VERKONVALVONTASOVELLUSTEN VERTAILU

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan sv.
Opinnäytetyö
Kevät 2007
Kimmo Vesa

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

VESA, KIMMO: Verkonvalvontasovellusten vertailu

Tietoliikennetekniikan opinnäytetyö, 52 sivua

Kevät 2007

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on verkonvalvontasovellusten vertailu. Verrattavina olevat ohjelmat ovat Nagios ja Zabbix. Tarkoituksena on löytää sopiva verkonvalvontasovellus HTK NetCommunication Oy:n käyttöön tarkkailemaan verkkopalvelimia ja palveluita.

Työn teoriaosassa tarkastellaan valvontaa yleisesti, OSI-mallia ja sen seitsemää eri kerrosta. Tarkastelussa on myös valvonnassa käytettyjä protokollia, kuten SNMP, IP, TCP, UDP, ICMP ja telnet. Tärkeimpänä näistä protokollista verkonvalvonnass on SNMP. SNMP on verkonvalvontaprotokolla, joka helpottaa hallintaa ja informaation vaihtoa eri verkkolaitteiden välillä. SNMP sisältää myös MIB-tietokannat ja SMI:n, joka on hallintatietojen rakenteiden määrittelyä. Alkuperäiset ja uudet valvontasovellukset käydään myös läpi.

Aiempia käytettyjä valvontasovelluksia yrityksessä ovat muun muassa Cacti, ipMonitor ja FortN, joiden avulla valvotaan verkon ja sen palvelimien tilaa. Tässä opinnäytetyössä etsittiin sovellusta, joka voisi yhdistää mahdollisimman monta hyvää ominaisuutta näistä kolmesta, alkuperäisestä sovelluksesta.

Nagios on erittäin hyvin muokattavissa oleva valvontasovellus, mutta ei itsessään tarjoa kuin rungon valvontasovellukselle. Toimiakseen kunnolla se tarvitsee paljon lisäosia, joita kuka tahansa voi itse kehittää. Nagioksen toimintakuntoon saattaminen voi vaatia valvottavasta verkosta riippuen todella paljon työtä. Zabbix on yksinkertaisella graafisella käyttöliittymällä toteutettu kokonainen sovellus. Zabbix mahdollistaa sekä hallinnan, että valvonnan graafisen käyttöliittymän kautta. Zabbix on käyttäjäystävällinen verkonvalvontasovellus.

Työssä päädyttiin suosittelemaan Zabbix-verkonvalvontasovellusta, sillä se vastasi parhaiten HTK NetCommunication Oy:n vaatimuksia. Alkuperäisten sovellusten, eli Cactin, ipMonitorin ja FortN:n hyvät puolet kasattiin yhteen ja niiden perusteella haettiin sopivinta sovellusta. Zabbix vastasi näihin vaatimuksiin, minkä takia sitä suositellaan otettavaksi käyttöön lisänä alkuperäisille sovelluksille.

Avainsanat: verkonvalvontasovellus, SNMP, Nagios, Zabbix

Lahti Polytechnic
Faculty of Technology

VESA, KIMMO: Comparison of network monitoring programs

Bachelor's Thesis in Telecommunications Technology, 52 pages

Spring 2007

ABSTRACT

The subject of this Bachelor's thesis is a comparison of network monitoring programs. The programs that are compared are Nagios and Zabbix. The aim is to find a suitable network monitoring program for HTK NetCommunication Oy for monitoring network servers and services.

Network monitoring, OSI reference model and its seven different layers are examined in the theory part of the thesis. Under examination are also protocols like SNMP, IP, TCP, UDP and telnet that are used in network monitoring. The most important protocol is SNMP. SNMP is a network monitoring protocol which helps managing and exchanging information between different network devices. SNMP also includes MIB database and SMI, which defines the structure of management information.

The company uses several network monitoring programs already, including Cacti, ipMonitor and FortN, which all help to monitor the condition of network services and servers. The object was to find a program that combines most of the useful properties of these original three programs.

Nagios is a very flexible program, but contains only the core to the program itself. It needs plugins to work properly and everyone can develop new plugins. Depending on the size of the network Nagios might need a lot of work to get fully operational. Zabbix has a simple graphical user interface and is a full program. Zabbix makes the monitoring and managing of a network possible through a graphical user interface. Zabbix is a user friendly program.

Based on user experience, Zabbix was the program chosen to be recommended for use as an addition, because it was closer to the expectations that HTK NetCommunication Oy had for the new monitoring program. Good properties from the original Cacti, ipMonitor and FortN programs were collected and those properties were used in search of a new program.

Key words: network monitoring programs, SNMP, Nagios, Zabbix

SISÄLLYS

LYHENNELUETTELO

ACK	Acknowledgment, kuittaus
AIX	Advanced Interactive eXecutive, IBM:n koneissa käytetty Unix-järjestelmä
ASCII	American Standard Code for Information Interchange, tietokoneiden kanssa käytetty merkistö
BSD	Berkeley Software Distribution, nimitys toiselle Unix-päähaaralle ja siitä polveutuville järjestelmille
CGI	Common Gateway Interface, tekniikka jonka avulla selain lähettää dataa palvelimilla suorittavalle ohjelmalle
DES	Data Encryption Standard, symmetrinen lohkosalain
DF	Don't Fragment, Don't Fragment -bitti määrittää yhteyden tuleviin paketteihin
DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla
DNS	Domain Name System, nimipalvelujärjestelmä
FTP	File Transfer Protocol, tiedonsiirtoprotokolla
GNU	GNU's Not Unix, järjestelmä
GPL	General Public License, vapaa ohjelmistolisenssi
GD	Graphics Draw, grafiikkakirjasto dynaamiseen kuvan muokkaukseen
HP-UX	Hewlett Packard UniX, HP:n Unix-järjestelmä
HTML	HyperText Markup Language, kuvauskieli
HTTP	HyperText Transfer Protocol, hypertekstin siirtoprotokolla
ICMP	Internet Control Message Protocol, kontrolliprotokolla
ICQ	“I seek you”, pikaviestinohjelma
IIS	Internet Information Services, palvelinohjelmistokokonaisuus
IMAP	Internet Message Access Protocol, sähköpostiprotokolla
IP	Internet Protocol, internetprotokolla
LTS	Long Term Support, palvelu tuelle
MAC	Media Access Control, osajärjestelmä
MD5	Message-Digest algorithm 5, tiivistealgoritmi
MIB	Management Information Base, tietokanta
MSN	Microsoft Network, Microsoftin monitoimiportaali

NNTP	Network News Transfer Protocol, uutisryhmäprotokolla
OS	Operating System, käyttöjärjestelmä
OSI	Open Systems Interconnection reference model, OSI-viitemalli
PC	Personal Computer, tietokone
PHP	PHP Hypertext Preprocessor, ohjelmointikieli
POP3	Post Office Protocol version 3, sähköpostiprotokolla
RAS	Remote Access Service, etäyhteyspalvelu
RFC	Request For Comments, suosituksia asiakirjamuodossa
ROI	Return Of Investment, laskennallinen määre
SLA	Service Level Agreement, laatusopimus
SMI	Structure of Management Information, hallintatietojen rakenteiden määritys
SMS	Short Message Service, lyhytsanomapalvelu
SMTP	Simple Mail Transfer Protocol, sähköpostiprotokolla
SNMP	Simple Network Management Protocol, tietoliikenneprotokolla
SQL	Structured Query Language, kyselykieli
SSH	Secure Shell, suojattu tiedonsiirtojärjestelmä
SSL	Secure Sockets Layer, salausprotokolla
TCP	Transmission Control Protocol, tietoliikenneprotokolla
UDP	User Datagram Protocol, yhteyskäytäntö
WINS	Windows Internet Naming Service, palvelinohjelmisto
WWW	World Wide Web, hajautettu hypertekstijärjestelmä

1 JOHDANTO

Palveluntarjoajat tarvitsevat mahdollisimman kattavat valvontajärjestelmät palvelimiensa ja palveluidensa tueksi helpottamaan jokapäiväistä työskentelyä. Ilman valvontajärjestelmiä työntekijöiden aika menisi tarkkaillessa lukemattomien palvelimien ja palveluiden tilaa.

Työ tehtiin HTK NetCommunication Oy:lle. Kyseinen yritys on Lahdessa toimivan paikallisen puhelinoperaattorin tytäryhtiö ja tarjoaa pääasiallisesti internetpalveluita lähinnä Päijät-Hämeen ja Kanta-Hämeen alueilla. Toimialana HTK NetCommunication Oy:llä ovat tietoliikenne ja ATK-palvelut. PHNet.fi on HTK NetCommunication Oy:n, Päijät-Hämeen Puhelin Oyj:n ja Esan Kirjapaino Oy:n tuottamien palveluiden tuotemerkki. (HTK NetCommunication Oy 2007a.)

Päijät-Hämeen Puhelin Oyj tarjoaa sekä yksityis- että yritysasiakkaille internetliittymiä ja HTK NetCommunication Oy palvelut näihin liittymiin. Esimerkiksi sähköpostipalvelut, kotisivupalvelut sekä erilaiset palvelinratkaisut kuuluvat HTK NetCommunication Oy:n tarjoamiin palveluihin. HTK NetCommunication Oy:n verkkopalveluihin kuuluvat myös Lukutulkki, joka auttaa englannin kielen ymmärtämisessä, sekä PHNet Musiikki, joka tarjoaa mahdollisuuden ladata musiikkia omalle tietokoneelle laillisesti. (HTK NetCommunication Oy 2007b.)

HTK NetCommunication Oy tarjoaa myös Päijät-Hämeen alueella tietoverkkojen hallintaan ja ylläpitoon, mikrotukeen sekä erilaisiin Internet-, Extranet- ja Intranet-ratkaisuihin liittyviä palveluita. Yritys toimii myös Lahden kaupunkiseudun aluetietoverkon hallintaorganisaationa. Aluetietoverkon asiakkaita ovat Päijät-Hämeen alueen kunnat. (HTK NetCommunication Oy 2007b.)

TAULUKKO 1. HTK Netcommunication Oy:n tarjoamien palveluiden yhteenveto (HTK NetCommunication Oy 2007b).

ISP-palvelut	**Palvelinhotelli**
Verkkotunnukset Sähköpostipalvelut Kotisivutila Tietokannat Nimipalvelut Virussuojauspalvelut Roskapostinsuodatus	Palvelintila Ylläpito Laitevuokraus
Mikrotuki	**Verkkopalvelut**
Työasemat Ohjelmat Laitteet	Analysointi Suunnittelu Tietoliikenne Etätyöpalvelu

HTK NetCommunication Oy käyttää apunaan laajaa valvontaohjelmistokokonaisuutta. Tämän työn tavoitteena on tutustua kahteen ilmaiseen verkonvalvontaohjelmistoon ja yrittää selvittää, voisiko niitä käyttää apuna yrityksen verkonvalvonnassa. Ohjelmat ovat Nagios ja Zabbix. Tutkimusongelmana on löytää varteenotettava valvontaohjelma, joka tarjoaa tarpeeksi monipuolisen kuvan verkon tilasta ja pystyy kertomaan sen mahdollisimman tehokkaasti valvojalle.

Tilanne on useissa IT-yrityksissä se, että verkonvalvojat ehtivät vain korjaamaan esiin tulevia vikoja, eikä heillä riitä aika palveluiden kehittämiseen, joka toisi samalla lisää luotettavuutta verkolle. Erilaiset valvontasovellukset helpottavat verkonvalvojan työtä, mutta sovellukset tulee valita tarkoin, jotta ne eivät kerää turhaa tietoa. Valvontasovelluksen tulee tarkkailla verkon ja palvelimien tilaa, ja ilmoittaa heti virheistä verkonvalvojalle mahdollisimman monipuolisesti ja tehokkaasti, jotta valvoja ehtii puuttua tilanteeseen.

Alustavasti työ tehdään tutkimustyönä ja myöhemmin nähdään, aletaanko sovelluksia kokeilla aidossa työympäristössä. Uuteen valvontasovellukseen tutustuminen vie usein paljon aikaa, jota verkonvalvojalla on harvoin liikaa käytössä. Tästä syystä molemmista sovelluksista täytyy löytää niiden oleellisimmat ominaisuudet, jotta voidaan alkaa miettiä, kannattaako niitä ottaa kokeiluun asti.

2 VERKONVALVONTA

2.1 Valvonta

2.1.1 Miksi valvontaa tarvitaan

Verkonvalvonta on tärkeässä asemassa nykypäivän tietoyhteiskunnassa, jossa palveluntarjoajat tarvitsevat mahdollisimman tehokkaat apuvälineet helpottamaan tarjoamiaan palvelimia ja palveluita. Liian suuri määrä valvontaohjelmia voi kuitenkin aiheuttaa sekaannuksia, joten yritykset tarvitsevat ohjelman, joka korvaisi mahdollisimman monta ominaisuutta muista valvontaohjelmistoista.

Valvontaohjelmien tulee olla vakaita, ja niiltä vaaditaan paljon. Esimerkiksi lokin kerääminen valvottujen palvelimien ja palveluiden tapahtumista on tärkeä ominaisuus. Tapahtuneista ongelmista ja muutoksista tulee myös saada monipuolisesti informaatiota, eikä riitä, että valvontaohjelmisto vain kirjoittaa ne ylös johonkin tietokantaan tai tiedostoon. On tärkeää, että verkonvalvojat saavat tiedon palvelimissa tai palveluissa tapahtuvista ongelmista niin, että he voivat reagoida tapahtuneeseen mahdollisimman pian.

