tilanne.

2.1 Keskeiset käsitteet

CIM, Common Information Model, avoin standardi, joka määrittelee miten hallitut elementit IT-ympäristöissä esitetään tunnettuina objekteina ja niiden väliset suhteet.

ICMP, Internet Control Message Protocol, protokolla, jolla IP-yhteyksissä olevat laitteet välittävät viestejä.

ITU-T, International Telegraph Union, jonka lopussa oleva T tarkoittaa televiestintäsektoria. ITU on järjestö, joka koordinoi televiestintäverkkoja ja palveluita kansainvälisesti. ITU toimii YK:n alaisena.

MIB, Management information base, tietokanta, jota käytetään entiteettien hallintaan viestintäverkossa.

OID, Object identifier, yksilöintitunnus, jolla yksilöidään kohde annetun standardin mukaisesti yksilöintijärjestelmässä.

OSI-Malli, Open Systems Interconnection Reference model, malli, joka kuvaa tiedonsiirtoprotokollien yhdistelmää.

RMON, Remote Network Monitoring, ohjelmisto tai laite, joka kerää tietoa ja analysoi verkon liikennettä.

SMI, Structure of Management Information, Tietorakenne, jota käytetään MIB-taulukossa hierarkia rakenteeseen ja objektien määrittelemiseen.

SNMP, Simple Network Management protocol, yleisin käytetty TCP/IP-verkkojen verkonvalvonta protokolla.

TCP/IP, Transmission Control Protocol / Internet Protocol, yhdistelmä useasta Internet-liikenteessä olevasta tietoverkkoprotokollasta.

UDP, User Datagram Protocol, tiedonsiirtoprotokolla, joka ei vaadi yhteyttä laitteiden välillä tiedonsiirrossa

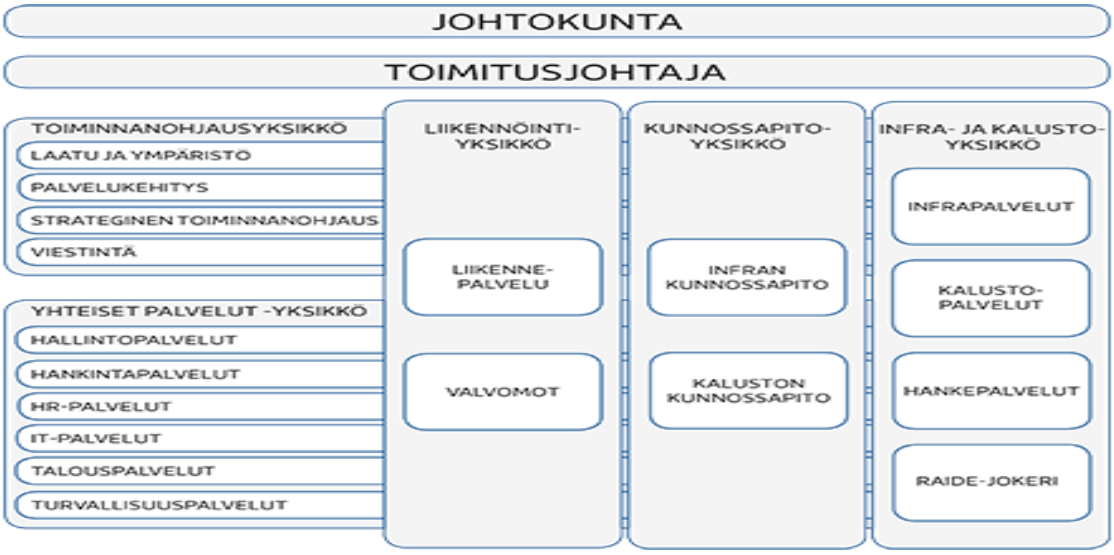
WBEM, Web-Based Enterprise Management, joukko hallinta ja internet standardi teknologioita, jotka on kehitetty yhteistämään hajautettuja tietojenkäsittely alustoja.

WMI, Windows Management Instrumentation, Windows ympäristöissä oleva infrastruktuuri, jolla mahdollistetaan hallintatietojen lähetys laitteiden välillä.

2.2 Yrityksen esittely

Helsingin kaupungin liikennelaitos (HKL) tarjoaa joukkoliikennevälineitä Helsingissä. Joukkoliikennevälineitä ovat metro, raitiovaunu ja Suomenlinnan lautta. HKL vastaa myös Helsingin alueen kaupunkipyöräpalvelusta. (Tämä on HKL 2017.)

Organisaation liikeidea on tuottaa laadukasta ja turvallista joukkoliikennettä vastuullisesti kansalaisille. Organisaatio koostuu eri yksiköistä, jotka yhdessä toteuttavat palvelut. Toimiala on joukkoliikenne. Liikennepalvelut ovat kattavat ja tulevaisuudessa tulevat kasvamaan laajasti muun muassa länsimetrolla ja raidejokerilla. Kuviossa 1 on esitetty yrityksen organisaatio. (Tämä on HKL 2017.)



Kuvio 1: HKL Organisaatiokaavio (HKL 2017)

HKL:n toiminta on jaettu eri yksiköihin, jotka ovat liikennöintiyksikkö, kunnossapitoyksikkö, Infra- ja kalustoyksikkö, toiminnanohjausyksikkö, yhteiset palvelut ja Suomenlinnan Liikenne Oy, joka on HKL:n tytäryhtiö.

Liikennöintiyksikkö vastaa metro- ja raitioliikenteestä sekä niiden liikenteenohjauksesta ja valvomotoiminnasta. Yksikön tarkoitus on tuottaa laadukasta ja turvallista liikennöintiä. Helsingin seudun liikenne (HSL) tilaa HKL:ltä liikennöintiä. Kunnossapitoyksikkö huolehtii metrojen, raitiovaunujen, ratojen, pysäkkien, asemien ja kiinteistöjen huollosta ja kunnossapidosta. Infra- ja kalustoyksikkö vastaa HKL:n infra- ja kalusto-omaisuuden investointien ja elinkaaren hyvästä hallinnasta. Toiminnanohjausyksikkö tarkastelee HKL:n toimintaa kokonaisnäkökulmasta ja varmistaa HKL:n pitemmän aikavälin tavoitteiden saavuttamisen sekä vastaa HKL:n viestinnästä. Yhteiset palvelut yksikkö palvelee koko Helsingin kaupungin liikelaitosta. Yksikkö tuottaa palveluja, jotka koskevat hallintoa, taloutta, hankintoja, henkilöstöä, turvallisuutta ja informaatioteknologiaa. Suomenlinnan Liikenne Oy huolehtii lauttaliikenteestä Helsingin ja Suomenlinnan merellisen kaupunginosan välillä. (Tämä on HKL 2017.)

Suomenlinnan lautat ovat osa Helsingin kaupunkiliikennettä, ja ne liikennöivät läpi vuoden. Vuonna 2015 HKL:n liikevaihto oli 153,9 miljoonaa euroa ja henkilöstöä oli 1084. Luvut ovat kasvaneet nykyhetkellä, koska palvelut ovat kasvaneet ja tulevat kasvamaan myös jatkossa uusien hankintojen toteuttamisen ylläpitämisen vuoksi. (Tämä on HKL 2017.)

2.3 Tutkimusmenetelmä

Opinnäytetyössä käytettiin tutkimusmenetelmänä empiiristä tutkimusta, jossa tutkimustulokset saadaan konkreettisilla havainnoilla tutkimuskohteesta. Empiiriseen tutkimukseen kuuluu myös analysoida ja mitata tutkimuskohdetta.

Empiiristä tutkimusmenetelmää käytetään opinnäytetyön aiheeseen liittyvään verkonvalvontaohjelmistoon, joka on tutkimuskohteena. Tutkimuskohteesta kerätään materiaalia tekemällä havaintoja siitä miten se toimii eri tilanteissa ja mitä sillä voidaan tehdä. Materiaali kerätään tutkimalla ohjelmiston toimintoja ja suorittamalla erilaisia testejä ohjelmiston omilla välineillä. (Empiirinen tutkimus 2015.)

3 Verkonvalvonta

Verkonvalvonnalla tarkoitetaan valvontaa, jossa esimerkiksi ohjelmisto jatkuvasti seuraa valvonnassa olevien laitteiden tilaa. Jos ohjelmisto havaitsee laitteissa vikoja tai hidastumista, ohjelmisto antaa tästä ylläpidolle määrätyllä tavalla tiedon. Verkonvalvonta on yksi osa verkonhallintaa. (Schimidt & Mauro, 2008, 19-20).

Verkonvalvonta toteutuu valvontaohjelmistosta, laitteesta, jota valvotaan ja protokollasta, jonka tehtävä on hoitaa kysely ohjelmiston ja laitteen välillä. Verkonvalvonnan tarkoitus on mahdollisissa vikatilanteissa antaa ylläpidolle tieto tästä, jotta viat saadaan korjattua mahdollisimman nopeasti ja ylläpidettyä verkon laitteet ja itse verkko toimintakunnossa luotettavasti. (Schimidt & Mauro, 2008, 19-20).

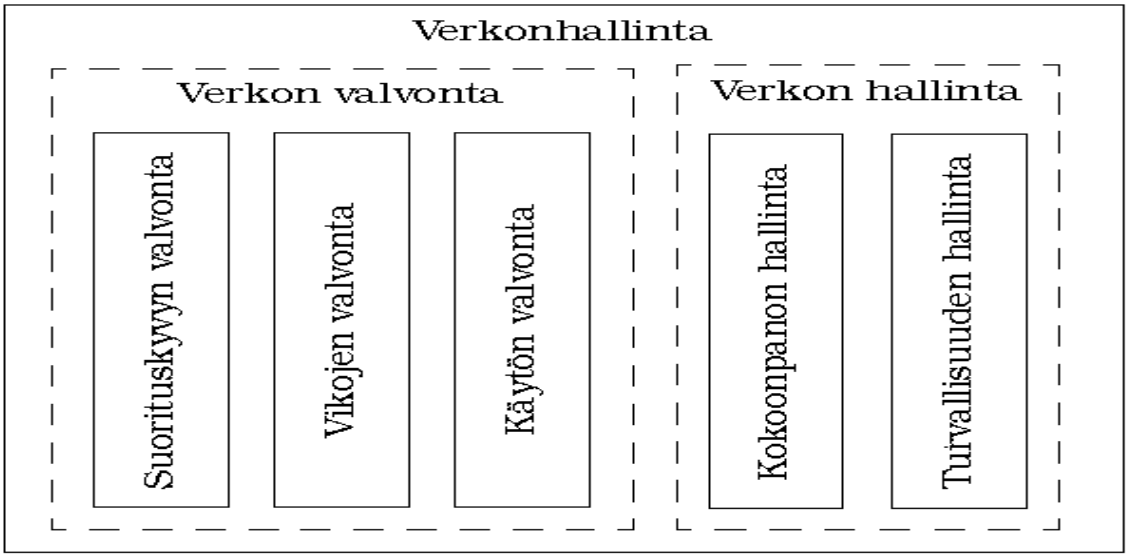
Jokaisessa tietoverkossa, joka tarjoaa palveluita, tulisi olla aina ajan tasalla oleva verkonvalvonta, jotta verkko toimii jatkuvasti ja luotettavasti. Jos verkonvalvontaa ei tällaisissa yrityksissä pidetä tärkeänä tai sitä ei toteuta ollenkaan, voi se aiheuttaa yritykselle kuluja, joita ei tulisi, jos verkonvalvonta olisi toteutettu kunnolla. (Schimidt & Mauro, 2008, 19-20).

Verkonvalvonnan havaitessa poikkeaman verkossa, on sen tarkoitus antaa tästä tieto ylläpidolle. Poikkeaman tiedotus ylläpidolle voi tapahtua erilaisilla tavoilla, kuten esimerkiksi sähköpostilla tai tekstiviestillä. Tiedon välityttyä ylläpidolle on ylläpidon tehtävä ratkaista ongelma, jotta laite saadaan takaisin normaaliin toimintakuntoon. Toimenpiteitä voi olla esimerkiksi laitteen vaihto kokonaan tai paikalla suoritettava uudelleen käynnistys laitteelle. Toimenpiteiden jälkeen tulisi aina tarkistaa verkonvalvonnasta, että tehty toimenpide on saanut laitteen takaisin toimivaan tilaan. (Schimidt & Mauro, 2008, 19-20).

3.1 Verkonvalvonta kokonaisuus

Verkonvalvonta vaatii paljon erilaisia palveluita ja protokollia, joiden avulla ylläpitäjät voivat pitää verkon toimintakunnossa. Palvelut ja protokollat mahdollistavat ylläpidolle toiminnot, joilla voidaan etsiä virheitä ja kontrolloida verkkoa. Verkonvalvonta on yksi osa verkonhallintaa, joka on iso kokonaisuus. ITU-T on luonut ja jakanut suosituksen verkonhallinnalle, jossa

verkonhallinnan vaatimukset on jaettu viiteen eri kategoriaan. Kategoriat ovat vikojen hallinta, käytön hallinta, kokoonpanon hallinta, suorituskyvyn hallinta ja turvallisuuden hallinta. (Haikonen 2000.) Kuviossa 2 on esitetty miten verkonhallinta voidaan jakaa.



Kuvio 2: Verkonhallinta jaettuna valvontaan ja hallintaan. (Hautaniemi 1994)

3.1.1 Vikojen valvonta

Vikojen hallinnan avulla ylläpidon täytyy pystyä nopeasti paikallistamaan verkossa olevien vikojen sijainti, havaitsemaan, mitä seuraamuksia viasta on verkolle ja sen palveluille, eristämään toimintakykyinen osa verkosta vian aiheuttamilta häiriöiltä, muuttamaan verkko siten, että minimoidaan vaikutukset verkon toimintaan ilman viallista komponenttia sekä korjaamaan tai vaihtamaan vialliset komponentit. (Haikonen 2000.)

Näitä toimenpiteitä ylläpito voi suorittaa verkolle, jotta voidaan palauttaa verkko alkuperäiseen tilaansa. Ylläpito tarvitsee myös varmistuksen siitä, että verkko on palautunut normaaliksi verkkoa häirinneen ongelman ratkettua. (Haikonen 2000.)

3.1.2 Käytön hallinta

Verkon resurssien seuraaminen käyttäjä- tai käyttäjäryhmätasolla on erittäin tärkeää tietoa verkkoa valvovalle ylläpidolle. Tiedon avulla varmistetaan, että verkko toimii tehokkaasti ja sen avulla verkkoa voi myös suunnitella ja parantaa. Ylläpidon on määritettävä, mitä tietoa kerätään, miten tietoa kerätään ja kuinka usein tieto kootaan yhteen. Kootut tiedot on pystyttävä myös analysoimaan. (Haikonen 2000.)

Etu, joka käytönhallinnasta saadaan on pääasiassa se, että verkon resurssien todellista käyttöä voidaan seurata. Saatu informaatio pystytään tulevaisuudessa kohdistamaan oikeisiin paikkoihin investointien muodossa. Verkon laajentamisessa on tärkeää tietää, mitä yhteyksiä ja palveluita todellisuudessa käytetään ja tarvitaan. (Haikonen 2000.)

3.1.3 Kokoonpanon hallinta

Kokoonpanon hallinnan tehtävänä on alustaa verkko, tarvittaessa käynnistää ja sammuttaa verkko tai sen osa hallitusti sekä verkon tai sen osien uudelleenkonfigurointi, joka on erittäin tärkeä viasta toipumisen yhteydessä. Kokoonpanon hallinnan tehtävänä on myös pitää yllä verkon osien konfigurointitietoja ja seurata muutoksia niissä. (Haikonen 2000.)

Ensisijaisena etuna kokoonpanon hallinnassa on mahdollisuus muuttaa verkon loogista rakennetta. Ongelmatilanteissa esimerkiksi on usein tarpeellista muuttaa reitityksiä siten, ettei viallinen laite aiheuta häiriötä verkon toimiviin osiin. Erityisesti laajoissa verkoissa on tarpeellista tietää, mitä laitteita niihin on kytketty ja mitkä ohjelmistoversiot kyseisissä laitteissa on. (Haikonen 2000.)

3.1.4 Suorituskyvyn hallinta

Suorituskyvyn hallinnalla verkon ylläpitäjä voi kerätä ja analysoida verkon suorituskykyä. Saatujen analyysien pohjalta voidaan arvioida esimerkiksi onko järjestelmän välityskyky vaaditulla tasolla tai ovatko vasteajat palveluissa asetettujen vaatimusten mukaisia tai esiintyykö verkon eri kohdissa poikkeuksia esimerkiksi suuria viiveitä. Suorituskyvyn hallinnalla täytyy olla myös toiminnallisuus, jolla voidaan hienosäätää verkon suorituskykyä. (Haikonen 2000.)

Ylläpidolle on erittäin tärkeää saada tilastoja suorituskyvystä, jotta on mahdollista suunnitella, hallita ja ylläpitää laajoja verkkoja. Tilastojen avulla voidaan havaita, jos verkossa on mahdollisia kohtia, jotka aiheuttavat jatkuvasti ongelmia. Mahdollisia ongelmia havaitessa voidaan suorittaa ennaltaehkäiseviä toimenpiteitä, ennen kuin loppukäyttäjälle aiheutuu ongelmasta haittaa. Toimenpiteitä mitä voidaan suorittaa ovat esimerkiksi reititystietojen muutos, liikenteen hajautus ruuhka-aikoina tai voimakkaasti kasvava liikenne jollain verkon alueella. (Haikonen 2000.)

Suorituskyvyn hallinnan edut ovat hyvin pitkälti samoja kuin käytön hallinnassa. Suorituskyvyn hallinnassa keskitytään enemmän itse verkon ja laitteiden suorituskykyyn kuin palveluiden käytön seurantaan. Suorituskyvyn hallinnalla pystytään keräämään informaatiota, jolla nähdään eri laitteiden käyttöasteet. Käytön hallinalla voidaan päättää, onko palvelujen kannalta tarpeen ryhtyä äärirajoilla toimivien resurssien laajentamiseen. (Haikonen 2000.)

3.1.5 Turvallisuuden hallinta

Turvallisuuden hallinta on verkkoon ja siihen liitettyihin laitteisiin pääsyn seurantaa ja kontrollointia, sekä pääsyä siihen tietoon, jota on kerätty verkon laitteista osana verkonhallintaa. Lokeihin kerääntyy tietoa, jotka ovat tärkeä osa turvallisuuden hallintaa. Tämän vuoksi turvallisuuden hallinta on suurimmalta osaltaan lokien keräystä, tallennusta ja analysointia.

