VERKONVALVONTAJÄRJESTELMÄN SUUNNITTELU

Mediatalo ESA

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2011
Jussi Hämäläinen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HÄMÄLÄINEN, JUSSI: Verkonvalvontajärjestelmän suunnittelu Mediatalo ESA

Tietoliikennetekniikan opinnäytetyö, 62 sivua

Kevät 2011

TIIVISTELMÄ

Useiden yritysten alati kasvavat tietoverkot tarvitsevat tuekseen jonkintasoisen verkonvalvontajärjestelmän. Verkonvalvontajärjestelmillä voidaan ehkäistä verkossa muodostuvien vikatilanteiden syntyminen ja vaikuttaa tarvittaessa nopeasti äkillisiin verkkovikoihin. Lisäksi verkonvalvontaohjelmilla saadaan kerättyä verkosta tietoa, jota voidaan hyödyntää esimerkiksi laskutuksessa tai tulevissa laitehankinnoissa.

Mediatalo ESA:n verkonvalvontajärjestelmä on vanhentunut ja järjestelmä tarvitsee uudistaa. Tämän opinnäytetyön tavoitteena on vertailla erilaisia verkonvalvontasovelluksia ja suunnitella yritykselle uusi verkonvalvontajärjestelmä vertailussa parhaaksi osoittautuneen verkonvalvontasovelluksen avulla. Vertailtavia ohjelmia ovat PRTG, OP5, ZenOSS, NetEye ja What's Up Gold. Tässä työssä perehdytään myös verkonvalvontaohjelmien ominaisuuksiin ja mittaustapoihin.

Tämä opinnäytetyö perustuu TCP/IP-verkkojen verkonvalvontaohjelmiin, jotka hyödyntävät SNMP-protokollaa. SNMP kerää verkon laitteista tietoa MIB-taulukoihin perustuvien objektien avulla. MIB-taulukoiden rakenne määritellään SMI-standardin avulla. Useimmat verkonvalvontasovellukset tukevat SNMP-protokollaa, protokollan eri versioita, toimintatapaa ja protokollaan liittyviä standardeja.

Verkonvalvontasovelluksien vertailu perustuu Mediatalo ESA:n määrittelemiin kriteereihin, jotka ovat käyttöjärjestelmä, hinta- ja laatu-suhde, klusterointimahdollisuus, käytettävyys, ohjelman verkonvalvontaominaisuuksien muokkausmahdollisuudet, verkkotopologiakartan toteutus, graafisten taulukkojen ominaisuudet, ohjelman tukemat protokollat, valvontatavat, hälytykset sekä mobiilivalvonta. Tässä vertailussa parhaaksi verkonvalvontasovellukseksi viidestä vertailuun valitusta sovelluksesta valittiin PRTG. Tämän ohjelman kokeiluun ja ohjelmasta hankittuun tietoon perustuen luotiin suunnitelma uuden verkonvalvontajärjestelmän käyttöönotosta. Mediatalo ESA:lla siirrytään käyttämään PRTG-ohjelmaa uudessa verkonvalvontatoteutuksessa kevään 2011 aikana.

Avainsanat: verkonvalvonta, verkonhallinta, SNMP, MIB, SMI, RMON, NetFlow, PRTG

Lahti University of Applied Sciences
Degree Programme in Information Technology

HÄMÄLÄINEN, JUSSI: Planning of a network monitoring system Mediatalo ESA

Bachelor's Thesis in Telecommunications

62 pages

Spring 2011

ABSTRACT

In many companies, continuously growing networks require some kind of monitoring system to support their networks. Such monitoring systems may prevent network faults, and enable network managers to react quickly when network errors occur. In addition, network monitoring programs are used to gather information on the web that can be utilized for example in billing, or any future equipment purchases.

Mediatalo ESA's network monitoring system is outdated and needs to be updated. The aim of this degree programme was to compare a variety of network monitoring software and plan a new network monitoring system for the company based on best software from the comparison. Programs that were compared were PRTG, OP5, ZenOSS, Neteye and What's Up Gold. The thesis also deals with features and measurement methods of network monitoring programs in general.

The thesis is based on network monitoring programs used in TCP/IP networks that use the SNMP protocol. SNMP collects data from the network devices using objects based on the MIB. Structure of the MIB tables is defined by the SMI standard. Most network monitoring applications support the SNMP protocol, its different versions, methods of operation and protocol standards.

The Comparison of network monitoring programs was based on criteria defined by Mediatalo ESA, which are operating system, price/quality ratio, clustering possibilities, usability, customization options for network monitoring, execution of network topology maps, features of graphical tables, program supported protocols, monitoring methods, alarms and mobile surveillance. In this comparison, the best program of the five participants was PRTG. The plan for the new network monitoring system was created based on testing this program and acquiring information about it. Mediatalo ESA is switching to the new PRTG network monitoring program in its new network monitoring implementation in spring 2011.

Key words: network monitoring, network management, SNMP, MIB, SMI, RMON, NetFlow, PRTG

SISÄLLYS

LYHENNELUETTELO

API	Application Programming Interface, ts. ohjelmointirajapinta on käyttöliittymä tietojen vaihtamiseen laitteiden välillä.
ASN.1	Abstract Syntax Notation One, merkintätapastandardi, joka määrittelee tiedon ilmaisutavan, koodauksen, lähetyksen ja dekoodauksen rakenteen.
CIM	Common Information Model, standardi, joka määrittelee hallinnollisten elementtien esitystavan IT-ympäristössä.
IAB	Internet Architechture Board, Internetin arkkitehtuuria hallinnoiva lautakunta.
ICMP	Internet Control Message Protocol, protokolla IP-verkoissa toimivien laitteiden saavutettavuuden raportointiin.
IETF	Internet Engineering Task Force, internetprotokollien standardoinnista vastaava organisaatio.
IP	Internet Protoocol, internetprotokolla, joka vastaa pakettien siirrosta internetissä.
ITU-T	International Telecommunication Union – Telecommunnication, kansainvälinen tele-alan standardeja ylläpitävä järjestö.
MIB	Management Information Base, hallintatietokanta SNMP-protokollalle, joka määrittelee verkonhallintaobjektit.
OSI	Open Systems Interconnection, malli, joka määrittelee tiedonsiirtoprotokollat seitsemässä kerroksessa.

PDU	Protocol Data Unit, eri protokollien pakettien sisältämä kehys, joka määritelee paketin sisältämän tiedon.
RMON	Remote network Monitoring, ohjelmisto tai laite, joka kerää mittaustietoja verkon laitteista ja tallentaa ne omaan tiedostoonsa.
SMI	Structure of Management Information, tietorakenne, joka määrittelee MIB-taulukon hierarkisen rakenteen ja objektit.
SNMP	Simpe Network Management Protocol, yleisin TCP/IP-verkkojen verkonvalvontaprotokolla.
TCP	Transmission Control Protocol, tiedonsiirron hallintaprotokolla.
UDP	User Datagram Protocol, tiedonsiirtoprotokolla, joka ei vaadi jatkuvaa yhteyttä laitteiden välille.
USM	User-based Security Model, käyttäjän tunnistamiseen perustuva turvallisuusmalliteknologia.
VACM	View-based Access Control, käytönvalvontaan perustuva turvallisuusteknologia.
WMI	Windows Management Instrumentation, Windowsin kehittämä laajennus, jolla mahdollistetaan hallintatietojen välitys laitteiden välillä.

1 JOHDANTO

Lähiverkkojen laajentuessa ja kasvaessa on verkonhallinnan ja -valvonnan merkitys kasvanut tärkeäksi osaksi yritysten ja erillisten toimijoiden jokapäiväistä elämää. Lähes jokaisen yrityksen käytössä on jonkinlainen tietoverkko, joka on joko yhtiön sisäinen lähiverkko, tai sitten tietoverkko on yhteydessä laajempaan verkkoon, kuten internetiin. Tällaisia verkkoja on tapeellista valvoa ja yrittää ennaltaehkäistä verkon ruuhkautumista ja vikaantumista sekä ylläpitää laitteiden tilaa. Tähän tarkoitukseen käytetään erilaisia verkonhallinnan työkaluja, joilla yleisesti tarkoitetaan sekä verkonhallintaan että -valvontaan suunnattuja laitteita, sovelluksia ja menetelmiä.

Verkonhallinta on käsitteenä laaja ja yleensä verkonhallinta jaetaankin kahteen kategoriaan: verkonhallintaan ja verkonvalvontaan. Verkonhallinta käsittää verkon turvallisuuden- ja kokoonpanonhallinnan ja verkonvalvonnalla taas tarkoitetaan verkon suorituskyvyn-, vikojen- sekä käytönvalvontaa. Tässä opinnäytetyössä keskitytään pääasiassa verkonvalvontaan, verkonvalvontasovelluksiin ja verkonvalvonnan toimintatapaan. Myös verkonhallinta tulee jossain määrin esille sovellusten esittelyssä ja käytössä, koska nykypäivänä verkonvalvontasovellukset sisältävät myös sellaisia ominaisuuksia, joilla pystytään osaksi hallitsemaan verkkoa ja verkon käyttöä.

TCP/IP-verkkojen (Transmission Control Protocol / Internet Protocol) yleisin valvontaprotokolla on SNMP (Simple Network Management Protocol). Tässä opinnäytetyössä perehdytäänkin tarkemmin TCP/IP-verkkojen verkonvalvontaan ja SNMP-pohjaisten verkonvalvontaohjelmien käyttöön. Valvottavissa verkkolaitteissa otetaan käyttöön SNMP-protokolla, jonka jälkeen asetetaan hallinta-asema hakemaan snmp-tietoja laitteista. Hallinta-asema muodostaa verkon laitteista verkkokuvan, kerää tilatietoja sekä muodostaa tiedoista graafisia taulukoita ja hälyttää ylläpitäjää verkon vikatilanteissa. SNMP-protokolla hyödyntää MIB-tietokantoja (Management Information Base), jotka koostuvat erillisistä yleisistä- ja toimittajakohtaisista MIB-objekteista. Objektit keräävät

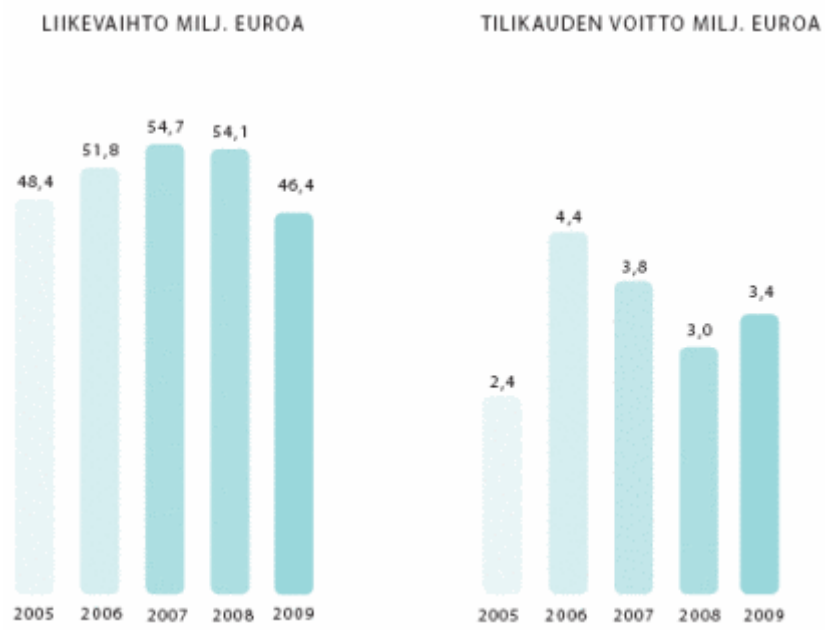
erilaisia tietoja laitteista, jotka sitten välitetään SNMP-protokollan avulla hallintatyöasemalle.

Mediatalo ESA:lla on tullut tarve päivittää verkonvalvontajärjestelmäänsä, koska vanha verkonvalvontatoteutus ei ole pysynyt kehityksen perässä ja toteutuksen sovellukset ovat hankalia hallita ja ominaisuudet vajaavaisia verrattuna nykypäivän verkonvalvontasovelluksiin. Tämä opinnäytetyö pohjautuu yhteiseen päätökseen Mediatalo ESA:n tietohallinnon toimijoiden kanssa päivittää heidän verkonvalvontajärjestelmänsä vertailemalla erilaisia verkonvalvontasovelluksia ja toteuttaa sitten uusi verkonvalvontajärjestelmä hyväksi havaitun sovelluksen avulla. Työssä perehdytään myös erilaisiin verkonvalvontamenetelmiin.

Mediatalo ESA on johtava viestintäkonserni Päijät-Hämeessä, joka tarjoaa palveluitaan sekä kuluttaja-asiakkaille että yrityksille. Palveluihin kuuluu viisi eri lehteä: Etelä-Suomen Sanomat, Itä-Häme, Mäntsälän uutiset, kaupunkilehti Uusi Lahti sekä pitäjälehti Seutuneloset. Lisäksi Mediatalo ESA:n palveluihin kuuluu verkkopalvelu ess.fi, paikallisradio Voima sekä paino- ja jakelupalvelut. (Mediatalo ESA 2011a.)

Mediatalo ESA on toiminut Päijät-Hämeessä kohta jo 111 vuotta. Toiminta alkoi vuonna 1900, jolloin saatiin virallinen lupa Etelä-Suomen Sanomien julkaisuun 18.4.1900. Vuosien varrella Mediatalo ESA:n toiminta on kasvanut huomattavasti eri medioissa, ja tänä päivänä Mediatalo ESA:n palvelut toimivatkin esimerkiksi radiossa ja verkossa lehtipalveluiden lisäksi. (Mediatalo ESA 2011b.)

Konsernin muodostavat Esan kirjapaino Oy sekä Esan kirjapaino Oy:n tytäryhtiöt, Esan paikallislehdet Oy, Esa Lehtipaino Oy, Esa Jakelut Oy, Esa Print Oy ja Monday’s Special Oy (Mediatalo ESA 2011d). Vuonna 2009 yhtiön liikevaihto oli 46,4 miljoonaa euroa (kuvio 1) ja konsernissa työskentelee n. 700 työntekijää. (Mediatalo ESA 2011c.)



KUVIO 1. Mediatalo ESA:n liikevaihto ja tilikauden voitto v. 2005 - 2009 (Mediatalo ESA 2011d)

Mediatalo ESA ottaa yhtiönä vastuuta myös yleisistä asioista. Yksi suurimmista kannanotoista lienee Vesijärvi-projekti, joka sai alkunsa Etelä-Suomen Sanomissa syntyneestä ideasta. Huolesta Vesijärven kuntoa kohtaan perustettiin Neuvottelukunta, jonka tuloksena syntyi Päijät-Hämeen Vesijärvisäätiö. Nykyään säätiö seuraa Vesijärven tilaa, kerää lahjoituksia sekä järjestää toimenpiteitä Vesijärven ympäristön kunnossapitämiseksi. (Mediatalo ESA 2011e.)

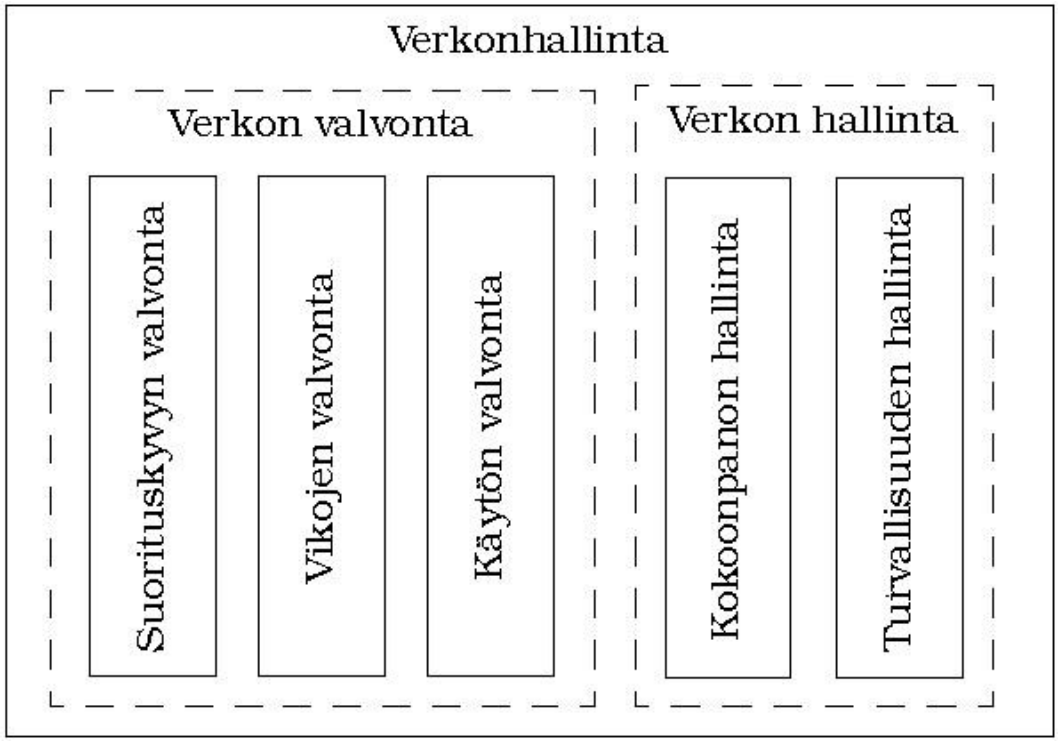
2 VERKONHALLINTA JA VALVONTA

2.1 Verkonhallinta

Yrityksillä on tarve valvoa tietoverkkoaan, jotta verkon tehokas toiminta saadaan taattua. Tähän tarvitaan verkon koosta riippuen verkonvalvontahenkilö tai -henkilöstö. Jotta verkon toimivuus voidaan taata, täytyy verkonvalvojan olla tietoinen verkon tilasta ja suorituskyvystä. Tunnettu tapa on seurata verkon toimintaa päivittäin siihen soveltuvan ohjelman avulla. Verkon jatkuvalla valvonnalla saadaan aikaiseksi hyvä kuva verkon tilanteesta ja täten voidaan etukäteen varautua esimerkiksi laajentamaan verkkoa tai ehkäistä vikatilanteita. (Microsoft 2000, 504.)

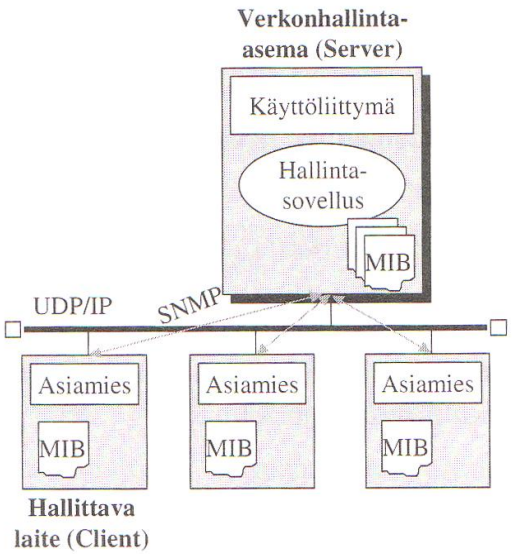
ITU-T (International Telecommunication Union - Telecommunication) määrittelee verkonhallintastandardin X.700. Standardi kattaa kaikki verkot ja erityisesti lähiverkkojen hallinnassa painotetaan tiettyjä osa-alueita, kuten vian, suorituskyvyn ja määrittelyjen hallintaa. Tässä opinnäytetyössä keskitytään X.700-standardin määrittelemään verkonhallinan yleiseen osa-aluejakoon, koska kyseinen osa-aluejako on laajalti hyväksytty ja arvostettu menetelmä. (Puska 2000, 306 - 307.)

Verkonhallinnasta puhuttaessa on syytä tiedostaa, että monesti verkonhallinnalla tarkoitetaan sekä verkonhallintaa että verkonvalvontaa. Keskityttäessä kuitenkin pelkkään verkon hallintaan huomataan, että verkonhallintaa voidaan verrata verkossa tapahtuviin kirjoitustoimenpiteisiin, kun taas verkonvalvontaa voidaan rinnastaa lukutoimenpiteisiin. Yritykset vaativat verkonhallinnalta erillisiä toimenpiteitä. Toimenpiteiden kartoitukseen käytetään x.700-standardin määrittelemää osa-aluejakoa, josta ilmenee myös mitkä osa-alueet kuuluvat verkonhallintaan- ja mitkä verkonvalvontaan (kuvio 2). (Hautaniemi 1994, 2.1.)



KUVIO 2. Verkonhallinnan osa-alueiden jakaminen (Hautaniemi 1994, 3)

Verkonhallinta koostuu erillisistä komponenteista (kuvio 3). Niihin kuuluu verkonhallinta-asema (server), joka sisältää käyttöliittymän ja hallintasovelluksen sekä MIB-tietokannan. Lisäksi komponentteihin kuuluu itse verkko, hallittava laite (client), joka sisältää ”SNMP-asiamiehen” (agent) tai mahdollisuuden käyttää SNMP-protokollaa, sekä laitekohtainen MIB-tietokanta.



KUVIO 3. Verkonhallintaympäristö SNMP järjestelmässä (Puska 2000, 308)

Hallinta asema kerää tietoa verkosta ja siihen liitetystä laitteista ja näyttää tiedot verkonvalvojalle sekä hälyttää valvojaa ja kirjaa lokiin mahdolliset verkon vikatilanteet. Hallinta-asema voidaan asettaa automaattisesti korjaamaan virhe verkon laitteessa, kuten esimerkiksi kylmäkäynnistämään laite uudelleen vikatilanteessa. Hallittavalla laitteella on oma MIB-tietokantansa, jonka mukaan SNMP:llä kerätään tietoa laitteesta. (Puska 2000, 308.)

ITU-T:n verkonhallintastandardi X.700 määrittelee verkonhallinnan viisi osa-aluetta seuraavasti:

- vikatilanteiden hallinta (Fault management)
- määrittelyjen/kokoonpanon hallinta (Configuration management)
- suorituskyvyn hallinta (Performance management)
- käytön ja laskutuksen hallinta (Acoounting management)
- turvallisuuden hallinta (Security management)

(Puska 2000, 306–307.)

2.1.1 Vikatilanteiden hallinta

Vikatilanteiden hallinnalla tarkoitetaan verkossa tapahtuvien tai jo siellä olevien vikojen havaitsemista, eristämistä ja korjaamista. Vikojenhallinta kirjaa ylös virhelokiin tiedot verkossa tapahtuneesta viasta. Hallinta-asema asetetaan suorittamaan haluttuja toimenpiteitä vikahavaintojen perusteella, kuten ilmoittamaan verkonvalvojaa tapahtuneesta viasta esimerkiksi sähköpostiviestillä, tai käynnistämään virheilevä laite uudestaan. Hallinta-asema voi suorittaa myös erinäisiä diagnostiikkatestejä verkolle tai hallittaville laitteille, jotta vikatilanteet voidaan ennakoida tai jopa estää. Hallinta-asema voi myös joissakin tapauksissa korjata vian omatoimisesti tai eristää vian, jotta verkonvalvoja voi korjata vian myöhemmin. Järjestelmässä voidaan myös hyväksikäyttää verkon eri laitteiden ominaisuuksia vikojen hallitsemisessa. Vikatilanteiden valvonta kuuluu verkonvalvonnan segmenttiin. (Jaakohuhta 2002, 303.)