Erilaisten kuvaajien ja graafien merkitys on kasvanut operaattoreille. Monet asiakkaat haluavat tietää, kuinka luotettava palveluntarjoaja on. Tällaisessa tilanteessa pelkkä lokitiedosto, joka sisältää tietoa esimerkiksi web-palvelimesta, ei kerro välttämättä asiakkaalle mitään. Kuvaajat voivat kertoa erittäin seikkaperäisesti palveluntarjoajan luotettavuudesta asiakkaalle niin, että he ymmärtävät sen. Tästä syystä on tärkeää, että valvontaohjelmisto kykenisi myös graafiseen tiedon ilmaisemiseen.

Verkonvalvonnassa käytetään hyväksi testejä. Esimerkiksi saavutettavuus, tiedon eheys ja vasteaika ovat kohteina testeissä. Kun löydetään ongelma, on verkonvalvojan ryhdyttävä toimiin. Yleensä toimiin kuuluvat seuraavat toimenpiteet:

1. Paikallistetaan täsmällisesti, missä vika on.

2. Eristetään muu verkko vian aiheuttamilta häiriöiltä.

3. Konfiguroidaan tai muutetaan verkkoa niin, että minimoidaan vikaantuneen komponentin vaikutukset muun verkon toimintaan.

4. Korjataan tai vaihdetaan vikaantuneet komponentit, jotta verkko voidaan palauttaa alkuperäiseen tilaan.

(Koljonen 2007b.)

Valvonta on erittäin kriittinen osa tietoverkkojärjestelmää, sillä vian ilmaantuessa asiakkaat ja verkon käyttäjät odottavat korjaamista välittömästi. Viasta on tultava ilmoitus ja se on korjattava heti. Tämä vaatii tehokasta valvontajärjestelmää, jotta verkonvalvoja saa tiedon heti, kun ongelma esiintyy. Valvontajärjestelmän avulla korjaustoimenpiteet voidaan aloittaa välittömästi. Verkonhallinta tehostuu, jos valvontajärjestelmä ilmoittaa mahdollisimman monipuolisesti ilmenneistä vioista. Esimerkiksi sähköposti- ja tekstiviesti-ilmoitukset ovat osoitus tehokkaasta vian ilmoittamisesta. On myös avuksi, jos järjestelmä osaa kertoa mihin vika vaikuttaa.

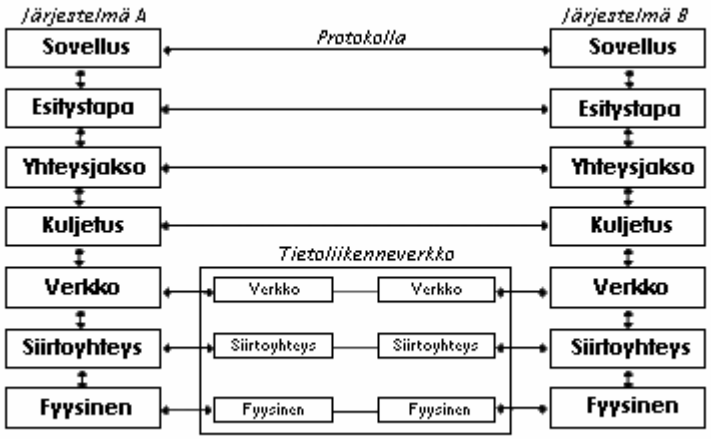
2.1.2 Valvonnan terminologiaa

- Polling:lla tarkoitetaan teleliikenteessä verkon kontrollointia, jossa verkossa olevia asemia pyydetään lähettämään dataa sekvensseissä yksi kerrallaan tietyin määrävälein (Koljonen 2007a).

- Trapping:lla tarkoitetaan teleliikenteessä sitä, kun jokin aktiivilaite lähettää tiedon havaitusta ongelmasta valvontasovellukselle. Trapping-ominaisuutta käytetään erityisesti SNMP-protokollan (Simple Network Management Protocol) yhteydessä. (Koljonen 2007a.)

2.2 OSI-malli

OSI-malli (Open Systems Interconnection) kehitettiin alun perin tietoliikennejärjestelmien suunnittelemisen helpottamiseksi. Se antaa yleisen kuvan siitä, miten tiedon välitys koostuu. OSI-mallissa tiedon välitys on jaettu seitsemään kerrokseen, jossa alin kerros on yksinkertaisin ja alkeellisin ja ylemmät monimutkaisempia mutta käyttävät alempia kerroksia hyväkseen. Kerrokset ovat siis sidoksissa toisiinsa, ja esimerkiksi sovelluksen käyttäessä verkkoa hyväkseen käydään kaikki OSI-mallin kerrokset läpi alkaen lähdepäässä sovellustasosta ja laskeutuen kohti fyysistä tasoa, josta päädytään vastaanottopään fyysiseen tasoon, josta noustaan takaisin sovellustasolle. (Ala-Mutka, Rintala, Savikko & Palviainen 2002.)



KUVIO 1. OSI-mallin rakenne (Ala-Mutka ym. 2002).

1. Fyysinen kerros:

OSI-mallin fyysiseen kerrokseen liittyvät tiedonsiirron loogiset, sähköiset sekä mekaaniset asiat. Tietoa voidaan siirtää kahdella tavalla: joko sarjamuotoisena tai rinnakkain. Sarjamuotoisena bitit siirretään peräjälkeen yksi kerrallaan. Rinnakkain siirretään kaikki bitit yhdestä merkistä kerrallaan omia linjoja pitkin. (Ala-Mutka ym. 2002.)

2. Siirtokerros:

OSI-mallin toinen kerros eli siirtoyhteyskerros hoitaa yhteyden luomisen ja purkamisen sekä virheiden korjaamisen. OSI-mallin toinen kerros ohjaa dataa fyysisten osoitteiden perusteella. Esimerkiksi verkkokorteilla on oma fyysinen osoitteensa, eli MAC-osoite (Media Access Control). Myös vuonvalvonta kuuluu siirtoyhteyskerrokselle. (Ala-Mutka ym. 2002.)

3. Verkkokerros:

OSI-mallin kolmas kerros eli verkkokerros hoitaa reitittämisen lähteeltä kohteelle. Se siis valitsee reitin, mitä kautta paketit kulkevat kohteeseen. Verkkokerroksessa lähde ja kohde tunnistetaan loogisten osoitteiden, eli IP-osoitteiden (Internet Protocol) perusteella. Verkkokerros pitää sisällään IP-protokollan. (Ala-Mutka ym. 2002.)

4. Kuljetuskerros:

OSI-mallin neljäs kerros eli kuljetuskerros takaa esimerkiksi luotettavan päästä päähän yhteyden tietoliikenteessä. Kuljetuskerros pitää huolen pakettien perillepääsystä ja oikeasta järjestyksestä. Myös vuonohjaus kuuluu kuljetus-kerrokselle. Kuljetuskerros sisältää kuljetusprotokollat TCP:n (Transmission Control Protocol) ja UDP:n (User Datagram Protocol), jotka eroavat toisistaan nopeudessa ja luotettavuudessa. TCP on luotettavampi kuljetusprotokolla mutta samalla hitaampi kuin UDP. UDP taas on nopeampi, mutta se on luokiteltu epäluotettavaksi. (Ala-Mutka ym. 2002.)

5. Yhteyskerros:

OSI-mallin viides kerros, eli yhteysjaksokerros takaa esityskerrokselle organisoitua ja synkronoitua tiedonsiirtoa (Ala-Mutka ym. 2002).

6. Esityskerros:

OSI-mallin kuudes kerros, eli esityskerros hoitaa tiedon esitystavan tiedonsiirrossa. Tarkoituksena on saattaa data sellaiseen muotoon, jota vastaanottopää ymmärtää. (Ala-Mutka ym. 2002.)

7. Sovelluskerros:

OSI-mallin seitsemäs kerros, eli sovelluskerros toimii apuna sille sovellukselle, jota tiedonsiirto tarvitsee. Verkossa käytettävistä sovelluksista, joita sovelluskerros hoitaa, voidaan mainita esimerkiksi FTP (File Transfer Protocol), telnet ja DNS (Domain Name System). (Ala-Mutka ym. 2002.)

2.3 SNMP

2.3.1 SNMP yleisesti

The Simple Network Management Protocol (SNMP) on sovellustason protokolla, joka helpottaa hallintainformaation vaihtoa verkkolaitteiden välillä. SNMP on määritelty RFC-dokumentissa 1157 (Request For Comments). SNMP on osa TCP/IP –protokollasarjaa. SNMP mahdollistaa verkonvalvojaa hallitsemaan verkon suorituskykyä, löytämään ja ratkaisemaan verkon ongelmia ja suunnittelemaan verkon kasvua. SNMP-protokolla käyttää apunaan MIB-tietokantaa (Management Information Base) (RFC1156) ja SMI:tä (Structure of Management Information) (RFC1155), joka on hallintatietojen rakenteiden määrittelyä. (Cisco Systems, Inc. 2006.)

SNMP on yhteydetön protokolla, ja se kulkee UDP-protokollan päällä. Oletuksena SNMP käyttää porttia 161 ja SNMP-trap –viestit käyttävät porttia 162. (Koljonen 2007a.)

SNMP-hallintajärjestelmään kuuluu:

- verkon solmuja, joissa on SNMP-osapuoli (SNMP entity). Näitä kutsutaan agenteiksi ja niillä on mahdollisuus päästä hallintavälineistöön (management instrumentation)
- vähintään yksi SNMP-osapuoli, jossa on hallintasovellus. Se on nimeltään hallinta-asema (manager)
- hallintaprotokolla, jolla SNMP-osapuolten välillä siirretään hallintatietoa

(Haikonen, Hlinovsky & Paju 2000.)

Hallintaosapuolet valvovat ja hallitsevat hallittavia osapuolia kyselyiden ja komentojen avulla. Hallittavat osapuolet ovat normaaleja verkon laitteita, kuten reitittimiä, työasemia ja verkkotulostimia, joissa on SNMP-agentti. (Haikonen ym. 2000.)

SNMP:ssä on viestejä, jotka voidaan jakaa kolmeen eri ryhmään:

- GET-viestit: Tässä viestissä hallinta-asema pyytää Get-request–viestillä agentilta jonkin muuttujan arvoa. Agentti lähettää vastauksen Get-response–viestillä. Hallinta-asema voi myös kysyä Get-next-request–viestillä MIB-tietokannan seuraavaa arvoa, johon agentti vastaa myös Get-response–viestillä.
- SET-viestit: Hallinta-asema pyytää Set-request –viestin avulla agenttia asettamaan jonkin tietyn arvon jollekin tietylle muuttujalle.
- TRAP-viestit: Näillä viesteillä agentti lähettää hallinta-asemalla tietoa verkon tapahtumista, kuten virhetilanteista. Hallinta-aseman tulee päättää mahdollisista toimenpiteistä viestiin liittyen.

(Haikonen ym. 2000.)

2.3.2 SNMP:n versiot

Toukokuussa 1990 SNMPv1 hyväksyttiin Internet-standardiksi. SNMP-protokollan ensimmäinen versio kärsi puutteellisesta tietoturvasta, joka johtui protokollan yksinkertaisuudesta. SNMPv1:ssä käytetään salasanaa ja lähettäjän IP-osoite tarkistetaan, jotta tiedetään, että SET-viestit tulevat oikeilta lähettäjiltä. Salasanat kulkevat kuitenkin selväkielisinä, eikä lähettäjän IP-osoitteen muuttaminen ole vaikeaa. (Haikonen ym. 2000.)

SNMPv2 on selvästi edeltäjäänsä monimutkaisempi. Esimerkiksi yhteyskäytäntöä otettiin mukaan kaksi uutta viestiä. GetBulkRequest-viestillä hallinta-asemat pyytävät suuria tietomääriä hallinta-agenteilta. InformRequest-viesti mahdollistaa trap-viestien tyyppisten viestien lähettämisen hallinta-asemalta toiselle hallinta-asemalle. (Javvin Technologies, Inc. 2005a.)

