VERKONVALVONTAJÄRJESTELMÄN TOTEUTTAMINEN

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2009
Matti Kurki

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KURKI, MATTI: Verkonvalvontajärjestelmän toteuttaminen

Tietoliikennetekniikan opinnäytetyö, 58 sivua, 8 liitesivua

Kevät 2009

TIIVISTELMÄ

Opinnäytetyön aiheena on verkonvalvontajärjestelmän toteuttaminen Lahden kaupungin langattomaan MASTONET-verkkoon. Verkon ylläpitäjänä toimii vuoden 2009 alusta Lahden ammattikorkeakoulu. Tavoitteena on saada valvottua verkon tukiasemia ja niiden liikenne- ja käyttäjämääriä. Testattujen valvontaohjelmistojen joukosta valitaan tämänhetkisiä tarpeita vastaava ohjelma ylläpidon käyttöön.

Opinnäytetyön teoriaosassa käydään läpi verkonvalvonnan tavoitteita ja verkonvalvonnan eri osa-alueita. Aluksi käydään läpi verkonvalvonnan ja hallinnan kannalta tärkeän SNMP-protokollan toiminta. SNMP-protokolla hyödyntää tietojen tallentamisessa MIB-tietokantaa, jonka esitysmuodon määrittelee SMI. Lisäksi voidaan hyödyntää RMON-protokollaa verkonvalvonnassa, kun halutaan saada tarkempaa tietoa tietoliikenneverkon eri segmenttien toiminnasta.

Vertailtaviksi verkonvalvontaohjelmistoiksi valittiin Cacti, Groundwork, Nagios ja Zenoss. Näiden verkonhallintaohjelmistojen laitteistovaatimukset ovat hyvin samankaltaiset. Nykyaikaisen kotitietokoneen kapasiteetti riittäisi hyvin vertailtavien ohjelmistojen käyttämiseen alle 150 laitteen verkossa. Kaikki vertailtavat ohjelmistot käyttävät SNMP-verkonhallintaprotokollaa laitteiden tietojen kyselyyn.

Opinnäytetyön käytännön osuus koostui verkonvalvontaan valittujen ohjelmistojen asennuksesta, käyttöönotosta ja ohjelmistojen tuottamien tulosten vertailusta. Nagios vaatii valtavasti aikaa, koska siihen tiedot syötetään komentorivin kautta. Muiden ohjelmistojen hallintaan käytetään www-selainta.

Työn tavoitteena oli saada toteutettua toimiva verkonvalvonta langattomaan verkkoon. Tässä tavoitteessa onnistuttiin. Verkonvalvontaohjelmistoiksi valittiin Cacti ja Zenoss, joita hyödynnetään eri tarkoituksiin. Cactin piirtämiä kuvaajia tullaan näyttämään käyttäjille www-sivujen kautta. Zenoss tulee olemaan ylläpidon käytössä, koska sille voidaan määritellä sähköpostin lähetykset laitteiden tapahtumien perusteella. Zenossin piirtämää verkkokuvaa laitteista tullaan myös hyödyntämään verkon laitteiden tilan seurannassa.

Avainsanat: Cacti, MIB, SNMP, verkonhallinta, verkonvalvonta, Zenoss

Lahti University of Applied Sciences
Faculty of Technology

KURKI, MATTI: Network management implementation

Bachelor´s Thesis in Telecommunications Technology, 58 pages, 8 appendixes

Spring 2009

ABSTRACT

The objective of this thesis was to select a network management program for wireless network MASTONET. Lahti University of Applied Sciences took the network management role in year 2009. The objective was that the governing body would be able to monitor network devices, network traffic and user numbers. From all the tested programs the most suitable for the above listed tasks was chosen.

The theory part of this thesis presents basics of network management and protocols used in handling of data in network monitoring. It is explained how SNMP-protocol uses MIB-database and how MIB defines the representation SMI. It is also introduced that the RMON-protocol can be used if more specific details are wanted of the different segments of network traffic.

The programs compared for network management were Cacti, Groundwork, Nagios and Zenoss. All of these selected programs need almost the same hardware capacity. The capacity is such that even a modern home personal computer could handle the network management of less than 150 devices without a problem.

In the practical part, the network management programs were installed and taken into use. After that the received results were compared. It was found that the Nagios program needed a lot of time because it is a text based system. Other programs use graphical interface and are for that reason faster.

The goal was to find a working network management program to monitor a wireless network and that goal was achieved. Network management programs for MASTONET will be Cacti and Zenoss. Cacti are used to draw graphical data to web pages for end users to look at. Zenoss will be used because of its ability to note device alarms to administrators. The network map drawn by Zenoss will be used in following the status of network devices.

Key words: Cacti, MIB, SNMP, network management, network monitoring, Zenoss

SISÄLLYS

LYHENTEET

Agentti	Hallittavassa laitteessa toimiva ohjelmisto, jonka avulla hallinta-asema voi kysyä tietoja laitteen tilasta SNMP-protokollan avulla.
ASN.1	Abstract Syntax Notation One. Kuvauskieli, jolla määritetään esimerkiksi SNMP:n käyttämä sanomien esitystapa.
CGI	Common Gateway Interface. Standardi, jonka avulla voidaan näyttää palvelimien tietoja www-sivujen välityksellä ja vaikuttaa palvelimen tietoihin.
CI	Component Interface. Laitteen komponenttitietojen rajapinta, jota SNMP-agentit käyttävät.
CIM	Common Information Model. Standardi, jolla määritetään hallintatietojen esittäminen.
CMDB	Configuration Management Database. Tietokanta, johon ylläpidon asetukset tallennetaan.
CMIP	Configure Management Information Protocol. OSI-arkkitehtuurissa käytössä oleva verkonhallintaprotokolla.
CMOT	CMIP over TCP/IP. OSI:n verkonhallintastandardi, joka on suunniteltu toimimaan TCP/IP-verkoissa.
CMIS	Common Management Information Services. Määrittelee palveluiden rajapinnan, jonka välityksellä laite ja hallinta-ohjelma voivat keskustella keskenään.
DMI	Desktop Management Interface. DMI:n avulla hallitaan tietokoneiden komponenttien tietoja ja luodaan niistä näkymä käyttäjälle ohjelmarajapinnan kautta.
DMTF	Distributed Management Task Force. Standardointiyhteisö, joka kehittää verkonhallinnan standardeja.
HMMP	Hyper Media Management Protocol. WBEM:in käyttämä hallinta protokolla www-sivujen kautta tapahtuvaan hallintaan.
HTTP	Hypertext Transfer Protocol. Sovellustason protokolla www-palvelimen ja selaimen väliseen tiedonsiirtoon.
IETF	Internet Engineering Task Force. Ryhmä, jonka tehtävänä on suunnitella Internet-verkon protokollia.
ISO	International Organization for Standardization. Kansainvälinen stan-

	dardointiorganisaatio.
MI	Management Interface. Rajapinta hallintasovelluksille laitteissa.
MIB	Management Information Base. Laitteessa oleva tietokanta, jota käytetään SNMP-agentin kysellessä laitteen tietoja ja tallentaessa uusia arvoja laitteen tietoihin.
MIF	Management Information Files. Laitteen komponenttitietoja kuvaava tiedosto.
MRTG	Multi Router Traffic Grapher. Ohjelmisto jonka avulla voidaan hakea tietoa verkon laitteilta ja piirtää niistä kuvaajia.
OID	Object Identifier. Kysyttäessä SNMP-viestillä tietoja laitteelta voidaan määrittää numerosarja (OID), jolla kohdistetaan haku haluttuun MIB-objektiin.
PHP	Hypertext Preprocessor. Ohjelmointikieli, jota käytetään web-palvelinten sivustojen luonnissa.
PDU	Protocol Data Unit. SNMP-protokollan käyttämä viesti.
RMON	Remote Monitoring. Verkonhallintaprotokolla, jolla kerätään tietoa verkon eri segmenttien liikenteestä, periaatteessa lisähaara MIB-muuttujiin.
RFC	Request for Comments. Standardin omaisia dokumentteja, joiden avulla määritellään Internetin toimintaa.
RRA	Round Robin Archives. Tietokannan tietojen tallentamisen määrittelevä aikajakso, luodaan RRDtoolin keräämille tiedoille.
RRDtool	Round Robin Database. Työkalu, jolla voidaan kerätä tietoja laitteilta ja piirtää kuvaajia aikajanaa vasten. Käyttää RRA:n tietojen perusteella tallennettuja tietoja kuvaajien piirtoon.
SMI	Structure of Management Information. SMI:n avulla määritellään MIB-muuttujien rakenne.
SMON	Switch Monitoring. Jatke RMON MIB-muuttujille, jolloin saadaan vielä tarkempaa tietoa liikenteestä.
SNMP	Simple Network Management Protocol. Verkonhallintaprotokolla, jonka avulla SNMP-agentti ja hallintasovellus keskustelevat keskenään.
SWIG	Simplified Wrapper and Interface Generator. Avoimen lähdekoodin ohjelma, jolla voidaan yhdistää ohjelmia ja niiden käyttämiä

	kirjastoja.
YUM	Yellow dog Updater. Modified. Avoimen lähdekoodin ohjelma, jolla voidaan hakea päivityksiä Linux-tietokoneisiin.
VRML	Virtual Reality Modeling Language. Standarditapa, jolla esitetään 3D-vektorigrafiikkaa vuorovaikutteisesti.
WBEM	Web-Based Enterprise Management. Www-liitynnän kautta tapahtuva laitteiden hallinta.
XML	eXtensible Markup Language. Merkintäkieli, jonka avulla voidaan järjestää paljon tietoa järjesteltyyn muotoon.

1 JOHDANTO

1.1 Työn tausta

Lahdessa vuodesta 2005 toiminut MASTONET on Lahden kaupungin ylläpitämä ilmainen langaton kaupunkiverkko. MASTONET-verkko on toteutettu yhdistämällä Lahden kaupungin koulujen langaton verkko Lahti Energia Oy:n rakentamaan langattomaan verkkoon. Ajatuksena on ollut tarjota kaupunkilaisille ja Lahdessa vieraileville henkilöille ilmainen langaton Internet-yhteys. Verkon tukiasemat sijaitsevat koulujen katoilla, korkeimpien rakennusten katoilla ja Lahti Energian voimalaitosten piipuissa. Lahti Energia vastasi verkon ylläpidosta vuoden 2008 loppuun asti, jolloin ylläpito siirtyi Lahden ammattikorkeakoululle. Tätä varten päätettiin toteuttaa LAMK:lle valvontajärjestelmät verkon ylläpitoon. Jatkossa verkon kuuluvuutta pyritään parantamaan alueilla joissa liikkuu paljon ihmisiä, kuten satamassa, kauppatorilla, urheilukeskuksessa, linja-auto- ja rautatieasemalla.

MASTONET-verkon mainetta pyritään parantamaan sen saaman huonon julkisuuden osalta. Mainetta parantavia keinoja ovat esimerkiksi uudet www-sivut, joiden kautta käyttäjille kerrotaan verkon toimintaan vaikuttavista huoltotöistä. Verkkosivut tulevat toimimaan myös yhteydenpitokanavana käyttäjien ja ylläpidon välillä. Sivuston kautta käyttäjät voivat kertoa verkon toimintaan liittyvistä ongelmista. Sivuille tullaan toteuttamaan myös kartta, josta voi nähdä langattoman verkon kattavuuden. Tätä opinnäytetyötä tehdessä uudet www-sivut olivat tekeillä, mutta niitä ei oltu vielä julkaistu. Ylläpidon siirtyessä LAMK:lle, voivat opiskelijat päästä mukaan verkon ylläpitoon kurssien ja harjoittelujaksojen myötä. Opiskelijat pääsevät näin ylläpitämään todellista langatonta kaupunkiverkkoa.

1.2 Työn tavoitteet

Tämän opinnäytetyön tavoitteena on löytää sopiva verkonvalvontaohjelmisto langattomaan MASTONET-verkkoon. Valinta tehdään tutkimalla erilaisia ilmaisia verkonvalvontaohjelmistoja, joita testataan myös käytännössä. Ohjelmistojen käy-

tännön testausten perusteella valitaan verkon ylläpidon tarpeita vastaava ohjelmisto MASTONET-verkon valvontaan. Ylläpidon kannalta oleellisia asioita ovat verkon laitteiden tilaa kuvaava tilatieto sekä hälytykset ongelmatilanteissa. Laitteelta voidaan pyytää kyselyjen avulla tietoa myös muista laitteen tiedoista, kuten laitteen liityntöjen liikennemääristä.

Valittavan ohjelmiston tulee ilmoittaa ylläpidolle, jos jokin verkon laite ei vastaa sille lähetettyyn kyselyyn. Näitä ovat esimerkiksi laitteen tilaa kuvaava tieto eli onko laite up- vai down-tilassa. Valvottavan verkon laitteista muodostetusta verkkokartasta nähdään yhdellä silmäyksellä laitteiden tilat. Kartassa olevan kuvakkeen kautta päästään myös näkemään tarkemmin kyseisen laitteen tietoja.

Verkonvalvontaohjelmiston tulee toimia CentOS5-käyttöjärjestelmässä. Valvontaohjelmistoon tulee voida kirjautua useita käyttäjiä eritasoisin käyttöoikeuksin. Ohjelmiston tallentamaa tietoa voidaan hyödyntää käyttäjille julkaistavilla www-sivuilla, esimerkiksi laitteiden käyttäjämäärät voidaan näyttää laitekohtaisesti.

Vertailtavista ohjelmistoista saatujen kokemusten perusteella valitaan ohjelmisto verkonvalvontaan. Ohjelmisto asennetaan palvelimeen ja saatetaan toimintakuntoon. Asennuksesta ja käyttöönotosta laaditaan lisäksi ohjeet ylläpidolle.

2 VERKONHALLINTA

2.1 Verkonhallinnan tavoitteet

Verkkojen kasvaessa laajalle alueelle on laitteiden valvonta ihmisvoimin turhan hankalaa ja työlästä. Tätä varten on kehitetty standardeja hallintaprotokollia, joita voidaan hyödyntää hallinta-ohjelmistojen avulla. Ohjelmistojen tarkoitus on helpottaa ylläpidon työtä, ei hankaloittaa sitä, joten ohjelmistojen käyttö ja ylläpito pitää olla mahdollisimman yksinkertaista. (Jaakohuhta & Lahtinen 1997, 493.)

Verkonvalvonnalla seurataan verkossa olevien laitteiden tilaa. Tämän avulla helpotetaan ylläpidon vianselvitystä. Näin saadaan esimerkiksi selville onko joissain osin verkkoa tarvetta tehokkaammille laitteille, jotta liikenteen läpäisy paranisi. Valvonta on reaaliaikaista, joten viat huomataan heti niiden ilmaannuttua. Verkon toiminnan kannalta ratkaisevia tietoja ovat suorituskyky, toiminta-aika ja saatavuus. Jos valvottavista laitteista jokin saavuttaa sille ennalta asetetun raja-arvon, tapahtuu liipaisu eli laite antaa hälytyksen. Tätä laitetta valvova ohjelmisto saa tiedon hälytyksestä ja reagoi siihen ylläpitäjän antamien asetuksien mukaisesti. (Feldman 1999, 362.)

2.2 Verkonhallinnan eri osa-alueet

Standardissa X.700 määritellään seuraavat verkonhallinnan osa-alueet:

- vikatilanteiden hallinta (Fault Management)
- määrittelyjen hallinta (Configuration Management)
- suorituskyvyn hallinta (Performance Management)
- käytön ja laskutuksen hallinta (Accounting Management)
- turvallisuuden hallinta (Security Management).

(Puska 1999, 278.)

Vikatilanteiden hallinta on tärkeimpiä osia valvonnassa. Siinä pyritään havaitsemaan muutoksia valvottavan laitteen tilassa, joihin reagoidaan lähettämällä ver-

konvalvojalle ilmoitus raja-arvon ylittäneestä muutoksesta. Vian lähteen paikallistamisen jälkeen voidaan suorittaa tarvittavat toimenpiteet verkon toimintakyvyn palauttamiseksi. Mahdollisia toimenpiteitä ovat esimerkiksi vikaantuneen laitteen vaihto tai konfiguraatiomuutokset. Joissain laitteissa on suositeltavaa käynnistää laite tietyin ajanjaksoin uudestaan, jolloin voidaan välttyä laitteen ohjelmiston aiheuttamilta ongelmilta. Vikoja korjattaessa siitä pitää olla mahdollisimman vähän haittaa toimivan verkon osille. Vian korjauksen jälkeen varmistetaan verkon toiminta myös muilta osin, jolloin huomataan mahdolliset asennuksesta aiheutuneet ongelmat, kuten konfiguroinnissa tapahtuneet näppäilyvirheet. (Jaakohuhta & Lahtinen 1997, 496.)

Määrittelyjen hallinnassa laaditaan laitteista verkkokuva, mistä käy ilmi laitteiden yhteydet toisiinsa. Lisäksi kerätään tarkat tiedot laitteista, kuten millaiset asetukset niihin on määritelty sekä luetteloidaan käytössä olevat ohjelmistot ja niiden päivitykset. Verkon mahdollisen laajennuksen tai korjauksen toteuttaminen on huomattavasti helpompaa, kun verkon ylläpitäjällä on ajantasainen tieto käytössä olevista laitteista ja niiden ohjelmista. (Jaakohuhta & Lahtinen 1997, 500.)

Suorituskyvyn hallinnalla pyritään pitämään verkossa tasainen vasteaika, mikä näkyy käyttäjille verkon tasaisena suorituskykynä. Käyttäjät ovat tyytyväisiä, kun verkossa ei ole liian pitkää viivettä. Suorituskyvyssä mitataan laitteiden ja verkon suorituskykyä, jolloin voidaan todeta jos jossakin verkon osassa tarvitaan lisää kapasiteettia liikenteen läpäisyn parantamiseksi. Suorituskyvyn hallinta on yleensä jaettu kahteen osaan: valvontaan ja hallintaan. Valvonnan tarkoituksena on seurata laitteiden tilaa ja liikennettä. Hallinnalla pyritään puolestaan tehostamaan verkon suorituskykyä kun jokin osa siitä alkaa valvonnan analysoinnin perusteella oleellisesti vaikuttaa verkon suorituskykyyn. (Jaakohuhta & Lahtinen 1997, 502.)

Käytön hallinnassa ylläpito seuraa käyttäjien resurssitarpeita. Näin saadaan tarkkaa tietoa siitä, onko jonkin käyttäjän tai käyttäjäryhmän tarpeet alimitoitettu parhaan työtehon saavuttamiseksi. Verkon ylläpidosta aiheutuneet kulut voidaan myös jakaa resurssien käytön perusteella eri osastoille. (Jaakohuhta & Lahtinen 1997, 499.)

Turvallisuuden hallinnalla varmistetaan, että vain tietyt pääsyoikeudet saaneet käyttäjät pääsevät hallitsemaan laitteita. Lokien avulla voidaan esimerkiksi huomata väärinkäytöksien yrityksiä. Lokien keräämisen idea ei ole vain viedä tilaa levyltä, vaan niiden analysoinnilla todella saavutetaan hyötyä, kun niitä tutkitaan tarkasti. Lokien tiedoista saadaan selville esimerkiksi mistä IP-osoitteesta on yritetty päästä laitteen hallintaa. Useilla laitteilla on ominaisuus, jonka avulla voidaan määrittää pääsylista eli sallitaan yhteydenotto laitteen hallintaan vain tietystä IP-osoitteesta. Laitteen tietoturvaa parantavia ominaisuuksia kannattaa hyödyntää mahdollisimman hyvin. Jos kaikesta huolimatta verkossa ilmenee väärinkäytöksiä, verkonvalvonnan on pyrittävä selvittämään haitan lähde mahdollisimman nopeasti, jolloin voidaan pienentää myös mahdollisia haittoja. Tutkimalla tapahtumat tarkasti voidaan estää vastaavanlaisen haitan toistuminen. (Jaakohuhta & Lahtinen 1997, 504.)

2.3 Hallintarajapinnat

Yrityksillä, jotka haluavat valvoa verkon laitteita ja niiden tilaa, on mahdollisuus käyttää yleisintä hallintaprotokollaa SNMP:tä hyödyntäviä ohjelmistoja. Ohjelmistot voivat käyttää laitteiden tilan tunnistamiseen esimerkiksi ping-käskyä. Valvonta-asema lähettää tietyin väliajoin tilakyselyn verkon laitteille ja vastausten perusteella ilmoittaa laitteiden tilatiedot ylläpidolle. (Puska 1999, 286.)

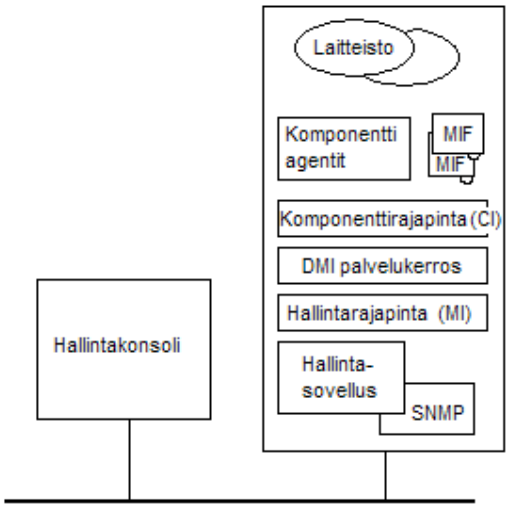
Valvottavien laitteiden tilan määrittelyyn on standardin X.731:n mukaan neljä tilaa, joita niiden tulee käyttää tilatietona:

- enabled, valmiina käyttöön, mutta ei käytössä
- disabled, ei voida käyttää
- active, laite aktiivinen ja valmiina käyttöön
- busy, tavoitettavissa, mutta ei voi suorittaa pyydettyjä pyyntöjä liian suuren kuormituksen vuoksi.

(Karila 1999.)