Erilaiset viat verkossa voivat aiheuttaa laajoja käyttökatkoksia yhtiöille, joten vikatilanteiden hallinnan nopea ja oikeanlainen toiminta on hyvin tärkeä osa verkonhallintajärjestelmää. Vikalokien tietoja voidaan hyväksikäyttää kun suunnitellaan verkkoa tai mietitään uusia laitehankintoja. (Puska 2000, 306.)

2.1.2 Määrittelyjen hallinta

Määrittelyjen hallinta kuuluu verkonhallinnan piiriin, koska sitä käytetään verkon sekä fyysisten että loogisten olioiden käsittelyyn, yksilöimiseen ja muokkaamiseen. Fyysisiksi olioiksi voidaan määritellä esimerkiksi liitäntäkortit ja sovittimet. Loogisiksi olioiksi kutsutaan esimerkiksi reititystauluja ja VLAN-määrittelyjä. (Jaakohuhta 2002, 304.)

Määrittelyjen hallinta mahdollistaa olioiden luomisen, alustamisen ja poistamisen. Lisäksi määrittelyjen hallinta sisältää sekä luku- että kirjoitusoikeudet eri muuttujille määrittelyissä. Määrittelyjen hallinnalla kerätään tietoa verkossa tapahtuvista muutoksista ja toiminnoista. Tätä voidaan hyväksikäyttää vianeristyksessä, vianhaussa ja verkon suunnittelussa. (Jaakohuhta 2002, 304.)

2.1.3 Suorituskyvyn hallinta

Suorituskyvyn hallinta mittaa verkkoa ja tarkkailee verkon suorituskykyä sekä analysoi keräämiään tietoja. Verkon laitteet käyttävät verkosta saatavilla olevia jaettuja resursseja, kuten siirtokaistaa, levytilaa ja muistia. Ohjelmilla ja laitteilla on erilaisia vaatimuksia resurssien suhteen, ja sovelluksille on hyvin tärkeää, että verkon suorituskyky on riittävällä tasolla. Hallinta-asema tarkkailee verkon tilaa ja tarvittaessa säätää verkon asetuksia, jotta verkkoon saadaan haluttu suorituskyky. Suorituskyvyn hallinta luokitellaan verkonvalvontaan. (Jaakohuhta 2002, 304.)

Suorituskyvyn mittareina käytetään yleensä vasteaikaa sekä verkon elementtien kuormitus- että kapasiteettitietoja. Suorituskyvyn mittaaminen on tärkeää myös

laitehankinnoissa, koska suorituskykyä mittaamalla saadaan selville esimerkiksi jonkun tietyn verkkosegmentin liiallinen ruuhkautuminen. (Puska 2000, 306–307.)

2.1.4 Käytön ja laskutuksen hallinta

Käytön ja laskutuksen hallintaa käytetään yrityksissä verkon käytön- ja palveluiden seurantaan. Tämä mahdollistaa yksiköiden tai projektien laskutuksen palveluiden käytöstä. Vaikka laskutuskäytäntöä ei olisi käytössä, on tärkeää, että verkonvalvoja voi seurata, mitä palveluita tai resursseja eri käyttäjät tai käyttäjäryhmät verkossa käyttävät. Koska seuranta käsittää lukutoimenpiteitä verkossa, niin käytön ja laskutuksen hallinta liitetään verkonvalvontaan. (Jaakohuhta 2002, 304.)

Verkon käyttötietoja voidaan lähiverkoissa hyödyntää verkkokapasiteetin mittaamisessa ja tätä kautta hyödyntää tietoa laitehankinnoissa. Lisäksi käyttäjätietoja voidaan hyväksikäyttää käyttäjäkohtaisten rajoitusten suunnittelussa. Käyttötietoja voidaan käyttää laskutuksen perustana, mikäli yhtiössä niin halutaan. (Puska 2000, 307.)

2.1.5 Turvallisuuden hallinta

Turvallisuuden hallintaa käytetään käyttäjien oikeuksien hallintaan ja mahdollisiin käyttöoikeuksrikkomusten seurantaan. Verkon laitteisiin määritellään laitekohtaisesti erilaisia käyttäjäprofiileja, joiden mukaan hallitaan verkkolaitteiden käyttäjäoikeuksia. Hallinta-asemalta voidaan suorittaa erilaisia tarkastustoimia, joilla valvotaan käyttöoikeuksia. (Jaakohuhta 2002, 305.)

Laitteilta kerätään lokitietoja, joita analysoidaan ja jotka tallennetaan myöhempää tarkkailua varten. Lokitiedoista voidaan valvoa, mitä muutoksia laitteen käytössä on tapahtunut, ja tätä kautta jäljittää mahdolliset käyttöoikeusrikkomukset tai -heikkoudet. Turvallisuuden hallinta valvoo, kenellä on oikeus päästä käsiksi eri laitteisiin ja palveluihin. Turvallisuuden hallinta määritellään osaksi

verkonhallintaa, koska käyttäjätietojen valvomisen lisäksi turvallisuuden hallinnan avulla voidaan muuttaa ja hallinnoida käyttäjätietoja. (Jaakohuhta 2002, 305.)

2.2 Verkonvalvonta

Verkon ylläpitäjän tulee olla tietoinen verkon suorituskyvystä ja varmistaa, että verkko toimii moitteettomasti. Kun verkkoon liitetään uusia laitteita tai asiakkaita, siihen saattaa kehittyä pullonkauloja. Verkonvalvojan tehtävänä on estää tällaiset pullonkaulat, jotka hidastavat liikennettä ja aiheuttavat verkon tai verkon laitteiden ylikuormittumista ja ruuhkautumista. Verkonvalvonnan avulla saadaan tärkeää tietoa laitteiden tilasta ja informaatiota verkossa liikkuvasta datasta. Verkonvalvojan kannattaa ylläpitää taulukkoa erilaisista raporteista, joita verkonvalvontaohjelmalta saadaan ja verrata niitä päivittäisiin lukemiin. Näin saadaan määriteltyä verkon perustaso. Jos mittaukset eivät vastaa perustasoa, huomataan, että verkossa on jotain vialla. (Keogh 2001, 276.)

Verkonvalvontaan käsitetään verkonhallinnan osa-alueista suorituskyvyn hallinta, vikatilanteiden hallita ja käytönhallinta, joista keskeisin verkonvalvonnan kannalta on suorituskyvyn hallinta. Verkonvalvonnan tärkeimpiä ominaisuuksia on varautua ennaltaehkäisemään ongelmat verkossa ja tiedottaa verkonvalvojaa vikatilanteista. Siksi verkkoa monitoroitaessa on tarpeellista keskittyä verkon suorituskykyvyn mittaamiseen, laitteiden käyntiaikaan ja palveluiden saatavuuteen. Suorituskykyä mittaamalla voidaan huomata, jos jokin verkon osa ruuhkautuu tai joku verkkolaite on ylikuormittunut ja siihen voidaan reagoida ennaltaehkäisevin keinoin, ennen kuin tilanteesta aiheutuu suurempia ongelmia. Jos joku verkon laitteista, esimerkiksi palvelin, on ollut liian pitkään yhtäjaksoisesti päällä, saattaa laite aiheuttaa verkkoon virheilyä, jonka takia käyntiaikaa on syytä pitää silmällä. Tekemällä verkonvalvonta-ohjelmalla testejä eri palveluita tai resursseja vastaan nähdään, ovatko ne toiminnassa. Mikäli joku palvelu on kaatunut, ohjelma ilmoittaa siitä verkonvalvojalle, joka voi ryhtyä toimenpiteisiin. Jos halutaan seurata joitain toimintoja tarkemmin, kuten vaikkapa palvelimen muistin tai kiintolevyn tilankäyttöä, voidaan asettaa resurssille eri

”liipaisuarvoja” eli rajoja, jolloin rajan ylittyessä verkonvalvojaa informoidaan palvelun tilasta hälytyksellä. (Feldman 1999, 362.)

Verkonvalvontaan kuuluu oleellisena osana verkon turvallisuuden valvominen. Turvallisuuden valvominen tarkoittaa sitä, että verkossa olevien ohjelmien, palveluiden ja laitteiden sisältämä tieto saadaan suojattua asianmukaisesti. Verkonvalvojan tulee määritellä, miten verkon eri resursseja käytetään ja millä tavoin tieto suojataan. Tärkein toimenpide on laatia verkossa oleville palveluille ja laitteille suojaukset (esimerkiksi salasanat) ja käyttäjäoikeudet, joita verkonvalvontaohjelmalla valvotaan. Käyttötietoja seurataan valvomalla laitteiden lokitiedostoissa tapahtuvia muutoksia ja hälytetään verkonvalvojaa käytönvalvontarikkeistä tai muista halutuista muutoksista lokitiedoissa. (Keogh 2001, 277.)

3 VERKONVALVONTAPROTOKOLLAT JA -TERMIT

3.1 SNMP yleisesti

Alunperin IAB:n (Internet Architecture Board) suosittelemia verkkostandardeja TCP/IP-pohjaisten verkkojen hallintaan oli kaksi. Lyhyellä aikavälillä haluttiin ottaa käyttöön SNMP-protokolla verkkosolmujen valvontaan ja myöhemmin laajempaan käyttöön OSI-malliin (Open Systems Interconnection) pohjautuva standardi. Tämän tiedon pohjalta kehitettiin kaksi verkonvalvontastandardia, SMI (Structure of Management Information) ja MIB, joihin SNMP-protokollan ja OSI-hallintastandardin tuli perustua. Nämä kaksi verkonhallintaprotokollaa poikkesivat kuitenkin paljon toisistaan, ja koska OSI-hallintastandardi viivästyi ja SNMP-protokolla oli jo käytössä, niin IAB päätti virallistaa SNMP-protokollan MIB:n ja SMI:n rinnalle kolmanneksi hyväksytyksi verkonhallintastandardiksi. SNMP viestit välitetään hyväksikäyttäen UDP-protokollaa (User Datagram Protocol). (RFC1157 1990, 1–3.)

SNMP-tuki on muodostunut osaksi laitteiden perusominaisuuksia, ja lähes kaikki verkonvalvontaohjelmat käyttävät ainakin jossain määrin SNMP-protokollaa. Hallittavissa laitteissa on SNMP-agentti, joka kerää laitteesta tilatietoja ja vastaa hallinta-aseman lähettämiin käskyihin sekä välittää hallinta-aseman pyytämiä tietoja eteenpäin. Mikäli hallittavassa laitteessa tai työasemassa ei ole agenttia, on niitä yleensä mahdollista asentaa jälkiasennuksena. Hallinta-asema voi lukea agentin välittämiä objekteja, kirjoittaa niihin tai lukea objektitaulun. Agentti voi myös lähettää suoraan tietoa laitteen tilasta hallinta-asemalle ilman hallinto-aseman käskyä, mikäli näin halutaan. (Puska 2000, 308–309.)

SNMP-protokollaa käytetään monitoroimaan hallintatietoja verkosta ja välittämään tiedot käyttäjälle. Lisäksi SNMP-protokollan avulla voidaan suorittaa erilaisia toimintoja kerättyjen tietojen perusteella. Sillä välitetään hallintatietoja verkkolaitteiden välillä ja samalla valvotaan verkon tilaa. SNMP-protokollaa on paranneltu vuosien varrella ja nyt protokolla on ehtinyt kolmanteen versioonsa.

Protokollalla on erilaisia toimintoja, joita hyödynnetään analysoitavan tiedon käsittelyssä. (RFC1157 1990, 4–7.)

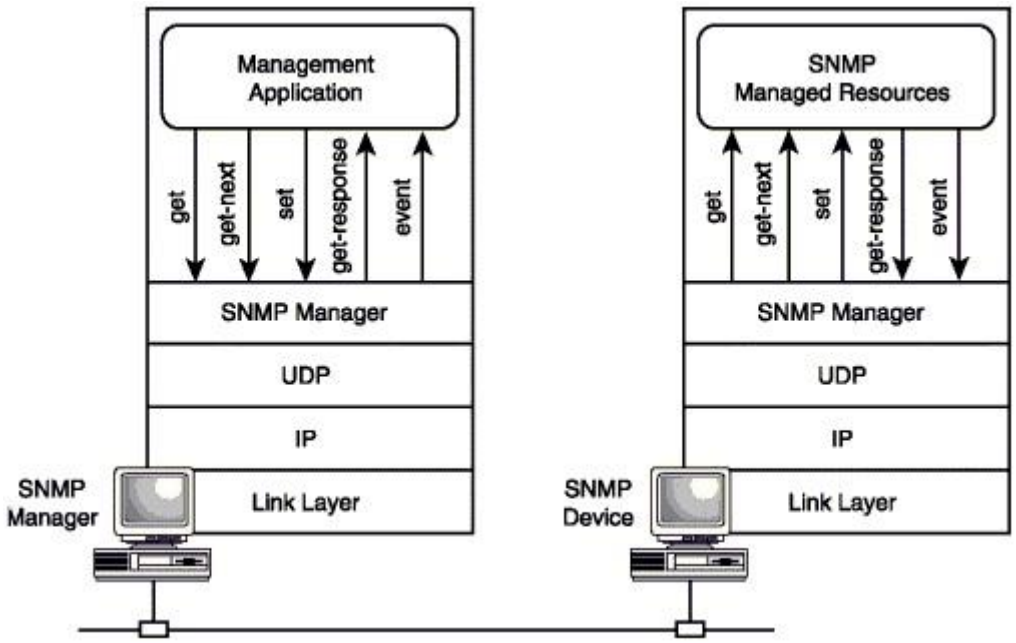
SNMP on suosittu yksinkertaisuutensa takia. SNMP sisältää pienen tietokannan, jota hyödyntämällä saadaan tietoa lähes millaisesta verkosta tai verkkolaitteesta tahansa. SNMP-tiedon kerääminen saattaa kuitenkin aiheuttaa verkkoon ruuhkaa ja voi ylikuormittaa hallinta-aseman. Tiedon keräämistä varten on olemassa laajennus MIB:iin, joka tunnetaan nimellä RMON (Remote network Monitoring), joka mahdollistaa agenttien käyttämisen välitysasemana ja tiedonkeruuelementtinä verkkosegmentissä. Tämä toimintatapa vähentää huomattavasti verkon kuormitusta verkonvalvonnassa. (Jaakohuhta 2002, 309.)

3.2 SNMP- protokollan perusoperaatiot

Ennen perehtymistä SNMP-protokollaan on syytä tuntea SNMP-protokollan perusoperaatiot. SNMP on pyyntö/vastaus-protokolla, joka käyttää perusoperaatioita tiedon hallitsemiseen hallinta-aseman ja mitattavan verkkolaitteen agentin välillä. Nämä viisi perusoperaatiota, jotka pätevät kaikkiin SNMP-protokollan versioihin, ovat seuraavanlaisia:

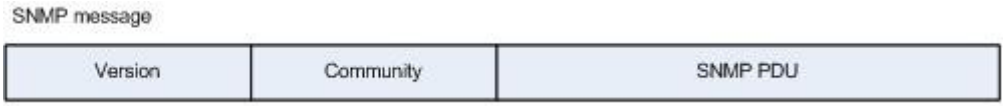
- Get Request on pyyntöviesti, jota hallinta-asema käyttää saadakseen määriteltyä MIB-objektin sisältämää tietoa agentilta.
- Get Next Request on pyyntöviesti, jota hallinta asema käyttää saadakseen MIB-tietokantataulukon seuraavan objektin sisältämän tiedon agentilta.
- Set Request on viesti, jonka hallinta-asema lähettää agentille asettaakseen tai muuttakseen MIB-objektin arvon.
- Get Response on vastausviesti, jolla agentti vastaa hallinta-aseman lähettämään Get- tai Set-pyyntöviestiin.
- Trap on viesti, jolla agentti ilmoittaa (käytännössä hälyttää) määrätyistä tapahtumista hallinta-asemalle. Trap viestiin ei kuitenkaan koskaan vastata hallinta-aseman toimesta. (H3C Technologies 2008, 8; Puska 2000, 311.)

3.3 SNMP- prototokolla



KUVIO 4. SNMP-arkkitehtuuri (Microsoft 2011)

SNMP-protokolla lähettää viestinsä käyttäen UDP-protokollaa, ja viestit liikkuvat verkossa kuvion 4 osoittamalla tavalla. Oletuksena SNMP-viestin neljää ensimmäistä operaatiota käsitellään UDP-portin 161 kautta. Trap-viestit lähetetään porttiin 162. Käyttämällä kahta eri porttia yksittäinen laite voi toimia agenttina ja hallinta-asemana samaan aikaan. (H3C Technologies 2008, 8–9.)



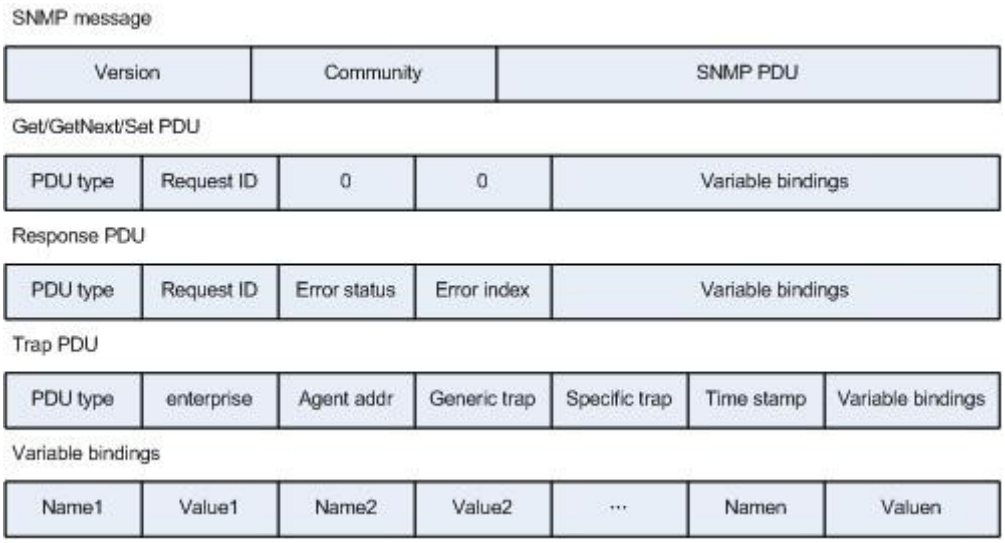
KUVIO 5. SNMP-viestin peruskehys (H3C Technologies 2008, 9)

Kaikki kolme SNMP-protokollan versiota sisältävät samat perustiedot SNMP-viestissään (kuvio 5). Versio-kenttä kertoo, mikä versio SNMP-protokollasta on käytössä. Community tarkoittaa hallinta-alueen nimeä, jolla verkko voidaan jakaa eri hallinta-alueisiin ja jota käytetään myös heikkona tunnistusmenetelmänä. SNMP-protokollan versiossa kolme, community on korvattu tietoturvallisemmalla ratkaisulla, josta kerrotaan myöhemmin. Lisäksi SNMP-viestin perustietoihin kuuluu PDU (Protocol Data Unit), joka sisältää SNMP-viestin varsinaisen datan.

SNMP-viestin PDU sisältää esimerkiksi operaatiotiedon, pyynnön numeron ja muuta vastaavaa informaatiota, jota käsitellään myöhemmin. (H3C Technologies 2008, 9; Puska 2000, 312.)

3.3.1 SNMPv1

SNMPv1 on ensimmäinen SNMP-protokollan versio. SNMPv1 sisältää minimaaliset verkonhallintaominaisuudet. MSI ja MIB ovat hyvin yksinkertaisia SNMPv1:ssä ja lisäksi siinä on huonot tietoturvaominaisuudet. SNMPv1:n kaikki sanomat kulkevat verkossa selväkielisinä ja ovat siksi helposti kaapattavissa väärään käyttöön. Tunnistus SNMPv1:ssä perustuu pelkästään myöskin selväkielisenä lähetettävään hallinta-alueen (community) nimeen, joka on huomattava tietoturvariski. Kaikki SNMP-paketit, jonka hallinta-alueen nimi ei läpäise tarkastusta yksinkertaisesti hylätään. (H3C Technologies 2008, 7; Puska 2000, 312.)



KUVIO 6 SNMPv1-viestin pohja (H3C Technologies 2008, 9)

SNMPv1-viestin kentät (kuvio 6), jotka kuuluvat SNMP PDU-pääkenttään, muodostuvat seuraavista arvoista version ja hallinta-alueen nimen lisäksi:

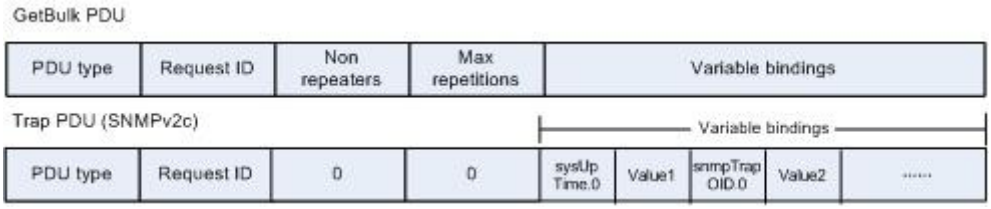
- Request ID, eli vastaustunnusta, käytetään yhdistämään pyyntö- ja vastausviestit. SNMP liittää jokaiseen pyyntöviestiin erilaisen tunnuksen.

- Error Status, eli virheiden tilaa, käytetään vastausviesteissä agenteilta hallinta-asemille ilmoittamaan virheistä, jotka ovat syntyneet agentin käsitellessä pyyntö-viestiä. Tällaisia virheilmoituksia ovat noError (ei virhettä), tooBig (liian iso), noSuchName (ei vastaavaa nimeä), badValue (huono arvo), readOnly (vain luku-oikeus) ja genErr (yleisvirhe).
- Error index, eli virheindeksi välittää tietoa muuttujista, jotka aiheuttivat virheen, kun virhe ilmeni.
- Variable bindings, eli muuttuvat liitokset, on pakattua tietoa nimistä ja arvoista joita halutaan lähettää.
- Enterpriseeli yritysmuuttuja, kertoo laitteen tyypin, joka muodostaa liipaisuja (trap).
- Agent addr, eli agentin osoite, ilmoittaa liipaisuja muodostavan laitteen osoitteen.
- Generic trap on yleinen liipaisumuuttuja, jolla on eri arvoja: coldStart (kylmä käynnistys), warmStart (”lempeä” käynnistys), linkDown (yhteys poikki), linkUp (yhteys toiminnassa), authenticationFailure (tunnistuksen epäonnistuminen, egpNeighborLoss (naapurilaite kateissa) ja enterpriseSpecific (yksityiskohtainen yritysmuuttuja).
- Specific Trap, erityinen liipaisu, joka tarkoittaa erillistä laitekohtaista liipaisuarvoa.
- Time stamp eli aikaleima, joka sisältää tiedon siitä, kuinka kauan järjestelmä on ollut toiminnassa snmp-viestien välityksellä. Tätä arvoa kutsutaan sysUPTimeksi, eli järjestelmän käyntiajaksi.
  (H3C Technologies 2008, 9–10.)