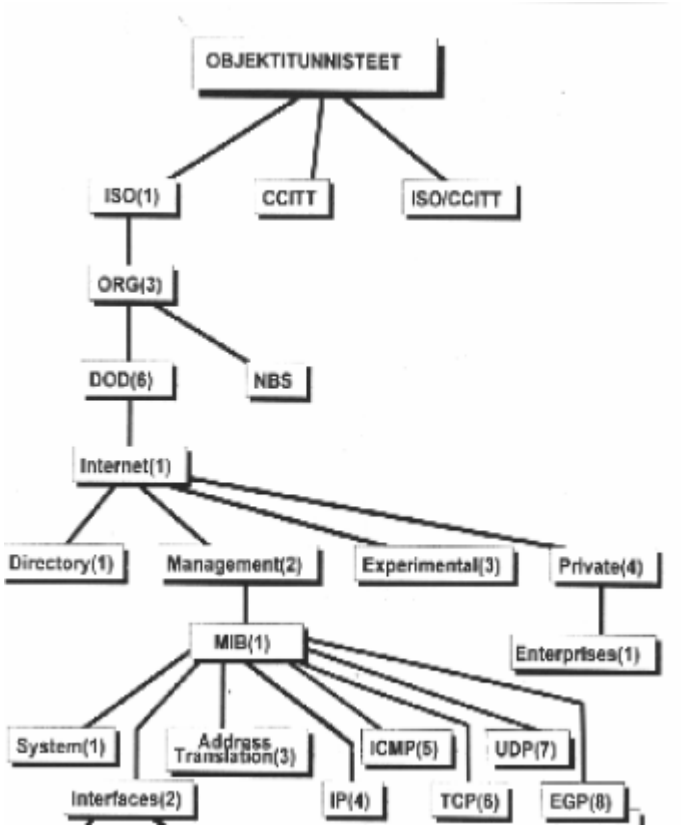
SNMPv2:ssa panostettiin turvallisuuteen. Autentikointi ja viestien eheys tapahtuu MD5-algoritmin (Message Digest algorithm 5) avulla ja tiedon salaukseen käytetään DES-algoritmia (Data Encryption Standard). (Kotiharju 1996.)

SNMPv3 lisää tietoturvaa ja etäkonfigurointimahdollisuuksia aiempiin versioihin verrattuna. Mukana ovat esimerkiksi autentikointi, yksityisyys ja pääsynvalvonta. (Javvin Technologies, Inc. 2005b.)

2.3.3 MIB ja SMI

MIB on puumainen tietokanta, jossa jokaisella muuttujalla on oma numero-tunnisteensa. Tunnisteen avulla haluttu tieto voidaan yksilöidä. MIB-tietokantoja on standardoitu kymmeniä kappaleita, ja ne on määritelty RFC-dokumenteissa. MIB-tietokannat ovat ASCII-pohjaisia (American Standard Code for Information Interchange) tekstitiedostoja, ja niillä pyritään valvomaan haluttuja laitteita ja kuvaamaan niiden ominaisuuksia. (Majorin 2007.)

MIB:lla on muuttujia, jotka jaotellaan kahdeksaan eri pääryhmään. Viisi pääryhmää koskee perusprotokollien (IP, ICMP, TCP, UDP ja EGP) hallinta-tietoa. Loput kolme pääryhmää määrittelevät laitteiden verkkotiloja, tarkemmin ARP, verkkoliitännät ja laitteen käyttämän käyttöjärjestelmän tilaa. Puumainen, eli hierarkkinen muuttuja-avaruus estää päällekkäisyyksien syntymisen, eri muuttujia ei voi siis johtaa toisistaan. Esimerkiksi muuttuja IP löydetään MIB-tietokannan puumaisesta rakenteesta seuraavasti: iso.org.dod.internet.mgmt.mib.ip. Sama voidaan esittää myös numeromuodossa seuraavasti: 1.3.6.1.2.1.4. (Majorin 2007.)



KUVIO 2. MIB-tietokannan puumainen rakenne (Koljonen 2007a).

MIB-tietokannoista on useita eri versiota. MIB-II on nykyään yleisin käytetty standardi. Monissa RFC-dokumenteissa on kuvattu erityyppisiä MIB-tietokantoja. (Majorin 2007.)

SMI määrittää hallintatietojen rakenteita. SMI:n mukaan kaikilla hallittavilla objekteilla on nimi, rakenne ja koodaus. Nimi on tunniste objektille. Rakenne määrittää sen tyypin, eli onko objekti esimerkiksi kokonaisluku tai merkkijono. Koodaus taas kertoo, kuinka hallittava informaatio muotoillaan verkkoon lähettämistä varten. (Koljonen 2007a.)

2.4 Muut käytetyt protokollat

2.4.1 IP

IP-protokolla määritellään RFC-dokumentissa 791, joka on julkaistu vuonna 1981. Kyseinen protokolla suunniteltiin yhdistämään pakettikytkentäisen tietoliikenneverkon tietokoneita. Se tarjoaa datapakettien lähettämistä lähteeltä kohteelle määriteltyjen osoitteiden perusteella bittipaketteina, suurien datapakettien paloittelemista sekä niiden uudelleenkokoamista. (Postel 1981a.)

IP-protokolla toimii päätteeltä-päätteelle protokollana, ja se pyytää paikallisen verkon protokollia kuljettamaan datapaketit seuraavalle yhdyskäytävälle tai kohteelle. (Postel 1981a.)

Protokolla pitää huolen pakettien kuljettamisesta, ja se sisältää lähettäjän ja vastaanottajan IP-osoitteet sekä 1-1500 tavua dataa. IP-osoitteiden perusteella verkossa olevat reitittimet osaavat huolehtia pakettien kuljetuksesta oikeaan paikkaan. Pakettien vaihteleva pituus aiheuttaa muutoksia käsittelyyn vievässä ajassa, joka voi tuottaa suurilla siirtonopeuksilla teknisiä vaikeuksia. (Postel 1981a.)

Osoitteistus ja fragmentointi ovat kaksi perusominaisuutta, joita IP-protokolla käyttää apuvälineinään. Internetissä kulkevien datapakettien kehyksissä on mukana IP-osoitteet, joiden perusteella paketit löytävät perille. IP-osoitteen perusteella löydetään paketin kohde, jonka jälkeen täytyy löytää vielä reitti kohteen luokse. Oikean reitin valitsemista verkossa kutsutaan reitityksekseksi. Datapaketteja saatetaan myös pilkkoa ja koota takaisin tarpeen mukaan, jos mennään ”pienipakettisten” verkkojen lävitse. (Postel 1981a.)

Jokainen tietokone ja yhdyskäytävä verkossa jakaa samat säännöt, jotka koskevat IP-protokollaa. Jokaisen tietokoneen ja yhdyskäytävän täytyy osata tulkita IP-osoitteita sekä ymmärtää pakettien pilkkomista ja kokoamista. Yhdyskäytävät sisältävät myös menettelytapoja reitityspäätöksien tekemiseksi. (Postel 1981a.)

Taatakseen palvelunsa IP-protokolla käyttää neljää eri mekanismia:

- Type Of Service kertoo, minkä tasoista palvelua halutaan käyttää lähetyksessä. Sitä käytetään yhdyskäytävissä määrittämään kuljetettavalle datapaketille kuljetusparametrit tietyille verkoille, valitsemaan seuraavan hypyn takana oleva verkko tai seuraava yhdyskäytävä.

- Time To Live kertoo paketin elinajan verkossa. Sen asettaa datapaketin alkuperäinen lähettäjä, ja siitä vähennetään pisteitä aina sen kulkiessa verkossa eteenpäin. Jos Time To Live –arvo laskee nollaan, ennen kuin datapaketti on päässyt perille, niin datapaketti tuhotaan.

- Optionsissa annetaan ohjaustoimintoja. Joskus niistä voi olla hyötyä, mutta useimmiten niitä ei tarvita datansiirrossa. Ne voivat sisältää esimerkiksi aikaleimoja, suojaehtoja ja erikoisreititysehtoja.

- Header Checksum auttaa määrittämään datapaketin tiedon oikeellisuuden. Jos Header Checksum -tarkistus saa väärän arvon, on data virheellistä. Tässä tapauksessa datapaketti hylätään sen pisteen toimesta, joka huomaa kyseisen virheen.

(Postel 1981a.)

IP-protokolla ei itse tarjoa luotettavaa tiedon välittämistä. Se ei tarjoa muita tarkistuksia kuin Header Checksum –arvon. Se ei pidä sisällään virheenhallintaa, vuonohjausta tai uudelleenlähetystä. Huomatut virheet ilmoitetaan ICMP-protokollan (Internet Control Message Protocol) avulla. (Postel 1981a.)

2.4.2 TCP

TCP määritellään RFC-dokumentissa 793. TCP-protokollaa käytetään erittäin luotettavana kuljetusprotokollana pakettikytkentäisissä verkoissa päätelaitteelta päätelaitteelle. Se on yhteydellinen ja luotettava lähteeltä kohteelle protokolla. TCP on suunniteltu sopimaan kerrokselliseen protokollapinoon, joita verkkosovellukset tukevat. (Postel 1981c.)

TCP on lähteeltä-kohteelle protokolla, ja sen avulla pystytään lähettämään kumpaan suuntaan tahansa rajaton määrä dataa segmentoimalla data lähetystä varten. Protokolla käyttää PUSH-funktiota avukseen. Sen avulla käyttäjä voi varmistua, että kaikki data, minkä TCP on käsitellyt lähetettäväksi, on päässyt perille asti. PUSH-funktio määrää datan välitettäväksi nopeasti perille kohteeseen. (Postel 1981c.)

Luotettavuus TCP-protokollassa tulee virheenkorjauksesta. Jos data vahingoittuu, häviää matkalla, toistuu tai tulee väärässä järjestyksessä perille, niin TCP:n tulee selvitä siitä. Jokainen lähetetty datapaketti saa sekvenssinumeron, jotka kaikki vaativat positiivisen kuittauksen, eli ACKin (Acknowledgment) vastaanotto-päästä. Jos kuittausta ei tule määritellyn aikakatkaisun aikana, lähetetään data uudelleen. Vastaanottopää tarkistaa sekvenssinumeron perusteella, ovatko segmentit tulleet oikeassa järjestyksessä perille ja onko sama segmentti tullut kopiona uudestaan. Vahingoittuneet segmentit tarkistetaan lähetysvaiheessa lisätyn tarkistussumman avulla. Vastaanottaja tarkistaa tarkistussumman ja hylkää vahingoittuneet segmentit. Kunhan TCP-protokolla toimii oikein, eikä verkossa kulkeva data pilkkoudu täysin, niin siirtovirheet eivät vaikuta oikean datan siirtymiseen. (Postel 1981c.)

TCP sisältää myös vuonohjauksen, jossa vastaanottaja päättää lähettäjän lähettämän datan määrän. Vastaanottaja palauttaa ikkunan jokaisen kuittauksen mukana, jossa on mukana sekvenssien määrä, jotka lähettäjä saa lähettää ennen uuden luvan saamista. (Postel 1981c.)

Multipleksointi antaa mahdollisuuden usealle eri prosesseille käyttää samanaikaisesti TCP-protokollan palveluja. TCP antaa tätä varten jokaiselle päätelaitteelle osoitteita ja portteja. Verkko- ja päätelaiteosoitteet muodostavat liittyessään niin sanotun socketin. Socket-parien avulla tunnistetaan jokainen yhteys. (Postel 1981c.)

Jokaisen portin liittäminen johonkin porttiin käsitellään yksittäisesti jokaisessa päätelaitteessa. Yleisesti käytetyt prosessit kannattaa liittää yleisesti tiedossa oleviin socket:ihin. Näihin prosesseihin päästään sitten käsiksi tunnettujen osoitteiden perusteella. (Postel 1981c.)

Luotettavuus ja vuonhallinta vaativat sen, että TCP-protokollan täytyy pitää jonkinlainen tilannetieto jokaisesta datavirrasta. Tätä tietoa, johon liittyvät socket:t, sekvenssinumerot ja ikkunakoot, kutsutaan yhteydeksi. Jos kaksi prosessia haluaa jutella keskenään, täytyy TCP-protokollan hankkia nämä tiedot molemmista päistä muodostaakseen yhteyden. Kun prosessien vaatima tehtävä on suoritettu, tuhotaan yhteys ja vapautetaan sen viemät resurssit. (Postel 1981c.)

TCP-protokollaa käytettäessä käyttäjän on mahdollista saada yhteydelleen arvojärjestys ja suojaus. Kun näitä ei tarvita, niin käytetään perusarvoja. (Postel 1981c.)

2.4.3 UDP

UDP määritellään RFC-dokumentissa 768. Toisin kuin TCP, UDP on yhteydetön ja epäluotettava protokolla. Se kuitenkin toimii TCP:n tavoin IP-protokollan päällä. UDP-protokolla tarjoaa mahdollisuuden sovelluksille lähettää viestejä toisille sovelluksille mahdollisimman vähillä protokollille ominaisilla mekanismeilla. (Postel 1980.)

Epäluotettavuus tulee siitä, että UDP ei varmista datan perillepääsyä eikä datan kahdentumista, kuten TCP-protokolla. Sovellusten, jotka vaativat luotettavaa kuljettamista, täytyy käyttää TCP-protokollaa UDP-protokollan sijasta. UDP-kehykseen kuuluvat lähettäjän osoite, vastaanottajan osoite, pituus, tarkistussumma ja data-kentät. (Postel 1980.)

Lähettäjän osoitteessa on lähettäjän IP-osoite, jotta tiedetään, mistä data on alun perin lähtöisin.

- Vastaanottajan osoitteessa on vastaanottajan IP-osoite, jotta tiedetään mihin data on menossa.
- Pituus-kenttä kertoo datakehyksen minimipituuden oktetteina. Pienin pituus on siis kahdeksan.
- Tarkistussumma on 16-bittinen komplementti IP- ja UDP-kehyksien otsikkotiedoista ja datasta.

(Postel 1980.)