Turvallisuuden hallinta osana verkkona ei siis tarkoita tietokonejärjestelmien sisäistä käyttäjien ja käyttäjäryhmien oikeuksien määrittely. Turvallisuuden hallinta keskittyy siihen kenellä, ja mistä on oikeus päästä käsiksi eri laitteiseen ja niistä saataviin palveluihin. (Haikonen 2000.)

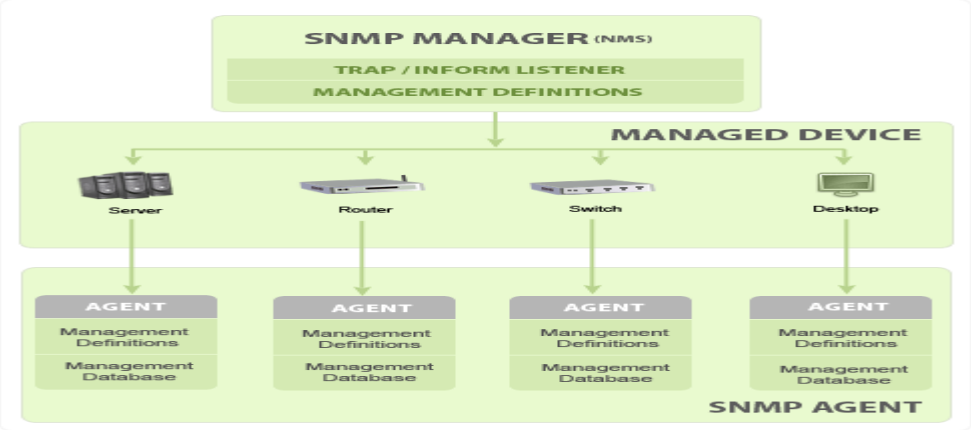
3.2 Verkonhallinnan protokollia

Verkonhallinnan protokollat tulevat aina jossain vaiheessa mukaan käyttöön, kun halutaan hallita, seurata ja analysoida eri laitteiden viestintää. Näitä tilanteita varten on kehitetty sarja protokollia, jotka mahdollistavat käyttäjät ymmärtämään laitteidensa viestinnän. Näistä yleisimmin tunnetut protokollat ovat Transmission Control Protocol (TCP) ja User Datagram Protocol (UDP).

Nämä ajan kanssa kehitetyt ja erikoistuneet protokollat ovat pohjimmiltaan aina tarpeen verkkojen luonteen vuoksi. Käyttäjä ei yksinkertaisesti pysty näkemään tavujen ja bittien liikkumista johdoissa. Tämän takia ainoa tapa ymmärtää verkon käyttäymistä on luottaa raportteihin, joita nämä protokollat tuottavat käsittelemästään datasta.

3.2.1 SNMP

SNMP (Simple Network Management Protocol) on yleisin käytetty verkonhallintaprotokolla. SNMP on suunniteltu yksinkertaiseksi ja helposti toteutettavaksi verkonhallintatyökaluksi TCP/IP verkkojen hallintaan. SNMP:tä käytetään informaation keräämiseen esimerkiksi laitteesta ja verkossa olevien tietoliikennelaitteiden konfigurointiin (esimerkiksi palvelimet, tulostimet, hubit, kytkimet ja reitittimet). Terminä SNMP viittaa joukkoon verkonhallintastandardeja, jotka kuvaavat itse protokollan (SNMP, Simple Network Management Protocol), hallintatietokantojen määrittelyn (MIB, Management Information Base) sekä joukon tieto-olioita (SMI, Structure of Management Information). (Zoho Corp 2017.) SNMP:n kommunikaatio havainnoitu kuviossa 3.



Kuvio 3: Havainne kuva SNMP:n kommunikaatiosta (Zoho Corp 2017)

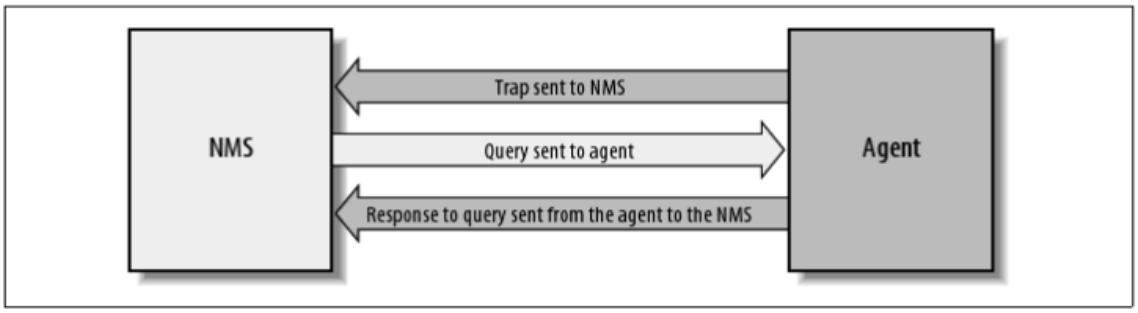
SNMP protokolla tuottaa erilaisia viestejä jotka ovat muuan muassa get, getnext, getbulk, set, getresponse, trap, notification, inform ja report. Get-viestillä SNMP-palvelin lähettää pyynnön laitteelle, jonka jälkeen laite vastaa pyyntöön. Pyyntöä kutsutaan get-requestiksi ja vastausta get-responseksi. Getnext on lähes sama kuin get, mutta getnext:ssä palautuva vastaus on seuraavan oidin arvo MIB-puussa. Set:llä käsketään laittelle uusi arvo tai muokkaamaan nykyistä arvoa. Käskeminen tapahtuu SNMP-palvelimella. Trap lähettää SNMP-tä hallitsevalle palvelimelle tietoja verkosta esimerkiksi, jos verkossa tapahtuu ongelmia. (Zoho Corp 2017.)

Kun TCP/IP:tä kehitettiin, ei ollut otettu vielä huomioon minkäänlaista verkonhallintaa. SNMP kehitettiin vuonna 1988, jotta on mahdollista seurata verkossa olevia laitteita. SNMP hyväksyttiin Internet standardiksi vuonna 1990 Internet Architecture Board (IAB) puolesta ja tämän jälkeen se on ollut erittäin laajassa käytössä. Tällä hetkellä verkkolaitteita tarjoavat yritykset ovat asettaneet laitteisiinsa SNMP tuen. (Schimidt & Mauro, 2008, 19).

SNMP toiminta perustuu malliin, jossa on palvelin ja asiakas. Mallissa palvelinta kutsutaan agentiksi ja asiakasta manageriksi. Manageri kommunikoi verkossa olevien SNMP-agenttien kanssa. Tyypillisesti manageri on tietokone, joka suorittaa verkonvalvontajärjestelmää. Managerin toimintoja ovat muun muassa kyselyt agenteilta, vastaanottaa vastaukset agenteilta, asettaa muuttujia agentteihin ja tiedostaa poikkeavat tapahtumat agenteilta.

Managerit tunnetaan myös nimellä NMS (Network Management Station). NMS suorittaa kyselyitä agenteille. Kyselyssä NMS kysyy agentin hallitsemalta laitteelta sen tietoja. Agentti lähettää takaisin managerille queryn, joka on kyselyn vastaus tai hälytys (trap). SNMP manageri tulee asentaa tehokkaalle alustalle, koska se vaatii paljon laskentatehoa prosessorilta ja levytilaa. (Zoho Corp 2017.)

Agentin tehtävä on kerätä tietoa laitteesta, johon se on asetettu. Kun manageri lähettää kyselyn agentille, agentti vastaa kyselyyn lähettämällä queryn managerille. Agentin tehtäviä on kerätä haluttua tietoa, tallentaa ja palauttaa haluttua tietoa niin kuin se on määritetty MIB:ssä ja tiedottaa manageria poikkeavista tapahtumista. NMS saattaa kysyä agentilta esimerkiksi jonkin laitteen porttien tilaa. (Zoho Corp 2017.) Yhteyden toiminta managerin ja agentin välillä havainnoituna kuviossa 4.

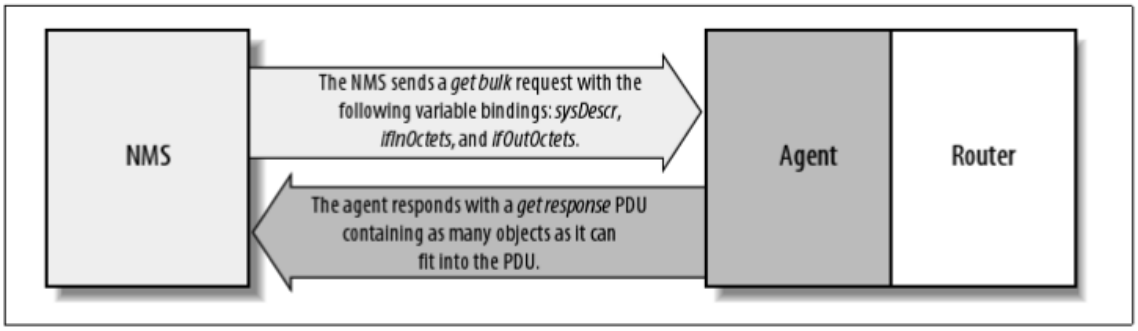


Kuvio 4: Havainnekuva managerin ja agentin välisestä yhteydestä (Schimidt & Mauro. 2008, 22)

3.2.2 SNMPv2

SNMPv2 oli seuraava versio SNMP:stä, jonka avulla pyrittiin parantamaan alkuperäisen version suorituskykyä, tietoturvaa, luotettavuutta ja managerilta-managerille yhteyttä. SNMPv2 laajensi myös uusilla operaatioilla SNMP-protokollaa. Uudet operaatiot, jotka lisättiin ovat GetBulk, Inform, notification ja report.

Getbulk-operaation avulla hallintaohjelma pystyy hakemaan yhdellä kerralla suuren määrän dataa tietokannasta. Eroavaisuus get- ja getbulk-operaatiolla on se, että getbulk kertoo agentille lähettävän niin paljon dataa, kun agentti pystyy lähettämään (ks. kuvio 5). Getbulkin saamat vastaukset voivat siis olla keskeneräisiä. Get-operaatio pystyy pyytämään enemmän kuin yhden objektin tietokannasta, mutta viestien koot rajoittuvat täysin agentin kapasiteettiin. Jos agentti ei pysty vastaamaan getin kaikkiin pyyntöihin, se vastaa vain virheviestillä, jossa ei ole ollenkaan dataa. Getbulk pyyntö toimii kahdella parametrillä, jotka ovat nonrepeaters ja max-repetitions. (Schimidt & Mauro, 2008, 71-72).



Kuvio 5: Getbulk-operaation pyyntö sekvenssi (Schimidt & Mauro. 2008, 72)

Inform-operaatio on ilmoitus mekaniikka, joka on hyödyllinen verkoissa, joissa on enemmän kuin yksi manageri. Kun inform lähetetään, vastaanottaja lähettää vastauksen lähettäjälle ja se on myös tiedostanut tapahtuman. (Schimidt & Mauro, 2008, 87).

Report-operaatio oli määritelty SNMPv2 luonnosversiossa, mutta sitä ei otettu käyttöön lopullisessa versiossa täytäntöön. Report-operaatio on otettu käyttöön SNMPv3-versiossa ja sen tehtävänä on mahdollistaa SNMP-järjestelmien kommunikointi keskenään ja esimerkiksi raportoida mahdollisista ongelmista SNMP-viestien prosessoinnissa. (Schimidt & Mauro, 2008, 87).

3.2.3 SNMPv3

Aikaisempien SNMP-versioiden suurin heikkous on ollut turvallisuus alusta alkaen. Autentikaatio SNMP:n versioissa yksi ja kaksi on ollut pelkkä salasana, jota lähetetään managerin ja agetin välillä. Salasanan onnistunut murtaminen on siis mahdollistanut sen, että manageri- ja agenttilaitteesta pystytään keräämään tietoa laitteistosta, muutamaan niiden määrityksiä tai jopa sulkea laitteet. (Schimidt & Mauro, 2008, 91).

SNMPv3 tiedostaa nämä turvallisuusongelmat, jotka ovat molemmissa aikaisemmissa versiossa. Käytännössä SNMPv3 tarkoitus on parantaa turvallisuutta ja muu toiminta perustuu täysin vanhojen versioiden toimintaan. SNMPv3 ei lisää esimerkiksi uusia operaatioita kuin edeltäjänsä SNMPv2. (Schimidt & Mauro, 2008, 91).

Tärkein muutos SNMPv3-versiossa on se, että se luopuu managerin ja agentin käsitteistä. SNMPv3-versiossa molempia, manageria ja agenttia, kutsutaan SNM- entiteetiksi. Jokainen entiteetti koostuu yhdestä SNMP-järjestelmästä ja yhdestä tai useammasta SNMP-sovelluksesta. Uudet konseptit ovat erittäin tärkeitä, koska ne määrittävät arkkitehtuurin, kun taas vain pelkistetyn joukon viestejä. Arkkitehtuuri helpottaa erottamaan erilaiset osat SNMP-järjestelmässä, mikä mahdollistaa turvallisuusmuutosten täytäntöönpanon. (Schimidt & Mauro, 2008, 91-92).

SNMPv3-järjestelmä koostuu neljästä eri osasta, jotka ovat lähettäjä, viestin käsittelyn alajärjestelmä, turvallisuus alajärjestelmä ja pääsyn hallinta alajärjestelmä. Lähettäjän tehtävä on lähettää ja vastaanottaa viestejä. Samalla lähettäjä yrittää myös selvittää vastaanottamansa viestin version (v1, v2, tai v3).Jos lähettäjän versio on tuettu, lähettäjä välittää viestin viestinkäsittelyalajärjestelmään. Lähettäjä myös lähettää SNM- viestejä toisille entiteeteille. (Schimidt & Mauro, 2008, 92).

Viestinkäsittelyalajärjestelmä valmistelee viestit lähettäväksi ja ottaa datan vastaanotetuista viesteistä. Viestinkäsittelyalajärjestelmä saattaa myös sisältää moninkertaisia viestin prosessointi moduuleita. Alajärjestelmällä saattaa olla moduulit prosessoida SNMPv1-, SNMPv2- ja SNMPv3-pyyntöjä. Alajärjestelmällä voi olla myös moduuli prosessoida vielä määrittämättömiä prossesointimoduleita. (Schimidt & Mauro, 2008, 92).

Turvallisuusalajärjestelmä tarjoaa todennuksen ja yksityispalveluita. Todennus käyttää joko yhteisömerkkijonoa tai SNMPv3-käyttäjä-perusteista todennusta. Käyttäjä-perusteinen todennus käyttää MD5- tai SHA-algoritmia todentaakseen käyttäjät ilman salasanan lähetystä. Yksityis palvelu käyttää DES-algoritmia salaukseen ja salauksen purkamiseen SNMP-viesteissä. DES on tällä hetkellä ainoa käytetty algoritmi, mutta tulevaisuudessa on mahdollisuus lisätä muita algoritmeja. (Schimidt & Mauro, 2008, 92-93).

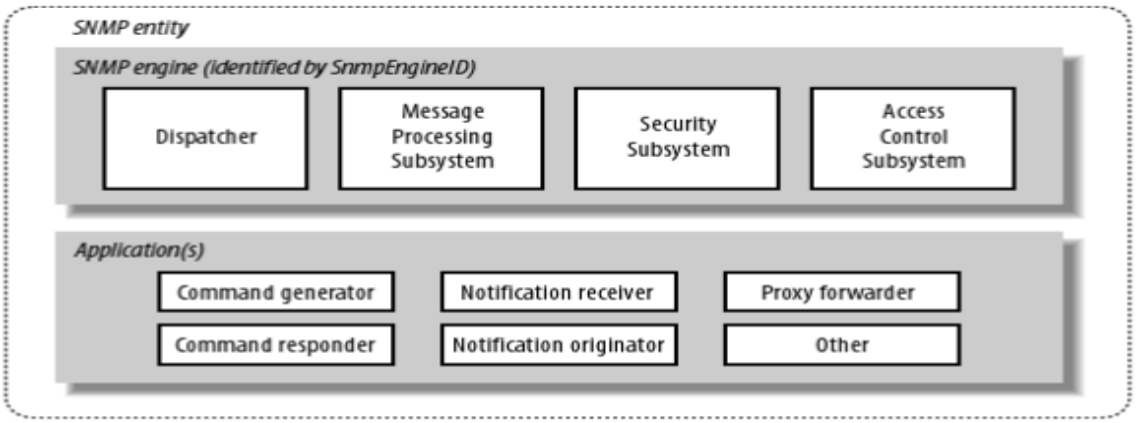
Pääsynhallinta-alajärjestelmä on vastuussa pääsemisestä MIB-objekteihin. Järjestelmällä voi valvoa mitä objekteja käyttäjä pääsee tarkistelemaan tai mitä operaatioita objektille voi suorittaa. Järjestelmällä voi esimerkiksi rajoittaa käyttäjän pääsemään vain lukemaan tietokannassa olevia objekteja. (Schimidt & Mauro, 2008, 93).

SNMP-versioissa olevat operaatiot esitetään SNMPv3:ssa omissa sovelluksissaan. Sovelluksia ovat Command generator, Command responder, Notification originator, Notification originator ja Proxy forwarder. Command generator tuottaa get, getnext, getbulk ja joukon käskyjä. Samalla se prosessoi vastaukset. Sovellus on toteutettu managerissa, jotta se pystyy luomaan kyselyitä ja joukon pyyntöjä entiteeteille, kytkimille ja muille isännille. (Schimidt & Mauro, 2008, 93).

Command responder vastaa get, getnext, getbulk ja joukko pyyntöihin. Sovellus on toteutettu Ciscon reitittimessä tai Unix-isännässä. SNMPv1- ja SNMPv2-versioissa command responder on toteutettu SNMP-agentissa. (Schimidt & Mauro, 2008, 93).

Notification originator tuottaa SNMP-trapit ja -ilmoitukset. Sovellus on toteutettu reitittimessä tai Unix-isännässä. Notification originator on aikaisemmissa SNMP-versioissa osa SNMP-

agenttia. Notification receiver vastaanottaa trapit ja ilmoitus viestit. Sovellus on toteutettu managerissa. Proxy forwarder helpottaa viestien kulkemista entiteettien välillä. (Schimidt & Mauro, 2008, 93). Kuviossa 6 SNMPv3:n entiteetti kokonaisuutena.



