KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Mirko Talka

VERKONVALVONTA KYMENLAAKSON AMMATTIKORKEAKOULUSSA

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

TALKA, MIRKO	Verkonvalvonta Kymenlaakson ammattikorkeakoulussa
Opinnäytetyö	50 sivua
Työn ohjaaja	lehtori Jouko Pahlama
Toimeksiantaja	KyAMK Tietohallinto
Maaliskuu 2011	
Avainsanat	verkonhallinta, verkonhallintasovellukset, verkonvalvonta, SNMP, tietoliikenne

Tietoverkot ovat nykypäivänä yritysten toiminnan kannalta erittäin tärkeitä resursseja. Siksi niiden toimivuuden ylläpitämiseen käytetään verkonvalvontaa. Verkonvalvonnan perusajatuksena on verkon palvelujen toimivuuden seuranta, vikojen etsintä sekä toimintojen kehittäminen esimerkiksi verkon liikennemääriä seuraamalla.
Tämän opinnäytetyön tarkoituksena oli selvittää Kymenlaakson ammattikorkeakoulun tietoverkkojen ja niiden valvonnan nykytilanne. Lisäksi tavoitteena oli vertailla kolmea eri valvontasovellusta, joista organisaation vaatimuksiin parhaiten soveltuva valitaan tuotantokäyttöön valvomaan verkon aktiivilaitteita, palvelimia ja palveluja. Lisäksi dokumentissa kuvataan ICT-laboratorioon asennettavan Zabbix-verkonvalvontasovelluksen käyttöönoton valmisteluvaihetta.

Työn teoriaosassa tarkastellaan yleisesti verkonhallintaa, sen vaatimuksia ja osa-alueita. Verkonhallinnan osa-alueet ovat vikojen hallinta, käytön hallinta, suorituskyvyn hallinta, kokoonpanon hallinta ja turvallisuuden hallinta. Tämän lisäksi teoriaosuudessa käsitellään verkonhallinnan yleisimmän protokollan SNMP:n (Simple Network Monitoring Protocol) sekä sen käyttämän MIB-tietokannan toimintaa.

Opinnäytetyössä suoritetun vertailun perusteella hankittavaksi valvontasovellukseksi suositellaan NetEye-tuoteperhettä, koska se on ominaisuuksiltaan ja kustannuksiltaan soveltuvin ratkaisu Kymenlaakson ammattikorkeakoulun tietoverkon valvontaan.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

TALKA, MIRKO	Network Monitoring in Kymenlaakso University of Applied Sciences
Bachelor's Thesis	50 pages
Supervisor	Jouko Pahlama, Senior Lecturer
Commissioned by	KyAMK Information Management
March 2011	
Keywords	network management, network management applications, network monitoring, SNMP, telecommunications

Information networks are important resources in modern-day businesses. That is why many organizations are using network monitoring to maintain the functionality of their networks. The basic idea of network monitoring is to monitor the performance of the services and to develop the operations in the network.

The purpose of this thesis work was to clarify the present situation of information networks and their monitoring in Kymenlaakso University of Applied Sciences. Another objective was to compare different monitoring software. The most appropriate solution would be selected for production use to monitor network devices, servers and services in Kymenlaakso University of Applied Sciences. Added to this, the document describes the introduction of the preparatory phase of the installation of the Zabbix network monitoring software, which will later be implemented in Metsola's ICT laboratory.

The theoretical section deals with network management in general and covers its requirements and the areas of function. The five areas of function are fault management, configuration management, accounting management, performance management and security management. In addition, the theoretical part discusses SNMP, the most common protocol used in network monitoring, and MIB, the management database of SNMP.

Based on the survey, NetEye was the most appropriate network monitoring software for Kymenlaakso University of Applied Sciences because of its features and costs.

SISÄLLYS

DES	Data Encryption Standard, tietotekninen salausalgoritmi
EGP	Exterior Gateway Protocol, Internetin reititysprotokolla
FDDI	Fiber Distributed Data Interface, optisiin siirtoyhteyksiin perustuva verkko, jonka perinteinen nopeus on 100Mb/s ja jonka siirtotienä toimii valokuitu
DHCP	Dynamic Host Configuration Protocol, IP-osoitteiden jakamiseen tarkoitettu verkkoprotokolla
DNS	Dynamic Name Server, nimipalvelujärjestelmä, joka muuntaa verkkotunnuket IP-osoitteiksi
HTTPS	Hypertext Transfer Protocol Secure, HTTP-protokollan suojattu versio
ICMP	Internet Control Message Protocol, kontrolliprotokolla, jolla lähetetään nopeasti viestejä koneesta toiseen
ICT	Information and Communication Technology, tieto- ja viestintäteknologia
IOS	Internetwork Operating System, Cisco-reitittimien ja -kytkimien käyttämä ohjelmisto
IP	Internet Protocol, TCP/IP-mallin protokolla, joka toimittaa pakettikytkentäisen verkon tietoliikennepaketit perille
ITU-T	The telecommunication standardisation sector of International Telecommunication Union, kansainvälisen televiestintäliiton televiestintäsektori, jonka päätehtäviä ovat mm. standardisointi
LDAP	Lightweight Directory Access Protocol, hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla, jonka pääasiallinen tehtävä on autentikointi

MD5	Message-Digest algorithm 5, salsanojen suojaamiseen tarkoitettu algoritmi
MIB	Management Information Base, verkon hallinnassa käytettävä virtuaalinen tietokanta
NMS	Network Management System, laitteistojen ja ohjelmistojen yhdistelmä, jolla hallitaan verkkoja
OID	Object Identifier, yksilöintitunnus, joka on kohteeseen liitettävä numerosarja
OSI	Open Systems Interconnection, malli, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
RFC	Request for Comments, Internetiä koskevia standardeja
RMON	Remote Network Monitoring, liikennepohjaisen tietoliikenteen tarkastelutekniikka
RPM	RPM Package Manager, alun perin RedHat Package Manager, paketinhallintaohjelma, joka hoitaa asennuksen käyttäjän puolesta ja asentaa tiedostot oikeille paikoilleen
SFTP	SSH File Transfer Protocol, protokolla, joka mahdollistaa tiedostojen käsittelyn SSH-protokollan yli
SGMP	Simple Gateway Monitoring Protocol, tietoverkkojen hallintaan käytettävä protokolla, SNMP:n edeltäjä
SHA1	Secure Hash Algorithm 1, salauksissa käytettävä kryptografinen tiivistefunktio
SMI	Structure of Management Information, määrittely, joka määrittää SNMP:n tietokannan objektit

SMTP	Simple Mail Transfer Protocol, sähköpostipalvelimien käyttämä TCP-pohjainen viestinvälitysprotokolla
SNMP	Simple Network Monitoring Protocol, tietoverkkojen hallintaan käytettävä protokolla
SSH	Secure Shell, ohjelmisto, jolla voidaan ottaa salattuja etäyhteyksiä järjestelmästä toiseen
TCP	Transmission Control Protocol, yhteyksien luomiseen tarkoitettu tietoliikenneprotokolla
TCP/IP	Transmission Control Protocol / Internet Protocol, usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä
UDP	User Datagram Protocol, yhteydetön tiedostonsiirtoprotokolla
VLAN	Virtual Local Area Network, virtuaalilähiverkko
VoIP	Voice Over Internet Protocol, tekniikka jonka avulla voidaan siirtää ääntä reaaliaikaisesti IP-protokollan välityksellä
VPN	Virtual Private Network, virtuaalinen yksityinen verkko
WLAN	Wireless Local Area Network, langaton lähiverkkotekniikka

1 JOHDANTO

Nykypäivän yritysmaailmassa tietoverkot ovat nousseet erittäin tärkeiksi resursseiksi, koska yhä enenevässä määrin organisaatioiden toiminnot siirtyvät toimimaan tietoverkkojen välityksellä. Näin ollen informaatio tukeutuu yhä enemmän tietoliikenteeseen ja informaatioteknologiaan sekä sen tarjoamiin sovelluksiin.

Verkkojen kasvaessa ja laitteiden lisääntyessä topologiat monimutkaistuvat ja verkkojen hallinta vaikeutuu. Tällöin on löydettävä paras mahdollinen keino tietoverkkojen toimivuuden ylläpitämiseksi. Tätä varten on kehitetty erilaisia hallintatyökaluja, jotka monitoroivat verkon laitteiden sekä palvelujen tilaa ja joiden avulla verkkoja pyritään pitämään jatkuvasti toimintakunnossa. Valvontasovellukset eivät pelkästään selkeytä verkonvalvontaa sekä -hallintaa vaan helpottavat ja tehostavat myös ylläpitoa ja ylläpitäjien työtä. Verkonvalvontasovellusten perusajatuksena on vikojen etsintä sekä toimintojen kehittäminen, mutta mahdollisten verkon väärinkäyttötapauksien estämiseksi nykysovellukset pystyvät seuraamaan myös käyttäjien verkonkäyttöä.

Opinnäytetyön tarkoituksena on toimia Kymenlaakson ammattikorkeakoulun (KyAMK) verkonvalvonnan suunnittelupohjana. Tämä koostuu KyAMK:n valvontaympäristön kartoituksesta, tarjolla olevien valvontasovellusten vertailusta sekä käytettävän sovelluksen valinnasta. Sovelluksen varsinainen käyttöönotto tullaan toteuttamaan tätä työtä apuna käyttäen.

Verkonhallinnan sekä -valvonnan ymmärtämiseksi työn teoriaosuudessa käsitellään pääpiirteittäin verkonhallinnan periaatteita sekä yleisimmän valvontasovellusten käyttämän protokollan SNMP:n toimintaa.

2 VERKONHALLINTA

Verkonhallinta on tärkeä osa nykypäivän yritysmaailmaa, sillä useimmat yritysten palvelut tukeutuvat tietoverkkoihin toimimalla niiden kautta. Tietoverkoissa kuljetetaan lisäksi yrityksen kannalta tärkeää informaatiota (esim. myynti, hankinta, tuotanto, logistiikka ja hallinto). (1:305)

Yritysten tietojärjestelmät koostuvat useimmiten tietoliikenteellä yhdistetyistä laitteista, jonka ytimenä toimii tietoverkko. Toimiva verkko vaatii valvontaa ja verkonhallinnan tarkoituksena onkin saada verkko sekä sen palvelut toimimaan luotettavasti ja eheästi. Verkonhallinnalla pyritään ennalta ehkäisemään verkon ongelmia sekä korjaamaan syntyneitä vikoja tehokkaasti ja turvaamaan verkon kautta käytettävien palveluiden saatavuus. (2:277)

Tietoverkkojen ylläpito ilman asianmukaista hallintatyökalua on suuremmissa kokonaisuuksissa hankalaa, sillä verkon eri osa-alueet voivat sijaita maantieteellisesti täysin eri paikoissa. Hyvänä esimerkkinä toimii Kymenlaakson ammattikorkeakoulu, jonka toimipisteitä sijaitsee ympäri Kymenlaaksoa (Metsola, Jylppy, Kuusankoski, Kasarminmäki). Toimipisteiden sisälläkin verkot voivat olla hajautettuja, kuten Kasarminmäen kampuksella, jossa tietoverkkoja sijaitsee monessa rakennuksessa, vaikka kyseessä on sama toimipiste. Hajautetut lähiverkot yhdistetään etäverkoilla yhdeksi toimivaksi verkoksi.

Kokonaisuutta, joka toteuttaa verkonhallinnan, kutsutaan verkonhallintajärjestelmäksi. Hallintajärjestelmät koostuvat yleensä sovelluksista, jotka monitoroivat verkkoa. Hallintasovellukset perustuvat yleisimmin SNMP-protokollaan ja käyttävät mahdollisesti myös telnet- ja www-pohjaisia laitehallintatyökaluja. Monitoroinnin avulla ylläpitäjä pystyy seuraamaan tietoverkkojen, sen palvelujen sekä laitteiden tilaa etänä, sillä verkon eri osissa sijaitsevat palvelut kommunikoivat keskitetylle verkonhallinta-asemalle asennetun valvontaohjelmiston kanssa ja antavat näin ylläpidolle kokonaiskuvan verkosta ja sen tilasta. Näin pystytään paikantamaan mahdolliset ongelmat verkossa sekä nopeuttamaan ongelmista toipumiseen kuluvaa aikaa tai korjaamaan ilmaantuneet viat ennen kuin mittavaa vahinkoa on päässyt tapahtumaan verkon käyttäjien tiedoille tai palveluille.

2.1 Verkonhallinnan vaatimukset

Riippuen näkökulmasta, verkonhallinnalle voidaan asettaa erilaisia vaatimuksia. Terplan on listannut niistä tärkeimmät:

- Organisaation omaisuuden kontrollointi. Tietoverkot eivät hyödytä yrityksien liiketaloudellisia tavoitteita ilman tehokasta valvontaa.

- Hallinnan kompleksisuus. Tietoverkkojen resurssien käytön uhkana on verkon laitteiden, käyttäjien, protokollien ja toimittajien määrän kasvu. Tämän takia verkon ylläpitäjien tulee olla koko ajan selvillä siitä, mitä verkkoon on liitetty ja kuinka sen resursseja käytetään.

- Palvelun parantuminen. Tietojärjestelmien kasvaessa ja hajautuessa, käyttäjät odottavat verkolta samanlaista tai parempaa palvelua kuin aikaisemmin.

- Tarpeiden tasapainottaminen. Eri käyttäjäryhmät tarvitsevat erilaisia palveluja ja resursseja joita yrityksen tietojärjestelmien tulee tarjota käyttäjilleen. Pitääkseen tarpeet tasapainossa tulee verkon ylläpitäjän kontrolloida sekä jakaa käytettäviä resursseja.