3.3.2 SNMPv2

SNMPv2 käyttää myös hallinta-alueen nimeä autentikointiin. SNMPv2 on yhteensopiva SNMPv1:n kanssa, mikä laajentaa SNMPv2:n käytettävyyttä. SNMPv2 parantaa hallinnan tietoturvaa, joustavuutta ja tehokkuutta, sekä laajentaa kuljetusprotokolla-ympäristöä. SNMPv2 sisältää myös tuen hallinnan hajauttamiseen. SNMPv2 tukee useampia datatyyppejä kuin SNMPv1 ja pystyy

siksi välittämään yksityiskohtaisempaa tietoa vioista. (H3C Technologies 2008, 10; Puska 2000, 312; RFC1908 1990 2–4.)



KUVIO 7. SNMPv2 eroavaisuudet SNMPv1:een (H3C Technologies 2008, 10.)

SNMPv2:een on lisätty operaatio GetBulk (kuvio7), joka on verrattavissa GetNext-operaatioon. Määrittämällä GetBulk-operaation Non repeaters- ja Max repetitions-parametrit, saadaan hallinta-asema hakemaan monta mittaustulosta agentilta samalla kertaa. Myös trap-viestit ovat hieman erilaisia SNMPv2:ssa. SNMPv2:n trap-viestin PDU perii pohjan SNMPv1:n Get-, GetNext- ja Set-PDU:sta. sysUPTime- ja snmpTrapOID-muuttujat pakataan ja liitetään viestiin. (H3C Technologies 2008, 10; Puska 2000, 312; RFC1908 1990, 2–4.)

3.3.3 SNMPv3

SNMP-protokollan kolmannessa versiossa on huomattavasti parannettu tietoturvaa ottamalla käyttöön USM- (User-based Security Model) ja VACM (View-based Access Control)-teknologiat. Näistä teknologioista USM valvoo autentikointia ja tiedon yksityisyyttä, kun taas VACM keskittyy hallinnoimaan käyttäjien pääsyä tiettyihin MIB:hin. USM määrittelee käyttäjätunnuksen ja ryhmän, johon käyttäjä kuuluu. Lisäksi USM:n voidaan muokata autentikointi- ja yksityisyystoimintoja. USM:llä voidaan todentaa käyttäjä ja estää luvaton käyttö sekä salata paketit Hallinto-aseman ja agentin välillä. USM varmistaa turvallisemman kommunikointiyhteyden hallinta-aseman ja agentin välille määrittämällä yksityisen autentikoinnin, julkisen autentikoinnin ja täysin julkisen kommunikointiyhteyden. VACM määrittelee viisi elementtiä: ryhmät, turvallisuusasteen, kontekstit, MIB-näkymät ja käytönvalvontapolitiikan. Nämä viisi elementtiä kontrolloivat käyttäjän lupaa päästä käsiksi hallintatietoihin. Vain

oikeilla käyttöoikeuksilla käyttäjä pääsee hallinnoimaan tietoa. VACM:lla voidaan luoda erilaisia käyttäjätyhmiä, joilla on erilaiset näkymät MIB-taulukoihin. Yhteen käyttäjäryhmään voidaan määrittää monta käyttäjää, jolla on sama MIB-näkymä. On syytä ottaa huomioon, että IETF (Internet Engineering Task Force) suosittelee nykyään käytettäväksi vain SNMPv3:a ja on muuttanut jo SNMPv1 ja SNMPv2 virallisen tilan historialliseksi. (H3C Technologies 2008, 10; SNMP Research International Inc. 2011.)

KUVIO 8. SNMPv3-viestin ero SNMP:n aikaisempiin versioihin (H3C Technologies 2008, 10.)

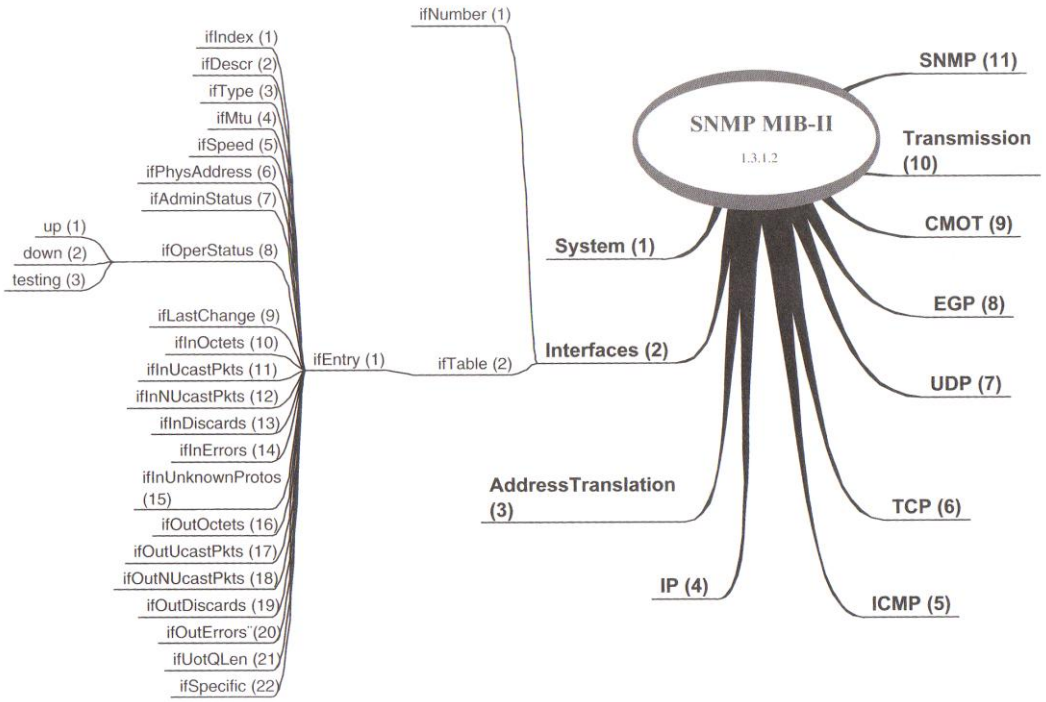
SNMPv3-viestin PDU-pohja on sama kuin SNMPv2:ssa, vaikka SNMPv3-viestin alustaa onkin muokattu. Koko viesti voidaan autentikoida ja viestin kolme viimeistä osiota on salattu. SNMPv3-viestin sisältö eroaa aikaisemmista versioista seuraavasti:

- Max-size, eli maksimikoko, määrittelee erikseen lähetettävän- ja vastaanotettavan viestin maksimikoon, jonka lähettäjän voi viesti sisältää.
- Flags, eli liput, ovat kooltaan vain yhden bitin ja sisällyttävät tiedon autentikoinnista ja viestin yksityisyydestä.
- SecurityModel, eli turvallisuusmalli, on arvoiltaan 0-3. 0 tarkoittaa mitä tahansa turvallisuusmallia. 1 tarkoittaa SNMPv1:n, 2 SNMPv2:n ja 3 SNMPv3:n turvallisuusmallia.
- ContextEngineID ilmoittaa yksityiskohtaisesti SNMP-yksikön. Tämän tiedon avulla päätetään, miten viesti käsitellään.
- ContextName kertoo kontekstin nimen. Jokaisella kontekstin nimi pitää olla erilainen SNMP-yksikkössä.
- AuthoritativeEngineID määrittelee snmpEngineID:n, jota käytetään viestien vaihtamisessa tunnistamiseen, autentikointiin ja salaamiseen.

- AuthoritativeEngineBoots määrittelee arvon, kuinka monta kertaa SNMPEngine on alustanut itsensä sen jälkeen, kun SNMPEngine on alunperin konfiguroitu.
- AuthoritativeEngineTime määrittelee ajan sen perusteella, kuinka monta kertaa SNMP Engine on puuttunut viestien vaihtoon. Käytetään aikaikkunan tarkastamiseen.
- UserName, eli käyttäjänimi määrittelee käyttäjän, jonka toimesta viestejä vaihdetaan. Käyttäjänimen täytyy olla sama hallinta-asemassa ja agentissa.
- AuthenticationParameters tarkoittaa avainta, jota käytetään autentikoinnin laskemiseen. Jos autentikointia ei suoriteta, tämä kenttä on tyhjä.
- PrivacyParameters tarkoittaa parametria, jota käytetään yksityisyyden laskemisessa. Jos viesti halutaan pitää julkisena, kenttä on tyhjä. (H3C Technologies 2008, 10.)

3.4 MIB

MIB on tietokanta tai toisaalta taulukko, joka sisältää erilaisia objekteja. Jokainen tällainen objekti mittaa tiettyä asiaa verkosta tai verkkolaitteesta. MIB-taulukko sisältää yleisiä ja laite- tai toimittajakohtaisia objekteja. Rekisteröityjä objekteja on yli tuhat. Jokainen objekti mittaa jotain arvoa verkon laitteista ja ylläpitää kerättyä tietoa, jota sitten välitetään SNMP:llä hallinta-asemalle. Jotta MIB-taulu olisi selkeä ja johdonmukainen, MIB-taulu on rakennettu puumalliseksi hierarkiaksi, jonka SMI-määrittelee tarkemmin. MIB-taulukosta on tehty kaksi versiota, MIB I ja MIB II, joista jälkimmäinen on laajempi kokonaisuus ja käsittää enemmän objekteja. (Jaakohuhta 2002, 309–311.)



KUVIO 9. SNMP MIB II-taulukko, jossa OID:it (Puska 2000, 310)

Puun yläosan objektit ovat ISO:n (International Standard Organization) määrittelemiä ja puun alaosan objektit määrittelevät eri laitetoimittajat tai organisaatiot. Jokaisella objektilla on tunnus (ID), ja siksi objekteihin viitataankin yleisesti OID-nimityksellä (Object IDentifier). OID:t määritellään sen mukaan, miten OID:t ovat sijoittuneet MIB-taulukkoon. Jokainen OID sisältää kentät, jotka määrittelevät nimen, luku- ja kirjoitusoikeudet sekä sijainnin SMI:n määrittelemässä MIB-hierarkiassa. Esimerkiksi kuvion 9 mukaan, liitynnän toimintatilaa kuvaa OID 1.3.1.2.2.2.1.8. (Jaakohuhta 2002, 309–311; Puska 2000, 310.)

3.5 SMI

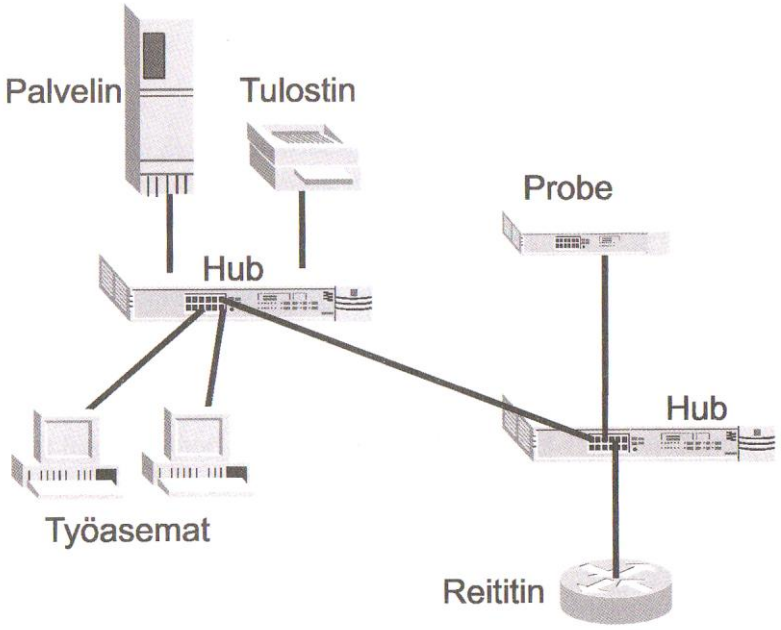
Objektit MIB-taulukossa on määritelty käyttämällä ASN.1-standardia (Abstract Syntax Notation One). Jokaisella objektilla MIB-taulukossa tulee olla nimi, syntaksi ja koodaus. Nimeä kutsutaan yleisesti OID:ksi, kuten aikaisemmin jo tässä työssä todettiin. Objektien nimet on määritelty niin, että nimet kuvaavat objektin keräämää tietoa ja nimet ilmoitetaan MIB-puussa. Syntaksi on tiivistelmä

tiedon rakenteesta, joka vastaa objektin tyyppiä. Objektin tyyppi on kokonaisluku tai merkkijono, joka määriellään objektin rakenteessa. Objektin tyypin koodauksella tarkoitetaan sitä, kuinka tietyn objektin tyypin tapaukset esitetään käyttäen objektin tyypin syntaksia. (RFC1155 1990, 1–8; Jaakohuhta 2002, 310.)

Yksinkertaistettuna käsite objektin syntaksista ja koodauksesta ilmoittaa, kuinka objekti on muotoiltu ennen kuin objektin sisältämä tieto lähetetään verkkoon. SMI määrittelee siis MIB-objektien hierarkisen nimirakenteen, sekä tunnistaa objekteista niiden tietotyypit ja määrittelee tiedon esitystavan. (RFC1155 1990, 1–8; Jaakohuhta 2002, 310.)

3.6 RMON

Hallinta-asemien kerätessä tietoa verkkolaitteiden tilasta SNMP-protokollan avulla verkkoon aiheutuu huomattavasti ruuhkaa ja pahimmassa tapauksessa hallinta-asema ylikuormittuu. Tämän estämiseksi on kehitetty RMON, joka on tiedonkeruumenetelmä, jossa verkkoon asennetaan erillinen laite- tai ohjelmisto, joka kerää tietoa verkosta ja tallentaa tiedon omaan tiedostoonsa (MIB). Tällöin verkkoon ei kehity verkonvalvonnan aiheutumaa ruuhkaa niin paljon kuin normaalia SNMP- tiedonkeruumenetelmää käytettäessä, vaan tiedot voidaan käydä lukemassa RMON-asemalta silloin, kun siihen on tarvetta. RMON:ssa on kehittyneemmät tiedonkeruu- ja raportointimahdollisuudet kuin SNMP:ssä ja sillä on oma MIB-taulukkonsa, jonne RMON tallentaa keräämänsä tiedot. (Jaakohuhta 2002, 311–315.)



KUVIO 10. RMON-tiedonkeruuyksikkö (probe) lähiverkossa (Jaakohuhta 2002, 312)

RMON-asemia sanotaan keruuyksiköiksi (probe) ja niitä voidaan sijoittaa lähes mihin tahansa verkkolaitteeseen (kuvio10). Saatavilla on myös erillisiä verkkoon liitettäviä RMON-laitteita, jolloin RMON-tiedonkeruuyksikköä ei tarvitse määritellä muihin verkkolaitteisiin. RMON toimintamallissa palvelin-asiakassuhde muuttuu päinvastaiseksi, jolloin hallinta-asema toimii asiakkaana ja RMON-keruuyksikkö toimii palvelimena. SNMP-protokollalla välitetään tietoa RMON-keruuyksikön ja hallinta-aseman välillä. Tieto välitetään kokonaisuutena RMON-asemalta hallinta-asemalle ja vain silloin kun sille on tarvetta. Siksi tämä menetelmä ei ruuhkauta verkkoa yhtälailla kuin SNMP-tiedonkeruumenetelmää käytettäessä. RMON-keruuyksikkö voi myös lähettäää hallinta-asemalle hälytyksen, jos joku asetettu vikakynnys ylittyy tai alittuu. (Jaakohuhta 2002, 311–315.)

3.7 SNMP-protokollaan perustuvan verkonvalvontasovelluksen toiminta

Hallinta-asemassa ajetaan verkonhallintasovellusta, joka kerää SNMP:llä tietoa verkon laitteista ja verkosta ja tallentaa tietoja omaan tietokantaansa. Lähes

kaikissa nykyisissä verkonvalvontasovelluksissa voidaan automaattisesti etsiä verkon laitteet erilaisilla hakukriteereillä ja muodostaa tiedoista valvottavan verkon topologia-kuva. Käyttäjällä on yleensä näkymä josta voi tarkkailla yleisesti verkon tilaa ja laitteita, tai sitten yksityiskohtaisia näkymiä, joissa voidaan tutkia tarkemmin jonkun tietyn laitteen tilaa ja laitteen tallentamaa tietokantaa. Yleisesti verkonvalvontasovelluksista löytyy toiminnot, joilla voidaan tarkkailla verkon tilaa, tutkia verkon topologia-karttaa, tarkkailla verkon liikennemääriä, muodostaa raportteja ja tarkastella historiatietoja. Agentit voivat lähettää hallinta-asemalle trap-viestejä joilla käynnistetään hälytystoiminta verkonvalvontasovelluksessa. Hälytys perustuu usein jonkun ennalta määritellyn raja-arvon ylitykseen tai alitukseen, kuten esimerkiksi liian suureen liikennemäärään. (Jaakohuhta 2002, 306–309.)

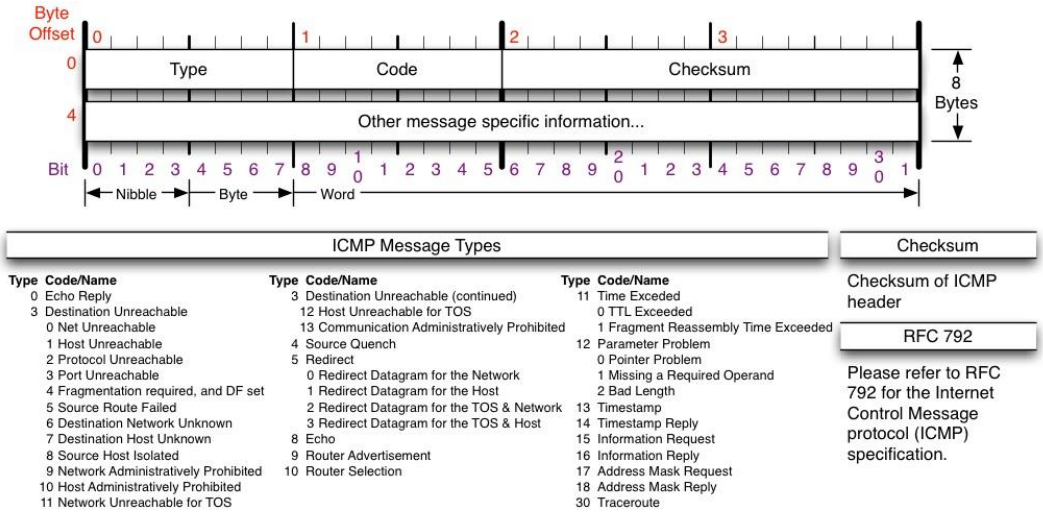
SNMP:n suurin heikkous on, että laitteiden MIB-tauluihin täytyy tallentaa suuri määrä tietoa. SNMP:tä käytettäessä on hyvin tärkeää ymmärtää mitä halutaan verkosta tai laitteesta mitata. Ylimääräisten ja turhien tietojen mittaaminen kuormittaa verkkoa ja hallinta-asemaa aivan turhaan. Siksi SNMP:n käyttäminen onkin yksinkertaisempaa, jos käytössä on hyvä verkonvalvontasovellus, joka tarjoaa hyvät työkalut SNMP:n käyttämiseen. Sovellukset sisältävätkin yleensä toimintosarjoja joilla saadaan verkosta ja laitteista perustiedot näkyviin. Hyvän verkonvalvontasovelluksen tunnuspiirteisiin kuuluukin, että sillä pystytään valvomaan eri valmistajien laitteita vain yhtä käyttöliittymää ja samoja työkaluja käyttäen. (Ballew 1998, 209–210.)

3.8 ICMP

ICMP (Internet Control Message Protocol) on luotu erilaisten virhetilanteiden välittämiseen verkossa. Protokollapinossa ICMP on heti IP:n yläpuolella. Oikeastaan ICMP on osa IP-protokollaa ja on siten käytössä kaikissa IP-moduuleissa. ICMP-viestejä lähetetään erilaisissa tilanteissa, kuten silloin kun paketti ei pääse kohdeosoitteeseensa tai yhdyskäytävällä ei ole kapasiteettia

välittää viestiä ja silloin kun tiedossa on lyhyempi reitti paketin välittämiseen. (RFC792 1981, 1–2.)

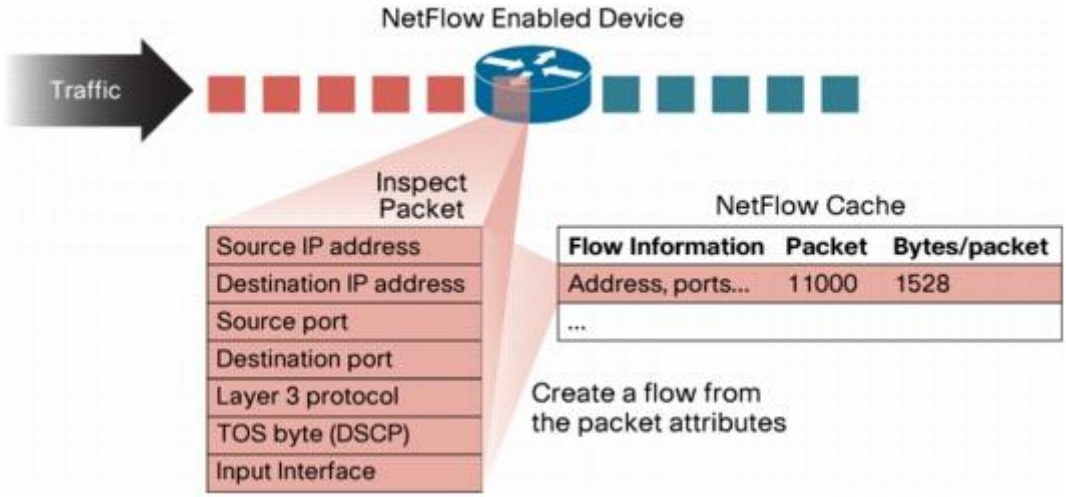
ICMP-sanomat kuljetetaan IP-sanoman sisällä. ICMP:llä oma kuljetustapakerroksen numero 1, joka mahdollistaa ICMP-viestin kuljettamisen IP-sanoman sisällä. ICMP-sanoma (kuvio 11) sisältää tyypin, koodin, tarkistussumman ja kentän, jossa määritellään muu viestiin liittyvä informaatio. (RFC792 1981, 4)



KUVIO 11. ICMP-sanoma (Boon, 2009, ICMP Header.)