Kuvio 6: SNMPv3:n Entiteetti (Schimidt & Mauro. 2008, 94)

3.2.4 TCP/IP, UDP ja OID

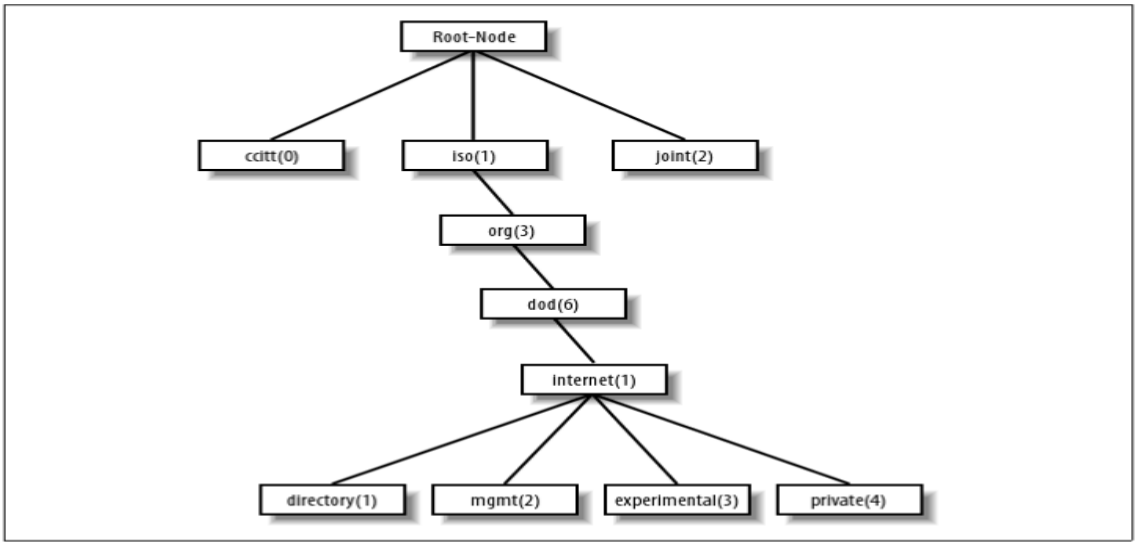
TCP/IP (Transmission Control Protocol/Internet Protocol) on joukko protokollia, jotka mahdollistavat kommunikaation internetissä. TCP keskittyy prosessoimaan ja käsittelemään dataa sovelluksista ja IP:n tehtävänä on lähettää ja vastaanottaa dataa sovelluksista. TCP/IP mahdollistaa erilaisten tietokoneiden tai muiden laitteiden käyttämään verkkoa ottaakseen toisiinsa yhteyttä ja jakamaan tietoa monilla ei tavoilla. (Sportack 2005.)

TCP/IP protokollat kartoittaa nelikerroksisen käsitemallin, joka tunnetaan nimellä DARPA-malli. DARPA-mallin neljä kerrosta ovat sovellus, kuljetus, verkko ja peruskerros. Sovelluskerros tarjoaa sovelluksille mahdollisuuden päästä palveluiden muihin kerroksiin ja määrittää protokollat, joita sovellukset käyttävät datan siirtämiseen. Kuljetuskerros mahdollistaa tietojen välittämisen koneelta koneelle. Verkkokerros on vastuussa osoittamisesta, paketoinnista ja reitittämisestä. Peruskerros on vastuussa pakettien lähettämisestä ja vastaanottamisesta.

UDP (User Datagram Protocol) on tiedonsiirto protokolla, jota SNMP käyttää lähettääkseen dataa managerien ja agenttien välillä. UDP valittiin SNMP:n käyttöön, koska se ei vaadi yhteyttä toimiakseen. UDP:ssä ei ole loppu-loppu -yhteyttä managerin ja agentin välillä, silloin kuin sillä lähetetään paketteja edestakaisin. Tämä ominaisuus tekee UDP:stä epäluotettavan siinä mielessä, että ei pystytä tietämään, kuinka paljon paketteja on lähetyksen aikana mahdollisesti hävinnyt protokolla kerroksessa. SNMP-sovelluksen tehtävän on selvittää, onko paketteja hävinnyt ja uudelleen lähettää hävinneet paketit, jos näin on määritetty. (Schimidt & Mauro, 2008, 37).

Manageri lähettää UDP-pyynnön agentille ja odottaa vastausta. Manageri odottaa vastausta sille määritetyn ajan verran. Jos vastaus ei saavu määritetyssä ajassa ja manageri ei ole saanut minkäänlaista tietoa agentilta, se määrittelee paketin hävinneen ja lähettää uudelleen pyynnön. Managerille voidaan asettaa tietty määrä uudelleenlähetyskertoja pyynnöille. (Schimidt & Mauro, 2008, 37).

Hallitut objektit järjestetään puumaiseen hierarkiaan. Tällainen struktuuri on alusta SNMP:n nimeämiskäytännölle (ks. kuvio 7). Objekti id (OID) muodostuu sarjasta kokonaislukuja, jotka pohjautuvat puussa olevista solmuista. (Schimidt & Mauro, 2008, 42).



Kuvio 7: Havainne kuva SMI objektipuusta (Schimidt & Mauro. 2008, 42)

3.2.5 SMI ja SMIv2

SMI (Structure of Management Information) määrittää tarkalleen, miten hallitut objektit nimetään ja täsmentää niihin liittyvät datatyypit. SMi:stä on kaksi eri versioita, jotka ovat SMIv1 ja SMIv2, joka parantaa SMIv1 versiota. (Schimidt & Mauro, 2008, 41).

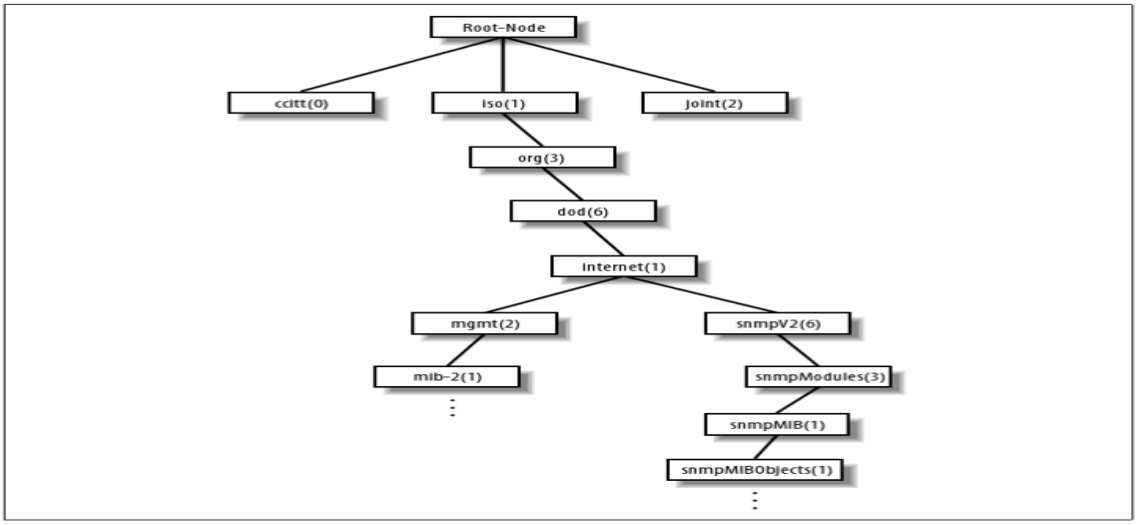
Hallitut objektit voidaan jakaa kolmeen eri attribuuttiin. Attribuutit ovat nimi, tyyppi ja syntaksi ja koodaus. Nimi attribuutti tai objektin tunniste (OID), määrittää yksilöllisesti hallitun objektin. Nimet yleisesti esiintyvät kahdessa eri muodossa: numeerisesti ja ”ihmisen luettavissa”. Molemmissa tapauksissa nimet ovat pitkiä ja hankalia. (Schimidt & Mauro, 2008, 41).

Hallitun objektin datatyyppi määritellään käyttämällä alijoukkoa ASN.1 (Abstract Syntax Notation One). ASN.1 on tapa, jolla täsmennetään, miten data esitetään ja lähetetään managerien ja agenttien välillä SNMP:n sisällössä. Hyvänä piirteenä ASN.1:sessä on se, että sen merkintätapa on laiteriippumaton. Tämä tarkoittaa sitä, että esimerkiksi tietokone, jossa on

käyttöjärjelemänä Windows 2000 pystyy kommunikoimaan Sun SPARC-laitteen kanssa ilman, että tarvitsee murehtia bittien järjestyksestä. (Schimidt & Mauro, 2008, 41).

Yksittäinen tapaus hallitussa objektissa koodataan oktetit-merkkijonona käyttäen BER:riä (Basic Encoding rules). Ber määrittää miten objektit koodataan ja dekoodataan, jotta ne voidaan lähettää esimerkiksi verkossa. (Schimidt & Mauro, 2008, 42).

SMIv2 laajentaa SMI-objekti puuta lisäämällä snmpV2-haaran internet ali-puuhun, joka lisää muutaman uuden datatyypin ja tehden useita muita mahdollisuuksia. Objektin määritelmä muuttuu SMIv2, jonkin verran SMIv1 määritelmään. Objektiin pääsyä on laajennettu ja objektille pystyy antamaan paremmat kuvaukset. (Schimidt & Mauro, 2008, 50). Kuviossa 8 havainnoidaan SMIv2 rekisteröinti SNPv2:seen.

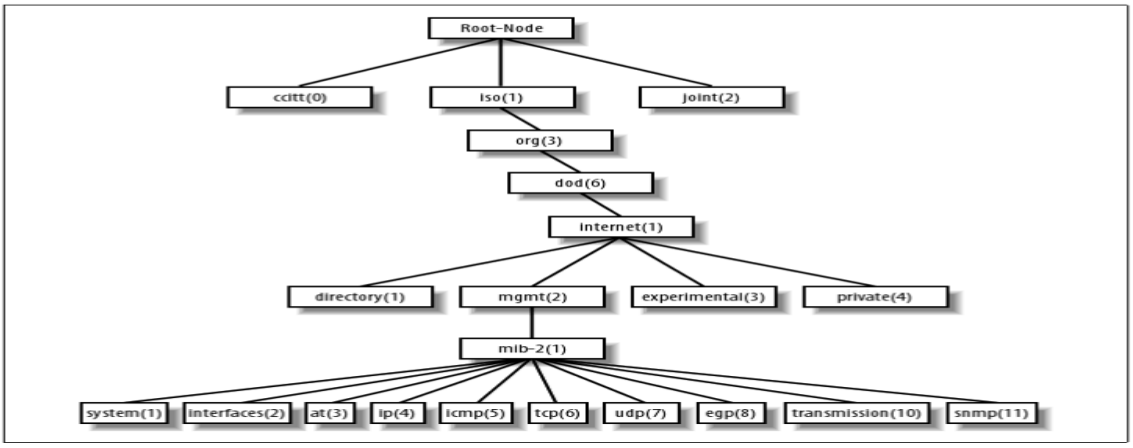


Kuvio 8: Havainne kuva SMIv2 rekisteröinnistä SNPv2:seen (Schimidt & Mauro. 2008, 51)

3.2.6 MIB ja ICMP

Management Information Base on tietokanta hallittavista objekteista, joita agentti seuraa. Minkälainen tahansa tilamuutos tai tilastollinen informaatio, johon pääsee managerilta on määritelty MIB:iin. SMI tarjoaa tavan määritellä hallittuja objekteja sillä aikaa, kun MIB on määritelmänä objekteille (ks. kuvio 9). MIB määrittää tekstinimen hallitulle objektille ja selittää objektin tarkoituksen. (Schimidt & Mauro, 2008, 22).

Agentti voi toteuttaa monia MIB:ejä, mutta jokainen agentti toteuttaa erityisen MIB:n, jota kutsutaan nimellä MIB-II. MIB-II on standardi, joka määrittelee muuttujia. Muuttujia voivat olla esimerkiksi jonkin rajapinnan tilastot, kuten rajanpinnan nopeus, lähetetyt tavut tai vastaanotetut tavut. MIB-II voi kertoa myös järjestelmään liittyviä tietoja esimerkiksi missä järjestelmä sijaitsee. Päätarkoituksena MIB-II:n on tarjota yleisestä TCP/IP hallintotietoa. MIB-II on erittäin tärkeä hallintaryhmä, koska jokaisen laitteen, joka tukee SNMP:tä tulee myös tueta MIB-II:sta. (Schimidt & Mauro, 2008, 22-23).



Kuvio 9: Havainnekuva MIB-II alipuusta (Schimidt & Mauro. 2008, 54)

Verkossa olevien IP-pakettien siirtyminen tapahtuu verkkojen ja niiden yhdistävien reitittimien avulla lähettäjältä vastaanottajalle. Siirtymien aikana saattaa esiintyä häiriöitä, kuten esimerkiksi reititin ei tiedä, miten reitittää paketti tai se ei löydä vastaanottajaa. Tällaisia tilanteita varten on kehitetty protokolla ICMP (Internet Control Message Protoko). ICMP on protokolla, jonka avulla voidaan virhetilanteissa lähettää reitittimien ja verkossa olevien laitteiden välillä virhe ja ohjausviestejä. ICMP on kiinteästi kytköksissä IP-protokollaan. ICM-protokollan tarkoitus on kertoa pelkästään verkossa olevista virheistä. Havaitut virheet korjataan muilla protokollilla tai verkon ylläpidon toimesta. ICMP käyttää toimiakseen IP:n tarjoamaa paketinvälityspalvelua. ICMP:n tekemät sanomat sijoittuu IP-paketissa olevaan datakenttään. ICMP:n sanomia voidaan myös kutsua pingiksi. (Postel 1981.)

3.2.7 OSI-malli

OSI (Open Systems Interconnection)-malli on tiedonsiirron standardi. Osi-malli koostuu seitsemästä eri kerroksesta, joiden avulla tiedon välitys muodostetaan. Kerrokset toimivat siten, että ylemmät kerrokset käyttävät alempia kerroksia, jotka ovat toiminnallisesti alkeellisempia (ks. kuvio 10). Kerrokset ovat fyysinen kerros, siirtoyhteyskerros, verkkokerros, kuljetuskerros, esitystapakerros ja sovelluskerros. (Tampere University of Technology 2002).

OSI-mallin alimpana kerroksena on fyysinen kerros. Fyysiseen kerrokseen liittyy kaikki tiedonsiirron loogiset, sähköiset ja mekaaniset kohdat. Tiedonsiirto voi tapahtua kahdella eri tavalla fyysisellä tasolla. Tavat ovat sarjamuotoinen tiedonsiirto ja rinnakkaismutoinen tiedonsiirto.

Sarjamuotoisessa tiedonsiirrossa siirretään bitit yksi kerrallaan peräkkäin. Etu sarjamuotoisesta tiedonsiirrosta on se, että tarvittavia siirtojohtimia ei tarvita välttämättä kuin kaksi. Jos halutaan kaksisuuntaista tiedonsiirtoa siirtojohtimia vaaditaan kolme. Kun bitit siirretään pe-

räkkäin, lähetettävien bittien, tavujen alku ja loppu täytyy merkitä jollain tavalla, jotta peräkkäin olevat bitit pystytään erottamaan toisistaan. (Tampere University of Technology 2002).

Rinnakkaismuotoinen tiedonsiirto tapahtuu siten, että yhden merkin kaikki bitit siirretään yhtä aikaa ja jokaisella bitillä on oma johdin. Sarjamuotoiseen tiedonsiirtoon verrattuna rinnakkaismuotoinen tiedonsiirto on huomattavasti nopeampaa. Peräkkäiset merkit erotetaan usein käytettävällä liipaisujohtimella, joka ilmoittaa uuden merkin alkamisen tulevalla signaalilla. Tiedonsiirto usealla rinnakkais johtimella ei ole suositeltavaa pitkillä matkoilla eikä myöskään langattomissa yhteyksissä. Yleinen käyttökohde rinnakkaiselle tiedonsiirrolle on tietokoneen sisältä tietokoneen lähelle oleviin oheislaitteisiin, kuten tulostimien välillä. (Tampere University of Technology 2002).

Siirtoyhteyskerros on OSI-mallin toinen kerros, joka hoitaa yhteyden luonnin, virheiden korjauksen ja yhteyden purkamisen. Yhteyden luominen ja purkautuminen tapahtuu fyysisestä kerroksesta riippuen. Siirtoyhteyskerros huolehtii myös vuonohjauksesta, eli siitä, ettei tietoa lähetetä nopeammin kuin mitä vastaanottaja pystyy tietoa käsitellä. Kolmas tehtävä siirtoyhteyskerroksella on huolehtia siitä, että tieto, joka kulkee sen läpi, on virheetöntä. Siirtoyhteyskerros varmistaa virheettömyyden virheitä havaitsevalla koodilla ja uudelleen lähettämällä virheellinen data. (Tampere University of Technology 2002).

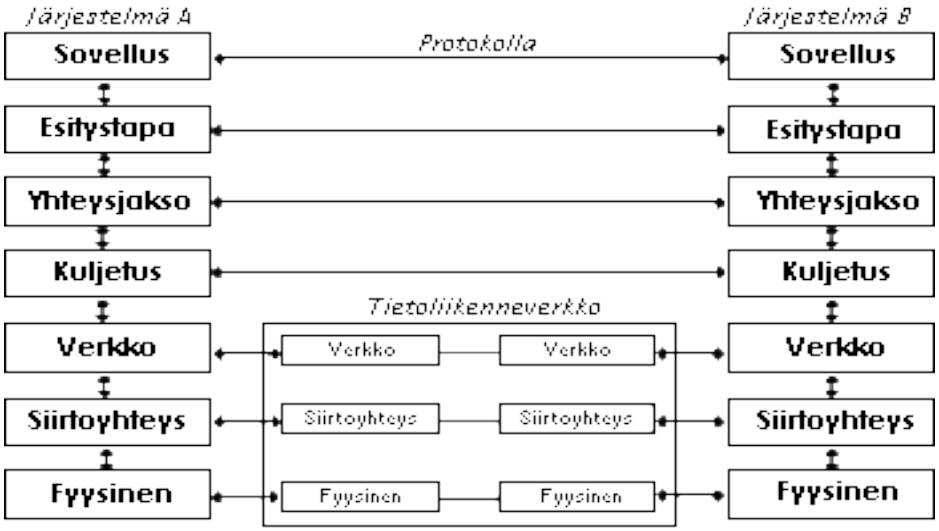
Verkkokerros on OSI-mallin kolmas kerros, joka tarjoaa riippumattoman tiedonsiirron verkon rakenteessa. Verkkokerroksen tarkoitus on piilottaa tiedonsiirron fyysisiin toteutuksiin liittyvät piirteet. Toiminnan ideana on se, että samalainen tietokoneverkko (samanlaisen verkkokerroksen omaava verkko) voidaan rakentaa fyysisesti eri tavalla. Esimerkiksi IP, jota voidaan käyttää puhelinlinjaa, lähiverkkoa kuin langatonta satelliittiyhteyttäkin pitkin. Verkkokerros valitsee monihaaraisessa tietokoneverkossa, mitä reittiä pitkin sanomat lähetetään. (Tampere University of Technology 2002).