2.4.4 ICMP

ICMP on määritelty RFC-dokumentissa 792. ICMP on osa IP-protokollaa ja sitä käytetään, jos yhdyskäytävä tai yksittäinen pääte kommunikoi toisen päätteen kanssa ilmoittaakseen virheestä datasiirrossa. ICMP viestejä lähetetään useassa eri tilanteessa esimerkiksi silloin, jos yhdyskäytävä haluaa ilmoittaa, että pääte voi lähettää liikenteen lyhyempää kautta tai jos data ei pääse perille kohteeseen. (Comer 2002, 130.)

ICMP-protokollan tavoite on tarjota tietoa ja palautetta verkossa tapahtuvista ongelmista. Sen tarkoitus ei ole tehdä IP-protokollasta luotettavaa. On mahdollista, ettei data pääse perille eikä siitä tule myöskään ilmoitusta ICMP-viestinä. ICMP-viestit raportoivat datan etenemisestä. ICMP-viesteistä ei kuitenkaan lähde ICMP-viestejä. Jos jokin pääte ei vastaa ja ICMP lähettää lähdekoneelle Destination Unreachable –viestin eikä sekään pääse perille, niin siitä ei enää lähde uutta ICMP-viestiä. (Postel 1981b.)

Itse ICMP-viestit lähetetään IP-kehyksen sisällä. Ensimmäinen oktetti dataosiosta on ICMP:n tyyppikenttä. Tämän kentän arvo määrittää jäljellä olevan datan muodon. (Comer 2002, 132.)

ICMP-viesteillä voidaan kertoa eri asioita. Sillä on useita viestityyppejä, joiden avulla suoritetaan erilaisia tehtäviä. Kun puhutaan verkonvalvonnasta, niin ICMP-viesteistä nousevat ylimmäisiksi Echo- ja Echo-Reply –viestit, joiden avulla tarkistetaan, vastaako palvelin kyselyihin. Palvelimelle lähetetään Echo-viesti ja jos palvelin on pystyssä ja yhteys toimii odotetulla tavalla, palauttaa se Echo-Replyn vastauksena. Toinen yleinen viesti verkonvalvonnassa on tietysti Destination Unreachable, joka kertoo, että kohde on saavuttamattomissa. (Postel 1981b.)

ICMP kehyksessä on tyyppikoodi, joka kertoo, millaisesta Destination Unreachable –viestistä on kyse. Taulukossa 2 on lista eri ICMP-viestien tyypeistä tyyppikoodeilla:

TAULUKKO 2. ICMP-viestien tyypit (Postel 1981b).

Tyyppikoodi:	Viestin tyyppi
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Destination Unreachable-viestit

Jos datapaketin kohdekenttä on yhdyskäytävän reititystaulun mukaan saavuttamattomissa, eli sen etäisyys on ääretön, niin yhdyskäytävä lähettää ICMP-viestin Destination Unreachable datapaketin alkuperäiselle lähettäjälle. Toinen vaihtoehto Destination Unreachable –viestille on, jos vastaanottopään IP-moduuli ei voi toimittaa datapakettia perille protokollan moduulin tai prosessin porttinumeron ollessa saavuttamattomissa. (Postel 1981b.)

Yhdyskäytävässä voi myös olla Don’t Fragment-lippu päällä, ja jos datapaketti pitäisi pilkkoa lähetettäessä eteenpäin yhdyskäytävän kautta, niin yhdyskäytävän on hylättävä datapaketti ja lähetettävä Destination Unreachable -viesti datapaketin alkuperäiselle lähettäjälle. (Postel 1981b.)

Koodi-kenttä kertoo ICMP-viestin kehysrakenteessa millaisesta Destination Unreachable -viestistä on kyse. Destination Unreachable -viestissä voi olla seuraavat arvot:

0 = net unreachable;

1 = host unreachable;

2 = protocol unreachable;

3 = port unreachable;

4 = fragmentation needed and DF (Don’t Fragment) set;

5 = source route failed.

(Postel 1981b.)

Time Exceeded –viestit:

Jos data välittävä yhdyskäytävä huomaa Time To Live –kentän olevan nollassa, sen on hylättävä kyseinen paketti. Yhdyskäytävä voi myös ilmoittaa hylkäyksestä lähettäjälle Time Exceeded –viestin avulla. Toinen vaihtoehto Time Exceeded –viestille on se, jos pilkkoutuneen datapaketin kokoaminen ei onnistu puuttuvien palojen vuoksi tietyn määritetyn ajan kuluessa. Tässä tapauksessa kokoamista yrittävä piste hylkää jälleen paketin ja voi lähettää Time Exceeded –viestin. (Postel 1981b.)

Parameter problem –viestit:

Jos yhdyskäytävä tai datapakettia käsittelevä palvelin huomaa ongelman kehyksen otsikkotiedoissa, niin sen täytyy hylätä datapaketti. Tämä voi tapahtua, jos huomataan, ettei pakettia voida kunnolla käsitellä otsikkotietojen perusteella. Sen voi aiheuttaa esimerkiksi väärä muuttuja. Yhdyskäytävä tai palvelin voi lähettää datapaketin hylkäämisestä Parameter Problem –viestin lähettäjälle. Viesti lähetetään vain, jos virhe aiheuttaa datapaketin hylkäämisen. (Postel 1981b.)

Osoitin kertoo alkuperäisen datapaketin otsikosta sen oktetin, josta virhe havaittiin. Esimerkiksi 1 ilmaisee vikaa Type of Servicessä, eli palvelunlaadussa ja 20 ilmaisee ongelmaa tyyppi-koodissa. (Postel 1981b.)

Source Quench -viestit:

Jos yhdyskäytävällä ei ole tarvittavaa puskuritilaa datapaketin jonoonlaittamista varten seuraavaan verkon reittiin kohdetta kohti, voi se hylätä datapaketin. Jos hylkäys tapahtuu, voi yhdyskäytävä lähettää Source Quench -viestin lähetäjälle. Myös vastaanottava kohde voi lähettää Source Quench -viestin lähettäjälle, jos datapaketti saapuu liian nopeasti käsiteltäväksi. (Postel 1981b.)

Source Quench –viestiä käytetään siis ilmoittamaan lähettäjälle, että sen täytyy hidastaa tahtia, jolla se lähettää dataa vastaanottajalle. Yhdyskäytävä voi lähettää jokaisesta hylkäämästään paketista Source Quench –viestin datapaketin alkuperäiselle lähettäjälle. Tässä tapauksessa lähettäjän täytyy hidastaa lähetysvauhtia, kunnes ei enää saa kyseisiä viestejä yhdyskäytävältä. Tämän jälkeen lähettäjä voi nostaa asteittain lähetysnopeutta, kunnes saa jälleen Source Quench -viestejä. (Postel 1981b.)

Yhdyskäytävän aiheuttanut datapaketti tai lopullinen kohde, voivat lähettää Source Quench -viestin, kun kapasiteetin raja tulee vastaan. Viesti lähetetään, ennen kuin se aiheuttaa kapasiteetin ylityksen. Tästä syystä kyseinen datapaketti voidaan vielä käsitellä, mikä aiheutti Source Quench -viestin. (Postel 1981b.)

Redirect–viestit:

Yhdyskäytävä lähettää uudelleenohjaus-viestin isäntäkoneelle seuraavassa tapauksessa. Kun yhdyskäytävä 1 saa datapaketin välitettäväksi ja huomaa, että seuraava yhdyskäytävä 2 on samassa verkossa yhdyskäytävän 1 kanssa, niin se lähettää isäntäkoneelle viestin, jossa neuvoo isäntäkonetta lähettämään datapaketit suoraan yhdyskäytävälle 2, koska se on lyhyempi reitti. (Postel 1981b.)

Jos datapaketissa on alkuperäiset IP-reitit asetettuna ja yhdyskäytävän osoite kohdeosoite-kentässä, niin uudelleenohjaus-viestiä ei lähetetä, vaikka löytyisi parempi reitti lopulliseen kohteeseen. (Postel 1981b.)

Echo- ja Echo Reply -viestit:

Echo Reply viesti on vastaus echo-viestiin, ja sen tulee sisältää Echo-viestin sisältö. Echo-viestit voidaan tunnistaa porttinumeron ja sekvenssinumeron perusteella ja Echo Reply -viestistä tulee tulla ilmi, mihin Echo-viestiin sillä vastataan. Kyseessä ovat siis kyselyviestit, joilla tarkistetaan, vastaako toinen pää kyselyyn. (Postel 1981b.)

Yksinkertaisesti sanottuna: jos esimerkiksi verkonvalvoja haluaa kokeilla, onko sähköpostipalvelin pystyssä, hän lähettää Echo-kyselyn sähköpostipalvelimelle. Jos hän saa vastauksen, eli Echo Replyn, on palvelin pystyssä. Echo ja Echo Reply -viesteihin viitataan usein myös Ping-nimellä, joka on TCP/IP-protokollassa käytetty apuväline. (Postel 1981b.)

Timestamp ja Timestamp Reply -viestit:

Jokaisen kehyksen mukana tulee aikaleima. Kehys saa aikaleiman sillä hetkellä, kun lähettäjä viimeisen kerran koskettaa kehystä ennen sen lähettämistä. Kehys saa aikaleiman myös kun vastaanottaja ensimmäisen kerran koskettaa kehystä ja kun se viimeisen kerran koskettaa sitä. Aikaleimojen avulla kiertoviiveiden tarkkaileminen helpottuu. (Postel 1981b.)

Information Request- ja Information Reply -viestit:

Nämä viestit antavat työasemalle mahdollisuuden saada selville verkkonsa numeron (Postel 1981b).

2.4.5 Telnet

Telnet-protokolla määritellään RFC-dokumentissa 854. Telnet on tarkoitettu tarjoamaan yleinen kaksisuuntainen yhteystapa kahden pisteen välille verkoissa. Se on TCP-protokollan kautta toimiva protokolla, jolla on kolme päätehtävää: Ensimmäinen on konsepti virtuaalisesta verkkopäätteestä, toinen on periaate neuvoteltavista mahdollisuuksista ja kolmas on symmetrinen näkymä päätteistä ja prosesseista. (Postel & Reynolds 1983.)

Kun telnet-yhteys muodostetaan, niin molemmat päät alkavat ja päättyvät virtuaaliseen verkkopäätteeseen. Se toimii välissä kuvitteellisena laitteena ja hoitaa välittämisen ja esitystavat kahden oikean päätteen välillä. (Postel & Reynolds 1983.)

Telnet on luotettava verkonvalvontaprotokolla, sillä telnet-yhteys käy kaikki seitsemän tasoa OSI-mallista läpi alkaen lähtöpisteen sovelluskerroksesta päättyen päätepisteen sovelluskerrokseen. Tämän avulla voidaan saada selville esimerkiksi jonkin palvelimen täysi toimivuus. (Postel & Reynolds 1983.)

3 ALKUPERÄISET VALVONTASOVELLUKSET

3.1 ipMonitor

IpMonitor on maksullinen valvontaohjelma. IpMonitorilla voi valvoa suurta määrää sovelluksia, tietokantoja ja palvelimia. Tuettuna ovat:

- Windows NT, Windows XP, Windows 2000 ja Windows 2003
- Microsoft Exchange, IIS (Internet Information Services), SQL (Structured Query Language), Site Server ja Transaction Server
- RAS (Remote Access Service), WINS (Windows Internet Naming Service), DHCP (Dynamic Host Configuration protocol)
- Oracle SQL
- palvelimia ja laitteistoja seuraavilta valmistajilta: Dell, Hewlett Packard, Cisco, Foundry Networks
- APC-varavirtajärjestelmät
- NetBotz-ympäristönvalvontatuotteet
- muisti, kaistanleveys, levytilan määrä, prosessori ja akut

(IPMONITOR CORPORATION 2006.)

IpMonitor voi antaa ilmoituksen määritellyille henkilöille SMS-viestinä (Short Message Service), puhelinsoittona, sähköpostitse tai hakulaitteeseen. Ilmoitus voi tulla esimerkiksi palvelutason alenemisesta, virheistä tai erikseen määritellyistä tapahtumista. IpMonitor voi virheen tapahtuessa yrittää korjata tilanteen käynnistämällä uudelleen virhetilaan joutuneen sovelluksen, Windows-palvelun tai itse laitteen, jossa virhetila ilmeni. Se voi myös ajaa ulkoisia sovelluksia ja ajaa korjauskomentoja. (IPMONITOR CORPORATION 2006.)

IpMonitor mahdollistaa reaaliajassa tulevat raportit sekä yksityiskohtaisen raportin aiemmin tapahtuneista asioista. IpMonitor ei tarvitse agenttia valvotulle palvelulle, ja se on nopea asentaa ja ottaa käyttöön. IpMonitorilla on oma konfiguraatiota varten tehty opastus, jonka avulla on helppoa käyttää verkkotarkistusta ja löytää valvottavat laitteet ja palvelut. (IPMONITOR CORPORATION 2006.)

IpMonitor tarjoaa graafisen, selainpohjaisen käyttöliittymän, jonka avulla on mahdollista hallita tehtäviä, käynnistää uudelleen palveluja ja palvelimia ja konfiguroida valvontaa paikasta riippumatta (IPMONITOR CORPORATION 2006).

IpMonitorin avulla voi hoitaa laaduntarkkailua esimerkiksi SQL-tietokannoilla, sähköposti- ja verkkopalvelimilla sekä sovelluksilla. IpMonitorissa on sisäänrakennettuna SNMP-työkalut ja ohjeistus, jotta tarkkailu SNMP:n avulla olisi helppoa esimerkiksi reitittimissä. (IPMONITOR CORPORATION 2006.)