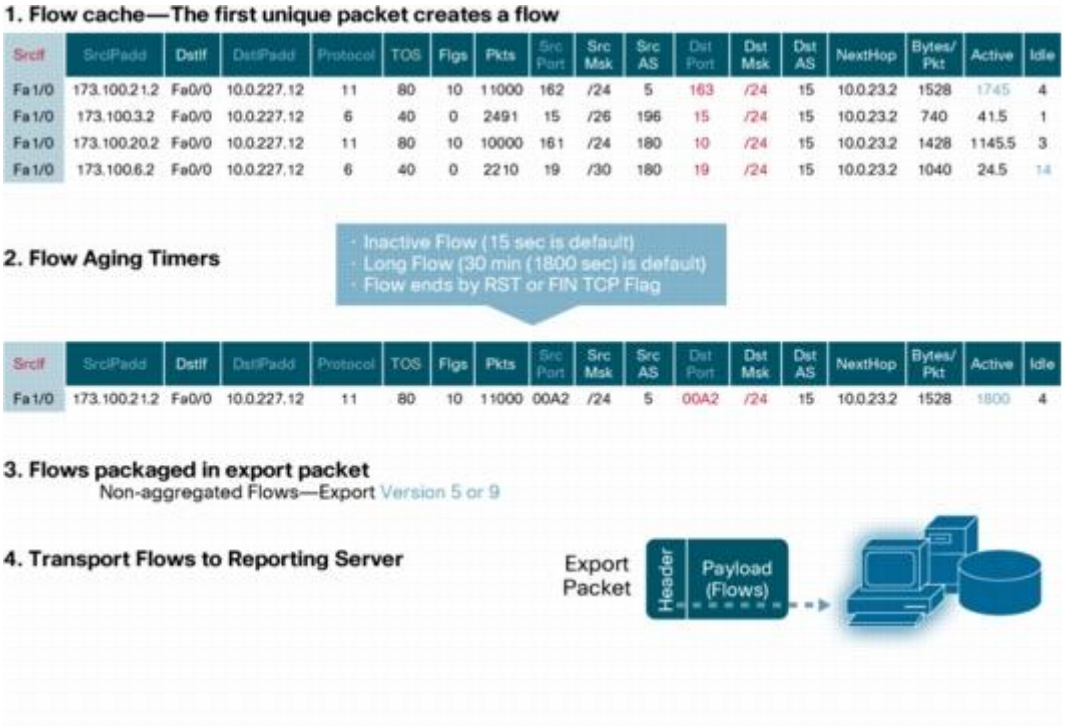
ICMP-sanomassa tyyppi-kenttä ilmoittaa minkälainen viesti on kyseessä. Koodi-kentällä tarkennetaan viestityypille ominaisia määrittelyjä. Tarkistussummaa käytetään paketin eheyden tarkistamiseen. (RFC792 1981, 5.)

3.9 NETFLOW



KUVIO 12. Cisco Netflow-protokollan toiminta (Cisco 2007.)

Netflow on Ciscon kehittämä protokolla IP-liikenteen seurantaan. Protokollalla saadaan verkosta yksityiskohtaisempaa tietoa verkon liikenteestä. Jos verkko esimerkiksi ruuhkaantuu, voidaan netflown avulla tutkia, mikä ohjelma, laite tai käyttäjä aiheuttaa verkon ruuhkaantumisen. Netflown IP-paketti sisältää lähde- ja kode IP-osoitteen, lähde- ja kohdeportin, IP-protokollan, palveluluokan sekä reitittimen tai kytkimen liitynnän (kuvio 12). (Cisco 2007.)



KUVIO 13. Esimerkki Netflow-protokollalla kerätystä liikenteestä verkossa (Cisco 2007.)

Netflow-protokollaan on kehitelty jo yhdeksän versiota. Niistä yleisin on versio viisi, koska suurin osa laitteista tukee sitä. Versio viisi rajoittuu Ipv4-liikenteen virran seurantaan, kun taas versio yhdeksään on otettu mukaan Ipv6-tuki. Netflow on hyvä protokolla verkon liikenteen tarkempaan valvontaan (kuvio 13), koska sillä päästään esimerkiksi vikatilanteissa jäljittämään verkkoa ruuhkauttava tekijä, tai ehkäisemään verkon ruuhkautuminen jo etukäteen. (Cisco 2007.)

3.10 WMI

WMI (Windows Management Instrumentation) on Windows-käyttöjärjestelmille kehitetty hallintatietojen ja operaatioiden infrastruktuuri. WMI:llä voidaan kirjoittaa skriptejä tai luoda ohjelmia, jotka toteuttavat hallinnollisia tehtäviä etä-koneilla. Lisäksi ohjelmalla voidaan kerätä verkonvalvontatietoja windows-pohjaisilta etäkoneilta. WMI:tä käytetään pääasiassa erilaisissa yrityssovelluksissa ja hallinnollisten skriptien luomisessa. WMI käyttää CIM-standardia (Common Information Model) järjestelmän, ohjelmien, verkon, laitteiden ja muiden valvottavien komponenttien määrittämiseen. (Microsoft 2011.)

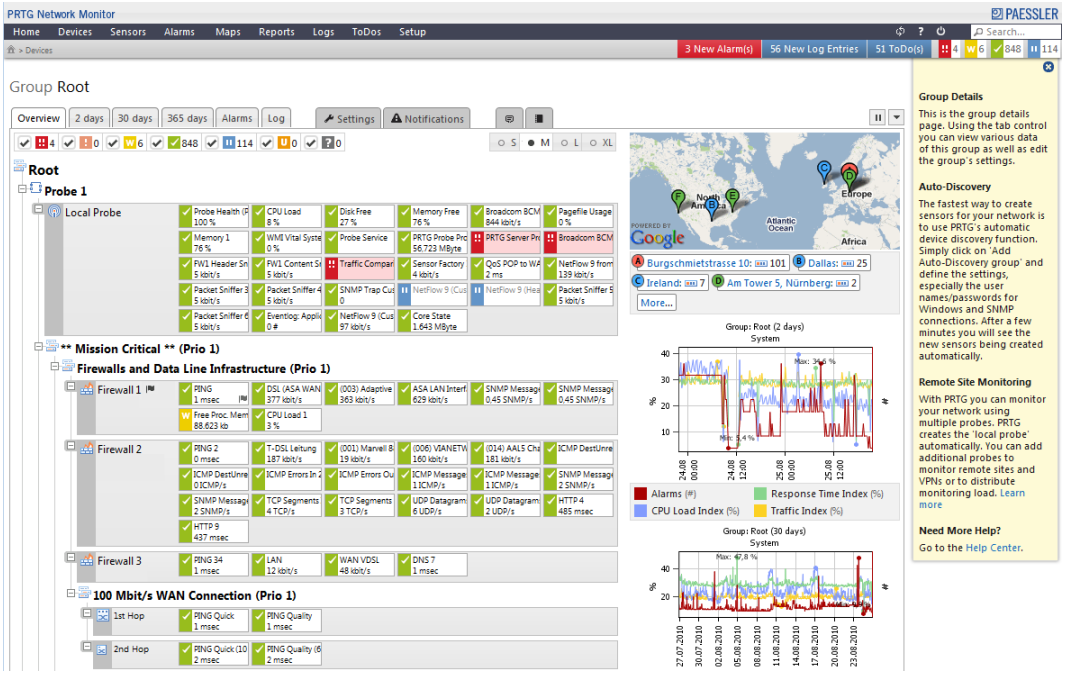
Verkonhallintatietoihin päästään käsiksi WMI:n avulla määrittelemällä ohjelmassa valvottavan windows-koneen nimi, käyttäjätunnus ja salasana. Etäkoneelta kerätään hallintatietoja, jotka on määritelty käytettävässä ohjelmassa. Lisäksi WMI:tä hyödyntävässä ohjelmassa voidaan toteuttaa WMI:n avulla myös hallinnollisia tehtäviä, kuten vaikkapa käynnistää etä-hallittava laite uudellen. (Microsoft 2011.)

4 TESTATTUJEN VERKONVALVONTASOVELLUSTEN ESITTELY

Tämän opinnäytetyön tavoitteena on tarkoitus perehtyä verkonvalvontaan, löytää mahdollisimman hyvä verkonvalvontaratkaisu Mediatalo ESA:lle sekä suunnitella uuden verkonvalvontajärjestelmän käyttöönotto. Mediatalo ESA:lla on käytössään MRTG-ohjelma, jolla valvotaan verkon liikennettä ja What's Up Gold, jolla valvotaan verkkoa yleisesti. Nämä ohjelmat ja verkonvalvontatoteutus ovat vanhoja ja siksi Mediatalo ESA haluaa uudistaa verkonvalvonnan.

Yhdessä Mediatalo ESA:n tietohallinnon yhteyshenkilön kanssa etsittiin tietoa erilaisista verkonvalvontajärjestelmistä ja -sovelluksista. Tämän opinnäytetyön tutkimuksien vertailuun otettiin viisi ohjelmaa: PRTG, OP5, ZenOSS, Neteye ja What's Up Gold-ohjelman uudempi versio.

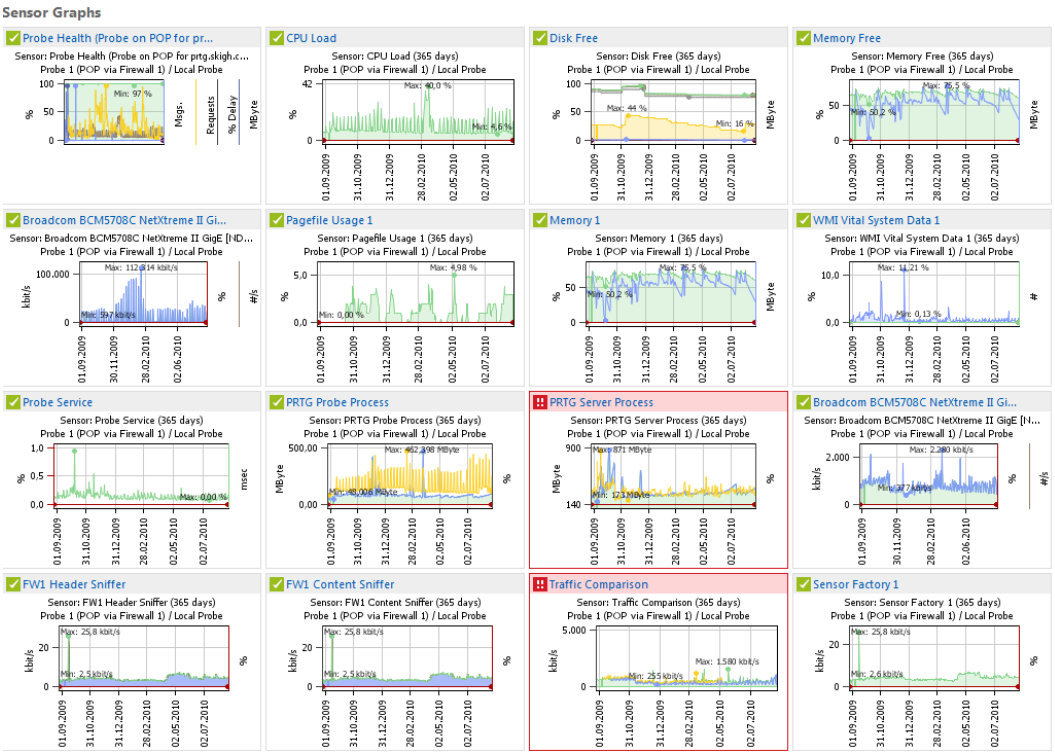
4.1 PRTG



KUVIO 14. PRTG-verkonvalvontaohjelman yleisnäkymä (Paessler 2011)

Saksalainen Paessler Company on kehittänyt verkonvalvontaohjelman nimeltä PRTG. Ohjelman parhaisiin ominaisuuksiin kuuluu automaattinen etsintä, joka ei

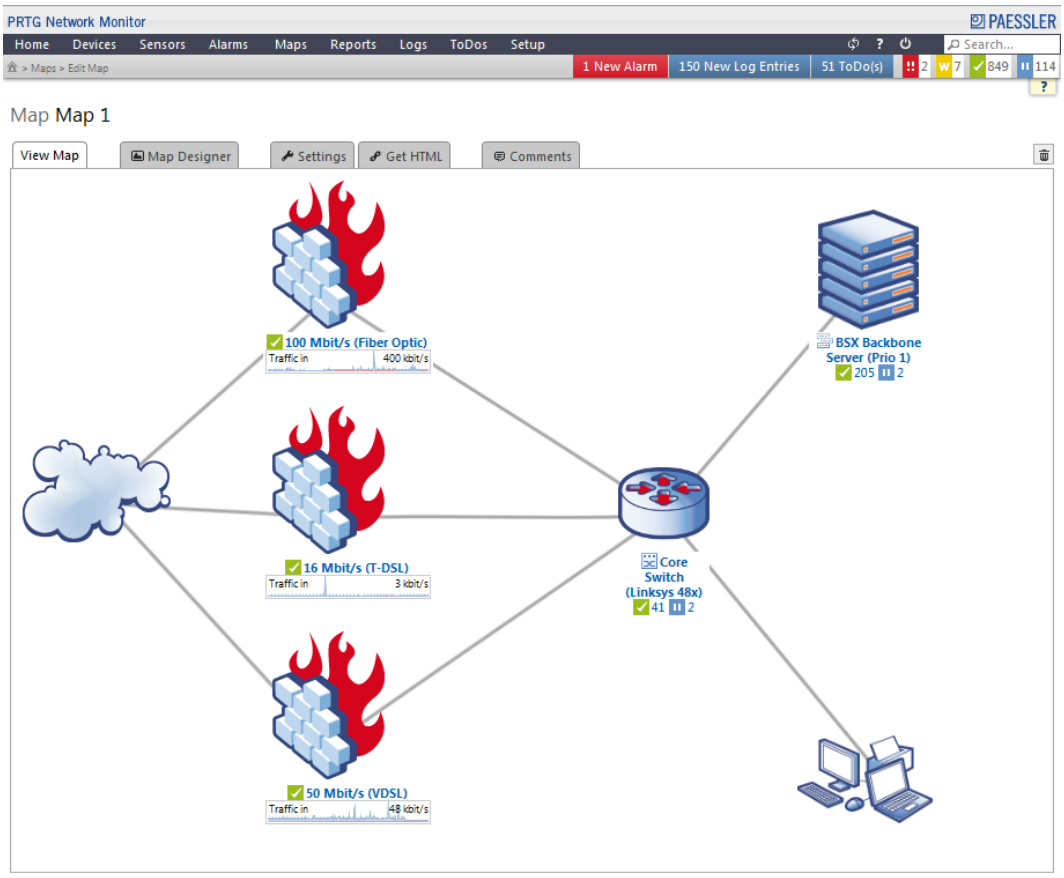
rajoitu pelkästään laitteiden etsimiseen, vaan ohjelmalla voi sisällyttää hakuun myös erilaiset laitteiden mittauskohteet eli sensorit. Ohjelma toimii windows xp- ja sitä uudemmilla alustoilla. Ohjelmaan kuuluu Web-hallinta-, Windows-hallinta- ja Mobiilihallinta-mahdollisuudet. Päänäkymä ohjelmassa on selkeä ja informatiivinen (kuvio 14). Ohjelman hallinta on helppokäyttöinen ja monipuolinen ja hallinta toimii jouhevasti ja johdonmukaisesti.



KUVIO 15. Esimerkkikuva PRTG:n graafisista talukoista (Paessler 2011)

Ohjelman vahvuuksiin kuuluu selkeät ja monipuoliset graafiset taulukot (kuvio15), joita pääsee tarkastelemaan yleisesti, laitekohtaisesti tai sensorikohtaisesti. Ohjelma tukee monia eri protokollia verkon laitteiden ja itse verko valvomiseen, joista tärkeimpänä mainittakoon ICMP, SNMP, Netflow ja SSH. Lisäksi ohjelma tukee WMI:tä ja API:a (Application Programming Interface), jotka mahdollistavat hallinta-aseman kirjautumisen verkkolaitteisiin ja sitä kautta pääsyn mitattaviin ominaisuuksiin. Ohjelmassa on paljon valmiita sensoreita, jotka perustuvat yleisesti rekisteröityihin MIB-objekteihin (OID). Lisäksi sovelluksen avulla voi luoda itse haluamiaan sensoreita. PRTG tarjoaa monipuoliset raportit, erilaiset vertalutaulukot ja tapahtumien loki- ja

historianseurannan. Hälytykset toimivat jouhevasti, ja niitä on mahdollisuus välittää eteenpäin verkonvalvojalle esimerkiksi sähköpostin ja tekstiviestin välityksellä. Ohjelmaan voi luoda käyttäjätilejä ja käyttäjäryhmiä. PRTG tarjoaa jokaisen lisenssin myötä myös mahdollisuuden verkonvalvonta-aseman klusterointiin, eli kahdentamiseen, joka mahdollistaa järjestelmän vikasietoisuuden. Ohjelmaan on tarjolla erilaisia lisäominaisuuksia, kuten Iphone-sovellus, erilaisia ladattavia plugin-komponentteja ja Windowsiin lisättävät gadgetit.



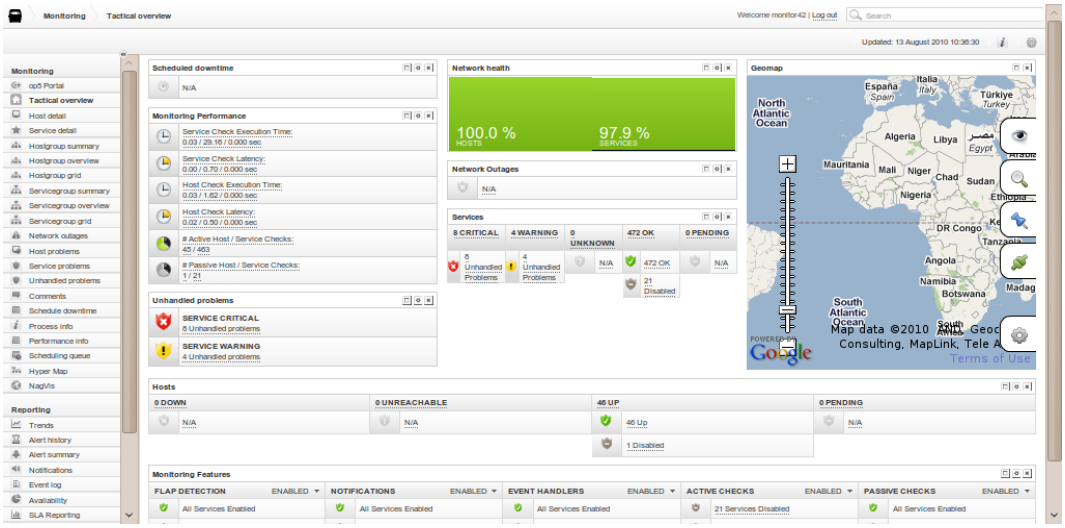
KUVIO 16. Esimerkkikuva PRTG:llä luodusta verkkotopologiakartasta (Paessler 2011)

Ohjelma tarjoaa mahdollisuuden verkon topologia- ja sijaintikarttojen luomiseen. Jos yrityksellä on etäkonttoreita tai toimipisteitä, jotka liittyvät valvontaan, on erilaiset toimipisteet mahdollista näyttää google-mapsin avulla karttakuvassa. Topologiakarttojen (kuvio 16) luominen on selkeää ja helppoa, mutta tätä

ominaisuutta PRTG:ssä voisi parantaa niin, että linkkien ruuhkautuminen näkyisi laitteiden välillä selkeämmin.

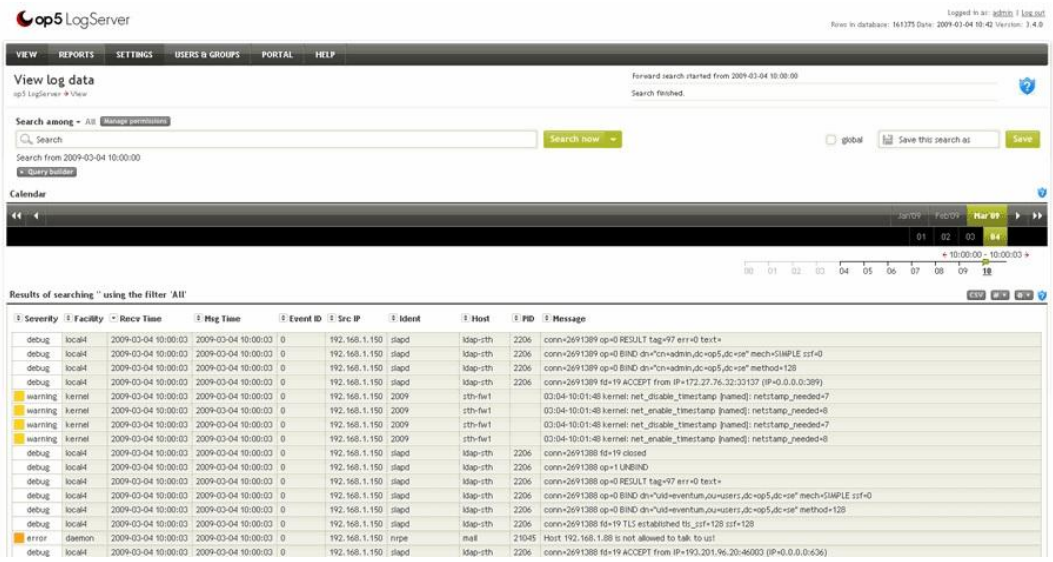
4.2 OP5

OP5 on unix-alustalle rakennettu verkonhallintasovellus, joka tukee RedHat- ja Centos-käyttöjärjestelmiä. OP5 Network Management Suite koostuu kolmesta osasta: OP5 Network Monitorista, OP5 Log Serveristä ja OP5 Statisticsista. Ohjelmat voi myös tilata erikseen, jos ei ole tarvetta kaikille kolmelle ohjelmalle. OP5 Network Monitor on suuniteltu verkonvalvontaa varten. OP5 Log serverillä voidaan seurata laitteiden lokitietoja ja OP5 statistics -ohjelmalla voidaan muodostaa karttoja ja kerätä verkosta statistiikkaa. OP5 perustuu Nagios-alustaan, joka on avoimeen lähdekoodiin perustuva verkonhallintaohjelma, joka on suunniteltu toimimaan linux- ja unix-pohjaisissa käyttöjärjestelmissä. Nagios käyttää Plugineja, eli pieniä lisäkomponentteja, joilla voidaan tehdä palvelin- ja palvelutarkastuksia ja kehittää niitä. Lisäksi Nagioksella valvotaan mm. HTTP, SMTP, PING, SSH, NNTP, FTP, DNS, POP ja Telnetiä. Netflow-tuki puuttuu OP5-ohjelmista kokonaan. Yrityksille tarjottava ohjelmalisenssi on kuukausiveloitteinen, joten ohjelman käytöstä muodostuu yritykselle helposti suuria kustannuksia.



KUVIO 17. OP5 Network -monitorin päänäkymä (OP5 2010)

OP5 on monipuolinen ohjelmakokonaisuus (kuvio 17), joka juuri monipuolisuutensa takia tuntuu melko sekavalta käyttää. Ohjelmasta löytyy paljon ominaisuuksia, jotka on esitetty tavalla, joka vaatii perinpohjaista perehtymistä ohjelman käyttöön. Ohjelma perustuu erilaisten template- eli alustojen luontiin. Näitä alustoja luodaan eri palveluille, hälytyksille, käyttäjäryhmille ja laitteille. Alustat otetaan sitten käyttöön eri laitteissa ja niiden avulla muodostetaan valvontakokonaisuus. Tämä on monimutkainen prosessi ja luo käyttäjälle sekavan kokemuksen ohjelman käytöstä. Mahdollisuus vaikuttaa erilaisiin komponentteihin eri alustoilla on erittäin hyvä. Alustoja muokkaamalla laitekohtaisesti, saadaan varmasti luotua erinomainen verkonvalvontakokonaisuus, mutta tämän toteuttaminen vaatii huomattavan suuren määrän työtä ja paljon aikaa.