Organisaatioissa, joissa halutaan seurata myös työasemien tietoja, törmätään siihen, että käytössä on hyvin suuri määrä eri valmistajien työasemia. DMI (Desktop

Management Interface) -standardi on määritelty sovellusrajapinnaksi, jolla saadaan työasemien laite- ja ohjelmistotietoja haettua hallintaohjelmistoon. Kuviossa 1 näkyy DMI-palvelukerros, joka toimii kahden rajapinnan välissä tarjoten hallintasovellukselle tietoja hallintarajapinnan MI (Management Interface) kautta. Laitteen komponenttien tiedoista saadaan vastaus komponenttirajapinnan CI (Component Interface) kautta, joka hyödyntää komponenttiagentteja. Komponenttien muuttumattomia tietoja kuvaavaa hallintatiedostoa MIF (Management Information Files) hyödynnetään, kun halutaan saada tietoa esimerkiksi laitteen kiintolevyjen kapasiteetista. (Puska 1999, 289.)



KUVIO 1. DMI-rakenne (Puska 1999, 289).

Hallintasovelluksesta riippuen voidaan DMI-kyselyiden tietoja hyödyntää, käyttämällä levyosion vapaan tilan seurantaan (kuvio 1). Komponentin saavuttaessa sille asetetun raja-arvon voidaan agentin välityksellä tehdä hälytys automaattisesti. (Puska 1999, 289.)

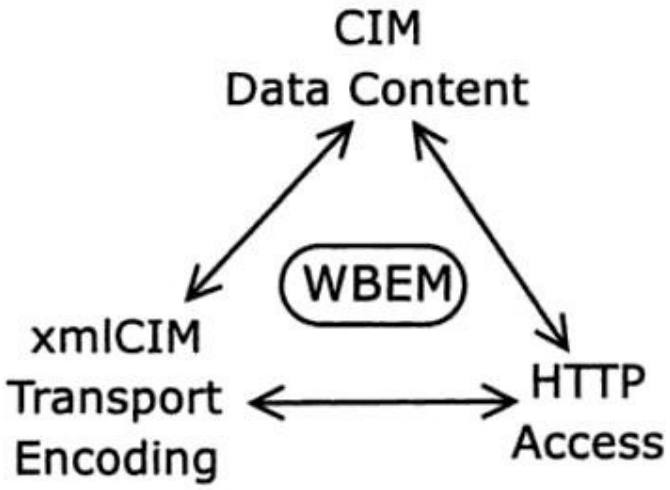
Verkonhallinnassa hyödynnetään nykyisin myös HTTP-protokollaa. Hallittavassa laitteessa on oltava toiminnassa www-palvelin, jolloin siihen voidaan muodostaa yhteys selaimella. WBEM (Web-Based Enterprise Management) -termillä viitataan www-selaimen välityksellä tapahtuvaan verkon laitteiden hallintaan. WBEM-

standardin ytimen on kehittänyt DMTF (Distributed Management Task Force) yhteistyössä useiden laite- ja ohjelmistovalmistajien kanssa. Tavoitteena on ollut täydentää nykyisiä hallintastandardeja ja tarjota tapa toteuttaa laitteiden hallinta HTTP-protokollan avulla. Laitteessa olevan tiedon esittämiseen käytetään HMMP (HyperMedia Management Protocol) -protokollaa. HMMP:n voidaan ajatella toimivan SNMP-protokollan tavoin, mutta nyt viestien siirtoon käytetään HTTP-protokollaa. WBEM:ssä käytetään CIM (Common Information Model) -mallia, jolla määritetään datalle standardi esitysmuoto. (Hobbs 2004, 18; Jaakohuhta 2005, 322.)

Kuviossa 2 on esitetty WBEM:n toiminta yleisesti ja sen käyttämät standardit:

- CIM, laitteen tiedoille määritelty standardi esitysmuoto
- xmlCIM, tieto määritellään XML:n määrittelemään muotoon
- HTTP Access, siirtoprotokolla, jolla siirretään tiedot ja käskyt verkossa.

(Hobbs 2004, 19.)



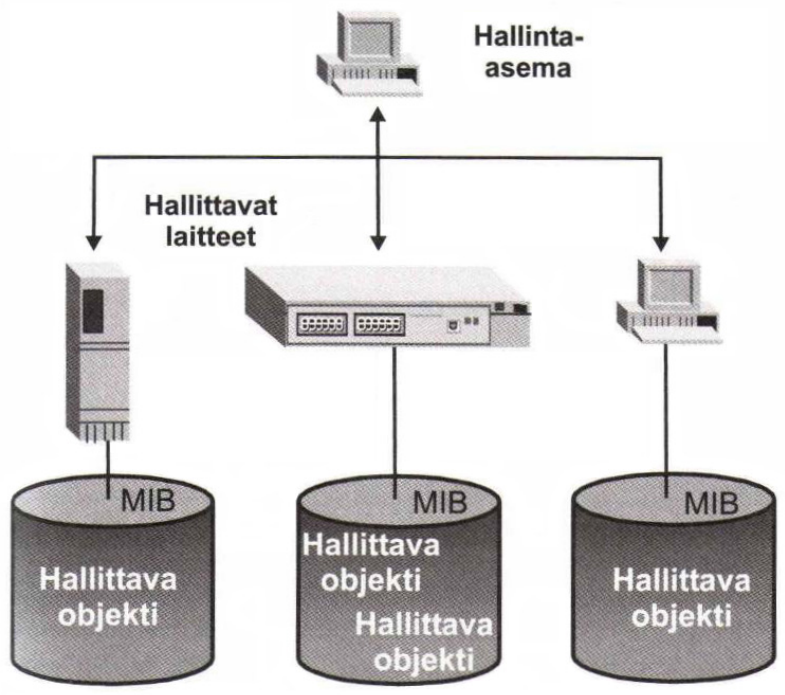
KUVIO 2. WBEM:n komponentit (Hobbs 2004, 19).

3 SNMP-PROTOKOLLA

3.1 SNMP-protokollan toiminta

SNMP (Simple Network Management Protocol) -protokolla on määritelty standardissa RFC 1067:ssä vuonna 1988 keskitettyä verkonhallintaa varten. SNMP-protokolla perustuu laitteiden hallintaan tietyn hallinta-aseman kautta. Hallinta-aseman kautta valvotaan ja konfiguroidaan laitteita, joissa toimii SNMP-agentti. (RFC1067.)

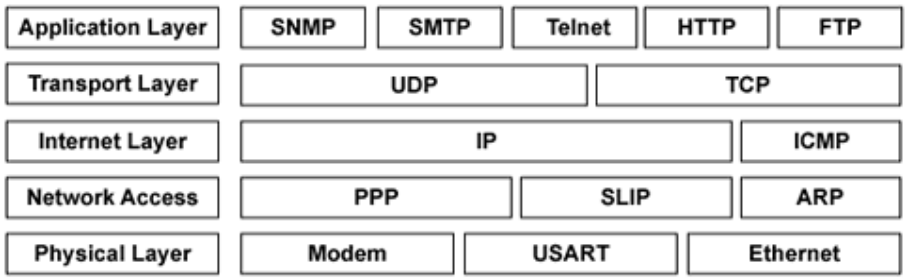
SNMP-protokolla on alun perin kehitetty IP-reititinverkkojen hallintaan. OSI-hallintastandardin viivästyessä laitteiden valmistajat alkoivat lisätä SNMP-tuen laitteilleen. Tästä seurasi myös SNMP-hallintaohjelmistojen yleistyminen markkinoilla. Nykyisin lähes kaikissa verkkoon liitetyissä laitteissa on SNMP-agentti, jota voidaan hyödyntää, kun halutaan saada tietoa laitteen tilasta ja toiminnasta. Kuviossa 3 on yleinen SNMP-hallintaympäristön rakenne. (Puska 1999, 280.)



KUVIO 3. SNMP-hallintaympäristön rakenne (Jaakohuhta 2005, 313).

Hallinta-asemassa toimiva valvontaohjelmisto kerää tietoa hallittavilta laitteilta tietokantaansa, jossa sitä voidaan säilyttää hyvinkin pitkiä aikoja. Hallittava laite pitää MIB (Management Information Database) -tietokannassaan vain reaaliaikaista tietoa. Laitteen saadessa uuden arvon tietokantaansa, kirjoitetaan vanhan tiedon päälle. (Jaakohuhta 2005, 313.)

SNMP-protokolla kommunikoi UDP (User Datagram Protocol) -protokollaa hyödyntävillä viesteillä. Viesteissä käytetään ASN.1 (Abstract Syntax Notation One) -koodausta. SNMP-viesti sisältää versiotiedon, yhteisömerkkijonon ja protokollan dataosuuden eli PDU:n (Protocol Data Unit). SNMP-protokolla käyttää tiedonsiirtoon UDP-porttia 161. Poikkeuksena ovat trap-viestit, joita lähettävät ainoastaan laitteiden agentit hallinta-asemalle sillä niiden vastaanottoon käytetään UDP-porttia 162. Protokolla on suunniteltu toimimaan TCP/IP (Transmission Control Protocol / Internet Protocol) -verkoissa. Kuviossa 4 on esitetty SNMP-protokollan ja sen käyttämän UDP-protokollan sijoittuminen TCP/IP-arkkitehtuurissa. (RFC1067.)



KUVIO 4. SNMP-protokollan sijoittuminen TCP/IP-arkkitehtuurissa (DenHartog 2009).

Standardin RFC (Request for Comments) 2571 määrittelyn mukaan SNMP-hallintajärjestelmä koostuu:

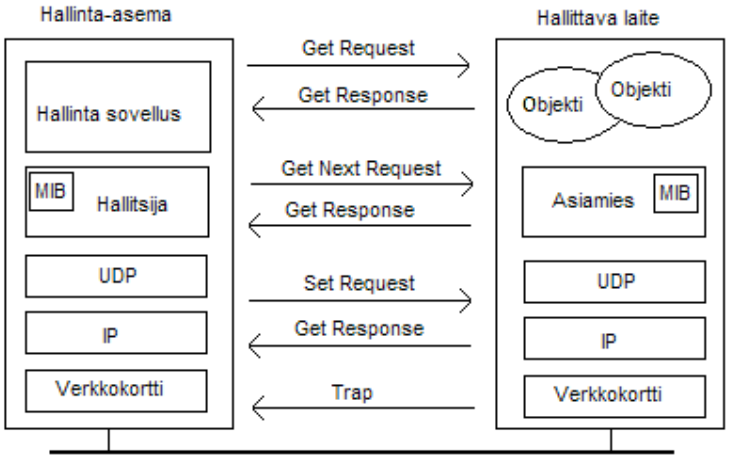
- useista solmuista, joissa toimivat sovellukset kommunikoivat agenttien välityksellä hallinta-asemalle
- vähintään yksi asema on hallintaan tarkoitettu, ja tällä asemalla voidaan lähettää SNMP-kyselyitä solmuille
- hallintatietoa siirretään käyttäen SNMP-protokollaa, joka välitetään verkossa UDP-protokollan avulla.

(RFC2571.)

SNMP perustuu pyyntöihin ja vastauksiin, missä hallintaohjelmisto lähettää halutun pyynnön hallittavalle laitteelle ja saa laitteelta vastauksen pyyntöön (kuvio 5). SNMPv1:ssä käytettäviä sanomia ovat:

- get request, tällä hallinta-asema pyytää määritellyn MIB-muuttujan arvon hallittavan laitteen agentilta
- get next request, pyydetään taulukon seuraavan muuttujan arvo
- set request, saadaan asetettua haluttu arvo hallittavan laitteen MIB-muuttujalle
- get response, hallinta-aseman vastaus get- tai set-pyyntöön
- trap, ilmoitetaan hallinta-asemalle poikkeuksellisesta tapauksesta. Näihin viesteihin ei vastata.

(Puska 1999, 283.)



KUVIO 5. SNMPv1:n sanomia (Puska 1999, 283).

SNMP:n toiminnot ovat jakamattomia, näin ollen jos yksikin kysytyistä objekteista antaa virheellisen arvon, mitään toimintoja ei suoriteta (Comer 2002, 565). Kuinka usein halutaan pyytää tietoa laitteilta, riippuu ylläpidosta. Ajastetulla toiminnolla voidaan asettaa hallintaohjelmisto kyselemään määrävälein laitteen tietoja, jolloin esimerkiksi 5 minuutin välein kysytään tietoja laitteen tietyn portin

kautta kulkevasta liikennemäärästä. Lisäksi laitteen saavuttaessa sille asetetun raja-arvon laite lähettää heti trap-viestin valvontaohjelmistolle. Hallinta-asema saa trap-viestin ja reagoi siihen esimerkiksi lähettämällä sähköpostia ylläpidolle tapahtuneesta. (Parker 1999, 718.)

SNMP-protokolla koostuu kolmesta eri standardista jotka ovat:

- MIB, tietokanta laitteen tiedoista
- SMI, kuinka viitataan MIB-kantaan
- SNMP, kuinka laite ja hallinta kommunikoivat.

(Parker 1999, 718.)

Laitteessa oleva MIB pitää kannassaan tietoa SMI:n (Structure of Management Information) määrittelemässä muodossa. SMI määrittelee kuinka MIB viittaa taulun arvoihin. SMI-standardi on tietojen esitysmuotoa kuvaava määritelmä, millä kaikki MIB-muuttujat on määriteltävä ja niihin on viitattava ISO:n (International Organization for Standardization) ASN.1-kuvauskielellä. (Comer 2002, 558.)

ASN.1-kuvauskielen avulla saadaan yhtenäinen muotokieli kannoille joissa muuttujat ovat. Käytettäessä ASN.1-kuvauskieltä tieto esitetään ihmiselle lukukelpoisessa muodossa ja sen lisäksi kuvauskieli määrittää tietojen esitystavan kommunikointiprotokollille. Kuvauskieli määrittää tarkasti, miten jokin numeerinen arvo esitetään ja kuinka siihen viittaavan objektin nimi koodataan sanomissa. Kaiken tarkoituksena on taata ristiriidattomuus muuttujien rakenteessa ja sisällön tiedoissa. (Comer 2002, 559.)

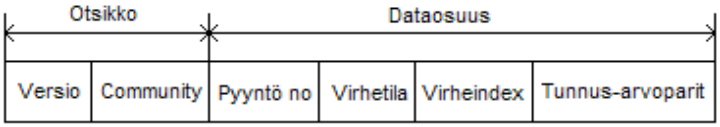
OID:lla (Object Identifier) viitataan tiettyyn kohtaan SMI-puussa, josta halutaan saada tietoja. Esitysmuotona käytetään numeerista tai selkokielistä tapaa. Numerosarjaa 1.3.6.1 vastaava tieto tekstinä on iso.org.dod.internet. Tästä on myös edetty siihen, että käyttäjä voi myös viitata OID:n 1.3.6.1 kohtaan sanalla *internet* ja saa saman tuloksen kuin edellä mainitut. (Barth 2009, 230.)

internet OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) 1 }

3.2 SNMP-protokollan eri versiot

SNMP-protokollan ensimmäinen versio SNMPv1 julkaistiin vuonna 1988. Ensimmäiset standardidokumentit SNMP-protokollasta ovat RFC 1065 - 1067 ja lisäksi SNMPv1:stä on päivitettyä tietoa standardeissa RFC 1155 - 1157. (Barth 2009, 233.)

Kun tietoliikenneverkot kasvavat ja halutaan turvata liikenne ulkopuolisilta, on ollut tarvetta parantaa tietoturvaa. SNMP:stä on nykyisin käytössä versiot 1, 2 ja 3. Versiot ovat monelta osin yhteensopivia, koska niissä käytetään samaa yleistä kehystä. Sanomien rakenne määritellään SNMP-protokollassa. SNMPv1-viesti koostuu otsikosta ja dataosuudesta kuvion 6 mukaisesti. (Comer 2002, 557.)



KUVIO 6. SNMPv1-viestin rakenne (Puska 1999, 284).

SNMP-viestin rakenne on seuraava:

- versio, joka sisältää käytettävän SNMP-protokollan versiotiedon
- community, joka on yhteisömerkkijono, jolla varmistetaan oikeudet saada vastaus kyselyihin
- pyyntö no, on lähettäjän lisäämä tunniste, siirtotienä käytetään yhteydetöntä yhteyttä, jolloin halutaan varmistaa vastaukset lähetettyihin pyyntöihin
- virhetila, jos käytetty operaatio käyttää tätä, muuten sijoitetaan nolla
- virheindex, jos käytetty operaatio käyttää, muuten asetetaan nolla
- tunnus-arvoparit, jotka ovat kyselytiedot.

(Javvin Technologies 2009a.)

Yhteisömerkkijonotietoa ei pidä jakaa jokaisen saataville, vaan sen tulisi olla tiedossa vain ylläpidolla, koska SNMP-protokollassa yhteisömerkkijonoa käytetään

osapuolten tunnistamiseen. Tämän tunnisteen avulla on mahdollista saada laite hallintaan, ja tästä syystä se pitää lukea salasanan arvoiseksi. (Thomas 2005, 225.)

SNMPv1:n huonoina puolina voidaan pitää sitä, että viestit ovat selkokielisiä kun ne lähetetään verkkoon. Jonkinlaista suojaa laitteille tarjoaa yhteisömerkkijono, jolla voidaan määrittää oikeustaso kuten, ei oikeutta, lukuoikeus ja kaiken salliva oikeus laitteiden tietoihin. (Barth 2009, 233.)

SNMPv2 julkaistiin vuonna 1993 ja se on määritelty standardeissa RFC 1441 - 1450. Parannuksia olivat SNMPv1:een verrattuna Inform ja Get-Bulk -viestit. Näiden viestien avulla voidaan lähettää toisille hallinta-asemille tietoa tapahtumista (Inform) ja voidaan pyytää laitteelta suurempia tietomääriä kerralla (Get Bulk). SNMPv2:n huonona puolena oli sen tietoturvaominaisuuksien tilanne SNMPv1-versioon nähden. Ne olivat samalla tasolla kuin SNMPv1:ssä, joten SNMPv2 ei tarjonnut parannuksia tietoturvaan, joka on osaltaan vaikuttanut siihen, että se ei ole syrjäyttänyt SNMPv1-protokollaa. (Karila 1999.)

SNMPv3 on IETF:n (Internet Engineering Task Force) kehittämä uusi versio SNMP-protokollasta, joka on julkaistu standardissa RFC 2570 vuonna 1999. Suurimmat muutokset koskevat suojausta ja hallintaa. Suojauksella ylläpito voi todentaa komentojen oikeellisuuden. Sanomien lukeminen hallittavan laitteen ja hallinta-aseman välillä on varmistettu msgID-kentällä SNMPv3-sanomassa. Kentässä olevan arvon avulla yksilöidään viesti, jolloin kyselyn vastauksessa pitää msgID:n olla sama kuin lähetetyssä viestissä. (Comer 2002, 572.)

3.3 SNMP-protokollan turvallisuus

Tietoturvasta ei pidä tinkiä verkon laitteissa eikä ohjelmistojen asetuksissa. Hallittavan laitteen tulee varmistaa SNMP-viestin oikeudet tehdä viestin pyyntöjen mukaisia toimintoja, kuten voidaanko muuttaa laitteen nimeä. SNMPv1-viestin oikeudet tarkistetaan käyttämällä yhteisömerkkijonoa. SNMPv1-viestit kuitenkin kulkevat verkossa selkokielisenä, joten verkkoon tunkeutunut urkkija voi saada

yhteisömerkkijonon haltuunsa. Tästä johtuen kannattaa käyttää eri salasanoja kirjoitus- ja luku-oikeuksiin. (Haikonen 2000.)

SNMPv2-viestit lähetetään myös selkokielisinä verkossa. Hallittava laite varmistaa viestin lähettäjän oikeudet myös SNMPv2-viestissä yhteisömerkkijonoa käyttäen, joten tietoturva on SNMPv1:n tasolla. SNMPv3 on huomattavasti kehittyneempi tietoturvan osalta kuin edeltävät versiot. SNMPv3:ssa on pakko määritellä jokin kolmesta eri tietoturvatasosta käyttöön. Käytetyt tasot ovat lueteltu alla:

- noAuthNoPriv, todennus käyttäjänimellä, salaamaton viesti
- authNoPriv, todennus MD5- tai SHA-salauksella, salaamaton viesti
- authPriv, todennus MD5- tai SHA-salauksella, viestin salaus DES-algoritmilla.

(Cisco Systems 2009.)

SNMP-protokollan tietoturvaa voidaan parantaa eriyttämällä hallintaviestit omaan VLAN:iinsa. VLAN:issa lisätään kehykseen ID, jolla se tunnistetaan kun viesti saapuu kytkimelle. Porttiin on määritelty tietty VLAN, joka laskee oikean ID:n omaavat läpi ja hylkää muut viestit. Näin SNMP-liikenne voidaan rajoittaa ainoastaan oman hallintaverkkonsa sisälle.