- Katkosten vähentäminen. Verkonhallinnalla on tärkeä rooli saatavuuden takaamiseksi, sillä tietojärjestelmien merkityksen myötä niiden ajallisen saatavuuden vaatimukset lähestyvät sataa prosenttia.

- Kustannusten hallinta. Resurssien käyttöastetta on seurattava, jotta voidaan taata käyttäjien olennaiset tarpeet kohtuullisilla kustannuksilla.

(3.)

2.2 Verkonhallinnan osa-alueet

Verkonvalvonta ja -hallinta muodostavat kokonaisuuden jota kutsutaan verkonhallinnaksi. ITU-T:n verkonhallintastandrdin X.700 mukaan verkonhallinta jakautuu viiteen eri osa-alueeseen:

Verkonvalvonnan osa-alueet:

- Vikojen hallinta
- Käytön hallinta
- Suorituskyvyn hallinta

Verkonhallinnan osa-alueet:

- Kokoonpanon hallinta
- Turvallisuuden hallinta

Vikojen, käytön sekä suorituskyvyn hallinnalla tarkoitetaan verkonvalvontaa ja kokoonpanon sekä turvallisuuden hallinnalla tarkoitetaan verkonhallintaa. Valvontaa pidetään verkon kannalta lukuprosessina, ja se sisältää verkon liikenteen valvonnan, kun taas hallinta käsitetään kirjoitusprosessina ja se mahdollistaa verkon suorituskyvyn tehostamisen. (4:303; 1:306.)

2.2.1 Vikojen hallinta

Vikatilanteiden hallinnalla pyritään havaitsemaan, kirjaamaan, ilmoittamaan viasta käyttäjälle sekä korjaamaan vika. Laajalle skaalautuvan verkon toimintakunnon ylläpitämiseksi on pidettävä huolta, että verkon jokainen laite on itsessään kunnossa. Kun vika havaitaan, ensimmäinen toimenpide on sen paikallistaminen sekä muun verkon eristäminen vian mahdollisten aiheuttamien häiriöiden estämiseksi. Jotta ilmaantuneen vian aiheuttamat häiriöt jäävät mahdollisimman pieniksi, muutetaan tarvittaessa laitteen konfiguraatiota. Tämän jälkeen vikaantuneet laitteet tai komponentit vaihdetaan,

jotta verkon toiminta pystyttäisiin palauttamaan entiselleen. Vikoihin tulee reagoida nopeasti, jotta verkon saatavuus turvataan sekä käyttökatkokset vähenisivät.

Lopulta, kun vika on korjattu, on varmistuttava siitä, että verkko toimii täysin oikein eikä vikaa ole enää olemassa eikä uusia ongelmia ole ilmentynyt. Vikojen hallinnan tulisi aiheuttaa mahdollisimman vähän haittaa verkon suorituskyvylle. (3.)

2.2.2 Käytön hallinta

Käytön hallinnalla seurataan verkon resurssien käyttöä. Jotta verkko olisi tarpeiden mukainen, käyttöasteen ja resurssien seuraamisesta saatuja tunnuslukuja käytetään kapasiteettisuunnittelussa eli verkon laajentamisen suunnittelussa sekä kehittämisessä. Käytön hallinnalla voidaan selvittää myös verkkoa kuormittavat väärinkäytökset sekä tehottomat käytöt, joita aiheuttavat useimmiten verkon käyttäjät. Loppukäyttäjille on kyettävä selvittämään mitä tietoa kerätään ja mistä sitä kerätään. Saatavia tunnuslukuja voidaan käyttää hyödyksi myös verkon käyttäjien laskutuksessa.(1:307.)

2.2.3 Suorituskyvyn hallinta

Suorituskyvyn hallinta koostuu valvonnasta sekä hallinnasta. Valvonnan avulla seurataan verkon liikennettä ja hallinnan avulla asetetaan verkon asetukset vastaamaan vaadittua suorituskyvyn tasoa. Suorituskyvyn hallinnalla pyritään pitämään verkon liikennemäärät hyväksyttävällä tasolla.

Suorituskyvyn kannalta tärkeimpiä mittareita ovat

- kapasiteetin käyttöaste
- liikenteen määrä
- vasteajat.

Suorituskyvyn hallinta ei seuraa verkon palveluiden käyttöä, vaan keskittyy enimmäkseen verkon ja laitteiden tilaan. (4:304.)

2.2.4 Kokoonpanon hallinta

Kokoonpanon hallinnan tehtäviin kuuluu verkon laitteiden määrittelytiedostojen hallinta. Tiedostojen avulla voidaan muuttaa haluttujen laitteiden attribuutteja ja ladata konfiguraatiotiedostoja verkon eri laitteisiin, jotta jokainen laite vastaisi senhetkisiä tarpeita ja vältyttäisiin mahdollisilta yhteensopivuusongelmilta. Jos ongelmia ilmenee voidaan konfiguraatiotiedostojen avulla palauttaa laitteet aikaisempaan tilaan. Tämä on tärkeä seikka vikatilanteista toipumiseen kuluvan ajan kannalta. Kokoonpanon hallinnan tärkeimpiä tehtäviä ovat myös laitteiden, laitekokoonpanojen tai verkon hallittu käynnistäminen sekä sammuttaminen ja verkon alustus. (1:306.)

2.2.5 Turvallisuuden hallinta

Turvallisuuden hallinnalla seurataan ja kontrolloidaan pääsyä verkon laitteisiin sekä sen tietoihin että palveluihin. Esimerkiksi yrityksen julkiset sivut ovat kaikkien saatavilla, kun taas intranet-sivut ovat vain rajatun käyttäjäryhmän saatavilla. Turvallisuudenhallinta keskittyy käyttäjäryhmien oikeuksien määrittämisen sijasta siihen, kenellä ja mistä on oikeus päästä eri laitteisiin käsiksi. (1:307.)

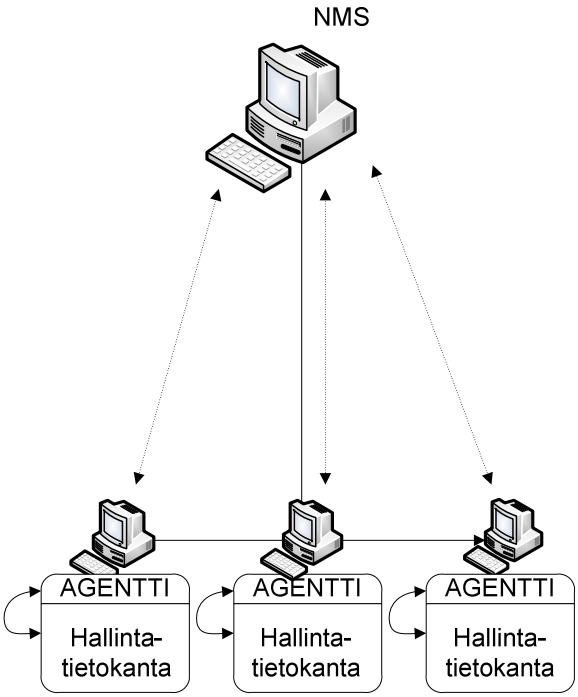
3 SNMP

SNMP on tällä hetkellä keskeisin verkonhallintajärjestelmissä käytetty hallintaprotokolla ja se on saavuttanut nykyisen suosionsa lähinnä yksinkertaisuutensa ansiosta. SNMP vaatii toimiakseen TCP/IP-protokollapinon, mutta käyttää tiedonsiirtoon yhteydetöntä UDP-protokollaa. SNMP:n avulla voidaan hallita verkon tapahtumia sekä helpottaa vianhakua verkossa. Protokolla on saatavana kaikille yleisille lähi- ja etäverkkolaitteille ja käytännössä sillä voidaan hallita mitä tahansa verkon laitetta, jossa on asennettuna SNMP-hallintasovellus. SNMP:n pääasialliset käyttöalueet ovat verkon sekä sen laitteiden että yhteyksien tilaa kuvaavien tietojen ylläpito sekä laitteiden konfigurointitiedot. (2:280.)

3.1 SNMP:n rakenne

SNMP:n rakenne koostuu kolmesta peruskomponentista. Tärkein on määriteltyjä tietoja keräävä hallinta-asema (Network Management Station, NMS). NMS:n lisäksi SNMP:aan kuuluvat hallittavissa kohteissa sijaitsevat agentit, joiden kanssa hallinta-

asema kommunikoi sekä hallintatietokanta MIB (Management Information Base), josta hallinta-asema hakee informaatiota (kuva 1).



Kuva 1. SNMP:n rakenne

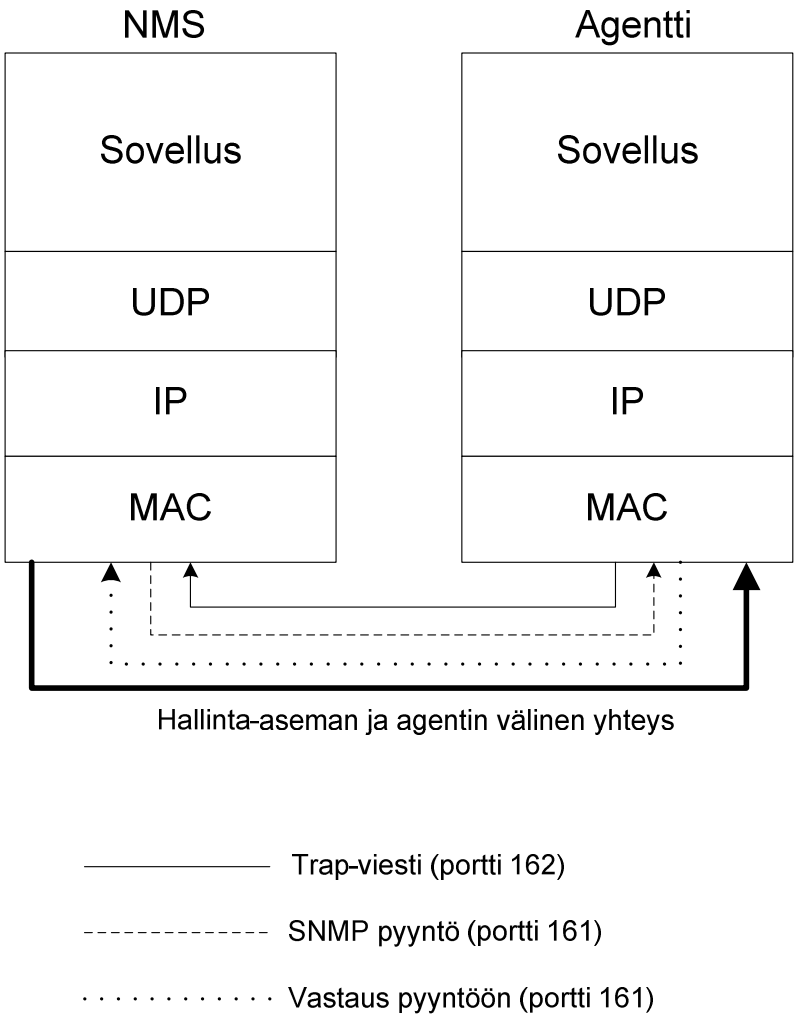
SNMP käyttää hallinta-aseman sekä agentin väliseen kommunikointiin erilaisia viestejä:

- GET
- GET-NEXT
- GET-BULK
- GET-RESPONSE (SNMPv2 & SNMPv3)
- SET
- TRAP
- NOTIFICATION (SNMPv2 & SNMPv3)

- INFORM (SNMPv2 & SNMPv3)

- REPORT (SNMPv2 & SNMPv3)

Agentin ja hallinta-aseman väliset UDP-viestit koostuvat versionumerosta, yhteisönimestä (community string) sekä PDU:sta (Protocol Data Unit). UDP käyttää viestin lähetykseen porttia 161 lukuun ottamatta agentin lähettämiä trap-viestejä, jotka käyttävät porttia 162. (5.)



Kuva 2. Hallinta-aseman ja agentin viestien käyttämät porttinumerot

Kun hallinta-asema tai agentti aikoo suorittaa SNMP-toiminnon (esim. trap- tai request-viestit), tapahtuu TCP/IP-protokollapinon eri kerroksissa seuraavaa:

- Sovelluskerros. SNMP toimii sovelluskerroksessa, jossa SNMP-sovellukset kommunikoivat keskenään UDP-porttien avulla. Sovelluskerroksesta välitetään tietoa loppukäyttäjälle käyttöliittymän kautta sekä lähetetään viestejä agenttien sekä hallinta-aseman välillä.

- UDP (Kuljetuskerros). Seuraavassa kerroksessa mahdollistetaan eri komponenttien keskustelu keskenään. Riippuen viestistä, käytettävä portti on joko 161 tai 162. Kyseisten porttien kautta lähetetään UDP-viestejä eteenpäin. Käytettävä portti on sisällytetty UDP-viestin kehykseen muiden tietojen ohella.

- IP (Internet-kerros). Seuraavana Internet-kerros kuljettaa SNMP-paketin IP-osoitteen perusteella haluttuun kohteeseen. Paketit kuljetetaan reitittimien avulla.

- MAC (Verkkokerros). Lopulta paketit kulkevat verkkokerrokselle, joka on fyysisten laitteiden rajapinta. Verkkokerroksen tehtävänä on määritellä, mille protokollalle tiedot annetaan käsiteltäväksi.

(5.)