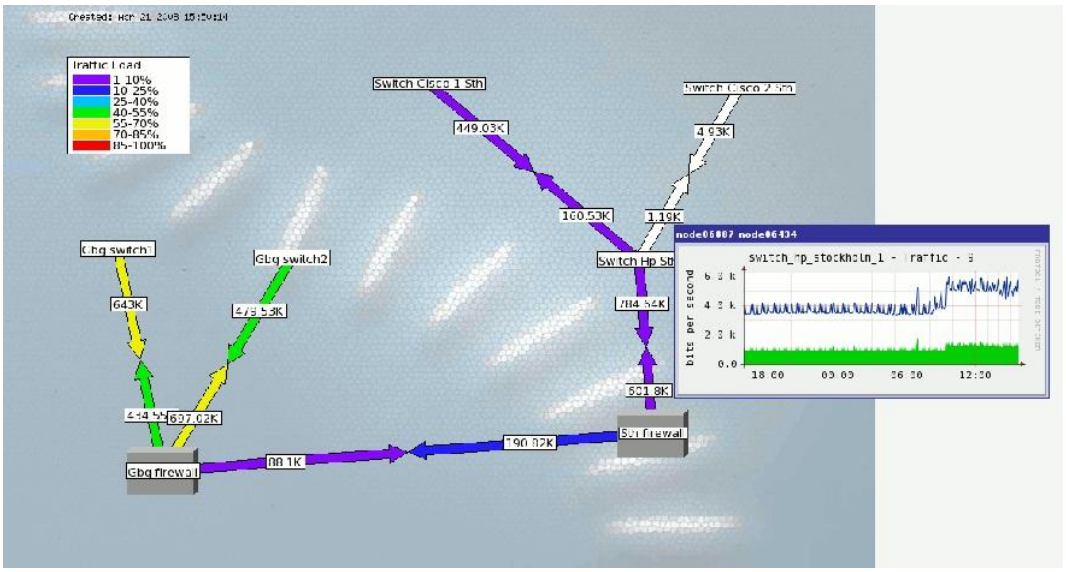


KUVIO 18. OP5 Log Server:in näkymä kerätyistä lokitiedoista (OP5 2010)

OP5 Log Server toimii hyvin, kun lokeja valvottavalle laitteelle luodaan asetukset ,joilla lokitiedot lähetetään lokipalvelimelle. Ohjelmalla voidaan kerätä tietoa lokeista (kuvio 18) ja asettaa hälytyksiä erilaisille lokimuutoksille. Ohjelma tallentaa lokit jälkitarkastelua varten. Lisäksi lokeista voi muodostaa erilaisia raportteja joilla voidaan valvoa lokitietoja.

KUVIO 19. OP5 Statistics- ohjelman muodostama Graafinen taulukko verkon liikenteestä (OP5 2010)

OP5 Statistics -ohjelmalla voidaan muodostaa graafisia taulukoita, jotka antavat verkonvalvojalle hyvän kuvan verkon tilasta ja tapahtumista (kuvio 19). Taulukot ovat selkeitä, ja niitä on melko helppo luoda eri laitteille.



KUVIO 20. OP5 Statistics ”weather-map” kartta (OP5 2010)

Ohjelman parhaisiin puoliin kuuluu kartat (kuvio 20), joita sillä voidaan luoda. Kertat antavat selkeän kuvan verkon ruuhkaantumisesta ja laitteiden välisten linkkien tilasta. Kartasta näkee laitteiden välisten linkkien liikenteen aiheuttaman kuorman selkeästi väreinä. Tämä ominaisuus puuttuu monesta muusta verkonvalvonta-ohjelmasta.

4.3 ZenOSS

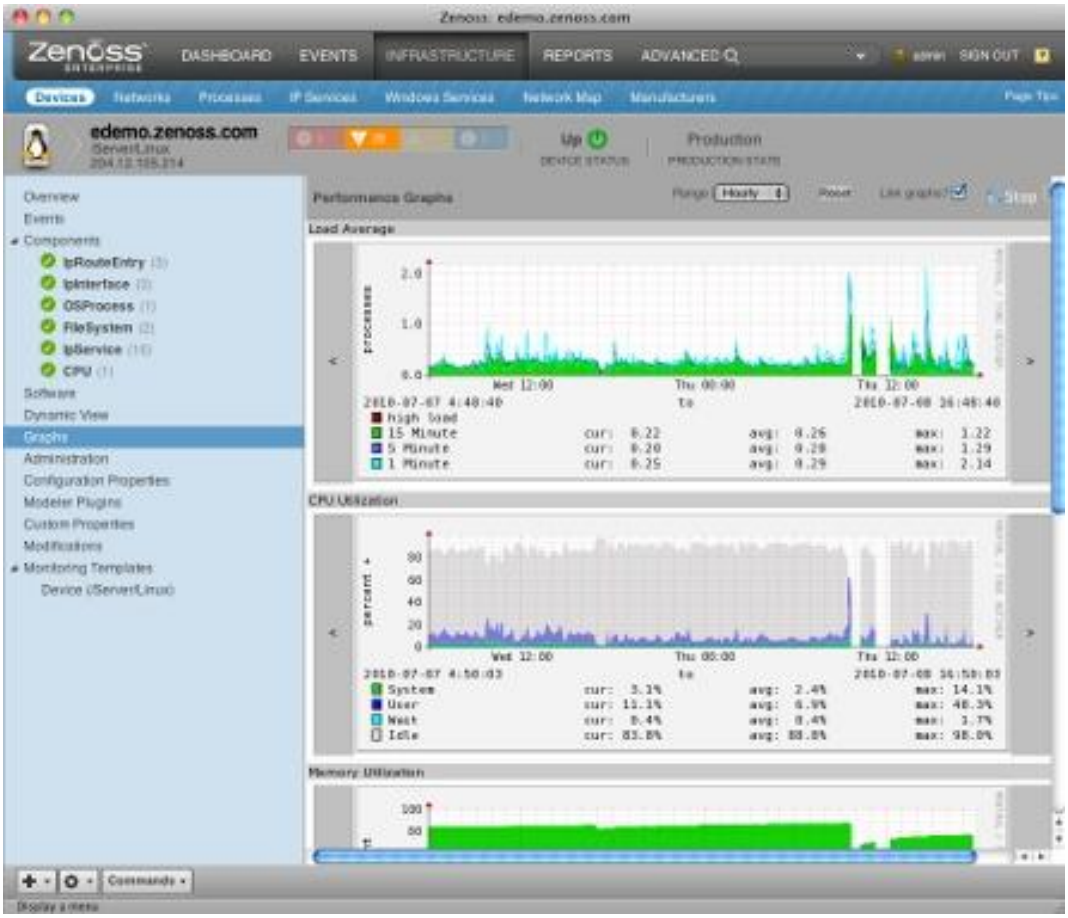
ZenOss on Open Source -ohjelma, johon on mahdollisuus ostaa (melkoisen kallis) lisenssi, jolla saadaan ohjelmalle asiantuntijatuki. Alustana ohjelmalle toimii eri unix-pohjaiset alustat, kuten CentOS, RedHat ja Ubuntu. Ohjelma on ilmainen ja jatkuvaa kehitystyötä tapahtuu Open Source -ohjelmien periaatteella. Päivitykset ovat ilmaisia, ja ongelmatilanteissa on helppo käyttää kehittäjien tekemiä foorumeja, jolloin ei tule tarvetta hankkia kallista lisenssiä asiantuntijatukea varten.

KUVIO 21. ZenOSS-ohjelman päänäkymä (ZenOSS 2011)

ZenOSS on käytettävyydeltään melko selkeä ja helppokäyttöinen niin kauan, kunnes halutaan lisätä uusia sensoreita laitteille tai laiteryhmille (kuvio 21). Erilaisille laiteryhmille, kuten esimerkiksi kytkimet ja reitittimet, on asetettu oletuksena tiettyjä mittausominaisuuksia. Näitä hallitaan ryhmäkohtaisilla template- eli alustapohjilla. Alustapohjat toimivat ihan hyvin siihen asti, kunnes halutaan jotain sellaista tietoa laitteesta, mitä ei valmiista alustasta löydy. Silloin ohjelma muuttuu hankalaksi käyttää, koska jokaiselta laitteelta joudutaan erikseen katsomaan, mitä MIB-tauluja ne tukevat. Sensorit täytyy määritellä OID kerrallaan laitekohtaisesti, mikä on työlästä ja aikaa kuluttavaa. MIB-tauluja erilaisille laitteille voidaan hakea internetin kautta ZenPack-pakettien avulla. Web-hallinta on melko raskas ja tuntuu välillä hieman takkuilevan eri selaimilla.

KUVIO 22. ZenOSS- ohjelmalla luotu kartta verkon laitteista (ZenOSS 2011)

Yksi innovatiivisimmista ominaisuuksista ZenOSS-ohjelmassa on ohjelmalla luodut kartat (kuvio 22). Nämä kartat voidaan luoda automaattisen laitteiden etsinnän yhteydessä. Ohjelma piirtää kartan automaattisesti. Kartan objekteja voi liikutella karttanäkymässä ja eri laitteiden ja verkkojen näkymään pääsee melko kätevästi niiden kuvakkeita napauttelemalla. Karttaan ei kuitenkaan voi itse lisäillä laitteita, mikä on hieman kömpelöä. Lisäksi kartta-ominaisuus vaatii flash-tuen, ja on siksi myös hieman raskaampi hallinta-aseman kannalta käyttää.

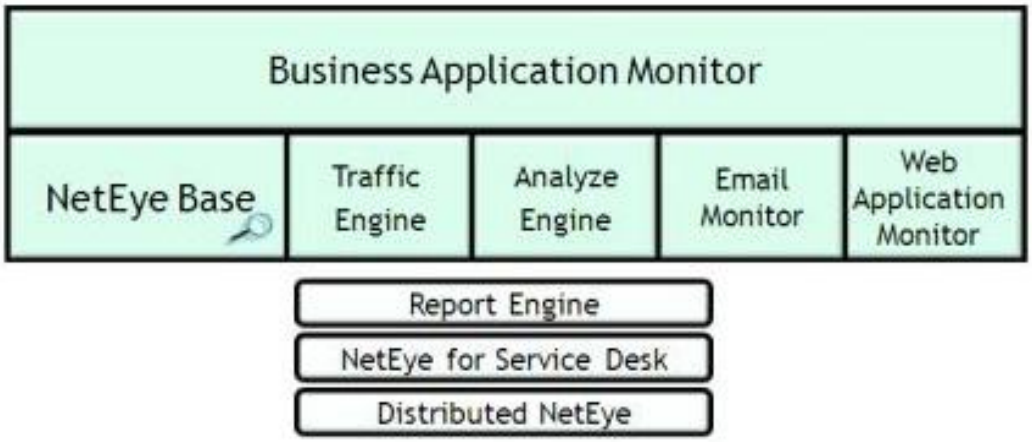


KUVIO 23. ZenOSS ohjelman muodostamat graafiset taulukot. (ZenOSS 2011)

ZenOSS ohjelmalla voidaan luoda graafisia taulukoita (kuvio 23) mittaustulosten perusteella. Jos sensoreita ei ole määritelty valmiiksi laitteelle, joudutaan ensin lisäämään sensorit OID:ien perusteella, minkä jälkeen luodaan graafiset taulukot itse määrittelemäällä taulukon arvot ohjelmaan. ZenOSS:lla on mahdollista myös

luoda ns. rack-näkymä eli näkymä siitä, kuinka laitteet on laitetilassa sijoitettu telineisiin. Lisäksi ohjelmalla voidaan piirtää pohjakuva yrityksen verkkolaitteista ja laitetiloista erikseen.

4.4 Neteye



KUVIO 24. Noval Neteyen tuotteet (Noval Networks 2011)

Neteye on suomalaisen Noval Networksin kehittelemä verkonvalvontakokonaisuus. Neteyeta myydään palveluna, johon kuuluu aina ennalta neuvoteltujen verkonvalvontapalveluiden käyttöönotto ja tukipalvelut. Neteye-tuoteperheeseen kuuluu seitsemän tuotetta, joista valitaan yritykselle sopiva kokonaisuus, jolla verkonvalvonta toteutetaan (kuvio 24). Nämä seitsemän tuotetta ovat

- Neteye base, joka on perustyökalu verkonvalvontaan
- Business Application Monitor, jolla toteutetaan käytettävyyden seuranta
- Analyze Engine, joka vastaa protokollatason analysoinnista ja vasteaikojen mittaamisesta
- Traffic engine, jolla mitataan verkon suorituskykyä ja toimivuutta
- Report Engine, jolla toteutetaan raportointi
- Network Device Backup Engine, joka varmistaa verkkolaitteiden konfiguraatioiden säilymisen ja hallinnan
- Backup Monitor, jolla valvotaan järjestelmän varmuuskopioita

Lisäksi Neteye-palveluun kuuluu yrityksen verkon ulkopuolinen valvonta Noval Networksin toimesta. Tämä mahdollistaa yrityksen verkkopalveluiden ja sähköpostin valvomisen yriyksen sisäverkon ulkopuolelta. (Noval Networks 2011)

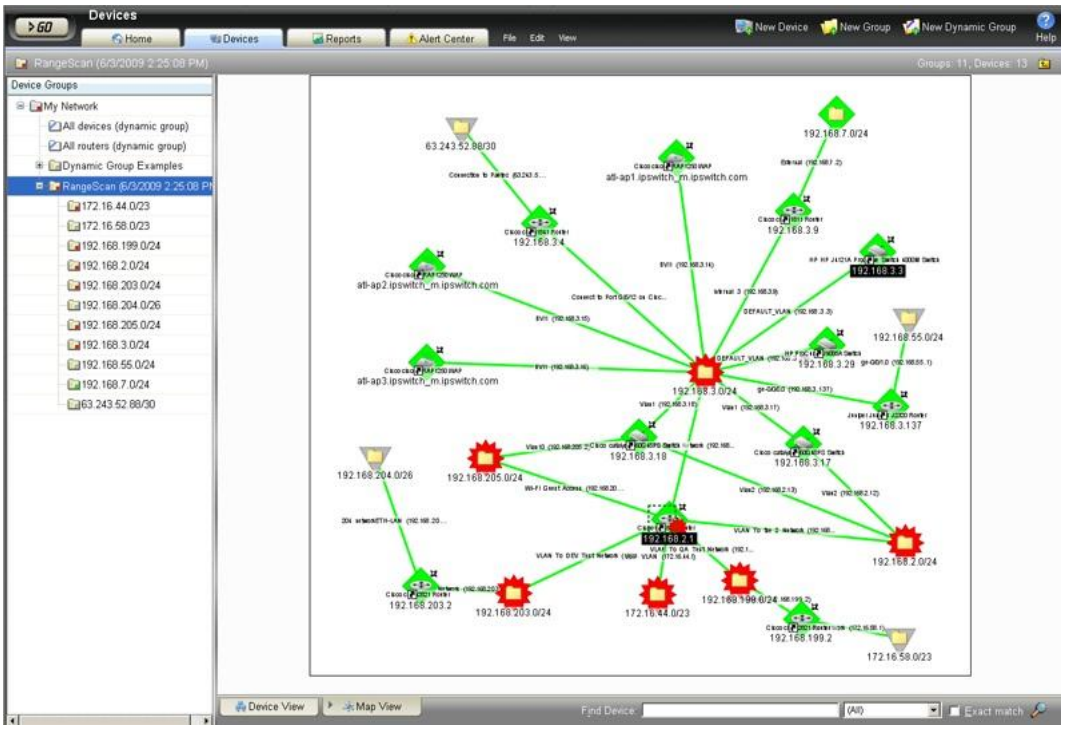
Ohjelma vaikuttaa selkeältä kokonaisuudelta. Ohjelman vahvimpiin ominaisuuksiin kuuluu laitteista mitattavien ominaisuuksien yhdistäminen yrityksen hallinnolliseen näkökulmaan. Tällä tarkoitetaan sitä, että ohjelmalla voidaan luoda taulukko esimerkiksi siitä, kuinka paljon jonkun tietyn laitteen toimimattomuus on aiheuttanut menetettyjä työtunteja, tai kuinka paljon laitteen toimimattomuus on maksanut yritykselle. Ohjelman käytettävyys on selkeä ja johdonmukainen. Graafiset taulukot ovat selkeitä ja käytännöllisiä.

Ohjelma on keskeneräinen, koska siitä puuttuu topologiakarttojen tekemisen mahdollisuus, sekä tietyt linkitykset ohjelman sisäisesti ovat puutteellisia. Ohjelma tukee pääasiassa vain ICMP- ja SNMP-protokollia, eikä heikon protokollatuen vuoksi kykene kovin monipuoliseen verkonvalvontaan verrattuna nykypäivän muihin verkonvalvontasovelluksiin. Lisäksi ohjelman käyttöönotto maksaa erikseen ja lisäksi palveluiden käytöstä joutuu maksamaan kuukausittaisen korvauksen, joten ohjelma muodostuu helposti kalliiksi. Erittäin hyvä ominaisuus ohjelmassa on yrityksen ulkoapäin toteutettava verkkopalveluiden ja sähköpostipalveluiden seuranta. Lisäksi tukipalvelut sijaitsevat lähellä ja apua ohjelman käytön kanssa saa suomeksi.

4.5 What’s up GOLD

What’s Up Gold toimii Windowsin päällä ja lisenssihinta on keskitason luokkaa. Lisenssiin kuuluu päivitykset ja asiantuntijatuki. Ohjelmassa on Windows-hallinta, Web-hallinta ja mahdollisuus myös mobiilihallintaan. What’s Up Goldiin on tarjolla erilaisia lisäkomponentteja, joista tärkeimpänä mainittakoon What’s Connected, jolla voidaan luoda topologiakarttoja ja tarkkailla verkkolaitteiden välisiä yhteyksiä. Toinen hyvä lisäkomponentti on Flowmonitor, jos verkkolaitteissa on mahdollista ottaa käyttöön Netflow-protokolla.

Verkkolaitteiden konfiguraatioiden hallintaan ja tallentamiseen on lisäksi tarjolla What’s Configured lisäkomponentti.

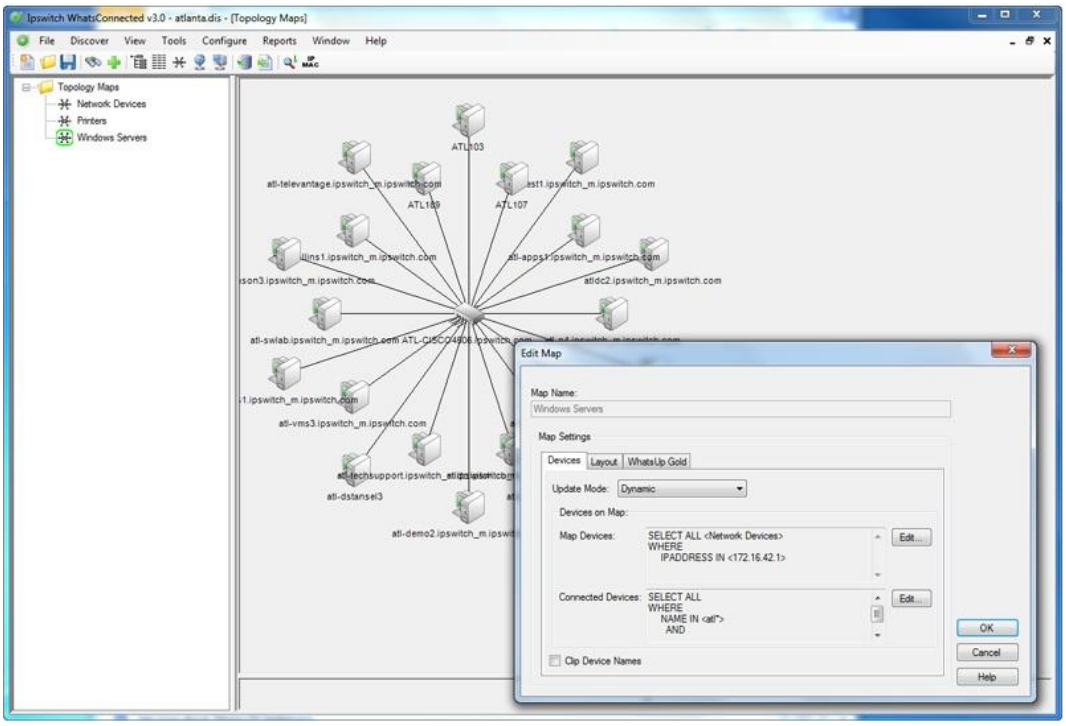


KUVIO 25. What’s Up Gold laitenäkymä kartalla (Ipswitch 2011)

Ohjelma on selkeä, monipuolinen ja melko helppokäyttöinen. What’s up goldilla saadaan selkeä puumainen rakenne verkon laitteista ja ohjelmalla on mahdollisuus muodostaa topologiakartta verkon laitteista (kuvio25). Molemmista, sekä puunäkymästä, että karttanäkymästä pääsee tutkimaan laitekohtaisia ominaisuuksia, muokkaamaan laitteiden valvonta-asetuksia ja määrittelemään erilaisia näkymiä mittaustuloksista. Ohjelma tuottaa kattavia ja informatiivisia raportteja verkon tilasta.

KUVIO 26. What's Up Goldin Graafisen taulukon esimerkkikuva (Ipswitch 2011)

Erinomaista ohjelmassa on pitkälle viedyt mahdollisuudet vaikuttaa laitteiden erilaisiin verkonvalvontamäärityksiin, kuten esimerkiksi hälytysten lähettämisen ajankohdan voi määritellä todella tarkasti. Sensoreiden lisääminen laitteeseen ei taas ole kovinkaan yksinkertaista, vaan ohjelmaan täytyy määrittää OID kerrallaan erilaiset sensorit. Tätä varten joutuu selailemaan MIB-taulukoita laitekohtaisesti, joka on aikaavievää ja työlästä. On myös hieman omituista, että web-hallinnasta ei pääse muokkaamaan tai luomaan topologiakarttoja, vaan kyseinen toiminto täytyy tehdä windows-hallinnan kautta. Ohjelmalla voi luoda todella paljon erilaisia ja näyttäviä sensorikohtaisia graafisia taulukoita (kuvio 26).



KUVIO 27. What's Connected lisäosan automaattisesti luotu verkkokuva (Ipswitch 2011)

What's Connected lisäosa on kätevä työkalu verkkotopologiakuvan luomiseen (kuvio 27). Ohjelma käyttää hyödykseen laitteiden ARP-tauluja, joilla ohjelma päättelee laitteiden väliset yhteydet. Verkkokuva muodostuu automaattisesti ja kartta on täysin siirrettävissä What's Up Goldiin tai Microsoft Visioon import-toiminnon avulla. Lisäksi What's Connected -ohjelmalla voi nähdä hyödyllistä tietoa laitteiden välisistä kytkennöistä, osoitteista ja tilasta taulukkomuodossa.