3.4 MIB

MIB-oliotietokanta pitää sisällään laitteen tiedot, jotka ovat puumaisessa hierarkiassa. Verkossa olevilla laitteilla on kullakin oma MIB-puunsa. Valmistajasta riippuu, mitä kaikkea tietoa laitteesta on mahdollista saada ulos, mutta tuki seuraaville standardeille löytyy kaikista laitteista:

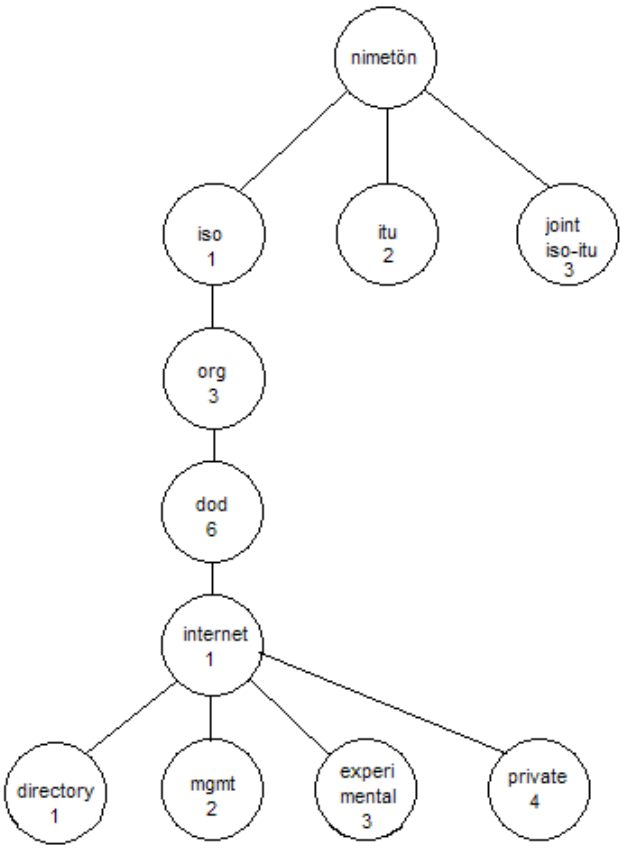
- MIB I yleisille TCP/IP-laitteille
- MIB II Ethernet, Token Ring- ja FDDI-lähiverkkolaitteille ja -verkoille
- Hub MIB Ethernet-keskittimille
- Bridge MIB Ethernet-silloille
- Host MIB tietokoneille ja työasemille
- Frame Relay MIB kehysvälitysverkon laitteille ja liitännöille

- RMON MIB verkon etämonitorointiin, tasot 1 -2
- RMON II MIB tasojen 1 -7 etämonitorointiin
- Manager-to-manager MIB hallinta-asemien väliseen sanomanvaihtoon SNMPv2.0:ssa.

(Puska 1999, 281.)

MIB-I ja MIB-II -muuttujia ovat esimerkiksi laitteelle annetut tiedot SysContact, SysName ja SysLocation. Liikennemääriä seurattaessa hyödyllisiä muuttujia ovat ifOutOctets ja ifInOctets, joiden avulla saadaan tietoa liitynnän tulevasta ja lähtevästä tavumäärästä. Saadut tiedot yhdistämällä voidaan luoda raportti, mistä käy ilmi laitteen nimi, paikka ja liikennemäärät. (Feldman 1999, 364.)

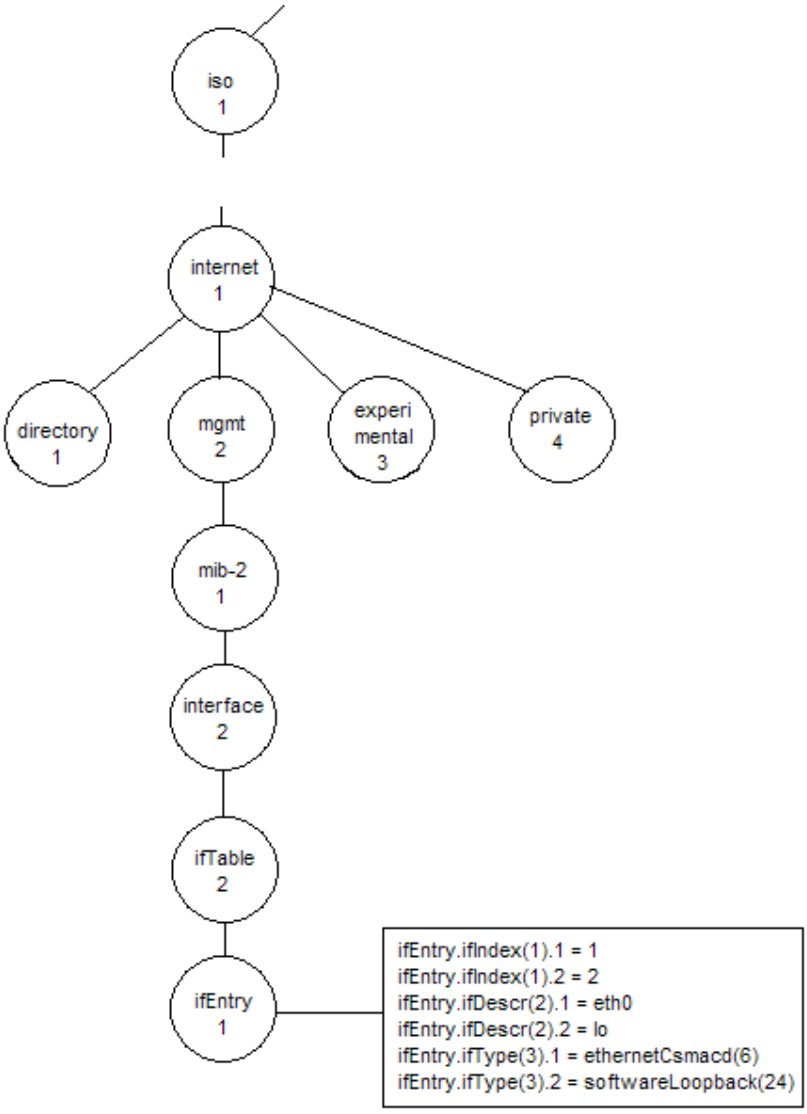
MIB-objektien nimien rakenne ja esitysmuoto on tarkkaan määritelty nimiavaruudessa. Nimiavaruus sisältää kaikki objektien nimet, joita laitteet voivat sisältää. Hierarkkinen rakenne, joita MIB-muuttujissa käytetään, on kuvion 7 mukainen. Ylin osa eli juuri on nimetön, ja sen alta löytyvät ISO, ITU ja JOINT ISO-ITU. (Comer 2002, 560.)



KUVIO 7. MIB-rakenne (Comer 2002, 560).

MIB-objektin nimestä voidaan käyttää nimeä lukujono. Jos laitteesta halutaan saada selville esimerkiksi IP:hen liittyvä informaatio, niin tämä tieto löytyy numerosarjan 1.3.6.1.2.1.4 haarasta. (Comer 2002, 561.)

Kun halutaan saada selville laitteen verkkoliittymän tietoja, voidaan seurata polkua kuvion 8 mukaisesti.



KUVIO 8. MIB-tiedot verkkoliitynnästä (Barth 2009, 230).

Kuviossa 8 esitetyn ifEntryn kautta voidaan laitteen liitynnän tietoja kyselevälle ohjelmistolle antaa tietoa, että liitynnän ifIndex numero on 1, sitä vastaa eth0 liityntä ja sen tyyppi on ethernetCsmacd eli kyseessä on ethernet-liityntä. IfIndex 2 on vastaavasti niin sanottu loopback-liityntä. (Barth 2009, 230.)

Linux-ympäristössä voidaan testata SNMP-protokollan toimintaa jos Linux-koneelle on asennettu siihen vaaditut SNMP-ohjelmistot. Verkkoon kytketyltä laitteelta voidaan hakea esimerkiksi tietoa laitteen liitynnöistä käyttäen MIB-II:n

objekteja. Tällöin annetaan snmpwalk-käsky tietyin parametrein josta esimerkki kuviossa 9.

```
user@linux: snmpwalk -v1 -c public localhost mib-2.interfaces
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER:1
IF-MIB::ifIndex.2 = INTEGER:2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: eth0
IF-MIB::ifDescr.2 = STRING: lo
IF-MIB::ifDescr.3 = STRING: eth1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
```

KUVIO 9. Snmpwalk-käsky

Käskyssä määritetään käytössä olevan SNMP-protokollan versio (v1), yhteisömerkkijono (public), mihin osoitteeseen kysely lähetetään (localhost) ja mitä halutaan tietää (mib-2.interfaces). Esimerkissä saadaan vastaus localhost-koneen liityntätiedoista. Ensimmäisellä rivillä oleva ifNumber sisältää laitteen liityntöjen määrän. Kolmella seuraavalla rivillä on liitynnät numeroitu, ja numeroita voidaan hyödyntää tarkemmassa kyselyssä. Liityntöjä kuvaavat tiedot ovat eth0, lo ja eth1. (Barth 2009, 236.)

Haluttaessa kysely voidaan kohdistaa ainoastaan tiettyyn objektiin. Jos halutaan tietää laitteen liityntöjen määrä eikä muuta, annetaan esimerkin mukainen käsky:

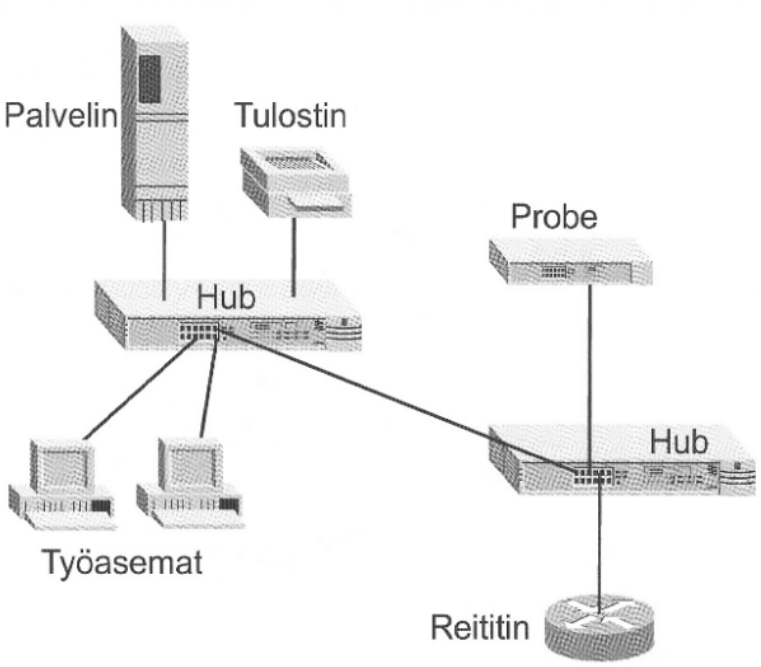
```
user@linux: snmpwalk –v1 –c public localhost mib-2.interfaces.1
IF-MIB::ifNumber.0 = INTEGER: 3
```

Kysely eroaa edellisestä esimerkistä lopussa olevalla ”.1”-tarkenteella, jolla saadaan kohdistettua kysely ifNumber-objektin arvoon. Vastauksen perusteella voidaan todeta, että localhost-koneessa on kolme verkkoliityntää. Laitteessa toimiva agentti on kerännyt ifNumber-objektiin liityntöjen määrän vaikka ne olisivat DOWN-tilassa. (RFC1213.)

3.5 RMON

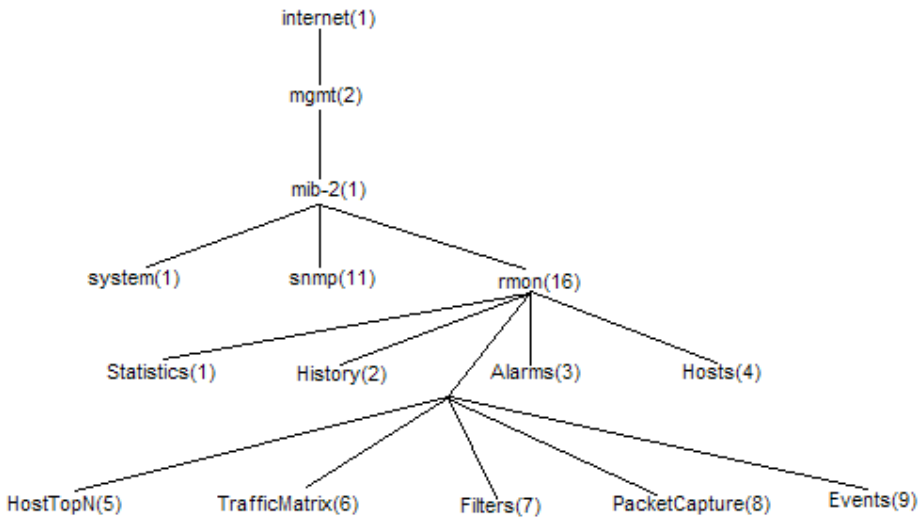
RMON (Remote Monitoring) on määritelty vuonna 1991 julkaistussa standardissa RFC 1271. RMON on kehitetty verkon etähallintaan, jolla voidaan tutkia verkon segmenttien tilaa agenttien avulla, joista käytetään nimitystä keruuyksikkö (probe). Keruuyksikön tehtävänä on pitää jatkuvasti kirjaa verkkoliikenteestä ja tallentaa tiedot myöhempää käyttöä varten. (Jaakohuhta 2005, 316.)

RMON:ia hyödyntävät etenkin tutkainlaitteet, jolloin vian sattuessa voidaan tutkia laitteen keräämää tietoa ja tehdä korjauksia niiden tietojen perusteella, joita RMON-tutkain on kerännyt verkon ollessa toimintakunnossa ja vian ilmettyä verkkoon. Kuviossa 10 on sijoitettu keruuyksikkö niin, että sillä nähdään koko verkon liikenne ja näin voidaan tallentaa tarvittavat tiedot. Vikatilanteessa, jossa palvelimen verkkoyhteys katkeaa ja se ei voi kerätä tietoa verkon laitteilta, voidaan tietoa noutaa keruuyksiköltä myös vian korjauksen jälkeen. (Feldman 1999, 365.)



KUVIO 10. RMON jaetun median lähiverkossa (Jaakohuhta 2005, 317).

RMON:in kehittämisellä haluttiin välttää verkon kuormittamista kyselyillä, joita SNMP tekee kun se pyytää tietoja laitteilta. RMON tallentaa omaan MIB-kantaansa tiedot ja lähettää ne hallinta-aseman niitä kysyessä. Kuviossa 11 on esitetty RMON:in MIB-rakenne, josta käyvät ilmi yleisimmät tiedot, joita tallennetaan myöhempää käyttöä varten. (Jaakohuhta 2005, 318.)



KUVIO 11. RMON:in MIB-rakenne (Jaakohuhta 2005, 318).

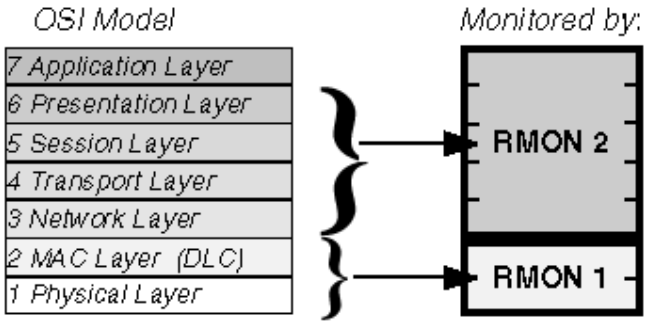
Hallinta-aseman käyttäjä voi tutkia RMON MIB-kantaan kerättyjä tietoja, joiden avulla voidaan selvittää esimerkiksi verkon hidastumiseen vaikuttavia tekijöitä:

- Statistics, ryhmästä saadaan tilastotietoja, joita probe on kerännyt Ethernet verkosta
- History, ryhmästä saadaan tilastollista dataa tapahtumahistoriasta, joita ovat näytteenottoväli ja mittausaika
- Alarms, ryhmästä saadaan laskurien ehtojen mukaisia hälytyksiä
- Hosts, ryhmästä saadaan tietoa lähiverkossa käytössä olevista MAC-osoitteista
- HostTopN, ryhmä kerää tietoa verkkoa eniten kuormittaneista MAC-osoitteista annettujen asetusten perusteella, joita ovat esimerkiksi pakettimäärä, tavut ja virheet
- TrafficMatrix, ryhmä kerää tietoja eri osoitteiden välisestä liikenteestä

- Filters, ryhmä vertaa annettuja ehtoja verkossa liikkuviin paketteihin ja reagoi niihin asetuksien mukaisesti
- PacketCapture, ryhmä kerää kehyksiä verkon liikenteestä ja on sidoksissa Filters-ryhmään
- Event, ryhmä reagoi laitteiden hälytyksiin.

(RFC1757; Jaakohuhta 2005, 319.)

RMON versio2:een on saatu ominaisuuksia joiden avulla saadaan tietoa esimerkiksi OSI-mallin 3-kerroksen liikennemääristä. Lisäksi on tehty ryhmä, jonka avulla saadaan tehtyä Ethernetin MAC-osoitteiden kartoitus. Ominaisuuksista löytyy myös sovelluskerroksen liikennemäärät kustakin verkkokerroksen osoitteesta. Näiden tietojen perusteella voidaan nähdä sovelluskohtaisesti niiden käyttö. Kuviossa 12 on kuvattu RMONv1:den ja RMONv2:den käyttämät kerrokset, joista niillä voidaan kerätä tietoa. (Spurgeon 2001, 426.)



KUVIO 12. OSI-malli RMON:lle (Javvin 2009b).

SMON (Switch Monitoring) -standardi on kehitetty lisäämään RMON-toimintoja. Se on määritelty RFC 2613:ssä vuonna 1999. SMON on osio, jonka avulla saadaan vieläkin tarkempaa tietoa kytkimen läpi kulkevasta liikennemääristä kuin pelkällä RMON-standardilla. Esimerkiksi SMON:lla saadaan VLAN-otsikosta prioriteetti, mitä RMON:lla ei saada valvottua. (RFC2613.)

3.6 CMIP-protokolla

OSI-mallille (Open Systems Interconnection) kehitetyn CMIP (Common Management Information Protocol) -protokollan tarkoituksena on toimia SNMP-protokollan tavoin verkonhallintaprotokollana. CMIP käyttää tietojen keruuseen CMIS (Common Management Information Services) -protokollaa, jonka avulla laitteen agentti ja hallinta-asema voivat vaihtaa tietoja keskenään. SNMP-protokolla käyttää yhteydetöntä tiedonsiirtoa (UDP), kun taas CMIP-protokolla käyttää luotettavaa ja yhteydellistä siirtoa (TCP). Hallinta-aseman ja laitteen agentin väliset viestit protokollissa ovat esiteltynä kuviossa 13.

CMIP	SNMP
get	get
	getnext
set	set
action	set
create	set
delete	set
event-report	trap

KUVIO 13. CMIP- ja SNMP-viestit

CMIP-protokollasta on kehitetty versio myös TCP/IP-mallille. Kyseinen versio on nimeltään CMOT (Common Management Information Services and Protocol over TCP/IP), josta on tarkoitus tehdä varteenotettava kilpailija SNMP-protokollalle TCP/IP-verkkoihin. (Parker 1999, 722.)

CMIP ei kuitenkaan ole saavuttanut suurta suosiota, koska se on hyvin monimuotoinen ja siten hyvin hankala ohjelmoida. Verkonhaltijalta vaaditaan perehtymistä protokollan toimintaa syvällisesti, jotta sitä voidaan hyödyntää kunnolla verkonvalvonnassa. (Software Engineering Institute 2009.)

4 VERKONHALLINTAOHJELMISTOT

4.1 Verkonhallinnan toteuttaminen

Ominaisuuksia joita vaaditaan hyvältä verkonhallintaohjelmistolta, on vaikea määrittää yksiselitteisesti. Ohjelmistolla pitää voida monitoroida eri valmistajien laitteita, jolloin tarvitaan tuki eri valmistajien MIB:eille. Käyttöliittymän kautta tulee selvitä laitteiden tilat ja verkon rakenne. Mitä enemmän verkossa on monitoroitavia laitteita, sitä hyödyllisempi lisä ohjelmistossa on automaattinen laitteiden etsintä. Käyttäjällä tulisi myös olla mahdollisuus vaikuttaa siihen, miten valvontaohjelmisto reagoi verkon laitteiden tilamuutoksiin. (Jaakohuhta & Lahtinen 1997, 508.)

Verkonhallintaohjelmistojen tarkoituksena on helpottaa ylläpidon työtä eikä lisätä sitä. Nykyisin useimmat ohjelmistot tarjoavatkin mahdollisuuden tehdä verkonhallintaan liittyvät konfiguroinnit helposti graafisen käyttöliittymän kautta. Ohjelmistojen tarkoituksena on kerätä tietoa verkon laitteilta, ja niiden perusteella piirtää kuvaajia saaduista tiedoista, joiden avulla voidaan tutkia verkon nykyistä suorituskykyä. (Jaakohuhta & Lahtinen 1997, 506.)

Verkonhallintajärjestelmää hankittaessa tulee aina kartoittaa tavoitteet ennen laitteiden ja ohjelmistojen hankintoja. Ohjelmistot sisältävät työkaluja, joiden avulla voidaan seurata verkon laitteiden tilaa. Valvonnan kannalta olennaisia ovat kriittiset pisteet verkossa, esimerkiksi palomuurilaitteisto, jonka läpi kulkee yrityksen koko tietoliikenne. Monitoroinnissa voidaan seurata kolmea asiaa, joiden perusteella nähdään verkossa tapahtuvat muutokset:

- suorituskyky
- käyntiaika
- saatavuus.

(Feldman 1999, 362.)

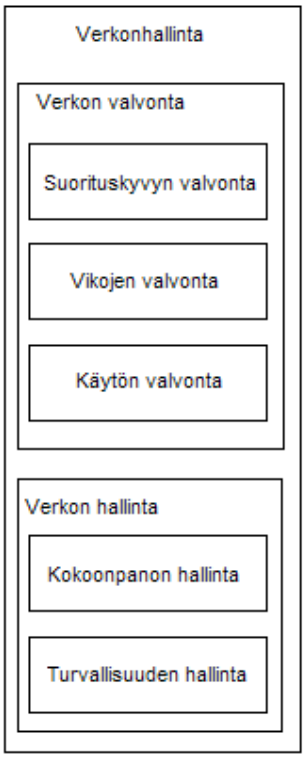
Verkonhallinta ja monitorointi tapahtuvat käyttöliittymän kautta, josta tulee ilmetä verkon laitteiden tilat ja sijainti. Laitetta kuvaavaa ikonia klikkaamalla saadaan

näkyviin tarkempaa tietoa laitteesta. Ikoneita, joilla kuvataan laitteita, tulisi voida vaihtaa halutunlaisiksi kuvakkeiksi. Näin saadaan verkkotopologissa näkymään kuvallinen tieto siitä millainen laite on kyseessä ilman, että tarvitsee klikata kuvaketta. (Jaakohuhta & Lahtinen 1997, 507.)