3.1.1 Hallinta-asema

Hallinta-asema on yleisimmin itsenäinen työasema tai palvelin, jolla ajetaan verkonhallintaohjelmistoa, jonka kanssa verkkolaitteissa olevat agentit kommunikoivat. Hallinta-asemia kutsutaan myös managereiksi tai NMS:ksi. Hallintajärjestelmä vastaanottaa agenteilta kyselyiden vastaukset (query) sekä hälytykset (traps). Hallintatoiminnot suoritetaan agenteilta saatujen verkon laitteiden mittaustuloksien ja tunnuslukujen perusteella. Näihin tietoihin perustuen NMS muodostaa myös graafisia kuvaajia, jotka kuvaavat verkon tilaa. Hallintaohjelmiston käytettävissä on erinäisiä työkaluja, jotka toimivat verkon hallittavien laitteiden rajapintana, joilla voidaan vaihtaa hallittavien laitteiden asetuksia sekä hakea tietoa verkon eri osa-alueista. Fyysisesti tarkasteltuna verkonhallinnassa käytettävä hallinta-asema on usein tehokas tietokone nopealla prosessorilla sekä suurella kiintolevy- ja keskusmuistikapasiteetilla. (5.)

3.1.2 Agentit

Agentit ovat ohjelmia, jotka sijaitsevat hallittavan verkon laitteissa ja joilla on pääsy laitteiden tilatietoihin. Ne voivat olla erillisiä ohjelmia, kuten Linuxin daemonit tai ne voivat olla sisällytettynä laitteen käyttöjärjestelmään, kuten esim. Cisco-reitittimien IOS. Nykypäivänä suurimmassa osassa verkkolaitteita on jonkinlainen sisäänrakennettu SNMP-agentti helpottamassa ylläpidon työtä. Nämä kyseiset agentit kommunikoivat hallinta-asemien kanssa antamalla informaatiota hallitsemistaan laitteista erilaisilla viesteillä. Huomatessaan verkossa tapahtuvan jotain normaalista poikkeavaa, agentti lähettää hälytyksen (trap) hallinta-asemalle, joka käsittelee hälytyksen. Tilasta palauduttuaan laitteet lähettävät ”all clear” viestin, jolloin tiedetään vikatilanteen ratkenneen. (5.)

3.1.3 MIB & SMI

MIB on agenttien ylläpitämä hierarkkinen tietokanta, joka kuvaa hallittavan laitteen tiedot muuttujina ja muuttujajoukkoina. Muuttujat on nimetty sekä merkitty numerotunnisteella, OID:lla (Object Identifier). Seurattavana oleva tapahtuma voi olla esimerkiksi reitittimen liitäntäportin tila (ylhäällä/alhaalla) tai liitäntään saapuneiden pakettien määrä. MIB-tietokannasta saatujen tietojen avulla hallinta-asema määrittelee verkkolaitteen tilan. Hallintatietokannan muodostuminen on määritelty SMI-standardin mukaisesti. SMI tarjoaa tavan objektien määrittelemiseksi, kun taas MIB-tietokanta on itse objektin kuvaus. Tekniikkaa voidaan verrata sanakirjaan, jossa ensin kerrotaan kuinka sana kirjoitetaan (SMI) ja lopulta kerrotaan, mitä kyseinen sana tarkoittaa (MIB). MIB:n muuttujat jaetaan kahdeksaan ryhmään, joista viisi koskee perusprotokollia (IP, ICMP TCP, UDP, EGP) ja loput kolme määrittelevät laitteiden verkkotiloja, verkkoliitäntöjä ja laitteen käyttämän käyttöjärjestelmän tilaa. (5.)

Käytettävät standardinmukaiset hallintamäärittelyt ovat seuraavat:

- MIB I yleisille TCP/IP-laitteille
- MIB II Ethernet-, Token Ring- ja FDDI-lähiverkkolaitteille ja -verkoille
- Hub MIB Ethernet-keskittimille

- Bridge MIB Ethernet-silloille
- Host MIB tietokoneille ja työasemille
- Frame Relay MIB kehysvälitysverkon laitteille ja liitännöille
- RMON MIB verkon etämonitorointiin, tasot 1-2
- RMON II MIB tasojen 1-7 etämonitorointiin
- Manager-to-manager MIB hallinta-asemien väliseen sanomanvaihtoon SNMPv2:ssa

(1:309.)

MIB-tietokannoista on siis monia eri versioita, mutta tällä hetkellä yleisin käytettävissä oleva on MIB-II -tietokanta. Tämä standardi määrittelee liittymäportista saatujen tilastojen muuttujia ja monia muita asioita, jotka liittyvät itse järjestelmään. MIB-II:n päätavoite on tarjota yleisesti TCP/IP-hallintainformaatiota. (5.)

3.2 SNMP:n versiot

SNMP:n varhainen versio kehitettiin New Yorkissa vuonna 1988 hallitsemaan suuren verkon reitittimiä. Protokolla kulki tällöin nimellä Simple Gateway Management Protocol (SGMP). Ajan kuluessa yleisemmän ja monipuolisemman verkonhallinnan tarve kasvoi, jolloin SGMP:n yksinkertainen toimivuus huomattiin IAB:n (Internet Activities Board) toimesta ja uutta protokollaa alettiin kehittämään SGMP:n pohjalta. (6.)

3.2.1 SNMPv1

Ensimmäinen käytössä ollut SNMP:n versio tunnetaan nimellä SNMPv1. Sen ensimmäiset RFC-suositukset ilmestyivät jo vuonna 1988, mutta lopullinen muoto saavutettiin vuonna 1990. SNMPv1 on käytännössä hyvin yksinkertainen ja se koituikin kyseisen protokollan heikkoudeksi. SNMPv1:ssä ei ole kunnollista käyttäjän autentikointia, vaan luottosuhteiden muodostaminen perustuu selkokielisenä kulkevaan salaamattomaan community string –avaimeen, joka toimii kuten salasana. Community string –

avainta käytetään oikeutena lukea tai kirjoittaa tietoa agentin hallitsemalta laitteelta. Tämän lisäksi pyynnön lähettäjän IP-osoitteet tarkistetaan, jotta varmistetaan pyynnön lähettäjän olevan oikea. Tämäkin on yksi merkittävä tietoturvauhka, sillä lähettäjän IP-osoitteen muuttaminen käy helposti, jonka takia SNMP:ssä pyyntöjä lähettäviä laitteita ei pystytä varmuudella tunnistamaan. (6.)

3.2.2 SNMPv2

SNMP:n turvallisuuden parantamiseksi alkoi SNMP:n parannellun version kehittäminen. Kehityksen tuloksena syntyi SMP (Simple Monitoring Protocol), jonka pohjalta kehitettiin uusi standardiehdotus SNMPv2 joka hyväksyttiin vuonna 1993. Versio 2 oli edeltäjäänsä verrattuna selkeästi monimutkaisempi protokolla, vaikka se pohjautui suurimmaksi osin SNMPv1:n tekniikkaan käyttäen muun muassa community string -avainta käyttäjän tunnistukseen. Uuden version oli tarkoitus parantaa tietoturvaa, suorituskykyä, luotettavuutta sekä hallinta-asemien välistä kommunikointia. Samalla SNMP:n reviiri laajeni, sillä versio 2 soveltui sekä TCP/IP että OSI-pohjaisiin verkkoihin. (6.)

3.2.3 SNMPv3

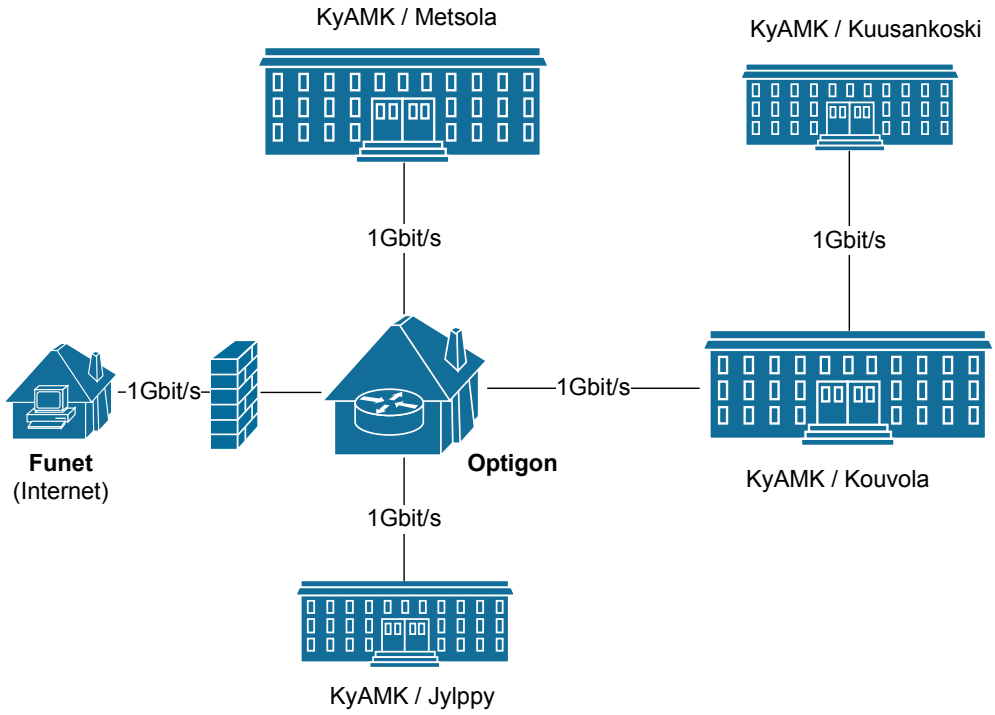
Viimeisin ja tietoturvallisin SNMP:n versio määriteltiin vuonna 2002. SNMPv3 kehitettiin parantamaan edellisten versioiden jättämiä tietoturva-aukkoja. Tietoturvaa parannettiin lisäämällä ominaisuuksiin autentikointimekanismi sekä salasanan salaus. Autentikoinnissa käytetään joko SHA1- tai MD5-algoritmiä ja salaus tapahtuu DES-kryptausalgoritmilla. SNMPv3:ssa community string–avaimen korvaa käyttäjäkohtaiset tunnukset ryhmänimi (Groupname) sekä käyttäjänimi (Username). (6.)

4 VERKONVALVONTA KÄYTÄNNÖSSÄ

Työn tarkoituksena on kartoittaa Kymenlaakson ammattikorkeakoulun vaatimuksiin sopiva verkonvalvontasovellus, joka sijoitetaan koulun tekniseen ympäristöön siten, että ohjelmiston valvonnan piiriin kuuluvat KyAMK:n jokainen toimipiste ja niissä toimivat palvelimet sekä verkkolaitteet. Verkkolaitteiden lisäksi tarkoituksena on valvoa yksityiskohtaisesti myös KyAMK:n tietoliikenneverkossa käytettävien eri protokollien sekä palvelujen toimintaa.

4.1 Valvontaympäristö

Toteutettava valvontaympäristö koostuu Kymenlaakson ammattikorkeakoulun toimipisteiden palvelimista ja verkkolaitteista. Kokonaisuudessaan ympäristössä on 25 fyysistä palvelinta, 73 virtuaalipalvelinta ja 50 kytkintä. Verkkolaitteiden lisäksi valvonta ulottuu jokaisen toimipisteen verkossa toimiviin eri palveluihin ja protokolliin. Toimipisteet sijoittuvat Kotkan (Metsola, Jylppy) sekä Kouvolan (Kasarminmäki, Kuusankoski) alueille. Internet-yhteyden palveluntarjoajana toimii Funet.



Kuva 4. KyAMK:n looginen verkkokuva

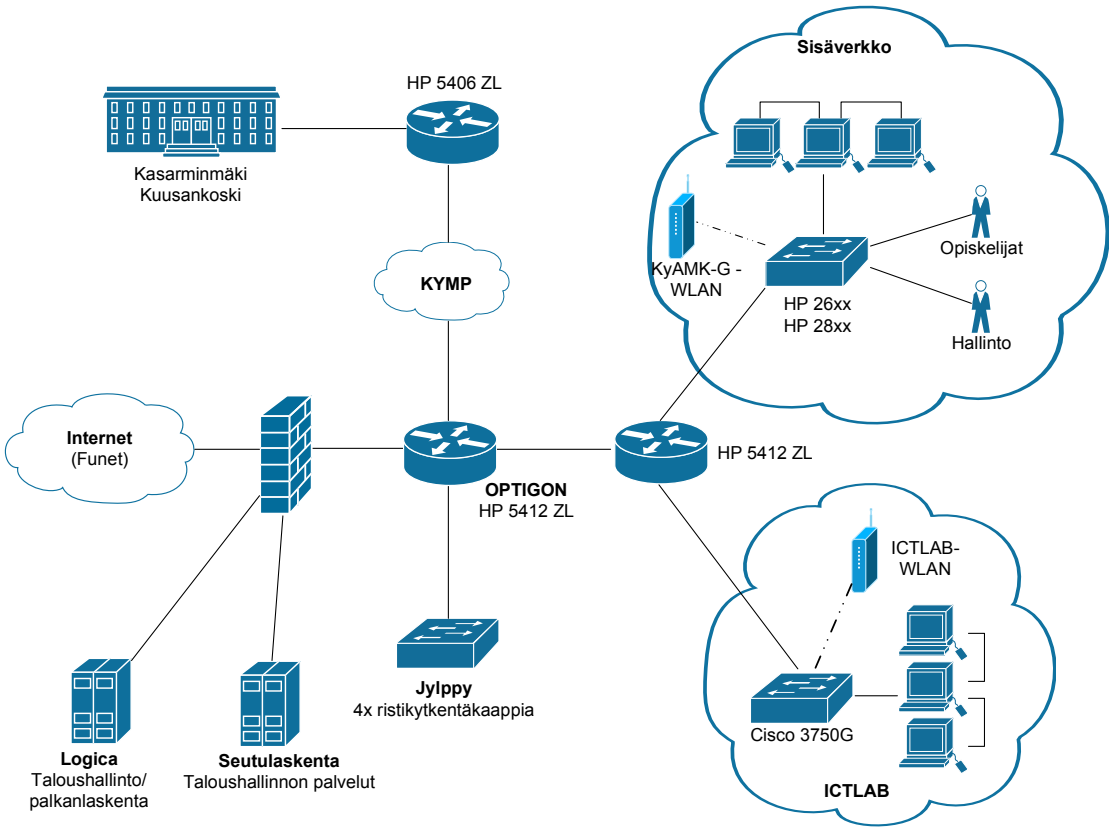
4.1.1 Kotka

Kotkan seudun verkko jakautuu maantieteellisesti kahteen eri osa-alueeseen:

- Metsola, tekniikan ja liikenteen alan opetustilat, tietohallinto
- Jylppy, sosiaali- ja terveysala

Kotkan toimipisteiden valvontaympäristö rakentuu 1 Gigabit/s runkoyhteyden ympärille. Yhteys Metsolan ja Jylpyn toimipisteiden sekä internetin välille muodostetaan Optigon-palvelinkeskuksen kautta, jossa sitaisee myös verkon palomuuri. Internetin

palveluntarjoajana toimii Funet. Metsolaan levittyvä verkko reititetään HP5412ZL-reitittimen kautta ICT-laboratiorioon sekä Metsolan toimipisteen sisäverkkoon. Koulun sisäverkossa yhteydet jaetaan eteenpäin HP:n 26xx ja 28xx kytkimillä, joiden kautta verkko jaetaan erinäisiin VLAN:eihin, joilla jokaisella on oma käyttötarkoituksensa. Sisäverkossa toimii myös Kymen Puhelimen tarjoama WLAN-yhteys, jonka valvonta ja ongelmatilanteiden ratkominen toteutetaan yhteistyössä Kymen Puhelimen kanssa. ICT-laboratoriossa verkko jaetaan Ciscon kytkimillä eteenpäin työasemille.