Kuljetuskerros on on OSI-mallin neljäs kerros, jonka tehtävänä on taata luotettava yhteys päästä-päähän -tietokoneverkossa. Verkossa voi välillä syntyä katkoksia monista eri syistä, kuten esimerkiksi johdon katkeaminen tai tietokone vikaantuu. Tällaisen tapauksen sattuessa kuljetuskerroksen tehtävä on huolehtia siitä, että tietoliikenteessä aletaan käyttämään vaihtoehtoista reittiä, jotta tietoliikenne ei katkea. (Tampere University of Technology 2002).

Yhteysjaksokerros on OSI-mallin viides kerros, joka huolehtii siitä, ettei tiedonsiirto sekoitu esimerkiksi, kun fyysinen yhteys katkeaa. Yhteysjaksokerroksella on myös muita tehtäviä, kuten tiedon salaaminen tarvittaessa. (Tampere University of Technology 2002).

Esitystapakerros on OSI-mallin kuuden kerros, jossa esitystapakerros hoitaa tiedon esitysmuodon oikeanlaiseksi tiedonsiirtojen yhteydessä. Esitystapakerros päättää esimerkiksi missä muodossa kokonaisluvut, tekstit, kuvat tai äänet esitetään tiedonsiirron yhteydessä. Tämän tarkoituksena on se, että tiedot ovat oikeassa muodossa, jotta vastaanottaja pystyy ymmärtämään sen. (Tampere University of Technology 2002).

OSI-mallin viimeinen kerros on sovelluskerros. Sovelluskerroksella on lähinnä yksi tehtävä ja se on toimia linkkinä ohjelmaan, joka tarvitsee tiedonsiirtoa. (Tampere University of Technology 2002).

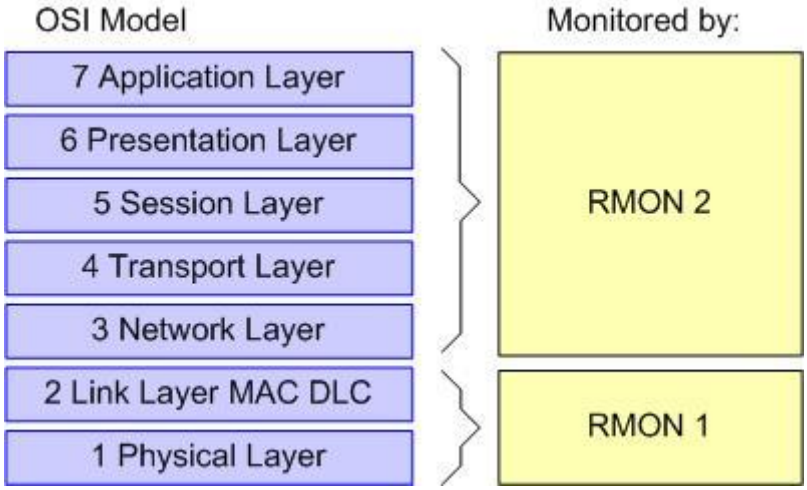


Kuvio 10: Osi-malli (Tampere University of Technology 2002)

3.2.8 RMON, Syslog ja CIM

RMON (Remote Network Monitoring) on samankaltainen verkonvalvontaprotokolla, kuten SNMP. RMON:in alkuperäinen tarkoitus oli täysin keskittyä verkon valvomiseen, mutta sen toimintaa on laajennettu valvomaan myös laitteita. RMON toimii SNMP tavoin myös asiakas-palvelin -mallilla. Kuvio 11 havainnoi RMON valvontaa, osi mallissa. Asiakkaat eli laitteet sisältävät RMON-agentteja, joiden tehtävänä on kerätä tietoa ja analysoida verkon liikennettä esimerkiksi pakettien siirtoa. RMON suurin eroavaisuus on siinä, että se tarkastelee tietoliikennettä, kun taas SNMP:tä käytetään yleisemmin laitepohjaiseen hallintaan. RMON siirtää hallintaohjelmalle tietoa ainoastaan, kun sitä pyydetään. (LUTEUS SARL 2004).

RMON:nin alkuperäistä versiota kutsutaan myös nimellä RMON1, joka keskittyy OSI Taso yksi- ja taso 2-tietoon verkossa. RMON1 sai laajennuksen, joka tunnetaan nimellä RMON2. RMON2 laajentaa verkkoliikenteen valvontaa korkeamman tason protokollille. Verkkoliikenteen tiedot ovat kriittisiä tietoja vianetsintää varten asiakas-palvelin -ympäristöissä. (LUTEUS SARL 2004).



Kuvio 11: Havainne kuva RMON valvonnasta OSI-mallissa (LUTEUS SARL 2004)

Syslog on protokolla, jolla voi lähettää lokiin kirjattuja tapahtumia eteenpäin. Tapahtumia voidaan lähettää esimerkiksi hallintapalvelimelle tai muulle määrätylle palvelimelle. Syslogilla on kolme eri kerrosta, jotka ovat syslog-sisältö, syslog-applikaatio ja syslog-lähetin. Syslog-sisällössä on tiedot tapahtumasta. Syslog-applikaatio on kerros, joka luo, tulkitsee, reitittää ja tallentaa viestin, sillä välin kun syslog-lähetin-kerros välittää viestin verkossa. (Parsons 2014.)

Common Information Model tarjoaa yhteisen määritelmän tiedonhallinnan järjestelmille, verkoille, sovelluksille ja palveluille ja valmistajan laajennuksille. CIM-standardi sisältää määritelmän ja kaavion sekä metamallin. (DMTF 2017).

CIM-malli tarjoaa varsinaiset mallikuvaukset. Hallintamallit ovat rakennuslohkoja hallinta-alustoille ja hallintasovelluksille, kuten laitteen määritys, suorituskyvynhallinta ja muutostenhallinta. (DMTF 2017).

CIM:iä voidaan käyttää monella eri tavalla ja CIM-määritys määrittelee yksityiskohdat integraatiota varten muiden hallintamallien kanssa. CIM:ssä oleva tieto tehtävien suorittamiseen on järjesteltyä, jotta eri ryhmissä olevat ihmiset voivat käyttää niitä. (DMTF 2017).

CIM-Metamalli määrittää semantiikan uusille rakenteilla oleville vaatimuksenmukaisille malleille ja kaavion, joka esittää näitä malleja. Mallinnusvaatimukset ja ympäristöt ovat usein erilaisia ja muuttuvat ajan kanssa. (DMTF 2017).

3.2.9 WMI ja WBEM

WMI (Windows Management Instrumentation) on Windows käyttöjärjestelmille tarkoitettu hallintatietojen ja operaatioiden infrastruktuuri. WMI:llä voi kirjoittaa omia skriptoja, luoda ohjelmia, jotka suorittavat automaattisesti ylläpidollisia tehtäviä etäyhteyksien päässä oleviin tietokoneisiin. WMI myös tarjoaa hallinta dataa muihin osiin käyttöjärjestelmässä ja ohjelmiin. WMI käyttää CIM (Common Information Model) standardia, kun sillä määritetään esimerkiksi ohjelmien, järjestelmien, verkkojen, laitteiden tai muita valvottavia komponentteja. WMI tekee hyödylliseksi se, että sillä pystytään tarkkailemaan ja hallitsemaan laitteita etänä Windows ympäristöissä, jotka ovat erittäin yleisiä yrityksissä. Näillä toiminnoilla pystytään helposti ennaltaehkäistä vikatilanteita ja selvittämään niitä. (Microsoft 2017).

WBEM (Web-Based Enterprise Management) on joukko hallinta- ja internetstandarditeknologioita, jotka on kehitetty yhteistämään hajautettuja tietojenkäsittely alustoja, helpottamaan datan siirtymistä erilaisten teknologioiden ja alustojen välillä. (DMTF 2017).

DMTF (Distributed Management Task Force) on kehittänyt ytimen joukolle standardeja, joista WBEM koostuu. Standardit ovat CIM, CIM-XML, CIM Query Language, WBEM Discovery, joka käyttää SLP:tä ja WBEM Universal Resource Identifier-kartoitus (URI). Lisäksi DMTF on kehittänyt WBEM-hallintaprofiili mallin, joka mahdollistaa yksinkertaistetun profiilin kehittämisen. Yksinkertaisella profiililla pyritään tarjoamaan valmis, itsenäinen määritelmä hallitsemaan tiettyä osaa järjestelmässä, alijärjestelmää, palvelua tai muuta entiteettiä. (DMTF 2017).

4 Verkonvalvontaohjelmistot

Verkonvalvontaohjelmistoja on saatavilla ilmaiseksi, mutta myös kaupallisia versioita on saatavissa. Ilmaiset ohjelmistot yleensä perustuvat vapaaseen lähdekoodin, joten ne ovat käytännössä kenen vain muokattavissa. Maksullisessa versioissa on yleensä parempi asiakastuki tuotteelle, mutta asiakas saattaa joutua myös loukkuun tuotteen kanssa. Esimerkiksi, jos tuotetta pitäisi saada räätälöityä omaan käyttöön paremmin toimivaksi, se saattaa olla mahdotonta tai erittäin kallista.

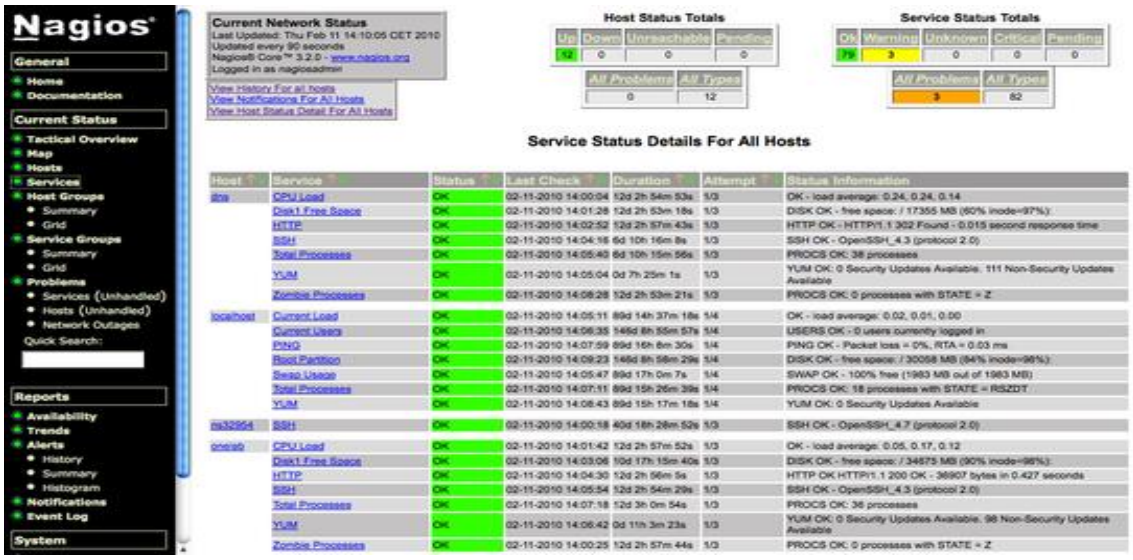
Laitevalmistajat myös valmistavat omia ohjelmistoja tuotteilleen, mutta toiminnot niissä ovat erittäin rajattuja, koska ne perustuvat yleensä vain ja ainoastaan valmistajan tuotteisiin. Tämä saattaa aiheuttaa paljon ristiriitoja, jos verkossa on toisen valmistajan laitteita, joita halutaan valvoa toisen valmistajan ohjelmistolla.

4.1 Vapaan lähdekoodin valvontaohjelmistot

Vapaan lähdekoodin valvontaohjelmistot ovat ilmaisia ladata ja käyttää. Yleisimpiä ja käytetyimpiä vapaaseen lähdekoodiin perustuvia valvontaohjelmistoja ovat esimerkiksi Nagios ja Nino.

4.1.1 Nagios

Nagios on kattava valvontaohjelmisto, joka oikein asennettuna ja määritettynä voi toimia erittäin hyvin pienissä ja isoissa yrityksissä. Ohjelmistossa on kaikki perustoiminnot saatavilla, kuten järjestelmän yleiskatsaus, karttanäkymä ja hälytysnäyttö (ks. kuvio 12). Nagios vie toiminnot astetta syvemmälle lisäämällä sektiot myös trendeille, taktiselle yleiskatsaukselle ja prosessi- ja suorituskykydatalle. Nagioksessa on myös mahdollisuus tutkia omaa verkkoa 3D-kartalla. (Schimidt & Mauro, 2008, 420).



Kuvio 12: Nagios-yleisnäkymä palveluiden tilasta (Nagios)

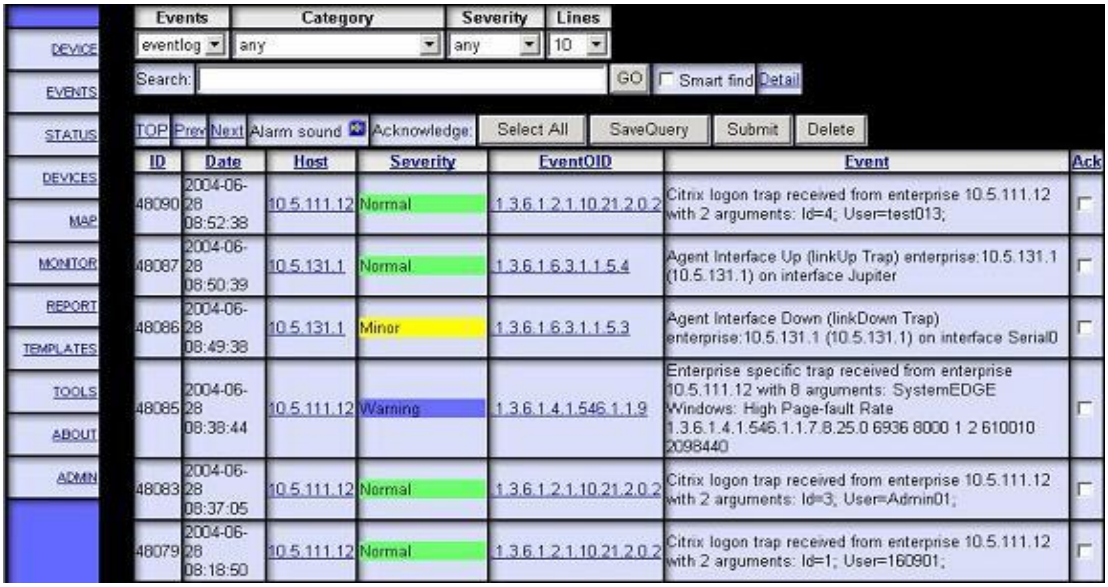
4.1.2 Nino

Nino on käyttöön, jossa halutaan paljon toimintoja ja loistetta ohjelmistolta. Nino sisältää kaikki normaalit toiminnot, joita verkonvalvontaohjelmistolta odotetaan, mutta Nino sisältää myös erikoisempia toimintoja, joita ei välttämättä kaikista vapaaseen lähdekoodiin perustuvista valvontaohjelmistoista löydy. (Schimidt & Mauro, 2008, 428).

Tällaisia toimintoja ovat esimerkiksi Nino hostmeter, interaktiivinen 3D-kartta, äänitoiminnot ja MIB-hakutyökalu. Nino hostmeter toiminolla saa erinomaisen näkymän objektin tilasta, jolla voi myös valvoa reitittimiä ja muita laitteita. Toiminolla näkee esimerkiksi laitteen levyjen tilat, prosessit ja prosessorin käytön (ks. kuvio 13). (Schimidt & Mauro, 2008, 429).

Interaktiivisella 3D-kartalla pystyy tutkimaan objekteja jokaisesta eri perspektiivistä tai laittamaan objektin kääntymään automaattisesti eri suuntiin kartassa. Äänitoimintoja voi määrittää esimeriksi, kun laite menee alas tai jokin muu tärkeä tapahtuma tapahtuu ja se vaatii huomiota. Äänitoimintoihin ei kuitenkaan voi luottaa täysin, koska verkon ylläpitäjä ei välttämättä ole tapahtuman tapahtuessa äänen kuuloetäisyydellä. (Schimidt & Mauro, 2008, 429).

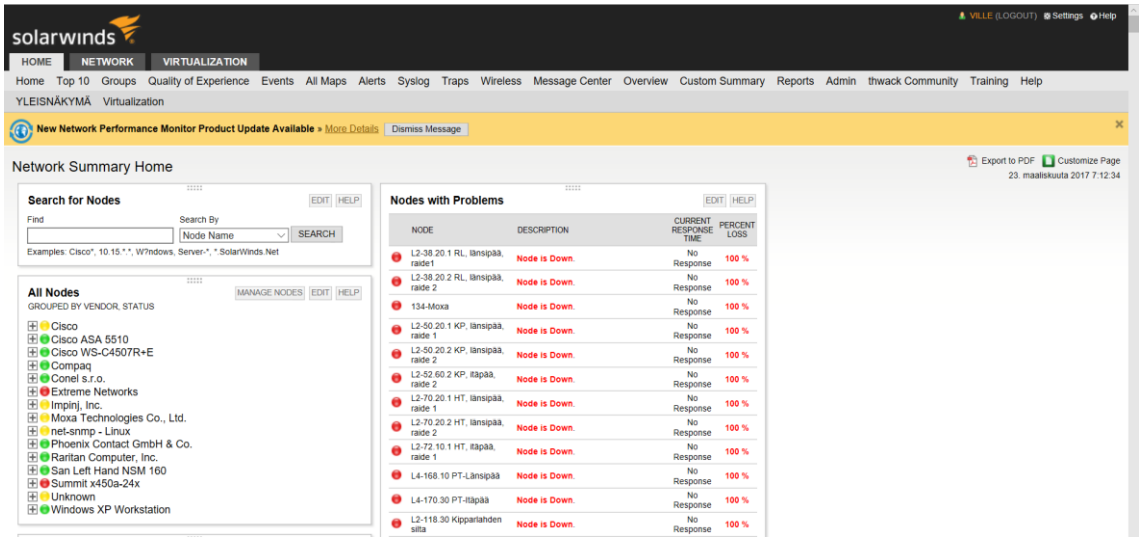
MIB-hakutyökalulla pystyy etsimään hakusanoilla tietoa MIB-tietokannasta. Kun hakusanalla löytyy haluttu tietoa, sitä voi tarkastella MIB-selaimessa ja tietoa voi laajentaa tarpeen mukaan. (Schimidt & Mauro, 2008, 429).