3.2 FortN

FortN on BaseNin vuonna 2001 julkistama palvelualusta. FortN on kerroksista riippumaton verkonvalvontapalvelu, ja sen arkkitehtuuri mahdollistaa hyvän skaalautuvuuden ja joustavuuden. (BaseN Corporation 2006.)

FortN tarjoaa tapahtumakorrelaatiota, tapahtumien hallintaa ja automaattisia hälytyksiä, joiden avulla virheistä saadaan nopeasti tieto. Sovellus tarjoaa myös ennustetyökalut, jotka auttavat suunnittelemaan verkon tulevia tarpeita. FortN mittaa dataa, käsittelee datan ja esittää datan lyhytsanaisesti ja ymmärrettävässä muodossa. (BaseN Corporation 2006.)

3.3 Cacti

Cacti on valvontaohjelma, joka tallettaa tarvittavat tiedot luodakseen graafeja ja lisää ne MySQL-tietokantaan. Sillä tarkkaillaan esimerkiksi verkossa kulkevaa liikenteen määrää. Käyttäjä voi syöttää Cactiin reitit ulkoisiin komentosarjoihin ja muihin komentoihin, joita käyttäjän täytyy lisätä. Cacti kerää annetut tiedot ja luo ne MySQL-tietokantaan. (The Cacti Group 2006.)

Cactilla voi luoda lukemattoman määrän graafeja verkon tilasta. Cacti kerää lähteistä omien työkalujen avulla dataa, joka sitten muutetaan graafiseen muotoon. Cactissa on myös SNMP-tuki, ja se voi käyttää PHP-SNMP:tä, UCD-SNMP:tä ja NET-SNMP:tä. Datan jäljittäminen on myös mahdollista SNMP:n avulla tai komentosarjan etsiminen indexin avulla. (The Cacti Group 2006.)

Käyttäjäkohtainen hallinta antaa mahdollisuuden luoda käyttäjiä ja antaa niille erikäyttötasoja, joilla päästä Cactin käyttöliittymään. Käyttötasot voi määritellä käyttäjille jokaisella graafilla erikseen, ja jokainen käyttäjä voi laittaa omat asetuksensa. (The Cacti Group 2006.)

4 NAGIOS

4.1 Yleistä Nagioksesta

Nagios on suosittu vapaan lähdekoodin järjestelmä, joka suorittaa verkon-valvontaa. Nagios tarkkailee määritettyjä isäntäkoneita ja palveluita ja ilmoittaa tapahtuvista muutoksista. Nagios tulee alun perin nimestä Netsaint. Nagioksen on tehnyt ja sitä ylläpitää Ethan Galstad apunaan suuri määrä kehittäjiä. Nagios on suunniteltu toimimaan Linuxilla, mutta se toimii muillakin Unix-järjestelmillä. Nagios on lisensoitu GNU (GNU's Not Unix) versio 2:lle, ja sen on julkaissut Free Software Foundation. Tämä antaa mahdollisuuden kopioida, jakaa ja muuttaa Nagiosta tietyin lisenssissä määrätyin ehdoin. (Galstad 2006.)

Nagioksella on paljon ominaisuuksia:

- verkkopalveluiden monitorointi seuraavien palveluiden osalta: SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol version 3), HTTP (HyperText Transfer Protocol), NNTP (Network New Transfer Protocol), ICMP, SNMP
- resurssien monitorointi (prosessorikuorma, levynkäyttö, järjestelmälokit) suurimmalle osalle verkkojärjestelmistä
- etämonitorointi kryptattujen SSH (Secure SHell) ja SSL (Secure Sockets Layer) -tunneleiden avulla
- yksinkertainen plugin-järjestelmä, joka mahdollistaa käyttäjän kehittämään omia palvelutarkastuksia
- rinnakkaiset palvelutarkastukset
- verkkolaitteiden hierarkiamääritykset, jossa on mahdollista erottaa palvelut, jotka ovat kaatuneet niistä, joihin ei saada yhteyttä
- mahdollisuus lähettää ilmoitus esimerkiksi sähköpostitse, hakulaitteelle, tai tekstiviestillä ongelmista
- mahdollisuus ajoittaa tapahtumia, mikä auttaa proaktiivisessa ongelmanratkonnassa
- automaattinen lokitiedostojen kierto

- vapaaehtoinen selainkäyttöliittymä esimerkiksi verkon tilanteen näyttämiseksi, muistutuksille ja lokitiedostoille.

(Galstad 2006.)

Jos selaimelle tarkoitettu käyttöliittymä halutaan ottaa käyttöön, tarvitaan siihen WWW-palvelin (mieluiten Apache) ja Thomas Boutellin GD-kirjaston(Graphics Draw) versio 1.6.3 tai uudempi. Tämä tarjoaa CGI:lle (Common Gateway Interface) eli käyttöliittymälle sen vaatimia ominaisuuksia. (Galstad 2006.)

4.2 Nagioksen toiminta

Nagios on yksinkertainen ohjelma. Nagios ei sisällä itsessään muuta kuin valmiin pohjan. Erilaisia toimintoja Nagiokselle saa erillisten pluginien avulla. Pluginit ovat käännettyjä suoritettavia sovelluksia tai skriptejä, joita voi ajaa komento-riviltä esimerkiksi tarkistamaan palvelimen tilanteen. Nagios käyttää plugineja määrittääkseen palvelun tason ja on ilman niitä tarpeeton. (Galstad 2006.)

Nagioksen plugineja tuotetaan SourceForgessa, joka on maailman suurin avoimen lähdekoodin ohjelmistokehittäjien yhteisö. Sieltä löytyy myös ohjeet, joiden avulla käyttäjä voi itse helposti tuottaa omia plugineja ja näin ollen palveluja sekä tarkistuksia Nagioksella. (Galstad 2006.)

Nagioksen avulla pystyy siis valvomaan käytännössä mitä tahansa. Jos valvonnan saa prosessiksi ja ohjelmaksi, voi valvonnan hoitaa Nagioksen avulla. On kehitetty jo paljon valmiita ulkoisia ohjelmia, jotka valvovat esimerkiksi prosessorin kuormaa, viivettä tai muistin käyttöä. Omien ohjelmien teko on tietenkin myös mahdollista. (Galstad 2006.)

Päätarkoitus Nagioksella on tarkkailla palveluja, jotka pyörivät fyysisillä isäntäkoneilla ja -palvelimilla. Jos kone tai palvelin kaatuu, kaikki sen tarjoamat palvelut kaatuvat myös. Jos koneelle tai palvelimelle ei saada yhteyttä, ei Nagios myöskään voi tarkkailla sen palveluita. (Galstad 2006.)

Kun jokin palvelu ei läpäise Nagioksen tarkistusta, se yrittää tarkistaa onko viallinen palvelu ”elossa”. Tyypillisesti se lähettää ping-kyselyjä palvelimelle ja tarkistaa, saako se vastauksia. Jos vastauksia ei tule, niin Nagios olettaa palvelimen olevan alhaalla. Silloin Nagios lopettaa kaikki mahdolliset hälytykset kyseisen palvelimen palveluihin ja ilmoittaa yhteyshenkilöä/yhteyshenkilöitä siitä, että palvelin on kaatunut tai ei vastaa. Jos Nagios saa vastauksen ping-kyselyyn, saa se tiedon siitä, että itse palvelin on kunnossa ja lähettää ilmoituksen, että palvelussa on jokin häiriö. (Galstad 2006.)

Paikalliset koneet sijaitsevat samassa segmentissä Nagiosta pyörittävän koneen kanssa. Paikallisten koneiden välissä ei ole reitittimiä tai palomuureja. Jos jokin kone paikallisessa verkossa menettää yhteyden, on vika helppo kartoittaa, sillä välissä ei ole reitittimiä tai ulkoisia verkkoja. Jos Nagios haluaa tarkistaa paikallisen koneen, se lähettää tarkistuksen koneelle. Jos vastaus ei tule perille, nähdään heti, että kyseisessä koneessa on vika. (Galstad 2006.)

Etäkoneet sijaitsevat eri verkkosegmentissä kuin Nagios-kone. Jos Nagios ei voi monitoroida etäkonetta, täytyy sen selvittää, onko etäkone kaatunut vai eikö se saa yhteyttä etäkoneeseen. Jos etäkoneelle lähetetty tarkistus ei onnistu, niin Nagios lähestyy verkkosegmentti kerrallaan kohdetta. Tällä tavalla Nagios selvittää, onko etäkone kaatunut, onko jokin verkkoyhteys nurin, vai onko kyse palveluhäiriöstä. (Galstad 2006.)

Nagiokseen saa lisäosan nimeltä outage CGI. Outage CGI auttaa verkonvalvojaa löytämään verkostakohteet , jotka aiheuttavat eniten ongelmia. Tämä helpottaa verkonvalvontaa erityisesti isompien verkkojen osalta. Verkonvalvojan on helppoa alkaa ratkaista ongelmaa, kun hän tietää ongelmakohdat verkosta. Outage CGI näyttää siis kohteet, jotka aiheuttavat ongelmia sekä kohteet topologiassa, joihin ongelma etenee. (Galstad 2006.)

4.3 Nagioksen ilmoitukset

Nagios päättää tiedonantojen lähettämisestä palvelutarkistuksen ja palvelin-tarkistuksen yhteydessä. Ilmoitus lähtee, jos laitteen tai palvelun tila muuttuu. On myös mahdollista asettaa tiedoksiannot niin, että mikäli palvelin tai palvelu on ollut edellisestä ilmoituksesta esimerkiksi tunnin kaatuneena, lähettää se uuden ilmoituksen. Useimmiten asetukset pidetään kuitenkin niin, että ongelmasta lähtee vain yksi ilmoitus. (Galstad 2006.)

Nagiokselle luodaan erikseen yhteyshenkilöryhmiä. Jokaisella palvelulla on määritelty oma yhteyshenkilöryhmänsä, jolloin voidaan määrätä, kenelle lähtee ilmoitus aina tietyn laitteen tai palvelun ongelmasta. Kun ongelma ilmenee jossain palvelussa, lähettää Nagios jokaiselle kyseisen palvelun yhteyshenkilöryhmässä olevalle valvojalle ilmoituksen. (Galstad 2006.)

Nagiokseen saa monta eri tapaa ilmoituksien lähettämiseen. Jokainen tarvitsee kuitenkin oman tarvittavan ohjelmistonsa ja konfiguraationsa toimiakseen. Mahdollisia ilmoitustapoja ovat sähköposti, hakulaite, SMS-viestit, WinPopup-viestit, Yahoo, ICQ (”I seek you”), MSN (Microsoft Network) ja äänivaroitukset. (Galstad 2006.)

Tiedonannoilla on myös oma suodatusjärjestelmänsä. Vaikka Nagiokselle tulisikin tarve lähettää ilmoitus yhteyshenkilöille, täytyy ilmoituksen vielä läpäistä monta suodatinta. Suodattimina ovat esimerkiksi ohjelmasuodatus, aikasuodatus ja henkilökohtainen suodatus. Ohjelmasuodatus on ensimmäinen suodatus, ja sen voi kytkeä päälle pääkonfigurointitiedostosta tai graafisen käyttöliittymän kautta.

Mitään suodatuksia ei lähetetä eteenpäin ilman ohjelmasuodatusta. Aika-suodatuksessa määritetään, milloin suodatuksia lähetetään. Henkilökohtaisessa suodatuksessa määritetään, mitkä ilmoitukset lähetetään kenellekin yhteys-henkilölle.(Galstad 2006.)

4.4 Palvelimien ja palveluiden tila

Nagios päättää palvelinten ja palvelujen tilan kahdella eri tavalla. Toinen on niiden asema, eli ovatko ne OK, varoituksessa, ylhäällä, vai alhaalla. Toinen tapa on niiden tila. Nagioksella on kaksi tilaa: ”Soft” ja ”hard". Nämä päättävät tapahtuma-käsittelyistä ja ilmoituksien lähettämisistä, joten ne ovat tärkeä osa Nagiosta. (Galstad 2006.)

Ennenkuin Nagios päättää, että palvelimella tai palvelulla on vakava ongelma, se tekee tietyn määrän tarkistuksia niihin. Tämä tehdään väärien hälytyksien eliminoimiseksi. Tarkistusten määrä voidaan asettaa <max_check)attempts> -kohtaan palvelu- ja palvelinmäärityksissä. Tila riippuu siitä, millainen tarkistus on menossa. (Galstad 2006.)

Käyttäjä voi itse määrätä mitä tapahtuu, jos palvelu tai palvelin käy läpi lievää virhetilaa tai lievän virhetilan palautusta. Ne voidaan esimerkiksi kirjoittaa lokiin, jos se on asetettu ”log service retries” tai ”log host retries” kohtiin pääkonfigurointi-tiedostossa. On myös mahdollista määrätä tapahtumakäsittelyjä lievän virhetilan koittaessa. Nagios ei lähetä mitään ilmoitusta yhteyshenkilöille lievistä virhetiloista, sillä palvelimilla tai palveluilla ei ole niissä vielä mitään todellista hätää. Lievien virhetilojen aikana tapahtumakäsittelyt ovat tärkeässä osassa, sillä niiden avulla voidaan korjata ongelma, ennen kuin se muuttuu vakavaksi. (Galstad 2006.)