Työtä helpottavana ominaisuutena ohjelmistossa on automaattinen laitteiden etsintä. Tämän avulla ohjelmisto muodostaa verkkoa kuvaavan kartan verkon laitteista ja niiden välisistä kytkennöistä. Verkkokuvasta käy ilmi, millainen laite on löytynyt ja mikä on sen verkkoliitännän toisessa päässä oleva laite. Laitteiden löydyttyä voidaan konfiguroida ohjelmistoon toimintoja, joilla reagoidaan laitteiden tilan muutoksiin. Voidaan esimerkiksi konfiguroida ohjelmisto ilmoittamaan sähköpostitse ylläpidolle laitteiden tilan muutoksista. (Jaakohuhta & Lahtinen 1997, 508.)

Valvottavien laitteiden tulee sisältää SNMP-agentti, jonka avulla saadaan laitteesta ulos tietoa SNMP-protokollalla. Hallinta-asema kysyy SNMP-viestillä tietoja laitteen agentilta, joka etsii vastauksen kysyttyyn objektiin ja lähettää tiedon vastauksena hallinta-asemalle. Laitteen agentti myös varmistaa, että kyselijällä on oikeus saada kyseisiä tietoja. Varmistus tapahtuu esimerkiksi SNMPv1:ssä yhteisömerkkijonolla, jolloin molempien osapuolten pitää käyttää samaa yhteisömerkkijonoa tunnistamisen onnistumiseksi. (Feldman 1999, 364; Comer 2002, 556.)

Verkonvalvonnan voidaan ajatella olevan verkon tilan seurantaa kun taas hallinnalla voidaan määrittää laitteiden asetuksia. Valvonta on siis laitteiden tietojen lukuprosessi ja hallinta kirjoitusprosessi. Kuviossa 14 on tehty karkea jako valvonnan ja hallinnan välille. (Jaakohuhta & Lahtinen 1997, 504.)



KUVIO 14. Verkonhallinta (Jaakohuhta & Lahtinen 1997, 505).

Standardiprotokollien lisäksi on tarjolla laitevalmistajien omia työkaluja monitorointiin. Ne ovat toimivia ratkaisuja, jos verkko on rakennettu juuri tietyn valmistajan laitteilla, eikä sitä olla laajentamassa muiden valmistajien laitteilla. Esimerkiksi Dell on päätynyt ratkaisuun, jossa se tarjoaa HP OpenView Server Manager -ohjelmasta muokattua versiota, jolla voidaan monitoroida vain Dellin palvelimia. (Feldman 1999, 366.)

Kolmannen osapuolen ilmaisia ja maksullisia ohjelmistoja on tarjolla runsaasti. Valikoimasta pitää vain valita tarpeiden mukainen ja halutun hintainen ohjelmisto. Maksullisissa on usein tuotetuki, jolloin ylläpito saa tarvittaessa apua valmistajalta. Ilmaisia ohjelmia ovat usein avoimen lähdekoodin ohjelmistot, joihin myös osa valmistajista tarjoaa maksullisen tuen. Kolmannen osapuolen ohjelmistot hyödyntävät usein SNMP-protokollaa verkonvalvontaan, koska SNMP:n käyttämä agentti toimii hyvin useiden eri laitevalmistajien laitteissa.

4.2 RRDtool

Käydään aluksi läpi RRDtool (Round Robin Database Tool), koska sitä hyödyntävät opinnäytetyössä vertailtavat verkonvalvontaohjelmistot. RRDtool on sovellus, jonka avulla kerätään tietoa verkon laitteista ja sovelluksista. Kerätyn tiedon perusteella piirretään aikasidonnaisia kuvaajia. RRDtool on avoimen lähdekoodin ohjelmisto, jonka kehittäjä on Tobias Oetiker. RRDtool on saavuttanut lähes standardin aseman tietojen keräämisessä ja piirtämisessä kuvaajiksi aikajanaa vasten. (Oetiker 2009.)

RRDtoolissa luodulle tiedostolle annetaan RRA:ssa (Round Robin Arcives) määritellyt tiedot ajanjaksoille, joista säilytetään tietoa. Suhteellisen vakioiksi ovat muodostuneet kuviossa 15 olevat aikajaksot tiedon säilyttämiselle.

```
1 sample "averaged" stays 1 period of 5 minutes
6 samples averaged become one average on 30 minutes
24 samples averaged become one average on 2 hours
288 samples averaged become one average on 1 day
```

KUVIO 15. RRA:n käyttämät oletus ajankohdat tiedon tallentamiselle (Bogaerdt 2009).

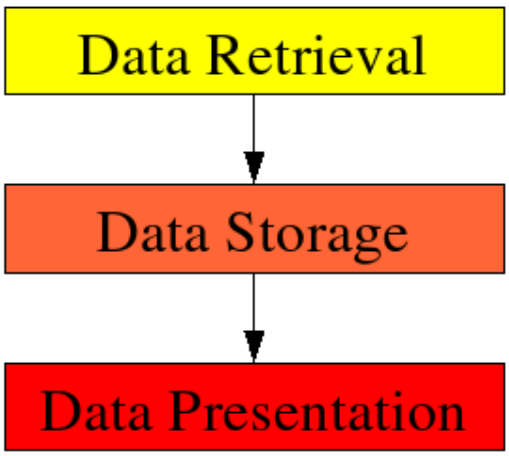
Käytettäessä tiedon tallennukseen RRA:n tapaa voidaan varmistaa, että tietokanta ei tule kasvamaan vuosien saatossa, jos kerättävät kohteet eivät muutu. Tietokannassa pidetään tallessa maksimissaan vuoden takaista tietoa. Näin kerätyistä ja tallennetuista tiedoista voidaan piirtää kuvaajia esimerkiksi laitteen prosessien määrästä viimeisen 24 tunnin ajalta 5 minuutin keskiarvolla sekä viimeisen vuoden ajalta päivän keskiarvolla. Kuvaajissa käytettävää tietoa voidaan yhdistää, piirtää käyriä eri väreillä ja voidaan käyttää myös hyvin monia muita mahdollisuuksia luoda kuvaajista halutunlaisia. (Bogaerdt 2009.)

4.3 Cacti

Cacti on avoimen lähdekoodin verkonvalvontaohjelmisto, jolla voidaan monitoroida verkon laitteita ja niiden sovelluksia. Käyttäjien oikeuksien määrittely ja laitteiden monitoroinnin hallinta tapahtuu www-selaimen kautta. RRDtoolin avulla voidaan piirtää kuvaajia käyttäjälle ja tiedot tallennetaan MySQL-tietokantaan. (Cacti 2009a.)

Cacti-ohjelmisto tarvitsee toimiakseen seuraavat ohjelmat: RRDtool, MySQL, PHP ja www-palvelimen kuten Apache. Laitteistovaatimuksista valmistaja ei anna tarkkoja tietoja, esimerkiksi kuinka tehon ja muistin tarve kasvaa monitoroitavien laitemäärien kasvaessa. (Cacti 2009a.)

Hallintasivut on toteutettu PHP-kielellä, jolloin käyttäjä voi myös halutessaan muokata hallintanäkymää toivotunlaiseksi. Cacti hyödyntää crontab polleria ajastuksiin, joilla laitteilta kerättyä tietoa näytetään käyttäjille kuvaajan muodossa. Tietojen siirto Cactissa voidaan jakaa kolmeen ryhmään kuvion 16 mukaisesti.



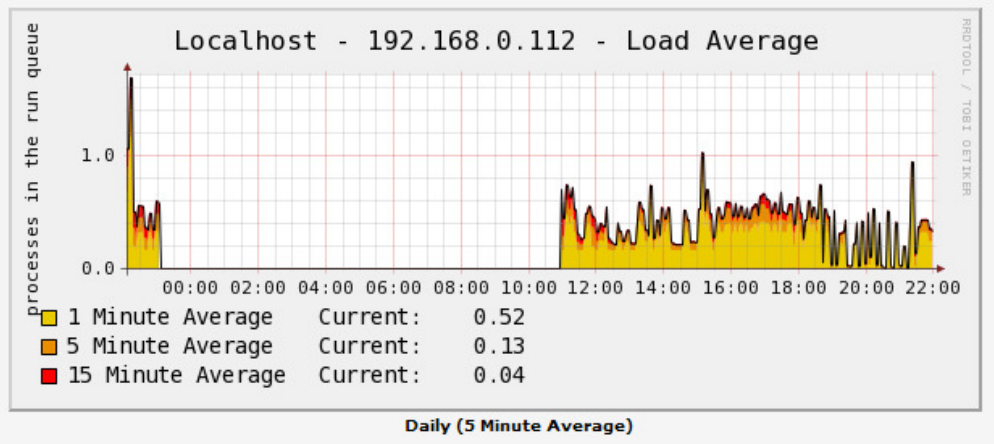
KUVIO 16. Cactin tietojen siirto (Cacti 2009b).

Tiedon hankintaan (Data Retrieval) varten Cactissa voidaan määritellä omia Data Queries -kyselyjä tai käyttää valmiita templates-pohjia. Templates-pohjista SNMP - Interface Statistics on hyödyllinen ja käyttökelpoinen lähes kaikille laitteille. Sillä saadaan laitteesta tietoa verkkoliitynnöistä kuten nimi, nopeus, MAC- ja IP-

osoitteet. Tietoa kysellään laitteilta halutuin väliajoin cmd.php:n avulla. Yleisin käytetty aika kyselyiden välillä on 5 minuuttia, ja muita valmiiksi ohjelmoituja aikajaksoja ovat esimerkiksi: 10, 20 ja 60 sekuntia. (Cacti 2009b.)

Tiedon tallennuksessa (Data Storage) Cacti käyttää RRDtoolia tiedon tallentamiseen rrd-tiedostoiksi. Jokaisesta laitteesta tallennetaan jokaista kyselyä vastaava tiedosto, jolloin yhtä laitetta varten voi olla kymmenkunta eri tiedostoa. Tietojen perusteella voidaan piirtää kuvaajia, joissa näkyy esimerkiksi päivän keskiarvo viimeisen vuoden jokaiselle päivälle liikennemääristä yhdessä liitynnässä. (Cacti 2009b.)

Tietojen esittämiseen kuvaajina (Data Presentation) Cacti käyttää crontab ajastustoimintoa. Siinä määritetään suoritettavaksi poller.php esimerkiksi 5 minuutin välein, jonka avulla piirretään halutut rrd-tiedostot www-sivuille. Kuviossa 17 on esimerkki localhostin kuormituksen kuvaajasta. Siitä näkee localhost-koneen kuormituksen määrän 1-, 5- ja 15 minuutin keskiarvoilla viimeisen vuorokauden aikana. (Cacti 2009b.)



KUVIO 17. Localhost Load Average -kuvaaja

Cactin hallintasivujen kautta voidaan lisätä käyttäjiä, joille voidaan esimerkiksi antaa vain katseluoikeus sivustolle. Käyttäjätunnus, jolle on määritelty ”admin”-oikeudet, voi www-sivujen kautta hallita Cactiin liittyviä asioita, kuten laitteen lisäys, kuvaajien lisäys laitteille ja käyttäjien lisäys ja poisto. Cactissa ei ole va-

kiona sähköpostin lähetystä laitteiden tilamuutoksista, vaan joudutaan asentamaan lisäosio ohjelmistoon. (Cacti 2009b.)
Cacti-ohjelmistolla voidaan luoda hyvin tietorikkaita kuvaajia monitoroitavista laitteista ja niiden prosesseista. Tietoturva on huomioitu, joten voidaan käyttää SNMP-protokollasta haluttua versiota. Laitteen tukiessa SNMPv3-versiota on suositeltavaa käyttää sitä, koska silloin viestien tietoturvataso on korkeimmillaan. Cactin käyttäjien hallinta tapahtuu lisäämällä käyttäjä ja antamalla sille halutut oikeudet hallintasivuille. Cactin hyvänä puolena voidaan pitää sen maksuttomuutta, joten sen käyttö verkonvalvontaan on kiinni verkon ylläpitäjästä eikä ohjelman hankintahinta muodostu esteeksi.

4.4 Zenoss

Zenoss Core (myöhemmin pelkkä Zenoss) on avoimen lähdekoodin ohjelmisto verkonvalvontaan. Hallinta tapahtuu www-käyttöliittymän kautta, jonka avulla voidaan valvoa verkkoa, luoda haluttuja raportteja tuloksista ja hyödyntää niitä verkon tarpeiden kartoituksessa. Zenoss on kirjoitettu Python-kielellä ja se hyödyntää Zope-palvelintoimintoa. (Zenoss 2009.)

Zenoss-ohjelmiston vaatimukset asennustyypin perusteella on esitetty kuviossa 18.

Asennus tyyppi	**Käyttöjärjestelmä**
Virtual Appliance	Windows
	Linux
Binary Installer	Red Hat Enterprise Linux 5
	Fedora Core 6
	SUSE
Source	Ubuntu
	FreeBSD
	Solaris 10
	Mac OS X
	Other Linux environments

KUVIO 18. Zenoss-ohjelmiston vaatimukset (Badger 2008, 3).

Käytettäessä Virtual Appliance -asennusta ei tarvitse asentaa muita lisäosia ohjelmistoon, mutta tehtäessä binary -asennusta tarvitsee lisäksi asentaa MySQL ja Python sekä molempien kehitystyökalut. Asennettaessa lähdekoodiversiota tarvitsee lisäksi asentaa SWIG, Autoconf ja SNMP.

Laitteistovaatimukset määräytyvät monitoroitavien laitteiden määrän mukaan seuraavasti:

- monitoroitavia laitteita alle 250 kappaletta
  - 4GM RAM
  - Core 2 Duo E6300 1.86/1066 RTL
  - 75 GB kovalevytilaa.
- monitoroitavia laitteita yli 250 kappaletta
  - 8GB RAM
  - XEON 5120 DC 1.86/1066/4Mb
  - 4 kpl 75GB kovalevyjä, jotka asennetaan kahtena RAID-1-parina.

  (Badger 2008, 3.)

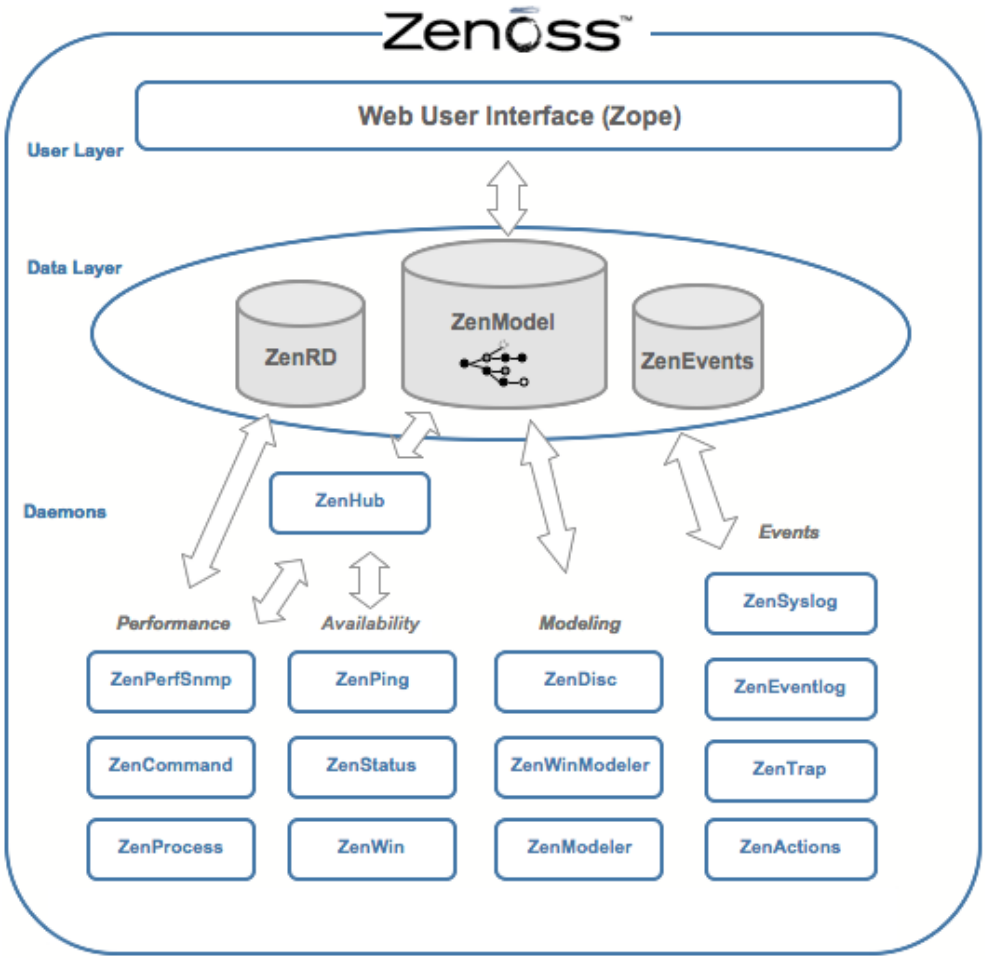
Zenoss-ohjelmisto tarjoaa mahdollisuuden ylläpidolle tehdä seuraavanlaisia toimintoja verkossa:

- laitteiden hallinta
- laitteiden tilat ja suorituskyvyn monitorointi
- tapahtumien hallinta
- raporttien luonti
- käyttäjien ja hälytysten hallinta.

(Badgre 2008, 9.)

Laitteiden hallintatiedot tallennetaan CMDB (Configuration Management Database) -tietokantaan, johon laitetiedot voidaan lisätä yksittäin tai auto-etsimen avulla. Lisäyksen jälkeen voidaan saada laitteelta vastauksia haluttuihin SNMP-kyselyihin, kunhan oikeudet on määritelty oikein. Laitteet voidaan lisäyksen jälkeen siirtää haluttuihin paikkoihin järjestelmässä. Esimerkiksi palvelimet voidaan sijoittaa server-device -kohtaan. (Badger 2008, 18.)

Zenoss-arkkitehtuuri on yksinkertaistaen jaettavissa kolmeen kerrokseen: käyttäjä (User Layer), tieto (Data Layer) ja keräys (Daemons). Näiden yhteydet on kuvattu kuviossa 19.



KUVIO 19. Zenoss-arkkitehtuuri (Zenoss 2009).

Käyttäjälle näkyvin kerros on User Layer, jonka näkymä avautuu kun otetaan yhteys Zenossiin www-selaimella. Kirjautumisen jälkeen voidaan hallita sen mukaan, mitä verkon laitteita valvotaan ja näin saadaan ylläpidolle tietoa laitteiden tilasta. Www-sivun kautta tapahtuva hallinta on mahdollista AJAX-liitynnän ansiosta, joka perustuu Zope-sovellukseen. Zope on avoimen lähdekoodin www-palvelintoiminto. User Layer on vuorovaikutuksessa Data Layeriin ja muuntaa saadut tiedot käyttöliittymän tiedoiksi. (Badger 2008, 15; Zenoss 2009.)

Data Layer on kerros, jossa kaikki systeemin tiedot ovat tallessa. Tässä kerroksessa on ohjelmiston ydin, ja se sisältää esimerkiksi:

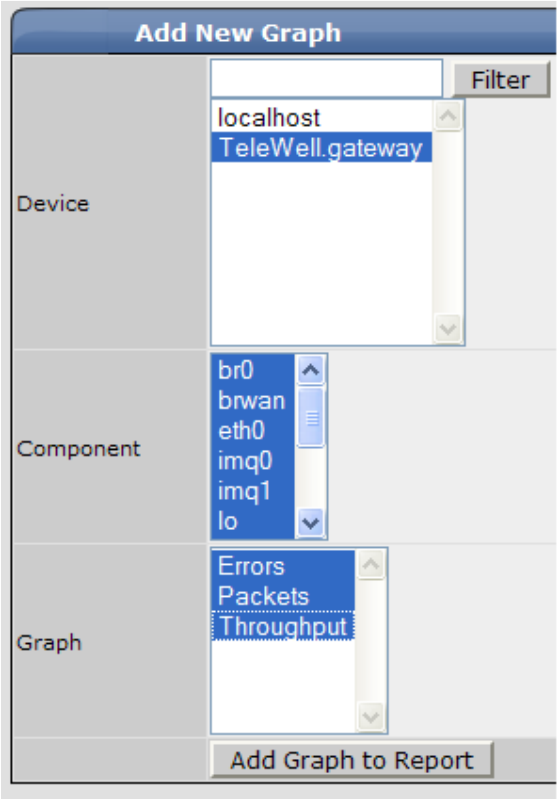
- zeoctl, joka huolehtii tietokantaan hallinnassa konfiguroidut tiedot
- zenrRRD, joka kerää tietoa aikajanaa vasten, kuten RRDtool
- zenevents, joka on vuorovaikutuksessa MySQL-tietokannan tapahtumien kanssa
- zenmodel, joka on yhteinen konfigurointimalli Zope-objekti tietokannalle.

(Zenoss 2009.)

Laitteiden tilan ja suorituskyvyn seurantaan voidaan käyttää ICMP (Internet Control Message Protocol) -protokollaa ja tietojen keräämiseen SNMP-protokollaa. Zenoss luo verkkokuvan verkosta kyselyillä saatujen reititystaulujen perusteella jossa näkyy laitteet ja mihin kukin laite on suoraan yhteydessä. Zenoss-ohjelmistoon voidaan myös yhdistää Google Maps-toiminto, jolloin voidaan seurata laajalla maantieteellisellä alueella olevien laitteiden tilaa kartan avulla. (Zenoss 2009.)

Raportin luonti on tehty hyvin helpoksi ylläpidolle. Kun halutaan luoda esimerkiksi graafinen raportti laitteen tai laitteiden porttien liikenteestä, valitaan vain halutut laitteet, niiden liitynnät ja mitä liitynnöistä monitoroidaan. Liian montaa tietokohdetta ei kannata valita yhteen raporttiin, koska raporttien lukemien muuttuu hankalaksi, jos kuvaajia on kovin pitkä lista.