Kuvio 13: Nino tapahtumanäkymä (Nino)

4.2 Solarwinds Orion NPM

Solarwinds Orion NPM on kaupallinen verkonvalvontaohjelmisto, jossa on kaikki tarvittavat komponentit verkonvalvontaa varten. Komponentteja ovat muun muassa kyselyitä suorittava järjestelmä, hälytysjärjestelmä ja raportointijärjestelmä. Kuvio 14 näyttää Solarwinds Orion NPM:n etusivun.

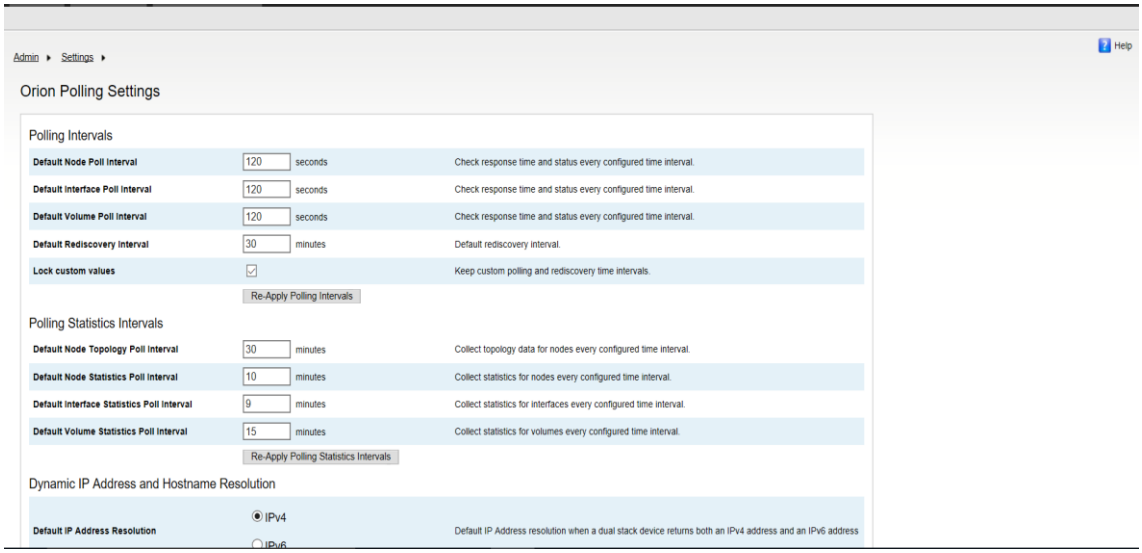


Kuvio 14: Solarwinds Orion NPM:n etusivu (HKL Sisäinen materiaali)

4.2.1 Kyselyjärjestelmä

Kyselyjärjestelmä suorittaa määrätyn ajan välein kyselyitä verkonvalvonnassa oleville laitteille, jos kyselyissä havaitaan poikkeuksia siitä aiheutuu hälytys, jos näin on määritetty poikkeuksen aiheuttavalle laitteelle. Poikkeus voi syntyä esimerkiksi, jos laitteen vastausaika on liian pitkä tai laite ei vastaa takaisin ollenkaan kyselyyn. Kun kysely ei saa vastausta laitteelta, kyselyjärjestelmä siirtyy nopeaan kyselymenetelmään.

Nopea kyselyly -menetelmä alkaa 10 sekunnin välein kutsumaan laitetta kahden minuutin ajan. Jos nopean kyselyn aikana kyselyjärjestelmä ei tavoita laitetta se määrittää laitteen down-tilaan. Laitteen mennessä down-tilaan saa verkonvalvoja tästä tiedon hälytyksenä. Asetuksia voidaan muokata Kuvio 15 esittämässä näkymässä.



Kuvio 15: Kyselyjärjestelmän asetusnäkymä (HKL Sisäinen materiaali)

4.2.2 Hälytysjärjestelmä

Hälytysjärjestelmän tehtävänä on kertoa tiedot hälytyksistä verkon ylläpidolle. Tiedoissa kerrotaan esimerkiksi mikä laite on kyseessä, laitteen sijainti, hälytyksen syy ja hälytyksen aikatiedot. Hälytysjärjestelmällä pystytään valvomaan esimerkiksi laitteiden lämpötiloja, tuulettimien nopeuksia ja virrankulutusta. Hälytyksen laukaisu voi tapahtua monesta eri syystä ja verkon ylläpito voi määrittää erittäin tarkasti, mistä syistä hälytys laukaistaan.

Yleisin syy, josta halutaan hälytys on, kun laite menee down-tilaan tai laitteen sisäiset toiminnot, kuten esimerkiksi muistit alkavat olla täynnä. Muistin mentyä täyteen tästä voi aiheutua esimerkiksi pakettihävikkiä, joka tarkoittaa, että lähetetyt paketit eivät pääse perille. Tämä voi aiheuttaa verkossa ongelmia, kuten suurta viivettä. Tällaisiin laitteisiin, jotka sisältävät muistia, on erittäin tärkeä määrittää hälytys, kun laitteen muisti on esimerkiksi 90% käytössä. Tämä mahdollistaa verkon ylläpidolle mahdollisuuden ajoissa reagoida ja tehdä toimenpiteet laitteelle ennen kuin laite on mennyt vikatilaan. Tällä pyritään siihen, että verkko toimii luotettavasti. Kuvio 16 esittelee minkälaisia tapahtumia verkonvalvonta on havainnut.

Quick Start | Current Events

Group By Network Node | Include | Refresh

Clear	Event Type	Event Type	Event Time	Message
VAP-210				
	Alert Reset		23.3.2017 6:59:55	Node VAP-210 has dropped its average response time from above 200ms to 20 ms which falls below the 100ms threshold.
	Alert Reset		23.3.2017 6:53:53	Node VAP-210's packet loss has dropped from above 40% to below 5% and is currently 0 %.
	Alert Triggered		23.3.2017 6:36:48	Node VAP-210 has an average response time of 373 ms which falls above the 200ms threshold.
	Alert Reset		23.3.2017 6:33:47	Node VAP-210 has dropped its average response time from above 200ms to 70 ms which falls below the 100ms threshold.
	Alert Triggered		23.3.2017 6:20:44	Node VAP-210 has an average response time of 452 ms which falls above the 200ms threshold.
	Alert Reset		23.3.2017 6:06:40	Node VAP-210 has dropped its average response time from above 200ms to 45 ms which falls below the 100ms threshold.
	Alert Triggered		23.3.2017 5:29:29	Node VAP-210 has an average response time of 271 ms which falls above the 200ms threshold.
	Alert Triggered		23.3.2017 5:26:29	Node VAP-210's packet loss has risen above 40% to 60 %.
	Alert Reset		23.3.2017 5:08:23	Node VAP-210 has dropped its average response time from above 200ms to 23 ms which falls below the 100ms threshold.
	Alert Triggered		23.3.2017 4:54:20	Node VAP-210 has an average response time of 270 ms which falls above the 200ms threshold.
	Alert Reset		23.3.2017 4:48:18	Node VAP-210 has dropped its average response time from above 200ms to 92 ms which falls below the 100ms threshold.
	Node Rebooted		23.3.2017 4:10:43	VAP-210 rebooted at 3/23/2017 4:10:00 AM
RFID 139-140				
	Alert Reset		23.3.2017 6:58:55	Node RFID 139-140's packet loss has dropped from above 40% to below 5% and is currently 0 %.
	Alert Reset		23.3.2017 6:23:45	Node RFID 139-140 is Up.
	Node Up		23.3.2017 6:23:40	RFID 139-140 is responding again. Response time is 4 milliseconds.
	Alert Triggered		23.3.2017 6:17:43	Node RFID 139-140 is Down.
	Node Down		**23.3.2017 6:17:14**	**RFID 139-140 has stopped responding (Request Timed Out)**
	Alert Reset		23.3.2017 6:09:41	Node RFID 139-140 is Up.
	Node Up		23.3.2017 6:09:14	RFID 139-140 is responding again. Response time is 10 milliseconds.
	Alert Triggered		23.3.2017 6:07:40	Node RFID 139-140 is Down.
	Node Down		**23.3.2017 6:06:45**	**RFID 139-140 has stopped responding (Request Timed Out)**
	Alert Reset		23.3.2017 6:03:39	Node RFID 139-140 is Up.
	Node Up		23.3.2017 6:02:45	RFID 139-140 is responding again. Response time is 3 milliseconds.
	Alert Triggered		23.3.2017 5:56:37	Node RFID 139-140 is Down.
	Node Down		**23.3.2017 5:56:24**	**RFID 139-140 has stopped responding (Request Timed Out)**
	Alert Reset		23.3.2017 5:50:36	Node RFID 139-140 is Up.
	Node Up		23.3.2017 5:50:26	RFID 139-140 is responding again. Response time is 7 milliseconds.
	Alert Triggered		23.3.2017 5:48:35	Node RFID 139-140 is Down.
	Alert Reset		23.3.2017 5:48:35	Node RFID 139-140 has dropped its average response time from above 200ms to which falls below the 100ms threshold.
	Node Down		**23.3.2017 5:47:41**	**RFID 139-140 has stopped responding (Request Timed Out)**
	Alert Triggered		23.3.2017 5:38:32	Node RFID 139-140 has an average response time of 210 ms which falls above the 200ms threshold.
	Alert Reset		23.3.2017 5:26:29	Node RFID 139-140 has dropped its average response time from above 200ms to 44 ms which falls below the 100ms threshold.
	Alert Reset		23.3.2017 5:22:28	Node RFID 139-140 is Up.
	Node Up		23.3.2017 5:21:40	RFID 139-140 is responding again. Response time is 15 milliseconds.
	Alert Triggered		23.3.2017 5:14:25	Node RFID 139-140 is Down.
	Alert Triggered		23.3.2017 5:14:25	Node RFID 139-140 has an average response time of 265 ms which falls above the 200ms threshold.
	Node Down		**23.3.2017 5:13:41**	**RFID 139-140 has stopped responding (Request Timed Out)**

Kuvio 16: Tapahtumien yleisnäkymä (HKL Sisäinen materiaali)

4.2.3 Raportointijärjestelmä

Raportointijärjestelmällä voidaan tarkastella laitteiden toimintaa raportin muodossa. Raportteja voidaan luoda tärkeistä laitteista, josta halutaan tietää esimerkiksi, mitkä laitteet on ollut eniten käytössä tai vähiten. Raportit ovat tärkeitä verkon ylläpitäjille, koska niiden avulla pystytään tulevaisuudessa suunnitelmaan ja kehittämään verkon ympäristöä. Kuukauden otanta liikennemäärästä verkossa kuviossa 17.

Average and Peak Traffic Rates by Access Point - This Month

NAME	CONTROLLER	VENDOR	IP ADDRESS	AVERAGE TRANSMIT BPS	PEAK TRANSMIT BPS	AVERAGE RECEIVE BPS	PEAK RECEIVE BPS
April 2017							
Syd-1130a-1	Syd-Cisco2106		10.199.20.101	251.738 kbps	550.172 kbps	465.0 kbps	1.062 Mbps
Syd-1130a-2	Syd-Cisco2106		10.199.20.102	275.127 kbps	570.286 kbps	701.667 kbps	1.594 Mbps
Syd-1130a-3	Syd-Cisco2106		10.199.20.103	200.172 kbps	510.368 kbps	840.0 kbps	2.046 Mbps
Syd-1130a-4	Syd-Cisco2106		10.199.20.104	349.108 kbps	534.93 kbps	279.211 kbps	451.053 kbps
Syd-1130a-5	Syd-Cisco2106		10.199.20.105	293.135 kbps	790.985 kbps	186.104 kbps	545.831 kbps
AustinAP1130.1	Aus-Cisco2106		10.199.20.121	248.543 kbps	430.43 kbps	1.102 Mbps	2.478 Mbps
AustinAP1130.2	Aus-Cisco2106		10.199.20.122	203.333 kbps	550.0 kbps	203.333 kbps	550.0 kbps
AustinAP1130.3	Aus-Cisco2106		10.199.20.123	230.072 kbps	380.172 kbps	443.333 kbps	892.0 kbps
AustinAP1130.4	Aus-Cisco2106		10.199.20.124	255.127 kbps	430.286 kbps	681.667 kbps	1.454 Mbps
AustinAP1130.5	Aus-Cisco2106		10.199.20.125	338.505 kbps	560.368 kbps	978.333 kbps	2.096 Mbps
Cisco1130-1-Cia	Cai-2106		10.199.20.141	285.578 kbps	746.905 kbps	207.568 kbps	584.074 kbps
Cisco1130-2-Cia	Cai-2106		10.199.20.142	269.261 kbps	559.114 kbps	265.676 kbps	554.811 kbps
Cisco1130-3-Cia	Cai-2106		10.199.20.143	206.876 kbps	510.43 kbps	1.06 Mbps	2.558 Mbps
CiaAP1130a-Guest	Cai-2106		10.199.20.144	237.205 kbps	452.646 kbps	244.918 kbps	461.902 kbps
CiaAP1130a-Lab	Cai-2106		10.199.20.145	282.868 kbps	539.442 kbps	268.364 kbps	522.037 kbps
Tok-M5200-1	Tok-ArubaM5200		10.199.20.161	366.667 kbps	580.0 kbps	366.667 kbps	580.0 kbps
Tok-M5200-2	Tok-ArubaM5200		10.199.20.162	145.072 kbps	380.172 kbps	358.333 kbps	892.0 kbps
Tok-M5200-Lobby	Tok-ArubaM5200		10.199.20.163	268.461 kbps	570.286 kbps	695.0 kbps	1.594 Mbps
BRAruba200-North	Bru-Aruba200		10.199.20.181	328.505 kbps	580.368 kbps	968.333 kbps	2.116 Mbps
BRAruba200-West	Bru-Aruba200		10.199.20.182	320.991 kbps	567.872 kbps	315.127 kbps	554.303 kbps
Lab-ArubaM5200	Bru-Aruba200		10.199.20.183	238.543 kbps	540.43 kbps	1.092 Mbps	2.588 Mbps
MeruTC1.1	MeruWC1		10.199.20.200	279.417 kbps	595.3 kbps	270.237 kbps	584.284 kbps

Kuvio 17: Esimerkki tukiasemien liikennemäärästä kuukauden otannalla (HKL Sisäinen materiaali)

5 Tutkimuksen toteutus

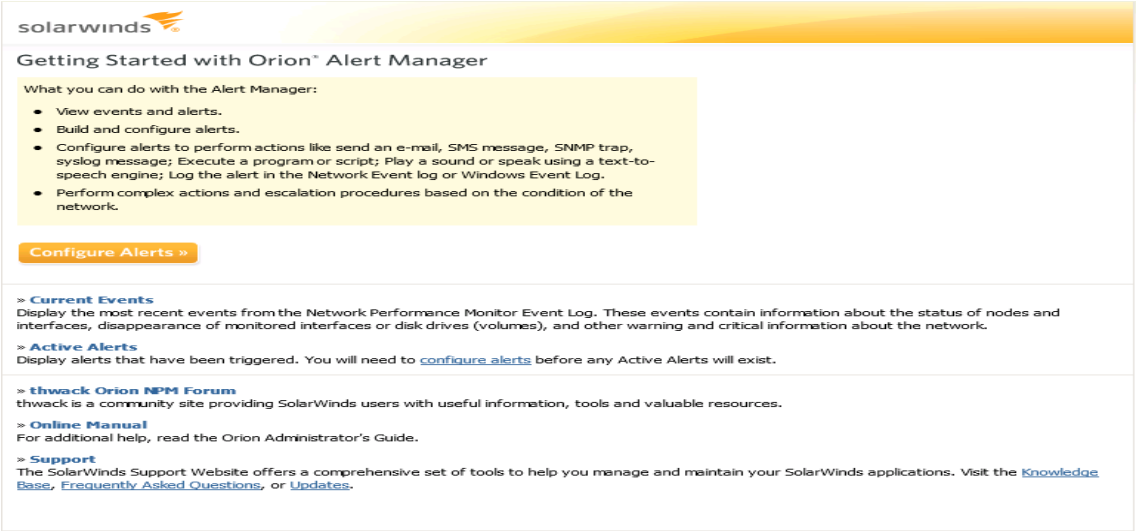
Toimeksiantajan tarkoituksena on saada valittujen kriittisten metrolan-verkon tietoliikennelaitteiden häiriöistä ja vikaantumisista reaaliaikainen hälytys. Hälytykset suunnitellaan siten, että tarpeettomat ja turhat hälytykset karsiutuvat pois ja jatkossa saadaan vain aiheellisista laitteista ja syistä hälytys. Hälytyksestä saatava tieto määritetään tulemaan sähköpostitse kohdennetuille käyttäjille. Laitteet, joista halutaan hälytys ovat runkoverkon laitteet, tukiasemat, rata-alueen kytkimet ja kaksi palvelinta.

Tutkimuksen alussa selvitettiin miten yrityksen verkonvalvontaohjelmisto toimii ja mihin verkonvalvontaohjelmisto pystyy. Tietoa ohjelmistosta pystyi lähinnä etsimään ohjelmiston verkkosivuilta ja hankaliin kysymyksiin vastauksia löytyi ohjelmiston omalta keskustelupalstalta. Keskustelupalstalla ohjelmiston kehittäjät vastaavat käyttäjien kysymyksiin ja usein kysymyksiä, joita syntyi tutkimuksen aikana oli kysytty jo keskustelupalstalla.

Tutkimusmateriaalin avulla aloitettiin testamaan ohjelmistoa erilaisilla hälytyksillä, jotta ohjelmistoon tehtävät viralliset muutokset voidaan ottaa käyttöön. Ohjelmistossa on oma Alert Manager, jolla hälytyksiä voidaan muokata ja testata hälytyksiä, ilman että ne ovat oikeasti käytössä (ks. kuvio 18). Testeissä muun muassa testattiin välittyykö hälytystieto sähköpostitse määrätyille käyttäjille, onko viestin tiedot määrätyn mukaisia ja välittyykö viesti määritetystä syystä. Toimeksiantajan pyytämä käyttöopas luotiin myös kerätystä tutkimusmateriaalista.

Hälytysten luonti ja määrittäminen voidaan suorittaa metrolan-verkon laitteille Solarwinds Orion NPM palvelimen hallinta tietokoneella. Hallinta tietokoneella täytyy kirjautua administrator tunnuksilla, jotta voidaan suorittaa tehtäviä muutoksia. Hallinta tietokoneelta löytyy Solarwinds Orion NPM ohjelmisto, joka avataan työpöydältä. Hälytysten hallinta tapahtuu Solarwinds Orion NPM ohjelmiston sisällä olevalla Advanced alert managerilla.