Kuva 4. Metsolan verkkoympäristö

4.1.2 Kouvola

Kouvolan seudulla Kymenlaakson ammattikorkeakoulun verkko jakautuu moneen eri alueeseen. Liikenne reititetään Mediakasarmilla sijaitsevan HP5406-reitittimen kautta eteenpäin seitsemään eri toimipisteeseen, jotka jakautuvat Kasarminmäen (Kouvola) sekä Sairaalamäen (Kuusankoski) kokonaisuuksiin.

Kasarminmäen eri alueita ovat

- Mediakasarmi, viestinnän koulutusohjelman tiloja

- Kasarminmäen päärakennus, Paraatikenttä 7, liiketalouden osaamisalan ja muotoilun suunnittelutilat, palveluyksiköiden tiloja

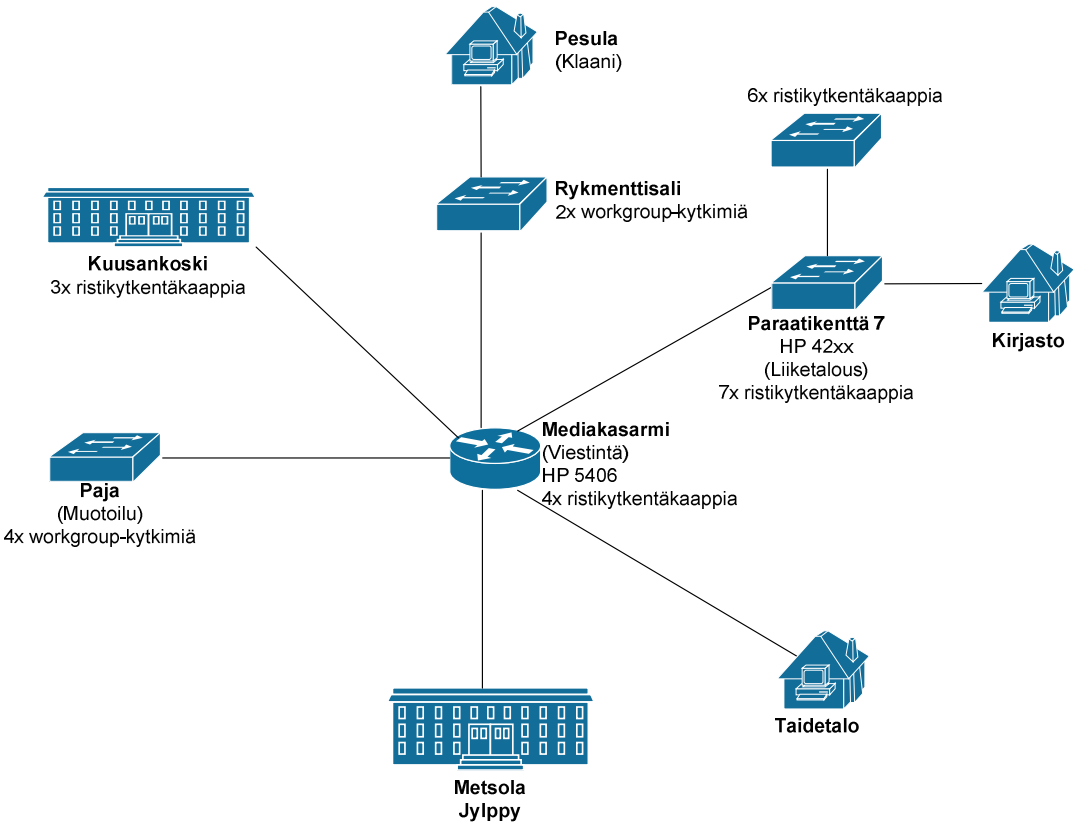
- Paja, muotoilun ja restauroinnin koulutusohjelman työpajatilat, viestintäpalvelut, tietohallinto

- Rykmenttisali, viestinnän koulutusohjelman opetustiloja sekä TV-studio ja muita av-median opetustiloja sekä Insider Student Magazinen toimitus

- Taidetalo, muotoilun, restauroinnin ja viestinnän koulutusohjelmien sekä kuvataiteen ja plastisen sommittelun opetus.

Opetustilojen lisäksi Kasarminmäellä sijaitsee kirjasto sekä opiskelijakunta Klaanin tilat. Kirjaston verkkoyhteys reititetään Kasarminmäen päärakennuksessa sijaitsevan HP 42xx-reitittimen kautta ja yhteys Klaanin tiloihin saapuu rykmenttisalin workgroup-kytkimien kautta.

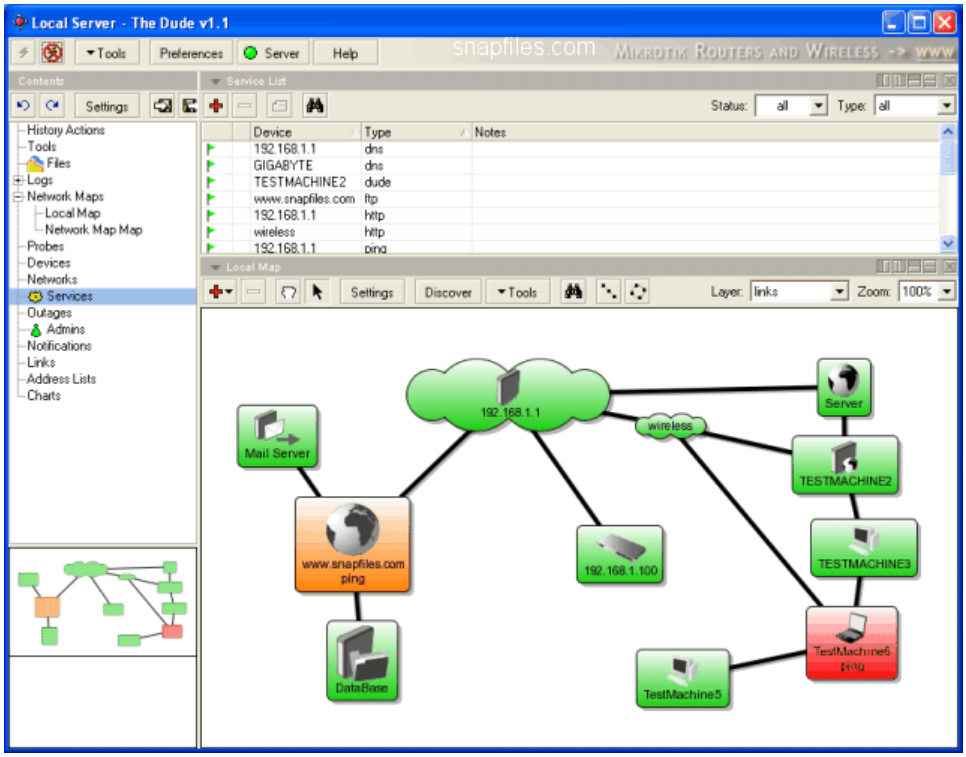
Kasarminmäen kokonaisuuden lisäksi valvonnan piiriin kuuluu myös sosiaali- ja terveysalan kampus Sairaalamäki, joka sijaitsee Kuusankoskella.



Kuva 6. Kouvolan verkkoympäristö

4.2 Nykytilanne

Tällä hetkellä Kymenlaakson ammattikorkeakoulun verkonvalvonta perustuu yksinkertaisen Dude-verkonvalvontasovelluksen toimintaan, jota tarkkailevat KyAMK:n tietohallinnon kahdeksan työntekijää kukin omalla painollaan. Käytännössä The Dude Network Monitor -ohjelma tarkkailee laitteiden ja linkkien tilaa ja ilmoittaa vikatilanteesta näyttöpäätteelle, jonka kautta verkkolaitteiden tilaa monitoroidaan.



Kuva 7. The Duden käyttöliittymä

4.3 Vaatimukset

Kymenlaakson ammattikorkeakoulun ympäristössä verkonvalvontaan kuuluu palvelimien sekä verkkolaitteiden lisäksi eri protokollia sekä palveluja. Monitoroitavia kohteita koulun verkossa on yhteensä toistasataa. Valvottavat kohteet koostuvat 25:stä fyysisestä palvelimesta, joista vähintään 10 tulisi olla valvonnan kohteena, 73:sta virtuaalisesta palvelimesta sekä 50:stä kytkimestä. Protokollat toimivat KyAMK:n tietoverkossa, joiden päällä toimii eri palveluja, joiden saatavuus on oltava korkeaa luokkaa johtuen palvelujen kuljettamasta informaatiosta. Valvottavia protokollia ovat DHCP, HTTP(S), LDAP, SSH, SFTP, SMTP ja SNMP. Näiden lisäksi valvottavia palveluja ovat Web-serverit (Apache), Active Directory -hakemistopalvelut, tietokannat (MySQL), DNS-nimipalvelin, levyjärjestelmät (EMC CX3), virtuaaliympäristöt

(VMware), Tomcat ja tulostimet/tulostusjonot. Valvottavat käyttöjärjestelmät ovat Linux-, MS Office- sekä Netware-käyttöjärjestelmiä, jotka toimivat mm. palvelimilla.

Koulun verkossa toimii myös erinäisiä sovelluksia, joiden saatavuus on pidettävä kiitettävällä tasolla. Sovellukset on luokiteltu eri ryhmiin niiden kriittisyyden perusteella. Valvottavia sovelluksia ovat

- Winha
- SoleOPS
- Sähköposti
- Moodle.

5 VERTAILTAVAT OHJELMISTOT

Verkonvalvontasovelluksen valinta tehdään kolmen kaupallisen ohjelmiston välillä. Palveluja on kartoitettu kyselemällä Datacenter Oy:n, Noval Networksin sekä HP:n tarjoamia ratkaisuja verkonvalvontaan. Vertailtavat ohjelmistot ovat Datacenter Oy:n tarjoama Nimsoft, Noval Networksin NetEye sekä HP:n IMC (Intelligent Management Center). Vertailussa tarkasteltiin ohjelmistojen ominaisuuksia, laitteistovaatimuksia sekä kustannuksia. Vertailu tehtiin haastattelemalla yritysten edustajia puhelimitse ja sähköpostitse sekä etsimällä tietoa ohjelmistojen verkkosivuilta.

5.1 Nimsoft

Datacenter Oy:n tarjoama Nimsoft Monitoring System (NMS) -ohjelmiston valvonnan piiriin kuuluvat seuraavat osa-alueet:

- Virtuaaliset ympäristöt. NMS:n avulla järjestelmänvalvojat pystyvät seuraamaan ja optimoimaan virtuaalisia ympäristöjä. NMS tukee kaikkien merkittävimpien virtualisoinnin toimittajien ratkaisuja, kuten VMware, Microsoft, Citrix, IBM ja Sun.

- Sovellusympäristöt. NMS kattaa sovellusten, kuten Microsoft Exchange, Active Directory ja IIS, Lotus Notes, SharePoint, VoIP, Citrix, WebSphere ja monien muiden, valvonnan.

- Palvelimet. NMS tarjoaa tuen iSeries AS400, Netware, Linux-, Windows- ja UNIX-palvelimien seurannalle.