5 TESTATTUJEN VERKONVALVONTASOVELLUSTEN VERTAILU

Eri verkonvalvontasovellusten vertailu perustuu ohjelmakohtaisiin käyttökokemuksiin. Kaikista muista ohjelmista, paitsi Neteyesta, asennettiin kokeiluversio VMware-ohjelmalla luotuihin virtuaalikoneisiin ja ohjelmien ominaisuuksia vertailtiin samassa testiympäristössä. Näissä neljässä ohjelmassa otettiin valvontaan Mediatalo ESA:n verkonhallinnan verkkosegmentti, joka sisälsi noin 30 laitetta. Neteye sovelluksesta ei ollut kokeiluversiota, vaan Noval networksin asiantuntijat pitivät Mediatalo ESAlle ohjelmasta ja ohjelman ominaisuuksista esittelyn, jonka perusteella ohjelma arvioitiin.

5.1 Vertailukriteerit

Aluksi uudelta verkonvalvontasovellukselta ei vaadittu kovin erikoisia ominaisuuksia, mutta kun huomattiin, mitä kaikkea nykyisillä verkonvalvontasovelluksilla voidaan tehdä kriteerejä lisättiin. Uudelta verkonvalvontajärjestelmältä toivottiin seuraavia ominaisuuksia:

- Käyttöjärjestelmän tulee olla mielellään Windows siitä syystä, että moni työtekijä Mediatalo ESA:n tietohallinnossa on perehtynyt enemmän Windows-pohjaisten kuin Unix-pohjaisten ohjelmien käyttöön.
- Hinta/laatu-suhteen pitää olla hyvä, jotta ohjelman hankkiminen kannattaa.
- Klusterointimahdollisuus ohjelmassa pitäisi olla, jotta saadaan luotua vikasietoinen verkonvalvontajärjestelmä.
- Ohjelman pitää olla helppokäyttöinen eli käytettävyysasteen tulee olla hyvä, jotta ohjelman käyttäminen on helppo sisäistää ja opettaa muille työntekijöille tietohallinnossa.

- Mahdollisuus vaikuttaa mahdollisimman paljon ohjelman ominaisuuksiin, eli hyvät muokkausominaisuudet, jotta ohjelma saadaan sopivaksi juuri Mediatalo ESA:n tarpeisiin.
- Mahdollisuus toteuttaa selkeä verkkotopologia-kartta, koska kartta selkeyttää huomattavasti verkonvalvontaa, kun tiedetään mitä segmenttiä verkosta käsitellään ja mihin osaan verkosta mahdolliset vikatilanteet vaikuttavat.
- Ohjelmassa tulisi olla selkeät, kuvaavat ja helposti saatavilla olevat graafiset taulukot sensoreiden arvojen seuraamista varten. Tämä on tärkeää, jotta ollaan selvillä siitä, mitä verkossa tapahtuu ja pystytään jäljittämään verkon viat.
- Ohjelman tulisi tukea mahdollisimman monia verkonvalvonnassa käytettäviä protokollia, jotta saadaan mahdollisimman paljon erilaisia mahdollisuuksia mitata asioita verkon laitteista.
- Kytkimistä tarvitsee mitata ping vasteaikoja, liikennemääriä ja porttivirheilyitä.
- Palvelimista on tärkeää pystyä valvomaan kovalevyjen, muistin ja prosessorien tilaa, mahdollisesti sähköpostia, tietokantoja ja palveluita, sekä seurata lokitietoja.
- Hälytykset tulisi olla helppo määritellä ja ne pitäisi pystyä lähettämään sekä sähköpostiviestinä, että tekstiviestinä. Tämä on tärkeää, jotta saadaan tieto tapahtuneista vikatilanteista välittömästi päivystävälle verkonhallinnan työntekijälle.
- Mobiilihallinta on hyvä lisä verkonvalvontaan. Mobiilihallinta mahdollistaa verkon tarkkailun muualta kuin töistä käsin.

5.2 Sovellusten vertailu

Ohjelmilla testattiin kriteerien mukaisia toimintoja ja ohjelmista otettiin selville minkälaisia verkonvalvontaominaisuuksia niissä on. Testien perusteella muodostettiin taulukko (taulukko 1), josta käy ilmi ohjelmien ominaisuudet ja joka havainnollistaa sitä kuinka ohjelmia vertailtiin. Pisteytys taulukossa perustuu

ohjelmakohtaisiin käyttökokemuksiin ja tuntemuksiin. Arvostelu ohjelmille on pisteytetty yhdestä viiteen, jossa yksi on huono ja viisi hyvä arvosana. Hinta on määritelty taulukossa suurpiirteisesti, koska yritykselle tehtyjä tarjouksia ei luonnollisesti voida julkisesti esittää.

TAULUKKO 1. Eri verkonvalvontasovelluksien ominaisuuksien vertailu

OHJELMA / OMINAISUUDET	**PRTG**	**OP5**	**ZenOSS**	**Neteye**	**What's Up Gold**
YLEISET:					
Hintataso	Edullinen	Edullinen, kuukausi-veloitus	Ilmainen Open Source tai kallis tukipalvelulisenssi	Edullinen, kuukausi-veloitus	Keski-tason hintainen
Operating System	Win	Unix	Unix	Win	Win
Asiantuntijatuki	1 vuosi / lisenssi	kuuluu lisenssiin	maksullinen	kuuluu lisenssiin	kuuluu lisenssiin
Päivitykset	X	X	X	X	X
Backupin luonti	X	X	X	X	X
Klusterointi	X	X			X
Kieli	Englanti	Englanti/ Suomi	Englanti	Suomi	Englanti
Hallintaympäristö	WEB / Win GUI	WEB / Console	WEB / Console	WEB	WEB / Win GUI
Erilliset laiteasennukset		Mahdollis-ta ostaa erillisiä sensoreita		Palvelin, mahdolli-set sensorit	
Mahdollisen ohjelmakohtaisen agentin asennus		X			
Käytettävyys	5	2	3	3	4
Muokkaus ominaisuudet	4	5	3	2	5
VISUAALISUUS:					
Käyttöliittymä	5	3	4	3	4
Kartta	4	5	3		4
Graafit	5	3	3	4	4
Linkkien tilat väreinä		X			X

PROTOKOLLAT JA TOIMINNOT:					
ICMP	X	X	X	X	X
SNMP	X	X	X	X	X
Netflow	X				X
TCP Portti	X	X	X		X
WMI	X		X		X
MITTAUKSET:					
Kytkimet					
Ping vasteajat	X	X	X	X	X
Liikennemäärä	X	X	X	X	X
porttien virheilyt	X	X	X	X	X
Palvelimet					
Kovalevyt, prosessorit yms.	X	X	X	X	X
Sähköposti	X	X	X		X
Tietokannat	X	X	X	X	X
Palvelut	X	X	X	X	X
VoIP	X				X
Windows	X	X	X	X	X
Linux	X	X	X	X	X
Mittaus ulkoapäin				X	
LISÄOMINAISUUDET:					
Sähköpostihälytys	X	X	X	X	X
Tekstiviestihälytys	X	X	X	X	X
Mobiiliclient	X				X

5.3 Yhteenveto

Kaikissa ohjelmissa on omat hyvät piirteensä ja ominaisuutensa, mutta vertailussa nousi selkeästi esille kaksi kriteerit omaavaa verkonvalvontasovellusta, joilla verkonvalvonta toteutettaisiin. Nämä kaksi ohjelmaa, PRTG ja What’s Up Gold, erottuivat joukosta heti jo siksi, että niiden hinta/laatu-suhde on hyvä. Vaikka ZenOSS on ilmainen, on ohjelman käyttäminen melko haastavaa ja hankalaa.

Lisäksi ZenOSS:n lisenssi, joka mahdollistaa asiantuntijatuen ja tukipalvelut, on erittäin hintava. OP5 on kallis kuukausiveloitusperiaatteensa vuoksi, ja käyttäminen on monimutkaista ja vaatii pitkäaikaista perehtymistä ja paljon työtä. OP5:ssa on kuitenkin esimerkillisellä tavalla toteutettu eri verkonvalvontaominaisuuksien muokkaaminen. Neteye ei vastannut kriteereihin niin kuin olisi toivottu, ja lisäksi ohjelma vaikutti vielä hieman keskeneräiseltä. Ohjelmasta puuttui kokonaan esimerkiksi topologiakartan luomisen mahdollisuus. Lisäksi ohjelma on kallis kuukausiveloituksen ja asennuskustannusten takia.

What’s up gold on edullinen, ja ohjelman käytettävyys on hyvä. Ohjelma erottuu edukseen sillä, että verkonvalvontaominaisuuksiin voi vaikuttaa paljon ja kartat ovat selkeitä ja helppo muodostaa. Ohjelmalla on helppo ”räätälöidä” juuri yrityksen tarpeisiin sopiva verkonvalvontajärjestelmä. Käyttöliittymässä on pieniä vikoja esimerkiksi navigoinnin suhteen ja välillä erilaiset laitenäkymät eivät toimi niin kuin niiden kuuluisi toimia. Käyttöliittymä on silti johdonmukainen valikoiden suhteen ja laitteiden ominaisuuksia on helppo muokata. Laitekohtaisten sensorien lisääminen on hieman monimutkaista ja välillä ohjelmalla määritellyt sensorit eivät keränneet tietoa laitteelta.

PRTG on hinta/laatu-suhteeltaan sovellusten parhaimmistoa. Ohjelma on helppokäyttöinen ja silti monipuolinen. Käyttöliittymä toimii esimerkillisesti, koska käyttöliittymä on selkeä ja johdonmukainen. Havainnollistavat graafiset taulukot kaikista asetetuista sensoreista ovat selkeästi näkyvillä lähes joka paikassa ohjelmaa käytettäessä. Tämä antaa miellyttävän kuvan ohjelmasta. Laitteiden etsiminen verkosta ja sensoreiden lisääminen on toteutettu erinomaisesti. Laitteiden lisääminen on helppoa ja sensoreiden ominaisuuksien muokkaaminen yksinkertaista. Ohjelma tukee kaikkia kriteereitä, paitsi sisäverkon ulkopuolista valvontaa. Tämäkin on mahdollista, jos valitaan kalliimpi lisenssi. Ohjelmassa olisi kehitettävää karttapalvelussa. Vaikkakin kartan tekeminen on helppoa ja kartan kautta pääsee laitenäkymiin, on kartan ominaisuuksissa pieniä puutteita verrattuna esimerkiksi What’s Up Goldiin.

Yhdessä Mediatalo ESA:n tietohallinnon työntekijöiden kanssa päädyttiin valitsemaan näistä viidestä parhaaksi verkonvalvontasovellukseksi Paesslerin PRTG:n. Verkonvalvonta tullaan toteuttamaan PRTG:llä, jonka käyttöönoton suunnittelu käydään läpi seuraavassa osiossa.

6 VERKONVALVONTAJÄRJESTELMÄN SUUNNITTELU

Verkonvalvontajärjestelmän suunnittelu perustuu Paesslerin PRTG-sovellukseen ja sovelluksen käyttöönottoon. Tämä verkonvalvontasovellus otetaan käyttöön Mediatalo ESA:n Ilmarisentien pääkonttorin toimipisteeseen.

Verkonhallinta-asemana tulee toimimaan palvelimelle VMware-ohjelmalla luotu Windows-pohjainen virtuaalikone, johon asennetaan PRTG-sovellus. Klusterointi toteutetaan asentamalla toinen PRTG-sovellus toisen konesalin palvelimelle asennetulle virtuaalikoneelle.

6.1 Mediatalo ESA:n verkkoympäristö

Mediatalo ESA:n verkkoympäristö koostuu neljästä kokonaisuudesta, jotka halutaan ottaa valvontaan. Nämä ovat Ilmarisentiellä sijaitsevat verkkolaitteet, DMZ-alue, ulkopuoliset alueet eli mm. etätoimipisteet ja palvelimet. Verkonvalvonta halutaan keskittää pelkästään verkkolaitteisiin. Yksittäisiä työasemia ei haluta sisällyttää valvontaan, koska silloin verkon kuormitus valvonnan takia kasvaisi liikaa.

Verkko sisältää kahdennetun palomuurin ja kahdennetun runkoverkkoyhteyden kahden keskusreitittimen kautta. Laitteiden jako ryhmiin toteutetaan niin, että verkkolaitteet jaotellaan edellämainittujen neljän pääryhmän alle. Pääryhmien alle määritellään alaryhmiä esimerkiksi laitteiden tyypin mukaan.

6.2 Verkonhallintaprotokollien käyttöönotto verkon laitteissa

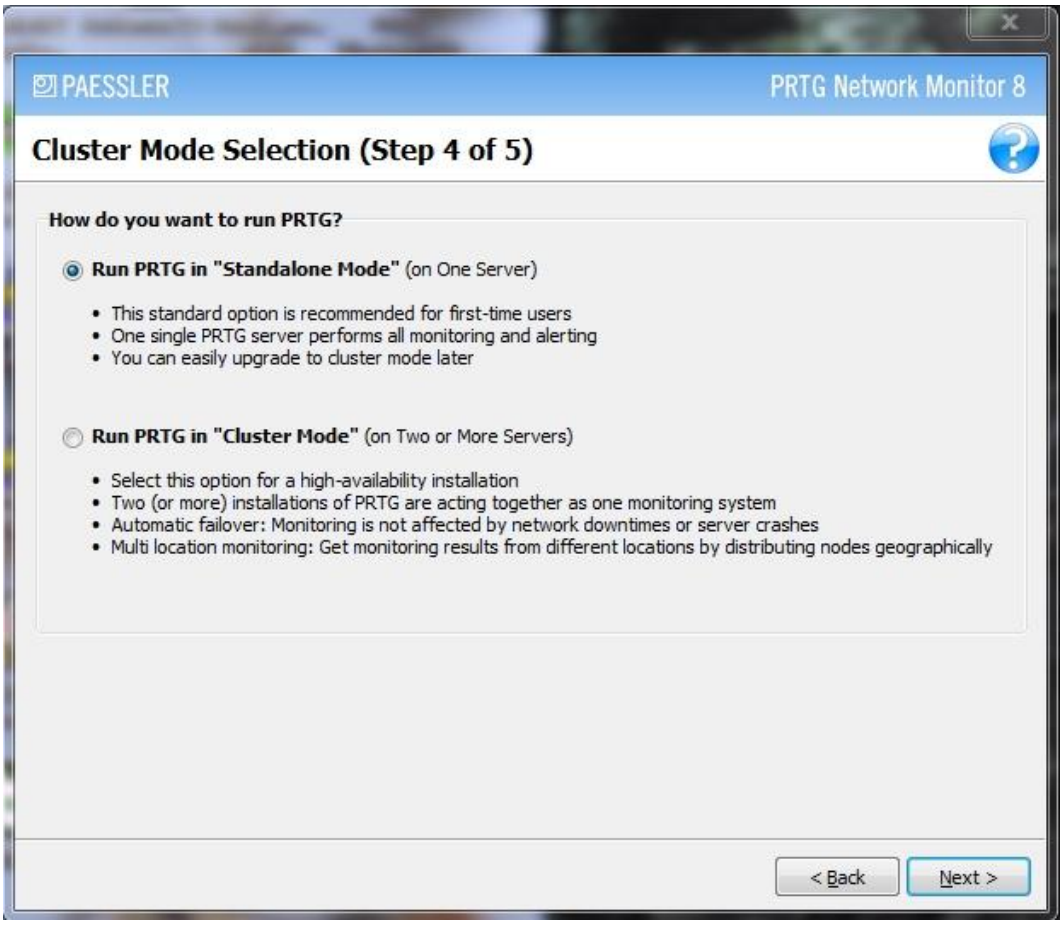
Verkon laitteisiin on jo valmiiksi asennettu käyttöön SNMP-protokolla vanhan verkonvalvontajärjestelmän vuoksi. Jokaisen verkkolaitteen snmp-community tulee olla kuitenkin määritelty niin, että snmp-community on hallinta-asemassa

asetettu samaksi kuin valvottavassa verkkolaitteessa. Myös valvottavan verkkolaitteen ja hallinta-asemalle määritetyn SNMP:n version tulee olla määritetty samaksi molemmissa laitteissa.

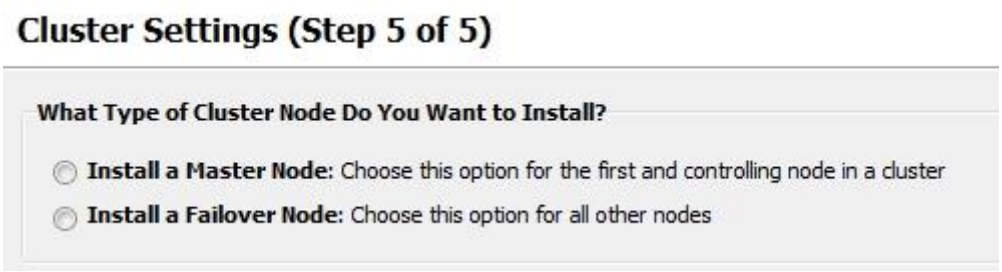
WMI-protokollaa käytettäessä tulee PRTG-ohjelmaan olla määritettynä joku sopiva kirjautumistunnus windows-palvelimelle. Jos sopivaa kirjautumistunnusta palvelimelle ei ole, ja WMI halutaan ottaa käyttöön jonkun arvon mittaamiseksi, täytyy kirjautumistunnus valvontaa varten luoda. Palomuureihin tulee olla määritelty, että SNMP, WMI ja muut verkonvalvontaan käytettävät protokollat on sallittu, jotta liikenne verkonhallinta-aseman ja valvottavien laitteiden välillä toimii.

6.3 Verkonvalvontasovelluksen asentaminen

PRTG:n asenteminen hallinta-asemalle on melko yksinkertaista. Ohjelma ladataan ensin Paesslerin internetsivustolta, minkä jälkeen asennusohjelma käynnistetään. Aluksi määritellään polku, jonne ohjelma halutaan asentaa, ja määritellään lisenssiavain. Seuraavaksi määritellään ohjelman käyttäjätunnus, salasana sekä sähköpostiosoite, jota hallintaan käytetään. Sitten ohjelma voidaan asentaa yksittäisesti tai vaihtoehtoisesti ottaa klusterointi käyttöön tässä vaiheessa (kuvio 28). Mediatalo ESA:n tapauksessa otetaan klusterointi käyttöön ja asennetaan ohjelma ensin master-tilaan ensimmäisellä hallinta-asemalla. Tämän jälkeen asennetaan toiselle hallinta-asemalle ohjelma failover-tilaan (kuvio 29), jolloin saadaan luotua vikasietoinen verkonvalvonta.



KUVIO 28. PRTG:n asennusvaihtoehdot

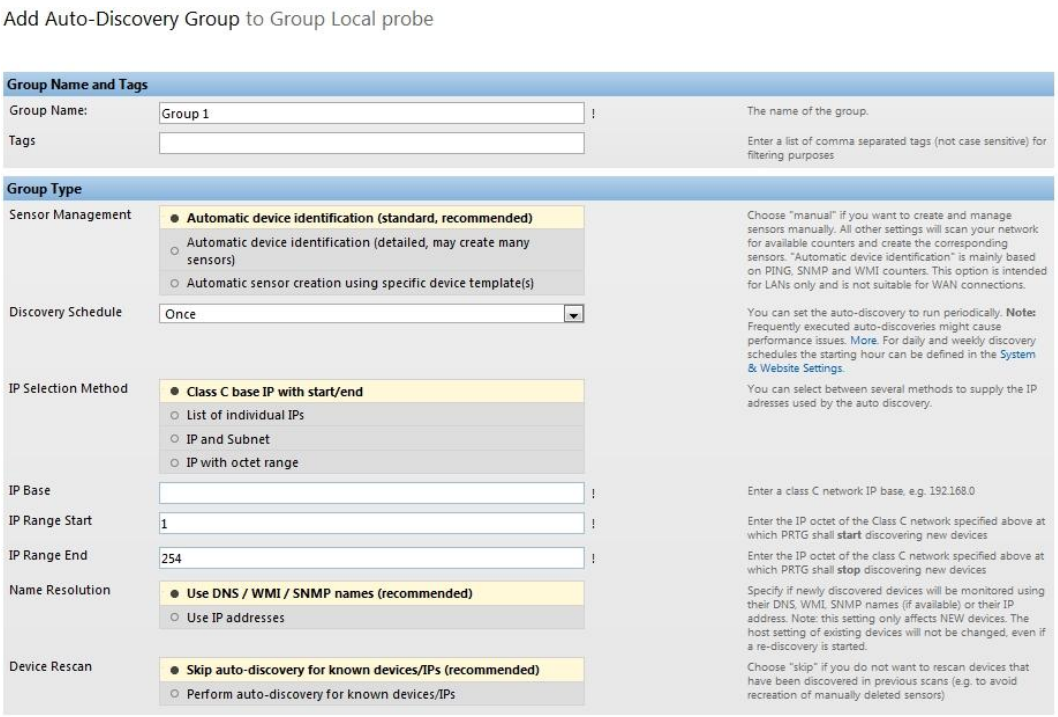


KUVIO 29. PRTG:n klusteroinnin määrittely

Ohjelma asentuu hallinta-asemalle ja web-hallinta tulee käyttöön hallinta-aseman localhost IP-osoitteessa. Web-hallintaan tai windows-hallintaan voidaan kirjautua asentamisen yhteydessä määritellyillä kirjautumistunnuksilla.

6.4 Laiteryhmien luominen ja laitteiden määrittely

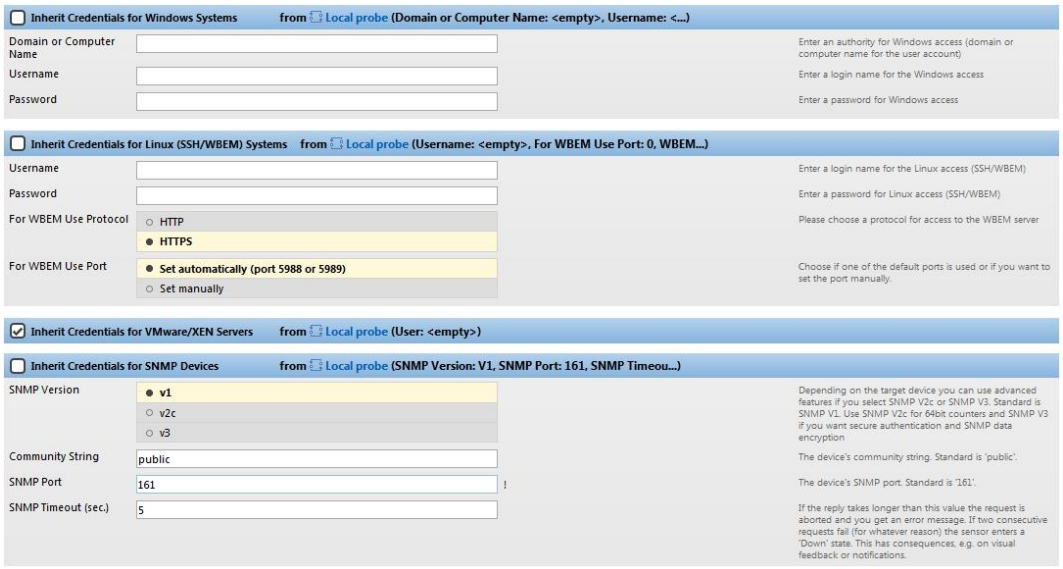
Aluksi kannattaa määritellä laiteryhmät, joihin verkonvalvontaan lisättävät laitteet jaetaan. Määrittely tapahtuu devices-välilehden alta add group -toiminnon avulla. Ryhmät tulevat näkymään devices-välilehden alla puumaisena näkymänä (kuvio 13). Ryhmien alle voi lisätä alaryhmiä, jos haluaa selkeyttää verkkonäkymää. Ryhmät voi aluksi lisätä erikseen ja määritellä laitteet ryhmiin myöhemmin. Toinen mahdollisuus on käyttää add auto-discovery group-toimintoa, jolla voidaan hakea halutulta ip-alueelta kaikki laitteet kyseiseen ryhmään, tai määritellä eri tavoilla halutut laitteet ryhmään (kuvio 30).