Solarwinds Orion NPM:ssä voidaan määrittää lähettämään hälytystieto erilaisista syistä, joita ovat muun muassa, kun laitteen tila on mennyt down, up, unknown, warning, unmanaged tai external. Laitteet mitkä on valittu metrolan-verkosta määritetään antamaan hälytys, kun laitteen tila menee down tai up.



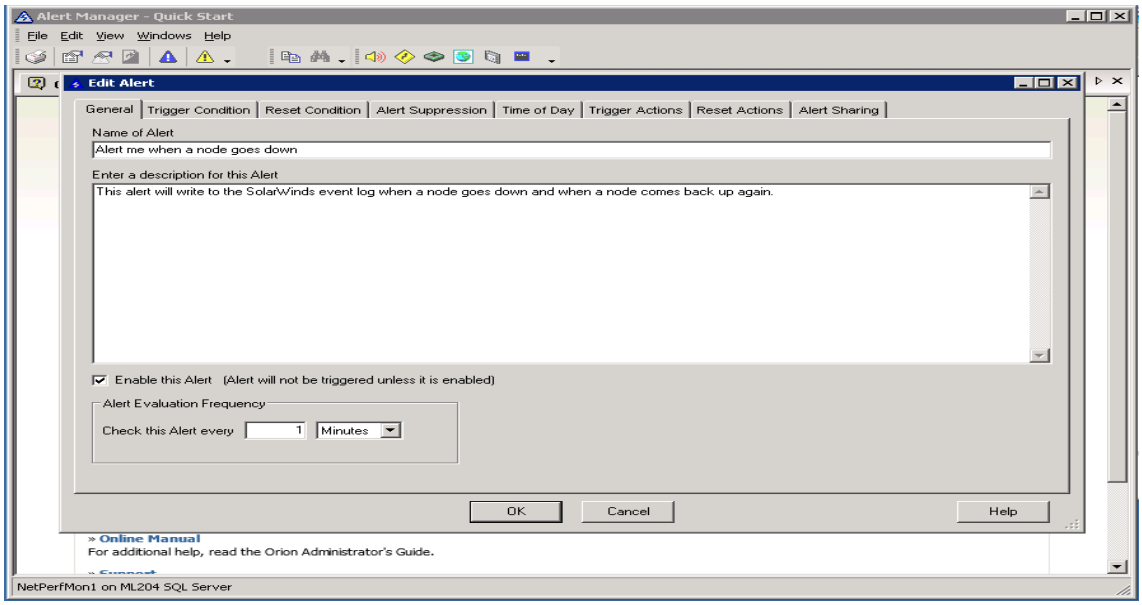
Kuvio 18: Solarwinds Orion NPM Alert manager (HKL Sisäinen materiaali)

Alert manager mahdollistaa hälytysten luomisen ja muokkaamisen. Solarwinds Orion NPM sisältää laajan valmiiksi luotuja hälytys vaihtoehtoja. Hälytys vaihtoehtoja ovat muun muassa hälytä, kun laite menee alas, hälytä, kun laite käynnistyy uudelleen tai hälytä, kun laite poistetaan. Toimeksiantaja haluaa hälytyksen, kun laite menee alas, joten luettelossa oleva hälytä, kun laite menee alas valmis vaihtoehto otetaan käyttöön ja siihen täytyy tehdä muutoksia. Hälytystä muuttaessa tulee ottaa huomioon mitä halutaan tietää hälytyksestä ja mikä laukaisee hälytyksen.

Hälytykselle määritetään nimi ja kuvaus (ks. kuvio 19). Hälytyksen nimi tulee olla selkeä, jotta verkon ylläpidon on helppo ymmärtää mistä hälytyksessä on kyse. Hälytykselle määritetään ehdot mistä hälytys laukeaa ja resetoituu. Laiteen mennessä alas ehtona toimii, kun kysely ei saa vastausta laitteelle ja kysely suorittaa nopean kyselyn. Jos nopean kyselyn jälkeen laitteesta ei saada vastausta, laite merkitään alas tilaan. Laitteen tullessa takaisin ylös, kun kysely tavoittaa laitteen ehtona toimii laite ylhäällä.

Laitteelle määritetään ajankohdat milloin laitetta valvotaan. Hälytyksiä voidaan Solarwinds Orion NPM:ssä määrittää tietyille ajankohdille päivän ja kellonajan tarkkuudella. Esimerkiksi, jos laite on vain arkipäivisin käytössä voidaan poistaa valvonnasta viikonloppu. Metrolan-verkon laitteistoa valvotaan jatkuvasti, joten määritykset valitaan joka päivälle kellon ympäri.

Hälytyksille tulee määrittää toiminnot mitä tapahtuu, kun hälytys laukeaa. Toimintoja ovat muun muassa lähetä sähköposti valituille käyttäjille, luo lokitiedosto määritettyyn kansioon, lähetä tekstiviesti valituille käyttäjille, suorita toiminto/ohjelma, sammuta laite, lähetä syslog viesti tai suorita skripta. Toimintoja on laajasti erilaisia ja niillä pystytään reagoimaan automaattisesti ilman ylläpidon tekemää manuaalista toimenpidettä.



Kuvio 19: Hälytyksen määritykset (HKL Sisäinen materiaali)

Metrolan-verkon laitteistosta halutaan saada sähköposti kohdennetuille käyttäjille, joka tapahtuu käyttämällä toimintoa lähetä sähköposti. Sähköpostin lähetys toiminto vaatii toiminnon asetuksissa määrittämään osoitteet, johon sähköposti lähetetään, viesti, jossa kerrotaan hälytyksen tiedot, palvelimen tiedot, jotta sähköposti saadaan lähetettyä, ajankohdat milloin sähköposti lähetetään ja toiminnon eskaloituminen. Eskaloitumis kohdassa on tärkeää määrittää etenkin sellaisten laitteiden kohdalla, jotka saatavat sammua sähkökatkoksen tai manuaalisen uudelleenkäynnistämisen kohdalla niin, että hälytyksen aikana toiminto suoritetaan esimerkiksi vain seitsemän päivän välein. Muutoin esimerkiksi, jos laitetta tiedostutusti käynnistetään uudelleen useita kertoja kohdennetut käyttäjät saisivat jatkuvasti turhaa sähköpostia hälytyksestä.

6 Yhteenveto ja johtopäätökset

Opinäytetyössä oli tarkoituksena ja tavoitteena kehittää yrityksen verkonvalvonnan hälytyksiä. Yrityksen verkonvalvonnassa on laaja määrä erilaisia tietoliikennelaitteita, joista yhdessä toimeksiantajan kanssa pohdittiin, mitkä laitteet ovat sellaisia, jotka vaativat reealiajassa saatavan hälytystiedon.

Laitteet, jotka määritettiin antamaan hälytystiedot, ovat radan varrella olevat tukiasemat, kytkimet ja kaksi palvelinta. Verkonvalvontaohjelmistossa suoritettiin muutoksia, jotta kyseisistä laitteista saadaan jatkossa sähköpostiviesti, kun laite menee alas ja nousee takaisin ylös. Tämä helpottaa laitteiden valvontaa, kun jatkossa mahdollisista ongelmista saadaan sähköpostin avulla tieto. Tieto lähtee kohdennetuille käyttäjille, joita voidaan lisätä tai poistaa jatkossa ohjelmiston kautta.

Empiirisen tutkimuksen, jossa tutkittiin verkonvalvontaohjelmistoa, aikana löytyi myös paljon kohtia, joita tulevaisuudessa olisi hyvä pohtia. Verkonvalvonnassa on lukuisia laitteita, joiden toiminta riippuu siitä, onko metrovaunu päällä. Jos metrovaunu esimerkiksi otetaan huoltoon, se sammutetaan ja tämän mukana laitteet myös sammuvat. Tästä aiheutuu verkonvalvonnassa kyseisistä laitteista hälytys. Tulevaisuudessa olisi hyvä pohtia, onko tällaisille laitteille mahdollista määrittää hälytys, joka laukeaa vain, kun sille on oikea syy. Kasvavan laitemäärän vuoksi verkko rasittuu entistä enemmän ja tämän kaltaisille ongelmille olisi hyvä etsiä ratkaisu, jotta verkon toimintaa saadaan kevennettyä.

Tutkimuksen validiteetti on luotettava ja pätevä, koska käytetyllä tutkimusmenetelmällä saavutettiin oikeat vastaukset kysymyksiin. Tutkimuksen reliabiliteetti on reliaabeli. Tehtyjen mittausten jälkeen vastaukset olivat aina samanlaisia ja mistään toistettavasta mittauksesta ei esiintynyt sattumanvaraisuutta.

Tutkittaessa verkonvalvontaohjelmiston toimintaa, josta löytyi tieto, miten verkonvalvontaohjelmisto merkitsee laitteen alas-tilaan, kun se ei saa vastausta pyyntöihinsä. Ohjelmisto pyytää laitteelta sen tilaa ja jos se ei saa ensimmäiseen pyyntöön vastausta ohjelmisto aloittaa fast polling-menetelmän, jossa se kysyy määritetyn ajan laitteelta vastausta kymmenen sekunnin välein. Jos laitteita menee esimerkiksi sähkökatkoksen vuoksi suuri määrä alas-tilaan tämä aiheuttaa verkonvalvonnassa mahdollisesti suuren piikin verkonkäytössä. Tämä saattaa hidastaa verkkoa ja verkon luotettavuus saattaa kärsiä. Tulevaisuudessa olisi hyvä miettiä, miten verkonvalvontaohjelmisto määrittää erilaiset laitteet alas tilaan, jottei mahdollisia verkonkäyttö piikkejä syntyisi.

Kun verkonvalvontaohjelmisto on saatu kokonaan määritettyä mahdollisimman kevyeksi ja esimerkiksi hälytykset ovat kaikkien laitteiden osalta määritetty mahdollisimman järkevästi, saadaan verkon rasitusta laskettua ja ylläpitäjien on helpompi reagoida ja hallita verkon laitteistoa. Laitteiston määrä kasvaa tulevaisuudessa lisää ja siinä vaiheessa hyvin määritetty verkonvalvonta helpottaa uusien laitteiden käyttöönottoa.

Lähteet

DMTF. 2017. Common Information Model. Viitattu 4.3.2017
http://www.dmtf.org/standards/cim

DMTF. 2017. Web-Based Enterprise Management (WBEM) FAQs. Viitattu 4.3.2017
https://www.dmtf.org/about/faq/wbem_faq

Haikonen, J. 2000. Johdanto. Viitattu 18.3.2017
https://www.netlab.tkk.fi/opetus/s38118/s00/tyot/47/

Hautaniemi, M. 1994. Toiminnallinen opinnäytetyö. Viitattu 11.3.2017
http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhall_toteutus.html

HKL. 2017. Tämä on HKL. Viitattu 2.3.2017
http://www.hel.fi/www/hkl/fi/tama-on-hkl/organisaatio/

Jyväskylän Yliopisto. 2015. Empiirinen tutkimus. Viitattu 17.4.2017
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

LUTEUS SARL. 2004. Introduction to RMON – Remote Monitoring GUI. Viitattu 5.3.2017
http://www.loriotpro.com/Products/RMON_GUI/RMON_GUI_Documentation.htm

Microsoft. 2017. About WMI. Viitattu 25.2.2017
https://msdn.microsoft.com/en-us/library/aa384642(v=vs.85).aspx

Microsoft. 2017. Using WMI. Viitattu 25.2.2017
https://msdn.microsoft.com/en-us/library/aa393964(v=vs.85).aspx

Microsoft. 2017. Windows Management Instrumentation. Viitattu 25.2.2017
https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx

NINO. 2009. About NINO. Viitattu 19.3.2017
http://nino.sourceforge.net/nino/index.html

Parsons, T. 2014. What is Syslog? Viitattu 19.3.2017
https://blog.logentries.com/2014/08/what-is-syslog/

Postel, J. 1981. Internet Control Message Protocol. Viitattu 26.2.2017
https://tools.ietf.org/html/rfc792

Schmidt, K. & Mauro, D. 2008. Essential SNMP. 2. painos.

Solarwinds. Available alert actions. Viitattu 4.3.2017
http://www.solarwinds.com/documentation/en/flarehelp/ncm/content/core-available-alert-actions-sw1076.htm

Sportack, M. 2005. The ABCs of TCP/IP. Viitattu 24.2.2017.
http://www.ciscopress.com/articles/article.asp?p=377101

Tampere University of Technology. 2002. Tietotekniikan peruskurssi. Viitattu 18.2.2017
http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html

Zoho Corp. 2017. What is SNMP?. Viitattu 26.2.207
https://www.manageengine.com/network-monitoring/what-is-snmp.html

Kuviot

Kuvio 1: HKL Organisaatiokaavio (HKL 2017) 9
Kuvio 2: Verkonhallinta jaettuna valvontaan ja hallintaan. (Hautaniemi 1994) 11
Kuvio 3: Havainne kuva SNMP:n kommunikaatiosta (Zoho Corp 2017) 14
Kuvio 4: Havainnekuva managerin ja agentin välisestä yhteydestä (Schimidt & Mauro. 2008, 22) 15
Kuvio 5: Getbulk-operaation pyyntö sekvenssi (Schimidt & Mauro. 2008, 72) 16
Kuvio 6: SNMPv3:n Entiteetti (Schimidt & Mauro. 2008, 94) 18
Kuvio 7: Havainne kuva SMI objektipuusta (Schimidt & Mauro. 2008, 42) 19
Kuvio 8: Havainne kuva SMIv2 rekisteröinnistä SNPv2:seen (Schimidt & Mauro. 2008, 51) 20
Kuvio 9: Havainnekuva MIB-II alipuusta (Schimidt & Mauro. 2008, 54) 21
Kuvio 10: Osi-malli (Tampere University of Technology 2002) 23
Kuvio 11: Havainne kuva RMON valvonnasta OSI-mallissa (LUTEUS SARL 2004) 24
Kuvio 12: Nagios-yleisnäkymä palveluiden tilasta (Nagios) 26
Kuvio 13: Nino tapahtumanäkymä (Nino) 27
Kuvio 14: Solarwinds Orion NPM:n etusivu (HKL Sisäinen materiaali) 28
Kuvio 15: Kyselyjärjestelmän asetusnäkymä (HKL Sisäinen materiaali) 28
Kuvio 16: Tapahtumien yleisnäkymä (HKL Sisäinen materiaali) 29
Kuvio 17: Esimerkki tukiasemien liikennemäärästä kuukauden otannalla (HKL Sisäinen materiaali) 30
Kuvio 18: Solarwinds Orion NPM Alert manager (HKL Sisäinen materiaali) 31
Kuvio 19: Hälytyksen määritykset (HKL Sisäinen materiaali) 32
Kuvio 20: Aloitusnäkymä (HKL Sisäinen materiaali) 38
Kuvio 21: Hälytystenhallinta (HKL Sisäinen materiaali) 38
Kuvio 22: Uuden hälytyksen määrittäminen (HKL Sisäinen materiaali) 39
Kuvio 23: Hälytyksen laukeaminen määritetty, kun laitteen tila menee alas. (HKL Sisäinen materiaali) 39
Kuvio 24: Hälytyksen purkaus määritetty, kun laitteen tila menee ylös. (HKL Sisäinen materiaali) 40
Kuvio 25: Alert Suppression (HKL Sisäinen materiaali) 40
Kuvio 26: Time of day (HKL Sisäinen materiaali) 41
Kuvio 27: Trigger actions (HKL Sisäinen materiaali) 41
Kuvio 28: Send an E-Mail / Page toiminto (HKL Sisäinen materiaali) 42
Kuvio 29: Email/page action (HKL Sisäinen materiaali) 42
Kuvio 30: E-Mail/Page action message (HKL Sisäinen materiaali) 43
Kuvio 31: SMTP Server (HKL Sisäinen materiaali) 43
Kuvio 32: Time of Day (HKL Sisäinen materiaali) 44
Kuvio 33: Alert Escalation (HKL Sisäinen materiaali) 44

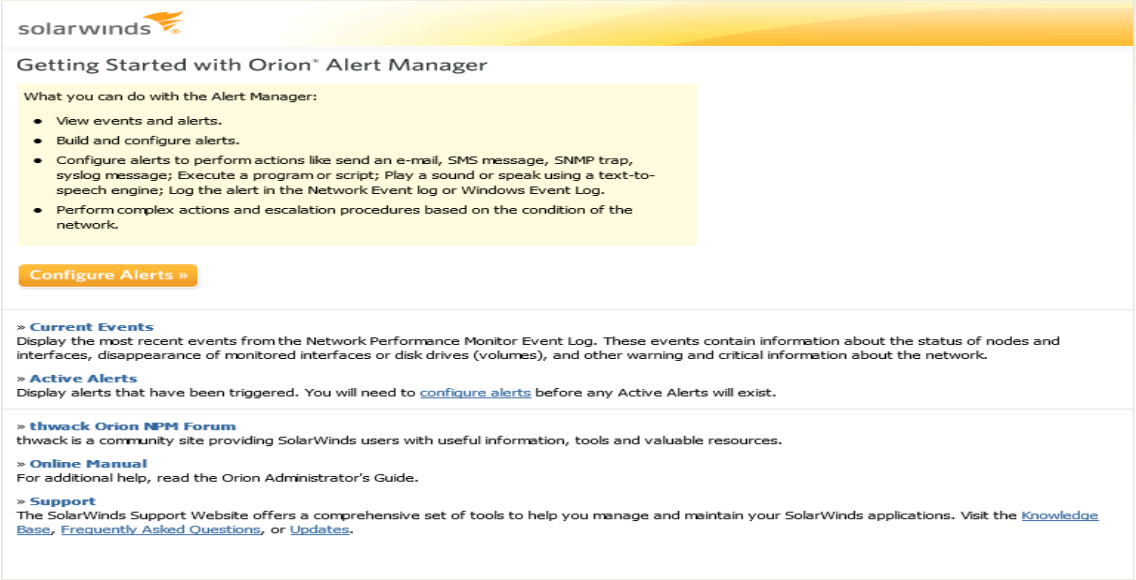
Liitteet

Liite 1: Käyttöopas hälytyksen luomiseen Solarwinds Orion NPM ohjelmistolla 38

Liite 1: Käyttöopas hälytyksen luomiselle Solarwinds Orion NPM:llä

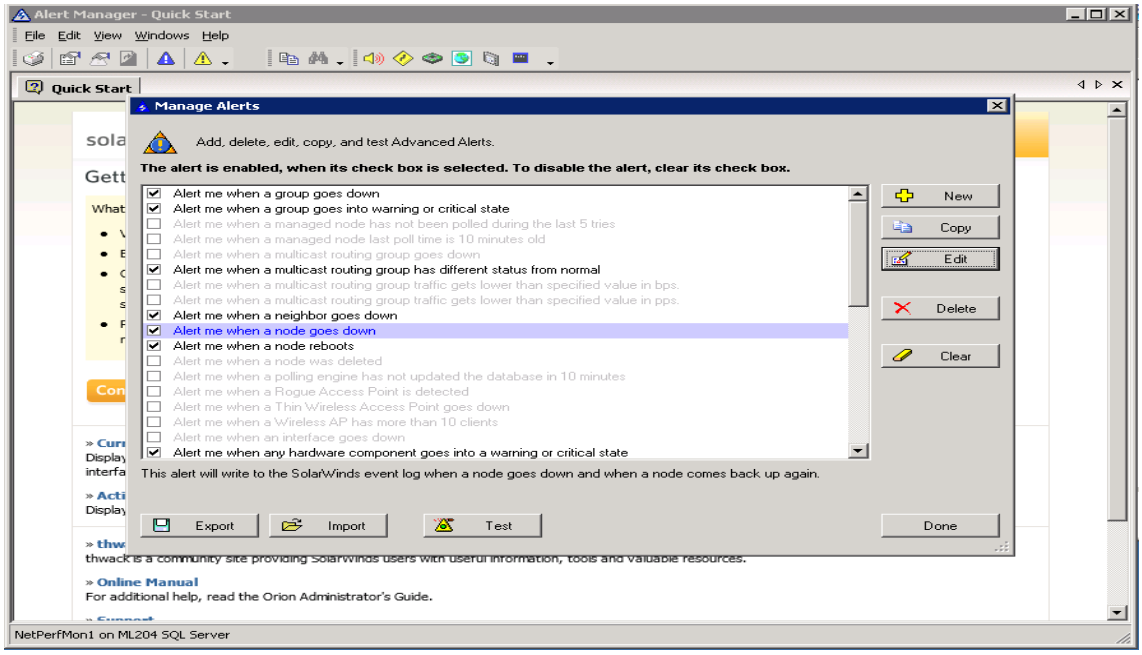
Uuden hälytyksen voi luoda vain Solarwinds Orion NPM-hallintatietokoneella. Tunnukset hallintatietokoneelle voi pyytää verkon ylläpidolta. Hälytyksen luonti käydään vaiheittain läpi ja hälytyksen luomista havainnoidaan screenshottien avulla.