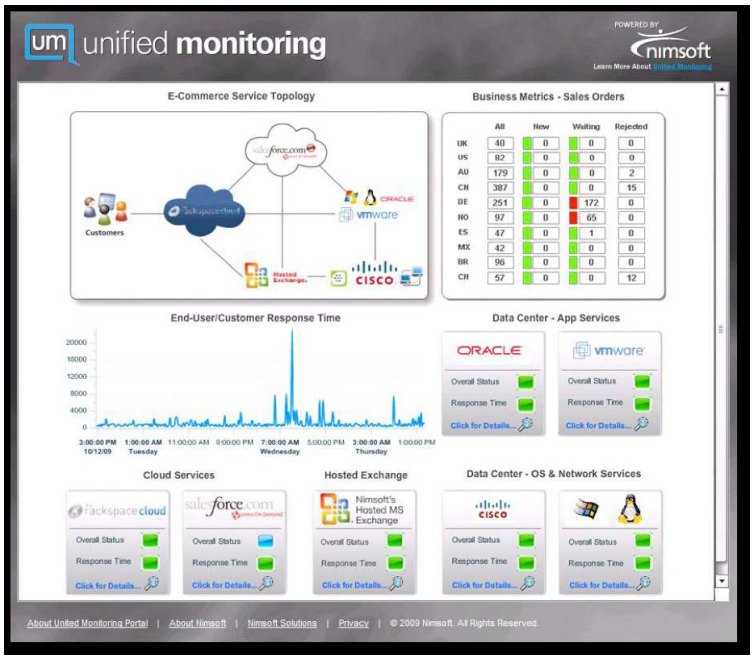
- Tietokannat. NMS tarjoaa reaaliaikaisen ja kattavan tietokantojen seurannan Oraclelle, Microsoft SQL Serverille, Sybaselle, MySQL:lle, DB2:lle ja Informix:lle.

- Verkkoympäristöt. Nimsoftin ohjelmisto kattaa erilaisten verkkoinfrastruktuurin elementtien seurannan kuten Cisco IPSLA, DNS, DHCP ja LDAP, SNMP, reitittimet ja kytkimet sekä verkkoliikenne.

- Käytön seuranta. NMS:n avulla voidaan seurata tunneittain käyttösastetta.

- Virrankulutuksen seuranta. NMS seuraa UPS:ja (Uninterruptible Power Supplies), jotta datakeskuksen operaattorit voivat nopeasti arvioida energiatehokkuutta.

(7.)



Kuva 8. Nimsoftin käyttöliittymä

5.2 NetEye

NetEye-valvontajärjestelmä koostuu seuraavista kokonaisuuksista:

- NetEye Base on NetEye-perheen ydin ja tarjoaa käyttöliittymän NetEye-työkaluihin. Lisäksi se sisältää verkon perusvalvonnan. NetEye Basen avulla voidaan hallita kapasiteettia, IP-pohjaisia laitteita (SNMPv1, SNMPv2c, SNMPv3) ja halytyksiä (sähköposti, SMS, SNMPTrap). NetEye Basen avulla pystytään myös luomaan varmuuskopiot laitteiden konfiguraatioista. Käyttöliittymä on selainpohjainen.

- Business Application Monitor tarjoaa ICT-palvelujen päästä päähän monitorointia, jonka avulla saadaan kuva palvelun kokonaiskäytettävyydestä.

- Analyze Engine analysoi verkkoprotokollia ja mittaa vasteaikoja todellisesta datasta, jolloin saadaan selville sovellusten toimivuus.

- Traffic Enginen avulla voidaan tutkia verkon suorituskykyä seuraamalla laatumääreitä aktiivimittauksella ja generoimalla liikennettä. Erilaisten toiminnallisuuksien valvontaan on erilaisia testityyppejä, joita voidaan ajaa probelaitteilta. Traffic Enginellä voidaan myös kartoittaa VoIP:n valmius sekä vikatilanteet.

- Report Engine tarjoaa ongelmatilanteista automatisoidun raportoinnin.

- Network Device Backup Enginen avulla pystytään hallitsemaan keskitetysti verkkolaitteiden konfigurointitiedostoja.

- Backup Monitor valvoo varmuuskopioiden onnistumista.

(8.)

5.3 IMC

HP:n tarjoama verkonhallintasovellus Intelligent Management Center yhdistää toiminassaan vianhallinnan, kokoonpanon hallinnan sekä verkonvalvonnan. IMC:ssä on tuki kolmannen osapuolen laitteille, joten sen avulla voidaan hallita kaikkia verkon osia erilaisilla automatisoiduilla tehtävillä. IMC:n arkkitehtuuri tarjoaa mahdollisuuden lisätä hallintaominaisuuksia lisäämällä kokonaisuuteen uusia moduuleja. Näitä moduuleja ovat mm. käytönhallinta, VPN-hallinta ja liikenteen analysointi. IMC:n avulla pystytään valvomaan myös virtuaaliympäristöjä. (9.)

IMC:n toiminnallisiin ominaisuuksiin kuuluvat muun muassa

- pääsylistojen hallinta
- käyttöoikeuksien hallinta
- Endpoint Admission Defense (EAD)
- Network Traffic Analyzer.

(9.)

IMC tarjoaa myös keskitetyn raportoinnin verkon tapahtumista. Raportteja voidaan tarkastella monessa eri muodossa (PDF, XLS) ja ne pystytään lähettämään automaattisesti sähköpostitse. (9.)

5.4 Vertailu

Vertailu tehtiin NetEyen, Nimsoftin sekä IMC:n kesken, joista jokaisen todettiin täyttävän Kymenlaakson ammattikorkeakoulun verkonvalvonnalle asettamat vaatimukset. Sovellusten kartoittamiseksi haastateltiin yritysten edustajia ja siten saatiin selville ohjelmistojen tarvittavat ominaisuudet sekä kustannusarviot.

NetEye tarjoaa isojen ympäristöjen lisäksi pienten ICT-ympäristöjen hallintaa. NetEyen ydin, NetEye Base, tarjoaa ICT-valvonnan perustyökaluja, joiden avulla voidaan hallita muun muassa verkon kapasiteettia sekä IP-laitteiden käytettävyyttä SNMP:n

avulla. Työkalujen käyttäminen tapahtuu selkeän selainpohjaisen käyttöliittymän kautta. Sovelluksen käyttöoikeuden lisäksi sopimus kattaa käyttötuen, joka sijaitsee Suomessa, HelpDeskin ja päivitykset. NetEyen yhtenä huonona puolena on valvonnan laajentaminen. Valvontaominaisuuksien lisäämiseksi joudutaan NetEye-verkonvalvontajärjestelmään hankkimaan uusia palvelukokonaisuuksia. Tämä tekee valvonnasta hieman monimutkaisempaa, valvonnan osien sijaitessa eri kokonaisuuksissa, mutta tarjoaa yrityksen tarpeiden mukaista skaalautuvuutta. NetEyen tarjoamien eri kokonaisuuksien avulla voidaan muun muassa seurata päästä- päähän -käytettävyyttä, toteuttaa protokollatason analysointia, mitata vasteaikoja, suorittaa palvelutasonhallintaa, hallita varmuuskopioita ja verkkolaitteiden konfiguraatiotiedostoja sekä määrittää automatisoitu raportointi ylläpidolle verkon tilasta. NetEyen ominaisuudet kattavat Kymenlaakson ammattikorkeakoulun verkonvalvonnan vaatimukset. Käyttöönoton kustannusarviosta saatiin selville, että perusvalvonnan käyttöönoton arvioitu hintaluokka liikkuu kohtuullisissa rajoissa. Tämä olikin NetEyen vahvin vertailukriteeri. Käyttöönottoon ja koulutukseen ei arvioitu menevän kauempaa kuin pari viikkoa.

Nimsoft-valvontasovelluksen vahvuutena ovat sen kattavat ominaisuudet, jotka vastaavat koulun verkonvalvonnan vaatimuksia. Nimsoftin valvonnan piiriin kuuluu laaja kirjo elementtejä, joita voidaan valvoa verkossa. Valvontaan kuuluvat muun muassa virtuaaliset ympäristöt, sovellusympäristöt, palvelimet, tietokannat sekä verkkoympäristöt. Vahvuudeksi voidaan lisätä myös valvonnan rakentuminen yhden ratkaisun ympärille, joten Nimsoft ei vaadi erillisiä moduuleja valvonnan laajentamiseksi. Työkalujen käyttäminen tapahtuu graafisen käyttöliittymän kautta. Kattavista ominaisuuksista huolimatta Nimsoftin kompastuskiveksi muodostui käyttöönoton kustannusarvio, joka oli kahteen muuhun vertailtavaan sovellukseen verrattuna moninkertainen. Käyttöönottoon sekä koulutukseen oli varattu noin toistakymmentä konsultointipäivää.

HP:n tarjoaman IMC:n mukaan ottaminen vertailuun johtui koulun HP-painotteisesta verkkoympäristöstä ja se olikin kyseisen sovelluksen vahvimpia puolia. IMC sisältää myös kaikki verkonvalvontaominaisuudet, joita Kymenlaakson ammattikorkeakoulun verkonvalvonnalta vaadittiin. IMC:n toiminta yhdistää vianhallinnan, kokoonpanon hallinnan sekä verkonvalvonnan, joita hallitaan graafisen käyttöliittymän kautta. Hinnoitteluarviosta saatiin selville, että sovelluksen käyttöönoton kustannukset olivat muiden vertailtavien sovellusten kustannuksia pienemmät. Poikkeuksena IMC:ssä on

laitetuki tietylle määrälle laitteita, kun taas muut vertailtavat ratkaisut pohjautuvat laitekohtaiseen käyttöönottoon ja hinnoitteluun. Sovelluksen hintaan kuuluu tuki sadalle laitteelle. Kymenlaakson ammattikorkeakoulun valvonnan piiriin kuuluu noin 150 verkkolaitetta, jonka takia huonona puolena voidaan pitää sitä, että käyttöönotto vaatisi vielä sadan laitteen lisätuen, jota HP tarjoaa lisämaksusta. Tämän lisäksi sovelluksen päivitykset ja käyttötuet eivät kuulu hintaan, vaan ne hoidetaan erillisillä Care Packeilla, joita on saatavissa myös HP:lta. Käyttöönoton erillisiä kustannuksia (käynnistysprojekti, koulutus) ei otettu huomioon, sillä kyseiset tiedot eivät ehtineet mukaan opinnäytetyöhön. Tästä huolimatta HP:lla arvioitiin käyttöönottoon kuluvan vain pari päivää.

Datacenterin tarjoama Nimsoft oli sovelluksista kattavin, mutta hinta-arvio oli varsin korkea verrattuna muihin ratkaisuihin. Lisäksi tiedon välittämisessä ilmeni pieniä ongelmia, sillä kaikkiin yhteydenottoihin ei vastattu. Hinta-arvion saaminenkin kesti monta viikkoa, eikä tämän syytä kerrottu kuin vasta viimemetreillä. HP:n IMC oli varsin potentiaalinen vaihtoehto valvontasovellukseksi, mutta ei pärjännyt vertailussa muille sovelluksille. HP:n henkilökunta vastasi sähköpostikyselyihin suhteellisen nopeasti, joten kustannusten ja ominaisuuksien selvittäminen sujui lähes vaivattomasti. Haastattelujen ja päätelmien perusteella parhaiten koulun vaatimuksiin soveltui Noval Networksin tarjoama NetEye, joka ominaisuuksiltaan ja kustannuksiltaan oli kolmesta vertailtavasta sovelluksesta tyydyttävin ratkaisu. Näiden lisäksi yhteydenpito Noval Networksin kanssa sujui ongelmitta ja halutut tiedot saapuivat nopeasti, joka antoi positiivisen kuvan yrityksen toiminnasta.

Hinta-arvioihin saattoi hieman vaikuttaa se, että kyseiset kustannusarviot ovat vain karkeita arvioita mahdollisista kustannuksista. Tämän lisäksi eri yritykset saattavat sisällyttää hinta-arvioonsa enemmän ominaisuuksia kuin toiset.

6 ZABBIXIN ASENNUS ICT-LABORATORIOON

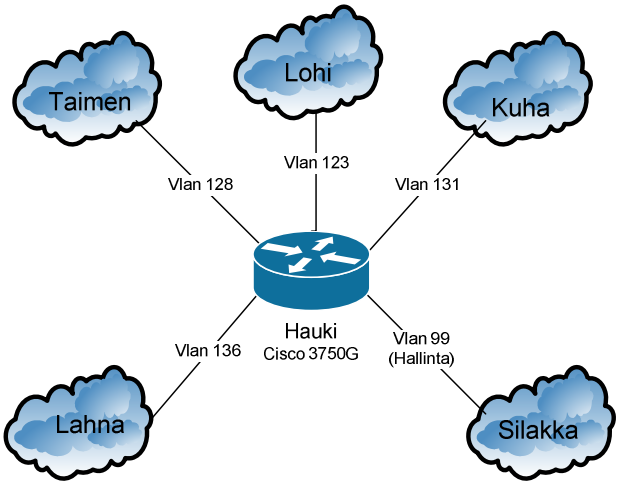
Kymenlaakson ammattikorkeakoulun varsinaisen verkonvalvonnan lisäksi ICT-laboratiorioon asennetaan Zabbix-verkonvalvontajärjestelmä monitoroimaan kulkevaa tietoliikennettä ja valvomaan tiloissa sijaitsevien verkkolaitteiden sekä SimuNet-hankkeen laitteiden tilaa. Zabbix on ilmainen vapaan lähdekoodin valvontasovellus, joka on saatavilla osoitteessa http://www.zabbix.com/download.php.

Zabbix asennettiin virtuaaliselle VMware-työasemalle Metsolan ICT-laboratorion LabESX-ympäristöön, jossa käyttöjärjestelmänä toimii Linuxin Fedora 13 distribuutio. Sovellusten asentaminen sekä niiden asetusten muuttaminen tapahtuu Linux-terminaalin kautta. Asennuksissa käytettiin paketinhallintatyökalu yum:ia (Yellow Dog Updater, Modified), jota käytetään RPM-pohjaisiin Linux-jakeluihin. Yum:n käyttö on yksinkertaista, sillä sen käskyt ovat aina muotoa

```
yum [optiot] [komennot] [paketit].
```

6.1 Valvontaympäristö

ICT-laboratorion verkkoympäristö rakentuu Hauki-verkossa sijaitsevan Ciscon 3750G-reitittimen ympärille, joka jakaa verkon eri virtuaalisiin lähiverkkoihin (kuva 9). SimuNet-hankkeen palvelimet sijaitsevat myös Hauki-verkossa muiden tärkeimpien laitteiden kanssa. Muut aliverkot sisältävät vain työasemia, WLAN-tukiasemia sekä printtereitä.