KUVIO 30. Auto-discovery groupin määrittely

Laiteryhmille määritellään tässä vaiheessa erilaisia asetuksia, kuten mm. Windows-järjestelmien kirjautumistunnukset (WMI:tä käytettäessä), mahdollisesti SSH-kirjautumistunnukset (jos halutaan käyttää SSH:ta laitteen valvontaan) ja SNMP-asetukset, joissa määritellään SNMP community- ja versiotiedot (kuvio 31). Kaikki laitteet tässä ryhmässä perivät nämä asetukset tästä ryhmästä, ellei

toisin määritellä. Myös ryhmät voivat periä asetuksensa PRTG:n hallinta-asemalle määritellyistä asetuksista. Uuden verkonvalvontajärjestelmän asennuksessa käytetään automaattista hakua ja eri ryhmille, haetaan ryhmän laitteet ip-alueen mukaisesti sekä määritellään ryhmäkohtaisesti SNMP- ja WMI-tiedot, minkä jälkeen niitä tarvittaessa muutetaan sellaisille laitteille, joissa ne eivät päde.



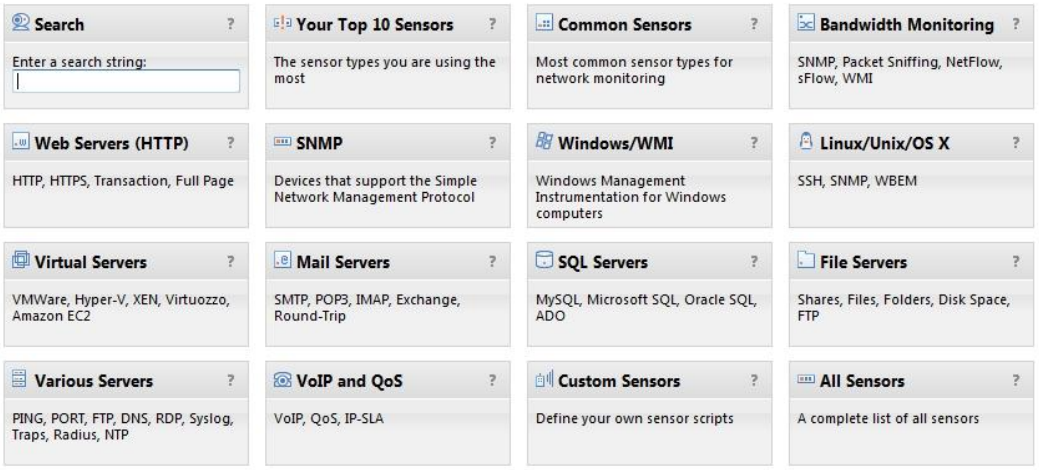
KUVIO 31. Ryhmäkohtaisten asetusten määrittely.

6.5 Sensoreiden määrittely

Sensorit voidaan määrittää kuten laitteetkin, eli sisällyttämällä sensorien haun automaattiseen hakuun laitekohtaisesti tai lisäämällä halutut sensorit jälkikäteen laitekohtaisesti. Automaattinen sensoreiden haku käyttää laitteille asetettuja SNMP- ja WMI-asetuksia, joiden tulee vastata laitteesta löytyviin asetuksiin. Mediatalo ESA:n tapauksessa käytetään automaattista sensoreiden hakua kaikille valvontaan otettaville laitteille, minkä jälkeen poistetaan sensorit, joita ei tarvita. Seuraavaksi lisätään laitekohtaisesti sellaiset sensorit, joita automaattinen haku ei sisältänyt ja jotka halutaan silti laitteelle määritellä.

Palvelimia tullaan valvomaan WMI-sensoreiden avulla ja muiden verkkolaitteiden valvontaan käytetään SNMP-sensoreita. Linux-palvelimilla käytetään mahdollisesti SSH-kirjautumisen avulla saatavia tietoja. Internet-palveluiden

valvontaan otetaan käyttöön HTTP-sensori, joka mahdollistaa esimerkiksi kokonaisen www-sivuston (esimerkiksi www.ess.fi) median lataamisen. Tällä valvotaan sitä, etteivät sivun latausajat nouse liian korkeiksi ja sivusto on toiminnassa. Sensoreiden lisääminen käsin tapahtuu menemällä laitekohtaiseen näkymään ja käyttämällä add sensor -toimintoa. Seuraavaksi määritellään, millainen sensori otetaan käyttöön (kuvio 32) ja mitä ominaisuuksia sensorille halutaan.



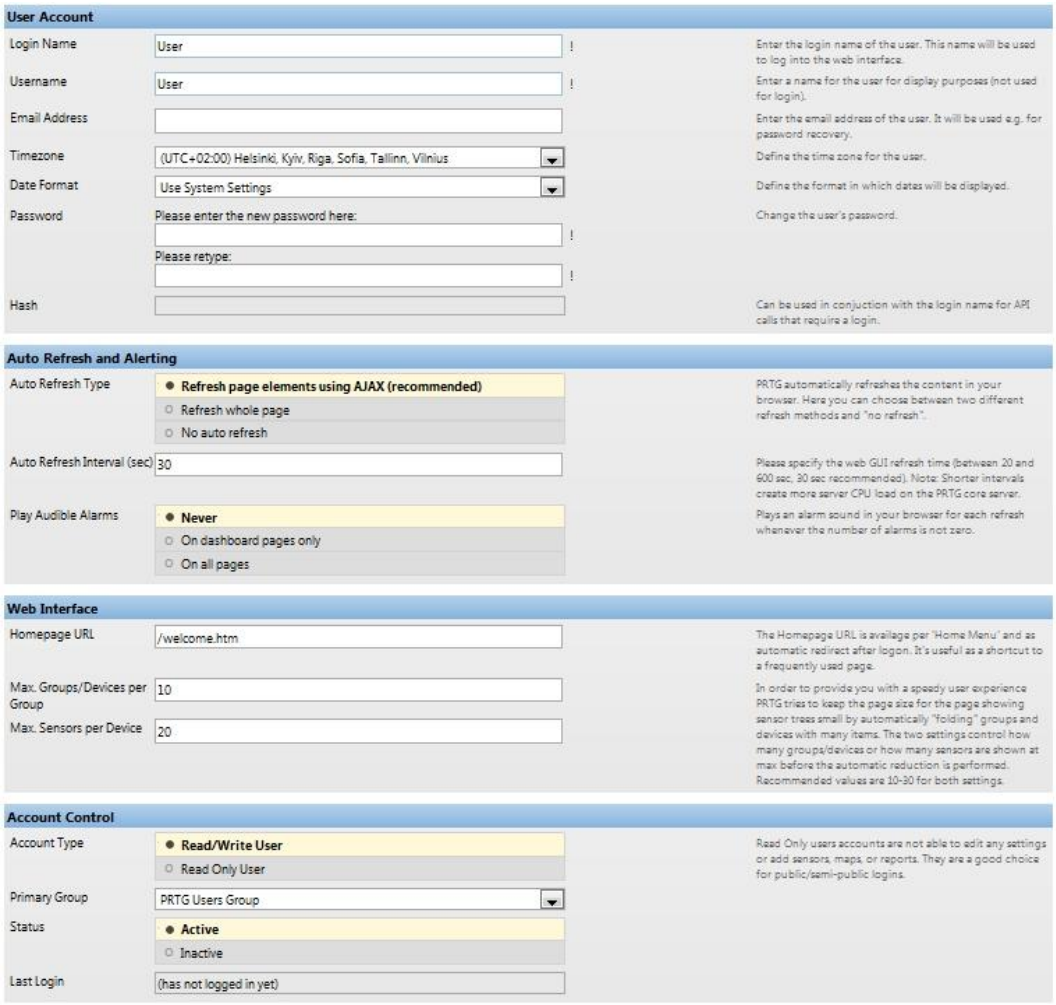
KUVIO 32. PRTG-ohjelman sensoriryhmät

Verkonvalvontasovelluksia testattaessa yritettiin käyttää Netflow-sensoreita liikenteen valvontaan. Mediatalo ESA:n laitteisto ei kuitenkaan sisältänyt vaadittavia laitekomponentteja, jotka olisivat mahdollistaneet Netflow-protokollan hyödyntämisen.

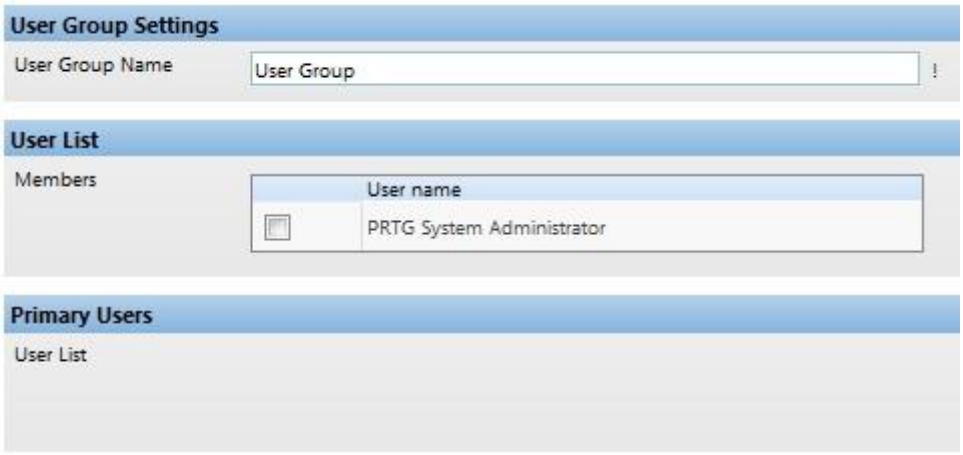
6.6 Käyttäjäprofiilien ja käyttäjäryhmien luominen

Admin-tunnuksilla päästään luomaan eri käyttäjiä (kuvio 33) ja käyttäjäryhmiä (kuvio 34) ohjelmalle. Käyttäjien- ja käyttäjäryhmien hallinnalla voidaan määritellä, millainen näkymä kullakin käyttäjällä on ja mihin ryhmään kukin käyttäjä kuuluu. Eri ryhmille voidaan asettaa erilaisia hälytysaikatauluja, vaikkapa niin että viikonloppuisin ei hälytetä tietyn ryhmän käyttäjiä vikatilanteissa. Ryhmille voidaan määrittää erilaisia kirjoitusoikeuksia esimerkiksi niin, että tietty

ryhmä ei voi muokata ohjelmalla laitteiden ominaisuuksia, vaan ryhmän jäsenet voivat vain tarkkailla verkon tilaa. Tilien- ja ryhmien hallinta tapahtuu setup-välilehden kautta user accounts- ja user groups -valikoiden alta. Ryhmien näkymät ja käyttö määritellään joko laiteryhmien-, laitteiden-, tai sensoreiden asetusten kautta. Voidaan esimerkiksi määrittää, että tietty laiteryhmä näkyy vain tietylle käyttäjäryhmälle, jolloin muut käyttäjäryhmät eivät näe kyseistä laiteryhmää.



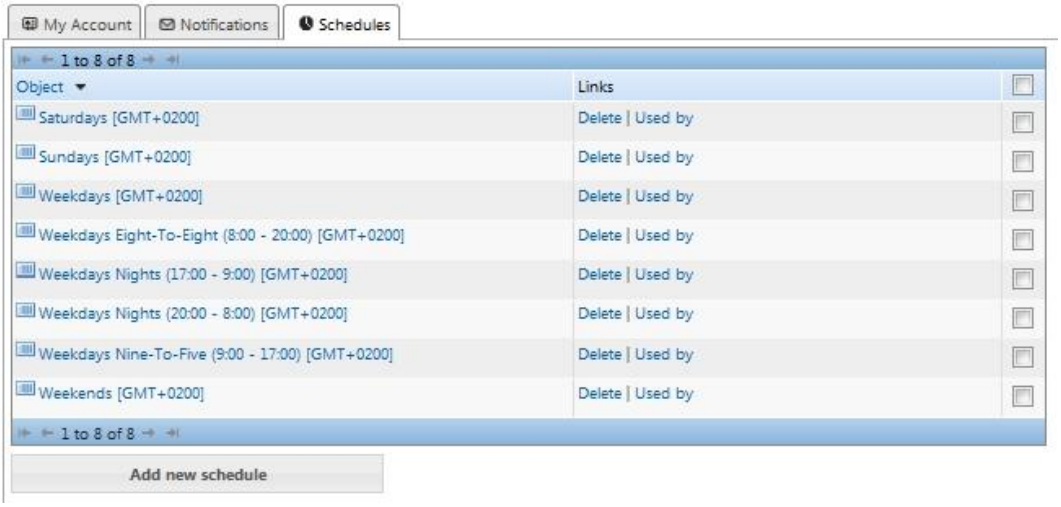
KUVIO 33. Käyttäjätilien luonti



KUVIO 34. Käyttäjäryhmien luonti

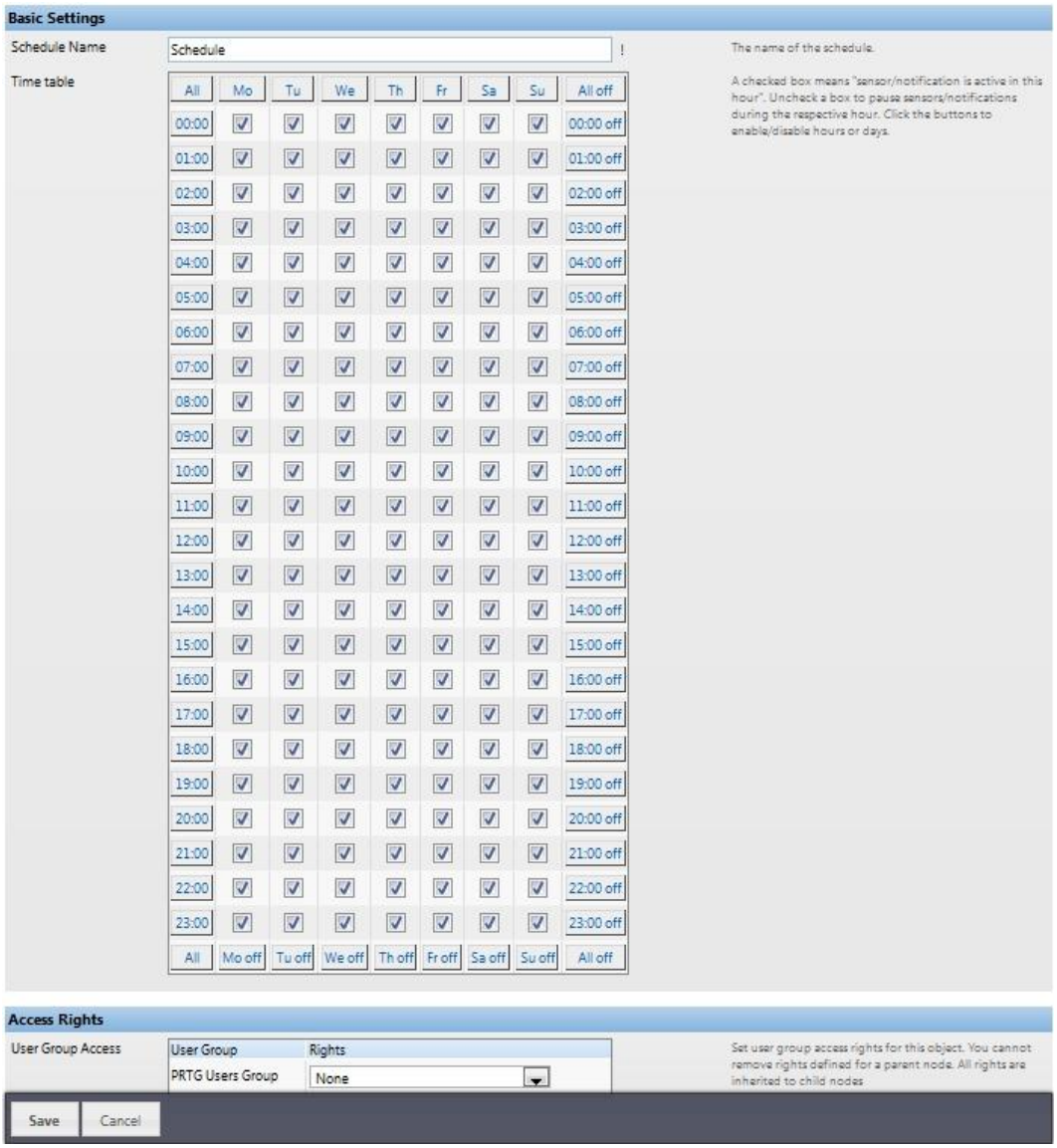
Mediatalo ESA:lle luodaan kaksi käyttäjäryhmää, joista ensimmäinen on hallintaryhmä, jonka käyttäjillä on täydet luku- ja kirjoitusoikeudet sovelluksen käyttöön. Toinen ryhmä on tarkoitettu pelkästään valvontaan, niin että asetuksia ei voida muuttaa. Tämä toteutetaan siksi, että kun halutaan pelkästään valvoa verkkoa, ei pelkillä lukuoikeuksilla voi vahingossakaan muokata järjestelmän asetuksia. Käyttäjiä lisätään näihin kahteen ryhmään sen mukaan, kenelle oikeudet valvontasovelluksen käyttöön annetaan.

6.7 Tiedotusajankohtien ja hälytysten määrittely



KUVIO 35. Tiedotusaikataulut

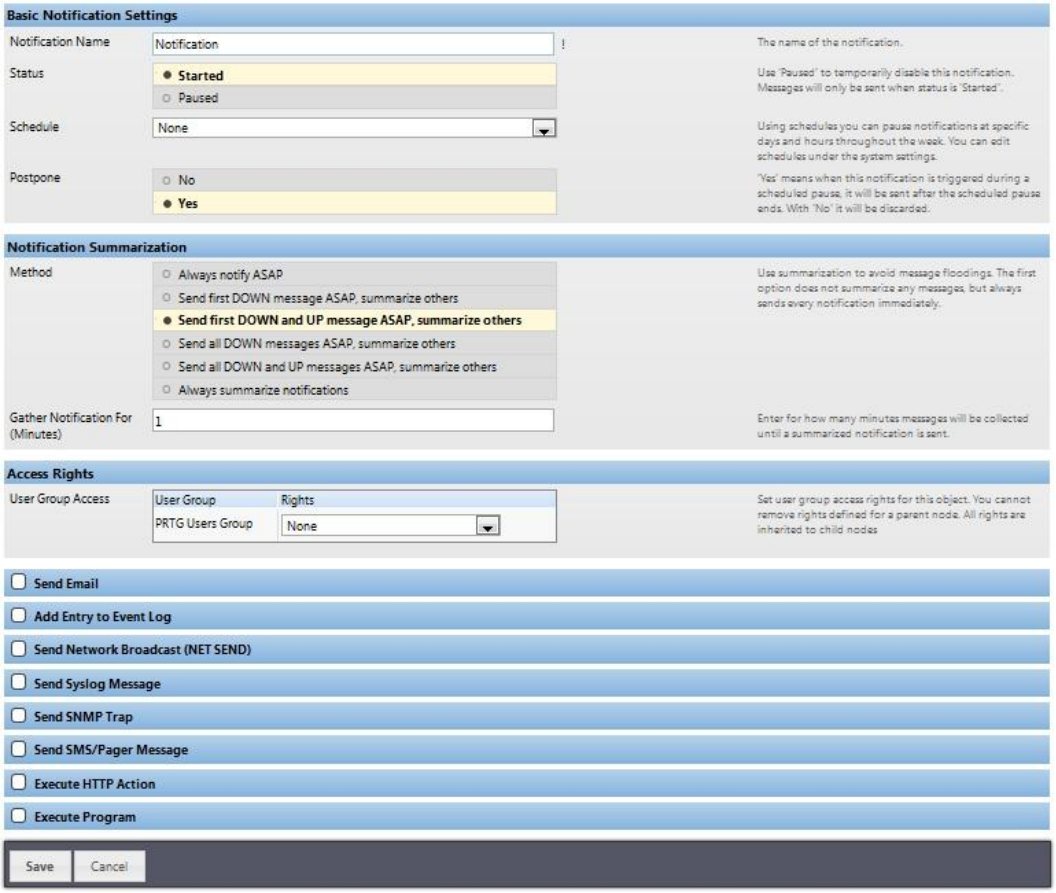
Tiedotusajankohdat määritellään setup-välilehden notifications -valikosta (kuvio 35). Tiedotusjankohdalla vaikutetaan siihen, mihin aikaan tiedotuksia verkon virheistä lähetetään verkonvalvojille. Ohjelmaan on tehty valmiiksi muutamia aikatauluja, mutta niitä voi tehdä itse sen mukaan, kun tarvetta on add schedule -toiminnon (kuvio 36) avulla.



KUVIO 36. Aikataulujen muokkaustoiminto

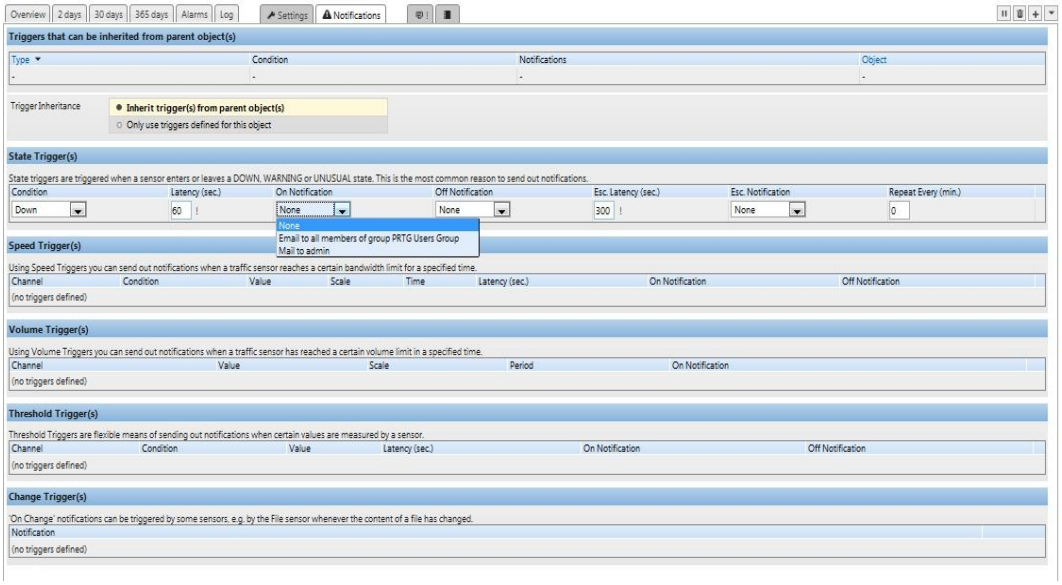
Mediatalo ESA:lle tehdään aikataulu, jossa hyväksytään tiedotusten lähettäminen viikolla työaikoina, mutta ei öisin eikä viikonloppuisin. Aikataulut otetaan käyttöön ilmoitustapojen muokkaamisen yhteydessä. Ilmoitukset määritellään setup-välilehden notifications -valikon kautta. Aikataulut määritellään eri

ryhmille, laitteille tai sensoreille niiden omien asetusten kautta erikseen, sen mukaan, mitä tiedotusaikataulua halutaan käyttää.