Kuviossa 20 on valittu raporttia varten TeleWell.gateway -niminen laite, josta on valittu kaikki liitynnät ja liityntöjen kaikki liikenne piirretään kuvaajiksi. Esimerkissä valittiin yksi laite ja saadaan luotua 32:n kuvaajan raportti, joten raporttia luodessa on syytä miettiä tarkkaan, mitä tietoa todella tarvitaan raporttiin.



KUVIO 20. TeleWell.gateway -laitteen graafisen raportin luonti

Palvelinohjelmia, joita Zenoss käyttää, voidaan hallita www-sivujen kautta. Sieltä voidaan esimerkiksi muuttaa ohjelman asetuksia, tutkia lokeja tai käynnistää haluttu palvelinohjelma uudelleen. Lisäksi nähdään tilatieto-kohdan avulla onko palvelu toiminnassa vai ei.

Zenossin tärkeimpiä ominaisuuksia, jotka helpottavat tietoliikenneverkon ylläpitoa, ovat:

- autoetsin-toiminto, jolla saadaan kerättyä halutusta IP-avaruudesta laitteiden tyypit ja niiden tarkat tiedot
- monitorointi, jolla saadaan tietoa laitteiden ja palveluiden tiloista
- suorituskyvyn monitorointi, reaaliaikaista tai historiatietoa suorituskyvystä ylläpidolle
- tapahtumien ja lokien hallinta, joilla kerätään tietoa esimerkiksi laitteiden tapahtumista

- hälytysten hallinta, jolloin voidaan määrittää, että lähetetään sähköposti ylläpidolle kun esimerkiksi laite on DOWN-tilassa
- www-hallintaliittymä, jolla hallitaan kaikki yllämainitut toiminnot sekä, käyttäjien oikeudet ja näkymien hallinta.

(Zenoss 2009.)

Zenoss-ohjelmistoa käytettäessä voidaan luoda hyvin nopeasti perusympäristö ylläpidolle hallittavasta verkosta. Laitteet voidaan etsiä automaattisella etsimellä, jolloin ei tarvitse syöttää laitteita yksitellen, ja niistä saadaan näkymään perusasetuksilla verkkoliitynnät. Löydetyistä laitteista ohjelmisto voi piirtää verkkokartan. Käyttäjien lisäys ja niiden oikeuksien määrittely tapahtuu helposti hallintasivuilta. Lisäksi voidaan käyttää SNMP-protokollan eri versioita, jos laitteesta löytyy niille tuki. Zenoss on ilmainen, joten sillä voidaan kokeilla verkonhallintaa hyvin pienin kustannuksin.

4.5 Nagios

Nagios on avoimen lähdekoodin ohjelmisto, jonka kehittäjä on Ethan Galstad. Nagios on Unix-pohjainen monitorointiohjelmisto, jossa on www-liittymä tietojen katseluun. Laitteet konfiguroidaan kuitenkin komentoriviltä muutamiin tiedostoihin. Verkkoon kytketyllä laitteella pitää olla IP-osoite, jotta Nagios tunnistaa sen, jolloin laitetta tai sen sovellusta voidaan monitoroida TCP/IP-arkkitehtuurissa. (Turnbull 2006, 20.)

Nagios voidaan asentaa Linux-käyttöjärjestelmään (tai Unix) ja C -kääntäjä pitää olla asennettuna. Lisäksi tarkistetaan TCP/IP-asetukset, koska palvelut vaativat verkon toimivan oikein. Laitteistovaatimukset kasvavat monitoroitavien laitteiden määrän kasvaessa. Taulukossa 1 on havainnollistettu, kuinka monitoroitavien laitteiden määrä vaikuttaa laitteistovaatimuksiin.

TAULUKKO 1. Nagioksen laitteistovaatimukset (Trunbull 2006, 4).

# Monitoroitavien laitteiden määrä	Prosessori kpl	Prosessorin nopeus	Muistin määrä	Kovalevyn kapasiteetti
< 100	1	800 MHz+	512MB+	5GB+
100 - 500	1	1GHz+	1GB+	10GB+
500 - 1000	1+	3GHz+	1GB+	20GB+
> 1000	1+	3GHz+	2GB+	40GB+

Valvottavassa laitteessa voi olla Microsoft Windows- tai Unix-pohjainen käyttöjärjestelmä, jolloin siitä voidaan saada tietoja esimerkiksi muistin käytöstä ja kiintolevyn kapasiteetistä. Valvontayhteyksiin voidaan käyttää HTTP, SNMP ja SSH (Secure Shell) protokollia. (Trunbull 2006, 20.)

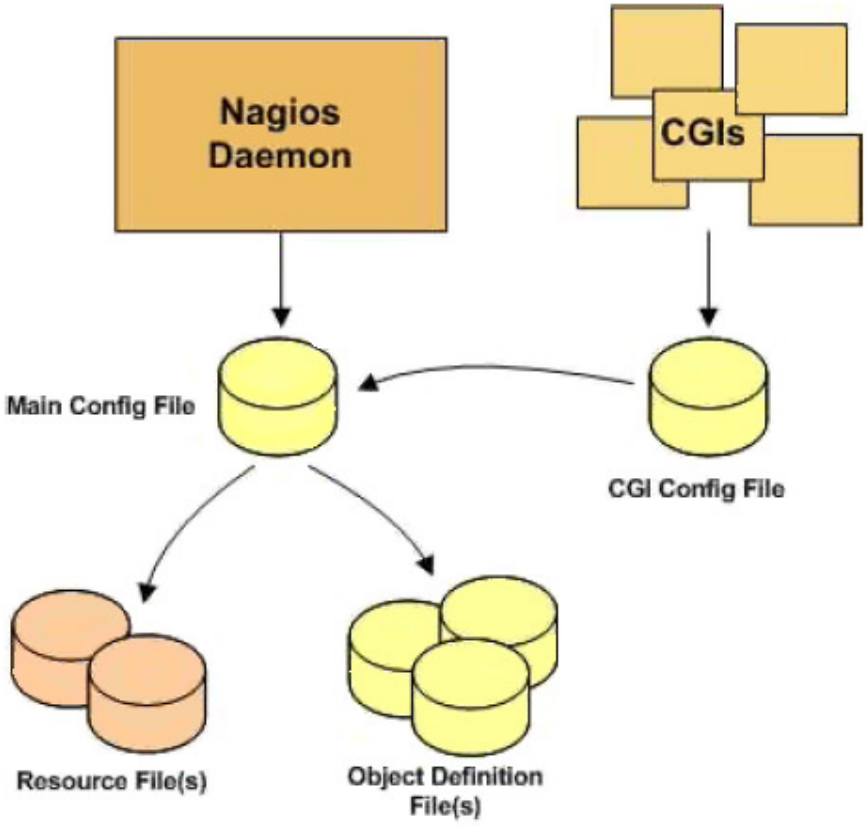
Nagios-ohjelmistolla voidaan valvoa esimerkiksi seuraavia asioita:

- verkon palvelut, joita ovat esimerkiksi: SMTP, POP3, WWW, DNS
- laitteiden käyttämät resurssit, joita ovat esimerkiksi prosessorin kuormitus ja muistin käyttö
- automaattinen lokien luonti valvottavista tapahtumista
- Nagios voi myös lähettää ylläpidolle tietoa laitteiden tilan muutoksista.

(Galstad 2008.)

Nagioksen konfiguroitavia tiedostoja ja niiden yhteyksiä on esitetty kuviossa 21.

- Main Configuration File, tässä tiedostossa määritellään kuinka Nagios toimii. Tiedosto on nimeltään nagios.cfg, ja sinne määritellään esimerkiksi mitä konfigurointitiedostoja käytetään ja kuinka usein tilatiedot päivitetään.
- Resource File sisältää tiedot käyttäjän määrittämistä makroista. Suurin hyöty on että CGI:n (Common Gateway Interface) kautta ei voi saada salasanoja näkyviin.
- Object Definition Files, jossa määritellään laitteet, palvelut, yhteystiedot ja monia muita asioita joita halutaan käyttää monitoroinnissa ja siitä tehtävissä ilmoituksissa.
- CGI Configuration File, jossa määritellään kuinka käyttöliittymä näkyy ja toimii käyttäjille.



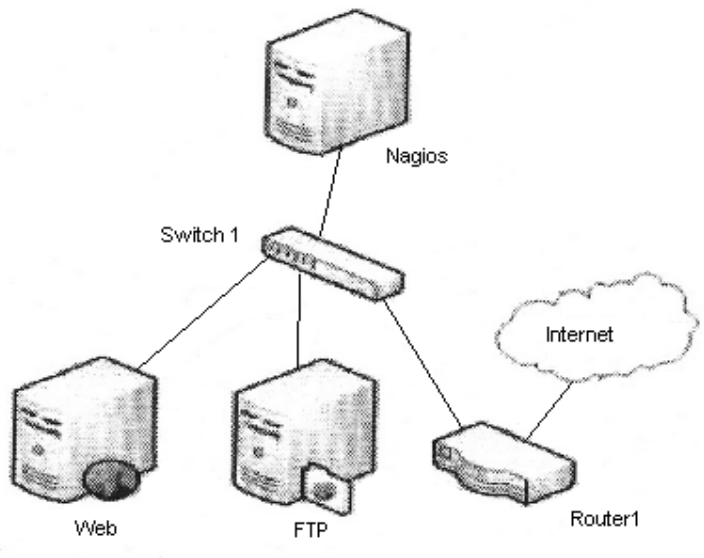
KUVIO 21. Nagioksen konfiguroitavien tiedostojen väliset yhteydet (Galstad 2008).

Verkkoon kytketyt laitteet, jotka vaikuttavat verkkokartan verkkotopologiaan, voidaan lisätä konfiguroimalla ne host.cfg-tiedostoon. Lisäämällä määrityksiin parents-kohta, saadaan laitteiden DOWN ja UNREACHABLE -tilat monitoroitua. (Galstad 2008.)

Kuviossa 22 olevan verkkokuvan tilatietojen esittämiseksi oikein Nagiokseen tarvitsee tehdä seuraavan esimerkin mukaiset asetukset host-tiedot määrittävään tiedostoon.

```
define host{
        host_name    Nagios
        }
define host{
        host_name    Switch1
```

```
                parents         Nagios
                }
define host {
                host_name       Web
                parents         Switch1
                }
```



KUVIO 22. Nagios parents -yhteydet (Galstad 2008).

Esimerkin mukaiset määrittelyt onnistuvat vielä hyvin kun verkon koko ei ole kovin suuri, eikä siinä tapahdu muutoksia. Nyt Nagios osaa kertoa tilatiedoilla onko jokin laite DOWN vai UNREACHABLE -tilassa. Tästä on suuri apu kun ylläpito selvittää mistä kohtaa verkkoa vika mahdollisesti löytyy. Jos verkossa oleva Switch1 menisi DOWN-tilaan, niin Nagios määrittäisi Web, FTP ja Router1 laitteiden tilaksi UNREACHABLE, koska niihin ei voida saada yhteyttä Switch1-laitteen ollessa DOWN-tilassa. (Galstad 2008.)

Nagioksen käyttämät tilat ja niiden merkitys verkon laitteille ovat:

- UP, vastaa kyselyyn
- DOWN, ei vastaa kyselyyn oikein ja on verkkotopologia huomioiden ensimmäinen laite mikä ei vastaa Nagioksen lähettämiin kyselyihin

– UNREACHABLE, ei saada yhteyttä, koska konfiguroinnissa laitteelle määritelty parents on DOWN-tilassa.

(Galstad 2008.)

Nagios luo verkkokuvan, josta voidaan värien perustella todeta, missä tilassa kukin laite on, kun kartta on päivitetty viimeisen kerran. Ohjelmiston luoma kartta on PNG-kuvatiedosto, ja jokaiselle laitteelle voidaan konfiguroida oma kuvake. Kartasta saadaan myös kolmiulotteinen näkymä, jos sellaista halutaan käyttää. Kolmiulotteisen kartan toiminta selaimessa vaatii VRML (Virtual Reality Modeling Language) -tuen asentamisen. Tämän jälkeen voidaan hallintasivulta tutkia verkon topologiaa eri suunnista, mutta tämä ominaisuus ei ole välttämätön Nagioksen toiminnan kannalta. (Galstad 2008.)

Nagios tarvitsee lisäosion esimerkiksi kun halutaan monitoroida SNMP-protokollan avulla laitteita. Nagios-ohjelmisto lähettää check_snmp -lisäosion avulla SNMP-protokollakyselyn verkon laitteelle. Laitteen agentti etsii kysyttyä OID:ia vastaavan tiedon MIB-kannasta ja lähettää vastauksen Nagiokselle. Jos Nagioksen halutaan piirtävän kuvaajan saadulle vastaukselle, tarvitsee olla asennettuna check_mrtgtraf -lisäosio, jonka avulla luodaan kuvaaja kyselyn perusteella. (Galstad 2008.)

Nagioksen käyttöönotto ja perehtyminen ohjelmiston konfiguroitaviin tiedostoihin vaatii aikaa, jotta saadaan luotua halutut tiedot ohjelmistoon. Tiedostoihin määritellään verkon laitteet, millaista tietoa monitoroidaan laitteista ja määritetään käyttäjien oikeudet. Laitteiden tietojen kyselyyn voidaan käyttää SNMP-protokollan eri versiota. Ohjelmistoon asennettavien lisäosien avulla voidaan monitoroida hyvin monipuolisesti verkon laitteita.

4.6 Groundwork

Groundwork on avoimen lähdekoodin ohjelmisto, ja sillä voidaan valvoa verkkoon kytkettyjä laitteita ja niiden sovelluksia. Saatavilla on kolme eri versiota: Community Edition Alpha, Professional ja Enterprise, joista Groundwork Monitor Commuity Edition Alpha valittiin, koska se on ilmainen. Ohjelmistoon on yhdistetty monia muitakin avoimen lähdekoodin sovelluksia, joista voidaan mainita Nagios, RRDtool ja nmap. Jos verkkoa on valvottu aikaisemmin Nagios-ohjelmistolla, niin sen asetukset voidaan siirtää Groundworkin asetuksiin. (GroundworkOpenSource 2009.)

Groundwork Community Edition toimii seuraavissa käyttöjärjestelmissä:

- Red Hat Linux Enterprise Linux 4 ja 5
- CentOS 5
- Novell Suse Linux Enterprise Server (SLES) 10
- Ubuntu 6.06 Server LTS
- Debian 4.

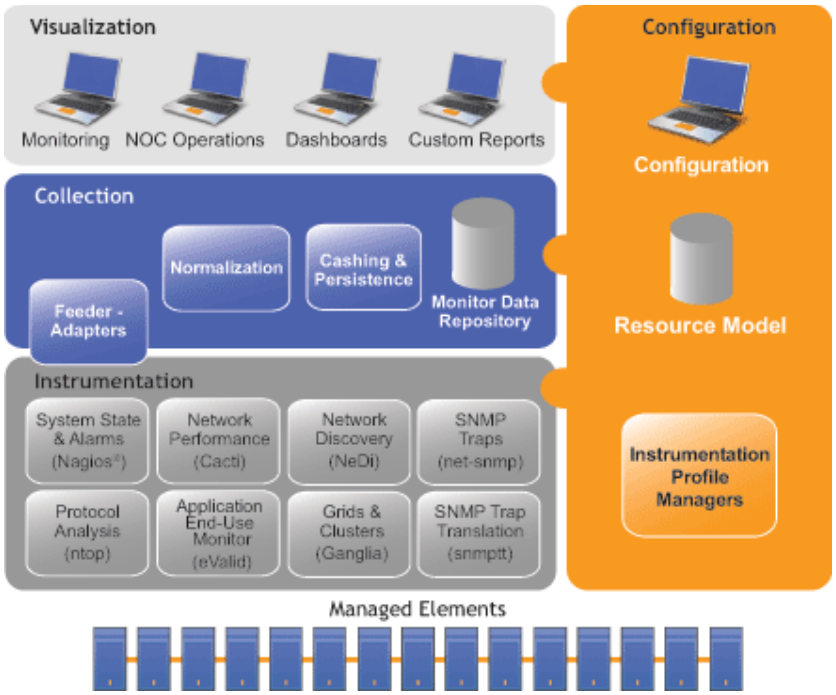
(GroundworkOpenSource 2009.)

Laitteistovaatimukset riippuvat valvottavien laitteiden määrästä, mutta vähimmäisvaatimuksena alle 150 laitteen monitorointiin ovat:

- 2GB RAM
- 1 prosessori, 2.8GHz P4 tai parempi
- 80GB kiintolevytilaa.

(GroundworkOpenSource 2009.)

Groundwork on oikeastaan kokoelma avoimen lähdekoodin ohjelmistoja, joita hyödynnetään yhdistämällä ne yhteen ohjelmistoon. Arkkitehtuurista on kuva kuviossa 23, josta käy ilmi mitä Groundwork hyödyntää valvontaan. Tietoa laitteilta voidaan kerätä useilla välineillä, joissa hyödynnetään esimerkiksi SNMP-protokollaa. Saatu tieto tallennetaan tietokantaan, josta sitä voidaan hakea ja näyttää ylläpidolle.



KUVIO 23. Groundwork-arkkitehtuuri (GrounworkOpenSource 2009).

Groundwork-ohjelmistolla voidaan myös luoda hallittavasta verkosta verkkokartta automaattisen laitteiden etsimen avulla. Hallittavasta verkosta voidaan esimerkiksi monitoroida tiettyjen laitteiden prosesseja. Kyselyihin voidaan käyttää SNMP-protokollan eri versioita. Käyttäjien oikeuksia voidaan konfiguroida hallintasivujen kautta, jossa määritetään esimerkiksi kenelle lähetetään sähköposti laitteiden tilamuutoksista.

4.7 Kaupalliset ohjelmistot

Valmistajien omille tuotteilleen tekemiä ohjelmistoja verkonvalvontaan löytyy useilta valmistajilta. Dell on tehnyt omille palvelimilleen sopivan ohjelmiston muokkaamalla HP Open Viewin Server Manageria. Ohjelmassa ei sinänsä ole mitään vikaa, mutta jos verkkoon kytketään muiden valmistajien palvelimia, tarvitsee niille hankkia oma ohjelmisto, koska niitä ei voida monitoroida Dellin ohjelmiston avulla. Samanlaisia sidoksia löytyy myös muilta suurilta valmistajilta. (Feldman 1999, 366.)

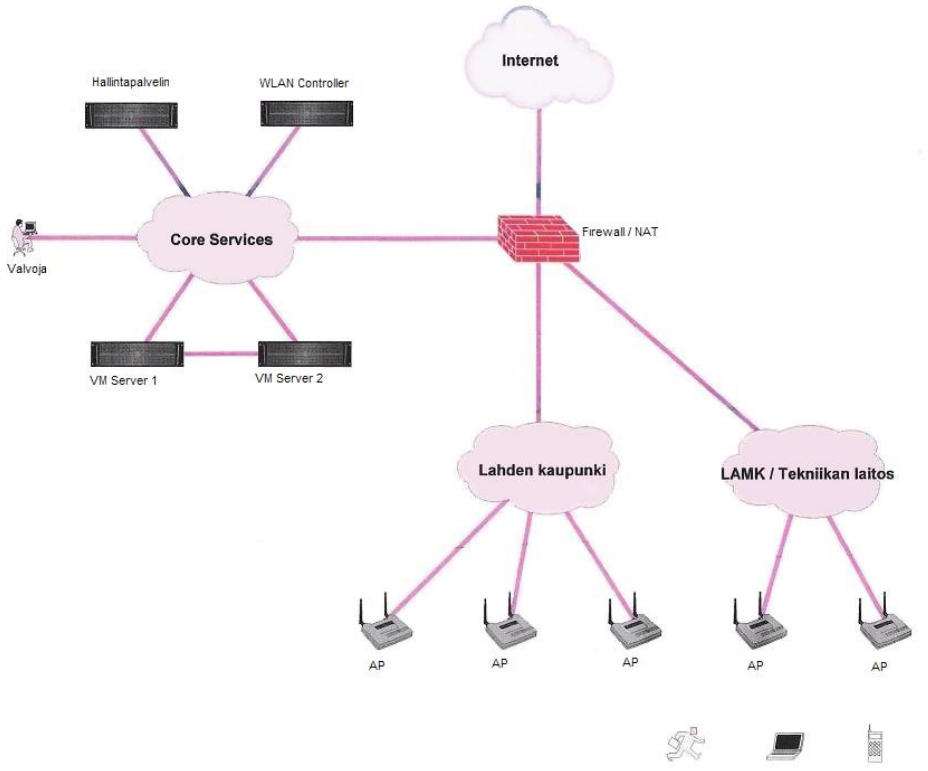
Maksullisten ohjelmistojen hyvänä puolena voidaan pitää niille saatavaa tukea, jota valmistajat tarjoavat viikon jokaiselle päivälle. Ilmaisia ohjelmistoja käytettäessä joudutaan usein turvautumaan ohjelmiston tekijän keskustelupalstoihin ongelmia ratkottaessa.

Maksullista ohjelmistoa verkonhallintaan myy esimerkiksi Castle Rock Computing, Inc. Heidän tarjonnastaan löytyy verkonhallintaan SNMPc7.1 Network Manager, josta on tarjolla kaksi versiota SNMPc Enterprise Edition ja SNMPc Workgroup Edition. Molemmista versioista löytyvät tärkeimmät toiminnot verkonhallintaan, joilla voidaan monitoroida SNMP-protokollalla laitteita. Kyselyihin voidaan käyttää kaikkia kolmea eri versiota SNMP:stä. Sähköpostiin voidaan lähettää ilmoituksia ja lisäksi löytyy hyvin paljon muita ominaisuuksia. Ohjelmisto ei täten paperilla eroa työssä vertailtavista ohjelmistoista ominaisuuksiltaan. Käytännön testit tosin voisivat tuoda ohjelmasta esille joitain ominaisuuksia, mitä tuotteen esitteessä ei kerrottu. Tässä opinnäytetyössä oli tavoitteena tutkia ilmaisia verkonhallintaohjelmistoja, joten kaupalliset ohjelmistot rajattiin tarkemman tarkastelun ulkopuolelle. (Castle Rock Computing 2009.)