Kuva 9. ICT-laboratorion verkkoympäristö

6.2 Zabbix-asennuksen alkuvalmistelut

Ennen asennusta valitaan asennusympäristö, joka määräytyy monitoroitavien kohteiden lukumäärän perusteella. ICT-laboratorion valvontaympäristö lukeutuu pienimpään kategoriaan, sillä valvottavia laitteita on enintään toistakymmentä.

Taulukko 1. Asennusympäristön valinta koon mukaan

Size	**Platform**	**CPU/Memory**	**Database**	**Monitored hosts**
Small	Ubuntu Linux	PII 350MHz 256MB	MySQL MyISAM	20
Medium	Ubuntu Linux 64bit	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64bit	Intel Dual Core 6400 4GB RAID10	MySQL InnoDB or PostgreSQL	>1000
Very Large	RedHat Enterprise	Intel Xeon 2xCPU 8GB Fast RAID10	MySQL InnoDB or PostgreSQL	>10000

6.2.1 Käyttöjärjestelmän valmistelut

Zabbix tarvitsee seuraavat paketit asennettuna käyttöjärjestelmään toimiakseen:

- net-snmp net-snmp-utils net-snmp-libs net-snmp-devel
- popt-devel
- rpm-devel

- curl curl-devel
- openssl openssl-devel libidn-devel
- glibc-devel zlib-devel
- libssh2-devel
- OpenIPMI-devel

Luodaan Zabbix-käyttäjä, jolla voidaan tehdä asennuksia pääkäyttäjän oikeuksilla.

```
useradd –m –s /bin/bash zabbix
```

Luodun käyttäjän kirjautuminen tapahtuu käskyllä:

```
su – zabbix
```

Käyttöjärjestelmään vaadittavat osat asennetaan käskyllä:

```
yum install [paketti]
```

6.2.2 MySQL:n valmistelut

Asennetaan MySQL:n vaadittavat osat hallinta-asemalle seuraavalla käskyllä:

```
yum install mysql mysql-server mysql-devel
```

Käynnistetään MySQL ja vaihdetaan root-salasana:

```
/etc/init.d/mysqld start
```

```
/usr/bin/mysqladmin -u root password salasana
```

6.2.3 Web-käyttöliittymän valmistelut

Asennetaan web-käyttöliittymän vaadittavat osat:

```
yum install httpd php php-mysql php-bcmath php-gd php-ldap
```

6.2.4 Network Time Protocol

Network Time Protocol asennetaan hallinta-asemaan, jotta tapahtumien aikatiedot ovat täsmällisiä. NTP:n asennus tapahtuu käskyllä:

```
yum install ntp
```

Käynnistetään Ntpd (Network Time Protocol daemon)-palvelu komennolla:

```
/etc/init.d/ntpd start
```

6.3 Zabbix Serverin asennus

Asennetaan Zabbix ja sen komponentit.

```
yum install zabbix zabbix-agent zabbix-web
```

Käsky asentaa Zabbix-serverin, Zabbix-agentin sekä Zabbixin web-käyttöliittymän.

6.3.1 MySQL tietokantojen luominen

Kirjaudutaan tietokantaan aiemmin luodulla MySQL-salasanalla ja luodaan Zabbix-tietokanta. Luodaan uusi käyttäjä tietokantaan ja annetaan sille käyttöoikeudet.

```
mysql> -u root -p
mysql> CREATE DATABASE zabbix;
mysql> GRANT
DROP,INDEX,CREATE,SELECT,INSERT,UPDATE,ALTER,DELETE ON zabbix.*
TO zabbixkäyttäjänimi@localhost IDENTIFIED BY ”zabbixmysqlsala-
sana”;
mysql> quit;
```

Siirrytään Zabbix-kansioon, jossa tietokantojen luominen tapahtuu.

```
cd zabbix-1.8.1
```

Seuraavaksi annetaan kannan luontikomennot, joihin tarvitaan aiemmin määritettyä salasanaa:

```
cat create/schema/mysql.sql | mysql -u zabbixmysqlkäyttäjä -p
zabbixmysqlsalasana zabbix
```

```
cat create/data/data.sql | mysql -u zabbixmysqlkäyttäjä -p zab-
bixmysqlsalasana zabbix
```

```
cat create/data/images_mysql.sql | mysql -u zabbixmysqlkäyttäjä
-p zabbixmysqlsalasana zabbix
```

6.3.2 Zabbix Server

Zabbixin konfigurointikäsky, joka syötetään Zabbix-kansiossa, määrittää Zabbixin toiminnan kannalta tarvittavat komponentit.

```
./configure --enable-server --with-mysql --with-net-snmp
--with-libcurl --with-jabber --with-openipmi –-enable-agent
```

Tämän jälkeen Zabbix-server asennetaan käskyllä:

```
make install
```

Luodaan palvelimelle /etc/-polun alle Zabbix-niminen kansio johon kopioidaan asetustiedostot.

```
mkdir /etc/zabbix
```

```
cp misc/conf/zabbix_server.conf /etc/zabbix
```

Muokataan nano-tekstieditorilla /etc/zabbix/ -polun alta löytyvää zabbix_server.conf –tiedostoa.

```
nano /etc/zabbix/zabbix_server.conf
```

Muutetaan kohdat, jotka määrittävät tietokannan käyttäjän ja salasanan sekä mysql.sock -tiedoston sijainnin.

```
DBUser=zabbixmysqlkäyttäjä

BPassword=zabbixmysqlsalasana

DBSocket=/var/lib/mysql/mysql.sock
```

Lisätään /etc/init.d/ -polun alta löytyviin zabbix_server- ja zabbig_agentd-tiedostoihin #!/bin/sh -kohdan yläpuolelle seuraavat parametrit:

```
chkconfig: 345 95 95

description: Zabbix Server tai Zabbix Agent (riippuen tiedostosta)
```

Lopuksi määritetään Zabbix käynnistymään automaattisesti.

```
chkconfig –level 345 zabbix_server on

chkconfig –level 345 zabbix_agentd on

chkconfig –level 345 httpd on

chkconfig –level 345 mysqld on
```

Varmistetaan, että Zabbixin käyttämät oletusportit 80, 10050 ja 10051 ovat auki. Portit avataan käskyillä:

```
echo ‘zabbix_agent 10050/tcp’ >> /etc/services

echo ‘zabbix_agent 10050/udp’ >> /etc/services

echo ‘zabbix_trap 10051/tcp’ >> /etc/services

echo ‘zabbix_trap 10051/udp’ >> /etc/services
```

6.3.3 Asennuksen loppuvalmistelut

Kopioidaan frontend-tiedostot Zabbixin html-kansioon:

```
cp -r frontends/php /var/www/html/zabbix
```

Muokataan php.ini -tiedoston asetuksia nano-tekstieditorilla.

```
nano etc/php.ini
```

Skriptien maksimiajoaika muutetaan 300 sekuntiin.

```
max_execution_time = 300
```

Asetetaan aikavyöhykkeen parametrit oikeiksi.

```
date.timezone = Europe/Helsinki
```

Käynnistetään Apache web-palvelinohjelma.

```
/etc/init.d/httpd start
```

Suoritetaan komento, jolla muutetaan konfiguraatiotiedostojen kirjoitusoikeudet.

```
chmod 777 /var/www/html/zabbix/conf
```

Tarkastetaan /var/www/html/zabbix/php/conf/ -polun alta löytyvä zabbix.conf.php -tiedosto. Sen sisältämän tiedon tulisi näyttää tältä:

```
global $DB_TYPE, $DB_SERVER, $DB_PORT, $DB_DATABASE,
$DB_USER,$DB_PASSWORD,$IMAGE_FORMAT_DEFAULT;
$DB_TYPE= “käytettävä tietokantatyyppi”;
$DB_SERVER= “Palvelimen ip-osoite”;
$DB_PORT= “0”;
$DB_DATABASE= “tietokannan nimi”;
$DB_USER= “zabbixmysqlkäyttäjä”;
```

```
$DB_PASSWORD= “zabbixmysqlsalasana”;
$IMAGE_FORMAT_DEFAULT= IMAGE_FORMAT_PNG;
```

Seuraavaksi käyttöliittymälle tulee syöttää tarvittavat tiedot, joka tapahtuu osoitteessa http://127.0.0.1/zabbix.

1. Sivu (Introduction)

Luetaan tekstit ja painetaan Next painiketta.

2. Sivu (License Agreement)

Luetaan GPL-lisenssi ja hyväksytään se laittamalla ruksi I Agree - kohtaan. Hyväksymisen jälkeen painetaan Next –painiketta

3. Sivu (Check of Pre-Requisites)

Tarkistetaan, että kaikki vaaditut osat on asennettu, minkä jälkeen painetaan Next.

Tässä vaiheessa ongelmia ilmeni post max sizen sekä memory limitin kanssa. Niistä selvittiin asettamalla /etc/php.ini -tiedoston arvo kohdassa mbstring.func_overload = 2 ja asentamalla puuttuva php.mbstring -osa:

```
yum install php-mbstring
```

Tämän jälkeen käynnistetään web-server uudestaan:

```
restart httpd
```

Lopuksi muutetaan /var/www/html/zabbix/conf/zabbix.conf.php:ssa tiedot oikeellisiksi.

4. Sivu (Configure DB Connection)

Luodaan yhteys tietokantaan antamalla asetukset. Alla ohjeet:

Type = Valitaan käytettävä tietokannan tyyppi
Host = Palvelimen IP-osoite. Jos tietokanta on asennettu samalle palvelimelle kuin käyttöliittymä, isäntänimi on localhost
Port = Käytettävä portti. Perusasetuksilla käytetään porttia 0.
Name = Aiemmin luodun MYSQL-tietokannan nimi
User = Luodun MYSQL-tietokannan käyttäjän nimi
Password = MYSQL-käyttäjän salasana

Tietojen syöttämisen jälkeen testataan yhteys painamalla Test connection -painiketta.

Mikäli yhteys toimii, painetaan Next.

5. Sivu (ZABBIX server details)

Annetaan Zabbix-serverin tiedot:

Host = Palvelimen IP-osoite. Jos käyttöliittymä on samalla koneella Zabbix-Serverin kanssa, voidaan käyttää arvoa localhost tai 127.0.0.1.
Port = Portti jota Zabbix-Server käyttää. Vakioasetuksilla portti on 10051.

Tarkistetaan asetukset ja painetaan Next.

6. Sivu (Pre-Installation Summary)

Varmistetaan annetut asetukset ja painetaan Next.

7. Sivu (Install)

Tallennetaan asetustiedosto painamalla Save configuration file -painiketta. Tallennus-hakemisto näkyy sivulla

Testataan asetustiedoston toimivuus painamalla Retry-painiketta.

Kun asetustiedosto toimii, painetaan Next.

8. Sivu (Finish)

Nyt käyttöliittymä on asennettu ja sitä voi siirtyä käyttämään painamalla Finish.

Lopuksi suoritetaan komennot:

```
chmod 755 /var/www/html/zabbix/conf

mv /var/www/html/zabbix/setup.php
/var/www/html/zabbix/setup.php.bk

/etc/init.d/zabbix_server start
```

6.4 Käyttöliittymä

Zabbixin web-käyttöliittymän valikko koostuu viidesta välilehdestä:

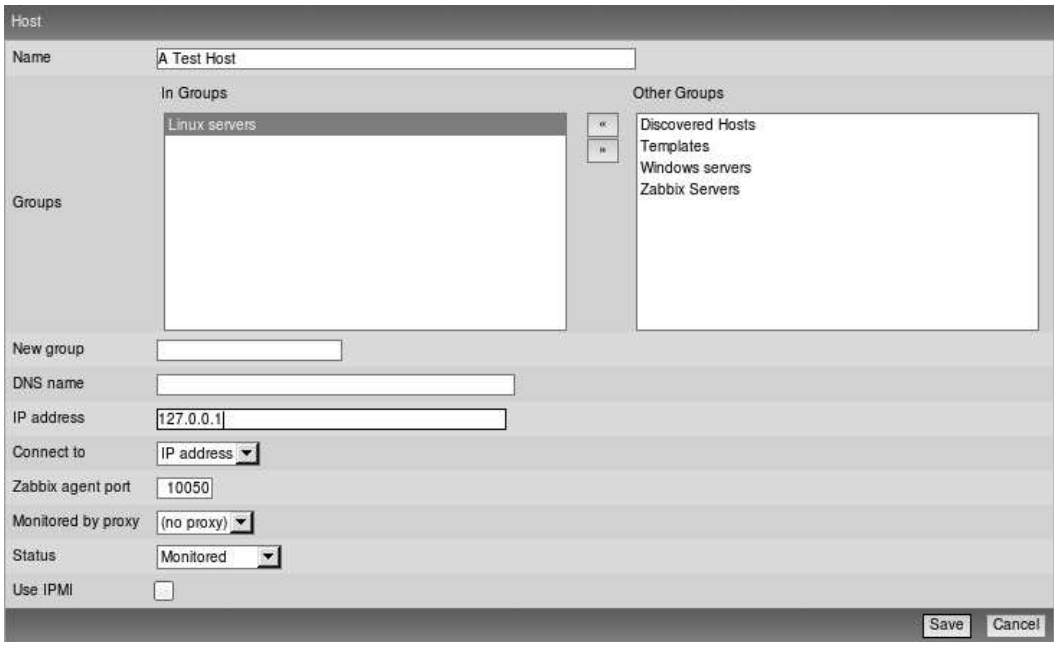
- Monitoring, joka sisältää useimmat seurantaan liittyvät sivut, joissa voidaan tarkastella valvottavien kohteiden tietoja, vikoja ja kaavioita.
- Inventory, joka kattaa valvottavista kohteista kerättyä tietoa
- Reports, joka sisältää valvottavien kohteiden raportit
- Configuration, jossa asetetaan valvottavien kohteiden parametrit, kuten esimerkiksi ilmoitukset ja hälytykset
- Administration, jossa voidaan asettaa käytettävät todentamismenetelmät sekä käyttäjiin kohdistuvat asetukset, kuten esimerkiksi käyttöoikeudet.