Avaa Solarwinds Orion NPM Advanced Alert Manager käynnistä -valikosta



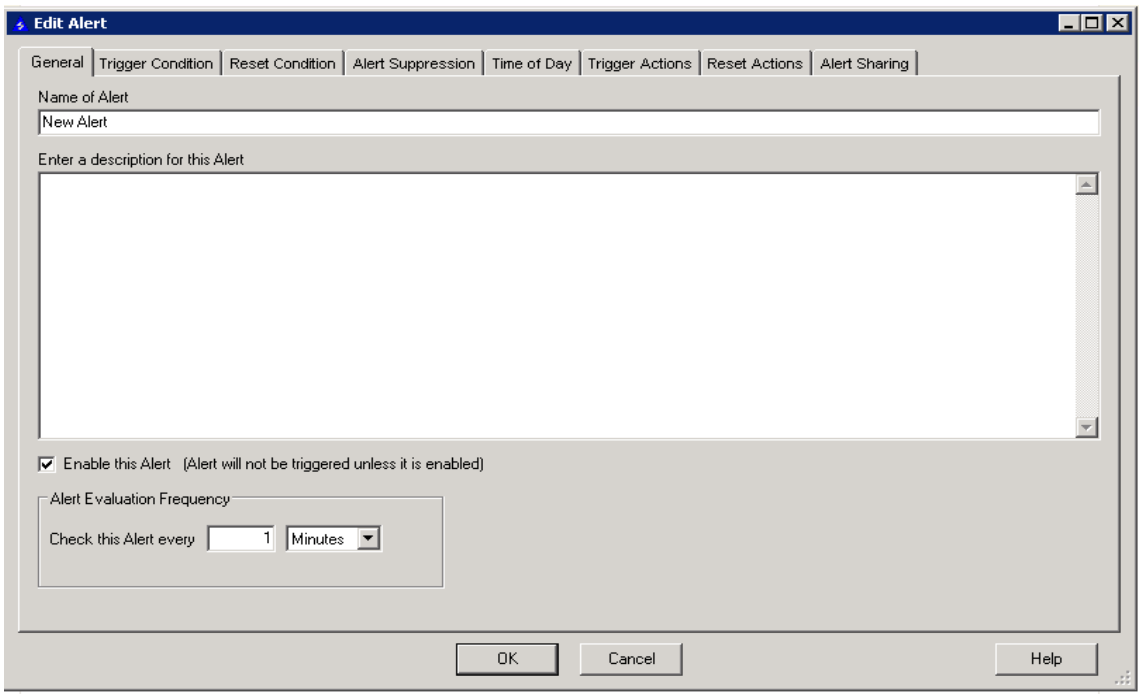
Kuvio 20: Aloitusnäkymä (HKL Sisäinen materiaali)

Klikkaa kohtaa Configure Alerts



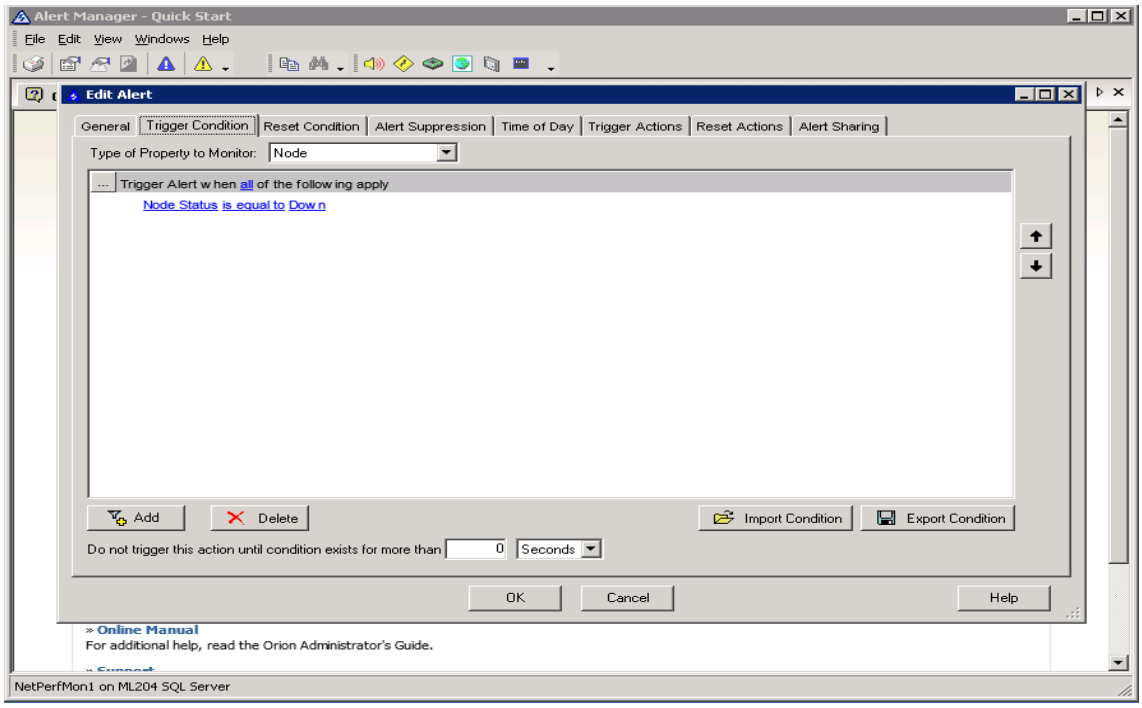
Kuvio 21: Hälytystenhallinta (HKL Sisäinen materiaali)

Klikkaa kohtaa New, jossa pääset määrittelemään uuden hälytyksen määritykset. Name of Alert-kohdassa annetaan uudelle hälytykselle nimi. Nimen tulee olla selkeä ja lyhyt, jotta se on helposti ymmärrettävissä. Enter a description for this Alert-kohdassa kuvataan hälytys.



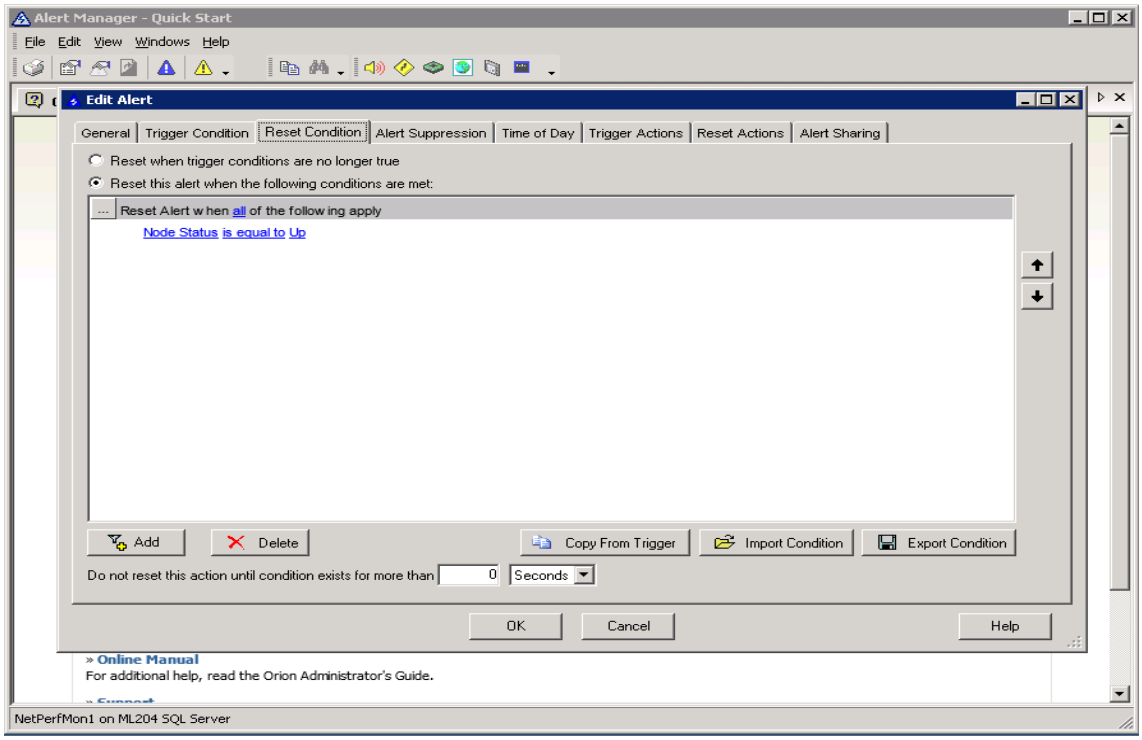
Kuvio 22: Uuden hälytyksen määrittäminen (HKL Sisäinen materiaali)

Trigger Condition-kohdassa määritetään ehto, josta hälytys laukeaa. Hälytyksen voi määrittää laukeamaan esimerkiksi, kun laite menee alas tai käynnistyy uudelleen.



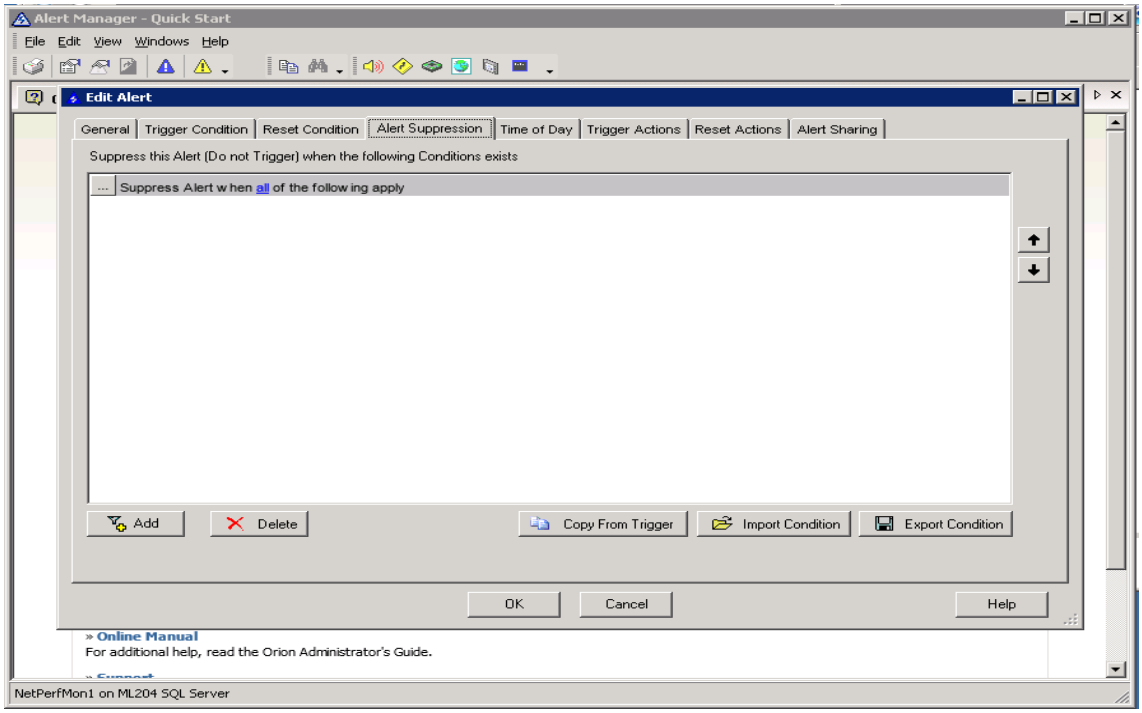
Kuvio 23: Hälytyksen laukeaminen määritetty, kun laitteen tila menee alas. (HKL Sisäinen materiaali)

Reset condition-kohdassa määritetään ehto hälytyksen purkautumiselle.



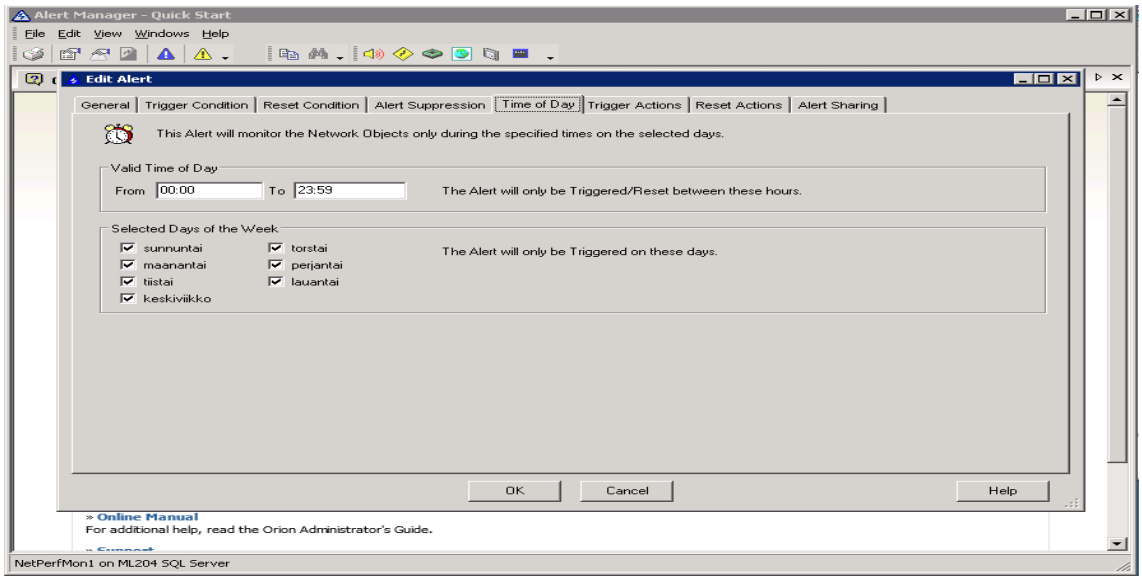
Kuvio 24: Hälytyksen purkaus määritetty, kun laitteen tila menee ylös. (HKL Sisäinen materiaali)

Alert Suppressiossa voidaan määrittää ehtoja, jos halutaan, etteivät hälytykset laukea, kun määritetyt ehdot täyttyvät. Ehto voi olla esimerkiksi, kun laitetta ohjaavan reitittimen tila on mennyt alas.



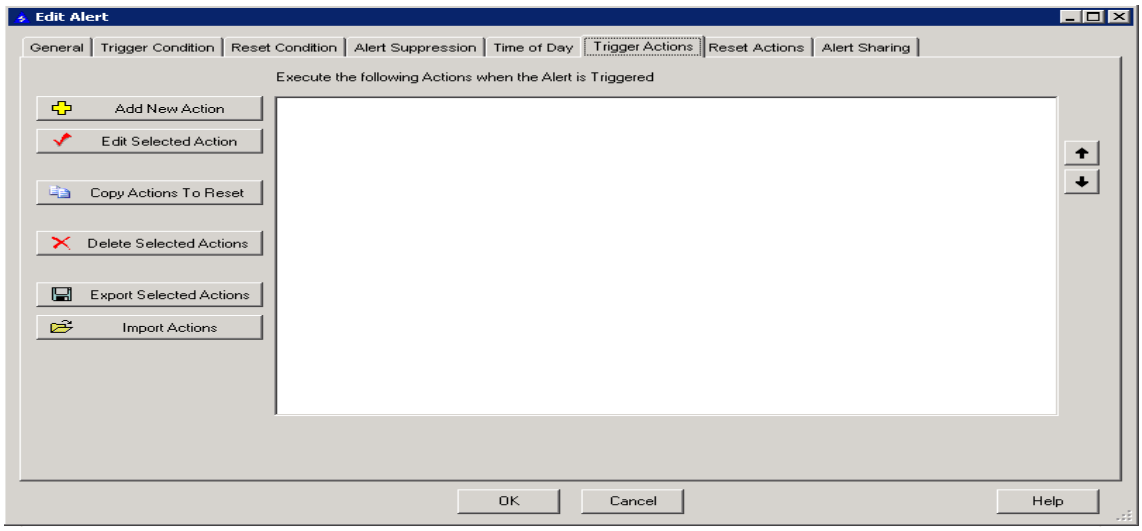
Kuvio 25: Alert Suppression (HKL Sisäinen materiaali)

Hälytyksen valvonnalle täytyy määrittää ajankohdat. Jos hälytys asetetaan esimerkiksi laitteille, joiden halutaan olevan jatkuvassa valvonnassa, asetetaan Valid Time of Day-kohtaan From 00:00 to 23:59 ja Selected Days of the Week, jokaisen päivän täppä valituksi.