5 KÄYTÄNNÖN TOTEUTUS

5.1 Ympäristön kuvaus

MASTONET-verkko koostuu tukiasemista, palvelimista, kytkimistä ja käyttäjien laitteista. LAMK:lle asennetaan palvelimet, joissa toimivat verkonvalvonta, nimipalvelut ja verkon liikenteen suodatus. Tässä työssä toteutetaan verkonvalvonta. Tietoverkon liikenne kulkee myös Lahden kaupungin verkossa ja on erotettu siellä omaksi VLAN:iksi. Ohjeissa tai työssä ei käytetä MASTONET-verkon salasanoja, IP-osoitteita tai muita verkon tietoturvaa heikentäviä merkintöjä. Kuviossa 24 on kokoukseen syksyllä 2008 tehty hahmotelma verkosta ja sen laitteista. Opinnäytetyötä tehdessä olivat käytössä VM Palvelimet, joissa verkonvalvontaohjelmistot toimivat. Lisäksi palomuuri erotti verkonvalvontapuolen eri IP-avaruuteen kuin hallittavat laitteet. Palvelimelta ei ollut yhteyttä Internetiin työtä tehdessä, mutta yhteys saadaan kunhan palvelimet sijoitetaan lopulliseen paikkaan.



KUVIO 24. Yleinen kuva verkosta (Mastonet kokous Jari Utriainen).

Valvottavat laitteet verkossa ovat langattomia tukiasemia. Lähes kaikki laitteet ovat ethernet-liitynnässä kiinni, mutta osa tukiasemista on langattoman linkin takana. Tällä ei ole vaikutusta laitteiden valvonnan kannalta. Tukiasemia verkossa on 84 kappaletta ja niiden tyypit ovat: Orinoco AP1000, AP2000, AP600 ja AP700. Katoilla olevat laitteet ovat yleensä AP1000- ja AP2000-mallisia. Rakennusten sisätiloissa on käytössä useimmiten AP600- ja AP700-mallit, joissa on oma sisäinen antenni. Tukiasemiin on liitetty ulkoinen antenni, jolla kohdistetaan kuluvuus tietylle alueelle. Käytössä on myös ympärisäteileviä antenneja, joilla kantama ei ole yhtä hyvä kuin suunta-antenneilla, mutta saadaan kuuluvuus jakautumaan tasaisesti ympäristöön. Verkon peittoalue on suhteellisen laaja, joka on kuvattu liitteessä 8. Kuuluvuusmittaus on tehty vuonna 2005, joten joitain muutoksia kuuluvuuteen on voinut tulla vuosien kuluessa.

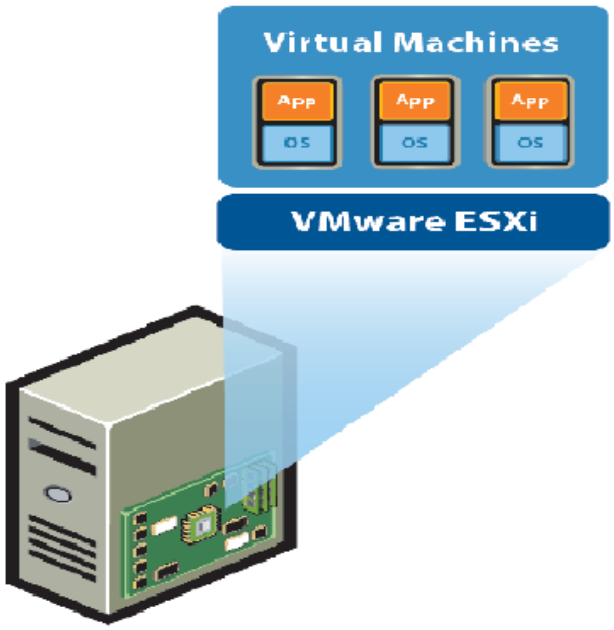
Ohjelmistojen lopullinen asennus suoritettiin virtualisointiympäristöön, mutta testivaiheessa käytettiin tavallisia pöytätietokoneita ohjelmistojen asennukseen ja käytön hallinnan testaamiseen. Tähän ratkaisuun päädyttiin, koska palvelimet eivät olleet vielä saatavilla testivaiheessa.

Lopulliset asennukset verkonvalvontaohjelmistoista asennettiin Dell PE2950III -palvelimeen. Verrattaessa laitteiston suorituskykyä verkonvalvontaohjelmistojen vaatimuksiin, voidaan niiden todeta riittävän nykyisen verkon ylläpitoon asennettaville ohjelmistoille mainiosti. Seuraavassa palvelimen tarkemmat tiedot:

- palvelin Dell PE2950III
    - 16GB keskusmuistia
    - 2 kpl Intel® Xeon® E5240 2.5GHz, 4 core
    - 4 kpl 146GB kiintolevyjä (RAID-0).

Palvelimeen asennettiin VMwaren ESXi-virtualisointipalvelin, jolla voidaan hyödyntää usealle samanaikaisesti ajossa olevalle käyttöjärjestelmälle samoja laiteresursseja. ESXi-palvelimessa voidaan ajaa myös VMware Workstation -ohjelmalla luotuja virtualikoneita, joihin on asennettu käyttöjärjestelmä ja halutut sovellukset. ESXi-palvelimessa valitaan haluttu virtualikone, joka käynnistää käyttöjärjestelmän. Kuviossa 25 on palvelin jossa toimii ESXi-ohjelmisto. Ohjelmis-

tossa ajetaan kolmea eri käyttöjärjestelmää ja jokaisessa niissä voidaan suorittaa omia sovelluksia.



KUVIO 25. ESXi-ohjelmistojen periaate (VMware 2009).

Virtualisoinnissa voidaan tehdä helposti varmuuskopio asennetusta ympäristöstä kun se on saatu toimintakuntoon. Näin voidaan helposti palata alkutilanteeseen, jos jostain syystä käytössä oleva käyttöjärjestelmä lakkaa toimimasta. Tästä johtuen olisi hyvä ottaa varmuuskopio myös valvontajärjestelmän keräämästä tiedosta määräajoin, jolloin ei menetetä arvokasta kerättyä tietoa.

VMware Workstation -ohjelmalla luotiin CentOS5.2-käyttöjärjestelmä asennuksesta yksi pohja, jota käytettiin asennettaville ohjelmistoille pohjana virtualisointiympäristössä. CentOS5.2 asennettiin ilman lisäosia, jonka jälkeen suoritettiin testattavan verkonhallintaohjelmiston asennus. Verkonhallintaohjelmistojen asennus jouduttiin uusimaan muutaman kerran, kunnes saatiin asennus onnistumaan ja verkonhallintaohjelmistoille voitiin tehdä toimivat asennusohjeet. Vertailtavia ohjelmistoja olivat Cacti, Zenoss, Groundwork ja Nagios. Näille yhtenäistä on, että ne ovat avoimen lähdekoodin ohjelmistoja, maksuttomia ja toimivat Linux-käyttöjärjestelmässä.

Asennusvaiheessa palvelin oli yhteydessä Internetiin, jotta voitiin varmistaa viimeisten päivitysten saatavuus. Yhteys Internetiin ei ollut kuitenkaan mahdollista käytetyssä valvontaverkossa, mutta siihen tulee muutos kun palvelimet saadaan lopulliseen sijoituspaikkaan ja muut tarvittavat laitteet voidaan asentaa toimintakuntoon.

5.2 Cacti-toteutus

Työssä käytetyt Cacti-asennusohjeet löytyvät liitteestä 1. Cacti-ohjelmiston voi ladata osoitteesta www.cacti.net ja sivustolta löytyvät myös dokumentit ohjelmiston käyttöön. Asennuksessa oli käytössä Cactin versio 0.8.7c. Ohjelmiston asennus aloitettiin varmistamalla yum-priorities ja rpmforge-release -asennuksilla, että asennuksessa ei tulisi alaspäin päivityksiä jo asennettuihin ohjelmiin. Tämän jälkeen päivitettiin CentOS ja päivitysten jälkeen asennettiin Cactin toiminnan kannalta tarvittavat paketit, joita ovat muun muassa: httpd, php, mysql ja rrdtool.

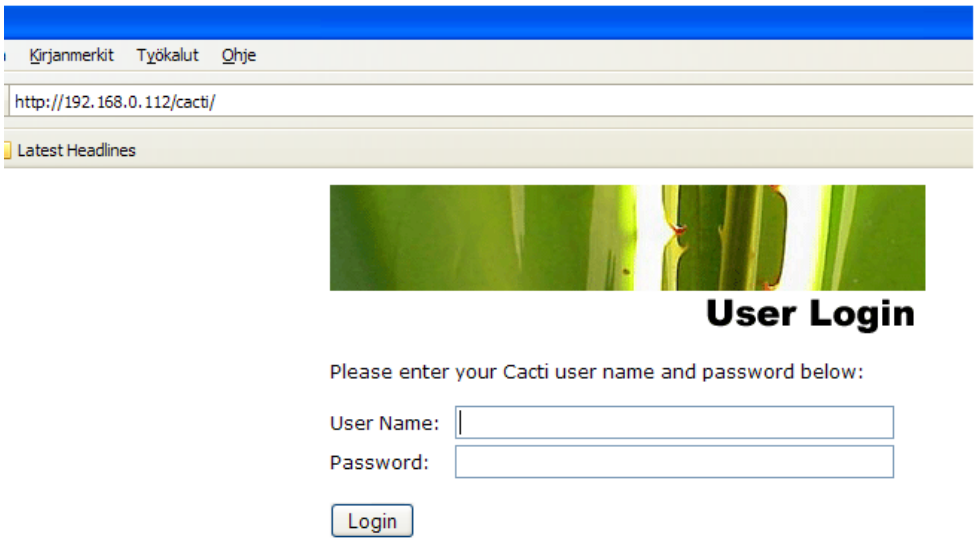
Tässä vaiheessa asennusta luodaan Cactille käyttäjä cactiuser, jolle annetaan oikeudet cacti.sql-tietokantaan. Tätä käyttäjää ei pidä sekoittaa www-selaimen kautta kirjautuviin käyttäjiin. Tälle käyttäjälle annetaan oikeuksia tehdä muutoksia palvelimen kansioihin, joihin tallennetaan tietoja kuvaajien piirtoa varten.

Käyttäjän luonnin jälkeen käynnistetään tietokantaohjelmisto root-käyttäjänä. Luodaan tietokanta cacti ja sallitaan cactiuser-käyttäjän käyttää tietokantaa cacti. Www-selaimen kautta kirjauduttaessa käytetään php-sivua, joten määritetään confis.php-tiedostoon parametrit cactiuser-käyttäjästä kohdilleen. Tarvittavia tietoja ovat tietokanta, käyttäjänimi ja salasana -kohdat. Näillä asetuksilla sallitaan www-hallinnan kautta tehdä muutoksia palvelimen valittuihin tiedostoihin, jotka sijaitsevat rra- ja log-kansioissa. Kuvaajissa käytettävät tiedot ovat tallessa rra-kansiossa.

Valvonnan kannalta oleellinen crontab laitetaan toimimaan cactiuser-käyttäjän oikeuksilla ja päivittämään tietoja 5 minuutin välein rrdtoolin kuvaajiin, joita voidaan katsoa www-sivujen kautta.

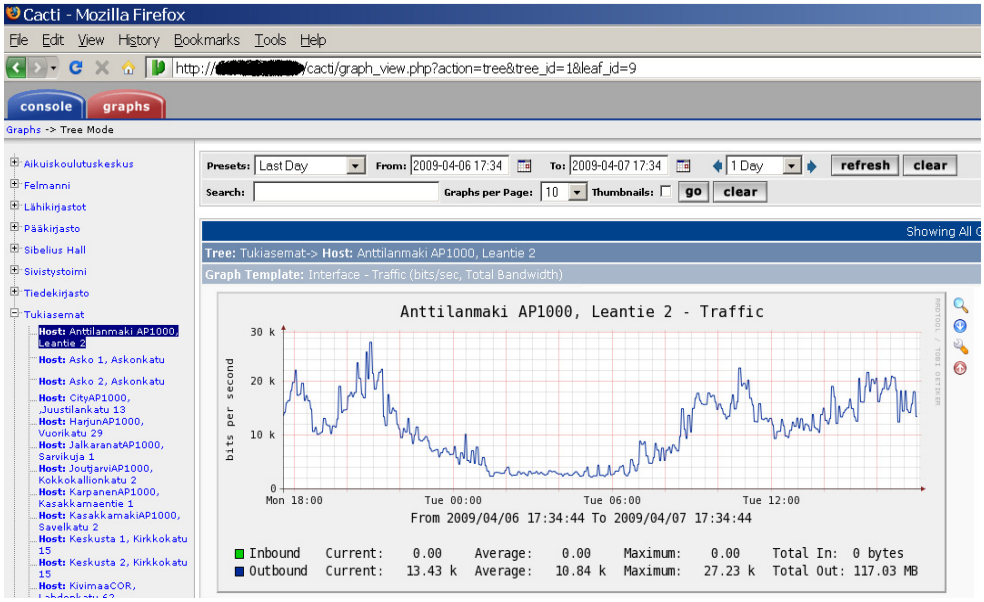
Asennuksen lopuksi varmistetaan, että ohjelmiston toiminta jatkuu normaalisti myös palvelimen uudelleen käynnistyksen jälkeen. Käyttöjärjestelmälle annetaan käsky käynnistää halutut palvelut uudelleen käynnistyksen jälkeen. Chkconfig-käskyllä määritetään mysqld ja httpd käynnistymään aina kun CentOS käynnistyy.

Ohjelman asentamisen jälkeen kirjaudutaan www-selaimen kautta hallintasivuille (kuvio 26). Ohjelmaan lisätään laitteet, joita halutaan valvoa. Valmiina löytyy localhost, josta valvotaan muistin varausta, avoimien prosessien määrää ja kuinka monta käyttäjää on kirjautuneena käyttöjärjestelmään.



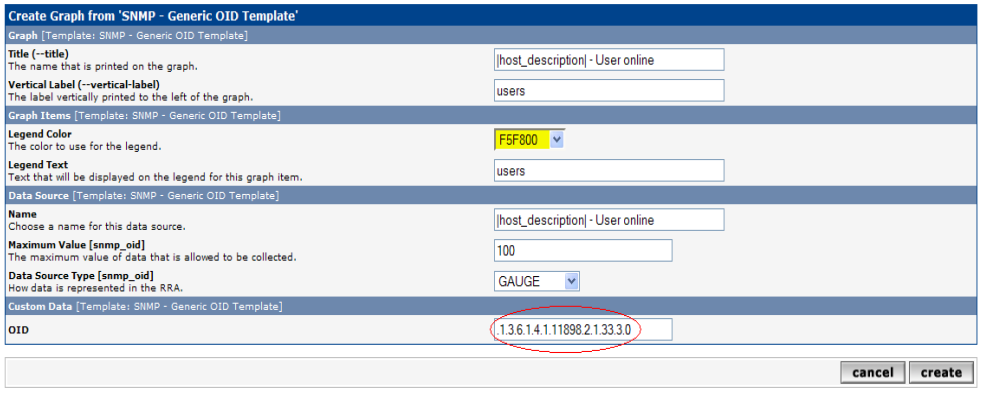
KUVIO 26. Cacti-kirjautuminen

Tukiaseman lisäys Cactiin tapahtuu IP-osoitteen perusteella (Liite 3). Laitetta lisättäessä annetaan laitetta kuvaavat tiedot, IP-osoite ja templateksi valitaan Generic SNMP Enabled Host, jossa on valmiina liityntöjen SNMP-kysely. Lisäksi valitaan SNMPv1 ja annetaan laitteen community-salasana. Tallennetaan laite ja nyt sille voidaan määritellä mitä tietoja siitä halutaan piirtää kuvaajina. Lopuksi lisätään laite Cactin puuhun, jolloin laitteen kuvaajia voidaan tarkastella graphs-välilehden kautta (kuvio 27).



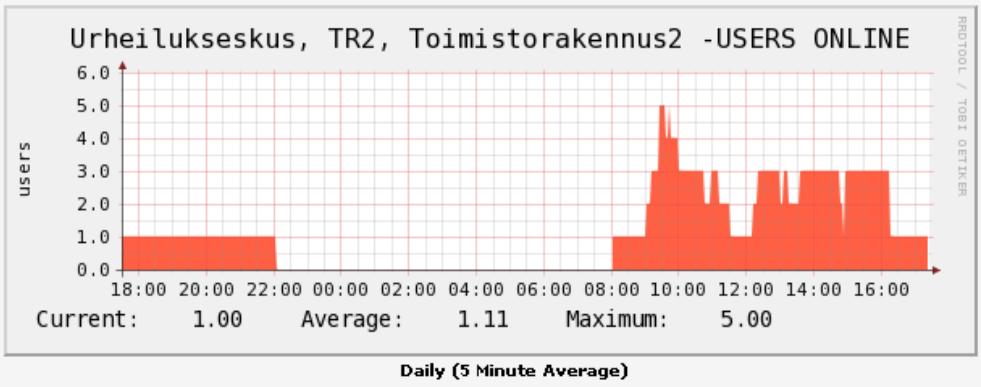
KUVIO 27. Cacti-laitteet puurakenteessa

Laitteen lisäämisen jälkeen sille voidaan lisätä myös muita valvottavia tietoja. MASTONET-verkossa halutaan tietää liikennöivien asiakkaiden määrä tukiasemakohtaisesti. Tätä varten lisätään ohjelmistoon tiettyä OID:ia käyttävä kuvaajan piirto, jolla saadaan selville Orinocon AP700-tukiaseman käyttäjämäärä (kuvio 28).



KUVIO 28. Tietyn OID:n lisäys Cactiin

OID kohdistaa kyselyn Orinocon AP700-tukiaseman MIB-kantaan ja siellä olevaan oriStationStatNumberOfClients-kohtaan. Kyseinen MIB-objekti pitää sisällään tukiasemaan kyselyhetkellä yhteydessä olevien langattomien laitteiden lukumäärän. Kyselyiden perusteella Cacti on piirtänyt kuvion 29 mukaisen kuvaajan. Kuvaajasta näkyy vuorokauden aikajaksolle 5 minuutin keskiarvolla piirretty käyttäjämäärä kuvaaja, jonka otsikkotiedot ovat Urheilukeskus, TR2, Toimistorakennus2 -USERS ONLINE.



KUVIO 29. Urheilukeskus-tukiaseman käyttäjämäärä kuvaaja

Laitteita lisättäessä ohjelmistoon todettiin, että niiden MIB-objektit eroavat hieman toisistaan, joten luotiin jokaiselle tukiasemamallille oma templates, mitä käytettiin kun laitteita lisättiin ohjelmistoon. Liitteessä 4 on tarkemmat ohjeet AP700-templates-pohjan konfigurointiin.

Käytännön testien aikana ilmestyi Cactin uusi versio, joten päästiin myös testaamaan ohjelmiston päivitys. Käytössä oleva Cacti oli 0.8.7c, mikä päivitettiin versioon 0.8.7d. Käytön kannalta päivityksellä ei huomattu olevan vaikutusta. Tärkeimpänä pidettiin päivitysmahdollisuutta ilman, että tarvitsee määritellä laitteita tai asetuksia uudelleen.

Cactin tallentamia rrd-tiedostoja halutaan tulevaisuudessa mahdollisesti hyödyntää uudistettavilla www-sivuilla. Tätä varten testattiin ajastettua tiedostojen siirtoa SSH-yhteyden avulla. Tiedostot eivät siirry julkisen verkon kautta, mutta tiedostojen siirrossa haluttiin kuitenkin ottaa tietoturva huomioon. Lähde- ja kohdepalve-

limiin tarvitsee luoda yksilöivä avain, jotta tunnetaan lähettäjä ja vastaanottaja. Tunniste luodaan lähettävään päähän ssh-keygen-käskyllä, jolla saatu tunniste kopioidaan vastaanottavaan päähän. Siirtojen ajastukseen käytetään crontab-ajastusta, johon määriteltiin 5 minuutin välein suoritettavaksi tiedostojen kopiointi kohteeseen. Kopiointi onnistui hyvin, hidastavia vaikutuksia ei huomattu olevan, mutta tarkkaa siirtonopeutta ei erikseen mitattu. Liitteessä 5 on tarkemmat asennusohjeet tiedostojen siirtoon.

Laitteiden tilatieto-, nimi- ja käytettävyystiedoille luotiin lisäksi oma www-sivu. Sivustolle ei vaadita kirjautumista. Php:llä luodaan yhteys tietokantaan, noudetaan tarvittavat tiedot ja suljetaan yhteys tietokantaan. Sivustossa käytetty koodi on liitteessä 6. Tämän testin tarkoituksena oli varmistaa, että voidaan luoda omia www-sivuja tietokannan tietojen noutoa varten, joten www-sivun ulkonäkö on hyvin pelkistetty. Liitteessä 7 on näkymä testi.php-sivusta.

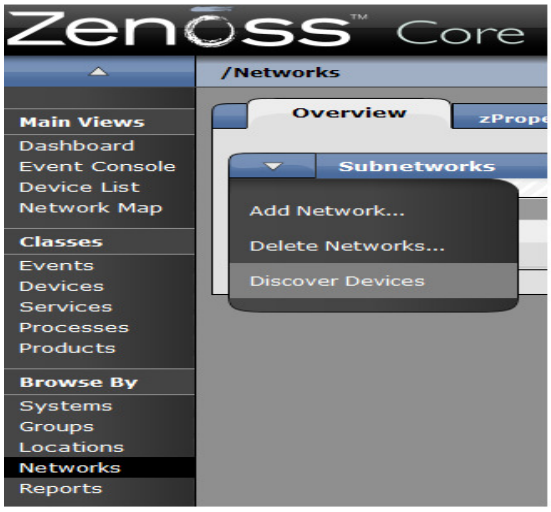
Cacti on erittäin hyödyllinen verkonhallintaohjelmisto, kun halutaan helposti saada selville verkkoon kytkettyjen laitteiden tietoliikennemäärät liityntäkohtaisesti. Aluksi oli suuri työ lisätä kaikki laitteet Cactin tietoihin. Käyttäjien luonti ja niiden oikeuksien määrittely sujui mutkattomasti, joten kuvaajia voidaan näyttää myös muille ilman, että heillä on oikeutta muuhun kuin kuvaajien katsomiseen. Laitteiden MIB-tuntemus avaa huomattavasti paremmat lähtökohdat saada hyvin monipuolisia kuvaajia aikaiseksi Cactin avulla.