6.5 Kohteiden asettaminen

Kun Zabbix-verkonvalvontajärjestelmä on asennettu, lisätään valvottavat kohteet Zabbixin selainpohjaisen käyttöliittymän kautta. Asennuksen viimeistelyn jälkeen selaimeen avautuu kirjautumissivu, johon kirjautuminen tapahtuu käyttäjänimellä admin ja salasanalla zabbix. Tunnukset ovat oletustunnuksia ja ne vaihdetaan Zabbixin käyttöliittymän käyttäjäasetuksista.

6.5.1 Valvottavan kohteen lisääminen

Jotta valvonnan pystyisi toteuttamaan, tulee valvontasovellukseen lisätä valvottavia kohteita. Tämä tapahtuu luomalla Zabbix-valvontajärjestelmään uusi laite (host). Testikäytössä valvottavaksi kohteeksi lisättiin valvonta-asema. Laitteen lisääminen tapahtuu Zabbixin käyttöliittymän valikosta menemällä Configuration-valikon Hosts-välilehteen. Painamalla Add Host -painiketta aukeaa sivu, jossa on täytettäviä kenttiä koskien valvottavan laitteen tietoja (kuva 10).



Kuva 10. Valvottavan kohteen lisääminen (10.)

Name: Syötetään host-laitetta kuvaava nimi (A Test Host)

Groups: Valitaan oikealla sijaitsevasta valikosta ryhmä, johon valvottava laite (host) lisätään. Työssä käytettiin Linux servers -ryhmää. Käytettävä Ryhmä valitaan << -painikkeella ja ylimääräiset ryhmät poistetaan >> -painikkeella. Valitun ryhmä tulisi olla kohdassa In Groups.

New group: Vaihtoehtoisesti voidaan luoda oma ryhmä nimeämällä se kohdassa New Group.

DNS name: Valitaan host-laitteelle DNS-nimi

IP address: Lisätään host-laitteen IP-osoite (127.0.0.1)

Connect to: Valitaan yhteyden muodostustapa. Vaihtoehtoina ovat IP-osoite tai DNS-nimi (IP-address)

Zabbix agent port: Lisätään portti, jota Zabbix-agent käyttää (10050)

Monitored by proxy: Valitaan käytettävä välityspalvelin

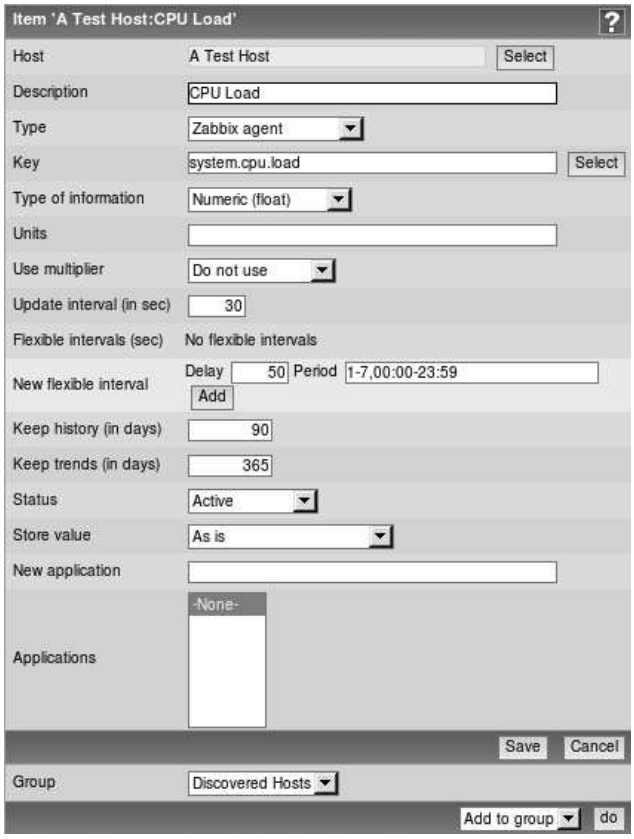
Status: Valitaan valvotaanko valvottavaa kohdetta suoraan kohteen lisäämisen jälkeen. Laitteen ollessa valmis valvottavaksi, valitaan Monitored-vaihtoehto.

Use IPMI: Valitsemalla Use IPMI -asetus saadaan IPMI:tä käytettäessä syötettyä tarvittavat arvot.

Tämän jälkeen painetaan Save-painiketta ja tarkastetaan löytyykö host-listasta juuri lisättyä kohdetta.

6.5.2 Item-määrityksen lisääminen

Valvottavien kohteiden (host) suorituskykyä sekä saatavuutta mitataan item-määrityksillä. Asetusten lisääminen tapahtuu menemällä Configuration-valikon Items-välilehteen. Sieltä valitaan aiemmin lisätty ryhmä (Linux Servers) Group-pudotusvalikosta ja painetaan Items-painiketta. Lopuksi valitaan Create Item, joka avaa item-määrityksen luomiseen tarkoitetun sivun (kuva 11). Testiympäristössä lisättiin valvottavaksi elementiksi host-laitteen prosessorin kuorma.



Kuva 11. Item-määrityksen asettaminen (10.)

Tärkeimpien kenttien selitykset:

Description: Lisätään määritystä kuvaava nimi (CPU Load)

Type: Valitaan tapa, jolla Zabbix saa tietonsa. (Zabbix agent)

Key: Syötetään kohteen "tekninen nimi", jonka avulla tunnistetaan mitä tietoa kerätään (system.cpu.load)

Type of information: Valitaan missä muodossa vastaanotettava tieto kulkee. (Numeric (float))

Update interval (in sec): Määritetään sekunteina kuinka usein tietoa päivitetään. (30)

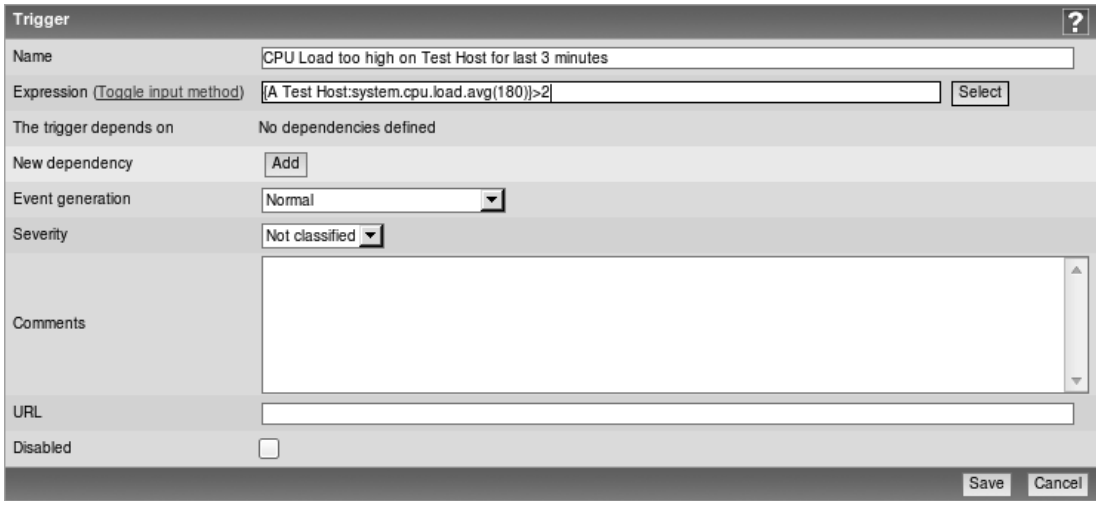
Tämän jälkeen painetaan Save-painiketta ja valikon tulisi näyttää seuraavalta:

Host	Description ▲	Last check	Last value	Change	History
A Test Host	- other - (1 Items)				
	CPU Load	01 Feb 2010 10:46:22	0.210000	-	Graph

Kuva 12. Luotu item-määritys (10.)

6.5.3 Trigger-määrityksen luominen

Trigger-määrityksillä valvotaan item-asetusten arvoa. Tässä tapauksessa järjestelmä asetetaan raportoimaan valvottavassa kohteessa havaittavasta ongelmatilanteesta. Tarkastelun kohteeksi valittiin prosessorin kuormitus. Trigger-määritys tekee raportointinsa host-laitteeseen lisätyn item-määrityksen pohjalta, jossa valvotaan prosessorin kuormitusta. Määrityksen lisääminen tapahtuu Configuration-valikon Hosts-välilehden kautta, josta löytyy painike Create Trigger. Tätä painamalla avautuu lomake, jossa on täytettäviä kenttiä liittyen trigger-asetukseen (kuva 13).



Kuva 13. Trigger-määrityksen luominen (10.)

Tällä kertaa täytettäviä kohtia on vain kaksi. Tärkeimpien kohtien selitykset:

Name: Kenttään kirjoitetaan määritystä kuvaava nimi (CPU Load too high on Test Host for last 3 minutes)

Expression: Lisätään item, jonka arvosta trigger-määrityksen tila riippuu, sekä asetetaan hälytysraja. ({A Test Host:system.cpu.load.avg(180)}>2)

Tämän jälkeen painetaan Save-painiketta, jonka jälkeen 30 minuutin kuluttua valikossa tulisi näkyä juuri luotu trigger-määritys (kuva 14).

Severity	Status	Last change	Age	Acknowledged	Host	Name	Comments
Not classified	OK	01 Feb 2010 13:20:22	30m 59s	Acknowledged	A Test Host	CPU Load too high on Test Host for last 3 minutes	Add

Kuva 14. Luotu trigger-määritys (10.)

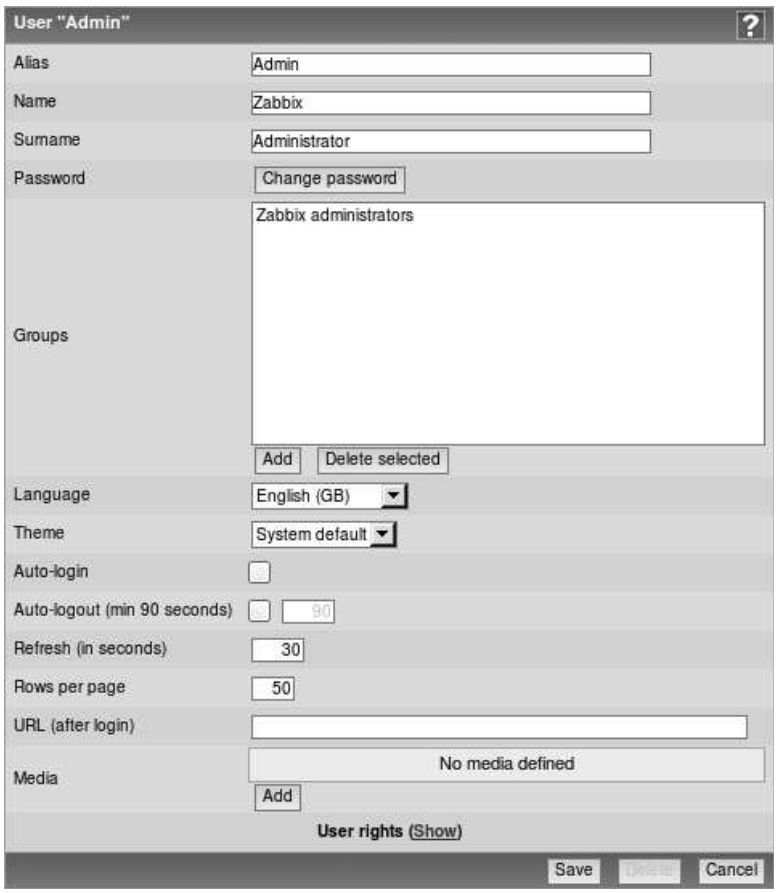
6.5.4 Ilmoitusten määrittäminen sähköpostiin

Ongelmatilanteiden raportointi asetetaan trigger-määrityksillä. Vikatilanteiden ilmoitus välitetään sähköpostilla järjestelmän ylläpidolle. Parametrien asettaminen tapahtuu Administration-valikon Media types -välilehden takaa, jossa on valittavana e-mail -painike. Tätä painamalla päästään konfiguroimaan sähköpostiasetuksia (kuva 15).

Kuva 15. Mediaparametrien asettaminen (10.)