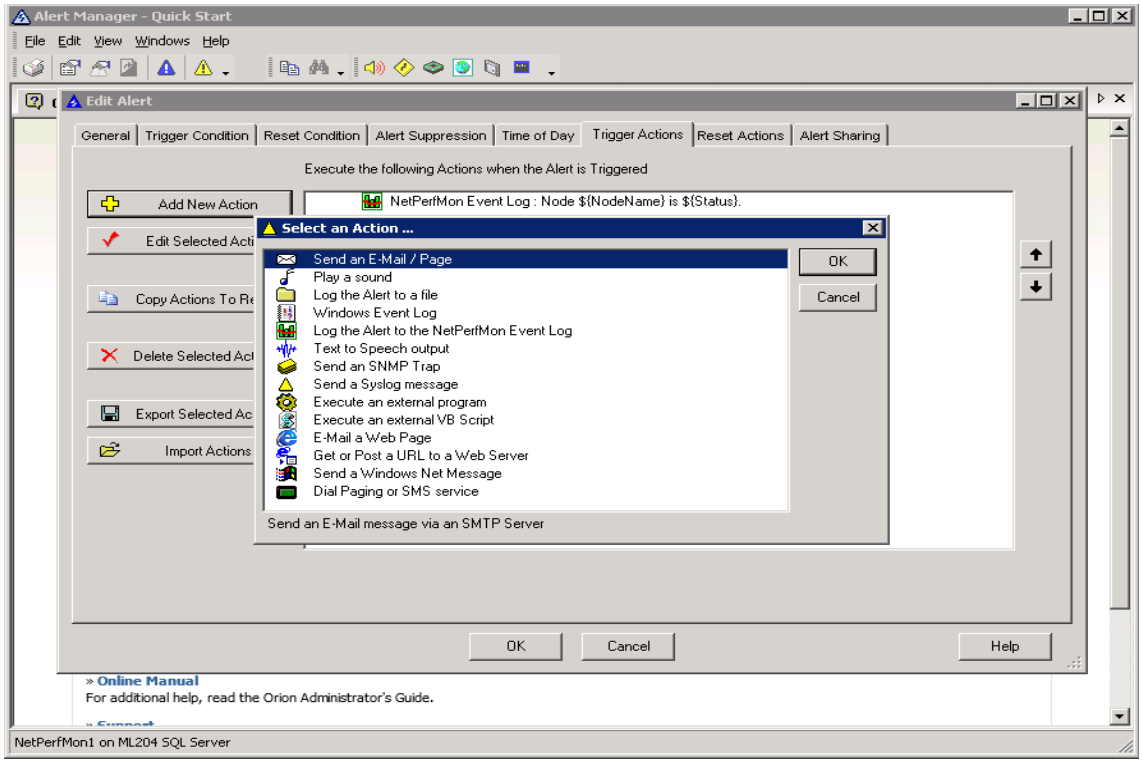
Kuvio 26: Time of day (HKL Sisäinen materiaali)

Hälytykselle määritetään toiminnot, jotka tapahtuvat hälytyksen lauetessa. Toiminnot voivat olla esimerkiksi sähköpostin lähetys tai sms-viestin lähetys valituille käyttäjille. Klikkaamalla kohtaa Add New Action voi lisätä toimintoja hälytykselle. Kohdasta Copy Actions to Reset voit kopioida tekemäsi toiminnot hälytyksen purkautumisen toimintoihin. Esimerkiksi, kun hälytys laukeaa, tapahtuu toiminto, jossa sähköposti lähtee käyttäjälle ja antaa tiedon laitteen mentyä alas ja kun laite nousee takaisin ylös käyttäjä saa tästä myös sähköpostin. Seuraavasta linkistä voit tutustua lisää Solarwinds Orion NPM hälytys toimintoihin http://www.solarwinds.com/documentation/en/flarehelp/sam/content/core-available-alert-actions-sw1076.htm



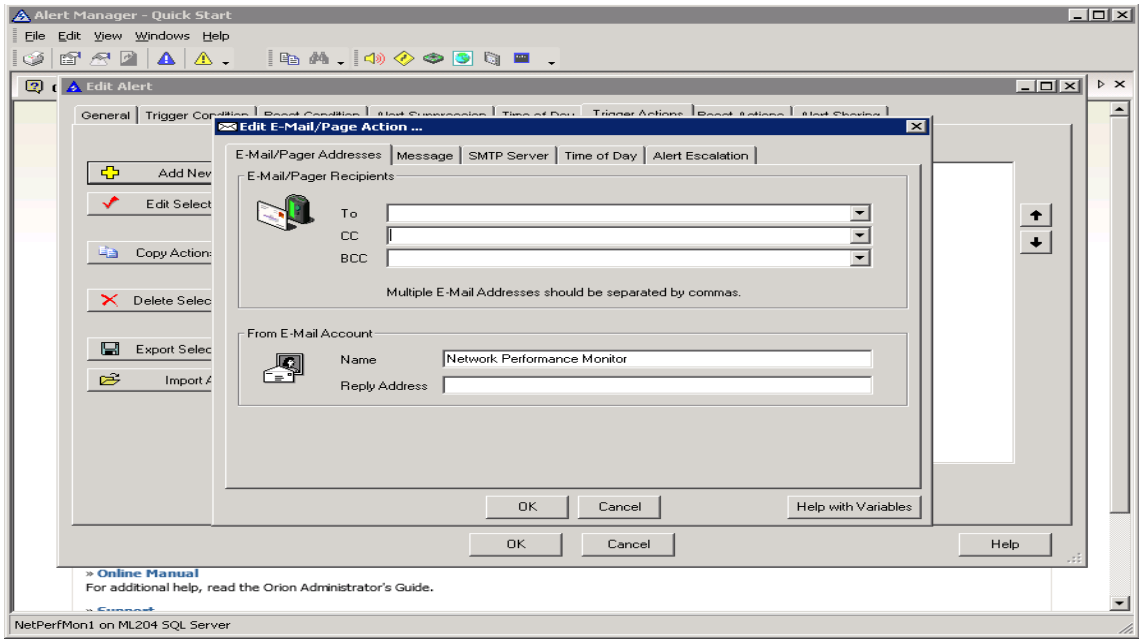
Kuvio 27: Trigger actions (HKL Sisäinen materiaali)

Hälytystieto sähköpostitse käyttäjille -toiminto vaatii tietoja, jotka saa tarvittaessa verkon ylläpidolta. Add New Action-kohdan jälkeen valitaan seuraavasta aukeavasta ikkunasta kohta Send and E-email / Page ja valitaan kohta ok.



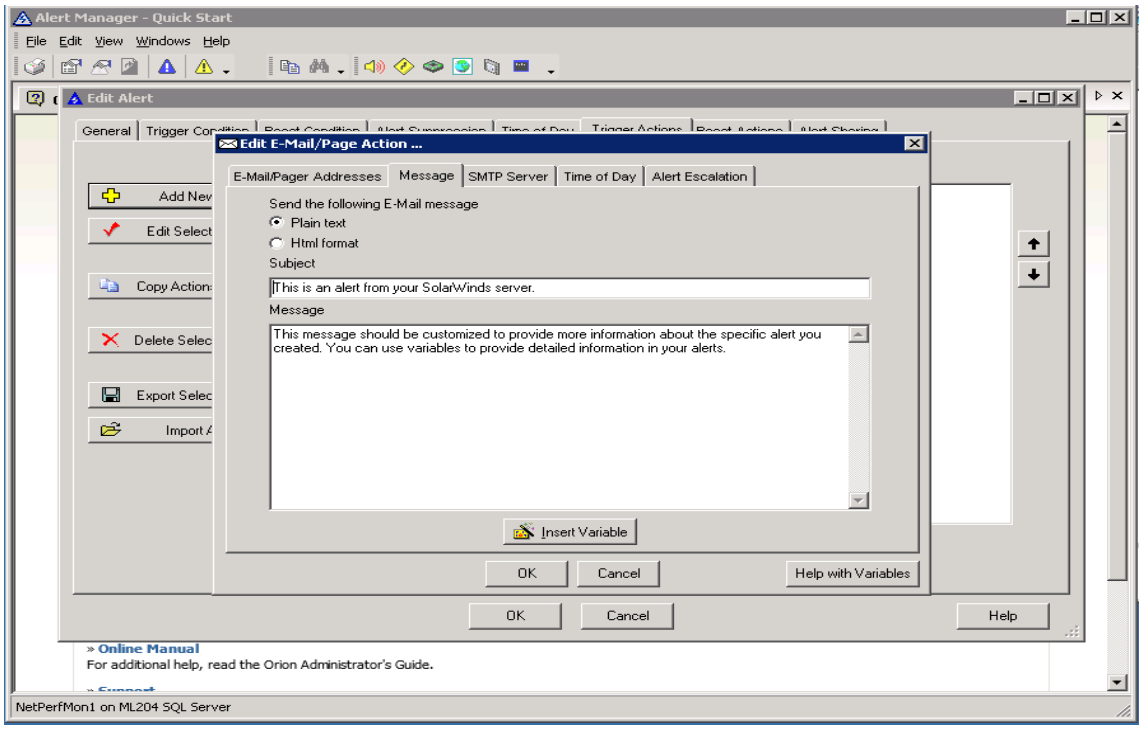
Kuvio 28: Send an E-Mail / Page toiminto (HKL Sisäinen materiaali)

E-Mail/Page Recipients to-kohdassa määritetään kenelle hälytystieto lähetetään.



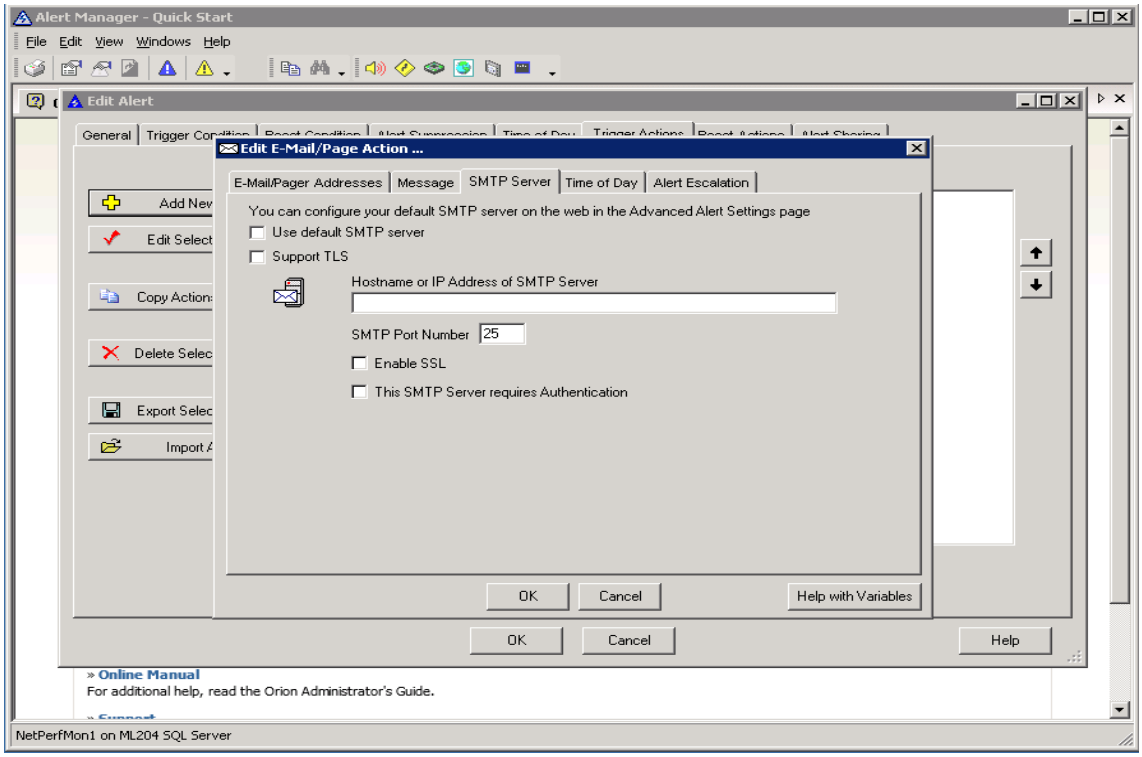
Kuvio 29: Email/page action (HKL Sisäinen materiaali)

Message kohdassa otsikoidaan hälytystieto ja viesti, jossa voi kertoa vapaasti hälytyksen tiedot.



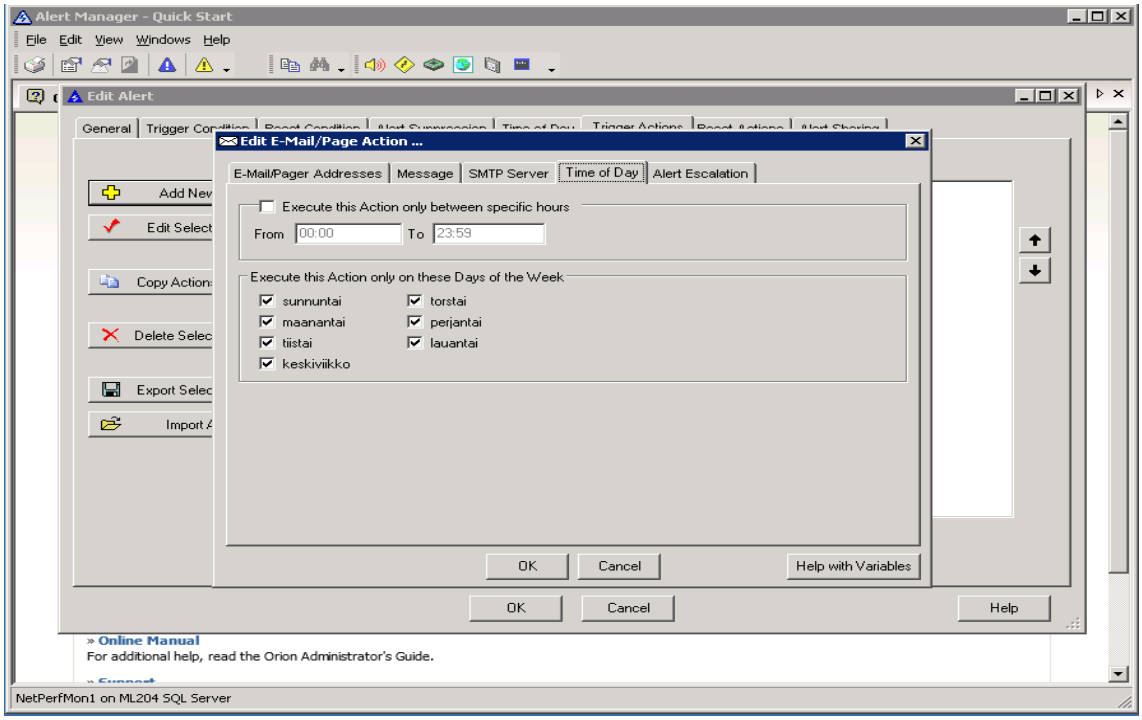
Kuvio 30: E-Mail/Page action message (HKL Sisäinen materiaali)

SMTP Server-alalehden kohtaan Hostname Or IP Address of SMTP Server määritetään SMTP Serveri, joka välittää sähköpostit käyttäjille. Osoitteen saa verkon ylläpitäjältä.



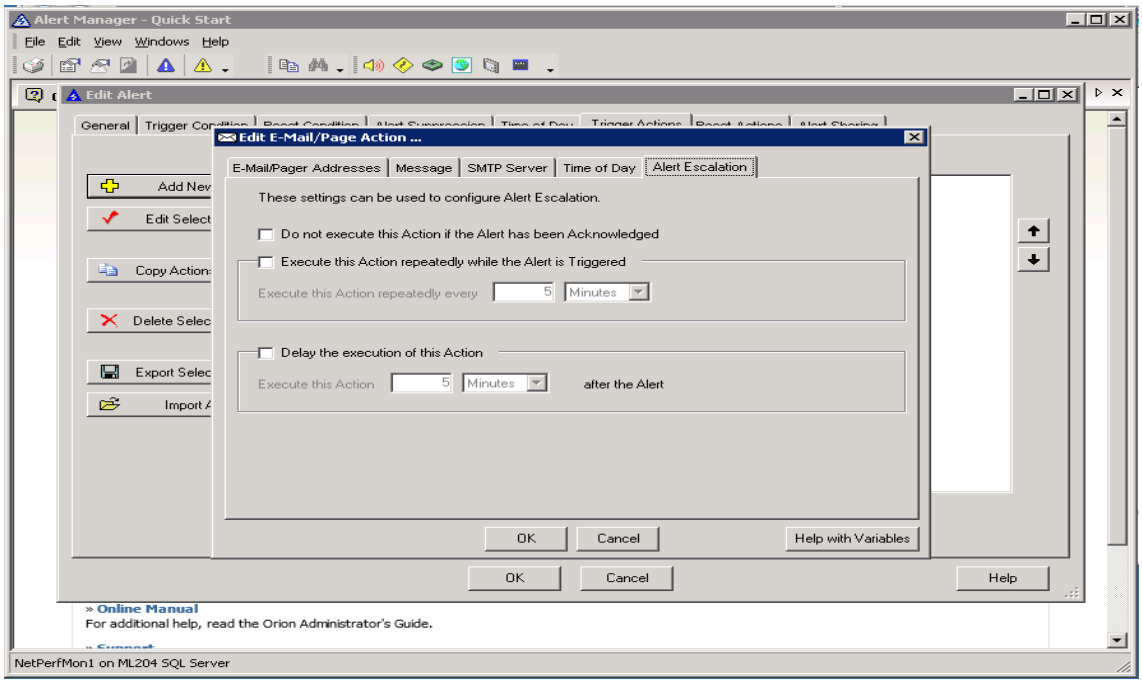
Kuvio 31: SMTP Server (HKL Sisäinen materiaali)

Time of Day-kohdassa määritetään ajat milloin hälytystieto lähetetään sähköpostitse.



Kuvio 32: Time of Day (HKL Sisäinen materiaali)

Alert Escalation-kohdassa voi määrittää sen, jos haluaa hälytyksen toiminnon vain kerran viikossa. Valitsemalla täpän Execute this Action repeatedly while the Alert is Triggered voi muokata kohtaa Execute this Action repeatedly every, johon määritetään 7 Days. Nyt toiminto lähettää käyttäjälle vain kerran viikossa hälytystiedon sähköpostiin.



Kuvio 33: Alert Escalation (HKL Sisäinen materiaali)