5.3 Zenoss-toteutus

Zenoss-ohjelmiston asennus suoritettiin testiasennusten perusteella tehtyjen ohjeiden mukaisesti, jotka löytyvät liitteestä 2. Zenoss-ohjelmisto on ladattavissa osoitteesta www.zenoss.org, josta löytyvät myös valmistajan dokumentit ohjelmalle. Asennuksen ja ohjelmiston toimimisen kannalta joudutaan SELINUX asettamaan pois päältä. Kirjaudutaan aluksi root-tunnuksilla CentOS-käyttöjärjestelmään ja asennetaan viimeisimmät päivitykset. Lisäksi asennetaan yum install -käskyllä Zenoss-ohjelmiston käyttämät lisäosiot, joita ovat muun muassa mysql-server ja net-snmp.

Käynnistetään seuraavaksi mysqld ja poistetaan MySQL:n root-tunnuksen salasana, koska Zenoss-ohjelmistoa ei voida muuten asentaa. Tämän jälkeen voidaan asentaa Zenoss-asennuspaketin versio 2.3.3 ja zenoss-core-zenpacks-asennuspaketin versio 2.3.3. Asennuspaketit ovat rpm-muodossa, jolloin asennus voidaan suorittaa antamalla käsky rpm -ivh zenoss-2.3.3.el5.x86_64.rpm ja käsky rmp -ivh zenoss-core-zenpacks-2.3.3.el5.x86_64.rpm. Zenoss tarvitsee myös toiminnan kannalta tärkeän zenoss-core-zenpacks-asennuspaketin asennuksen, jonka avulla saadaan muun muassa uusia ominaisuuksia käyttöliittymään. Käynnistetään asennuksen lopuksi Zenoss ja mysql uudestaan, jonka jälkeen voidaan kirjautua www-hallintasivulle ja aloittaa valvottavien laitteiden lisääminen ohjelmistoon.

Valvottavien laitteiden lisääminen voidaan toteuttaa helposti automaattisen etsimen avulla, jolla voidaan hakea tietystä IP-avaruudesta valvottavia laitteita. Kuviossa 30 näkyy etsin-toiminto, jonka avulla ohjelma alkaa etsiä laitteita annetusta osoiteavaruudesta. Löydetyt laitteet näkyvät Device List -kohdan takaa Discovered -kohdasta. Tämän jälkeen ne voidaan siirtää halutun laitealustan kohdalle. Listaan voidaan luoda myös omia laitealustoja. Valvottavien laitteiden lisääminen voidaan tehdä myös yksitellen ilman etsin-toiminnon käyttämistä.

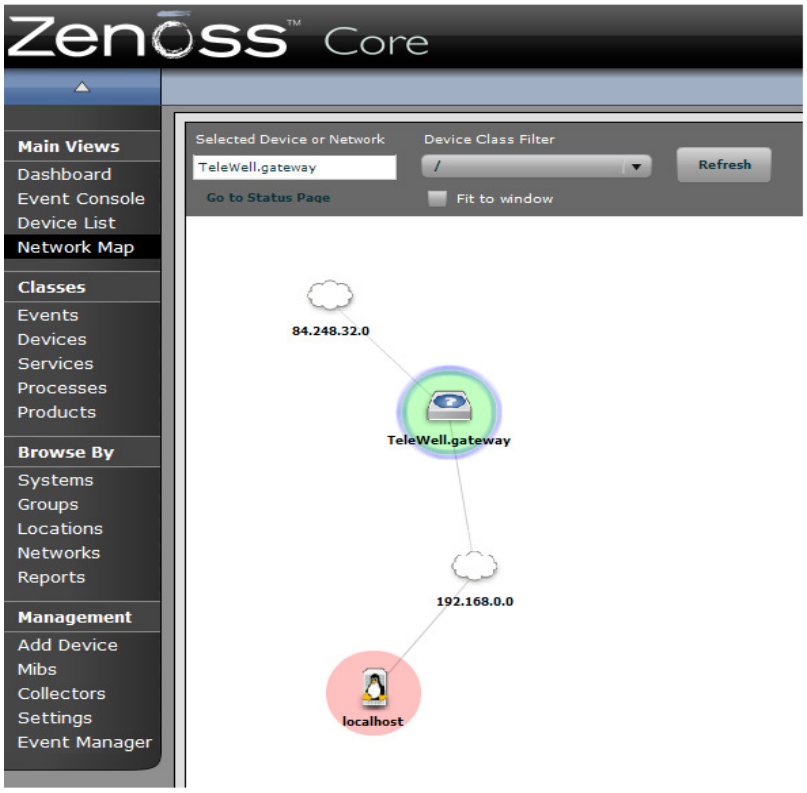


KUVIO 30. Laitteiden etsin-toiminto

Zenoss-ohjelmiston perusasetuksilla laitteista kerätään laitteiden perustiedot sekä laitteen verkkoliitännät ja niiden liikennemäärät. Nämä tiedot ohjelmisto saa sel-

ville tavallisilla SNMP-kyselyillä. Laitteiden tietojen keräämistä varten tarvitsee asettaa community-asetukset kuntoon, jonka jälkeen Zenossilla on hallintaoikeus valvottaviin laitteisiin.

Laitteiden lisäämisen jälkeen voidaan katsoa verkosta muodostettua karttaa (kuvio 31). Siinä näkyvät laitteet ja niiden IP-osoitteet ja jokaisen toimintakuntoisen laitteen ympärillä on vihreä ympyrä. Mahdollisista muista tiloista piirretään muun värinen ympyrä. Käyttäjille voidaan myös määrittää aukeamaan oletuksena tietyn IP-avaruuden kartta verkkokartta-näkymässä.



KUVIO 31. Zenoss-ohjelmiston piirtämä verkkokartta

Jos Zenoss-ohjelmistolle annetaan väärä community-salasana, niin sen seurauksena verkkokartassa näkyy laitteen kohdalla snmp punaisena ja laitteesta ei saada tietoja.

Zenossin asentaminen sujui helposti, kun oli saatu tehtyä toimivat asennusohjeet. Käyttöönotto ja asetusten konfigurointi sujuivat suhteellisen helposti. Ohjelmis-

tossa on paljon mahdollisuuksia ja kaikkien ominaisuuksien hyödyntäminen ei ollut tarpeen asennetussa verkossa. Tärkeimpänä voidaan pitää verkkokuvan luontia ja laitteiden etsin-toiminnan helppoutta. Raporttien luonti-ominaisuus on todella helpottava apu kun halutaan esimerkiksi tutkia tiettyjen laitteiden liikennettä yhdellä raportointiruudulla. Ilmoituksien lähettämistä sähköpostiin ei voitu testata, joka oli suuri puute lopullisen toteutuksen kannalta. Tutkiessa hallintasivuilta mitä kaikkea voidaan säätää sähköpostin lähetystä varten, löytyi hyvin monipuolisia mahdollisuuksia toteuttaa ilmoituksia ja mitä tietoja viesteissä ilmoitetaan vastaanottajalle. Esimerkiksi voidaan määritellä laitekohtaisesti kenelle ja millainen viesti lähetetään tapahtuneesta.

5.4 Groundwork-toteutus

Groundwork-ohjelmisto on ladattavissa osoitteesta www.groundworkopensource.com ja sivuilta löytyvät myös valmistajan dokumentit ohjelmaan. Aluksi suoritettiin Groundwork Community Edition Alpha 5.3.0 -ohjelmiston asennus valmistajan ohjeiden mukaisesti, jonka jälkeen kirjauduttiin www-hallintasivulle. Ohjelmisto sisältää autoetsin-toiminnon, jonka avulla etsittiin verkon laitteita valvottavasta verkosta. Etsintä tuntui hyvin hitaalta, mutta laitteita löytyi hiljalleen. Laitteiden valvonnassa koettiin ongelmia kun ei saatu kuvaajia näkymään. Kuvaajan tilalla oli virheilmoitus, joka viittasi tietokantaongelmaan. Asennus suoritettiin uudelleen eri asennustiedostolla, mutta törmättiin samaan ongelmaan. Asennettu versio oli juuri julkaistu sitä testattaessa, joten ongelmat ovat voineet johtua uudesta versiosta. Ohjelmiston edeltäviä versioita ei asennettu testattavaksi. Virheen pysyessä ohjelmiston testaamista verkon valvontaa varten ei voitu toteuttaa halutulla tavalla. Ohjelmiston toimiessa oikein, kuvaajia varten tiedostot tallennetaan rrd-muodossa, jolloin niitä voidaan tarvittaessa hyödyntää myös muissa ohjelmissa.

Ohjelmiston hallintasivut toimivat muuten hyvin, joten ohjelmiston käyttöä testattiin ilman kuvaajia. Hallintasivujen kautta voidaan tehdä hyvin monipuolisia säätöjä. Laitteelle voidaan asettaa ryhmä mihin se kuuluu. Tälle ryhmälle asetetaan valvojan tiedot, jolle lähetetään sähköpostitse ilmoitukset ryhmään kuuluvien lait-

teiden tilojen muutoksista. Hallintasivujen kautta pyrittiin selvittämään myös tietokannan virheilmoitusta, siinä kuitenkaan onnistumatta.

Groundworkin tietokantavirheen takia kunnollista kokonaiskuvaa ohjelmiston toimivuudesta verkonhallintaohjelmistona ei päästy muodostamaan. Ohjelmiston käyttöliittymän valikoita tutkimalla huomattiin, että käyttäjien oikeuksien kautta voidaan rajoittaa laitteiden näkyvyyttä ja mitä ja kenelle ilmoitetaan virhetilanteissa.

5.5 Nagios-toteutus

Nagios-ohjelmiston asennus suoritettiin valmistajan ohjeiden mukaisesti. Ohjelmiston asennustiedostot ja dokumentit löytyvät osoitteesta www.nagios.org. Asennus tapahtui palvelimen komentorivin kautta root-käyttäjänä. Ennen Nagioksen asennusta tarvitsee asentaa muun muassa httpd, gcc ja gd development kirjastot.

Seuraavaksi luotiin käyttäjät nagios ja nagcmd, joista jälkimmäiselle annettiin oikeudet käskyjen suorittamiseen www-hallintaliitynnän kautta. Käyttäjien luonnin jälkeen asennettiin nagios-3.0.6. Tämän jälkeen on käytettävissä aloituskonfiguraatio, jota muokkaamalla voidaan aloittaa verkonvalvonta.

Nagioksessa konfiguroitiin contacts.cfg-tiedostoon ylläpidon sähköpostiosoite, mutta sen toimivuutta ei päästy toteamaan, koska palvelimelta ei ollut yhteyttä Internetiin. Vielä ei päästy käyttämään ohjelmaa vaan ensin tarvitsi asentaa www-käyttöliittymä kuntoon. Ensin luotiin käyttäjä, jolla kirjaudutaan Nagioksen www-hallintaan ja lopuksi viimeisteltiin asennus asentamalla nagios-plugins-1.4.13, jonka jälkeen voitiin käynnistää ohjelmisto.

Nagioksen www-hallintasivujen kautta voidaan vain katsella valvontaan liittyviä asioita. Kaikki konfigurointi tehdään komentoriviltä tiedostoja muokkaamalla. Käyttöönottovaiheessa tuntui hyvin hankalalta muistaa, mitä piti konfiguroida minnekin, jotta laitteita voitiin valvoa. Aluksi tarvitsi konfiguroida nagios.cfg-

tiedostoon polku, jolla viitataan monitoroitavien laitteiden tiedostoon, esimerkiksi switch.cfg. Tiedostoon piti antaa tiedot laitteesta kuten nimi, IP-osoite ja mihin ryhmään laite kuului. Laitteen tietojen kysely SNMP:n avulla piti määritellä myös laitteen tiedostoon. Näin saatiin laite lisättyä hallittavien laitteiden listalle.

Nagioksen tietojen syöttö oli komentorivipohjaista, joka koettiin hyvin hankalaksi ja vaatisi paljon aikaa kunnolliseen perehtymiseen. Käyttötesti jäi muutaman valvottavan laitteen luontiin ja verkkokartan testaamiseen.

5.6 Ohjelmistojen vertailu

Kaikki vertailut ohjelmistot olivat avoimen lähdekoodin ohjelmistoja ja ne olivat maksuttomia. Tällöin ohjelmiston hinta ei ollut vaikuttava kriteeri valintaa tehtäessä. Ohjelmistojen käyttöönotto, käytön helppous ja verkon toimivuuden näyttäminen ylläpidolle olivat ratkaisevat tekijät valinnassa.

Ohjelmistoasennukset sujuivat vertailtavien ohjelmistojen kohdalta suhteellisen ongelmitta lukuun ottamatta Groundwork-ohjelmistoa. Groundwork-ohjelmistosta jouduttiin testin myöhemmässä vaiheessa luopumaan, koska sitä ei saatu toimimaan halutulla tavalla lukuisista yrityksistä huolimatta.

Määriteltäessä verkonvalvontaohjelmistoon laitteita ja asetuksia alkoivat graafisen hallintaliittymän edut tulla esille. Cacti, Groundwork ja Zenoss -ohjelmistoissa oli valmiiksi laitteiden ja käyttäjien hallinta toteutettuna www-liittymän kautta. Nagios-ohjelmiston hallinta oli merkkipohjainen ja ohjelmistossa tarvitsi antaa tietoja useaan eri tiedostoon, joka koettiin hankalaksi. Toki lisäosia on tehty, joilla saadaan hallinta toteutettua www-selaimella, mutta testeissä pyrittiin säilyttämään ohjelmistojen alkuperäinen kokoonpano, jotta vertailu olisi tasapuolista ohjelmistojen kesken.

Kaikki vertailussa mukana olleet ohjelmistot hyödyntävät SNMP-protokollaa laitteiden tietojen kyselyissä, joten jokaisessa ohjelmistossa on mahdollisuus muuttaa SNMP-kyselyn oikeuksien määrityksiä. Ohjelmistoista löytyi tuki myös eri

SNMP-versioille. Jokaiseen ohjelmistoon voidaan myös antaa tiettyä OID-numeroa käyttävä SNMP-kysely, jolla saadaan esimerkiksi haettua laitteen valmistajan määrittelemästä MIB-tietokannasta tietoja.

Verkon valvottavia laitteita määriteltäessä ohjelmistoon huomattiin, että autoetsintoiminto löytyy Groundwork- ja Zenoss-ohjelmistoista. Molemmissa automaattinen etsin löysi verkon laitteet, Groundwork tosin oli hieman hitaampi tässä osiossa, mutta huomattavasti nopeampi tietojen käsinsyöttöön verrattuna. Cactissa tarvitsee lisätä jokainen valvottava laite manuaalisesti hallintaliittymän kautta. Nagios-ohjelmistossa tiedot tarvitsi kirjoittaa komentorivin kautta tiedostoihin. Laitteiden määrittelyjen jälkeen tutkittiin saatuja kuvaajia, joita ohjelmistot piirsivät. Groundwork ei toiminut toivotulla tavalla, joten kuvaajia ei saatu toteutettua. Nagioksen konfigurointi ontui kuvaajien luonnin kohdalta, joten niitä ei myöskään saatu toteutettua.

Käyttäjiä määriteltäessä Cactista ja Zenossista löytyi hallinta, jossa voidaan rajoittaa käyttäjän oikeuksia esimerkiksi vain kuvaajien katsomiseen. Cactilla ei voida lähettää ilmoituksia käyttäjille sähköpostiin vakiona, sitä varten tarvitsee asentaa lisäosio. Zenoss on huomattavasti monipuolisempi virheilmoituksien lähettämisessä sähköpostiin. Siinä voidaan määrittää esimerkiksi käyttäjäkohtaisesti sähköpostit joihin ilmoitetaan halutuista tapahtumista. Groundworkista löytyivät myös monipuoliset säädöt käyttäjille. Nagioksessa määritellään contact-tiedostoon ylläpidon henkilöt joille ilmoitetaan tapahtumista sähköpostitse.

Käyttäjien ja laitteiden konfiguroinnin jälkeen tutkittiin kuinka ohjelmistot hoitavat niille olennaisen tehtävän eli verkon valvonnan. Nagios ja Zenoss näyttivät verkosta tehdyn verkkokuvan, josta näkyi aiemmin konfiguroidut laitteet. Groundwork piirsi myös samanlaisen kartan kuin Nagios, koska se hyödyntää taustalla Nagiosta. Laitteiden tilaa kuvattiin väreillä, joista kävi selvästi ilmi onko laite toiminnassa vai ei. Cacti ei piirrä verkkokuvaa, joten laitteiden tilan voi nähdä ainoastaan hallintasivulla missä laitteet on lueteltu.

5.7 Toteutettu ympäristö

Neljästä testatusta ohjelmistosta valittiin kaksi asennettavaksi MASTONET-verkon valvontaan, asennettavat ohjelmistot olivat Cacti ja Zenoss. Testien aikana Groundwork ei toiminut odotetulla tavalla ja Nagioksen komentorivipohjainen hallinta koettiin työlääksi hallita.

Asennukset suoritettiin aluksi kahdelle pöytätietokoneelle, koska palvelimet eivät olleet vielä käytettävissä. Asennuksissa käytettiin käytännön testien pohjalta luotuja ohjeita. Myöhemmin asennukset toteutettiin myös palvelimeen samoilla ohjeilla. Palvelimelle asennettuun virtualisointiympäristöön tehtyjen asennusten jälkeen ovat molemmat ohjelmistot toimineet odotetusti ja keränneet tietoa verkon laitteilta. Sähköpostin lähetystä ei päästy vielä asentamaan toimintakuntoon, koska palvelimet eivät ole lopullisessa toimintaympäristössään. Lopullinen toimintaympäristö tulee tarjoamaan yhteyden Internetiin, jolloin saadaan virheiden ilmoitustoiminto testattua. Tätä ominaisuutta ei tässä työssä päästy testaamaan.

Käyttäjämäärien seuranta Cactin avulla on ollut hyvä lisäys, jolloin on voitu esimerkiksi seurata, kuinka tietyllä alueella oleva tapahtuma lisää tukiaseman käyttäjämäärää. Valitettavasti joidenkin laitteiden MIB-tietokannasta ei löydetty tukea käyttäjämäärä tiedolle. Zenossin luoman verkkokartan perusteella ylläpito on voinut seurata verkon laitteiden tilaa yhden valvontaruudun avulla.

6 YHTEENVETO

Tässä opinnäytetyössä perehdyttiin neljään verkonhallintaohjelmistoon, niiden asennukseen ja käyttöön. Työn tavoitteena oli saada valittua sopiva verkonhallintaohjelmisto MASTONET-verkkoon, jonka ylläpito tulee olemaan LAMK:lla. Tässä tavoitteessa onnistuttiin ja valitut ohjelmistot asennettiin ylläpidon käyttöön.

Verkonvalvontaan käytetään usein standardeja protokollia, joista suurimman huomion teoriaosuudessa sai yleisimmin käytetty SNMP-protokolla. Lähestulkoon kaikki nykyiset tietoliikenneverkkoon kytkettävät laitteet hyödyntävät SNMP:tä. Laitteissa toimivien agenttien avulla saadaan kerättyä haluttua tietoa laitteista ja laitteiden vastauksien perusteella verkonvalvontaohjelmisto voi piirtää kuvaajia ylläpidolle.

Työssä käytiin läpi vertailtavien verkonvalvontaohjelmistojen asennukset sekä verkonvalvontaan valittujen ohjelmistojen tärkeimmät kohdat. Verkonvalvontaan valittavalle ohjelmistolle asetetut vaatimukset olivat, että sillä voidaan valvoa verkon laitteiden tilatietoa ja niiden verkkoliikennettä. Ohjelmistot olivat ilmaisia avoimen lähdekoodin ohjelmistoja. Maksullisia ohjelmistoja ei testattu käytännössä tässä opinnäytetyössä, joten eroja maksullisen ja ilmaisen ohjelmiston välillä ei voida tältä osin analysoida. Opinnäytetyössä vertailtujen ohjelmistojen maksullisiin versioihin saa tuen valmistajalta ja niihin tarjotaan tukea valmiiksi joidenkin käyttöjärjestelmien valvontaan valmiiksi asennettujen lisäosien avulla.

Joitain toimintoja ohjelmistoista ei valitettavasti saatu toimimaan halutulla tavalla verkon senhetkisen rakenteen vuoksi. Suurin puute oli sähköpostin lähetys vikatilanteissa, koska hallintaverkosta ei ollut vielä muodostettu yhteyttä Internet-verkkoon. Ohjelmistojen testaus oli antoisaa aikaa ja virheistä oppi paljon. Linux-käyttöjärjestelmään asennettaessa ohjelmistoja tarvitaan myös muita paketteja, jotta ohjelmisto saadaan asennettua ja lopulta toimimaan halutulla tavalla. Asennukset eivät aina toimi valmistajan ohjeiden mukaisesti, ja siitä aiheutui turhia viivästyksiä aikatauluun.

Asennusten jälkeen huomattiin Zenossin asennusohjeissa virhe, joka korjattiin ja ohjelmisto toimii nyt myös virtakatkosten jälkeen. Chkconfig-käskyt puuttuivat asennusohjeista, joilla määritetään mitkä sovellukset käynnistyvät samalla käyttöjärjestelmän kanssa. Asennusten jälkeen ohjelmistot ovat toimineet hyvin ja vastanneet niille asetettuja odotuksia verkonvalvontaohjelmistoina. Ylläpidon henkilöt ovat voineet seurata laitteiden tilaa ohjelmistojen avulla ja reagoida vikatilanteisiin ohjelmistoista saatujen tietojen perusteella.