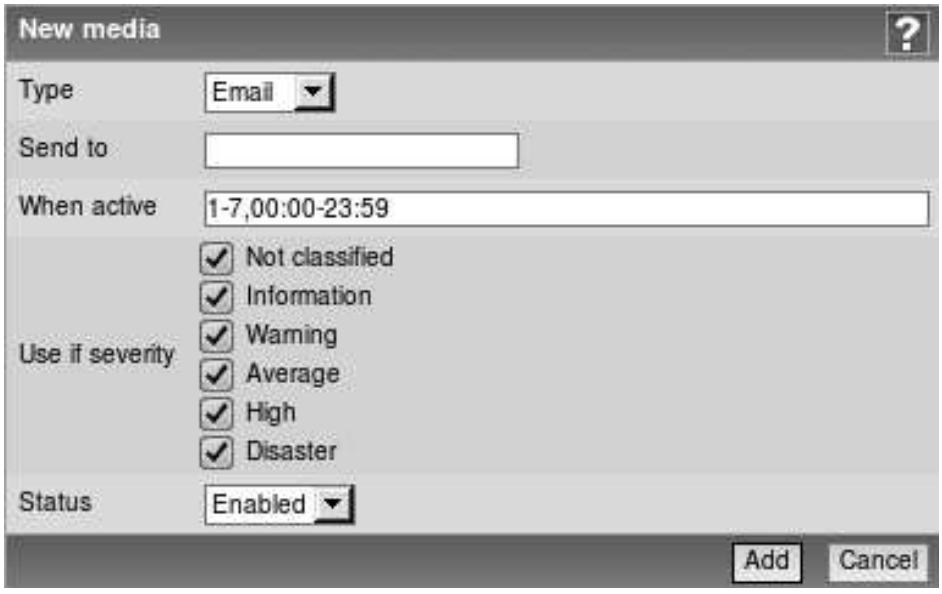
Kenttiin asetetaan vastaanottajan sähköpostiosoite sekä välityspalvelimen SMTP-palvelinosoite.

Kun tämä on tehty, tulee Zabbixiin lisätä käyttäjän tiedot, jotta järjestelmä tietää mihin ilmoitukset tulee lähettää. Tämä tapahtuu Administration-valikon Users-välilehden takaa. Pudotusvalikosta valitaan Users, jota painamalla tulisi näkyä käyttäjät Admin sekä guest. Valitaan Admin-käyttäjä, jonka jälkeen avautuu lomake jossa voidaan määritellä käyttäjän tietoja (kuva 16).



Kuva 16. Käyttäjän määrittäminen (10.)

Syötetään käyttäjän tiedot sille vaadittuihin kenttiin ja lisätään käytettävä media painamalla Media-rivin kohdalta Add-painiketta. Tämän jälkeen avautuu median määritykseen tarkoitettu sivu (kuva 17).



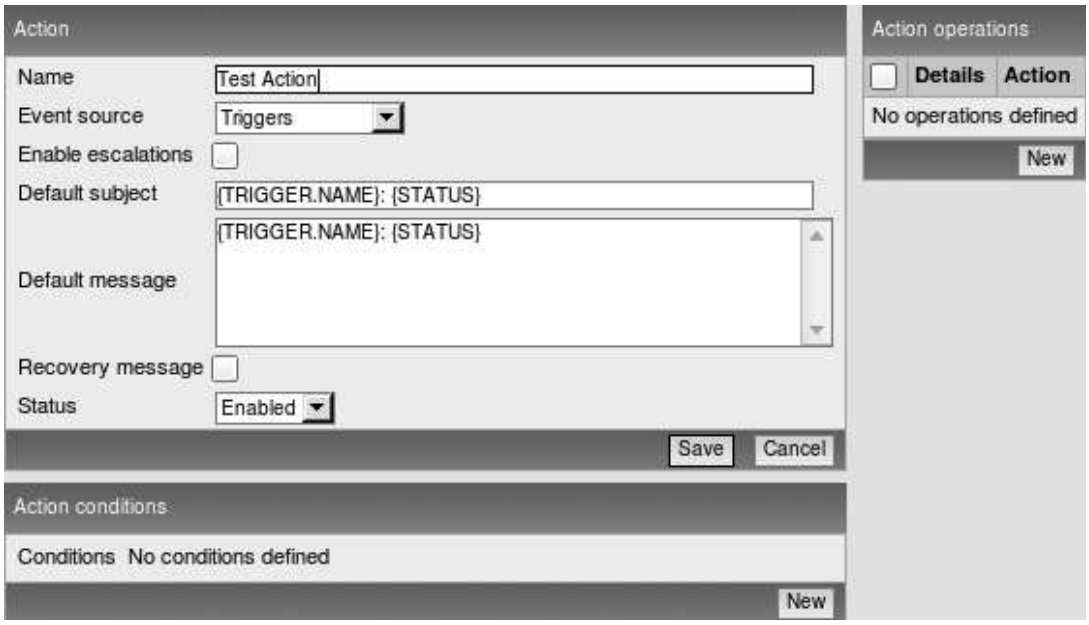
Kuva 17. Käytettävän median määrittäminen (10.)

Type: Valitaan käytettävä mediatyyppi

Send to: Syötetään käyttäjän sähköpostiosoite

6.5.5 Action-määrityksen lisääminen

Action-määrityksellä valitaan trigger-asetuksen aktivoituessa suoritettava toiminto. Testiympäristössä action-määrityksellä asetettiin Zabbix raportoimaan käyttäjälle mahdollisesta ongelmatilanteesta. Määrityksen lisääminen tapahtuu painamalla Configuration-valikon Actions-välilehden takaa löytyvää Create Action-painiketta. Tämän jälkeen avautuu action-asetusten luomiseen tarkoitettu sivu (kuva 18).



Kuva 18. Action-määrityksen lisääminen (10.)

Kenttien selitykset:

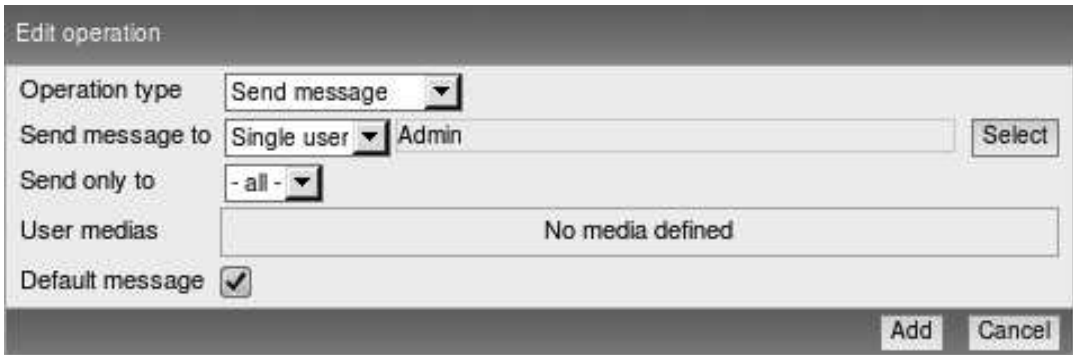
Name: Syötetään määritystä kuvaava nimi (Test Action)

Event source: Lähde, johon tapahtuma perustuu (Triggers)

Default subject: Lähetettävän viestin aihe

Default message: Lähetettävän viestin sisältö

Lisätäkseen tapahtuman, joka tulee käytäntöön kun prosessorilla on liikaa kuormaa, siirrytään Action operations -valikon kautta uuden operaation lisäämiseen painamalla New-painiketta.



Kuva 19. Uuden operaation lisääminen (10.)

Tärkeimpien kenttien merkitykset:

Operation type: Valitaan tapa, jolla ongelmatilanteen hälytys lähetetään

Send message to: Valitaan käyttäjä, jolle hälytys lähetetään

Näiden ominaisuuksien lisäksi Zabbix sisältää lukuisia vaihtoehtoja valvonnan toteuttamiseksi. Aikataulun vuoksi työssä ei käydä läpi kuin yksinkertaisimpien kohteiden ja tapahtumien luonti.

7 YHTEENVETO

Työn tärkeimpänä päämääränä oli selventää koulun verkonvalvonnan tila kartoittamalla Kymenlaakson ammattikorkeakoulun verkkoympäristö ja valvonnan piiriin kuuluvat verkkolaitteet sekä -palvelut. Työssä vertailtiin myös kolmea eri verkonvalvontasovellusta, joista parhaiten koulun vaatimuksiin sopiva tullaan hankkimaan myöhemmin tuotantokäyttöön. Sovelluksen lopullista valintaa ei ehditty tehdä opinnäytetyön aikana, mutta työssä esitetään päätelmiä parhaiten soveltuvasta valvontatyökalusta ominaisuuksien, käyttöönoton sekä kustannusten perusteella. Näiden lisäksi työssä käytiin läpi ICT-laboratorioon asennettavan Zabbix-verkonvalvontasovelluksen käyttöönotto. Opinnäytetyön tarkoituksena oli myös perehtyä verkonvalvonnan sekä sen käyttämän SNMP-protokollan toimintaan yleisesti.

Opinnäytetyö perehdytti verkonvalvontaan ja opetti ymmärtämään sen toimintaa sekä siitä saatavaa hyötyä. Verkonvalvontaa käytettäessä ylläpitoon käytettävä aika vähenee huomattavasti ja ongelmatilanteiden paikallistaminen helpottuu. SNMP-protokollaan perehtyminen auttoi ymmärtämään valvontasovellusten ja verkonhallintatyökalujen toimintaa.

Kymenlaakson ammattikorkeakoulun verkkoympäristön kartoittaminen selvensi valvottavien kohteiden sijainteja sekä verkon loogista rakennetta. Verkkoympäristön kartoittamiseksi haastateltiin koulun tietohallinnon henkilökuntaa. Haastatteluilla selvitettiin verkon eri osien laitekokoonpanot sekä niiden väliset fyysiset yhteydet. Verkon rakenteen selvittäminen sujui lähes ongelmitta, sillä tietohallinnolta saadusta informaatiosta selvisi eri toimipisteiden maantieteelliset sijainnit sekä niiden väliset verkkoyhteydet. Kymenlaakson ammattikorkeakoulun tämänhetkisestä verkosta ei ollut ajan tasalla olevaa loogista verkkokuvaa.

Työssä saatiin yleiskuva mukaan valituista kolmesta kaupallisesta valvontasovelluksesta. Sovelluksia vertailtiin ominaisuuksien sekä kustannusten perusteella. Jokaisen vertailtavan sovelluksen ominaisuudet kattoivat ainakin perusvalvontaan lukeutuvat toiminnot, joita Kymenlaakson ammattikorkeakoulu vaati verkonvalvonnalta. Tämän pohjalta ne soveltuivat kaikki Kymenlaakson ammattikorkeakoulun verkkoympäristön valvontaan. Painavimmaksi kriteeriksi valintaprosessissa muodostui sovelluksen ko-

konaiskustannukset sekä käyttöönottoprosessi. Kustannusarviot kerättiin yrityksiltä sähköpostitse sekä puhelimitse haastattelemalla. Kustannuksista tuli tietää sovelluksen, käyttöönoton sekä koulutuksen osuus kokonaiskustannuksesta. Selvityksen perusteella Kymenlaakson ammattikorkeakoulun käyttöön suositellaan Noval Networksin tarjoamaa NetEye-tuoteperhettä, joka vakuutti ominaisuuksillaan ja sen kustannukset ovat kohtuulliset eikä käyttöönottoprosessiin (koulutus, käyttöönotto) arvioida menevän kuin enintään kaksi viikkoa. Lisäksi yrityksen kanssa viestiminen tapahtui vaivattomasti niin puhelimitse kuin sähköpostitsekin ja vaaditut tiedot saatiin nopeasti ilman väärinkäsityksiä.

Ilmaisen verkonvalvontaohjelmiston Zabbixin asennusta testattiin ensimmäisen kerran 2010 kesän työharjoittelujaksolla, jonka vuoksi asennus sujui LabESX-ympäristöön ilman suurempia ongelmia. Käyttöönoton apuna käytettiin Richard Olupsin Zabbix 1.8 Network Monitoring –kirjaa. Suurimpana hidasteena sovelluksen käyttöönotossa oli VMware-virtuaaliympäristöissä toimiminen. Virtuaalinen palvelin ei jaksanut jokaisessa tilanteessa pyörittää hallintajärjestelmää eikä Zabbixin käyttöliittymää huolimatta siitä, että Zabbix on varsin kevyt sovellus. Tästä ongelmasta päästään eroon asettamalla virtuaalikoneen käyttöön enemmän muistia. Zabbix tulee myöhemmin varsinaiseen käyttöön valvomaan ICT-laboratorion verkkoa sekä siellä sijaitsevia SimuNet-hankkeen laitteita.

LÄHTEET

1. Puska, M. 1999. Lähiverkkojen tekniikka – Pro Training. Helsinki: Satku – Kauppakaari.

2. Saarelainen, K. 1993. Lähiverkkojen tekniikka. Espoo: Suomen Atk-kustannus Oy.

3. Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Helsingin teknillinen korkeakoulu: Diplomityö. Saatavissa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/diplomityo.book.html [Viitattu 7.3.2011]

4. Jaakohuhta, H. 2002. Lähiverkot – Ethernet. Helsinki: IT Press.

5. Mauro, D. R. & Schmidt, K. J. 2001. Essential SNMP. Sebastopol: O'Reilly & Associates, Inc. Saatavissa: http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ [Viitattu 10.3.2011]

6. Lummevaara,V. 2008. SNMP V3 verkonhallinta & Ciscoworks. Satakunnan ammattikorkeakoulu: Opinnäytetyö. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/740/Lummevaara%20Vesa.pdf?sequence=1 [Viitattu 10.3.2011]

7. Nimsoft. Saatavissa: http://www.nimsoft.com [Viitattu 4.4.2011]

8. Noval Networks. Saatavissa: http://www.novalnetworks.com [Viitattu 4.4.2011]

9. HP Intelligent Management Center. Saatavissa: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-0694ENW.pdf [Viitattu 4.4.2011]

10. Olups, R. 2010. Zabbix 1.8 Network Monitoring. Birmingham: Packt Publishing.