Nagios tarkkailee tilannetta, ja mikäli vakavaa tilanmuutosta ei tapahdu ja palvelu tai palvelin on yhä ei-OK tilassa, niin siitä ilmoitetaan yhteyshenkilöille uudelleen tietyn ajan kuluessa, mikäli niin on määritelty (Galstad 2006).

5 ZABBIX

5.1 Yleistä Zabbixista

Zabbixin on alun perin kehittänyt Alexei Vladishev. Kyseessä on ilmainen 24x7 valvontaohjelma, joka voi valvoa lukemattomia määriä palvelimia ja verkon tilaa. Zabbix tarjoaa nopeaa reagointia palvelinongelmiin ja ilmoittaa niistä valvojille. Tarjolla on myös raportointi ja datan visualisointi. (ZABBIX SIA. 2006.)

Zabbixin raportteihin ja statistiikkaan pääsee käsiksi selainpohjaisen käyttöliittymän avulla. Myös konfiguraatioparametrit onnistuvat tätä kautta. Selainpohjainen käyttöliittymä mahdollistaa verkon ja palvelimien tilan tarkkailemisen mistä tahansa. Ohjelma sopii sekä pienille että suurille yrityksille. (ZABBIX SIA. 2006.)

Zabbix on julkaistu GPL (General Public License) alla, joten sen lähdekoodia voi vapaasti kuka tahansa jakaa eteenpäin. Zabbixille tarjotaan sekä ilmaista että mainostuksellista tukea. (ZABBIX SIA. 2006.)

Zabbix tarjoaa seuraavia ominaisuuksia:

- tukee sekä polling, että trapping-mekanismeja
- palvelinohjelmisto seuraaville alustoille: Linux, Solaris, HP-UX (Hewlett Packard UniX), AIX (Advanced Interactive eXecutive), Free BSD (Berkeley Software Distribution), Open BSD, sekä OS X (Operating System)
- clientit seuraaville alustoille: Linus, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP
- palvelimien valvonta ilman agentin asennusta
- salattu käyttäjän autentikointi
- joustavat käyttäjäsäännöt

- selainpohjainen käyttöliittymä
- joustava sähköpostin kautta toimiva ilmoitusjärjestelmä ennakoiduille tapahtumille
- korkean tason (kaupallisen) näkymä valvonnasta

(ZABBIX SIA. 2006.)

Syitä Zabbixin käytölle:

- vapaan lähdekoodin ratkaisu
- erittäin tehokkaat agentit UNIX ja WIN32 alustoille
- matala oppimisaste
- korkea ROI (Return Of Investment), sillä kaatuneet palvelimet ja palvelut tulevat kalliiksi
- matala omistajamaksu
- yksinkertainen konfigurointi
- keskitetty valvontajärjestelmä. Kaikki konfiguraatiot ja suoritusdatat tallennetaan säännöllisesti tietokantaan.
- tuki SNMP:lle (v1, v2). Sekä polling että trapping.
- kyky visualisoinnille

(ZABBIX SIA. 2006.)

5.2 Zabbixin toiminta

Tärkein Zabbixin ominaisuus on suorituskyvyn valvonta. Se valvoo esimerkiksi prosessorin kuormaa, pyörivien prosessien lukumäärää, levyn aktiviteettia, näennäismuistin (swap space) tilaa ja muistin käyttöastetta. Zabbix tarjoaa ajoitetun järjestelmänvalvonnan, joka antaa tietoa palvelimista. Se voi myös luoda kuvaajia, jotta voidaan selvittää mahdolliset verkon ongelma-alueet. Tämä auttaa myös järjestelmänvalvojaa suunnittelemaan seuraavia laitteistopäivityksiä. (ZABBIX SIA. 2006.)

Järjestelmän valvoja voi käyttää monenlaisia lausekkeita, jotka määrittävät, milloin Zabbix lähettää ilmoituksen järjestelmästä. Kun jokin lauseke saa positiivisen tai negatiivisen arvon, lähettää Zabbix sähköpostilla tiedon sähköpostiosoitteisiin, jotka järjestelmänvalvoja on määritellyt. Erillisillä ulkoisilla ohjelmilla on mahdollista määrittää Zabbix lähettämään ilmoituksia myös SMS-viesteinä ja soittohälytyksinä. (ZABBIX SIA. 2006.)

Zabbixin keskitetty läyttöliittymä valvoo palvelimien lisäksi myös kriittisiä konfiguraatiotiedostoja, binäärejä, kerneliä, scriptejä ja HTML-palvelimen (HyperText Markup Language) sivuja. Valvoja saa siis myös ilmoituksen, jos johonkin näistä tehdään muutoksia. Kaikki valvotut parametrit myös talletetaan tietokantaan mahdollista myöhempää käyttöä varten. Yksi tärkeä osa Zabbixia on sen mahdollisuus valvoa myös SLA–sopimuksia (Service Level Agreement), joita palvelin- ja palveluntarjoaja voi tehdä jokaisen asiakkaan kanssa. Se pitää yllä dataa, joka helpottaa verkon heikkojen kohtien tunnistamista. (ZABBIX SIA. 2006.)

Sidokset ovat tärkeitä palvelin- ja palveluntarjoajalle. Jos esimerkiksi palvelin A kaatuu, voi se vaikuttaa esimerkiksi palveluihin B, C ja D. Zabbix valvoo myös sidoksia, eli se voi näyttää esimerkiksi, mistä kaikesta Web-palvelin on riippuvainen. Mahdollisia ovat esimerkiksi prosessorikuorma palvelimessa, verkkoyhteys ja levykoko. (ZABBIX SIA. 2006.)

Zabbix käsittelee aikakatkaisuja sekä verkon virheitä. Zabbixin voi konfiguroida tekemään jaksollisesti kyselyjä SNMP-agenteille ja Zabbixille, jotta saadaan päivitettyä tietoa suorituskyvystä ja yhteyksistä. Jos aikakatkaisua ei kyselyssä tapahdu, ottaa Zabbix yhteyden agenttiin, kysyy tarvitut tiedot, vastaanottaa datan, sulkee yhteyden ja prosessoi vastaanotetun informaation. (ZABBIX SIA. 2006.)

Jos kuitenkin aikakatkaisu tapahtuu, niin Zabbix kirjaa sen ylös, odottaa määritetyn ajan (joka on oletuksena 15 sekuntia) ja yrittää uudelleen. Kun palvelimeen ei ole saatu määritettyyn aikaan mennessä (oletuksena 45 sekuntia) yhteyttä, muuttuu palvelimen tila Zabbixin mukaan tavoittamattomaksi (UNREACHABLE). Kun palvelimeen ei saada yhteyttä tarpeeksi pitkään aikaan, muuttuu palvelimen tilaksi saavuttamattomaksi (UNAVAILABLE). (ZABBIX SIA. 2006.)

6 LÄHTÖKOHTA VERTAILULLE

6.1 Nykytilanne

HTK NetCommunication Oy:llä on käytössään useita verkonvalvontasovelluksia. Tärkeimmät sovellukset ovat IpMonitor, FortN ja Cacti. Myös telnet-protokollaa käytetään avuksi yrityksen verkonvalvonnassa. IpMonitor, FortN ja Cacti valvovat yrityksen palvelimia ja palveluita helpottaen verkonvalvojien tehtäviä. Jokaisella näistä sovelluksista on omat hyvät ja huonot puolensa. Tämän työn tavoitteena on löytää sovellus, jossa yhdistyisi kaikkien alkuperäisten sovelluksien hyvät puolet mahdollisimman hyvin.

IpMonitor on yksi HTK NetCommunication Oy:n valvontaohjelmistoista. IpMonitor valvoo esimerkiksi reitittimiä ja palvelimia. Taulukossa 3 käydään läpi IpMonitorin hyvät ja huonot puolet.

TAULUKKO 3. IpMonitor-ohjelman hyvät ja huonot puolet.

IpMonitor	
Hyvät puolet	Huonot puolet
Käyttöliittymä on helppokäyttöinen Laaja tuki erilaisille kohteille Toimiva Yksinkertainen	Ei kunnollista raportointitoiminnallisuutta Ei voi tehdä asiakaskohtaisia näkymiä

FortN-järjestelmää käytetään lähinnä palvelimien valvontaan käyttöjärjestelmätasolla. FortN-järjestelmä on hidas reagoimaan tapahtumiin, sillä se pyrkii suodattamaan turhia hälytyksiä. Taulukossa 4 käydään läpi FortN-järjestelmän hyvät ja huonot puolet.

TAULUKKO 4. FortN-järjestelmän hyvät ja huonot puolet.

FortN-järjestelmä	
Hyvät puolet	Huonot puolet
Valvonta ja raportointi on yhdistetty Raportointi on kattava Voidaan toteuttaa asiakaskohtaisia näkymiä Kohteet näkyvät kartalla niiden sijaintien mukaan Kohteiden massalisäykset mahdollisia	Vaikea käyttöliittymä (wiki-pohjainen) Monimutkainen Hidas reagointiaika (15-30 min) Raportointien kuvaajat voisivat olla selkeämpiä

Cacti-raportointijärjestelmällä HTK NetCommunication Oy valvoo lähinnä IP-runkoverkon kuormitusasteita. Taulukossa 5 käydään läpi Cacti-raportointijärjestelmän hyvät ja huonot puolet.

TAULUKKO 5. Cacti-raportointijärjestelmän hyvät ja huonot puolet.

Cacti-raportointijärjestelmä	
Hyvät puolet	Huonot puolet
Hyvät kuvaajat raportointiin Yksinkertainen käyttöliittymä Voidaan valvoa mitä tahansa SNMP-kohdetta Modulaarinen	Valvonta puuttuu Ei voi tehdä asiakaskohtaisia näkymiä

6.2 Vaatimukset uudelle järjestelmälle

HTK NetCommunication Oy tarvitsee sovelluksen, joka yhdistäisi mahdollisimman hyvin jo käytössä olevien valvontasovellusten hyviä puolia. Esimerkiksi helppokäyttöisyys ja yksinkertaisuus, kattava raportointi ja kohdetuki, asiakaskohtaiset näkymät ja mahdollisuus kuvaajiin ovat ominaisuuksia, joita uudelta sovellukselta haetaan. Valittavan sovelluksen tulee siis olla monipuolinen ja sen tulee vastata yrityksen tarpeita.

Helppokäyttöisyys ja yksinkertaisuus ovat tärkeitä ominaisuuksia, sillä verkonvalvojilla ei ole aikaa tutustua liian monimutkaiseen sovellukseen. HTK NetCommunication Oy tarvitsee myös kattavan raportoinnin ja hyvät kuvaajat, joista näkyy selvästi esimerkiksi palvelujen ja palvelimien toimivuustaso. Asiakaskohtaisien näkymien mahdollisuus on tärkeä ominaisuus, sillä sen avulla verkonvalvoja voi tarkkailla esimerkiksi yhden asiakkaan kaikkia palveluja helposti.

7 VERTAILTAVIEN SOVELLUSTEN ASENNUS

7.1 Työn aloittaminen ja perusvaatimukset

Työn ensimmäinen vaihe oli tutustuminen sovellusten perusvaatimuksiin. Pienen tutkimisen jälkeen oli selvää, että molemmat sovellukset vaativat mieluiten unix-pohjaisen käyttöjärjestelmän. Oli siis löydettävä sopiva käyttöjärjestelmä työ-alustaksi, jonka päälle itse sovellukset tulisivat. Tutustumisvaiheessa on tärkeää, että käyttöjärjestelmä on jollakin tapaa tuttu. Muuten jo pelkän käyttöjärjestelmän oppimiseen kuluisi liikaa aikaa.

Valitettavasti kokemus Unix-käyttöjärjestelmistä oli hyvin rajallinen, mutta muutaman kurssin avulla oli saatu alustava kuva Ubuntu-käyttöjärjestelmästä. Ubuntu on vapaista ohjelmistoista koostuva ilmainen käyttöjärjestelmä, jossa on suomalaislähtöinen Linux-ydin. Ubuntu siis valittiin sovellusten tutustumis-vaiheessa käytettäväksi käyttöjärjestelmäksi.

Työssä käytettiin opinnäytetyön tekijän omaa kannettavaa Fujitsu-Siemens–merkkistä kannettavaa kotitietokonetta. Kannettavassa tietokoneessa oli ennen Windows XP Pro –käyttöjärjestelmä, joka vaati jo ennestään uudelleenasennusta, joten kiintolevyt päätettiin tyhjentää ja asentaa pelkkä Ubuntu-käyttöjärjestelmä kannettavan tietokoneen kiintolevyille.