KUVIO 37. Ilmoitusten luonti

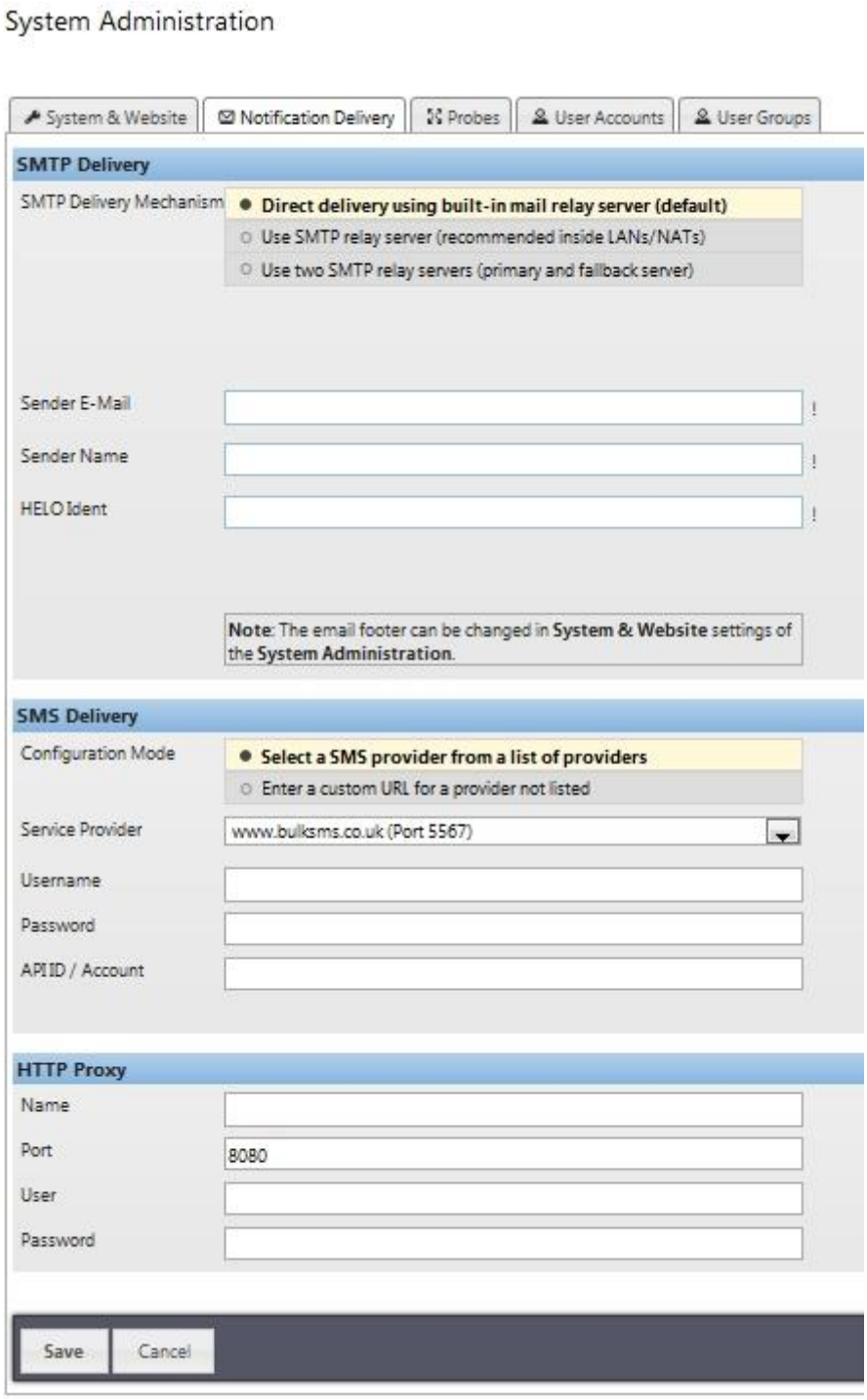
Ilmoituksilla määritellään aluksi tiedotustapa, joka määrittää, lähetetäänkö viesti aina, kun laite on alhaalla, vai lähetetäänkö viesti esimerkiksi myös silloin, kun laite nousee takaisin toimintavalmiuuteen (kuvio 37). Lisäksi ilmoitukseen määritellään toiminto, mitä käytetään silloin, kun ilmoitus muodostetaan. Erilaisia toimintoja on mm. sähköpostin lähetys, tekstiviestin lähetys tai snmp-trap, jolla saadaan esimerkiksi käynnistettyä laite uudestaan. Kun ilmoitukset on luotu, ne otetaan käyttöön eri laiteryhmien, laitteiden tai sensoreiden tiedotus-välilehden alla. Laitteille voi määritellä erilaisia tiedotuksen ”liipaisu”-rajoja, jolloin ilmoitus halutusta tapahtumasta generoidaan (kuvio 38).



KUVIO 38. Ilmoitusten käyttöönotto

6.7.1 Sähköpostihälytykset

Mediatalo ESA:lla otetaan käyttöön sähköpostitiedotukset verkon vioista. Ne määritellään edellämainitulla tavalla ilmoituksien yhteydessä niin, että tiedote lähetetään tiettyyn sähköpostiin aina, kun laite tai sensori ensimmäisen kerran lakkaa vastaamasta ja silloin kun laite- tai sensori on takaisin toimintatilassa. Viestit välitetään tulevassa verkonvalvonnassa niin, että palvelimien tila välitetään palvelimien valvojien sähköpostiin ja muiden verkkolaitteiden virheet toiseen erilliseen sähköpostiosoitteeseen. Sähköpostiasetukset tulee määritellä ensin setup -välilehden notification delivery -valikon kautta (kuvio 39).



KUVIO 39. Tiedotteiden välitysasetukset

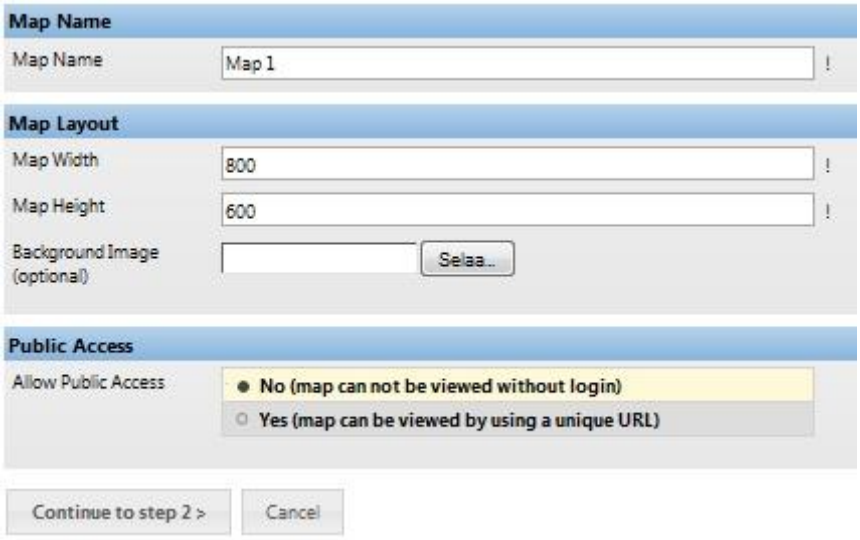
Lähetettävää sähköpostiviestiä pääsee muokkaamaan ohjelman asetuksista setup -välilehden system & website -valikon kautta. Ohjelma käyttää oletuksena PRTG:n omaa pohjaa, joka sisältää tiedot vikakohteesta.

6.7.2 Tekstiviestihälytykset

Tekstiviestihälytykset määritellään myös ilmoitusten luonnin yhteydessä. Laitekohtaisesti tekstiviestihälytykset otetaan uudessa verkonvalvonnassa käyttöön vain kaikkein kriittisimmissä tilanteissa ja liitynnöissä. Muissa tapauksessa lähetetään pelkästään sähköpostiviesti.

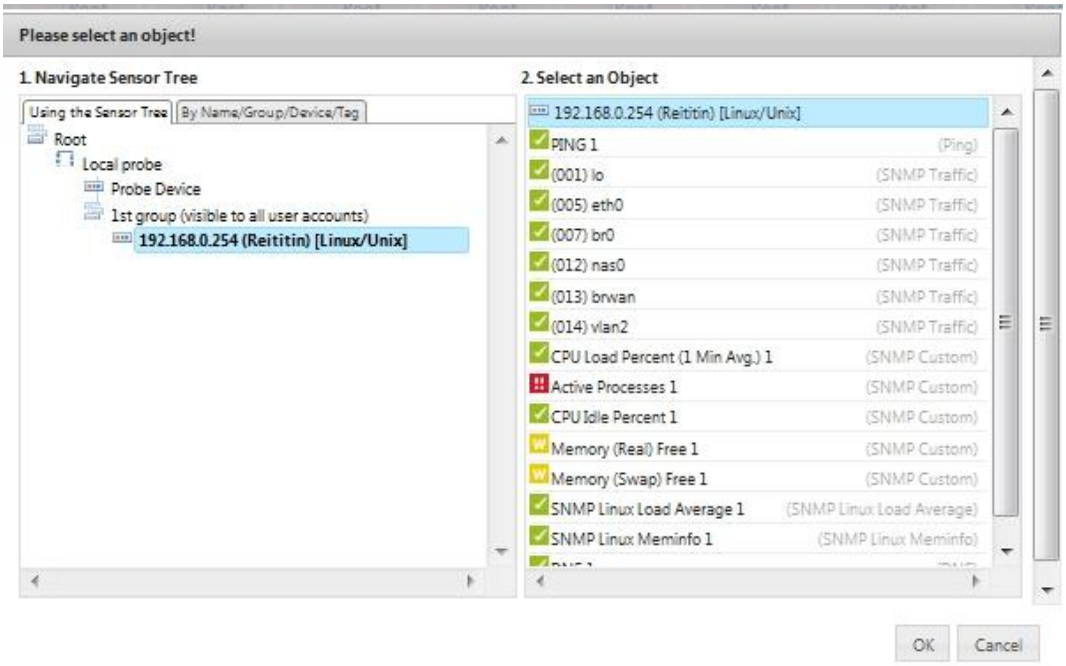
SMS-viestien asetukset määritellään setup välilehden notification delivery asetusten kautta (kuva 39). Mediatalo ESA:lla on oma palvelin SMS-viestien lähettämistä varten, joka määritellään edellämainittuihin asetuksiin.

6.8 Verkkotopologia-kartan luominen



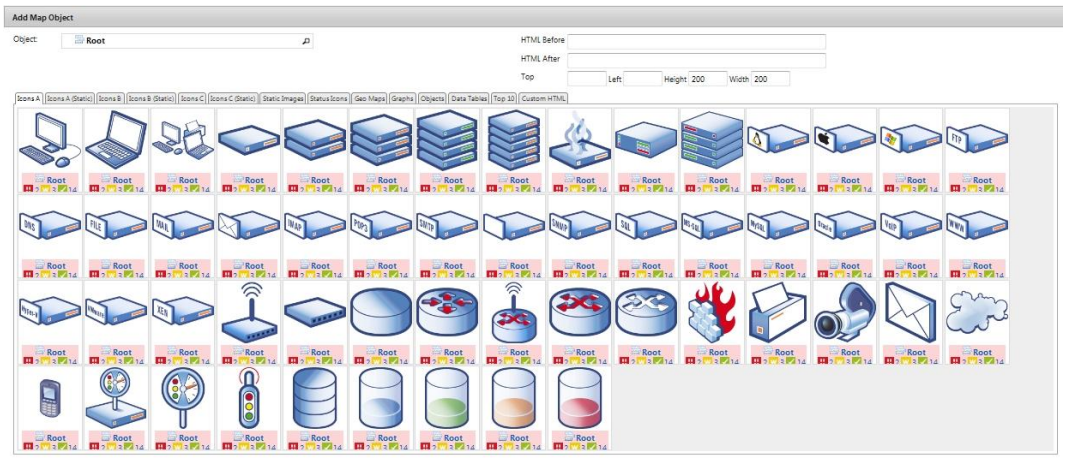
KUVIO 40. Verkkotopologia-kartan määrittely

Verkkotopologia-kartan tekeminen tapahtuu maps-välilehden kautta. Aluksi määritellään uuden kartan nimi, koko ja näyttöoikeudet (kuvio 40). Seuraavaksi lisätään karttaan laitteet map designer -välilehden add map item -toiminnon avulla. Toiminnon kautta valitaan ensin objekti (kuvio 41), eli laite, sensori tai ryhmä, joka halutaan lisätä karttaan.



KUVIO 41. Karttaobjektin valinta

Sitten objektille valitaan kuva tai taulukko (kuvio 42), minkälaisena objekti halutaan kartalla näyttää. Seuraavaksi yhdistetään laitteet kartta-objekteihin muodostuvien linkkien avulla (kuvio 16). Karttaan voi lisätä erilaisia html-lisäosia tai erillisiä taulukoita, jotka auttavat laitteiden tilan tarkkailua.



KUVIO 42. Kartalle lisättävien objektien kuvat

Mediatalo ESA:lle tullaan muodostamaan verkonvalvontasovelluksen käyttöönoton yhteydessä neljä erillistä karttaa laitteille luotujen pääryhmien mukaisesti. Tämä tehdään siksi, että kartasta tulisi selkeä ja johdonmukainen. Jos

kaikki Mediatalo ESA:n verkon laitteet määriteltäisiin samalle kartalle, tulisi kartasta liian iso ja siksi epäkäytännöllinen. Jokaisen kartan pienoiskuva olisi tarkoitus liittää yhteen suureen pää-karttaan, joista pääsisi navigoimaan näille neljälle pienemmälle kartalle. Kartalla pitää näkyä laitteiden tila ja mahdollisesti laitteiden välisten linkkien ruuhkaisuus.

7 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli vertailla erilaisia SNMP-protokollaa käyttäviä verkonvalvontasovelluksia ja suunnitella uusi verkonvalvontajärjestelmä Mediatalo ESA:n tarpeisiin sopivalla tavalla. Lisäksi tässä opinnäytetyössä perehdyttiin verkonvalvontajärjestelmien toimintaan ja protokolliin. Työssä käsiteltiin tarkemmin PRTG-sovelluksen käyttöönottoa Mediatalo ESA:n tietoverkkoon.

Perehtyminen verkonvalvonnan käsitteeseen ja verkonvalvonnan toimintatapoihin auttoi ymmärtämään verkonvalvonnan tärkeyden yrityksissä. Hyvin toteutetulla verkonvalvonnalla voidaan ehkäistä vikatilanteiden syntyminen verkossa ja verkkolaitteissa sekä toimia nopeasti vikatilanteissa niiden korjaamiseksi. Verkonvalvontasovelluksella saadaan aikaan yksityiskohtainen kuva verkon tilanteesta ja voidaan seurata monien eri verkkoelementtien toimintaa samanaikaisesti yhdestä hallintonäkymästä. Hyvä verkonvalvontasovellus on selkeä ja helppokäyttöinen sekä tarjoaa monipuoliset työkalut verkon valvomiseen.

PRTG osoittautui verkonvalvontasovellusten vertailussa parhaaksi sovelluksesi. Tämä johtunee pitkälti siitä, että ohjelman suunnittelussa on ajateltu paljon ohjelman käyttäjää. Tämän trendin huomaa tekniikassa tänä päivänä hyvin monessa ohjelmassa. Monesta verkonvalvontaohjelmasta löytyy paljon ominaisuuksia, mutta usean ohjelman heikkoutena on epäselkeä käyttöliittymä tai käyttäjän kannalta monimutkainen hallinta. Koska PRTG on hyvin monipuolinen ja silti helppokäyttöinen, ohjelma antaa käyttäjälle positiivisen kokemuksen ohjelman käytöstä. Lisäksi PRTG täytti Mediatalo ESA:n verkonvalvonnan kriteerit ja oli selkeästi edullinen verrattuna sekä ohjelman monipuolisiin ominaisuuksiin että muihin verkonvalvontasovelluksiin.

Yllätyksenä verkonvalvontasovellusten testaamisen yhteydessä tuli verkonvalvontasovellusten kehitys muutaman lähivuoden aikana. Ne eivät painotu pelkästään SNMP-protokollan käyttöön tai ns. ”pollaus”-menetelmään, vaan ohjelmat pystyvät hyödyntämään esimerkiksi kirjautumista verkkolaitteisiin SSH:n tai WMI:n avulla. Tämä antaa lisää erilaisia mahdollisuuksia verkonvalvontaan.

Tämän opinnäytetyön tuloksena löydettiin oikea verkonvalvontasovellus Mediatalo ESA:n uuteen verkonvalvontajärjestelmään ja toteutettiin yksityiskohtainen suunnitelma ohjelman käyttöönotosta. Mediatalo ESA:lla tullaan siirtymään verkonvalvontajärjestelmän käyttöön huhtikuun ja toukokuun välisenä aikana. PRTG otetaan yrityksessä käyttöön tämän opinnäytetyön suunnitelmaan perustuen.

Kasvavat tietoverkot ja tietoverkkojen kehitys sekä verkkolaitteiden kehitys tulevat muodostamaan haasteita verkonvalvontajärjestelmien ja -sovellusten kehittäjille. Hiljattain ollaan siirtymässä Ipv6-protokollan käyttöön, joka edellyttää Ipv6:een perustuvien verkonvalvontamenetelmien ja verkonvalvontaprotokollien huomioon ottamista tulevaisuuden verkonvalvontajärjestelmissä ja -sovelluksissa. Lisäksi verkonvalvontaan tulee varmasti vaikuttamaan esimerkiksi nanoteknologian vaikutus verkkolaitteiden kehittymiseen.

Tekniikka kehittyy ja tietoverkot kasvavat huimaa vauhtia, joten on tärkeää yritysten kannalta seurata, onko yrityksen verkonvalvontajärjestelmä pysynyt kehityksen mukaisena. Verkkojen jatkuvasti lisääntyvä käyttö lisää yritysten tarvetta valvoa verkkoa tarkemmin ja yksityiskohtaisemmin. Tämän takia verkonvalvonnan merkitys kasvaa ja verkonvalvontajärjestelmiltä vaaditaan paljon uusia ominaisuuksia ja uusien verkonvalvontamenetelmien kehitystä. Jotta yrityksissä saadaan pidettyä yrityksen oma tietoverkko turvallisena ja toimivana, edellyttää tietoverkon ylläpito hyvää verkonvalvonnan toteutusta.

LÄHTEET

Ballew, S. 1998. Tehokäyttäjän opas - IP-verkkojen hallinta. Jyväskylä: Gummerus.

Boon, L. 2009. Serial Communication [viitattu 27.3.2011]. Saatavissa: http://www.siongboon.com/projects/2006-03-06_serial_communication/ICMP-Header.png

Cisco. 2007. Introduction to Cisco IOS NetFlow - A Technical Overview [viitattu 15.3.2011]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html

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

H3C Technologies. 2008. SNMP Technology White Paper [viitattu 3.3.2011]. Saatavissa: http://www.h3c.com/portal/Products___Solutions/Technology/System_Management/Technology_White_Paper/200805/606347_57_0.htm

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Helsingin teknillinen korkeakoulu [viitattu 2.3.2011]. Saatavissa: http://www.tct.hut.fi/julkaisut/tyot/diplomityot/611/thesis.html

Ipswitch. 2011. What's Up Gold overview [viitattu 20.3.2011]. Saatavissa: http://www.whatsupgold.com/products/whatsup-gold-core/whatsup-gold-premium/index.aspx

Jaakohuhta, H. 2002. Lähiverkot – Ethernet. Helsinki: Edita.

Keogh, J. 2001. Verkkotekniikat – tehokas hallinta. Helsinki: Edita.

Mediatalo ESA. 2011a. Etusivu [viitattu 2.3.2011]. Saatavissa: http://www.mediataloesa.fi/mediataloesa/index.tmpl

Mediatalo ESA. 2011b. Historia [viitattu 2.3.2011]. Saatavissa: http://www.mediataloesa.fi/mediataloesa/tekstisivu.tmpl?sivu_id=416

Mediatalo ESA. 2011c. Mediatalo ESA [viitattu 2.3.2011]. Saatavissa: http://www.mediataloesa.fi/mediataloesa/tekstisivu.tmpl?sivu_id=405

Mediatalo ESA. 2011d. Tilinpäätös 2009 [viitattu 2.3.2011]. Saatavissa: http://www.mediataloesa.fi/liitetiedostot/editori_materiaali/493.pdf

Mediatalo ESA. 2011e. Yritysvastuu [viitattu 2.3.2011]. Saatavissa: http://www.mediataloesa.fi/mediataloesa/tekstisivu.tmpl?sivu_id=409

Microsoft. 2000. Verkkotekniikka+ Training Kit. Jyväskylä: Gummerus.

Microsoft. 2011. Network Management for Microsoft Networks Using SNMP [viitattu 3.3.2011]. Saatavissa: http://technet.microsoft.com/en-us/library/cc723469.aspx

Noval Networks. 2011. Neteye [viitattu 20.3.2011] Saatavissa: http://www.novalnetworks.com/neteye.html

OP5. 2010. OP5 Network Management Suite [viitattu 20.3.2011]. Saatavissa: http://www.op5.com/op5/products/network-management-suite

Paessler. 2011. PRTG Network Monitor [viitattu 15.3.2011]. Saatavissa: http://www.paessler.com/prtg

Puska, M. 2000. Lähiverkkojen tekniikka –Pro Training. Jyväskylä: Gummerus.

RFC792. 1981. Internet Control Message Protocol [viitattu 27.3.2011]. Saatavissa: http://www.ietf.org/rfc/rfc792.txt

RFC1155. 1990. Structure and Identification of Management Information for TCP/IP-based Internets [viitattu 4.3.2011]. Saatavissa: http://www.ietf.org/rfc/rfc1155.txt

RFC1157. 1990. A Simple Network Management Protocol (SNMP) [viitattu 3.3.2011]. Saatavissa: http://www.ietf.org/rfc/rfc1157.txt

RFC1908. 1990. Coexistence between SNMPv1 and SNMPv2 [viitattu 4.3.2011]. Saatavissa: http://www.ietf.org/rfc/rfc1908.txt

SNMP Research International inc. 2011. The SNMP Protocol [viitattu 4.3.2011]. Saatavissa: http://www.snmp.com/protocol/

ZenOSS. 2011. ZenOSS Enterprise [viitattu 20.3.2011]. Saatavissa: http://www.zenoss.com/product/tours/enterprise

LIITTEET