Tulevaisuudessa voidaan asennettuihin verkonhallintaohjelmistoihin asentaa lisäosioita, joiden avulla saada huomattavasti enemmän informaatiota valvottavasta verkosta. Cactiin suositellaan asennettavaksi weathermap-lisäosio, jonka avulla saadaan hallitavan verkon liikennemäärät näkyviin verkkokartan muodossa. Verkossa olevia laitteita on useita malleja, joten kaikkien laitteiden MIB-tietokannoista ei saatu haluttuja tietoja ylläpidolle. Puuttuvien MIB-tietojen selvittäminen, jotta voidaan piirtää kuvaajia kaikkien laitteiden halutuista tiedoista, onkin yksi jatkokehityskohteista.

LÄHTEET

Badger, M. 2008. Zenoss Core Network and System Monitoring. UK, Birmingham: Published by Packt Publishing Ltd.

Barth, W. 2009. Nagios: System and Network Monitoring - 2nd ed. Published by Open Source Press GmbH, Munich, Germany.

Berry, I. & Roman, T. 2009. Cacti Manual 0.8.7. Official Cacti Documentation Site [viitattu 3.3.2009]. Saatavissa: http://docs.cacti.net/manual:087.

Bogaerdt, A. 2009. rrdtutorial. [viitattu 18.2.2009]. Saatavissa: http://oss.oetiker.ch/rrdtool/tut/rrdtutorial.en.html.

Cacti. 2009a. What is Cacti?. The Cacti Group [viitattu 2.3.2009]. Saatavissa: http://www.cacti.net/what_is_cacti.php.

Cacti. 2009b. Cacti Manuals. The Cacti Group [viitattu 20.3.2009]. Saatavissa: http://docs.cacti.net/wiki:documentation.

Castle Rock Computing, Inc. 2009. SNMPc Network Manager Introduction. California: Castle Rock Computing, Inc [viitattu 19.03.2009]. Saatavissa: www.castlerock.com/products/snmpc/default.php.

Cisco Systems, Inc. 2009. SNMPv3. San Jose: Cisco Systems, Inc [viitattu 6.3.2009]. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html.

Comer, E. 2002. TCP/IP. Jyväskylä: Gummerus Kirjapaino Oy.

DenHartog, M. 2009. The Fast Track Introduction to SNMP Alarm Monitoring. Fresno: DPS Telecom [viitattu 4.3.2009]. Saatavissa: http://dpstele.com/white-papers/snmp-tutorial/index.php.

Feldman, J. 1999. Verkonhallinta Trainer. Jyväskylä: Gummerus Kirjapaino Oy.

Galstad, E. 2008. Nagios Version 3.x Documentation. Nagios Group [viitattu 20.2.2009]. Saatavissa: http://nagios.sourceforge.net/docs/nagios-3.pdf.

Groundwork Open Source, Inc. 2009. Groundwork Monitor Community Edition. San Francisco: Groundwork Open Source [viitattu 28.1.2009]. Saatavissa: http://www.groundworkopensource.com/resources/datasheets/GWM-Community.pdf.

Haikonen, J., Hinovsky, J. & Paju, A. 2000. Verkonhallinta. Espoo: Tietoliikenne ja tietoverkkotekniikan laitos [viitattu 16.3.2009]. Saatavissa: http://keskus.hut.fi/opetus/s38118/s00/tyot/47/index.shtml.

Hobbs C. 2004. A Practical Approach to WBEM/CIM Management, CRC Press.

Jaakohuhta, H. 2005. Lähiverkot - Ethernet Ethernet-tekniikan soveltaminen käytännössä. Helsinki: Edita Prima Oy.

Jaakohuhta, H. & Lahtinen, T. 1997. Tietoliikenneverkot Tehokäyttäjän opas. Jyväskylä: Gummerus Kirjapaino Oy.

Javvin Technologies, Inc. 2009a. SNMPv1: Simple Network Management Protocol version 1. California, Javvin Technologies, Inc [viitattu 30.3.2009]. Saatavissa: http://www.javvin.com/protocolSNMPv1.html.

Javvin Technologies, Inc. 2009b. RMON: Remote Monitoring MIBs (RMON1 and RMON2). California, Javvin Technologies, Inc [viitattu 30.3.2009]. Saatavissa: www.javvin.com/protocolRMON.html.

Karila, A. 1999. Sähköposti, verkonhallinta. Espoo: Teknillinen Korkeakoulu [viitattu 2.2.2009]. Saatavissa: www.tml.tkk.fi/Opinnot/Tik-110.300/2000/Luennot/tla20001019.pdf.

Oetiker, T. 2009. RRDtool. RRDtool [viitattu 10.2.2009]. Saatavissa: http://oss.oetiker.ch/rrdtool/.

Puska M. 1999. Lähiverkkojen tekniikka Pro Training, Jyväskylä: Gummerus Kirjapaino Oy.

RFC1067. 1988. Case, J. A Simple Network Management Protocol. Request for Comments: 1067 [viitattu 2.2.2009]. Saatavissa: www.ietf.org/rfc/rfc1067.txt.

RFC1213. 1991. McCloghrie, K. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Request for Comments: 1213 [viitattu 14.3.2009]. Saatavissa: www.ietf.org/rfc/rfc1213.txt.

RFC1757. 1995. Waldbusser, S. Remote Network Monitoring Management Information Database. Request for Comments 1751 [viitattu 28.3.2009]. Saatavissa: www.faqs.org/rfcs/rfc1757.html.

RFC2613. 1999. Waterman, R. Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0. Request for Comments 2613 [viitattu 10.3.2009]. Saatavissa: www.ietf.org/rfc/rfc2613.txt.

RFC2571. 1999. Harrington, D. An Arcitehture for Describing SNMP Management Frameworks. Request for Comments 2571 [viitattu 6.2.2009]. Saatavissa: www.ietf.org/rfc/rfc2571.txt.

Software Engineering Institute. 2009. Software Technology Roadmap. Pittsburgh, Software Engineering Institute [viitattu 2.3.2009]. Saatavissa: http://www.sei.cmu.edu/str/str.pdf.

Spurgeon, E. 2001. Ethernet Tehokäyttäjän opas. Jyväskylä: Gummerus Kirjapaino Oy.

Thomas, T. 2005. Verkkojen tietoturva perusteet. Helsinki: Edita Prima Oy.

VMware, Inc.2009. VMware ESXi Data Sheet. Palo Alto:VMware, Inc. [viitattu 2.4.2009]. Saatavissa: http://www.vmware.com/files/pdf/vmware_esxi_datasheet.pdf.

Zenoss, Inc. 2009. Zenoss Administrator Guide. Annapolis: Zenoss, Inc [viitattu 10.2.2009]. Saatavissa: www.zenoss.com/communityt/docs/zenoss-guide/2.3.0.

LIITTEET

CACTI-asennusohje

Ohjeet muokattu http://openmaniak.com/cacti_tutorial.php -ohjeen pohjalta

Asennus aloitetaan poistamalla SELINUX käytöstä
muokkaa /etc/selinux/config - > SELINUX=disabled ja service iptables stop

1. Asenna RPMforge Repository

   [root@localhost ~]# yum -y install yum-priorities

2. Muokataan tiedostoa

   [root@localhost ~]# Edit /etc/yum/pluginconf.d/priorities.conf

   [main]

   enabled=1

3. Ladataan ja asennetaan RPMforge

   [root@localhost ~]#

   http://apt.sw.be/redhat/el5/en/x86_64/RPMS.dag/rpmforge-release-0.3.6-1.el5.rf.x86_64.rpm

   [root@localhost ~]# rpm –import

   http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt

   [root@localhost ~]# rpm -K rpmforge-release-0.3.6-1.el5.rf.*.rpm

   [root@localhost ~]# rpm -i rpmforge-release-0.3.6-1.el5.rf.*.rpm

   [root@localhost ~]# yum –y update

4. Asennetaan tarvittavat osiot.

   [root@localhost ~]# yum install httpd php mysql mysql-devel php-mysql mysql-server php-snmp net-snmp net-snmp-utils rrdtool

5. Luodaan käyttäjä ja annetaan salasana

   [root@localhost ~]# groupadd cacti

   [root@localhost ~]# useradd -g cacti cactiuser

   [root@localhost ~]# passwd cactiuser

   Changing password for user cactiuser.

   New UNIX password:

   Retype new UNIX password:

   passwd: all authentication tokens updated successfully.

6. Ladataan cacti

[root@localhost ~]# wget http://www.cacti.net/downloads/cacti-0.8.7c.tar.gz

7. Asennetaan cacti

[root@localhost ~]# tar zxvf cacti-0.8.7c.tar.gz

8. Siirretään kansiot /var/www/html/

[root@localhost ~]# mv cacti-0.8.7c /var/www/html/

[root@localhost ~]# cd /var/www/html/

[root@localhost html]# mv cacti-0.8.7c cacti

[root@localhost html]# cd /cacti

9. Käynnistetään mysql palvelu

[root@localhost cacti]# service mysqld start

Starting MySQL: [OK]

10. Luodaan tietokanta cacti

[root@localhost cacti]# mysqladmin -u root password password

[root@localhost cacti]# mysqladmin -u root -p

Enter password:

mysql> create database cacti;

Query OK, 0 rows affected (0.00 sec)

11. Käyttäjä cacti saa oikeudet cacti tietokantaan

mysql> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY ‘cactipassword’;

Query OK, 0 rows affected (0.00 sec)

12. Tuodaan tiedosto cacti.sql tietokantaan cacti.

[root@localhost cacti]# mysql -u root -p cacti < cacti.sql

13. Muokataan tiedostoa include/config.php

[root@localhost cacti]# nano include/config.php

$database_type = “mysql”;

$database_default = “cacti”;

$database_hostname = “localhost”;

$database_username = “cactiuser”;

$database_password = “password”;

$database_port = “3306″;

14. Vaihdetaan käyttäjä kansiolle rra and log

[root@localhost cacti]# chown -R cactiuser rra/ log/

15. Luodaan crontab cactille

[root@localhost cacti]# crontab –e –u cactiuser

*/5 * * * * php /var/www/html/cacti/poller.php > /dev/null 2>&1

16. Käynnistetään uudelleen mysql ja varmistetaan mysqld:n ja httpd:n käynnistyminen

[root@localhost cacti]# service mysqld restart

[root@localhost cacti]# chkconfig –levels 235 mysqld on

[root@localhost cacti]# /etc/init.d/mysqld start

[root@localhost cacti]# chkconfig –levels 235 httpd on

[root@localhost cacti]# /etc/init.d/httpd start

[root@localhost cacti]# yum –y update

17. Kirjaudu web-sivun kautta hallintaan

http://ip-osoite/cacti/

ZENOSS-asennusohje

(muokkaa /etc/selinux/config - > SELINUX=disabled ja service iptables stop)

1.Kirjaudu root-tunnuksilla.

2.SELinux pois
vi /etc/selinux/config
SELINUX=disabled
3.Asenna tarvittavat paketit
yum –y install mysql mysql-server net-snmp net-snmp-utils gmp swig autoconf wget

4.MySQL aloitus(tyhjällä salasanalla!!!!!)
/etc/init.d/mysqld restart
/usr/bin/mysqladmin –u root password ‘’
/usr/bin/mysqladmin –u root –h YOUR_SERVER_NAME password ‘’

5.Lataa Zenoss(varmista mikä versio)
wget http://downloads.sourceforge.net/zenoss/zenoss-2.3.3.el5.x86_64.rpm

6.Asennetaan Zenoss
rpm –ivh zenoss-2.3.3.el5.x86_64.rpm

7.Käynnistä Zenoss
/etc/init.d/zenoss start

8.Asenna Zenoss Core Packs
wget http://downloads.sourceforge.net/zenoss/zenoss-core-zenpacks-2.3.3.el5.x86_64.rpm

9.Asenna ZCP
rpm –ivh zenoss-core-zenpacks-2.3.3.el5.x86_64.rpm

10.Käynnistä MySQL ja Zenoss uudelleen
/etc/init.d/mysqld restart
/etc/init.d/zenoss restart

11.Tarkista päivitykset
yum –y update

12.Varmista, että tarvittavat ohjelmat käynnistyvät bootin jälkeen
chkconfig –levels 235 mysqld on

13.Kirjaudu web sivulle
http://serverIP:8080
user: admin
password: zenoss

Cacti-ohjelmistoon laitteen lisäys

Lisää laite(Device)
(Ohjeet ovat lähinnä suuntaa antavia)
Console-> Device -> Add

General Host Options
    Description: ”Laitteen kuvaus”
    Hostname: Anna IP
    Host Template: Generic – SNMP-enabled Host
Availibility/ Reachability Options
    ….
SNMP Options
    SNMP Version: Version 1(kun tämän valitsee muuttu Availibility)
SNMP Community: “laitteen salasana”
SNMP Port: 161
SNMP Timeout: 500
Maximun O..: 10
paina create

Luodaan AP700-tukiasemalle templates, jossa interface ja käyttämäärä kyselyt.

1.Data Templates paina add
Data Templates
Nimi: AP700 - useronline,
Data SOurce
Data Input Method: Get SNMP Data
Associated RRA's: Daily, Weekly, Monthly ja Yearly
Data Source Item
Internal Data SOurce Name: useronline
Paina create
Custom Data
OID: .1.3.6.1.4.1.11898.2.1.33.3.0
paina save
2.Graph Templates paina add
Template
Name: AP700 - Useronline - graafi
Graph Template
Title: Users
paina create
Graph Template Items
paina add
Graph Template Items
Data Source: AP700 - USER OID Template - (useronline)
Color: FF4105
Graph Item Type: AREA
Text Format: Users
paina create
Graph Template Items
paina add
Graph Template Items
Graph Item Type: LEGEND
paina create
paina save
3.Host Template paina add
Host Templates
Name: AP700 - USER OID - Host Template
paina create
Associated Graph Templates
Add Graph Template: AP700 - Useronline - graafi
paina add
Associated Data Queries
Add Data Query: SNMP - Interface Statistics
paina add
paina save

Rrd-tiedostojen siirto Cactista

Kirjaudu palvelimeen, josta kopioidaan tiedostot

Anna seuraavat komennot:

1.ssh-keygen –t rsa hyväksy enterillä

2.Kopio id_rsa.pub -> authorized_keys2

3. Kopio authorized_keys2 tietokoneeseen, mihin olet siirtämässä tiedostoja (/root/.ssh/ authorized_keys2)

4.crontab lisää seuraava rivi (mistä kopioidaan kone):

a.scp –r /var/www/html/cacti/rra ”kohde IP”:/tmp (mistä mihin)

Varmista toimivuus 3 kohdan jälkeen antamalla 4.a kohta komentorivillä. Tietoturvan kannalta kannattaa luoda käyttäjät, joita käytetään molemmissa päissä ilman kirjautumisoikeuksia palvelimeen.

Testi.php www-sivun koodi

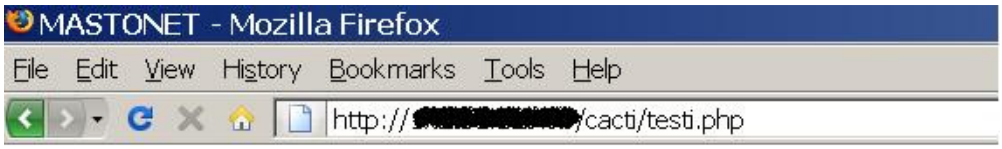
```
<HTML><HEAD>
<TITLE>MASTONET</TITLE></HEAD>
<BODY>
<TABLE ALIGN=center><TR><TD>

<?php
//näiden pitää vastata config.php tietoja
$username = "xxxxxxx";
$password = "xxxxxxx";
$hostname = "xxxxxxx";
$dbh = mysql_connect($hostname, $username, $password)
        or die("Unable to connect to Cacti DataBase");
print "Connected to Cacti DataBase!!!<br><br>";
$selected = mysql_select_db("cacti",$dbh)
        or die("Could not select cacti");

//mita tietoja noudetaan ja mista taulusta
$result = mysql_query("SELECT description, status, availability FROM host");
print "<TABLE BORDER=1>\n";
print "<TR>\n";
print "<TD>Status</TD><TD>Hostname</TD><TD>Availability</TD>\n";
print "</TR>\n";
while ($row = mysql_fetch_array($result,MYSQL_ASSOC))
{
//kannasta saatu arvo muutetaan tekstiksi
print "<TR>\n";
        if ($row[status] == 3 )
        {
                print "<TD>UP</TD>";
        }
        elseif ($row[status] == 2 )
        {
                print "<TD>Recovering</TD>";
        }
        elseif ($row[status] == 1 )
        {
                print "<TD>DOWN</TD>";
        }
        else
        {
                print "<TD>Unknown</TD>";
        }
print   "<TD>$row[description]</TD>
        <TD>$row[availability]</TD>\n";
print "</TR>\n";
}
print "</TABLE>\n";
```

```
//suljetaan yhteys tietokantaan
mysql_close($dbh);
?>
</TD></TR></TABLE>
</BODY></HTML>
```

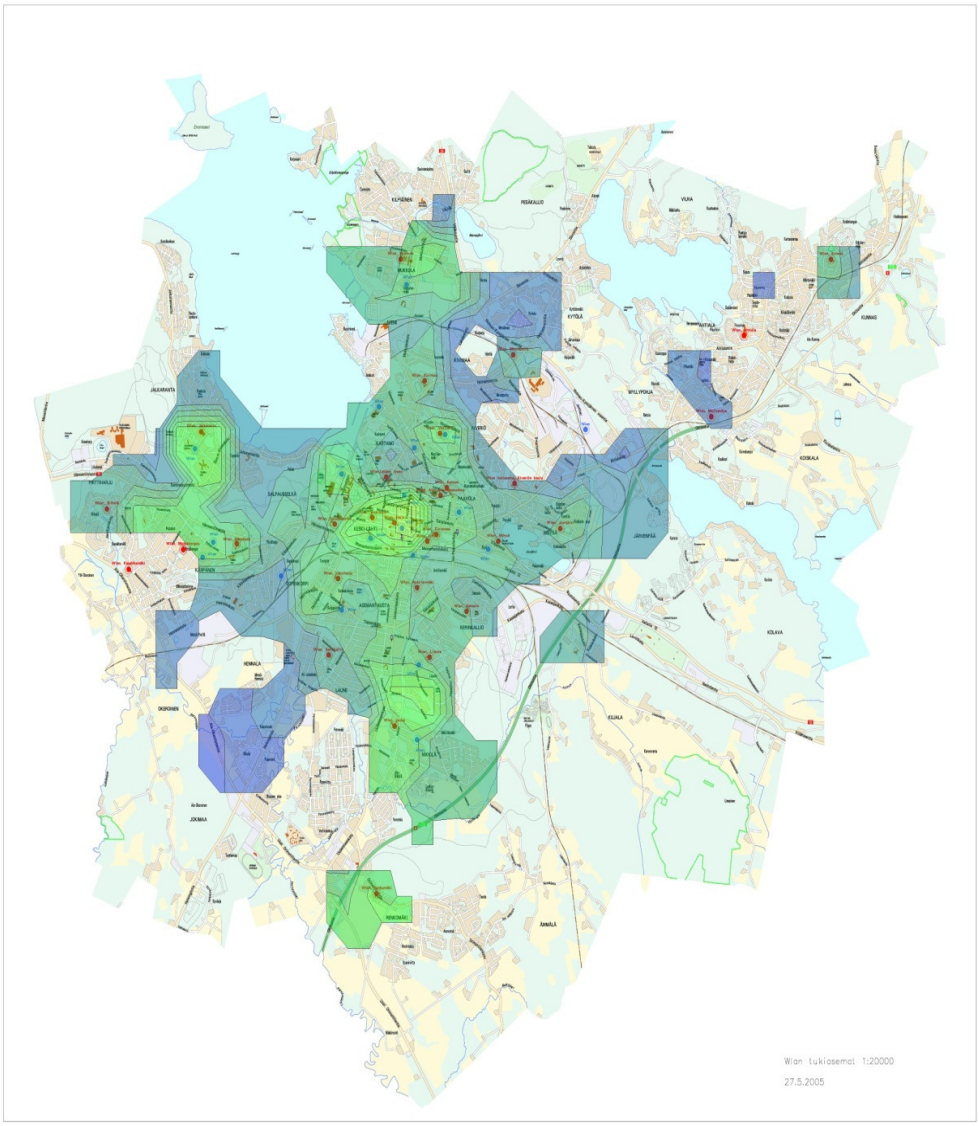
Testi.php www-sivun näkymä



Connected to Cacti DataBase!!!

Status	Hostname	Availability
UP	Localhost	100.00000
UP	Vesitorni 1, Juustilankatu 13	99.85304
UP	Myllypohjankoulu, Vanha ahtialantie 93	99.83151
UP	Anttilanmaki AP1000, Leantie 2	99.29673
Unknown	Asko 1, Askonkatu	100.00000
UP	Asko 2, Askonkatu	99.98474
UP	CityAP1000, ,Juustilankatu 13	100.00000
UP	HarjunAP1000, Vuorikatu 29	99.97965
UP	JalkaranatAP1000, Sarvikuja 1	99.88809
UP	JoutjarviAP1000, Kokkokallionkatu 2	99.27761
UP	KarpanenAP1000, Kasakkamaentie 1	100.00000
UP	KasakkamakiAP1000, Savelkatu 2	99.97965
UP	Keskusta 1, Kirkkokatu 15	98.95192
UP	Keskusta 2, Kirkkokatu 15	98.95701
UP	KivimaaCOR, Lahdenkatu 62	99.88298
UP	KunnasAP1000, Opinkatu 4	99.99491
UP	Kyvo 1, ,Kymijarven Voimalaitos	99.99491
UP	Kyvo 2, Kymijarven Voimalaitos	99.99491
UP	LE 1, Kauppakatu 31	99.97456

MASTONET-verkon peittoalue



MASTONET-verkon kuuluvuus, lähde Jyrki Rautkivi Lahden tiede- ja yrityspuisto Oy, Mastonet wlan verkon kehittämien.