Asennuksen alku sujui hyvin, mutta pian asennuksen aikana tapahtuvan kiinto-levyjen alustuksen jälkeen Ubuntun ladatessa koneelle tarvittavia paketteja tietokone lopetti lataamisen täysin. Puolen tunnin odottelun jälkeen asennus oli yhä samassa kohdassa, joka vahvisti ongelman. Pienen tutkimisen jälkeen selvisi, että joko Ubuntun suomalaisilta sivuilta haetussa levykuvassa oli jotain vikaa tai sitten levykuvan poltto-prosessissa tyhjälle cd-levylle oli tapahtunut virhe. Levy-kuva poltettiin uudelleen toiselle tyhjälle levylle, mutta asennus jäi yhä samaan kohtaan. Ubuntun virallisilta sivuilta löytyi ShipIt-palvelu, jonka kautta pystyi tilaamaan ilmaiseksi kotiin kuljetettuna Ubuntun 6.06 LTS-version (Long Term Support). Alle viikon kuluessa saapui viisi Ubuntu 6.06 LTS –versiota valmiiksi poltettuna, ja asennus vanhan 6.06 LTS -version kanssa meni ensimmäisellä yrittämällä läpi. Kotona tehtävässä vertailutyössä päätettiin siis käyttää 6.06 LTS versiota Ubuntusta.

7.2 Nagioksen asennus

Ensimmäisenä kahdesta vertailtavasta sovelluksesta yritettiin asentaa Nagiosta. Nagioksen sivuilta löytyi ohjeet ohjelman asennusta varten, jossa kerrottiin pää-vaiheet läpi, mitä asennuksessa tapahtuu. Pian kävi selväksi, että asennus ei ole suoraviivaista, ja että riippuen päätteestä ja käyttöjärjestelmästä poikkeuksia löytyy paljonkin. Internetin keskustelupalstat ovat kuitenkin täynnä käyttäjien ohjeita ja kokemuksia ohjelman asennuksesta, joten niistä sai hieman apua ongelmiin. Suurin osa ongelmista johtui Linux-käyttöjärjestelmien vähäisestä tuntemuksesta, minkä takia kaikkia tehtyjä komentoja ja muutoksia ei aina suoralta kädeltä ymmärtänyt. Koulussa oli kuitenkin syksyn ja talven ajan käynnissä Tietoverkkojen erikoistyö –kurssi, jonka sisältönä oli Ubuntu-käyttöjärjestelmän asentaminen Virtual PC –ympäristöön (Personal Computer) ja erilaisiin Linux-toimintoihin tutustuminen. Tämä kurssi lisäsi tietoa Unix-käyttöjärjestelmistä ja niihin liittyvistä toiminnoista, mikä puolestaan auttoi ymmärtämään Nagioksen asentamisessa tarvittavia komentoja ja muutoksia paremmin.

Nagios vaati toimiakseen Linux-pohjaisen käyttöjärjestelmän ja C-ohjelmointikielen kääntäjän. Ohjelma mahdollistaa myös http-selaimen avulla katsottavan käyttöliittymän, jota varten Ubuntuun piti asentaa mieluiten Apache-palvelinohjelma sekä Thomas Boutell'n GD-kirjaston versio 1.6.3 tai uudempi, jota http-pohjaisen käyttöliittymän ominaisuudet vaativat.

Itse asennus tapahtui normaaliin Linux-käyttöjärjestelmille ominaiseen tapaan omine sovelluskohtaisine lisäyksineen. Ensimmäisenä haettiin sovelluksen uusin versio sen sivuilta. Versio oli pakattuna, joten ensimmäisenä pakattu tiedosto purettiin. Käyttö-järjestelmään luotiin oma käyttäjänsä ja oma ryhmänsä. Tämä käyttäjä ja ryhmä laitettiin omistajaksi Nagios-kansiolle, jonne sovellus asennettiin.

Ulkoisia komentoja varten piti tunnistaa Apache-palvelimen käyttäjä, joten luotiin uusi ryhmä, joka sisälsi Nagios-käyttäjän ja Apache-palvelimen käyttäjän. Ainoastaan tämän uuden ryhmän jäsenet pääsevät hallinnoimaan Nagiosta.

Konfiguraatio-skriptillä alustettiin tarvittavat muuttujat. Komento make all käänsi binäärit ja make install asensi binäärit sekä HTML-tiedostot. Binäärit ja HTML-tiedostot sisälsivät dokumentaatiot ja pääsivun. Selainkäyttöliittymä piti konfiguroida erikseen Apacheen, jotta se osasi avata selaimessa juuri Nagioksen. Tämän jälkeen täytyi tarkastaa, että vain oikeat käyttäjät pääsevät käsiksi sovellukseen.

Nagioksen asennuksessa tuli paljon virheilmoituksia ja ongelmia, mutta niihin selvisi syy tutkimalla virheilmoitusta tarkemmin. Verkosta löytyi myös muutaman käyttäjän laatima ohje Nagioksen asentamiseen, joiden avulla asennus saatiin menemään loppuun asti.

Koska pelkän Nagios-sovelluksen mukana tulee vain sovelluksen runko, tarvitsee se erillisiä laajennuksia eli plugineja. Pluginit hoitavat Nagioksessa kaikki toiminnot ja tarkkailut ja itse ohjelma tulostaa ne käyttäjälle selainkäyttöliittymään. Riippuen valvottavista palvelimista ja palveluista, Nagiokselle täytyy etsiä tai kehittää itse sopivat pluginit. Tämä tekee Nagioksesta erittäin monipuolisesti muokattavan, sillä itse pääsovellusta ei tarvitse muokata, jos haluaa esimerkiksi itse kehittää jonkin uuden toiminnon. Tällainen ominaisuus tuo toisaalta Nagioksen hallittavuudelle haastetta, sillä uuden käyttäjän ei ole välttämättä helppoa löytää juuri hänelle sopivaa laajennusta. Nagioksen saattaminen toimintakuntoon vie aluksi aikaa valvojalta verkosta riippuen jopa todella paljon. Tämän jälkeen valvonnan pitäisi teoriassa kuitenkin toimia helposti.

7.3 Zabbixin asennus

Zabbixin sivut sisälsivät myös sovelluksen dokumentaation, missä kerrottiin sovelluksen vaatimuksista. Se toimii usealla eri alustalla, kuten Linux 2.xx, Solaris 2.xx ja Mac OS/X. Käytössä on kuitenkin jo Linux-käyttöjärjestelmä, joten myös Zabbix päätettiin asentaa Ubuntu 6.06 LTS version alle. Zabbix vaati myös Apache-palvelinohjelman version 1.3.12 tai uudemman, MySQL-tietokannan version 3.22 tai uudemman, PHP-moduulin (PHP Hypertext Preprocessor), jotta se ymmärtää PHP-kieltä, HTTP-selaimen, NET-SNMP-kirjaston ja binäärit sekä Open-SSL-kirjaston ja sen binäärit.

MySQL:n sijasta on mahdollista käyttää vaihtoehtoisesti PostgreSQL-olio-relaatiotietokantapalvelinohjelmistoa, mutta MySQL:n käyttöä suositellaan, koska se on jopa kymmenen kertaa nopeampi kuin PostgreSQL.

Zabbix koostuu:

1. Palvelimesta, joka valvoo verkon palveluita käyttäen yksinkertaisia tarkistuksia ja johon agentit voivat lähettää raportteja ja statistiikkaa.

2. Agentista, joka asennetaan valvottaviin palvelimiin. Se voi monitoroida esimerkiksi kiintolevyjä, muistia ja prosessoritehoja. Agentti kerää statistiikkaa määrätyistä ominaisuuksista ja lähettää ne palvelimelle.

3. Selainkäyttöliittymästä, joka mahdollistaa helpon näkymän valvonnalle.

Zabbixin asennus noudattaa paljonkin samaa kaavaa kuin muiden Linux-sovellusten, kuten esimerkiksi Nagioksen. Zabbixin asennus sisältää tietysti sovelluskohtaisia eroja. Ensin Zabbixille luodaan käyttäjä, jonka alla Zabbix-palvelin pyörii. Tässä vaiheessa täytyy muistaa, ettei Zabbixin käyttäjäksi aseta root- eli pääkäyttäjää, vaan sille on luotava oma käyttäjänsä.

Asennusta varten haetaan Zabbix-paketti ja puretaan se tietokoneelle. Zabbixille luodaan MySQL-tietokanta, sillä Zabbix käyttää SQL-skriptejä luomaan vaadittuja tietokantakaavoja. Konfiguraatio-skriptillä käännetään lähdekoodi järjestelmälle. Komento make install asensi kaiken. Kaikissa Zabbixin agenteissa, joissa zabbix_agent on asennettu, täytyy käydä konfiguroimassa etc/zabbix/zabbix_agent.conf –tiedostoa.

Jos palvelimia on yli kymmenen, niin suositellaan konfiguroitavaksi palvelimella /etc/zabbix/zabbix_server.conf –tiedostoa. Alle kymmenen tietokoneen valvomiseen pitäisi riittää oletusparametrit. Lopuksi ajetaan agentit ja palvelin päälle omilla komennoillaan ja konfiguroidaan selainkäyttöliittymä kuntoon.

Zabbixin asennus tuotti kuitenkin odottamattomia ongelmia, sillä ohjeiden mukaan tehty asennus tuotti paljon virheilmoituksia käyttöjärjestelmästä. Useimmiten virheet johtuivat joidenkin pakettien tai sidosten puuttumisesta, mutta välillä virhe-ilmoituksessa ei tullut ilmi tarkempaa syytä, mistä ongelma johtui.

Usean eri yrityksen jälkeen löytyi verkosta ohje, jossa Zabbix versio 1.1 on valmiina binääreinä, ja sen asennus onnistuisi suoraan asentamalla valmiit paketit ja peruskonfiguraatiot. Linux-käyttöjärjestelmään piti vain lisätä kirjastoihin lähde, josta käyttöjärjestelmä hakee kyseiset paketit. Tämäkään ohje ei kuitenkaan tuottanut tulosta, sillä ohje ja valmiit paketit oli suunnattu Debian-käyttöjärjestelmälle.

Lopuksi asennettiin Ubuntu 6.06 LTS –käyttöjärjestelmän päälle Debian-käyttöjärjestelmän uusin versio verkkoasennuksen avulla, jossa tarvitaan vain asennuslevyke, joka aloittaa käyttöjärjestelmän asennuksen, ja loput tarvittavat paketit haetaan suoraan internetistä.

Debianin asennuksen ja päivityksen jälkeen kokeiltiin jälleen hakea Zabbix versio 1.1 valmiina binääreinä ja asentaa se suoraan auttavien skriptien avulla. Tällä kertaa asennus meni ensimmäisellä yrittämällä läpi ja Zabbix-palvelin saatiin pyörimään. Samalle koneelle asennettiin myös Zabbix-client, eli asiakasohjelma, jonka avulla valvottiin tietokonetta, jossa itse Zabbix-palvelin oli asennettuna.

Zabbix on kokonainen sovellus, joka tarjoaa suoraan palvelimien ja palveluiden valvonnan. Siihen saa asetettua myös sähköpostiin tiedoksiannot määrätyistä tapahtumista ja ongelmista. Tämä tekee Zabbixista sovelluksen, joka on helppo oppia. Sen käyttö ei tarvitse aiempaa teknistä osaamista, mutta Unixin ymmärtäminen on kuitenkin oleellista.

8 VERTAILU

Nagios ja Zabbix ovat molemmat vapaan lähdekoodin sovelluksia, jonka vuoksi ne valittiin vertailun kohteiksi. Vapaan lähdekoodin sovelluksiin ei tarvitse maksaa käyttömaksua, ja sen muokkaus on mahdollista kenelle tahansa.

Yksi pääeroista Nagioksen ja Zabbixin välillä on se, että päinvastoin kuin Zabbixissa, Nagioksen mukana tulee vain pohja sovellukselle. Se tarvitsee erillisiä laajennuksia eli plugineja voidakseen tehokkaasti valvoa verkon palvelimien sekä palvelujen tilaa. Riippuen hallittavasta ja valvottavasta verkosta laajennuksia voi tulla suuri määrä. Jopa niin suuri, että on helpompaa valvoa useamman eri valvontasovelluksen avulla verkkoa, kuin asentaa aina uusi laajennus uudelle palvelulle.

Nagioksessa ja Zabbixissa on molemmissa omat hyvät sekä huonot puolensa. Riippuu täysin hallittavasta verkosta kumpi soveltuu paremmin käyttöön. Nagios on haastava sovellus konfiguroitavaksi, mutta kun kaiken on saanut kuntoon, on sen ylläpitäminen helppoa. Zabbix tarjoaa hyvän selainpohjaisen käyttöliittymän, jonka kautta sekä valvonta että konfigurointi onnistuu. Tämä tekee Zabbix-ohjelmasta käyttäjäystävällisemmän varsinkin, jos ajatellaan käyttäjiä, joilla ei ole aiempaa kokemusta valvontasovelluksista ja niiden toiminnasta, voi Zabbix olla parempi vaihtoehto. Nagioksessa konfigurointi joudutaan suorittamaan erikseen suoraan konfiguraatiotiedostoihin. Tämä taas voi olla jopa erittäin hankalaa ensikertalaiselle, jolloin käyttäjä voi mahdollisesti jopa luovuttaa ja vaihtaa sovellusta. Zabbix taas soveltuu paremmin ensikertalaiselle, kunhan hän tuntee ja ymmärtää Unix-järjestelmien toimintaa. IpMonitor-ohjelma on helppokäyttöinen ja se luetaan ehdottomasti positiiviseksi ominaisuudeksi HTK NetCommunication Oy:ssä. Yksi etsittävä ominaisuus uudelle ohjelmalle on helppokäyttöisyys, sillä verkonvalvojilla ei aina ole tarpeeksi aikaa tutkia vastaantulevia ongelmia, jotka johtuvat ohjelman vaikeaselkoisuudesta. Zabbix osoittautuu tämän ominaisuuden perusteella toimivammaksi ratkaisuksi kohdeyritykselle.

Yksi tärkeä ominaisuus valittaessa valvontaohjelmaa ovat nykyään kuvaajat. Kuvaajat kertovat monille enemmän kuin tuhat sanaa ja ovat helpompia ymmärtää kuin pelkät tekstipohjaiset lokit, varsinkin asiaan perehtymättömille. Zabbix tarjoaa suoraan kuvaajia, kun taas Nagioksen avulla se onnistuu yhäkin vain erillisten lisäosien avulla. Esimerkiksi nagiostat- ja NagiosGrapher-lisäosat tarjoavat mahdollisuuden kuvaajien laatimiseen. Alkuperäisistä sovelluksista Cacti ja FortN kykenevät luomaan kuvaajia raportointia varten, mikä on erittäin hyödyllinen ominaisuus valvonnan kannalta. Kuvaaja-ominaisuutta toivotaan uudelta valvonta-sovellukselta. Nagios ja Zabbix kykenevät molemmat luomaan kuvaajia, joten molemmat ohjelmat kävisivät sen ominaisuuden puolesta sopivaksi ohjelmaksi verkonvalvontakäyttöön HTK NetCommunication Oy:lle.

Zabbixilla on suoraan käytössä ominaisuus, jonka avulla tiettyjä palvelimia tai palveluita voidaan yhdistää tietyn nimikkeen alle. Tätä ominaisuutta voidaan käyttää apuna, kun halutaan asiakaskohtaisia näkymiä. Nagioksella asiakaskohtaiset näkymät saadaan toimimaan eri kirjautumistunnuksien tai henkilötietoryhmien avulla. Alkuperäisissä sovelluksissa vain FortN-järjestelmissä kyettiin asiakaskohtaisiin näkymiin, ja se on yksi ominaisuus, mitä uudelta ohjelmalta toivottaisiin käyttöön.

9 YHTEENVETO

Projekti aloitettiin epävirallisesti jo syksyllä 2006. Projektin aikana kuitenkin ilmeni paljon ongelmia, mikä aiheutti sen, että työ voitiin aloittaa kunnolla vasta joulukuussa 2006. Siihen saakka tutustuttiin lähinnä teoriaosuuteen ja Nagioksen ja Zabbixin kirjattuihin ominaisuuksiin.

Työssä saatiin yleiskuva kahdesta verkonvalvontasovelluksesta. Zabbix ja Nagios ovat molemmat ilmaisia, vapaan lähdekoodin järjestelmiä, joka oli perusteena valituille sovelluksille, jotka ovat vertailussa mukana.

Nagioksen etuna on sen suuri muokattavuus, sillä se on oletuksena pelkkä tyhjä kuori, ja kaikki toiminnallisuus tulee erillisten laajennuksien mukana, joita voi itsekin kehittää. Nagios on kuitenkin vaikeampi saattaa toimintakuntoon verkonvalvontaa varten varsinkin kokemattomalta verkonvalvojalta. Itse kuntoon saattaminen voi viedä todella paljon valvojan aikaa, mikä riippuu verkon suuruudesta ja valvotuista palveluista.

Zabbixin etuna on taas sen yksinkertaisuus, sillä valvonta ja hallinta tapahtuvat molemmat suoraan selainpohjaisen käyttöliittymän avulla. Se ei vaadi käyttäjältään aiempaa kokemusta verkonvalvonnasta tai verkonvalvonta-sovelluksista, mutta Unix-järjestelmien ymmärtäminen on kuitenkin oleellista. Zabbix on kokonainen sovellus, johon ei tarvita erillisiä laajennuksia, mikä tekee sovelluksen aloituskynnyksestä matalamman. Tämä kuitenkin aiheuttaa myös sen, että sovellus ei välttämättä ole aivan yhtä muokattavissa kuin Nagios.

HTK NetCommunication Oy haki ohjelmalta muun muassa seuraavia ominaisuuksia, joita arvostettiin alkuperäisissä valvontaohjelmissa:

- yksinkertainen käyttöliittymä
- voidaan toteuttaa asiakaskohtaisia näkymiä
- hyvät kuvaajat raportointiin
- monipuolinen.

Zabbix ja Nagios tarjoavat molemmat monipuolisen sovelluksen ja kuvaajia raportointia varten. Nagios tarvitsee kuitenkin erillisiä lisäosia palveluiden ja valvonnan toteuttamiseen, ja sillä on huomattavasti hankalampi käyttöliittymä kuin Zabbixilla. Zabbix taas tarjoaa yksinkertaisen ja helposti omaksuttavan käyttöliittymän verkonvalvojan käyttöön. Molemmat sovellukset ovat hyviä verkonvalvontasovelluksia, mutta tämän työn lähtökohtien perusteella Zabbix sopisi paremmin HTK NetCommunication Oy:n käyttöön erityisesti yksinkertaisen käyttöliittymänsä ansiosta.

Nagios olisi liian työläs valvontasovellus käyttöönottoa varten, sillä sen opettelu veisi paljon aikaa, jota verkonvalvojalla ei usein ole. Jos uusia kohteita tulisi lisättäväksi, tulisi ne lisätä Nagiokseen konfigurointitiedostojen avulla ja kohteesta riippuen Nagios voi tarvita aina uuden lisäosan, jotta osaisi valvoa uutta kohdetta kunnolla. Zabbixiin lisääminen tapahtuu nopeasti, eikä sovellukseen tarvitse etsiä uusia lisäosia uutta valvottavaa kohdetta varten.

Zabbix-sovelluksessa on automaattisesti mukana ominaisuus, jossa voidaan yhdistää palvelimet ja palvelut eri nimikkeiden alle. Tämä ominaisuus auttaa luomaan asiakaskohtaisia näkymiä, mikä oli yksi uudelle sovellukselle haettavista ominaisuuksista. Myös Nagiokselle voi varmasti tehdä samanlaisen ominaisuuden sisältämän lisäosan, jos sellaista ei valmiina löydy.

HTK NetCommunication Oy:n käyttöön suositellaan Zabbix-valvontasovellusta, sillä siitä löytyy niitä ominaisuuksia, joita yritys uudelta valvontasovellukselta etsii. Se on tarpeeksi yksinkertainen ja monipuolinen ja mahdollistaa asiakaskohtaiset näkymät ja kuvaajat raportteja varten. Ohjelmaa suositellaan lisäykseksi aiempien ohjelmien rinnalle, sillä se ei kykene täysin korvaamaan useaa alkuperäistä valvontasovellusta. Esimerkiksi kuvaajat voisivat olla hieman monipuolisemmat ja esimerkiksi kohteiden massalisäykset eivät onnistu yhtä hyvin kuin FortN-järjestelmällä. Zabbix toimisi hyvin alkuperäisten sovellusten rinnalla ja helpottaisi varmasti joidenkin ominaisuuksien valvontaa.

HTK NetCommunication Oy:n tarkoitus oli löytää verkonvalvontasovellus, joka voisi yhdistää aiemmin käytettyjen sovelluksien hyödyllisiksi todettuja ominaisuuksia. Uuden sovelluksen tehtävä olisi siis vähentää tarvittavien verkonvalvontasovelluksien määrää. Työssä vertailtiin Nagios ja Zabbix -sovelluksia, joista Zabbix onnistui paremmin yhdistämään vaadittuja ominaisuuksia. Zabbix ei kuitenkaan onnistu ominaisuuksiltaan tarpeeksi hyvin korvaamaan useampaa aiemmin käytetyistä sovelluksista, joten sitä suositellaan vain lisäykseksi aiempien sovelluksien rinnalle. Tästä syystä kumpaakaan vertailtavissa olevista sovelluksista ei luultavasti tulla ottamaan käyttöön, sillä verkonvalvontasovelluksien määrää halutaan laskea eikä nostaa.

Verkonvalvonta tulee esittämään tulevaisuudessa yhä tärkeämpää osaa yrityksissä. Tietoverkot ovat kasvattaneet suosiotaan niin paljon, että ne ovat yleensä tärkein osa yrityksen tiedonvälityksessä ja tiedon tallentamisessa. Yrityksien on pidettävä huolta siitä, että verkko toimii mahdollisimman hyvin. Verkonvalvonta helpottaa yrityksen verkon ylläpitoa huomattavasti. Jos jotain ongelmia ilmenee, on verkonvalvojien saatava siitä tieto mahdollisimman tehokkaasti, jotta viat voidaan korjata. Toimiva ja luotettava tietoverkko antaa hyvän kuvan yrityksestä mahdollisille asiakkaille sekä myös työntekijöille. Verkonvalvonta tulee olemaan tulevaisuudessa yksi kriittisimmistä osa-alueista yrityksen kannalta.

10 LÄHTEET

Ala-Mutka, K., Rintala, M., Savikko, V. & Palviainen, J. 2002. OSI-malli [verkkodokumentti]. [viitattu 20.1.2007]. Saatavilla: http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html

BaseN Corporation. 2006. The BaseN Platform Description [verkkodokumentti]. [Viitattu 30.12.2006]. Saatavilla: http://www.basen.net/europe/platform/operators_description.html

Cisco Systems, Inc., 2006, Simple Network Management Protocol [verkkodokumentti], [Viitattu: 1.3.2007]. Saatavilla: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

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

Galstad, E. 2006. Nagios ® version 2.x Documentation [verkkodokumentti]. [Viitattu 20.12.2006]. Saatavilla: http://nagios.sourceforge.net/docs/2_0/toc.html

Haikonen, J., Hlinovsky, J. & Paju,A. 2000. Verkonhallinta – SNMP [verkkodokumentti]. [Viitattu: 1.3.2007]. Saatavilla: http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/47/snmp.shtml

HTK NetCommunication Oy. 2007a. Esittely [verkkodokumentti]. [viitattu 20.1.2007]. Saatavilla: http://htknetcommunication.fi/index.htm

HTK NetCommunication Oy. 2007b. Palvelut ja tuotteet [verkkodokumentti]. [viitattu 20.1.2007]. Saatavilla: http://htknetcommunication.fi/palvelut.htm

IPMONITOR CORPORATION. 2006. Product Brief [verkkodokumentti]. [viitattu 15.1.2007]. Saatavilla: http://www.ipmonitor.com/pdf/ipMonitor8_Brief.pdf

Javvin Technologies, Inc. 2005a. SNMPv2: Simple Network Management Protocol version 2 [verkkodokumentti]. [Viitattu: 1.3.2007]. Saatavilla: http://wwww.javvin.com/protocolSNMPv2.html

Javvin Technologies, Inc. 2005b. SNMPv2: Simple Network Management Protocol version 3 [verkkodokumentti]. [Viitattu: 1.3.2007]. Saatavilla: http://www.javvin.com/protocolSNMPv3.html

Koljonen, J. 2007a. SNMP:n perusteet [verkkodokumentti]. [viitattu 10.2.2007]. Saatavilla: http://reppu.lamk.fi/ (vaatii kirjautumisen)

Koljonen, J. 2007b. Verkonhallinta ISO - OSI alueet [verkkodokumentti]. [viitattu 10.2.2007]. Saatavilla: http://reppu.lamk.fi/ (vaatii kirjautumisen)

Kotiharju, Asi. 1996. SNMP Verkonhallinta [verkkodokumentti]. [Viitattu: 1.3.2007]. Saatavilla: http://www.netlab.tkk.fi/opetus/s38116/1996/esitelmat/37651p/#SECTION00073000000000000000

Majorin, P. 2007. RFC 1156 – Summary [verkkodokumentti]. [Viitattu: 1.3.2007]. Saatavilla: http://www.tml.tkk.fi/Opinnot/Tik-110.350/Tehtavat/rfc/1156_1.html

Postel, J. 1980. RFC 768 – User Datagram Protocol [verkkodokumentti]. [viitattu 30.12.2006]. Saatavilla: http://www.faqs.org/rfcs/rfc768.html

Postel, J. 1981a. RFC 791 - Internet Protocol [verkkodokumentti]. [viitattu 30.12.2006]. Saatavilla: http://www.faqs.org/rfcs/rfc791.html

Postel, J. 1981b. RFC 792 - Internet Control Message Protocol [verkkodokumentti]. [viitattu 30.12.2006]. Saatavilla: http://www.faqs.org/rfcs/rfc792.html

Postel, J. 1981c. RFC 793 – Transmission Control Protocol [verkkodokumentti]. [viitattu 30.12.2006]. Saatavilla: http://www.faqs.org/rfcs/rfc793.html

Postel, J. & Reynolds, J. 1983. RFC 854 – Telnet Protocol Specification [verkkodokumentti]. [viitattu 30.12.2006]. Saatavilla: http://www.faqs.org/rfcs/rfc854.html

The Cacti Group. 2006. Features [verkkodokumentti]. [Viitattu 15.1.2007]. Saatavilla: http://cacti.net/features.php

ZABBIX SIA. 2006. ZABBIX Manual v1.1 [verkkodokumentti]. [Viitattu 21.12.2006]. Saatavilla: http://www.zabbix.com/manual/v1.1/